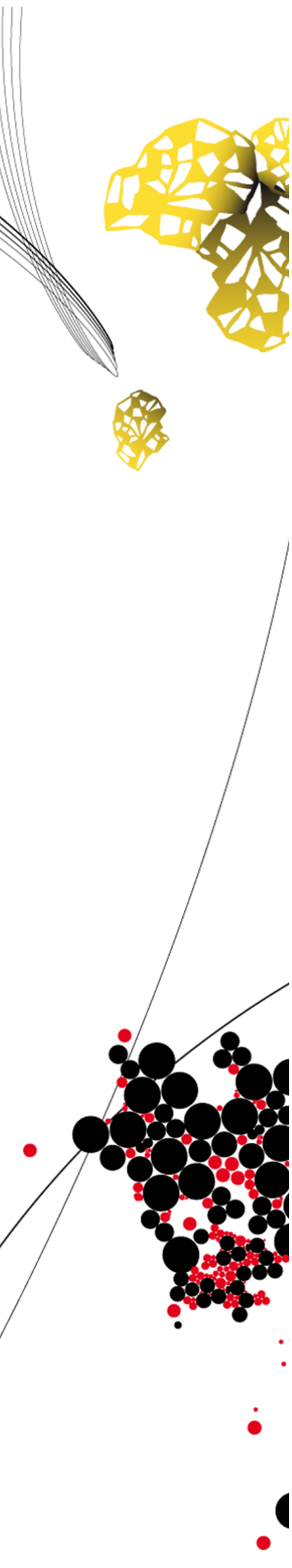


UNIVERSITY OF TWENTE.

Faculty of Electrical Engineering, Mathematics & Computer Science

Detecting Adaptive Data Exfiltration in HTTP Traffic

Thijs S. van Ede

Master Thesis
December 2017

Graduation committee:
Dr. A. Peter
R. Bortolameotti M.Sc.
Dr. M. H. Everts

Services Cyber Security & Safety Group
Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

Detecting Adaptive Data Exfiltration in HTTP Traffic

Thijs S. van Ede
University of Twente
Enschede, the Netherlands
t.s.vanede@student.utwente.nl

ABSTRACT

Our work introduces a new type of attack which adapts the network communication of an adversary such that it mimics communication of the applications active on an infected host. By doing so, the adversary aims to remain undetected by fully blending in with benign traffic. We demonstrate this novel attack through several case studies in which we created multiple variants of data exfiltrating malware, which adapt their communication to mimic the HTTP traffic of the browser application of the infected host. In addition, we introduce novel heuristics to detect adaptive data exfiltration and combine them in our Adaptive Browser-Imitating Data Exfiltration Detector (ABIDED). We compare our solution to DECANTeR [9] and DUMONT [38], two state-of-the-art detection mechanisms which detect covert communication over HTTP. Our analysis shows that ABIDED's performance is comparable to existing solutions in detecting existing exfiltrating communication. However, it greatly improves detection of adaptive exfiltration with a detection rate of 93.3% against 5.2% for DECANTeR and 23.2% for DUMONT. Moreover, our analysis shows that the false positive rate of ABIDED is significantly lower than that of the other systems, making it a powerful solution for detecting data exfiltration.

KEYWORDS

Adaptive Data Exfiltration, Anomaly Detection, Network Security

ACM Reference Format:
Thijs S. van Ede. 2017. Detecting Adaptive Data Exfiltration in HTTP Traffic. *Master Thesis, University of Twente.* Enschede, the Netherlands, 78 pages.

1 INTRODUCTION

The latest Gemalto Breach Level Index [22] reported an increase in data breaches of 164% over the last semester of 2017 compared with the same period in 2016. This increase suggests a growth of malicious communication over the network. This statement is supported by the surge of botnets using various internet protocols to send vast amounts of traffic to targeted machines [1]. Moreover, attackers regularly change their communication pattern to avoid being discovered by state-of-the-art detection systems [15].

In addition, the documents revealed by Snowden indicate the existense of malware developed by intelligence agencies [6]. Such state-sponsored malware is likely to be more sophisticated than average malware known to research communities. This stresses the importance of offensive security. Our research attempts to build more advanced attacks to predict future adversary capabilities.

Over the last decade, network-based mechanisms for detecting malware communication improved substantially [2, 9, 29, 38, 40]. We observe a shift from traditional signature-based detection to anomaly-based detection. In case of data exfiltration this signature-based detection is mostly executed by Data Leakage Prevention (DLP) systems [28] which analyse whether outgoing traffic contains known sensitive information. As stated previously, attackers try to obfuscate the data such that it cannot be detected by DLP systems. This introduced the need for anomaly-based detection mechanisms of covert communication [8, 9, 38]. These anomaly-based systems are able to cope with adversaries trying to remain undetected by obfuscating data. However, they fail to recognise that the attacker may also adapt its communication to conform to regular traffic.

To address this issue, we first present a taxonomy of different levels of covertness which an attacker is able to achieve on a network level, by using several building blocks to hide its communication. These blocks consist of data obfuscation, packet specific adaptation, and communication stream adaptation. Analogous to our taxonomy, we introduce two novel types of adaptive attacks in which the adversary actively hides its HTTP communication in regular network traffic. These attacks sniff the traffic of the infected host and construct a model for the observed communication known as a template. Next, the adversary transforms its own communication such that it fits the template, thereby adapting to the benign traffic.

We show the feasibility of these attacks by creating different malware versions which exfiltrate sensitive data over HTTP by adapting to the browser present on the host. This malware operates under several strategies to exfiltrate data. We have build a dataset containing a mix of benign traffic and malicious traffic performing our attacks. We use this dataset to compare our own detection solution with different state-of-the-art detection techniques.

Finally, we present our own solution to detect browser-imitating malware: ABIDED. Our evaluation shows that ABIDED achieves similar results on known attacks as existing solutions, but has much higher detection rates for these new type of attacks.

In short, our paper makes the following contributions:

- We introduce the concept of an adaptive communication attack over HTTP, allowing adversary communication to be nearly indistinguishable from benign traffic. We expect that this attack may be generalised for all protocols.
- We show that these attacks are practical by implementing data exfiltrating malware which uses our attacks to adapt to browser traffic. Moreover, we have built a dataset containing the traces of this attack, which will be publicly available.
- We present ABIDED, a solution to detect adaptive data exfiltration over HTTP. Our approach leverages the irregular

Master Thesis, University of Twente, December 2017, the Netherlands

dynamic behaviour of benign HTTP traffic to limit exfiltration capabilities of an adversary trying to stay undetected.

2 RELATED WORK

Several studies focus on the different types of covert communication used by existing malware. Zander et al. [47] set forth an overview of covert communication through several protocols, including DNS [12, 16], HTTP [27], and WLAN [13, 26, 37]. This type of communication is either based on encoding messages in redundant bits in the protocol or on employing time channel attacks.

In addition to this overview, numerous case studies address the use of covert communication channels by botnets and other malevolent software. Different works analyse covert C&C communication over DNS channels, which is still one of the main protocols used for covert communication [12, 16, 39]. Other works analyse steganography over various protocols, including VoIP [31] and the IP/TCP stack [32]. A different type of covert communication is described by Biswas et al. [7], who give an overview of both theoretical and practical applications of timing channel attacks. These attacks can be executed over different protocols such as TCP [30] and SSH [24].

There are several mimicking attacks described in the literature. The first network mimicking attack was introduced by Kolesnikov and Lee [25] who used polymorphic worms to hide from signature-based detection by changing the payload of the worms without altering its functionality. Because this polymorphic worm requires an encryptor and decryptor to be present in the code, it can still be detected by more advanced detection mechanisms such as ANAGRAM [43], which uses N-grams to detect these small changes. The authors of ANAGRAM observe that an attacker needs to mimic the structure of the *entire* packet to remain undetected, increasing the effort required from an adversary to execute a successful attack.

Bouché et al. [10] describe a statistical mimicry attack in which the adversary bypasses anomaly detectors Snort and SnortAD based on the traffic load they send out. In this attack, the adversary observes traffic volumes and adapts its own flows to stay within acceptable bounds. Another statistical attack was introduced by Yu et al. [46]. They propose a DDoS attack tool which mimics human browser behaviour following the Zipf-like, Pareto and Gaussian distributions to imitate timing intervals and browsing paths. However, deep packet inspection (DPI) systems would still be able to detect this type of statistical attacks. Casenove [14] supports obfuscation through XOR, Cesar131, and byte substitution in combination with statistical features such as activity time, port frequency, and packet delays to mimic benign traffic. This way of mimicking benign traffic has advantages over other methods, as it obfuscates data and tries to adapt to certain statistical features. However, detection systems might use other features to detect anomalies in traffic than those mimicked by the author. Furthermore, due to the obfuscation, the structure of a message would not resemble that of benign traffic. This offers possibilities for detection, as stressed by Wang et al. [43].

All of the previously described attacks find a predefined way of hiding their communication, regardless of their target. In contrast, our adaptive attacks automatically adjust their communication patterns to the infected host. Hereby, an attacker mimics many of the statistical features of the targeted system. Moreover, these adaptive attacks conform the structure of malicious messages to that of benign traffic. This gives an additional layer of covertness over the malicious traffic generated by the adversary.

The prime focus of much research is in *detecting* covert malware communication by leveraging the knowledge obtained by analysis of state-of-the-art malware. In contrast to most detection systems used in industry - which rely on signature-based detection - academic research focuses on anomaly-based detection [21]. We limit our research to detection of stealthy communication over HTTP, which is a prominent protocol described in the literature [8, 9, 38]. We refer to Sections 6.3 and 6.2 for a more in depth overview of the systems DUMONT [38] and DECANTeR [9], which we use as comparison for our own detection process. DUMONT uses several SVM's to detect anomalies in statistical features, making it an ideal target for an adaptive attack. In their work, the authors of DECANTeR pointed out that their system is vulnerable to adaptive attacks. Hence our work analyses the effectiveness of our attack against these systems.

3 THREAT MODEL

This section introduces the adaptive communication attack. In this attack, a malicious application aims to communicate *indistinguishably* from a benign application in the network. We describe the attack as if malware would adapt to a single benign application. In reality, malware adaptation is not limited to a single application. However, the described techniques can be generalised to adapt to multiple applications simultaneously.

3.1 Definitions

We describe the communication on a network as a set of messages sent between a set of hosts $H = \{h_1, ...h_n\}$ and a set of servers $S = \{s_1, ...s_m\}$. Each host runs a set of applications. In our model, this set of applications for a host h_i is described as $A_i = \{a_{i,1}, ...a_{i,j}\}$. An application $a_{i,k}$ communicates using messages $M_{i,k} = \{m_{i,k,1}, ...m_{i,k,p}\}$. A host h_i is *infected* if $\exists a_{i,q}$ defined as *malicious* and communicates with a *malicious* server s_r.

We note that the definition of *malicious* depends on the definition given by a security operator. To avoid loss of generality, we refrain from giving an exact definition of *malicious* to describe the attack.

Our work introduces the function $D(a, m)$ used by a detection mechanism D to determine whether a message originates from a given application. The function evaluates to $True$ if the message m originates from the application a or $False$ otherwise. We define an application $a_{i,a}$ to be *D-indistinguishable* from $a_{i,b}$ if $\forall m_{i,a,x} \in M_{i,a} : D(a_{i,b}, m_{i,a,x}) = True$. Note that our definition of D-indistinguishability only applies to applications on the same host. The same application running on different hosts is never indistinguishable.

3.2 Building Blocks

Our definition of *D-indistinguishable* depends both on the capabilities of the application and the method of detection D. From this point forward we assume the detection mechanism D is a network-level DPI detection mechanism and for the purpose of readability we refer to *D-indistinguishability* as *indistinguishability*. With the rise of machine learning, detection mechanisms have become more

powerful. Hence, malware has to increase its efforts to remain undetected. We present three types of building blocks to increase covertness of communication in increasing order of sophistication:

3.2.1 Data Obfuscation. Data obfuscation is performed through a combination of encoding, compression and encryption of data, making it unreadable for any entity but the attacker. This technique prevents trivial detection of known patterns which are unauthorised to enter or leave the network. Hence, signature-based detection will be unable to discriminate messages from a malicious application adopting data obfuscation techniques. This building block is often sufficient to bypass most DLP systems deployed in industry. Most existing data-exfiltrating malware apply this building block as described in several works [2, 3, 35, 45].

3.2.2 Packet Adaptation. Obfuscation of the communication will not trigger alerts in DPI systems as the content cannot be retrieved. However, statistical methods such as byte distribution might still find anomalies in packets without being able to reveal the original content. To overcome this problem, malware will try to craft its messages in such a way that each individual packet is *indistinguishable* from a benign packet. We define packet adaptation as the capability of controlling the structure of a message to fit benign traffic. To achieve this, malware could monitor the traffic of the victim's machine and collect information about individual packets, e.g. header values and average sizes. Subsequently, the adversary crafts its own packets in such a way that they are *indistinguishable* from benign applications, adapting its sent packets to the ones observed. By adapting its own communication, it tries to circumvent detection. To the best of our knowledge, packet adaptation has not yet been adopted by malware. However, there are several techniques which enable packet adaptation. First, by analysing the packets of well-known applications and predefining packet-equivalent communication between malware and its servers. Second, anti-censorship techniques such as Format Transforming Encryption (FTE) - proposed by Dyer et al. [18] and used in the TOR browser - could enable malware to adapt to the infected machine and communicate using packet adaptation in real time.

3.2.3 Stream Adaptation. Packet adaptation forces individual packets to be indistinguishable from individual packets in benign applications. However, detection systems which are able to correlate multiple packets might find anomalous patterns which are not present in regular traffic. Such detection techniques are used in e.g. botnet detection [23] and stateful protocol analysis methods [17]. To avoid detection by systems employing these techniques, malware will control the correlation between packets. We define this as *stream adaptation*. To achieve stream adaptation, malware monitors the victim's network, collecting information about packet streams instead of observing individual packets. This includes monitoring bandwidth and activity frequency of its host as well as correlating data received by the machine with data sent by it. Using this information, the intruder mimics the stream behaviour of its host machine. For example, stream adaptation for the HTTP protocol could include sending out additional requests to retrieve embedded objects from received HTML pages. As with packet adaptation, to the best of our knowledge, stream adaptation has not yet been observed as a technique used by malware. And as with packet adaptation, stream adaptation might be performed through a predetermined pattern extracted from well-known applications, or at real time. Both strategies could be executed by anti-censorship tools such as Marionette [19], allowing the user to define stream behaviour through programmable state machines.

3.3 Taxonomy

Combinations of the previously described techniques may be used by malware to hide its communication from network-level detection mechanisms. As the level of sophistication required for each technique increases we propose a taxonomy for network-observable malware according to the following scheme:

(M0) Naive malware. This is the most basic type of malware. It is not capable of applying any of the aforementioned detection avoidance building blocks.

(M1) Obfuscating malware. This type of malware only applies the data obfuscation building block to hide its exfiltration attempts. It is not capable of applying adaptive data exfiltration techniques. It has been observed in practice [2] and has been analysed [33].

(M2) Packet-adapting malware. In addition to applying obfuscation techniques, this malware also applies packet adaptation. It is unable to perform stream adaptation methods. Since (M2) malware does not control its communication stream, its stream structure might be influenced by the host's activities. To the best of our knowledge, this type of malware has not yet been observed in practice.

(M3) Stream-adapting malware. This final type of malware exploits all three stealth techniques to avoid detection, i.e. it adopts data obfuscation, packet adaptation and stream adaptation. Because (M3) malware has full control over its communication, it can be independent of the traffic produced by the infected host. To the best of our knowledge, stream-adapting malware has not yet been observed in practice.

4 MALWARE ATTACKS

To demonstrate how realistic such malware attacks are, and how difficult it is to detect them, we have implemented different types of malware for all (M0)-(M3) attacks which exfiltrate data over HTTP. The objective of our malware is to exfiltrate predefined text files of sensitive data from the infected host and remain undetected by trying to adapt to the infected host's browser application. We have chosen the browser as an application to mimic as its dynamic characteristic shows the capability of malware to adapt to complex communication structures. Furthermore, it is common for the browser to send and receive vast amounts of data, which makes it an ideal application to mimic for exfiltrating data without being detected. In our scenario, we assume the malware is already active on the host, i.e. we eliminate the infection phase and go straight to the attack.

4.1 Strategy

Apart from being capable of performing an (M0)-(M3) attack, malware might influence detection by how aggressively it tries to exfiltrate data. This depends on the amount of data malware exfiltrates,

the speed at which it exfiltrates, and the packet sizes it uses. Therefore, we discuss several strategies malware might use to further avoid detection. This will help us quantify and evaluate our detection mechanism and make more realistic comparisons with other state-of-the-art solutions.

4.1.1 Data Size. The amount of data being exfiltrated influences the adversary's choice of strategy. Small amounts of data such as a private key are no more than a couple of kilobytes, while an entire database is much larger. The amount of data which is exfiltrated influences the strategy used to remain hidden. Small amounts might be exfiltrated aggressively without being detected, whilst large amounts of data require more covert techniques. Research has shown that most data-exfiltrating malware does not target specific data, but tries to exfiltrate everything it finds [5, 41]. Hence, we identify the size of data being exfiltrated as a major component of an exfiltration strategy.

4.1.2 Exfiltration Speed. To remain undetected, malware can choose to exfiltrate data slower than the limit imposed by the outgoing bandwidth. In this way, the exfiltrating data does not dramatically increase the amount of traffic, making it more difficult to be detected. However, a disadvantage is that the increased exfiltration time slows down the attack. Additionally, a lower exfiltration speed requires a longer open connection to the malicious server, providing detection mechanisms with an opportunity to disclose connections with prolonged activity. We define the exfiltration speed as the goodput over the network. The speed influences the amount of exfiltrated data, not necessarily the amount of data sent over the network as this is defined by the throughput.

4.1.3 Packet Size. We define the exfiltration speed as the goodput over the network. When simple exfiltration methods are used, such as (M0) or (M1), the goodput is almost equal to the throughput. However, more advanced exfiltration methods - such as (M2) and (M3) - offer limited goodput per message, as they require outbound packets to follow a given syntax. Malware could increase packet size to enhance the goodput of malicious data sent out. As a consequence, this would decrease covertness as large packets raise alerts in most detection solutions. Therefore, stealthy malware will optimise its balance between packet size and exfiltration speed to remain undetected.

4.1.4 Strategy Aggressiveness. The previously described components make up the aggressiveness of the exfiltration strategy. However, certain combinations of parameters do not make sense for an attacker. Therefore, the number of realistic strategies can be dramatically reduced. For our case study, we define five realistic strategies attackers could employ to exfiltrate data. (see Table 1). Note that we kept packet sizes to an average of 1 Kb as this provides reasonable throughput while not exceeding default MTU sizes of 1500 bytes. More advanced malware might learn an acceptable throughput from observing the regular behaviour of the host. However, due to the scope of this research we leave it to future studies to provide more insights into the effectiveness of learning such thresholds. Furthermore, it does not make sense for small amounts of data to be exfiltrated at a slow speed as it requires only a few packets to send them. Finally, large amounts of data are usually not exfiltrated very stealthily as it would take weeks or even months of continuous exfiltration to obtain them.

4.1.5 Exfiltration Location. Another way in which malware might influence detection is related to the exfiltration location within a packet. Most protocols use header fields to send control information and a body field to send data. Adversaries can use both types of field. Depending on the protocol some fields allow for more data capacity than others. Furthermore, the level of covertness will also change depending on the chosen field for exfiltration. Widely used protocols such as HTTP even allow headers to be extended with custom implementations [20], which provide adversaries with even more capacity to send data.

Due to the simplistic nature of (M0)-(M1) attacks, we have limited the exfiltration location of implementation of those malwares to the URI GET parameters. For (M2)-(M3) malware, the location of data exfiltration is more important as it has to adapt to the syntax of the application it tries to mimic. As the protocol in our attack scenario is HTTP, and the application the malware tries to mimic is a browser, we have identified five different locations where malware might exfiltrate data:

(1) The HTTP Body of a request.
(2) The HTTP *Cookie* header field - a variable header field.
(3) The HTTP *Data* header field - a custom HTTP header field.
(4) The HTTP *User-Agent* header field - a constant header field.
(5) The *URI parameters* of an HTTP GET request.

4.1.6 Exfiltration Distribution. While our implementation only addresses the aforementioned strategic choices, we are also aware of the scenario where malware distributes its exfiltration process, thereby further obfuscating data exfiltration in the network. Distributing the exfiltrated data over multiple malicious servers in the network makes each malicious connection less likely to be detected due to the lower amount of data flowing over it. Furthermore, connections only have to be maintained for a shorter period of time. This type of exfiltration is relatively inexpensive for malware; it merely requires additional servers to send data to. However, we do note that it is unrealistic to assume that the attacker controls an unlimited amount of servers over which data can be distributed.

Our implementation of the malware does not employ this technique as it is beyond the scope of this paper. We reason that the same effect of straightforward distribution can be reached by exfiltrating smaller amounts of data to a single IP address. However, more advanced methods of distribution could adapt its pattern to the observed host, thereby bypassing detection systems by exfiltrating small amounts of data per server.

We distinguish three techniques for exfiltration distribution:

(1) *Single-Server Distribution.* This does not make any attempt to distribute its traffic over different servers and therefore does not add any covertness to an exfiltration attempt.
(2) *Round-Robin Distribution.* This distribution requires malware to send each stream of packets containing exfiltrated data to a different malicious server. Once the last server has been reached, it will send the next stream of packets to the first server and continues its cycle in a round-robin fashion.
(3) *Random Distribution.* This type of distribution randomises the amount of data in the data streams sent to the attacker.

Table 1: Exfiltration strategies comprised of parameters data size, exfiltration speed, and packet size.

Strategy	File size	Interval	Packet size	Goodput	Example
S1	< 10 Kb	0.0 s	~ 1Kb	> 1.0 Mb/s	Exfiltration of RSA private key
S2	10 Kb - 10 Mb	0.0 s	~ 1Kb	> 1.0 Mb/s	Stealthy exfiltration of .pdf or .docx document
S3	10 Kb - 10 Mb	0.5 s	~ 1Kb	~ 1.0 Kb/s	Normal exfiltration of .pdf or .docx document
S4	10 Kb - 10 Mb	5.0 s	~ 1Kb	< 0.2 Kb/s	Aggressive exfiltration of .pdf or .docx document
S5	> 10 Mb	0.0 s	~ 1Kb	> 1.0 Mb/s	Aggressive exfiltration of large database

Connections will be opened at random and random amounts of information are sent to different malicious servers. This makes it more difficult for detection mechanisms to recognise patterns, but requires the attacker to reconstruct data on the receiving end.

Distributing data over multiple machines will increase the covertness of the exfiltration attempt in that it reduces the amount of data sent over each malicious connection in the network. However, it requires the attacker to maintain multiple malicious servers which in turn increases the chances of being blacklisted. Furthermore, due to more connections present in the system, a detection mechanism might be able to correlate the different connections, thereby nullifying the effect of exfiltration distribution. In conclusion, exfiltration distribution might affect the exfiltration of data in both positive and negative ways depending on the detection method.

4.2 Architecture

In this section, we describe the architecture of our (M0)-(M3) malware implementations[1]. For each malicious application, we have created a version which exfiltrates according to strategies S1-S5 as outlined in Table 1. As described in Section 4.1.5, (M0) and (M1) malware use the URI parameters to exfiltrate data, whereas (M2) and (M3) have five different exfiltration locations for each strategy. All (M0)-(M3) malware come with a corresponding (M0)-(M3) server which is able to receive the requests.

4.2.1 Strategy Implementation. To implement the strategies S1-S5, we have defined three different text files - for S1, S2-4, and S5 respectively - comprised of "Lorem ipsum" which are exfiltrated by the malware:

(1) A 1 Kb text file, containing 20 lines of 50 characters.
(2) A 100 Kb text file, containing 2 k lines of 50 characters.
(3) A 10 Mb text file, containing 200 k lines of 50 characters.

Additionally, we have implemented the interval for the S3 and S4 strategies as shown in Table 1. When these strategies are applied, the malware will sit idle for 500 ms and 5 s, respectively, between each message sent out.

4.2.2 (M0) Malware. (M0) malware exfiltrates data in its most straightforward form. It reads the data from an input file line by line and sends it in an HTTP GET message to the malicious (M0) server using CURL/7.35.0. To send a GET request to the malicious server, we used the command:

```
curl -X GET x.x.x.x/?<secret_data>
```

where `x.x.x.x` is the IP address of our malicious server and `<secret_data>` is the data we exfiltrate in plain text. This generates an HTTP GET request as illustrated in Figure 1a.

4.2.3 (M1) Malware. (M1) malware exfiltrates data by a combination of encryption, compression, and obfuscation to ensure that patterns of known sensitive data are invisible in the communication. In our implementation of (M1) malware, data is first encrypted using AES-256-CBC encryption with a key of the bytes in the ASCII message `SuperSecretKey12` and an initialisation vector of the bytes in the ASCII message `MyInitialVector1`, and then encoded using Base64 encoding. The encrypted message is then sent to the server in the GET parameters of the URI as illustrated in Figure 1b. At the server side, first the Base64 encoding is removed and then the AES-256-CBC encryption to obtain the original message.

4.2.4 (M2) Malware. The (M2) malware modifies its packets based on the observed packets sent out from the infected host. To modify the packet to a desired output we used FTE [18]. This scheme takes an input message and encrypts it using AES-256-CBC encryption resulting in a binary string. This binary string is fitted into any desired regular expression, known as an FTE template. The FTE process fits the binary string into the template using a process called ranking. Hereby, the binary string is interpreted as a number n and fitted to the regular expression by computing the n^{th} string in the language defined by the regular expression. For example, in an FTE template defined as `/[a-z]+/`, `a` is the 0^{th} string in the language, `b` the 1^{st}, and `aa` the 26^{th}. After this process, the ciphertext message is sent to the server. Upon receiving the encoded message, the server - which has the same FTE template - will reverse the process by unranking the template and decrypting the message, thereby obtaining the plaintext message. The challenge for the malware is to construct such an FTE template from observing an application in the infected host.

The objective of our malware is to adapt to the browser active on the infected host. To this end, the malware starts to sniff all traffic on port 80, i.e. all HTTP packets. For each HTTP message observed, the malware collects the method, URI, version, header fields and subsequent values, and body. From these collected values, the malware creates its own FTE template. For this purpose, the malware first selects the header set, i.e. the ordered set of HTTP header fields used for its FTE template. As not all HTTP messages contain the same header fields, the malware selects the most frequently used header set. Next, it will generate a regular expression by combining all collected methods, URIs, versions, header fields and values from the selected header set, and all bodies. This combined FTE template

[1] A full Python implementation of all malware variants is available upon request.

```
GET          /?Lorem ipsum dolor sit amet HTTP/1.1
User-Agent:  curl/7.35.0
Host:        x.x.x.x
Accept:      */*
```

(a) HTTP GET request of exfiltrating (M0) malware, where x.x.x.x is the IP address of our malicious server.

```
GET                /?7zhGaSUsKOG5dz730q7ESB0yQP2fMsBh
                   Z6WXbdfNpsFgAOqfqpMLn12MJ1q/T/HGdv
                   EQu1VHmmXP44dQS+NTCA== HTTP/1.1
Host:              x.x.x.x
Accept-Encoding:   gzip, deflate, compress
Accept:            */*
User-Agent:        python-request/2.2.1 CPython/2.7.
                   6 Linux/4.4.0-89-generic
```

(b) HTTP GET request of exfiltrating (M1) malware, where x.x.x.x is the IP address of our malicious server.

```
GET                /v6exp3/6.gif?GiLkCysFOapHVYg2lkNX
                   u9c7gKkXGMmGkqSsw0AxCvFwkk4IyjwIdr
                   OXj2eFKjVQMX2Z2DkqY4aNejsDPzHY8BQg
                   NGm1XDfVKvogwTXPP9nygXRPGMSbU7sHch
                   ppbWvxS9aubJ6mM0gZZjZLbfFwhGGhKLJQ
                   bxdDVPjJfth7AJaVc8qytn1MuehkwSn6nU
                   Cd5s8Qx7XkpyknfGymD HTTP/1.1
Accept-Language:   en-us,en;q=0.5
Accept-Encoding:   gzip, deflate
Host:              p4-e4mhg56qfazha-uz2cfj4xtooqfrr6-
                   773673-i2-v6exp3-v4.metric.gstatic
                   .com
Accept:            image/png,image/*;q=0.8,*/*;q=0.5
User-Agent:        Mozilla/5.0 (X11; Linux i686; rv:
                   14.0) Gecko/20121001 Firefox/14.0
                   .1
Connection:        keep-alive
Referer:           http://p4-e4mhg56qfazha-uz2cfj4xto
                   oqfrr6-if-v6exp3-v4.metric.gstatic
                   .com/v6exp3/iframe.html
```

(c) HTTP GET request of exfiltrating (M2) and (M3) malware. Both malware are equivalent on packet level.

Figure 1: HTTP GET requests of (M0)-(M3) malware exfiltrating "Lorem ipsum dolor sit amet" in the URI.

gives some space to send out data by choosing different combinations of possible values. However, this makes it impossible for the receiving server to decode the message as it requires the complete FTE template to deduce which fields were used for encoding. As this FTE template was constructed at the client side, the server side has no way of knowing the used FTE template. To solve this problem, we identify a specific exfiltration field in which we do not use the values of the FTE template, but adopt a predefined encoding scheme, in our case Base64. For the (M2)-(M3) malware, we use the URI GET parameters, cookie, data, or user-agent header fields, or request body as an exfiltration field as described in Section 4.1.5. After the Base64 regular expression `[a-zA-Z0-9]*` has been added, the FTE template is ready to encode messages.

We omit the implementation of the (M2) server as it is beyond the scope of this paper. However, when the exfiltration field is known, the aforementioned process of creating an FTE template is easily reversed using the Format Transforming Decryption scheme proposed by Dyer et al. [18]. Furthermore, we should note that the (M2) malware only uses FTE to adapt outgoing messages. Finally, our server implementation is a dummy server, which receives any HTTP request and outputs a predefined HTML web page.

Figure 1c gives an example of a message encoded using the described technique. As we can see from the User-Agent field, the malware has adapted its message to the Mozilla Firefox browser running the infected Linux machine. In addition, we see that the malware has identified the default language of the infected host to be US-English and set its corresponding field. The example message appears to request a .gif image from a content delivery network. In reality, it exfiltrates data through the GET parameters in the request.

4.2.5 (M3) Malware. Analogous to (M2) malware, (M3) malware modifies its packets based on the ones observed. However, hitherto, malware has only generated its template based on individual messages. (M3) malware takes the entire communication stream of an application into account. To model and later reproduce such a stream, we required a way to create individual FTE templates as described in Section 4.2.4 and replay them in a structured way. To this end, we used the Marionette [19] architecture. Marionette is a programmable network traffic obfuscation system which combines the execution order of FTE templates in a programmable state machine dictating the order in which FTE templates are to be used. We defined this order in a Marionette template. This Marionette template includes both sides of the communication, i.e. both HTTP requests and HTTP responses are modelled using Marionette.

There is, however, a problem with such an adaptive (M3) scheme, namely that adapting the server to messages intercepted on the host requires some way of communication from the infected host to the server. There is no way to covertly send this information to the malicious server without using any predefined communication scheme. Moreover, once such an adapted template has been sent to the server, it cannot learn any new template as it would consume space in the recently adapted template. Therefore, an (M3) adversary will have to learn a predefined communication template in order to exchange data. Our implementation adopts a predefined Marionette template for a Google query and adapts its host-dependent fields such as `Accept-Language` and `User-Agent` to the infected host analogous to the method described in Section 4.2.4. The predefined Marionette template itself was created from a Google query in one of the datasets used for analysis. By choosing one of the traces from an infected machine, we tried to simulate the strongest possible (M3) attack. However, this strongest type of attack is unlikely to occur due to the problem described above.

5 DETECTION

Several state-of-the-art network-based covert communication detection systems are described in the literature. Predominant systems

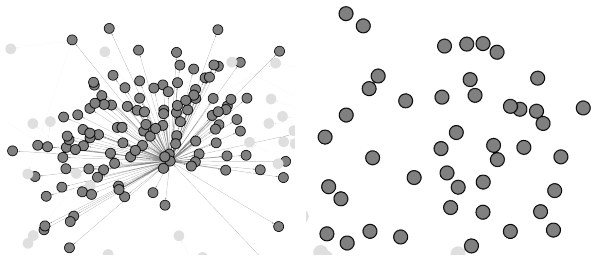
include WebTap [8], DECANTeR [9], and DUMONT [38]. However, none of these systems are designed to withstand an adaptive communication attack as introduced in this paper. Therefore, we required a new network-based detection technique which is able to distinguish adaptive behaviour from benign behaviour. There are few aspects of communication which cannot be spoofed. In our attack model, we assume that the attacker only controls the host and the server, but not the infrastructure. Therefore, the only limit on adapting communication messages is that malware cannot adapt the IP address. A perfect detection mechanism is likely not possible due to the freedom of malware to adapt to benign traffic. Nevertheless, we introduce novel heuristics which constrain the malware exfiltration capabilities. We note that our proposed detection mechanism is aimed at HTTP browser traffic, whereas the aforementioned state-of-the-art solutions are aimed at general HTTP traffic. By developing a detection mechanism for our use case of a data exfiltration attack over HTTP, we hope to find the limits of malware in adapting to a host application.

5.1 Architecture

Our Adaptive Browser-Imitating Data Exfiltration Detector (ABIDED) aims to distinguish HTTP browser traffic from traffic generated by a malicious application imitating the browser active on the host. To this end, the first step in our approach is to capture the dynamic behaviour of benign browser traffic. The rationale behind this is that a browser will interact with web pages by requesting an HTML page, and upon receiving the response will issue additional requests for embedded objects such as images, JavaScript, and CSS. Malicious data-exfiltrating malware on the other hand will not interact with any web pages as their prime objective is to send data from the infected host to a malicious server. Unless the malware adapts to the browser in such a way that it imitates this dynamic behaviour, it will immediately be detected and raise an alert when exfiltrating too much data. The second step is to leverage the context provided by this model to detect exfiltration attempts of adaptive malware. This is done through several heuristics for (M2) and (M3) malware, which all have to trigger in order to raise an alert.

5.2 Referrer Graph

To model browser behaviour from traffic traces, we have constructed a graph which encodes relations between HTTP request-response pairs. In the literature, multiple methods to achieve such a relation-based graph have been proposed [34, 44, 48]. ClickMiner [34] uses a proxy browser to analyse HTTP responses and see which requests the proxy generates. When the host's browser issues a new request, it will be linked to the response if the request was also issued by the proxy browser. This method requires an intensive analysis of all traffic and is therefore unsuitable for high volumes of traffic. Zhang et al. [48] link HTTP requests based on the user's click behaviour in the browser. They correlate the time at which the user clicks on a web page with the HTTP requests issued in a short time period thereafter. As this method requires access to user interaction with the host, it is unsuitable for our network-based approach. Finally, ReSurf [44] tries to infer user click behaviour on web pages from the referrer header field in HTTP requests. In benign traffic, this field indicates if an HTTP request originated



(a) rottentomatoes.com (b) (M1) malware

Figure 2: Referrer graphs for visit of a benign website (a) and malware (b).

from a different website, e.g. when the user clicked on a website link or when the request retrieved an image placed on the page. With this technique, requests are linked if there exists a referrer link and if there is at least a time τ between the issue of the possible parent request and the child request. This delay is built in because ReSurf aims to reconstruct user behaviour and assumes a user employs a certain delay between clicks on links in a web page. This last method is suitable in our approach as it only depends on network traffic and is computationally inexpensive. However, we required all requests to be linked instead of only the requests generated by the user. Hence, we omitted the time threshold τ and based our graph on the HTTP referrer field of the collected data. We call our resulting graph the Referrer Graph[2,3] and define it as a directed graph where each node n_i represents an HTTP request-response pair and each edge $e_{i,j} = (n_i \rightarrow n_j)$ represents a referrer link from an HTTP response node n_i spawning an HTTP request node n_j.

ABIDED leverages the context provided by the Referrer Graph to define whether traffic is malicious. A distinctive characteristic of benign browser traffic is the web pages visited by its users. This is represented in the Referrer Graph through a node which has spawned multiple other nodes for the retrieval of embedded objects in the page. We define a *page visit* as a subgraph $\hat{G}$ in Referrer Graph G, comprised of a parent node n_p with at least one outgoing edge and all its direct children. Note that the parent node in a *page visit* may be a child of a different *page visit*.

Using this method, we have constructed a Referrer Graph for benign data of a web visit to rottentomatoes.com and for data exfiltration of our implementation of (M1) malware. Both graphs are illustrated in Figure 2, where each node represents an HTTP request-response pair. The figure shows that the benign web visit is fully connected, whilst the malware is completely disconnected. All observed real-world malware that obfuscates its traffic is a type of (M1) malware and therefore also produces disconnected nodes. Note that this is an ideal situation; in reality, benign traffic contains disconnected nodes and (M2) and (M3) malware produce connected nodes as they adapt their referrer field to the benign traffic.

[2] A similar method - which limits nodes to be linked only to head nodes, i.e. nodes which are able to generate new requests such as HTML, CSS, JavaScript - has been successfully implemented in DECANTeR [9].

[3] A full Python implementation of the Referrer Graph is available on https://github.com/Thijsvanede/Master-Thesis.

5.3 (M2) Heuristics

Now that we have modelled the dynamic HTTP behaviour, we are able to leverage the additional context it gives to the network trace to detect malicious data exfiltration activities. As (M2) malware will adapt the referrer field in its messages to the ones used by benign applications, it is able to hook onto a page visit in the Referrer Graph. Therefore, merely separating connected and disconnected nodes is not enough to detect either type of malware. In an effort to overcome this problem, we have identified two characteristics inherent to data exfiltration: large amounts of outgoing data with respect to incoming data; and a steady stream of data flowing over a connection. From these characteristics we define four different statistical detection mechanisms, which we combine to enable our detector to detect (M2) malware.

5.3.1 outgoing information Threshold. This threshold - which we call τ_{oi} - is the most basic and focuses on the amount of data leaving the network. The outgoing information (OI) [9] is defined as the size of the first packet added to the Levenshtein distance between subsequent packets in a connection between the host and the malicious server as shown in Equation 1. In this equation, $p_0, ...p_n$ are the packets in a connection ordered by timestamp, and the function $ld()$ computes the Levenshtein distance between two packets. The rationale behind this threshold is that in data exfiltration, messages need to change their contents in order to send out the data. Whilst all HTTP requests will send out data, the amount per connection will be larger for data-exfiltrating malware. If the outgoing information of a connection exceeds the set threshold τ_{oi}, the connection is marked as suspicious.

$$\mathrm{OI}(P) = |p_0| + \sum_{i=0}^{n-1} ld(p_i, p_{i+1}) \tag{1}$$

5.3.2 Volatility Threshold. This threshold - $\tau_{volatility}$ - is the lower bound to the volatility of a page visit. We define the volatility as the standard deviation of the gradient in outgoing information between subsequent packet pairs. Equation 2 gives the formula to compute the gradient between a pair of packets, i.e. the additional outgoing information between packets divided by the time between packets. Equation 3 uses the gradient formula to compute the standard deviation over a set of packets, resulting in the volatility. In the detection, we compute the volatility over a time window $t = 10$ seconds. This window was empirically chosen as smaller windows give unstable volatility measures and larger windows make malicious volatility measures indistinguishable from benign ones. The rationale behind our Referrer Graph assumes that retrieval of a web page spawns requests for embedded elements on the website, resulting in a burst of requests. This burst covers relatively little time, while sending out large amounts of data. Conversely, malware trying to covertly exfiltrate data has to steadily send out data spread over larger periods of time to avoid raising alarms. This is well illustrated in Figure 3, where we plot the outgoing information described in the previous section to time. We can clearly see that the exfiltrating malware hooked to a page visit - represented by the red line - as it has a distinctly different pattern than the normal behaviour. After the initial benign burst, the adaptive malware hooks to a page visit in the Referrer Graph and starts to exfiltrate data.

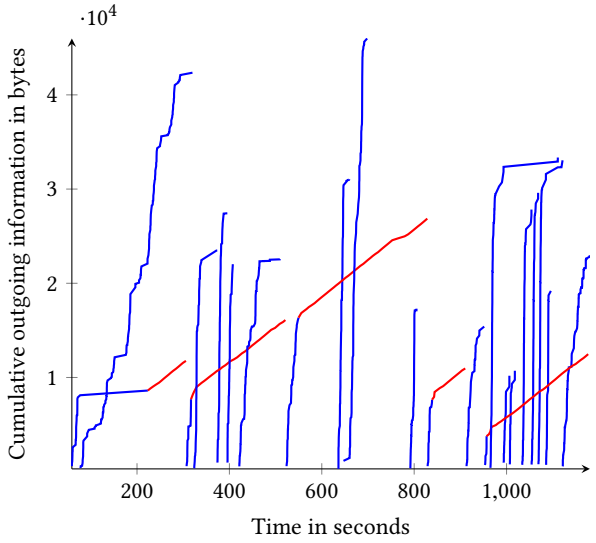


Figure 3: Outgoing information plotted against time, showing (M2) data-exfiltrating malware using S4 strategy and custom exfiltration field (red) and regular traffic (blue).

It can hook to the Referrer Graph by adapting its referrer field to the one of regular data. From this point, we see a steady increase in the cumulative outgoing information. If the volatility becomes too low, it means that there is a steady stream of outgoing information, indicating the presence of data-exfiltrating malware.

$$\mathrm{G}(p_x, p_y) = \frac{OI(p_0, ..., p_y) - OI(p_0, ..., p_x)}{t_y - t_x} \tag{2}$$

$$\mathrm{V}(p_0, ..., p_n) = \sqrt{\frac{\sum_{i=0}^{n-1} \left(G(p_i, p_{i+1}) - \frac{OI(p_0, ..., p_n)}{n}\right)^2}{n-1}} \tag{3}$$

5.3.3 IO Ratio Threshold. The third measure - the IO ratio threshold τ_{io} - consists of the ratio of incoming information versus outgoing information as computed from Equation 1. The IO ratio is computed per page visit under the same rolling window of 10 seconds as used in the volatility measure. We use a rolling window instead of a set value because malware will hook onto the Referrer Graph at an unknown point in time. Hence, we need to omit the traces from benign data to exclusively capture the behaviour of the malware. Because the prime objective of our adversary is to exfiltrate data, the amount of outgoing data should far exceed the amount of incoming data. We note that adapting the server responses to circumvent the IO ratio detection falls under the (M3) malware type and is not detectable by the IO ratio. If the IO ratio becomes too low, we see that too much data is flowing out with respect to the response data, indicating data exfiltration.

5.3.4 IP Volatility Threshold. The final detection mechanism is the IP volatility - τ_{ip}. It is computed as the standard deviation of a rolling time window of 10 seconds for the amount of IP addresses active in a page visit. The rationale behind this detection mechanism is that exfiltrating malware only communicates with

a predefined set of IP addresses. We assume that this set remains constant throughout the exfiltration process. Note that this assumption will not hold in case of randomised IP distribution and would therefore need other detection mechanisms. Benign traffic will not trigger this threshold as many different IP addresses are accessed during a benign page visit, because websites distribute their content over multiple servers and advertisement networks load their advertisements from different sources than the web page displaying them.

5.4 (M3) Heuristics

In the (M3) detection we assume that the only way in which malware can communicate is over HTTP. From this assumption, we can conclude that (M3) malware communicates through a predefined template as there is no way of transferring a template through any other means than sending it through a predefined template, which would result in an endless loop of exfiltrating new templates. Furthermore, we assume there is a limit to the amount of steps in a template as the malware binary would become too large and will easily be detected before being able to infect a host. This step limitation results in a template which needs to be repeated when large amounts of data are exfiltrated. Therefore, our (M3) detection technique tries to identify patterns from the predefined template.

In a predefined template, the malware does not know which HTTP request-response pairs are issued by the host. Therefore, it cannot hook to a page visit in the Referrer Graph, but has to create its own subgraph. As the template has to be repeated due to its limited size, there will be multiple (M3)-created subgraphs in the Referrer Graph. Hence, our (M3) detection focusses on finding similarly structured subgraphs in the Referrer Graph.

Determining graph similarity is possible through multiple methods. First, we can check whether subgraphs are isomorphic [42]. This is a straightforward method of determining similarity, but is not flexible if malware finds ways to slightly alter its graph structure, e.g. by creating noise through sending out HTTP requests to obfuscate its own exfiltration. A more advanced way is to compute the edit distance between graphs [11]. Hereby, we compute the number of nodes and edges in the subgraph which have to be altered to obtain the compared graph. This allows for some changes in the exfiltration pattern which can be determined by a given threshold. Finally, it is possible to determine the maximum common subgraph [11] as the comparison metric between two graphs. Here, we could expose the exfiltration pattern within subgraphs by removing the possibly randomly generated noise. ABIDED uses the edit distance as a metric to compare graphs as it is more adaptable for a security operator. Further research needs to point out whether this method is preferable over the maximum common subgraph. Using this metric for (M3) detection as well as the metrics described in Section 5.3, ABIDED makes an effort to detect adaptive data exfiltration compared to existing solutions.

6 EVALUATION & RESULTS

To show that the adaptive attack is able to circumvent detection by state-of-the-art detection mechanisms, we generated a dataset containing traces of all types of malware described in Section 4. We ran the detection on our own ABIDED system[4] as well as on DECANTeR [9] and DUMONT [38]. We showed that advanced versions of the adaptive attack are able to evade detection by the latter systems, but are detected by ABIDED.

6.1 Datasets

To fully compare the three systems, we created three different datasets: a dataset containing the adaptive attack; a dataset containing real malware exfiltrating data; and a benign dataset containing traces of actual users.

6.1.1 Adaptive Dataset. Our adaptive dataset was used to show the capabilities of the novel adaptive attack and to illustrate how to defend against it. It contains traces of the (M0)-(M3) malware for each strategy and exfiltration location. We used the publicly available dataset of ClickMiner[5] [34], containing browser HTTP traces of 25 users. From this dataset, we used the 10 traces with the most HTTP request-response pairs, each trace containing 20 minutes of captured data. For each malware type, strategy, and exfiltration location, we replayed the HTTP traffic of the 10 traces using `tcpreplay`, while simultaneously running the corresponding malware. During these experiments, we captured all traffic using `tcpdump`, resulting in 600 20-minute pcap files summarised in Table 3 in the Appendix.

6.1.2 Exfiltration Dataset. The exfiltration dataset from DECANTeR [9] was used to compare ABIDED with state-of-the-art solutions in detection rates of actual malware. It was created by running a Windows XP and Windows 7 virtual machine containing several login credentials as well as sensitive documents. In each experiment, the virtual machine ran for 1 hour with a malware sample from seven different malware families. These families included COSMIC_DUKE, FAREIT, FTPINFOSTEAL, SHAKTI, SPYWARE, TIM, and URSNIF. The experiment resulted in a dataset of 92 pcap files, each of which contains traces of one of the previously described malware families. A summary of the exfiltration dataset can be found in Table 4 in the Appendix.

6.1.3 User Dataset. The user dataset from DECANTeR [9] was used to determine the false-positive rates of all compared solutions, giving a better insight into the practical aspect of using state-of-the-art solutions in real-world environments. The dataset consists of browser traces from four researchers at our university. None of the researchers had any active malware on their machine during the collection phase which lasted several days. The collection gathered all HTTP traffic from the monitored hosts. Subsequently, all HTTP traffic related to a browser User-Agent was extracted to produce the resulting dataset as summarised in Table 5 in the Appendix.

6.2 DECANTeR

We compared our system with DECANTeR[6] [9], a fingerprinting system which detects applications active on a host, based on the HTTP requests it sends out. It detects malware when it finds a new application active on the system. To detect applications, DECANTeR uses a learning phase to study all benign applications

[4] Using the implementation of github.com/Thijsvanede/Master-Thesis/tree/master/ABIDED
[5] Available at http://clickminer.nis.cs.uga.edu.
[6] Using the implementation of github.com/rbortolameotti/decanter.

active on the host. The learning phase is divided into two modules. The first module clusters HTTP requests per time window of $t = 10$ minutes based on their User-Agent and labels requests as originating from a browser or background application based on whether they show dynamic behaviour by being connected in their version of the Referrer Graph. The second module creates an application fingerprint per labelled cluster from the previous phase, consisting of the set of domains from each request; the header fields present in each request of the cluster; the average size of requests; the User-Agent of the cluster; the Accept-Language HTTP field; and the outgoing information of a cluster.

After the training phase, DECANTeR is able to detect which traffic belongs to learned applications and which traffic belongs to new applications through its detection phase. In this stage, the two modules of the learning phase are repeated to obtain a fingerprint of the newly analysed data. Next, the new fingerprint is compared with learned fingerprints to see if the traffic originated from a known application. If this is not the case, it triggers an alert when the application has exfiltrated more than $\sigma = 1000$ bytes of data.

6.3 DUMONT

Apart from DECANTeR, we also studied the performance of ABIDED in comparison with DUMONT[7] [38]. This system learns 22 one-class SVMs from 17 numerical features and combinations of these features based on their type. The features include metrics about the length of requests, their structure, the entropy of their content, and temporal features. These one-class SVMs are trained by analysing benign data based on a desired false-positive rate given to the system as a parameter. Next, the SVMs are calibrated by generating an ROC curve from a combination of benign and malicious training data. Then, the SVM kernel with an ROC curve closest to the point (0, 1.0) is chosen as the classifier. After this training phase, DUMONT is able to detect covert communication in HTTP by analysing unseen HTTP requests. A request is classified as anomalous if at least one of the one-class SVMs in the system classifies a request as anomalous.

6.4 Evaluation Setup

All implementations of the evaluated systems required some data preprocessing before being able to analyse the datasets. We used Bro[8] [36] to generate logs of HTTP request and response events from the pcap packet traces of the datasets. DECANTeR [9] and DUMONT [38] require HTTP request headers and some metadata to be present in these logs. ABIDED requires HTTP response headers in addition to the data extracted for the other two systems, as it correlates HTTP request-response pairs in its detection.

6.4.1 Parameters ABIDED. The implementation of ABIDED uses manually set thresholds for its detection as well as the window for analysing time series data. As explained in Section 5.3, the time window is empirically determined to be optimal at 10 seconds. Hence, this window is also used in the analysis. As for the other thresholds, we set them at the following values:

$\tau_{oi} = 10000$. The threshold of 10 Kb for outgoing information was set as sensitive data - apart from private keys - is usually stored in files much larger than 10 Kb. Therefore, exfiltrating malware will always exceed this threshold. Conversely, benign traffic will send out data when requesting web pages, but rarely exceeds 10 Kb.

$\tau_{volatility} = 200$. This threshold was empirically determined by examining the volatility of our user dataset in combination with the original ClickMiner dataset. We combined these datasets and found that the lowest 5^{th} percentile had a volatility of ~ 8.0, and the lowest 10^{th} percentile had a volatility of ~ 212.1. As the volatility of the exfiltrating dataset is expected to be at the lower end of the spectrum, we have set this threshold at 200.

$\tau_{io} = 0.1$. This threshold value implies that the amount of outgoing information should be at least 10 times larger than the amount of incoming information. For (M2) malware, this assumption is valid as it does not adapt the incoming information stream. We empirically determined this threshold at 0.1 as the lowest 5^{th} percentile had a ratio of ~ 0.10, and the lowest 10^{th} percentile had a ratio of ~ 0.20. Hence, setting the value at 0.1 ensures that benign traffic is unlikely to trigger this mechanism.

$\tau_{ip} = 0.01$. This threshold was set near zero, because we expected malware to communicate with a static set of IP addresses. This is the case when malware does not apply random IP distribution.

$\tau_{ed} = 1$. The maximum edit distance between graphs was chosen to be 1 as we expected few inconsistencies in the structure of malware graphs. Note that this is a liberal threshold in that slightly differing graph structures will pass without being detected as anomalous.

6.4.2 Parameters DECANTeR. For DECANTeR, we used the default thresholds as defined in their work [9]: the maximum outgoing information threshold being $\sigma = 1000$, the time per batch analysis $t = 10$ minutes, the amount of checks to trigger before raising an alert for background applications $\alpha = 2.5$, and the amount of checks to trigger before raising an alert for browser applications $\beta = 2.0$. To make a more fair comparison, we also ran DECANTeR with $\sigma = 10000$, analogous to ABIDED. In this second analysis, all other parameters remained the same.

6.4.3 Parameters DUMONT. DUMONT [38] only has a single parameter: the desired false-positive rate. However, the implementation we used requires an additional parameter α, which substitutes the automatic optimisation discussed in the paper. We chose a desired false-positive rate of 0.001 analogous to the comparison in the DECANTeR paper and varied our α value between 0.1 and 1.0 in steps of 0.1, resulting in 10 different detection rates with increasing false-positive rates. Next, we also ran an evaluation of DUMONT with an additional threshold, where at least 10 Kb per IP has to be exfiltrated before raising an alert. This creates a fairer comparison with ABIDED and DECANTeR.

6.4.4 Training Phase. Finally, both DECANTeR and DUMONT require a training phase in which they analyse traffic to learn its classifiers. DECANTeR demands training data without any malicious traces, whereas DUMONT requires both malicious and benign traces. The benign training traces are equivalent for both systems and are comprised of the original ClickMiner traces for the adaptive dataset; traces of the VMs without any running malware for

[7] Using the implementation of github.com/rbortolameotti/decanter/tree/master/dumont.
[8] Scripts for generating log files from Bro can be found on github.com/Thijsvanede/Master-Thesis/tree/master/analysis/logs.

the exfiltration dataset; and for each user, the first day of traces captured in the user dataset. In the case of DUMONT, we also used malicious data. For this, we randomly selected one-third of the malicious traces in the adaptive dataset and exfiltration dataset for their respective analyses. For the user dataset, we did not input any malicious traces as this dataset does not contain any. In the analyses of both systems, we used the remainder of traces in the dataset, including *all* malicious traces.

6.5 Results

We ran all three systems using the previously described datasets. A summary of our analysis can be found in Table 2, showing the performance of ABIDED, DECANTeR with $\sigma = 1000$ and $\sigma = 10000$, and DUMONT with an alpha value of 0.1, with and without the 10 Kb threshold. We chose DUMONT with the lowest alpha value, giving the lowest false-positive rate. Even so, choosing the lowest false-positive rate turned out to be orders of magnitude higher than both other systems. Hence, it will not be useful in practice. Furthermore, all detection rates of DUMONT were found to be significantly lower, due to the low α value chosen in this analysis. For the complete results, please see the Appendix.

Upon scrutinisation, we found that ABIDED and DECANTeR perform relatively similarly on the (M0) and (M1), and exfiltration datasets. DECANTeR slightly outperforms ABIDED on our newly created dataset with the low threshold, and is notably better in the detection of the actual malware samples. This is mainly due to the lower threshold for outgoing information as can be seen from the drop in detection when we use the threshold of 10 Kb. Some of the malware samples exfiltrate between 1 Kb and 10 Kb and will therefore not get detected. However, on the adaptive (M2) and (M3) datasets, ABIDED shows considerably better results with detection rates of 86.7% and 99.5% compared to rates of 8.5% and 2% in the case of DECANTeR. In addition, ABIDED shows the lowest false-positive rate of all three systems in the user dataset with 0.86%, compared with 5.5% for DECANTeR, and 38.8% for DUMONT. Future work could combine aspects of ABIDED and DECANTeR to achieve high detection rates of actual malware like DECANTeR while still being able to detect (M2) and (M3) malware as ABIDED does.

Finally, we observe that for both ABIDED and DECANTeR, the aggressiveness of the strategy is positively correlated with the detection rate. Both systems fail in detecting exfiltration with the S1 strategy, with the exception of (M1) exfiltration using the S1 strategy, which is detected by DECANTeR. DUMONT does not distinguish between strategies in detecting exfiltration. Furthermore, we find that the most detected exfiltration location for both ABIDED and DECANTeR is the URI. This is due to the creation of the Referrer Graph in both cases. When the URI changes, the graphs will not be linked and therefore the messages are more likely to trigger an alert. The HTTP body seems to be the best exfiltration location. Because both ABIDED and DECANTeR do not analyse the body value, but merely its size, no contextual data can be identified which makes it the optimal strategy. Nevertheless, ABIDED still detects 71.4% of (M2) body exfiltration. DECANTeR only detects 9.5% of (M2) body exfiltration. DUMONT does not distinguish between exfiltration locations in detecting exfiltration.

Table 2: Summary of the detection performance of ABIDED, DECANTeR and DUMONT. We include the number of true positives (TP), true negative (TN), false positives (FP), false negatives (FN), true-positive rate (TPR), false-positive rate (FPR) and accuracy (Acc). All amounts are $\times$ 1000.

(a) Summary of ABIDED.

Dataset	TP	TN	FP	FN	TPR	FPR	Acc
M0	88.9	211.1	2.3	0.2	99.8%	1.10%	99.2%
M1	32.0	213.3	2.3	0.2	99.4%	1.07%	99.0%
M2	71.9	1075.0	11.6	11.0	86.7%	1.07%	98.1%
M3	87.4	1070.5	11.7	0.4	99.5%	1.08%	99.0%
Malware	3.2	0.0	0.0	1.5	67.6%	0.00%	67.6%
Users	0.0	50.6	0.4	0.0	0.0%	0.86%	99.1%

(b) Summary of DECANTeR $\sigma = 1000$.

Dataset	TP	TN	FP	FN	TPR	FPR	Acc
M0	88.9	214.0	0.1	0.2	99.7%	0.06%	99.9%
M1	32.2	216.3	0.0	0.0	100.0%	0.01%	100.0%
M2	7.0	1089.9	0.2	75.9	8.5%	0.02%	93.5%
M3	1.8	1085.3	0.3	86.0	2.0%	0.03%	92.6%
Malware	3.7	0.0	0.0	1.2	75.3%	0.00%	75.3%
Users	0.0	28.8	1.7	0.0	0.0%	5.50%	94.5%

(c) Summary of DECANTeR $\sigma = 10000$.

Dataset	TP	TN	FP	FN	TPR	FPR	Acc
M0	85.4	214.1	0.0	3.7	95.9%	0.01%	98.8%
M1	30.5	216.3	0.0	1.8	94.4%	0.01%	99.3%
M2	7.0	1089.9	0.2	75.9	8.5%	0.02%	93.5%
M3	0.0	1085.4	0.2	87.8	0.0%	0.02%	92.5%
Malware	3.4	0.0	0.0	1.5	69.1%	0.00%	69.1%
Users	0.0	28.6	1.8	0.0	0.0%	6.05%	94.0%

(d) Summary of DUMONT, $\alpha = 0.1$.

Dataset	TP	TN	FP	FN	TPR	FPR	Acc
M0	5.7	184.4	29.7	83.4	6.4%	13.9%	62.7%
M1	2.4	190.3	26.1	29.9	7.6%	12.0%	77.5%
M2	18.9	924.3	165.8	64.0	22.8%	15.2%	80.4%
M3	20.7	924.1	161.6	67.1	23.6%	14.9%	80.5%
Malware	1.2	0.0	0.0	3.6	25.7%	0.0%	25.7%
Users	0.0	18.6	11.8	0.0	0.0%	38.8%	61.2%

(e) Summary of DUMONT $\sigma = 10000$, $\alpha = 0.1$.

Dataset	TP	TN	FP	FN	TPR	FPR	Acc
M0	18.3	206.9	7.3	70.7	20.6%	3.4%	74.3%
M1	6.9	206.9	9.5	25.4	21.5%	4.4%	86.0%
M2	21.5	1047.8	42.3	61.5	25.9%	3.9%	91.2%
M3	34.8	1050.0	35.6	53.0	39.7%	3.3%	92.5%
Malware	1.2	0.0	0.0	3.7	23.8%	0.0%	23.8%
Users	0.0	25.3	5.1	0.0	0.0%	16.7%	83.3%

7 DISCUSSION

Our work has shown that it is possible to bypass most state-of-the-art detection techniques such as DECANTeR and DUMONT. Furthermore, we have introduced a novel detection technique to cope with this new type of attack. However, we made several assumptions with regard to the malware and its detection which might differ in practice. On the one hand, we assumed the malware is able to observe the host which might pose difficulties in practice. On the other hand, we assumed malware to exhibit constant flows of exfiltration which in practice can be randomised to avoid detection. In this section we discuss the limitations of our research and suggest approaches to fixing this in future research.

First, we assume that malware is able to listen to traffic on the host. In UNIX systems, TCP ports 0-1023 require root privileges, i.e. the malware demands root privileges in order to listen to most traffic on the infected host. This decreases the likelihood of an attack as malware either needs to obtain root access or needs to find different ways of mimicking the host's traffic.

Second, (M2) malware is able to hook to a page visit in the Referrer Graph. However, when it exfiltrates too much data duringth such a page visit, it might seem anomalous to a detection system. ABIDED does not check for this property as it expects that adaptive malware will try not to exceed any imposed traffic limit. Nevertheless, (M2) malware benefits from not exfiltrating too much data in a single page visit to avoid other detection methods. This limits the exfiltration rate of this malware type as page visits are initiated by the user. As Figure 3 illustrates, these are not very frequent: only 22 page visits occur in 20 minutes of browsing time. Therefore, the rate at which data can be exfiltrated is limited. Future research could explore the limits this heuristic brings to malware.

As stated earlier, another complication - specifically for the (M3) attacker - is that it is difficult to alter its communication pattern. There are two possible scenario's. First, the attacker could use state machines to define its behaviour. Hereby, adapting to new patterns from the host requires sending out data to the server using a predefined pattern, as the server would otherwise be unable to respond appropriately. Second, the malicious server might communicate by embedding its communication in validly generated application response messages unknown to the malware on the infected host. In this case, malware is required to interpret the response as if it were the actual application it tries to imitate. More complex applications - such as a browser - would require an engine such as the Servo used by Firefox Quantum [4] to correctly interpret the received messages. Simple scripting in combination with a program as CURL would be insufficient as message interpretation becomes too complex. The downside for malware is that this would increase resource consumption and the size of its binary, making it easier to be discovered in host-based detection.

Finally, the strategies that we used in the creation of exfiltrating malware were theoretically substantiated and set a priori. However, a strategy could also be set in real-time by observing regular traffic from the infected host and determining the maximum speed at which data could be exfiltrated. Future research could experiment with malware which observes its host to learn the optimal exfiltration strategy for the communication channel it tries to mimic.

The previously described limitations make it more difficult for an adversary to carry out an (M2) or (M3) attack. First, as malware will have difficulties sniffing traffic on the host, it becomes more difficult to adapt its own messages to observed ones. Second, because there are other possible detection techniques such as anomaly detection in traffic volume which impose limitations on the exfiltration speed of malware. However, we have also made some critical assumptions in our detection system ABIDED which might not be present in all exfiltrating malware.

First, we assumed that (M2) malware exfiltrates data at a constant speed, giving rise to our volatility threshold. However, if malware were to randomise the amount of time between messages or the amount of data it exfiltrates per message, the volatility of its connection would increase. By behaving in such a way, malware would be able to circumvent our detection system with relatively little effort. To counter this problem, we suggest to make it more difficult for an attacker to attach itself to a page visit in the graph. At this moment, the attacker can hook itself onto the graph by setting the referrer field of its own messages. However, if a graph is linked in ways where the attacker does not control the linking process, an attacker would be unable to influence the volatility of a page visit. For example, ClickMiner [34] presents an approach which links requests based on analysing the HTTP response messages of servers which the attacker cannot control. This would remove the limitation imposed by the volatility threshold.

Second, we assumed that malware does not distribute its exfiltration over different IP addresses. If it were so, malware would be able to stay below the 10 Kb threshold of outgoing information as long as it distributes over enough IP addresses. By randomising the distribution in a clever way, malware could also deceive our IP volatility threshold. The increase in the amount of additional IPs required to exfiltrate data can be described as a linear function of the amount of data to exfiltrate per time unit with respect to the outgoing information threshold. Thus, this method of exfiltrating data will also increase costs for the adversary as it needs to maintain multiple servers and coordinate the exfiltration. Albeit, the coordination of exfiltration over multiple IP addresses only needs to be designed once. Additionally, the costs of operating multiple servers are rather low, e.g. when the adversary controls a botnet containing a vast amount of machines. However, using multiple IP addresses increases the probability of communicating with a blacklisted IP, and thus of being detected. Nevertheless, this makes IP distribution attacks a potential threat for our detection technique. We suggest further research into combining our solution with techniques such as IP blacklisting to complement this weakness in ABIDED.

Finally, in the (M3) detection, we assumed the malware to follow a predetermined pattern. As discussed before, this assumption is valid because setting up learned communication requires using some predefined pattern first, and using more advanced parsing of messages would require too many resources for malware to remain undetected by host-based anomaly detection systems. However, in our detection, we assumed that the pattern defined by the malware is almost completely static, i.e. we conjectured that the Referrer Graph created by malware has an edit distance of at maximum 1 between other Referrer Graphs created by the same malware. This is a rather strict assumption to make, as the malware might send out noisy data to different servers, e.g. requesting images from Google

or Facebook. Hence, to avoid overfitting to our implementation of the malware, detection might prove to be more flexible in exposing other implementations of (M3) malware when we use the largest common subgraph as a detection metric. However, future research would need to verify whether this is the case.

The final set of suggested improvements are at a more global level of detection. ABIDED currently does not have a training phase in which it learns its parameters. The current parameters *were* empirically determined, but this was done manually. Using a training phase could automate this process and thereby increase applicability of the system. Another improvement might be made in the modelling of HTTP behaviour, which is currently done through a Referrer Graph. As we have seen, malware is capable of hooking onto the graph by adapting its HTTP referrer field. However, there exist several other methods of linking, some of which restrict the capabilities of (M2)-(M3) malware to hook onto such a graph. Future research should verify whether strengthening the dynamic model against attacks will compensate for the loss of efficiency.

8 CONCLUSION

Our work introduced a novel malware communication attack over HTTP, capable of bypassing state-of-the-art detection systems. This attack learns the behaviour of its victim and adapts its communication such that it is indistinguishable from benign traffic by a network level detection mechanism. Although we described the attack as HTTP based, we expect it to be generalisable for other protocols as well. We introduced a taxonomy to distinguish between various levels of attacker sophistication. Next, we proved the feasibility of such an attack by creating malware which tries to exfiltrate sensitive data from an infected machine by imitating the communication of the victim's browser application. This malware was able to go largely undetected by state-of-the-art detection systems DECANTeR (detection rate of 5.2%) and DUMONT (detection rate of 23.2%). To tackle the problem of detection, we introduced several heuristics for the dynamic behaviour of browser applications and combined these into our detection system ABIDED. This novel system yielded an improved detection rate as compared to the other state-of-the-art solutions, totalling 93.3%.

REFERENCES

[1] Dilara Acarali, Muttukrishnan Rajarajan, Nikos Komninos, and Ian Herwono. 2016. Survey of approaches and features for the identification of HTTP-based botnet traffic. *Journal of Network and Computer Applications* 76 (2016), 1–15.

[2] Areej Al-Bataineh and Gregory White. 2012. Analysis and detection of malicious data exfiltration in web traffic. In *Malicious and Unwanted Software (MALWARE), 2012 7th International Conference on*. IEEE, 26–31.

[3] Mamoun Alazab, Sitalakshmi Venkatraman, Paul Watters, Moutaz Alazab, and Ammar Alazab. 2012. Cybercrime: the case of obfuscated malware. *Global Security, Safety and Sustainability & e-Democracy* (2012), 204–211.

[4] Brian Anderson, Lars Bergstrom, Manish Goregaokar, Josh Matthews, Keegan McAllister, Jack Moffitt, and Simon Sapin. 2016. Engineering the servo web browser engine using Rust. In *Proceedings of the 38th International Conference on Software Engineering Companion*. ACM, 81–89.

[5] Elisa Bertino and Gabriel Ghinita. 2011. Towards mechanisms for detection and prevention of data exfiltration by insiders: keynote talk paper. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. ACM, 10–19.

[6] Sam Biddle. 2016. The NSA leak is real, Snowden documents confirm. https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/. (August 2016).

[7] Arnab Kumar Biswas, Dipak Ghosal, and Shishir Nagaraja. 2017. A Survey of Timing Channels and Countermeasures. *ACM Computing Surveys (CSUR)* 50, 1 (2017), 6.

[8] Kevin Borders and Atul Prakash. 2004. Web tap: detecting covert web traffic. In *Proceedings of the 11th ACM conference on Computer and communications security*. ACM, 110–120.

[9] R. Bortolameotti, T.S. van Ede, M. Caselli, M.H. Everts, P.H. Hartel, R. Hofstede, W. Jonker, and A. Peter. 2017. DECANTeR: DEteCtion of Anomalous outbouNd HTTP TRaffic by Passive Application Fingerprinting. In *Proceedings of the 33rd Annual Computer Security Applications Conference, ACSAC (ACM)*.

[10] Johannes Bouché, Denis Hock, and Martin Kappes. 2016. On the Performance of Anomaly Detection Systems Uncovering Traffic Mimicking Covert Channels.. In *INC*. 19–24.

[11] Horst Bunke. 1997. On a relation between graph edit distance and maximum common subgraph. *Pattern Recognition Letters* 18, 8 (1997), 689–694.

[12] Patrick Butler, Kui Xu, and Danfeng Yao. 2011. Quantitatively analyzing stealthy communication channels. In *Applied Cryptography and Network Security*. Springer, 238–254.

[13] Laurent Butti and Franck Veysset. 2006. Wi-fi advanced stealth. *Proc. Black Hat US* (2006).

[14] Matteo Casenove. 2015. Exfiltrations using polymorphic blending techniques: Analysis and countermeasures. In *Cyber Conflict: Architectures in Cyberspace (CyCon), 2015 7th International Conference on*. IEEE, 217–230.

[15] Wentao Chang, Aziz Mohaisen, An Wang, and Songqing Chen. 2015. Measuring botnets in the wild: Some new trends. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. ACM, 645–650.

[16] Christian J Dietrich, Christian Rossow, Felix C Freiling, Herbert Bos, Maarten Van Steen, and Norbert Pohlmann. 2011. On Botnets that use DNS for Command and Control. In *Computer Network Defense (EC2ND), 2011 Seventh European Conference on*. IEEE, 9–16.

[17] Holger Dreger, Anja Feldmann, Michael Mai, Vern Paxson, and Robin Sommer. 2006. Dynamic Application-Layer Protocol Analysis for Network Intrusion Detection.. In *USENIX Security Symposium*. 257–272.

[18] Kevin P Dyer, Scott E Coull, Thomas Ristenpart, and Thomas Shrimpton. 2013. Protocol misidentification made easy with format-transforming encryption. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 61–72.

[19] Kevin P Dyer, Scott E Coull, and Thomas Shrimpton. 2015. Marionette: A programmable network traffic obfuscation system. In *24th USENIX Security Symposium (USENIX Security 15)*. 367–382.

[20] Roy Fielding, Jim Gettys, Jeffrey Mogul, Henrik Frystyk, Larry Masinter, Paul Leach, and Tim Berners-Lee. 1999. *Hypertext transfer protocol–HTTP/1.1*. Technical Report.

[21] Pedro Garcia-Teodoro, J Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security* 28, 1 (2009), 18–28.

[22] Gemalto. 2017. *Breach Level Index*. Technical Report. Gemalto.

[23] Guofei Gu, Phillip A Porras, Vinod Yegneswaran, Martin W Fong, and Wenke Lee. 2007. BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation.. In *USENIX Security Symposium*, Vol. 7. 1–16.

[24] Negar Kiyavash and Todd Coleman. 2009. Covert timing channels codes for communication over interactive traffic. In *Acoustics, Speech and Signal processing, 2009. ICASSP 2009. IEEE international conference on*. IEEE, 1485–1488.

[25] Oleg Kolesnikov and Wenke Lee. 2005. *Advanced polymorphic worms: Evading ids by blending in with normal traffic*. Technical Report. Georgia Institute of Technology.

[26] Christian Krätzer, Jana Dittmann, Andreas Lang, and Tobias Kühne. 2006. WLAN steganography: a first practical review. In *Proceedings of the 8th workshop on Multimedia and security*. ACM, 17–22.

[27] Zbigniew Kwecka. 2006. Application layer covert channel analysis and detection. *Undergraduate Project Dissertation, Napier University* (2006).

[28] Simon Liu and Rick Kuhn. 2010. Data loss prevention. *IT professional* 12, 2 (2010).

[29] Yali Liu, Cherita Corbett, Ken Chiang, Rennie Archibald, Biswanath Mukherjee, and Dipak Ghosal. 2009. SIDD: A framework for detecting sensitive data exfiltration by an insider attack. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*. IEEE, 1–10.

[30] Xiapu Luo, Edmond WW Chan, and Rocky KC Chang. 2008. TCP covert timing channels: Design and detection. In *Dependable Systems and Networks With FTCS and DCC, 2008. DSN 2008. IEEE International Conference on*. IEEE, 420–429.

[31] Wojciech Mazurczyk and Krzysztof Szczypiorski. 2008. Steganography of VoIP streams. *On the move to meaningful Internet systems: OTM 2008* (2008), 1001–1018.

[32] Steven J Murdoch and Stephen Lewis. 2005. Embedding covert channels into TCP/IP. In *Information hiding*, Vol. 3727. Springer, 247–261.

[33] Tarique Mustafa. 2013. Malicious data leak prevention and purposeful evasion attacks: an approach to advanced persistent threat (APT) management. In *Electronics, Communications and Photonics Conference (SIECPC), 2013 Saudi International*. IEEE, 1–5.

[34] Christopher Neasbitt, Roberto Perdisci, Kang Li, and Terry Nelms. 2014. Clickminer: Towards forensic reconstruction of user-browser interactions from network traces. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and*

Communications Security. ACM, 1244–1255.
[35] Philip O'Kane, Sakir Sezer, and Kieran McLaughlin. 2011. Obfuscation: The hidden malware. *IEEE Security & Privacy* 9, 5 (2011), 41–47.
[36] Vern Paxson. 1999. Bro: a system for detecting network intruders in real-time. *Computer networks* 31, 23 (1999), 2435–2463.
[37] Huyu Qu, Qiang Cheng, and Ece Yaprak. 2005. Using Covert Channel to Resist DoS attacks in WLAN.. In *ICWN*. 38–44.
[38] Guido Schwenk and Konrad Rieck. 2011. Adaptive detection of covert communication in http requests. In *Computer Network Defense (EC2ND), 2011 Seventh European Conference on*. IEEE, 25–32.
[39] Stephen Sheridan and Anthony Keane. 2017. Improving the Stealthiness of DNS-Based Covert Communication. (2017).
[40] Xiaokui Shu and Danfeng (Daphne) Yao. 2012. Data Leak Detection as a Service.. In *SecureComm*. Springer, 222–240.
[41] Colin Tankard. 2011. Advanced persistent threats and how to monitor and deter them. *Network security* 2011, 8 (2011), 16–19.
[42] Julian R Ullmann. 1976. An algorithm for subgraph isomorphism. *Journal of the ACM (JACM)* 23, 1 (1976), 31–42.
[43] Ke Wang, Janak Parekh, and Salvatore Stolfo. 2006. Anagram: A content anomaly detector resistant to mimicry attack. In *Recent Advances in Intrusion Detection*. Springer, 226–248.
[44] Guowu Xie, Marios Iliofotou, Thomas Karagiannis, Michalis Faloutsos, and Yaohui Jin. 2013. Resurf: Reconstructing web-surfing activity from network traffic. In *IFIP Networking Conference, 2013*. IEEE, 1–9.
[45] Ilsun You and Kangbin Yim. 2010. Malware obfuscation techniques: A brief survey. In *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on*. IEEE, 297–300.
[46] Shui Yu, Guofeng Zhao, Song Guo, Yang Xiang, and Athanasios V Vasilakos. 2011. Browsing behavior mimicking attacks on popular web sites for large botnets. In *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*. IEEE, 947–951.
[47] Sebastian Zander, Grenville Armitage, and Philip Branch. 2007. A survey of covert channels and countermeasures in computer network protocols. *IEEE Communications Surveys & Tutorials* 9, 3 (2007), 44–57.
[48] Hao Zhang, Danfeng Daphne Yao, Naren Ramakrishnan, and Zhibin Zhang. 2016. Causality reasoning about network events for detecting stealthy malware activities. *computers & security* 58 (2016), 180–198.

A DATASETS

In section we give a broader overview of the datasets used for the analysis. For the analysis we use three different datasets: the adaptive dataset; the exfiltration dataset; and the user dataset. The first contains regular traces as well as malicious traces created by our implementation of the adaptive attack introduced in this paper. The second contains traces of exfiltrating malware in the wild, and the last contains benign traces of four researchers from our university.

A.1 Adaptive Dataset

The adaptive dataset was created by replaying the browser traces of the 10 user traces from the ClickMiner [34] dataset which contained the most HTTP request-response pairs. While doing this, we ran our different implementations of the (M0)-(M3) malware. The total was recorded using `tcpdump` and is summarised in Table 3.

A.2 Exfiltration Dataset

The exfiltration dataset used from the DECANTeR paper was created by running different instances of malware in a Cuckoo sandbox. The malware ran in either a Windows XP or Windows 7 virtual machine. All communication was captured using `tcpdump` and is summarised in Table 4. Note that in the cases of malware, all traces are considered malicious as there was no user interaction with the machines.

A.3 User Dataset

Finally, the user dataset used from the DECANTeR paper was recorded by observing the traffic from four researchers at our university. They did not have any active malware on their machine and thus all traffic is considered benign. Table 5 contains a summary of the user dataset.

Table 3: Summary of Adaptive Dataset.

Malware	Files	Total Size	Benign requests	Benign responses	Malicious requests	Malicious responses
M0	50	5.3 GB	524009	613075	89066	0
M1	50	5.3 GB	561773	561789	32296	32280
M2	250	26.2 GB	2728495	2728524	82965	82936
M3	250	26.1 GB	2718066	2733638	87801	72229
Total	600	62.9 GB	6532343	6637026	292128	187445

Table 4: Summary of Exfiltration Dataset.

Malware	Files	Total Size	Benign requests	Benign responses	Malicious requests	Malicious responses
COSMIC_DUKE	15	12.6 MB	0	0	6691	6629
FAREIT	15	0.8 MB	0	0	150	165
FTPINFOSTEAL	9	0.4 MB	0	0	207	110
SHAKTI	3	12.7 MB	0	0	460	431
SPYWARE	12	3.4 MB	0	0	2018	1352
TIM	4	20.1 MB	0	0	153	127
URSNIF	34	253.8 MB	0	0	3139	2887
Total	92	303.8 MB	0	0	12818	11701

Table 5: Summary of User Dataset.

User	Capture length	Total Size	Benign requests	Benign responses	Malicious requests	Malicious responses
User 1	7 days	2.5 GB	10833	10833	0	0
User 2	4 days	1.4 GB	180669	23427	0	0
User 3	9 days	8.2 GB	1280818	56400	0	0
User 4	4 days	2.9 GB	20840	21359	0	0
Total	-	15 GB	1493160	112019	0	0

B ANALYSIS ABIDED

This part of the appendix contains the results from the analysis of ABIDED performed on three datasets:

- Adaptive dataset
- Exfiltration dataset
- User dataset

For this analysis, ABIDED used the parameters displayed in Table 6.

Table 6: Parameters ABIDED analysis

Parameter	Value
window	10 seconds
max_outgoing_info_volatility	200
max_io_ratio	0.1
max_ip_volatility	0.01
max_outgoing_info	10000
max_edit_distance	1

B.1 Results Adaptive Dataset

The results of the adaptive dataset can be found in Tables 7-17. Each Table contains the analysis for malware (M0)-(M3) as well as the result for the total dataset. We present a summary of the analysis in Table 7 and have split the data per strategy in Tables 8-12 and per exfiltration field in Tables 13-17. Note that for the latter, (M0) and (M1) display 0 samples as they do not specify any exfiltration field. In reality, they both use the URI to exfiltrate data.

B.2 Results Exfiltration Dataset

The results of the exfiltration dataset can be found in Table 18. It contains traces from five different malware samples. Note that not all packets in the dataset were exfiltrating data, some where C&C communication which were not detected as exfiltrating data packets. Furthermore, the TIM malware sample did not exfiltrate enough data to be detected at all. I.e. it did not exceed the exfiltration threshold of 10Kb used for the ABIDED detection.

B.3 Results User Dataset

The results of the user dataset can be found in Table 19. It contains traces from 4 different university researchers. The devices of these researchers did not contain any exfiltrating malware and are therefore used to determine a reliable false positive rate of the ABIDED system. As Table 19 indicates, ABIDED achieves a false positive rate of 0.86%.

Table 7 ABIDED - Overall analysis adaptive dataset

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	302511	88857	211116	2338	200	0.9978	0.0110	0.9916
M1	247965	32096	213354	2315	200	0.9938	0.0107	0.9899
M2	1169631	71891	1075051	11615	11074	0.8665	0.0107	0.9806
M3	1169985	87401	1070530	11654	400	0.9954	0.0108	0.9897
Total	2890092	280245	2570051	27922	11874	0.9594	0.0107	0.9862

Table 8 ABIDED - Analysis adaptive dataset - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	43310	0	42647	463	200	0.0000	0.0107	0.9847
M1	42965	0	42302	463	200	0.0000	0.0108	0.9846
M2	217449	0	214962	2315	172	0.0000	0.0107	0.9886
M3	214962	0	212174	2388	400	0.0000	0.0111	0.9870
Total	518686	0	512085	5629	972	0.0	0.0109	0.9873

Table 9 ABIDED - Analysis adaptive dataset - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	61610	19940	41150	520	0	1.000	0.0125	0.9916
M1	54575	11514	42598	463	0	1.000	0.0108	0.9915
M2	232377	12082	215842	2320	2133	0.8499	0.0106	0.9808
M3	245582	29247	214054	2281	0	1.000	0.0105	0.9907
Total	594144	72783	513644	5584	2133	0.9715	0.0108	0.987

Table 10 ABIDED - Analysis adaptive dataset - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	62578	19366	42745	467	0	1.0000	0.0108	0.9925
M1	50843	7892	42488	463	0	1.0000	0.0108	0.9909
M2	230799	11103	215347	2320	2029	0.8455	0.0107	0.9812
M3	237895	22649	212919	2327	0	1.0000	0.0108	0.9902
Total	582115	61010	513499	5577	2029	0.9678	0.0107	0.9869

Table 11 ABIDED - Analysis adaptive dataset - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	45971	2912	42596	463	0	1.0000	0.0108	0.9899
M1	45784	2311	43010	463	0	1.0000	0.0107	0.9899
M2	225771	8154	214112	2294	1211	0.8707	0.0106	0.9845
M3	226034	8202	215509	2323	0	1.0000	0.0107	0.9897
Total	543560	21579	515227	5543	1211	0.9469	0.0106	0.9876

Table 12 ABIDED - Analysis adaptive dataset - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	89042	46639	41978	425	0	1.0000	0.0100	0.9952
M1	53798	10379	42956	463	0	1.0000	0.0107	0.9914
M2	263235	40552	214788	2366	5529	0.88	0.0109	0.9700
M3	245512	27303	215874	2335	0	1.0000	0.0107	0.9905
Total	651587	124873	515596	5589	5529	0.9576	0.0107	0.9829

Table 13 ABIDED - Analysis adaptive dataset - Body field exfiltration

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233099	13179	212314	2319	5287	0.7137	0.0108	0.9674
M3	231161	15303	213447	2331	80	0.9948	0.0108	0.9896
Total	464260	28482	425761	4650	5367	0.8414	0.0108	0.9784

Table 14 ABIDED - Analysis adaptive dataset - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	232924	12808	216304	2189	1623	0.8875	0.0100	0.9836
M3	237902	21061	214480	2281	80	0.9962	0.0105	0.9901
Total	470826	33869	430784	4470	1703	0.9521	0.0103	0.9869

Table 15 ABIDED - Analysis adaptive dataset - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235306	15100	215989	2319	1898	0.8883	0.0106	0.9821
M3	231120	14590	214123	2327	80	0.9945	0.0108	0.9896
Total	466426	29690	430112	4646	1978	0.9375	0.0107	0.9858

Table 16 ABIDED - Analysis adaptive dataset - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234268	15764	216003	2473	28	0.9982	0.0113	0.9893
M3	232675	16978	213221	2396	80	0.9953	0.0111	0.9894
Total	466943	32742	429224	4869	108	0.9967	0.0112	0.9893

Table 17 ABIDED - Analysis adaptive dataset - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234034	15040	214441	2315	2238	0.8705	0.0107	0.9805
M3	237127	19469	215259	2319	80	0.9959	0.0107	0.9899
Total	471161	34509	429700	4634	2318	0.9371	0.0107	0.9852

Table 18: ABIDED - Analysis exfiltration dataset

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	377	0	0	21	0.9472	0.0000	0.9472
SPYWARE	1229	1219	0	0	10	0.9919	0.0000	0.9919
TIM	47	0	0	0	47	0.0000	0.0000	0.0000
URSNIF	2320	953	0	0	1367	0.4108	0.0000	0.4108
Total	4673	3157	0	0	1516	0.6756	0.0000	0.6756

Table 19: ABIDED - Analysis user dataset

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
User 1	651	0	651	0	0	0.0000	0.0000	1.0000
User 2	5211	0	5066	145	0	0.0000	0.0278	0.9722
User 3	27151	0	27000	151	0	0.0000	0.0056	0.9944
User 4	18041	0	17897	144	0	0.0000	0.0080	0.9920
Total	51054	0	50614	440	0	0.0000	0.0086	0.9914

C ANALYSIS DECANTER

This part of the appendix contains the results from the analysis of DECANTeR performed on three datasets:

- Adaptive dataset
- Exfiltration dataset
- User dataset

For this analysis, DECANTeR used the parameters displayed in Table 22 Note that. Apart from setting the parameters, DECANTeR needs training samples before it is able to analyse data. Hence for each dataset we have selected training data as described in Table 23.

C.1 Results Adaptive Dataset

The results of the adaptive dataset can be found in Tables 20-43. Each Table contains the analysis for malware (M0)-(M3) as well as the result for the total dataset. We present a summary of the analysis in Tables 20 and 21 and have split the data per strategy in Tables 24-33 and per exfiltration field in Tables 34-43. Note that for the latter, (M0) and (M1) display 0 samples as they do not specify any exfiltration field. In reality, they both use the URI to exfiltrate data.

C.2 Results Exfiltration Dataset

The results of the exfiltration dataset can be found in Tables 44 and 45. They contain traces from 7 different malware samples. The detection rate of DECANTeR is higher than that of ABIDED, because the amounts of exfiltrated data did not exceed ABIDED's threshold of 10Kb, but did exceed DECANTeR's threshold of 1Kb. This can be seen from Table 45 as this is comparable to ABIDED's performance.

Table 22: Parameters DECANTeR analysis

Parameter	Value
background_threshol	2.5
browser_threshold	2.0
outgoing_threshold	1000 & 10 000
update_threshold	0.1
known_browser_str	[Firefox, Chrome, MSIE, Edge, Opera, Safari]

Table 23: Training data for DECANTeR & DUMONT

Dataset	Training files
Adaptive dataset	Original ClickMiner traces.
Exfiltration dataset	VM traces without active malware.
User dataset	First day of capturing.

C.3 Results User Dataset

The results of the user dataset can be found in Tables 46 and 47. It contains traces from 4 different university researchers. The devices of these researchers did not contain any exfiltrating malware and are therefore used to determine a reliable false-positive rate of the DECANTeR system. As Table 46 indicates, DECANTeR achieves a false-positive rate of %5.50 for $\sigma = 1000$ and 6.05% for $\sigma = 10000$.

Table 20: DECANTeR - Overall analysis adaptive dataset - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TP-rate	FP-rate	Accuracy
M0	303192	88824	213999	136	233	0.9974	0.0006	0.9988
M1	248650	32296	216334	20	0	1.0000	0.0001	0.9999
M2	1173056	7031	1089863	228	75934	0.0847	0.0002	0.9351
M3	1173410	1765	1085299	310	86036	0.0201	0.0003	0.9264
Total	2898308	129916	2605495	694	162203	0.4447	0.0003	0.9438

Table 21: DECANTeR - Overall analysis adaptive dataset - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	85406	214115	20	3651	0.9590	0.0001	0.9879
M1	248650	30498	216334	20	1798	0.9443	0.0001	0.9927
M2	1173056	7031	1089863	228	75934	0.0847	0.0002	0.9351
M3	1173410	4	1085402	207	87797	0.0000	0.0002	0.9250
Total	2898308	122939	2605714	475	169180	0.4209	0.0002	0.9415

Table 24: DECANTeR - Analysis adaptive dataset - Strategy 1 - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	43243	4	200	0.0000	0.0001	0.9953
M1	43102	200	42898	4	0	1.0000	0.0001	0.9999
M2	218134	5	217933	29	167	0.0291	0.0001	0.9991
M3	215647	0	215120	127	400	0.0000	0.0006	0.9976
Total	520330	205	519194	164	767	0.2109	0.0003	0.9982

Table 25: DECANTeR - Analysis adaptive dataset - Strategy 1 - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	43243	4	200	0.0000	0.0001	0.9953
M1	43102	0	42898	4	200	0.0000	0.0001	0.9953
M2	218134	5	217933	29	167	0.0291	0.0001	0.9991
M3	215647	0	215223	24	400	0.0000	0.0001	0.9980
Total	520330	5	519297	61	967	0.0051	0.0001	0.9980

Table 26: DECANTeR - Analysis adaptive dataset - Strategy 2 - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	19929	41683	120	11	0.9994	0.0029	0.9979
M1	54712	11514	43194	4	0	1.0000	0.0001	0.9999
M2	233062	987	218781	66	13228	0.0694	0.0003	0.9430
M3	246267	546	216998	22	28701	0.0187	0.0001	0.8834
Total	595784	32976	520656	212	41940	0.4402	0.0004	0.9292

Table 27: DECANTeR - Analysis adaptive dataset - Strategy 2 - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	19423	41799	4	517	0.9741	0.0001	0.9916
M1	54712	11514	43194	4	0	1.0000	0.0001	0.9999
M2	233062	987	218781	66	13228	0.0694	0.0003	0.9430
M3	246267	3	216998	22	29244	0.0001	0.0001	0.8812
Total	595784	31927	520772	96	42989	0.4262	0.0002	0.9277

Table 28: DECANTeR - Analysis adaptive dataset - Strategy 3 - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	19366	43345	4	0	1.0000	0.0001	0.9999
M1	50980	7892	43084	4	0	1.0000	0.0001	0.9999
M2	231484	982	218324	28	12150	0.0748	0.0001	0.9474
M3	238580	428	215861	70	22221	0.0189	0.0003	0.9066
Total	583759	28668	520614	106	34371	0.4548	0.0002	0.9409

Table 29: DECANTeR - Analysis adaptive dataset - Strategy 3 - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	19366	43345	4	0	1.0000	0.0001	0.9999
M1	50980	7868	43084	4	24	0.9970	0.0001	0.9995
M2	231484	982	218324	28	12150	0.0748	0.0001	0.9474
M3	238580	1	215861	70	22648	0.0000	0.0003	0.9048
Total	583759	28217	520614	106	34822	0.4476	0.0002	0.9402

Table 30: DECANTeR - Analysis adaptive dataset - Strategy 4 - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	2912	43192	4	0	1.0000	0.0001	0.9999
M1	45921	2311	43606	4	0	1.0000	0.0001	0.9999
M2	226456	717	217011	80	8648	0.0766	0.0004	0.9615
M3	226719	167	218464	53	8035	0.0204	0.0002	0.9643
Total	545204	6107	522273	141	16683	0.2680	0.0003	0.9691

Table 31: DECANTeR - Analysis adaptive dataset - Strategy 4 - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	0	43192	4	2912	0.0000	0.0001	0.9368
M1	45921	737	43606	4	1574	0.3189	0.0001	0.9656
M2	226456	717	217011	80	8648	0.0766	0.0004	0.9615
M3	226719	0	218464	53	8202	0.0000	0.0002	0.9636
Total	545204	1454	522273	141	21336	0.0638	0.0003	0.9606

Table 32: DECANTeR - Analysis adaptive dataset - Strategy 5 - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	46617	42536	4	22	0.9995	0.0001	0.9997
M1	53935	10379	43552	4	0	1.0000	0.0001	0.9999
M2	263920	4340	217814	25	41741	0.0942	0.0001	0.8417
M3	246197	624	218856	38	26679	0.0229	0.0002	0.8915
Total	653231	61960	522758	71	68442	0.4751	0.0001	0.8951

Table 33: DECANTeR - Analysis adaptive dataset - Strategy 5 - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	46617	42536	4	22	0.9995	0.0001	0.9997
M1	53935	10379	43552	4	0	1.0000	0.0001	0.9999
M2	263920	4340	217814	25	41741	0.0942	0.0001	0.8417
M3	246197	0	218856	38	27303	0.0000	0.0002	0.8889
Total	653231	61336	522758	71	69066	0.4704	0.0001	0.8942

Table 34: DECANTeR - Analysis adaptive dataset - Body exfiltration - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	1747	215211	107	16719	0.0946	0.0005	0.9280
M3	231846	0	216441	22	15383	0.0000	0.0001	0.9336
Total	465630	1747	431652	129	32102	0.0516	0.0003	0.9308

Table 35: DECANTeR - Analysis adaptive dataset - Body exfiltration - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	1747	215211	107	16719	0.0946	0.0005	0.9280
M3	231846	0	216441	22	15383	0.0000	0.0001	0.9336
Total	465630	1747	431652	129	32102	0.0516	0.0003	0.9308

Table 36: DECANTeR - Analysis adaptive dataset - Cookie field exfiltration - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	8	219148	30	14423	0.0006	0.0001	0.9381
M3	238587	0	217425	21	21141	0.0000	0.0001	0.9113
Total	472196	8	436573	51	35564	0.0002	0.0001	0.9246

Table 37: DECANTeR - Analysis adaptive dataset - Cookie field exfiltration - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	8	219148	30	14423	0.0006	0.0001	0.9381
M3	238587	0	217425	21	21141	0.0000	0.0001	0.9113
Total	472196	8	436573	51	35564	0.0002	0.0001	0.9246

Table 38: DECANTeR - Analysis adaptive dataset - Custom field exfiltration - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	0	218971	22	16998	0.0000	0.0001	0.9279
M3	231805	0	217110	25	14670	0.0000	0.0001	0.9366
Total	467796	0	436081	47	31668	0.0000	0.0001	0.9322

Table 39: DECANTeR - Analysis adaptive dataset - Custom field exfiltration - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	0	218971	22	16998	0.0000	0.0001	0.9279
M3	231805	0	217110	25	14670	0.0000	0.0001	0.9366
Total	467796	0	436081	47	31668	0.0000	0.0001	0.9322

Table 40: DECANTeR - Analysis adaptive dataset - URI exfiltration - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	5275	219148	13	10517	0.3340	0.0001	0.9552
M3	233360	3	216128	174	17055	0.0002	0.0008	0.9262
Total	468313	5278	435276	187	27572	0.1607	0.0004	0.9407

Table 41: DECANTeR - Analysis adaptive dataset - URI exfiltration - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	5275	219148	13	10517	0.3340	0.0001	0.9552
M3	233360	3	216231	71	17055	0.0002	0.0003	0.9266
Total	468313	5278	435379	84	27572	0.1607	0.0002	0.9409

Table 42: DECANTeR - Analysis adaptive dataset - User-Agent field exfiltration - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	1	217385	56	17277	0.0001	0.0003	0.9262
M3	237812	1762	218195	68	17787	0.0901	0.0003	0.9249
Total	472531	1763	435580	124	35064	0.0479	0.0003	0.9255

Table 43: DECANTeR - Analysis adaptive dataset - User-Agent field exfiltration - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	1	217385	56	17277	0.0001	0.0003	0.9262
M3	237812	1	218195	68	19548	0.0001	0.0003	0.9175
Total	472531	2	435580	124	36825	0.0001	0.0003	0.9218

Table 44: DECANTeR - Analysis exfiltration dataset - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	68	0	0	0	1.0000	0.0000	1.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	398	0	0	0	1.0000	0.0000	1.0000
SPYWARE	1241	982	0	0	259	0.7913	0.0000	0.7913
TIM	67	65	0	0	2	0.9701	0.0000	0.9701
URSNIF	2472	1534	0	0	938	0.6206	0.0000	0.6206
Total	4857	3655	0	0	1202	0.7525	0.0000	0.7525

Table 45: DECANTeR - Analysis exfiltration dataset - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	68	0	0	0	1.0000	0.0000	1.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	398	0	0	0	1.0000	0.0000	1.0000
SPYWARE	1241	866	0	0	375	0.6978	0.0000	0.6978
TIM	67	65	0	0	2	0.9701	0.0000	0.9701
URSNIF	2472	1351	0	0	1121	0.5465	0.0000	0.5465
Total	4857	3356	0	0	1501	0.6910	0.0000	0.6910

Table 46: DECANTeR - Analysis user dataset - $\sigma = 1000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3936	21	0	0.0000	0.0053	0.9947
User 2	243	0	241	2	0	0.0000	0.0082	0.9918
User 3	17210	0	16679	531	0	0.0000	0.0309	0.9691
User 4	9011	0	7894	1117	0	0.0000	0.1240	0.8760
Total	30421	0	28750	1671	0	0.0000	0.0550	0.9451

Table 47: DECANTeR - Analysis user dataset - $\sigma = 10000$

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3936	21	0	0.0000	0.0053	0.9947
User 2	243	0	241	2	0	0.0000	0.0082	0.9918
User 3	17210	0	16680	530	0	0.0000	0.0308	0.9692
User 4	9011	0	7725	1286	0	0.0000	0.1427	0.8573
Total	30421	0	28582	1839	0	0.0000	0.0605	0.9395

D ANALYSIS DUMONT

This part of the appendix contains the results from the analysis of DUMONT performed on three datasets:

- Adaptive dataset
- Exfiltration dataset
- User dataset

DUMONT uses two parameters for its detection, the predefined false-positive rate, from here on referred to as *fp* and a parameter *alpha* used to calibrate its detectors. For this detection we have chosen an *fp* of 0.001 and 10 different *alpha*'s, ranging from 0.1 to 1.0. As with DECANTeR, DUMONT requires a training phase, we used the same training samples as DECANTeR, which are described in Table 23. Furthermore, DUMONT also requires malicious samples for its training phase. Since the training data used in DECANTeR does not contain any malicious samples, we have randomly chosen one-third of the test data as malicious samples for the training data. Note that the full test data - including the samples used for training - are tested in the analysis. Finally, we have executed the analysis with both the DUMONT system as described in the paper, and performed an analysis with the addition of an exfiltration threshold of 10 Kb. These results are marked with $\sigma = 10000$.

D.1 Results Adaptive Dataset

The results of the adaptive dataset can be found in Tables 48-267. Each Table contains the analysis for malware (M0)-(M3) as well as the result for the total dataset. Each Table indicates the alpha that was used for the analysis, which ranges from 0.1 to 1.0. Furthermore, each Table indicates whether it was executed with or without the outgoing information threshold of 10 Kb.

We present a summary of the analysis per alpha in Tables 48-57 for the regular DUMONT and in Tables 158-167 for DUMONT with the threshold of 10 Kb. Next, we have split the data per strategy in Tables 58-107 and per exfiltration field in Tables 108-157 for regular DUMONT. For DUMONT with the 10 Kb threshold, we show the data per strategy in Tables 168-217 and per exfiltration field in Tables 218-267. Note that for the latter, (M0) and (M1) display 0 samples as they do not specify an exfiltration field. In reality, they both use the URI to exfiltrate data.

D.2 Results Exfiltration Dataset

The results of the exfiltration dataset can be found in Tables 268-277 for regular DUMONT and in Tables 278-287 for DUMONT with $\sigma = 10000$. Again each Table represents a different alpha value. It contains traces from 7 different malware samples.

D.3 Results User Dataset

The results of the user dataset can be found in Tables 288-297 for regular DUMONT and in Tables 298-307 for DUMONT with the threshold. Again each Table represents a different alpha value. It contains traces from 4 different university researchers. The devices of these researchers did not contain any exfiltrating malware and are therefore used to determine a reliable false-positive rate of the DUMONT system. The false-positive rates range from 38.8% to 99.9% for regular DUMONT and 16.7% to 49.7% for DUMONT with the 10 Kb threshold, depending on the alpha value. We observe that for lower false-positive rates, the detection rate will be lower as well.

Table 48 DUMONT - Overall analysis adaptive dataset - Alpha = 0.1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	5685	184469	29666	83372	0.0638	0.1385	0.6272
M1	248650	2435	190270	26084	29861	0.0754	0.1206	0.7750
M2	1173056	18933	924331	165760	64032	0.2282	0.1520	0.8041
M3	1173410	20732	924056	161553	67069	0.2361	0.1488	0.8052
Total	2898308	47785	2223126	383063	244334	0.1636	0.147	0.7835

Table 49 DUMONT - Overall analysis adaptive dataset - Alpha = 0.2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	13230	158546	55589	75827	0.1486	0.2596	0.5666
M1	248650	5854	152741	63613	26442	0.1813	0.2940	0.6378
M2	1173056	33247	738539	351552	49718	0.4007	0.3225	0.6579
M3	1173410	41313	741575	344034	46488	0.4705	0.3169	0.6672
Total	2898308	93644	1791401	814788	198475	0.3206	0.3126	0.6504

Table 50: DUMONT - Overall analysis adaptive dataset - Alpha = 0.3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	13324	155172	58963	75733	0.1496	0.2754	0.5557
M1	248650	6305	135275	81079	25991	0.1952	0.3748	0.5694
M2	1173056	38612	678905	411186	44353	0.4654	0.3772	0.6117
M3	1173410	47769	688693	396916	40032	0.5441	0.3656	0.6276
Total	2898308	106010	1658045	948144	186109	0.3629	0.3638	0.6086

Table 51: DUMONT - Overall analysis adaptive dataset - Alpha = 0.4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	20343	124888	89247	68714	0.2284	0.4168	0.4790
M1	248650	9131	112063	104291	23165	0.2827	0.4820	0.4874
M2	1173056	50137	549136	540955	32828	0.6043	0.4962	0.5109
M3	1173410	60353	514822	570787	27448	0.6874	0.5258	0.4902
Total	2898308	139964	1300909	1305280	152155	0.4791	0.5008	0.4971

Table 52: DUMONT - Overall analysis adaptive dataset - Alpha = 0.5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	26529	106743	107392	62528	0.2979	0.5015	0.4396
M1	248650	13564	91839	124515	18732	0.4200	0.5755	0.4239
M2	1173056	55555	384552	705539	27410	0.6696	0.6472	0.3752
M3	1173410	69457	401173	684436	18344	0.7911	0.6305	0.4011
Total	2898308	165105	984307	1621882	127014	0.5652	0.6223	0.3966

Table 53: DUMONT - Overall analysis adaptive dataset - Alpha = 0.6

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	34520	69519	144616	54537	0.3876	0.6753	0.3431
M1	248650	20552	68277	148077	11744	0.6364	0.6844	0.3572
M2	1173056	59625	271633	818458	23340	0.7187	0.7508	0.2824
M3	1173410	76368	235451	850158	11433	0.8698	0.7831	0.2657
Total	2898308	191065	644880	1961309	101054	0.6541	0.7526	0.2884

Table 54: DUMONT - Overall analysis adaptive dataset - Alpha = 0.7

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	40709	30922	183213	48348	0.4571	0.8556	0.2363
M1	248650	25590	22947	193407	6706	0.7924	0.8939	0.1952
M2	1173056	66266	134276	955815	16699	0.7987	0.8768	0.1710
M3	1173410	83091	107413	978196	4710	0.9464	0.9011	0.1624
Total	2898308	215656	295558	2310631	76463	0.7382	0.8866	0.1764

Table 55: DUMONT - Overall analysis adaptive dataset - Alpha = 0.8

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	42861	14092	200043	46196	0.4813	0.9342	0.1878
M1	248650	28682	2566	213788	3614	0.8881	0.9881	0.1257
M2	1173056	72913	27277	1062814	10052	0.8788	0.9750	0.0854
M3	1173410	86045	21377	1064232	1756	0.9800	0.9803	0.0915
Total	2898308	230501	65312	2540877	61618	0.7891	0.9749	0.1021

Table 56: DUMONT - Overall analysis adaptive dataset - Alpha = 0.9

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	54143	11660	202475	34914	0.6080	0.9455	0.2170
M1	248650	30848	1037	215317	1448	0.9552	0.9952	0.1282
M2	1173056	81254	7235	1082856	1711	0.9794	0.9934	0.0754
M3	1173410	87299	8629	1076980	502	0.9943	0.9921	0.0818
Total	2898308	253544	28561	2577628	38575	0.8679	0.9890	0.0973

Table 57: DUMONT - Overall analysis adaptive dataset - Alpha = 1.0

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	89057	8	214127	0	1.0000	1.0000	0.2938
M1	248650	32296	0	216354	0	1.0000	1.0000	0.1299
M2	1173056	82965	5	1090086	0	1.0000	1.0000	0.0707
M3	1173410	87801	113	1085496	0	1.0000	0.9999	0.0749
Total	2898308	292119	126	2606063	0	1.0000	1.0000	0.1008

Table 58: DUMONT - Analysis adaptive dataset - Alpha = 0.1 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	60	35916	7331	140	0.3000	0.1695	0.8280
M1	43102	0	37222	5680	200	0.0000	0.1324	0.8636
M2	218134	34	185073	32889	138	0.1977	0.1509	0.8486
M3	215647	116	179972	35275	284	0.2900	0.1639	0.8351
Total	520330	210	438183	81175	762	0.2160	0.1563	0.8425

Table 59: DUMONT - Analysis adaptive dataset - Alpha = 0.2 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	80	31962	11285	120	0.4000	0.2609	0.7375
M1	43102	9	29737	13165	191	0.0450	0.3069	0.6901
M2	218134	78	156792	61170	94	0.4535	0.2806	0.7191
M3	215647	178	151873	63374	222	0.4450	0.2944	0.7051
Total	520330	345	370364	148994	627	0.3549	0.2869	0.7124

Table 60: DUMONT - Analysis adaptive dataset - Alpha = 0.3 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	80	30976	12271	120	0.4000	0.2837	0.7148
M1	43102	9	26495	16407	191	0.0450	0.3824	0.6149
M2	218134	93	144016	73946	79	0.5407	0.3393	0.6606
M3	215647	226	135986	79261	174	0.5650	0.3682	0.6316
Total	520330	408	337473	181885	564	0.4198	0.3502	0.6494

Table 61: DUMONT - Analysis adaptive dataset - Alpha = 0.4 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	100	24248	18999	100	0.5000	0.4393	0.5604
M1	43102	49	20614	22288	151	0.2450	0.5195	0.4794
M2	218134	117	118965	98997	55	0.6802	0.4542	0.5459
M3	215647	286	102625	112622	114	0.7150	0.5232	0.4772
Total	520330	552	266452	252906	420	0.5679	0.4870	0.5131

Table 62: DUMONT - Analysis adaptive dataset - Alpha = 0.5 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	103	22097	21150	97	0.5150	0.4891	0.5110
M1	43102	66	15207	27695	134	0.3300	0.6455	0.3543
M2	218134	120	85199	132763	52	0.6977	0.6091	0.3911
M3	215647	328	77994	137253	72	0.8200	0.6377	0.3632
Total	520330	617	200497	318861	355	0.6348	0.6140	0.3865

Table 63: DUMONT - Analysis adaptive dataset - Alpha = 0.6 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	106	15003	28244	94	0.5300	0.6531	0.3478
M1	43102	101	13016	29886	99	0.5050	0.6966	0.3043
M2	218134	131	63790	154172	41	0.7616	0.7073	0.2930
M3	215647	372	42375	172872	28	0.9300	0.8031	0.1982
Total	520330	710	134184	385174	262	0.7305	0.7416	0.2592

Table 64: DUMONT - Analysis adaptive dataset - Alpha = 0.7 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	109	6381	36866	91	0.5450	0.8525	0.1494
M1	43102	132	3903	38999	68	0.6600	0.9090	0.0936
M2	218134	149	32169	185793	23	0.8663	0.8524	0.1482
M3	215647	395	14338	200909	5	0.9875	0.9334	0.0683
Total	520330	785	56791	462567	187	0.8076	0.8907	0.1107

Table 65: DUMONT - Analysis adaptive dataset - Alpha = 0.8 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	109	3156	40091	91	0.5450	0.9270	0.0751
M1	43102	144	518	42384	56	0.7200	0.9879	0.0154
M2	218134	165	5705	212257	7	0.9593	0.9738	0.0269
M3	215647	399	4364	210883	1	0.9975	0.9797	0.0221
Total	520330	817	13743	505615	155	0.8405	0.9735	0.0280

Table 66: DUMONT - Analysis adaptive dataset - Alpha = 0.9 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	126	2562	40685	74	0.6300	0.9408	0.0619
M1	43102	180	209	42693	20	0.9000	0.9951	0.0090
M2	218134	170	1713	216249	2	0.9884	0.9921	0.0086
M3	215647	399	1713	213534	1	0.9975	0.9920	0.0098
Total	520330	875	6197	513161	97	0.9002	0.9881	0.0136

Table 67: DUMONT - Analysis adaptive dataset - Alpha = 1.0 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	200	2	43245	0	1.0000	1.0000	0.0046
M1	43102	200	0	42902	0	1.0000	1.0000	0.0046
M2	218134	172	1	217961	0	1.0000	1.0000	0.0008
M3	215647	400	35	215212	0	1.0000	0.9998	0.0020
Total	520330	972	38	519320	0	1.0000	0.9999	0.0019

Table 68: DUMONT - Analysis adaptive dataset - Alpha = 0.1 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	918	36894	4909	19022	0.0460	0.1174	0.6124
M1	54712	866	38190	5008	10648	0.0752	0.1159	0.7138
M2	233062	3115	186771	32076	11100	0.2191	0.1466	0.8147
M3	246267	6527	186579	30441	22720	0.2232	0.1403	0.7841
Total	595784	11426	448434	72434	63490	0.1525	0.1391	0.7719

Table 69: DUMONT - Analysis adaptive dataset - Alpha = 0.2 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	3370	31617	10186	16570	0.1690	0.2437	0.5667
M1	54712	2066	30666	12532	9448	0.1794	0.2901	0.5983
M2	233062	5936	145604	73243	8279	0.4176	0.3347	0.6502
M3	246267	13535	148887	68133	15712	0.4628	0.3139	0.6595
Total	595784	24907	356774	164094	50009	0.3325	0.3150	0.6406

Table 70: DUMONT - Analysis adaptive dataset - Alpha = 0.3 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	3370	31190	10613	16570	0.1690	0.2539	0.5597
M1	54712	2243	27217	15981	9271	0.1948	0.3699	0.5385
M2	233062	6740	134955	83892	7475	0.4741	0.3833	0.6080
M3	246267	15722	141028	75992	13525	0.5376	0.3502	0.6365
Total	595784	28075	334390	186478	46841	0.3748	0.3580	0.6084

Table 71: DUMONT - Analysis adaptive dataset - Alpha = 0.4 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	5272	25181	16622	14668	0.2644	0.3976	0.4932
M1	54712	3152	22621	20577	8362	0.2738	0.4763	0.4711
M2	233062	9142	107981	110866	5073	0.6431	0.5066	0.5025
M3	246267	19863	105702	111318	9384	0.6791	0.5129	0.5099
Total	595784	37429	261485	259383	37487	0.4996	0.4980	0.5017

Table 72: DUMONT - Analysis adaptive dataset - Alpha = 0.5 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	5957	20869	20934	13983	0.2987	0.5008	0.4345
M1	54712	4468	19346	23852	7046	0.3880	0.5522	0.4353
M2	233062	9745	77167	141680	4470	0.6855	0.6474	0.3729
M3	246267	23183	81746	135274	6064	0.7927	0.6233	0.4261
Total	595784	43353	199128	321740	31563	0.5787	0.6177	0.4070

Table 73: DUMONT - Analysis adaptive dataset - Alpha = 0.6 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	7908	13601	28202	12032	0.3966	0.6746	0.3484
M1	54712	7258	13775	29423	4256	0.6304	0.6811	0.3844
M2	233062	10716	53472	165375	3499	0.7539	0.7557	0.2754
M3	246267	25150	52927	164093	4097	0.8599	0.7561	0.3170
Total	595784	51032	133775	387093	23884	0.6812	0.7432	0.3102

Table 74: DUMONT - Analysis adaptive dataset - Alpha = 0.7 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	9227	6162	35641	10713	0.4627	0.8526	0.2492
M1	54712	8898	4919	38279	2616	0.7728	0.8861	0.2525
M2	233062	11560	26573	192274	2655	0.8132	0.8786	0.1636
M3	246267	27697	23846	193174	1550	0.9470	0.8901	0.2093
Total	595784	57382	61500	459368	17534	0.7660	0.8819	0.1995

Table 75: DUMONT - Analysis adaptive dataset - Alpha = 0.8 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	9646	2590	39213	10294	0.4838	0.9380	0.1982
M1	54712	10339	523	42675	1175	0.8980	0.9879	0.1985
M2	233062	12786	5773	213074	1429	0.8995	0.9736	0.0796
M3	246267	28605	4125	212895	642	0.9780	0.9810	0.1329
Total	595784	61376	13011	507857	13540	0.8193	0.9750	0.1249

Table 76: DUMONT - Analysis adaptive dataset - Alpha = 0.9 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	11591	2198	39605	8349	0.5813	0.9474	0.2233
M1	54712	11029	188	43010	485	0.9579	0.9956	0.2050
M2	233062	13916	1460	217387	299	0.9790	0.9933	0.0660
M3	246267	29041	1830	215190	206	0.9930	0.9916	0.1254
Total	595784	65577	5676	515192	9339	0.8753	0.9891	0.1196

Table 77: DUMONT - Analysis adaptive dataset - Alpha = 1.0 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	19940	2	41801	0	1.0000	1.0000	0.3230
M1	54712	11514	0	43198	0	1.0000	1.0000	0.2104
M2	233062	14215	1	218846	0	1.0000	1.0000	0.0610
M3	246267	29247	28	216992	0	1.0000	0.9999	0.1189
Total	595784	74916	31	520837	0	1.0000	0.9999	0.1258

Table 78: DUMONT - Analysis adaptive dataset - Alpha = 0.1 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	1772	37191	6158	17594	0.0915	0.1421	0.6213
M1	50980	589	37872	5216	7303	0.0746	0.1211	0.7544
M2	231484	3391	184634	33718	9741	0.2582	0.1544	0.8123
M3	238580	5891	184900	31031	16758	0.2601	0.1437	0.7997
Total	583759	11643	444597	76123	51396	0.1847	0.1462	0.7816

Table 79: DUMONT - Analysis adaptive dataset - Alpha = 0.2 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	3786	31395	11954	15580	0.1955	0.2758	0.5610
M1	50980	1388	31332	11756	6504	0.1759	0.2728	0.6418
M2	231484	5740	143522	74830	7392	0.4371	0.3427	0.6448
M3	238580	10785	148104	67827	11864	0.4762	0.3141	0.6660
Total	583759	21699	354353	166367	41340	0.3442	0.3195	0.6442

Table 80: DUMONT - Analysis adaptive dataset - Alpha = 0.3 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	3786	30952	12397	15580	0.1955	0.2860	0.5539
M1	50980	1525	27617	15471	6367	0.1932	0.3591	0.5716
M2	231484	6412	133256	85096	6720	0.4883	0.3897	0.6034
M3	238580	13025	135568	80363	9624	0.5751	0.3722	0.6228
Total	583759	24748	327393	193327	38291	0.3926	0.3713	0.6032

Table 81: DUMONT - Analysis adaptive dataset - Alpha = 0.4 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	5178	25349	18000	14188	0.2674	0.4152	0.4868
M1	50980	2283	23281	19807	5609	0.2893	0.4597	0.5015
M2	231484	8478	107877	110475	4654	0.6456	0.5059	0.5026
M3	238580	15985	100973	114958	6664	0.7058	0.5324	0.4902
Total	583759	31924	257480	263240	31115	0.5064	0.5055	0.4958

Table 82: DUMONT - Analysis adaptive dataset - Alpha = 0.5 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	7185	21039	22310	12181	0.3710	0.5147	0.4500
M1	50980	3558	19325	23763	4334	0.4508	0.5515	0.4489
M2	231484	9237	75869	142483	3895	0.7034	0.6525	0.3677
M3	238580	18062	79578	136353	4587	0.7975	0.6315	0.4093
Total	583759	38042	195811	324909	24997	0.6035	0.6240	0.4006

Table 83: DUMONT - Analysis adaptive dataset - Alpha = 0.6 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	8692	13416	29933	10674	0.4488	0.6905	0.3525
M1	50980	4949	14329	28759	2943	0.6271	0.6674	0.3781
M2	231484	10027	50838	167514	3105	0.7636	0.7672	0.2629
M3	238580	19980	47626	168305	2669	0.8822	0.7794	0.2834
Total	583759	43648	126209	394511	19391	0.6924	0.7576	0.2910

Table 84: DUMONT - Analysis adaptive dataset - Alpha = 0.7 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	10120	6145	37204	9246	0.5226	0.8582	0.2593
M1	50980	6179	4771	38317	1713	0.7829	0.8893	0.2148
M2	231484	11206	25257	193095	1926	0.8533	0.8843	0.1575
M3	238580	21813	19199	196732	836	0.9631	0.9111	0.1719
Total	583759	49318	55372	465348	13721	0.7823	0.8937	0.1793

Table 85: DUMONT - Analysis adaptive dataset - Alpha = 0.8 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	10722	2711	40638	8644	0.5537	0.9375	0.2142
M1	50980	6954	541	42547	938	0.8811	0.9874	0.1470
M2	231484	12158	5045	213307	974	0.9258	0.9769	0.0743
M3	238580	22224	4135	211796	425	0.9812	0.9809	0.1105
Total	583759	52058	12432	508288	10981	0.8258	0.9761	0.1105

Table 86: DUMONT - Analysis adaptive dataset - Alpha = 0.9 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	13594	2206	41143	5772	0.7020	0.9491	0.2519
M1	50980	7503	211	42877	389	0.9507	0.9951	0.1513
M2	231484	12879	1258	217094	253	0.9807	0.9942	0.0611
M3	238580	22515	1935	213996	134	0.9941	0.9910	0.1025
Total	583759	56491	5610	515110	6548	0.8961	0.9892	0.1064

Table 87: DUMONT - Analysis adaptive dataset - Alpha = 1.0 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	19366	0	43349	0	1.0000	1.0000	0.3088
M1	50980	7892	0	43088	0	1.0000	1.0000	0.1548
M2	231484	13132	1	218351	0	1.0000	1.0000	0.0567
M3	238580	22649	27	215904	0	1.0000	0.9999	0.0950
Total	583759	63039	28	520692	0	1.0000	0.9999	0.1080

Table 88: DUMONT - Analysis adaptive dataset - Alpha = 0.1 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	344	37486	5710	2568	0.1181	0.1322	0.8205
M1	45921	254	38109	5501	2057	0.1099	0.1261	0.8354
M2	226456	2348	182631	34460	7017	0.2507	0.1587	0.8168
M3	226719	2270	186374	32143	5932	0.2768	0.1471	0.8321
Total	545204	5216	444600	77814	17574	0.2289	0.1490	0.8250

Table 89: DUMONT - Analysis adaptive dataset - Alpha = 0.2 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	774	31402	11794	2138	0.2658	0.2730	0.6978
M1	45921	564	30019	13591	1747	0.2441	0.3116	0.6660
M2	226456	4095	147070	70021	5270	0.4373	0.3225	0.6675
M3	226719	4133	147199	71318	4069	0.5039	0.3264	0.6675
Total	545204	9566	355690	166724	13224	0.4197	0.3191	0.6699

Table 90: DUMONT - Analysis adaptive dataset - Alpha = 0.3 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	868	30308	12888	2044	0.2981	0.2984	0.6762
M1	45921	580	26543	17067	1731	0.2510	0.3914	0.5906
M2	226456	4975	131896	85195	4390	0.5312	0.3924	0.6044
M3	226719	4677	137786	80731	3525	0.5702	0.3694	0.6284
Total	545204	11100	326533	195881	11690	0.4871	0.3750	0.6193

Table 91: DUMONT - Analysis adaptive dataset - Alpha = 0.4 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	1244	23702	19494	1668	0.4272	0.4513	0.5410
M1	45921	774	22465	21145	1537	0.3349	0.4849	0.5061
M2	226456	6166	105612	111479	3199	0.6584	0.5135	0.4936
M3	226719	5841	102902	115615	2361	0.7121	0.5291	0.4796
Total	545204	14025	254681	267733	8765	0.6154	0.5125	0.4929

Table 92: DUMONT - Analysis adaptive dataset - Alpha = 0.5 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	1415	20920	22276	1497	0.4859	0.5157	0.4844
M1	45921	1176	18407	25203	1135	0.5089	0.5779	0.4264
M2	226456	6673	72213	144878	2692	0.7125	0.6674	0.3484
M3	226719	6612	83271	135246	1590	0.8061	0.6189	0.3965
Total	545204	15876	194811	327603	6914	0.6966	0.6271	0.3864

Table 93: DUMONT - Analysis adaptive dataset - Alpha = 0.6 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	1579	13561	29635	1333	0.5422	0.6861	0.3284
M1	45921	1570	13602	30008	741	0.6794	0.6881	0.3304
M2	226456	6874	52197	164894	2491	0.7340	0.7596	0.2608
M3	226719	7369	44280	174237	833	0.8984	0.7974	0.2278
Total	545204	17392	123640	398774	5398	0.7631	0.7633	0.2587

Table 94: DUMONT - Analysis adaptive dataset - Alpha = 0.7 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	1632	5858	37338	1280	0.5604	0.8644	0.1624
M1	45921	1924	4774	38836	387	0.8325	0.8905	0.1459
M2	226456	7407	25573	191518	1958	0.7909	0.8822	0.1456
M3	226719	7804	23243	195274	398	0.9515	0.8936	0.1369
Total	545204	18767	59448	462966	4023	0.8235	0.8862	0.1435

Table 95: DUMONT - Analysis adaptive dataset - Alpha = 0.8 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	1830	2697	40499	1082	0.6284	0.9376	0.0982
M1	45921	2098	462	43148	213	0.9078	0.9894	0.0557
M2	226456	8339	5255	211836	1026	0.8904	0.9758	0.0600
M3	226719	8063	4536	213981	139	0.9831	0.9792	0.0556
Total	545204	20330	12950	509464	2460	0.8921	0.9752	0.0610

Table 96: DUMONT - Analysis adaptive dataset - Alpha = 0.9 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	2235	2184	41012	677	0.7675	0.9494	0.0958
M1	45921	2232	176	43434	79	0.9658	0.9960	0.0524
M2	226456	9207	1347	215744	158	0.9831	0.9938	0.0466
M3	226719	8174	1519	216998	28	0.9966	0.9930	0.0428
Total	545204	21848	5226	517188	942	0.9587	0.9900	0.0497

Table 97: DUMONT - Analysis adaptive dataset - Alpha = 1.0 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	2912	2	43194	0	1.0000	1.0000	0.0632
M1	45921	2311	0	43610	0	1.0000	1.0000	0.0503
M2	226456	9365	1	217090	0	1.0000	1.0000	0.0414
M3	226719	8202	11	218506	0	1.0000	0.9999	0.0362
Total	545204	22790	14	522400	0	1.0000	1.0000	0.0418

Table 98: DUMONT - Analysis adaptive dataset - Alpha = 0.1 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	2591	36982	5558	44048	0.0556	0.1307	0.4437
M1	53935	726	38877	4679	9653	0.0699	0.1074	0.7343
M2	263920	10045	185222	32617	36036	0.2180	0.1497	0.7399
M3	246197	5928	186231	32663	21375	0.2171	0.1492	0.7805
Total	653231	19290	447312	75517	111112	0.1479	0.1444	0.7143

Table 99: DUMONT - Analysis adaptive dataset - Alpha = 0.2 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	5220	32170	10370	41419	0.1119	0.2438	0.4193
M1	53935	1827	30987	12569	8552	0.1760	0.2886	0.6084
M2	263920	17398	145551	72288	28683	0.3776	0.3318	0.6174
M3	246197	12682	145512	73382	14621	0.4645	0.3352	0.6426
Total	653231	37127	354220	168609	93275	0.2847	0.3225	0.5991

Table 100: DUMONT - Analysis adaptive dataset - Alpha = 0.3 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	5220	31746	10794	41419	0.1119	0.2537	0.4145
M1	53935	1948	27403	16153	8431	0.1877	0.3709	0.5442
M2	263920	20392	134782	83057	25689	0.4425	0.3813	0.5880
M3	246197	14119	138325	80569	13184	0.5171	0.3681	0.6192
Total	653231	41679	332256	190573	88723	0.3196	0.3645	0.5724

Table 101: DUMONT - Analysis adaptive dataset - Alpha = 0.4 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	8549	26408	16132	38090	0.1833	0.3792	0.3920
M1	53935	2873	23082	20474	7506	0.2768	0.4701	0.4812
M2	263920	26234	108701	109138	19847	0.5693	0.5010	0.5113
M3	246197	18378	102620	116274	8925	0.6731	0.5312	0.4915
Total	653231	56034	260811	262018	74368	0.4297	0.5012	0.4850

Table 102: DUMONT - Analysis adaptive dataset - Alpha = 0.5 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	11869	21818	20722	34770	0.2545	0.4871	0.3777
M1	53935	4296	19554	24002	6083	0.4139	0.5511	0.4422
M2	263920	29780	74104	143735	16301	0.6463	0.6598	0.3936
M3	246197	21272	78584	140310	6031	0.7791	0.6410	0.4056
Total	653231	67217	194060	328769	63185	0.5155	0.6288	0.4000

Table 103: DUMONT - Analysis adaptive dataset - Alpha = 0.6 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	16235	13938	28602	30404	0.3481	0.6724	0.3383
M1	53935	6674	13555	30001	3705	0.6430	0.6888	0.3751
M2	263920	31877	51336	166503	14204	0.6918	0.7643	0.3153
M3	246197	23497	48243	170651	3806	0.8606	0.7796	0.2914
Total	653231	78283	127072	395757	52119	0.6003	0.7570	0.3144

Table 104: DUMONT - Analysis adaptive dataset - Alpha = 0.7 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	19621	6376	36164	27018	0.4207	0.8501	0.2915
M1	53935	8457	4580	38976	1922	0.8148	0.8948	0.2417
M2	263920	35944	24704	193135	10137	0.7800	0.8866	0.2298
M3	246197	25382	26787	192107	1921	0.9296	0.8776	0.2119
Total	653231	89404	62447	460382	40998	0.6856	0.8806	0.2325

Table 105: DUMONT - Analysis adaptive dataset - Alpha = 0.8 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	20554	2938	39602	26085	0.4407	0.9309	0.2634
M1	53935	9147	522	43034	1232	0.8813	0.9880	0.1793
M2	263920	39465	5499	212340	6616	0.8564	0.9748	0.1704
M3	246197	26754	4217	214677	549	0.9799	0.9807	0.1258
Total	653231	95920	13176	509653	34482	0.7356	0.9748	0.1670

Table 106: DUMONT - Analysis adaptive dataset - Alpha = 0.9 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	26597	2510	40030	20042	0.5703	0.9410	0.3264
M1	53935	9904	253	43303	475	0.9542	0.9942	0.1883
M2	263920	45082	1457	216382	999	0.9783	0.9933	0.1763
M3	246197	27170	1632	217262	133	0.9951	0.9925	0.1170
Total	653231	108753	5852	516977	21649	0.8340	0.9888	0.1754

Table 107: DUMONT - Analysis adaptive dataset - Alpha = 1.0 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	46639	2	42538	0	1.0000	1.0000	0.5230
M1	53935	10379	0	43556	0	1.0000	1.0000	0.1924
M2	263920	46081	1	217838	0	1.0000	1.0000	0.1746
M3	246197	27303	12	218882	0	1.0000	0.9999	0.1109
Total	653231	130402	15	522814	0	1.0000	1.0000	0.1996

Table 108: DUMONT - Analysis adaptive dataset - Alpha = 0.1 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	6247	182832	32486	12219	0.3383	0.1509	0.8088
M3	231846	5602	182017	34446	9781	0.3642	0.1591	0.8092
Total	465630	11849	364849	66932	22000	0.3501	0.1550	0.8090

Table 109: DUMONT - Analysis adaptive dataset - Alpha = 0.2 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	8571	144992	70326	9895	0.4642	0.3266	0.6569
M3	231846	10786	143059	73404	4597	0.7012	0.3391	0.6636
Total	465630	19357	288051	143730	14492	0.5719	0.3329	0.6602

Table 110: DUMONT - Analysis adaptive dataset - Alpha = 0.3 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	9754	128425	86893	8712	0.5282	0.4036	0.5911
M3	231846	11634	130612	85851	3749	0.7563	0.3966	0.6135
Total	465630	21388	259037	172744	12461	0.6319	0.4001	0.6022

Table 111: DUMONT - Analysis adaptive dataset - Alpha = 0.4 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	13742	96809	118509	4724	0.7442	0.5504	0.4729
M3	231846	12469	101081	115382	2914	0.8106	0.5330	0.4898
Total	465630	26211	197890	233891	7638	0.7744	0.5417	0.4813

Table 112: DUMONT - Analysis adaptive dataset - Alpha = 0.5 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	14232	47908	167410	4234	0.7707	0.7775	0.2658
M3	231846	14034	71364	145099	1349	0.9123	0.6703	0.3683
Total	465630	28266	119272	312509	5583	0.8351	0.7238	0.3169

Table 113: DUMONT - Analysis adaptive dataset - Alpha = 0.6 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	15102	35999	179319	3364	0.8178	0.8328	0.2186
M3	231846	14671	40086	176377	712	0.9537	0.8148	0.2362
Total	465630	29773	76085	355696	4076	0.8796	0.8238	0.2273

Table 114: DUMONT - Analysis adaptive dataset - Alpha = 0.7 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	16941	18930	196388	1525	0.9174	0.9121	0.1534
M3	231846	14847	20388	196075	536	0.9652	0.9058	0.1520
Total	465630	31788	39318	392463	2061	0.9391	0.9089	0.1527

Table 115: DUMONT - Analysis adaptive dataset - Alpha = 0.8 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	17435	4087	211231	1031	0.9442	0.9810	0.0921
M3	231846	15197	4093	212370	186	0.9879	0.9811	0.0832
Total	465630	32632	8180	423601	1217	0.9640	0.9811	0.0876

Table 116: DUMONT - Analysis adaptive dataset - Alpha = 0.9 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	18465	720	214598	1	0.9999	0.9967	0.0821
M3	231846	15383	2506	213957	0	1.0000	0.9884	0.0772
Total	465630	33848	3226	428555	1	1.0000	0.9925	0.0796

Table 117: DUMONT - Analysis adaptive dataset - Alpha = 1.0 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	18466	0	215318	0	1.0000	1.0000	0.0790
M3	231846	15383	6	216457	0	1.0000	1.0000	0.0664
Total	465630	33849	6	431775	0	1.0000	1.0000	0.0727

Table 118: DUMONT - Analysis adaptive dataset - Alpha = 0.1 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	1151	187210	31968	13280	0.0798	0.1459	0.8063
M3	238587	7383	182100	35346	13758	0.3492	0.1626	0.7942
Total	472196	8534	369310	67314	27038	0.2399	0.1542	0.8002

Table 119: DUMONT - Analysis adaptive dataset - Alpha = 0.2 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	2777	152239	66939	11654	0.1924	0.3054	0.6636
M3	238587	14692	137363	80083	6449	0.6950	0.3683	0.6373
Total	472196	17469	289602	147022	18103	0.4911	0.3367	0.6503

Table 120: DUMONT - Analysis adaptive dataset - Alpha = 0.3 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	5424	129093	90085	9007	0.3759	0.4110	0.5758
M3	238587	17146	116502	100944	3995	0.8110	0.4642	0.5602
Total	472196	22570	245595	191029	13002	0.6345	0.4375	0.5679

Table 121: DUMONT - Analysis adaptive dataset - Alpha = 0.4 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	6614	101451	117727	7817	0.4583	0.5371	0.4626
M3	238587	19250	79790	137656	1891	0.9106	0.6331	0.4151
Total	472196	25864	181241	255383	9708	0.7271	0.5849	0.4386

Table 122: DUMONT - Analysis adaptive dataset - Alpha = 0.5 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	9124	70789	148389	5307	0.6323	0.6770	0.3421
M3	238587	20049	58946	158500	1092	0.9483	0.7289	0.3311
Total	472196	29173	129735	306889	6399	0.8201	0.7029	0.3365

Table 123: DUMONT - Analysis adaptive dataset - Alpha = 0.6 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	9195	38371	180807	5236	0.6372	0.8249	0.2036
M3	238587	20333	32941	184505	808	0.9618	0.8485	0.2233
Total	472196	29528	71312	365312	6044	0.8301	0.8367	0.2136

Table 124: DUMONT - Analysis adaptive dataset - Alpha = 0.7 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	10967	23229	195949	3464	0.7600	0.8940	0.1464
M3	238587	20832	16327	201119	309	0.9854	0.9249	0.1557
Total	472196	31799	39556	397068	3773	0.8939	0.9094	0.1511

Table 125: DUMONT - Analysis adaptive dataset - Alpha = 0.8 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	12578	4149	215029	1853	0.8716	0.9811	0.0716
M3	238587	20976	3297	214149	165	0.9922	0.9848	0.1017
Total	472196	33554	7446	429178	2018	0.9433	0.9829	0.0868

Table 126: DUMONT - Analysis adaptive dataset - Alpha = 0.9 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	14431	854	218324	0	1.0000	0.9961	0.0654
M3	238587	21047	1435	216011	94	0.9956	0.9934	0.0942
Total	472196	35478	2289	434335	94	0.9974	0.9948	0.0800

Table 127: DUMONT - Analysis adaptive dataset - Alpha = 1.0 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	14431	0	219178	0	1.0000	1.0000	0.0618
M3	238587	21141	86	217360	0	1.0000	0.9996	0.0890
Total	472196	35572	86	436538	0	1.0000	0.9998	0.0755

Table 128: DUMONT - Analysis adaptive dataset - Alpha = 0.1 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	3828	188396	30597	13170	0.2252	0.1397	0.8145
M3	231805	1947	187250	29885	12723	0.1327	0.1376	0.8162
Total	467796	5775	375646	60482	25893	0.1824	0.1387	0.8154

Table 129: DUMONT - Analysis adaptive dataset - Alpha = 0.2 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	7662	148978	70015	9336	0.4508	0.3197	0.6638
M3	231805	4531	152701	64434	10139	0.3089	0.2967	0.6783
Total	467796	12193	301679	134449	19475	0.3850	0.3083	0.6710

Table 130: DUMONT - Analysis adaptive dataset - Alpha = 0.3 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	8856	145388	73605	8142	0.5210	0.3361	0.6536
M3	231805	5097	147589	69546	9573	0.3474	0.3203	0.6587
Total	467796	13953	292977	143151	17715	0.4406	0.3282	0.6561

Table 131: DUMONT - Analysis adaptive dataset - Alpha = 0.4 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	11853	117457	101536	5145	0.6973	0.4636	0.5479
M3	231805	7590	113429	103706	7080	0.5174	0.4776	0.5221
Total	467796	19443	230886	205242	12225	0.6140	0.4706	0.5351

Table 132: DUMONT - Analysis adaptive dataset - Alpha = 0.5 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	11975	93159	125834	5023	0.7045	0.5746	0.4455
M3	231805	9215	99394	117741	5455	0.6282	0.5422	0.4685
Total	467796	21190	192553	243575	10478	0.6691	0.5585	0.4569

Table 133: DUMONT - Analysis adaptive dataset - Alpha = 0.6 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	13823	75699	143294	3175	0.8132	0.6543	0.3793
M3	231805	10528	61253	155882	4142	0.7177	0.7179	0.3097
Total	467796	24351	136952	299176	7317	0.7689	0.6860	0.3448

Table 134: DUMONT - Analysis adaptive dataset - Alpha = 0.7 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	15472	44696	174297	1526	0.9102	0.7959	0.2550
M3	231805	12798	32968	184167	1872	0.8724	0.8482	0.1974
Total	467796	28270	77664	358464	3398	0.8927	0.8219	0.2265

Table 135: DUMONT - Analysis adaptive dataset - Alpha = 0.8 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	16811	4497	214496	187	0.9890	0.9795	0.0903
M3	231805	14211	6411	210724	459	0.9687	0.9705	0.0890
Total	467796	31022	10908	425220	646	0.9796	0.9750	0.0896

Table 136: DUMONT - Analysis adaptive dataset - Alpha = 0.9 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	16998	1509	217484	0	1.0000	0.9931	0.0784
M3	231805	14531	1846	215289	139	0.9905	0.9915	0.0706
Total	467796	31529	3355	432773	139	0.9956	0.9923	0.0746

Table 137: DUMONT - Analysis adaptive dataset - Alpha = 1.0 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	16998	0	218993	0	1.0000	1.0000	0.0720
M3	231805	14670	9	217126	0	1.0000	1.0000	0.0633
Total	467796	31668	9	436119	0	1.0000	1.0000	0.0677

Table 138: DUMONT - Analysis adaptive dataset - Alpha = 0.1 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	4241	179743	39418	11551	0.2686	0.1799	0.7831
M3	233360	3109	184561	31741	13949	0.1823	0.1467	0.8042
Total	468313	7350	364304	71159	25500	0.2237	0.1634	0.7936

Table 139: DUMONT - Analysis adaptive dataset - Alpha = 0.2 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	6128	146643	72518	9664	0.3880	0.3309	0.6502
M3	233360	6090	151625	64677	10968	0.3570	0.2990	0.6758
Total	468313	12218	298268	137195	20632	0.3719	0.3151	0.6630

Table 140: DUMONT - Analysis adaptive dataset - Alpha = 0.3 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	6198	136910	82251	9594	0.3925	0.3753	0.6091
M3	233360	6944	145505	70797	10114	0.4071	0.3273	0.6533
Total	468313	13142	282415	153048	19708	0.4001	0.3515	0.6311

Table 141: DUMONT - Analysis adaptive dataset - Alpha = 0.4 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	8173	114266	104895	7619	0.5175	0.4786	0.5211
M3	233360	9347	116762	99540	7711	0.5480	0.4602	0.5404
Total	468313	17520	231028	204435	15330	0.5333	0.4695	0.5307

Table 142: DUMONT - Analysis adaptive dataset - Alpha = 0.5 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	9248	86313	132848	6544	0.5856	0.6062	0.4067
M3	233360	11600	92968	123334	5458	0.6800	0.5702	0.4481
Total	468313	20848	179281	256182	12002	0.6346	0.5883	0.4273

Table 143: DUMONT - Analysis adaptive dataset - Alpha = 0.6 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	9745	66165	152996	6047	0.6171	0.6981	0.3231
M3	233360	14684	55214	161088	2374	0.8608	0.7447	0.2995
Total	468313	24429	121379	314084	8421	0.7437	0.7213	0.3113

Table 144: DUMONT - Analysis adaptive dataset - Alpha = 0.7 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	10078	25546	193615	5714	0.6382	0.8834	0.1516
M3	233360	16317	19561	196741	741	0.9566	0.9096	0.1537
Total	468313	26395	45107	390356	6455	0.8035	0.8964	0.1527

Table 145: DUMONT - Analysis adaptive dataset - Alpha = 0.8 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	11578	8476	210685	4214	0.7332	0.9613	0.0854
M3	233360	16635	5053	211249	423	0.9752	0.9766	0.0929
Total	468313	28213	13529	421934	4637	0.8588	0.9689	0.0891

Table 146: DUMONT - Analysis adaptive dataset - Alpha = 0.9 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	14924	1559	217602	868	0.9450	0.9929	0.0702
M3	233360	16936	1517	214785	122	0.9928	0.9930	0.0791
Total	468313	31860	3076	432387	990	0.9699	0.9929	0.0746

Table 147: DUMONT - Analysis adaptive dataset - Alpha = 1.0 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	15792	0	219161	0	1.0000	1.0000	0.0672
M3	233360	17058	0	216302	0	1.0000	1.0000	0.0731
Total	468313	32850	0	435463	0	1.0000	1.0000	0.0701

Table 148: DUMONT - Analysis adaptive dataset - Alpha = 0.1 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	3466	186150	31291	13812	0.2006	0.1439	0.8078
M3	237812	2691	188128	30135	16858	0.1377	0.1381	0.8024
Total	472531	6157	374278	61426	30670	0.1672	0.1410	0.8051

Table 149: DUMONT - Analysis adaptive dataset - Alpha = 0.2 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	8109	145687	71754	9169	0.4693	0.3300	0.6552
M3	237812	5214	156827	61436	14335	0.2667	0.2815	0.6814
Total	472531	13323	302514	133190	23504	0.3618	0.3057	0.6684

Table 150: DUMONT - Analysis adaptive dataset - Alpha = 0.3 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	8380	139089	78352	8898	0.4850	0.3603	0.6283
M3	237812	6948	148485	69778	12601	0.3554	0.3197	0.6536
Total	472531	15328	287574	148130	21499	0.4162	0.3400	0.6410

Table 151: DUMONT - Analysis adaptive dataset - Alpha = 0.4 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	9755	119153	98288	7523	0.5646	0.4520	0.5492
M3	237812	11697	103760	114503	7852	0.5983	0.5246	0.4855
Total	472531	21452	222913	212791	15375	0.5825	0.4884	0.5171

Table 152: DUMONT - Analysis adaptive dataset - Alpha = 0.5 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	10976	86383	131058	6302	0.6353	0.6027	0.4148
M3	237812	14559	78501	139762	4990	0.7447	0.6403	0.3913
Total	472531	25535	164884	270820	11292	0.6934	0.6216	0.4030

Table 153: DUMONT - Analysis adaptive dataset - Alpha = 0.6 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	11760	55399	162042	5518	0.6806	0.7452	0.2861
M3	237812	16152	45957	172306	3397	0.8262	0.7894	0.2612
Total	472531	27912	101356	334348	8915	0.7579	0.7674	0.2736

Table 154: DUMONT - Analysis adaptive dataset - Alpha = 0.7 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	12808	21875	195566	4470	0.7413	0.8994	0.1478
M3	237812	18297	18169	200094	1252	0.9360	0.9168	0.1533
Total	472531	31105	40044	395660	5722	0.8446	0.9081	0.1506

Table 155: DUMONT - Analysis adaptive dataset - Alpha = 0.8 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	14511	6068	211373	2767	0.8399	0.9721	0.0877
M3	237812	19026	2523	215740	523	0.9732	0.9884	0.0906
Total	472531	33537	8591	427113	3290	0.9107	0.9803	0.0892

Table 156: DUMONT - Analysis adaptive dataset - Alpha = 0.9 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	16436	2593	214848	842	0.9513	0.9881	0.0811
M3	237812	19402	1325	216938	147	0.9925	0.9939	0.0872
Total	472531	35838	3918	431786	989	0.9731	0.9910	0.0841

Table 157: DUMONT - Analysis adaptive dataset - Alpha = 1.0 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	17278	5	217436	0	1.0000	1.0000	0.0736
M3	237812	19549	12	218251	0	1.0000	0.9999	0.0823
Total	472531	36827	17	435687	0	1.0000	1.0000	0.0780

Table 158: Dumont - Overall analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	18342	206873	7262	70715	0.2060	0.0339	0.7428
M1	248650	6945	206870	9484	25351	0.2150	0.0438	0.8599
M2	1173056	21450	1047822	42269	61515	0.2585	0.0388	0.9115
M3	1173410	34821	1050005	35604	52980	0.3966	0.0328	0.9245
Total	2898308	81558	2511570	94619	210561	0.2792	0.0363	0.8947

Table 159: Dumont - Overall analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	30512	196099	18036	58545	0.3426	0.0842	0.7474
M1	248650	12881	193555	22799	19415	0.3988	0.1054	0.8302
M2	1173056	33992	967388	122703	48973	0.4097	0.1126	0.8537
M3	1173410	56945	979746	105863	30856	0.6486	0.0975	0.8835
Total	2898308	134330	2336788	269401	157789	0.4598	0.1034	0.8526

Table 160: Dumont - Overall analysis adaptive dataset - σ = 10000 - Alpha = 0.3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	30512	195890	18245	58545	0.3426	0.0852	0.7467
M1	248650	15818	189190	27164	16478	0.4898	0.1256	0.8245
M2	1173056	37345	951370	138721	45620	0.4501	0.1273	0.8429
M3	1173410	63551	962456	123153	24250	0.7238	0.1134	0.8744
Total	2898308	147226	2298906	307283	144893	0.5040	0.1179	0.8440

Table 161: Dumont - Overall analysis adaptive dataset - σ = 10000 - Alpha = 0.4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	54413	190544	23591	34644	0.6110	0.1102	0.8079
M1	248650	22291	184767	31587	10005	0.6902	0.1460	0.8327
M2	1173056	49244	928449	161642	33721	0.5936	0.1483	0.8335
M3	1173410	76309	921941	163668	11492	0.8691	0.1508	0.8507
Total	2898308	202257	2225701	380488	89862	0.6924	0.1460	0.8377

Table 162: Dumont - Overall analysis adaptive dataset - σ = 10000 - Alpha = 0.5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	75181	186868	27267	13876	0.8442	0.1273	0.8643
M1	248650	28296	178883	37471	4000	0.8761	0.1732	0.8332
M2	1173056	54597	879759	210332	28368	0.6581	0.1929	0.7965
M3	1173410	84092	894769	190840	3709	0.9578	0.1758	0.8342
Total	2898308	242166	2140279	465910	49953	0.8290	0.1788	0.8220

Table 163: Dumont - Overall analysis adaptive dataset - σ = 10000 - Alpha = 0.6

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	77458	179172	34963	11599	0.8698	0.1633	0.8464
M1	248650	31639	173328	43026	657	0.9797	0.1989	0.8243
M2	1173056	56184	847752	242339	26781	0.6772	0.2223	0.7706
M3	1173410	86160	855116	230493	1641	0.9813	0.2123	0.8022
Total	2898308	251441	2055368	550821	40678	0.8607	0.2114	0.7959

Table 164: Dumont - Overall analysis adaptive dataset - σ = 10000 - Alpha = 0.7

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	83092	164911	49224	5965	0.9330	0.2299	0.8180
M1	248650	31857	161844	54510	439	0.9864	0.2519	0.7790
M2	1173056	61454	808683	281408	21511	0.7407	0.2582	0.7418
M3	1173410	86462	806493	279116	1339	0.9847	0.2571	0.7610
Total	2898308	262865	1941931	664258	29254	0.8999	0.2549	0.7607

Table 165: Dumont - Overall analysis adaptive dataset - σ = 10000 - Alpha = 0.8

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	87263	159262	54873	1794	0.9799	0.2563	0.8131
M1	248650	32096	155043	61311	200	0.9938	0.2834	0.7526
M2	1173056	64395	779439	310652	18570	0.7762	0.2850	0.7193
M3	1173410	87016	779525	306084	785	0.9911	0.2819	0.7385
Total	2898308	270770	1873269	732920	21349	0.9269	0.2812	0.7398

Table 166: Dumont - Overall analysis adaptive dataset - σ = 10000 - Alpha = 0.9

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	87530	158278	55857	1527	0.9829	0.2608	0.8107
M1	248650	32096	154641	61713	200	0.9938	0.2852	0.7510
M2	1173056	65415	773045	317046	17550	0.7885	0.2908	0.7148
M3	1173410	87127	775101	310508	674	0.9923	0.2860	0.7348
Total	2898308	272168	1861065	745124	19951	0.9317	0.2859	0.7360

Table 167: Dumont - Overall analysis adaptive dataset - σ = 10000 - Alpha = 1.0

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	303192	88857	153443	60692	200	0.9978	0.2834	0.7992
M1	248650	32096	154274	62080	200	0.9938	0.2869	0.7495
M2	1173056	66273	771103	318988	16692	0.7988	0.2926	0.7138
M3	1173410	87240	771579	314030	561	0.9936	0.2893	0.7319
Total	2898308	274466	1850399	755790	17653	0.9396	0.2900	0.7331

Table 168: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.1 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	41821	1426	200	0.0000	0.0330	0.9626
M1	43102	0	40727	2175	200	0.0000	0.0507	0.9449
M2	218134	0	210350	7612	172	0.0000	0.0349	0.9643
M3	215647	0	206807	8440	400	0.0000	0.0392	0.9590
Total	520330	0	499705	19653	972	0.0000	0.0378	0.9604

Table 169: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.2 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	39663	3584	200	0.0000	0.0829	0.9129
M1	43102	0	38381	4521	200	0.0000	0.1054	0.8905
M2	218134	0	199402	18560	172	0.0000	0.0852	0.9141
M3	215647	0	197431	17816	400	0.0000	0.0828	0.9155
Total	520330	0	474877	44481	972	0.0000	0.0856	0.9126

Table 170: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.3 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	39663	3584	200	0.0000	0.0829	0.9129
M1	43102	0	37531	5371	200	0.0000	0.1252	0.8707
M2	218134	0	196428	21534	172	0.0000	0.0988	0.9005
M3	215647	0	192794	22453	400	0.0000	0.1043	0.8940
Total	520330	0	466416	52942	972	0.0000	0.1019	0.8964

Table 171: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.4 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	38630	4617	200	0.0000	0.1068	0.8891
M1	43102	0	36535	6367	200	0.0000	0.1484	0.8476
M2	218134	0	191949	26013	172	0.0000	0.1193	0.8800
M3	215647	0	184107	31140	400	0.0000	0.1447	0.8537
Total	520330	0	451221	68137	972	0.0000	0.1312	0.8672

Table 172: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.5 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	37688	5559	200	0.0000	0.1285	0.8674
M1	43102	0	35142	7760	200	0.0000	0.1809	0.8153
M2	218134	0	182934	35028	172	0.0000	0.1607	0.8386
M3	215647	0	177735	37512	400	0.0000	0.1743	0.8242
Total	520330	0	433499	85859	972	0.0000	0.1653	0.8331

Table 173: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.6 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	35808	7439	200	0.0000	0.1720	0.8242
M1	43102	0	34528	8374	200	0.0000	0.1952	0.8011
M2	218134	0	176468	41494	172	0.0000	0.1904	0.8090
M3	215647	0	167533	47714	400	0.0000	0.2217	0.7769
Total	520330	0	414337	105021	972	0.0000	0.2022	0.7963

Table 174: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.7 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	32877	10370	200	0.0000	0.2398	0.7567
M1	43102	0	31586	11316	200	0.0000	0.2638	0.7328
M2	218134	0	165169	52793	172	0.0000	0.2422	0.7572
M3	215647	0	158138	57109	400	0.0000	0.2653	0.7333
Total	520330	0	387770	131588	972	0.0000	0.2534	0.7452

Table 175: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.8 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	32137	11110	200	0.0000	0.2569	0.7397
M1	43102	0	30791	12111	200	0.0000	0.2823	0.7144
M2	218134	0	156143	61819	172	0.0000	0.2836	0.7158
M3	215647	0	155277	59970	400	0.0000	0.2786	0.7201
Total	520330	0	374348	145010	972	0.0000	0.2792	0.7194

Table 176: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.9 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	31902	11345	200	0.0000	0.2623	0.7343
M1	43102	0	30675	12227	200	0.0000	0.2850	0.7117
M2	218134	0	154733	63229	172	0.0000	0.2901	0.7093
M3	215647	0	154700	60547	400	0.0000	0.2813	0.7174
Total	520330	0	372010	147348	972	0.0000	0.2837	0.7150

Table 177: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 1.0 - Strategy 1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	43447	0	30873	12374	200	0.0000	0.2861	0.7106
M1	43102	0	30632	12270	200	0.0000	0.2860	0.7107
M2	218134	0	154220	63742	172	0.0000	0.2924	0.7070
M3	215647	0	154141	61106	400	0.0000	0.2839	0.7148
Total	520330	0	369866	149492	972	0.0000	0.2878	0.7108

Table 178: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.1 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	1031	40866	937	18909	0.0517	0.0224	0.6786
M1	54712	3437	41191	2007	8077	0.2985	0.0465	0.8157
M2	233062	3396	210707	8140	10819	0.2389	0.0372	0.9187
M3	246267	11828	210946	6074	17419	0.4044	0.0280	0.9046
Total	595784	19692	503710	17158	55224	0.2629	0.0329	0.8785

Table 179: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.2 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	5861	38375	3428	14079	0.2939	0.0820	0.7165
M1	54712	5563	38617	4581	5951	0.4832	0.1060	0.8075
M2	233062	5754	192914	25933	8461	0.4048	0.1185	0.8524
M3	246267	20414	196117	20903	8833	0.6980	0.0963	0.8793
Total	595784	37592	466023	54845	37324	0.5018	0.1053	0.8453

Table 180: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.3 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	5861	38375	3428	14079	0.2939	0.0820	0.7165
M1	54712	6739	37767	5431	4775	0.5853	0.1257	0.8135
M2	233062	5947	189707	29140	8268	0.4184	0.1332	0.8395
M3	246267	22187	192950	24070	7060	0.7586	0.1109	0.8736
Total	595784	40734	458799	62069	34182	0.5437	0.1192	0.8384

Table 181: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.4 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	11946	37342	4461	7994	0.5991	0.1067	0.7983
M1	54712	8642	36971	6227	2872	0.7506	0.1442	0.8337
M2	233062	9087	185201	33646	5128	0.6393	0.1537	0.8336
M3	246267	26957	185115	31905	2290	0.9217	0.1470	0.8611
Total	595784	56632	444629	76239	18284	0.7559	0.1464	0.8413

Table 182: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.5 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	15940	36649	5154	4000	0.7994	0.1233	0.8517
M1	54712	10313	36087	7111	1201	0.8957	0.1646	0.8481
M2	233062	9286	175884	42963	4929	0.6533	0.1963	0.7945
M3	246267	28833	179411	37609	414	0.9858	0.1733	0.8456
Total	595784	64372	428031	92837	10544	0.8593	0.1782	0.8265

Table 183: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.6 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	17940	36009	5794	2000	0.8997	0.1386	0.8738
M1	54712	11514	34797	8401	0	1.0000	0.1945	0.8465
M2	233062	9286	167768	51079	4929	0.6533	0.2334	0.7597
M3	246267	29247	172179	44841	0	1.0000	0.2066	0.8179
Total	595784	67987	410753	110115	6929	0.9075	0.2114	0.8035

Table 184: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.7 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	17940	33173	8630	2000	0.8997	0.2064	0.8278
M1	54712	11514	32394	10804	0	1.0000	0.2501	0.8025
M2	233062	9470	161651	57196	4745	0.6662	0.2614	0.7342
M3	246267	29247	163621	53399	0	1.0000	0.2461	0.7832
Total	595784	68171	390839	130029	6745	0.9100	0.2496	0.7704

Table 185: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.8 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	19940	31815	9988	0	1.0000	0.2389	0.8382
M1	54712	11514	30890	12308	0	1.0000	0.2849	0.7750
M2	233062	9958	156535	62312	4257	0.7005	0.2847	0.7144
M3	246267	29247	156132	60888	0	1.0000	0.2806	0.7528
Total	595784	70659	375372	145496	4257	0.9432	0.2793	0.7486

Table 186: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.9 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	19940	31580	10223	0	1.0000	0.2446	0.8344
M1	54712	11514	30838	12360	0	1.0000	0.2861	0.7741
M2	233062	9958	154950	63897	4257	0.7005	0.2920	0.7076
M3	246267	29247	154958	62062	0	1.0000	0.2860	0.7480
Total	595784	70659	372326	148542	4257	0.9432	0.2852	0.7435

Table 187: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 1.0 - Strategy 2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	61743	19940	30434	11369	0	1.0000	0.2720	0.8159
M1	54712	11514	30757	12441	0	1.0000	0.2880	0.7726
M2	233062	9958	154475	64372	4257	0.7005	0.2941	0.7055
M3	246267	29247	154446	62574	0	1.0000	0.2883	0.7459
Total	595784	70659	370112	150756	4257	0.9432	0.2894	0.7398

Table 188: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.1 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	3790	41383	1966	15576	0.1957	0.0454	0.7203
M1	50980	1349	41878	1210	6543	0.1709	0.0281	0.8479
M2	231484	4452	209223	9129	8680	0.3390	0.0418	0.9231
M3	238580	10182	209015	6916	12467	0.4496	0.0320	0.9188
Total	583759	19773	501499	19221	43266	0.3137	0.0369	0.8930

Table 189: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.2 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	9607	39135	4214	9759	0.4961	0.0972	0.7772
M1	50980	2823	39500	3588	5069	0.3577	0.0833	0.8302
M2	231484	6007	190800	27552	7125	0.4574	0.1262	0.8502
M3	238580	14907	194836	21095	7742	0.6582	0.0977	0.8791
Total	583759	33344	464271	56449	29695	0.5289	0.1084	0.8524

Table 190: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.3 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	9607	39135	4214	9759	0.4961	0.0972	0.7772
M1	50980	3626	38609	4479	4266	0.4595	0.1040	0.8285
M2	231484	6139	187431	30921	6993	0.4675	0.1416	0.8362
M3	238580	16954	191608	24323	5695	0.7486	0.1126	0.8742
Total	583759	36326	456783	63937	26713	0.5762	0.1228	0.8447

Table 191: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.4 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	13493	38102	5247	5873	0.6967	0.1210	0.8227
M1	50980	6022	37721	5367	1870	0.7631	0.1246	0.8580
M2	231484	8395	183269	35083	4737	0.6393	0.1607	0.8280
M3	238580	20543	183654	32277	2106	0.9070	0.1495	0.8559
Total	583759	48453	442746	77974	14586	0.7686	0.1497	0.8414

Table 192: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.5 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	17493	37526	5823	1873	0.9033	0.1343	0.8773
M1	50980	7129	36902	6186	763	0.9033	0.1436	0.8637
M2	231484	8594	173235	45117	4538	0.6544	0.2066	0.7855
M3	238580	22367	180191	35740	282	0.9875	0.1655	0.8490
Total	583759	55583	427854	92866	7456	0.8817	0.1783	0.8281

Table 193: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.6 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	17493	35816	7533	1873	0.9033	0.1738	0.8500
M1	50980	7892	34667	8421	0	1.0000	0.1954	0.8348
M2	231484	8594	167310	51042	4538	0.6544	0.2338	0.7599
M3	238580	22649	173410	42521	0	1.0000	0.1969	0.8218
Total	583759	56628	411203	109517	6411	0.8983	0.2103	0.8014

Table 194: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.7 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	17493	33265	10084	1873	0.9033	0.2326	0.8093
M1	50980	7892	32497	10591	0	1.0000	0.2458	0.7923
M2	231484	8594	160762	57590	4538	0.6544	0.2637	0.7316
M3	238580	22649	161698	54233	0	1.0000	0.2512	0.7727
Total	583759	56628	388222	132498	6411	0.8983	0.2545	0.7620

Table 195: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.8 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	19366	32139	11210	0	1.0000	0.2586	0.8213
M1	50980	7892	31097	11991	0	1.0000	0.2783	0.7648
M2	231484	8875	155722	62630	4257	0.6758	0.2868	0.7111
M3	238580	22649	155832	60099	0	1.0000	0.2783	0.7481
Total	583759	58782	374790	145930	4257	0.9325	0.2802	0.7427

Table 196: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.9 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	19366	31904	11445	0	1.0000	0.2640	0.8175
M1	50980	7892	30967	12121	0	1.0000	0.2813	0.7622
M2	231484	8875	154850	63502	4257	0.6758	0.2908	0.7073
M3	238580	22649	154817	61114	0	1.0000	0.2830	0.7438
Total	583759	58782	372538	148182	4257	0.9325	0.2846	0.7389

Table 197: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 1.0 - Strategy 3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	62715	19366	30874	12475	0	1.0000	0.2878	0.8011
M1	50980	7892	30886	12202	0	1.0000	0.2832	0.7607
M2	231484	8875	154464	63888	4257	0.6758	0.2926	0.7056
M3	238580	22649	154253	61678	0	1.0000	0.2856	0.7415
Total	583759	58782	370477	150243	4257	0.9325	0.2885	0.7353

Table 198: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.1 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	0	42073	1123	2912	0.0000	0.0260	0.9125
M1	45921	189	41470	2140	2122	0.0818	0.0491	0.9072
M2	226456	1939	208578	8513	7426	0.2070	0.0392	0.9296
M3	226719	2176	212442	6075	6026	0.2653	0.0278	0.9466
Total	545204	4304	504563	17851	18486	0.1889	0.0342	0.9334

Table 199: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.2 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	347	40423	2773	2565	0.1192	0.0642	0.8842
M1	45921	649	38420	5190	1662	0.2808	0.1190	0.8508
M2	226456	3454	192394	24697	5911	0.3688	0.1138	0.8648
M3	226719	3513	195682	22835	4689	0.4283	0.1045	0.8786
Total	545204	7963	466919	55495	14827	0.3494	0.1062	0.8710

Table 200: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.3 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	347	40423	2773	2565	0.1192	0.0642	0.8842
M1	45921	649	37496	6114	1662	0.2808	0.1402	0.8307
M2	226456	3634	188909	28182	5731	0.3880	0.1298	0.8502
M3	226719	4192	193300	25217	4010	0.5111	0.1154	0.8711
Total	545204	8822	460128	62286	13968	0.3871	0.1192	0.8601

Table 201: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.4 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	347	39301	3895	2565	0.1192	0.0902	0.8599
M1	45921	858	36641	6969	1453	0.3713	0.1598	0.8166
M2	226456	5008	183884	33207	4357	0.5348	0.1530	0.8341
M3	226719	4828	185376	33141	3374	0.5886	0.1517	0.8389
Total	545204	11041	445202	77212	11749	0.4845	0.1478	0.8368

Table 202: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.5 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	743	38352	4844	2169	0.2552	0.1121	0.8479
M1	45921	1438	35319	8291	873	0.6222	0.1901	0.8004
M2	226456	5207	173568	43523	4158	0.5560	0.2005	0.7894
M3	226719	6390	180302	38215	1812	0.7791	0.1749	0.8235
Total	545204	13778	427541	94873	9012	0.6046	0.1816	0.8095

Table 203: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.6 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	1020	36206	6990	1892	0.3503	0.1618	0.8074
M1	45921	1854	35118	8492	457	0.8023	0.1947	0.8051
M2	226456	5207	167568	49523	4158	0.5560	0.2281	0.7630
M3	226719	6961	171244	47273	1241	0.8487	0.2163	0.7860
Total	545204	15042	410136	112278	7748	0.6600	0.2149	0.7799

Table 204: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.7 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	1020	32980	10216	1892	0.3503	0.2365	0.7374
M1	45921	2072	32977	10633	239	0.8966	0.2438	0.7632
M2	226456	5411	159884	57207	3954	0.5778	0.2635	0.7299
M3	226719	7263	161975	56542	939	0.8855	0.2588	0.7465
Total	545204	15766	387816	134598	7024	0.6918	0.2576	0.7402

Table 205: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.8 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	1318	31766	11430	1594	0.4526	0.2646	0.7175
M1	45921	2311	31064	12546	0	1.0000	0.2877	0.7268
M2	226456	5411	155104	61987	3954	0.5778	0.2855	0.7088
M3	226719	7817	156388	62129	385	0.9531	0.2843	0.7243
Total	545204	16857	374322	148092	5933	0.7397	0.2835	0.7175

Table 206: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.9 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	1585	31644	11552	1327	0.5443	0.2674	0.7207
M1	45921	2311	31012	12598	0	1.0000	0.2889	0.7257
M2	226456	5411	154193	62898	3954	0.5778	0.2897	0.7048
M3	226719	7928	155556	62961	274	0.9666	0.2881	0.7211
Total	545204	17235	372405	150009	5555	0.7563	0.2871	0.7147

Table 207: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 1.0 - Strategy 4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	46108	2912	30902	12294	0	1.0000	0.2846	0.7334
M1	45921	2311	30931	12679	0	1.0000	0.2907	0.7239
M2	226456	5411	153922	63169	3954	0.5778	0.2910	0.7036
M3	226719	8041	154392	64125	161	0.9804	0.2935	0.7165
Total	545204	18675	370147	152267	4115	0.8194	0.2915	0.7132

Table 208: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.1 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	13521	40730	1810	33118	0.2899	0.0425	0.6083
M1	53935	1970	41604	1952	8409	0.1898	0.0448	0.8079
M2	263920	11663	208964	8875	34418	0.2531	0.0407	0.8360
M3	246197	10635	210795	8099	16668	0.3895	0.0370	0.8994
Total	653231	37789	502093	20736	92613	0.2898	0.0397	0.8265

Table 209: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.2 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	14697	38503	4037	31942	0.3151	0.0949	0.5966
M1	53935	3846	38637	4919	6533	0.3706	0.1129	0.7877
M2	263920	18777	191878	25961	27304	0.4075	0.1192	0.7982
M3	246197	18111	195680	23214	9192	0.6633	0.1061	0.8684
Total	653231	55431	464698	58131	74971	0.4251	0.1112	0.7962

Table 210: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.3 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	14697	38294	4246	31942	0.3151	0.0998	0.5942
M1	53935	4804	37787	5769	5575	0.4629	0.1325	0.7897
M2	263920	21625	188895	28944	24456	0.4693	0.1329	0.7977
M3	246197	20218	191804	27090	7085	0.7405	0.1238	0.8612
Total	653231	61344	456780	66049	69058	0.4704	0.1263	0.7932

Table 211: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.4 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	28627	37169	5371	18012	0.6138	0.1263	0.7378
M1	53935	6769	36899	6657	3610	0.6522	0.1528	0.8096
M2	263920	26754	184146	33693	19327	0.5806	0.1547	0.7991
M3	246197	23981	183689	35205	3322	0.8783	0.1608	0.8435
Total	653231	86131	441903	80926	44271	0.6605	0.1548	0.8083

Table 212: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.5 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	41005	36653	5887	5634	0.8792	0.1384	0.8708
M1	53935	9416	35433	8123	963	0.9072	0.1865	0.8315
M2	263920	31510	174138	43701	14571	0.6838	0.2006	0.7792
M3	246197	26502	177130	41764	801	0.9707	0.1908	0.8271
Total	653231	108433	423354	99475	21969	0.8315	0.1903	0.8141

Table 213: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.6 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	41005	35333	7207	5634	0.8792	0.1694	0.8560
M1	53935	10379	34218	9338	0	1.0000	0.2144	0.8269
M2	263920	33097	168638	49201	12984	0.7182	0.2259	0.7644
M3	246197	27303	170750	48144	0	1.0000	0.2199	0.8044
Total	653231	111784	408939	113890	18618	0.8572	0.2178	0.7971

Table 214: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.7 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	46639	32616	9924	0	1.0000	0.2333	0.8887
M1	53935	10379	32390	11166	0	1.0000	0.2564	0.7930
M2	263920	37979	161217	56622	8102	0.8242	0.2599	0.7548
M3	246197	27303	161061	57833	0	1.0000	0.2642	0.7651
Total	653231	122300	387284	135545	8102	0.9379	0.2593	0.7801

Table 215: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.8 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	46639	31405	11135	0	1.0000	0.2618	0.8751
M1	53935	10379	31201	12355	0	1.0000	0.2837	0.7709
M2	263920	40151	155935	61904	5930	0.8713	0.2842	0.7430
M3	246197	27303	155896	62998	0	1.0000	0.2878	0.7441
Total	653231	124472	374437	148392	5930	0.9545	0.2838	0.7638

Table 216: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.9 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	46639	31248	11292	0	1.0000	0.2654	0.8734
M1	53935	10379	31149	12407	0	1.0000	0.2849	0.7700
M2	263920	41171	154319	63520	4910	0.8934	0.2916	0.7407
M3	246197	27303	155070	63824	0	1.0000	0.2916	0.7408
Total	653231	125492	371786	151043	4910	0.9623	0.2889	0.7613

Table 217: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 1.0 - Strategy 5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	89179	46639	30360	12180	0	1.0000	0.2863	0.8634
M1	53935	10379	31068	12488	0	1.0000	0.2867	0.7685
M2	263920	42029	154022	63817	4052	0.9121	0.2930	0.7428
M3	246197	27303	154347	64547	0	1.0000	0.2949	0.7378
Total	653231	126350	369797	153032	4052	0.9689	0.2927	0.7595

Table 218: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.1 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	11027	208370	6948	7439	0.5972	0.0323	0.9385
M3	231846	11807	208412	8051	3576	0.7675	0.0372	0.9499
Total	465630	22834	416782	14999	11015	0.6746	0.0347	0.9441

Table 219: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.2 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	13321	194138	21180	5145	0.7214	0.0984	0.8874
M3	231846	15184	194115	22348	199	0.9871	0.1032	0.9028
Total	465630	28505	388253	43528	5344	0.8421	0.1008	0.8950

Table 220: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.3 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	15958	189634	25684	2508	0.8642	0.1193	0.8794
M3	231846	15303	189531	26932	80	0.9948	0.1244	0.8835
Total	465630	31261	379165	52616	2588	0.9235	0.1219	0.8814

Table 221: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.4 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	18245	181620	33698	221	0.9880	0.1565	0.8549
M3	231846	15303	182809	33654	80	0.9948	0.1555	0.8545
Total	465630	33548	364429	67352	301	0.9911	0.1560	0.8547

Table 222: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.5 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	18245	165612	49706	221	0.9880	0.2308	0.7864
M3	231846	15303	174273	42190	80	0.9948	0.1949	0.8177
Total	465630	33548	339885	91896	301	0.9911	0.2128	0.8020

Table 223: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.6 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	18245	162438	52880	221	0.9880	0.2456	0.7729
M3	231846	15303	167569	48894	80	0.9948	0.2259	0.7888
Total	465630	33548	330007	101774	301	0.9911	0.2357	0.7808

Table 224: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.7 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	18429	159008	56310	37	0.9980	0.2615	0.7590
M3	231846	15303	162288	54175	80	0.9948	0.2503	0.7660
Total	465630	33732	321296	110485	117	0.9965	0.2559	0.7625

Table 225: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.8 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	18429	155688	59630	37	0.9980	0.2769	0.7448
M3	231846	15303	155264	61199	80	0.9948	0.2827	0.7357
Total	465630	33732	310952	120829	117	0.9965	0.2798	0.7403

Table 226: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.9 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	18429	154245	61073	37	0.9980	0.2836	0.7386
M3	231846	15303	154707	61756	80	0.9948	0.2853	0.7333
Total	465630	33732	308952	122829	117	0.9965	0.2845	0.7360

Table 227: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 1.0 - Body exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233784	18429	154131	61187	37	0.9980	0.2842	0.7381
M3	231846	15303	153932	62531	80	0.9948	0.2889	0.7299
Total	465630	33732	308063	123718	117	0.9965	0.2865	0.7340

Table 228: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.1 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	0	211756	7422	14431	0.0000	0.0339	0.9065
M3	238587	8622	210912	6534	12519	0.4078	0.0300	0.9201
Total	472196	8622	422668	13956	26950	0.2424	0.0320	0.9134

Table 229: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.2 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	0	194231	24947	14431	0.0000	0.1138	0.8314
M3	238587	17128	193394	24052	4013	0.8102	0.1106	0.8824
Total	472196	17128	387625	48999	18444	0.4815	0.1122	0.8572

Table 230: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.3 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	0	186722	32456	14431	0.0000	0.1481	0.7993
M3	238587	19303	186646	30800	1838	0.9131	0.1416	0.8632
Total	472196	19303	373368	63256	16269	0.5426	0.1449	0.8316

Table 231: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.4 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	1790	183907	35271	12641	0.1240	0.1609	0.7949
M3	238587	20253	178123	39323	888	0.9580	0.1808	0.8315
Total	472196	22043	362030	74594	13529	0.6197	0.1708	0.8134

Table 232: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.5 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	3928	173572	45606	10503	0.2722	0.2081	0.7598
M3	238587	20751	173359	44087	390	0.9816	0.2027	0.8136
Total	472196	24679	346931	89693	10893	0.6938	0.2054	0.7870

Table 233: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.6 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	3928	164795	54383	10503	0.2722	0.2481	0.7222
M3	238587	20917	166020	51426	224	0.9894	0.2365	0.7835
Total	472196	24845	330815	105809	10727	0.6984	0.2423	0.7532

Table 234: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.7 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	5994	159765	59413	8437	0.4154	0.2711	0.7096
M3	238587	21061	159576	57870	80	0.9962	0.2661	0.7571
Total	472196	27055	319341	117283	8517	0.7606	0.2686	0.7336

Table 235: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.8 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	5994	155279	63899	8437	0.4154	0.2915	0.6904
M3	238587	21061	155992	61454	80	0.9962	0.2826	0.7421
Total	472196	27055	311271	125353	8517	0.7606	0.2871	0.7165

Table 236: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.9 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	5994	154750	64428	8437	0.4154	0.2940	0.6881
M3	238587	21061	154716	62730	80	0.9962	0.2885	0.7367
Total	472196	27055	309466	127158	8517	0.7606	0.2912	0.7127

Table 237: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 1.0 - Cookie field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	233609	5994	154223	64955	8437	0.4154	0.2964	0.6858
M3	238587	21061	154382	63064	80	0.9962	0.2900	0.7353
Total	472196	27055	308605	128019	8517	0.7606	0.2932	0.7108

Table 238: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.1 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	1838	211475	7518	15160	0.1081	0.0343	0.9039
M3	231805	1956	210150	6985	12714	0.1333	0.0322	0.9150
Total	467796	3794	421625	14503	27874	0.1198	0.0333	0.9094

Table 239: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.2 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	5291	194772	24221	11707	0.3113	0.1106	0.8478
M3	231805	5559	198148	18987	9111	0.3789	0.0874	0.8788
Total	467796	10850	392920	43208	20818	0.3426	0.0991	0.8631

Table 240: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.3 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	6007	194061	24932	10991	0.3534	0.1138	0.8478
M3	231805	6010	194353	22782	8660	0.4097	0.1049	0.8644
Total	467796	12017	388414	47714	19651	0.3795	0.1094	0.8560

Table 241: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.4 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	9980	187872	31121	7018	0.5871	0.1421	0.8384
M3	231805	9162	185619	31516	5508	0.6245	0.1451	0.8403
Total	467796	19142	373491	62637	12526	0.6045	0.1436	0.8393

Table 242: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.5 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	9980	181594	37399	7018	0.5871	0.1708	0.8118
M3	231805	12202	183924	33211	2468	0.8318	0.1530	0.8461
Total	467796	22182	365518	70610	9486	0.7005	0.1619	0.8288

Table 243: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.6 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	10594	176360	42633	6404	0.6232	0.1947	0.7922
M3	231805	13974	176269	40866	696	0.9526	0.1882	0.8207
Total	467796	24568	352629	83499	7100	0.7758	0.1915	0.8063

Table 244: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.7 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	12586	167911	51082	4412	0.7404	0.2333	0.7648
M3	231805	13974	164070	53065	696	0.9526	0.2444	0.7681
Total	467796	26560	331981	104147	5108	0.8387	0.2388	0.7664

Table 245: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.8 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	12586	155308	63685	4412	0.7404	0.2908	0.7114
M3	231805	14205	156539	60596	465	0.9683	0.2791	0.7366
Total	467796	26791	311847	124281	4877	0.8460	0.2850	0.7239

Table 246: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.9 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	12586	154744	64249	4412	0.7404	0.2934	0.7091
M3	231805	14316	155403	61732	354	0.9759	0.2843	0.7322
Total	467796	26902	310147	125981	4766	0.8495	0.2889	0.7205

Table 247: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 1.0 - Custom field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	235991	12586	154230	64763	4412	0.7404	0.2957	0.7069
M3	231805	14429	154384	62751	241	0.9836	0.2890	0.7283
Total	467796	27015	308614	127514	4653	0.8531	0.2924	0.7175

Table 248: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.1 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	6380	207564	11597	9412	0.4040	0.0529	0.9106
M3	233360	9464	209254	7048	7594	0.5548	0.0326	0.9373
Total	468313	15844	416818	18645	17006	0.4823	0.0428	0.9239

Table 249: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.2 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	10020	191877	27284	5772	0.6345	0.1245	0.8593
M3	233360	11671	195839	20463	5387	0.6842	0.0946	0.8892
Total	468313	21691	387716	47747	11159	0.6603	0.1096	0.8742

Table 250: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.3 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	10020	190300	28861	5772	0.6345	0.1317	0.8526
M3	233360	13440	195253	21049	3618	0.7879	0.0973	0.8943
Total	468313	23460	385553	49910	9390	0.7142	0.1146	0.8734

Table 251: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.4 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	11901	186475	32686	3891	0.7536	0.1491	0.8443
M3	233360	16135	188157	28145	923	0.9459	0.1301	0.8754
Total	468313	28036	374632	60831	4814	0.8535	0.1397	0.8598

Table 252: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.5 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	13818	180315	38846	1974	0.8750	0.1772	0.8263
M3	233360	16978	182408	33894	80	0.9953	0.1567	0.8544
Total	468313	30796	362723	72740	2054	0.9375	0.1670	0.8403

Table 253: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.6 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	14791	175549	43612	1001	0.9366	0.1990	0.8101
M3	233360	16978	173817	42485	80	0.9953	0.1964	0.8176
Total	468313	31769	349366	86097	1081	0.9671	0.1977	0.8138

Table 254: Dumont - Analysis adaptive dataset - σ = 10000 - Alpha = 0.7 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	14995	161277	57884	797	0.9495	0.2641	0.7502
M3	233360	16978	160309	55993	80	0.9953	0.2589	0.7597
Total	468313	31973	321586	113877	877	0.9733	0.2615	0.7550

Table 255: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.8 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	15764	157198	61963	28	0.9982	0.2827	0.7362
M3	233360	16978	156471	59831	80	0.9953	0.2766	0.7433
Total	468313	32742	313669	121794	108	0.9967	0.2797	0.7397

Table 256: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.9 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	15764	154858	64303	28	0.9982	0.2934	0.7262
M3	233360	16978	155244	61058	80	0.9953	0.2823	0.7380
Total	468313	32742	310102	125361	108	0.9967	0.2879	0.7321

Table 257: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 1.0 - URI exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234953	15764	154509	64652	28	0.9982	0.2950	0.7247
M3	233360	16978	154362	61940	80	0.9953	0.2864	0.7342
Total	468313	32742	308871	126592	108	0.9967	0.2907	0.7295

Table 258: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.1 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	2205	208657	8784	15073	0.1276	0.0404	0.8984
M3	237812	2972	211277	6986	16577	0.1520	0.0320	0.9009
Total	472531	5177	419934	15770	31650	0.1406	0.0362	0.8996

Table 259: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.2 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	5360	192370	25071	11918	0.3102	0.1153	0.8424
M3	237812	7403	198250	20013	12146	0.3787	0.0917	0.8648
Total	472531	12763	390620	45084	24064	0.3466	0.1035	0.8537

Table 260: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.3 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	5360	190653	26788	11918	0.3102	0.1232	0.8351
M3	237812	9495	196673	21590	10054	0.4857	0.0989	0.8669
Total	472531	14855	387326	48378	21972	0.4034	0.1110	0.8511

Table 261: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.4 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	7328	188575	28866	9950	0.4241	0.1328	0.8346
M3	237812	15456	187233	31030	4093	0.7906	0.1422	0.8523
Total	472531	22784	375808	59896	14043	0.6187	0.1375	0.8435

Table 262: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.5 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	8626	178666	38775	8652	0.4992	0.1783	0.7979
M3	237812	18858	180805	37458	691	0.9647	0.1716	0.8396
Total	472531	27484	359471	76233	9343	0.7463	0.1750	0.8189

Table 263: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.6 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	8626	168610	48831	8652	0.4992	0.2246	0.7551
M3	237812	18988	171441	46822	561	0.9713	0.2145	0.8008
Total	472531	27614	340051	95653	9213	0.7498	0.2195	0.7781

Table 264: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.7 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	9450	160722	56719	7828	0.5469	0.2608	0.7250
M3	237812	19146	160250	58013	403	0.9794	0.2658	0.7544
Total	472531	28596	320972	114732	8231	0.7765	0.2633	0.7398

Table 265: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.8 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	11622	155966	61475	5656	0.6726	0.2827	0.7140
M3	237812	19469	155259	63004	80	0.9959	0.2887	0.7347
Total	472531	31091	311225	124479	5736	0.8442	0.2857	0.7244

Table 266: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 0.9 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	12642	154448	62993	4636	0.7317	0.2897	0.7119
M3	237812	19469	155031	63232	80	0.9959	0.2897	0.7338
Total	472531	32111	309479	126225	4716	0.8719	0.2897	0.7229

Table 267: Dumont - Analysis adaptive dataset - $\sigma = 10000$ - Alpha = 1.0 - User-Agent field exfiltration

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
M0	0	0	0	0	0	0.0000	0.0000	0.0000
M1	0	0	0	0	0	0.0000	0.0000	0.0000
M2	234719	13500	154010	63431	3778	0.7813	0.2917	0.7137
M3	237812	19469	154519	63744	80	0.9959	0.2921	0.7316
Total	472531	32969	308529	127175	3858	0.8952	0.2919	0.7227

Table 268: DUMONT - Analysis exfiltration dataset - Alpha = 0.1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	0	0	0	608	0.0000	0.0000	0.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	311	0	0	87	0.7814	0.0000	0.7814
SPYWARE	1241	0	0	0	1241	0.0000	0.0000	0.0000
TIM	67	1	0	0	66	0.0149	0.0000	0.0149
URSNIF	2472	936	0	0	1536	0.3786	0.0000	0.3786
Total	4857	1248	0	0	3609	0.2569	0.0000	0.2569

Table 269: DUMONT - Analysis exfiltration dataset - Alpha = 0.2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	0	0	0	608	0.0000	0.0000	0.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	333	0	0	65	0.8367	0.0000	0.8367
SPYWARE	1241	0	0	0	1241	0.0000	0.0000	0.0000
TIM	67	33	0	0	34	0.4925	0.0000	0.4925
URSNIF	2472	936	0	0	1536	0.3786	0.0000	0.3786
Total	4857	1302	0	0	3555	0.2681	0.0000	0.2681

Table 270: DUMONT - Analysis exfiltration dataset - Alpha = 0.3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	0	0	0	608	0.0000	0.0000	0.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	333	0	0	65	0.8367	0.0000	0.8367
SPYWARE	1241	0	0	0	1241	0.0000	0.0000	0.0000
TIM	67	60	0	0	7	0.8955	0.0000	0.8955
URSNIF	2472	936	0	0	1536	0.3786	0.0000	0.3786
Total	4857	1329	0	0	3528	0.2736	0.0000	0.2736

Table 271: DUMONT - Analysis exfiltration dataset - Alpha = 0.4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	9	0	0	599	0.0148	0.0000	0.0148
FAREIT	68	47	0	0	21	0.6912	0.0000	0.6912
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	333	0	0	65	0.8367	0.0000	0.8367
SPYWARE	1241	1226	0	0	15	0.9879	0.0000	0.9879
TIM	67	61	0	0	6	0.9104	0.0000	0.9104
URSNIF	2472	990	0	0	1482	0.4005	0.0000	0.4005
Total	4857	2666	0	0	2191	0.5489	0.0000	0.5489

Table 272: DUMONT - Analysis exfiltration dataset - Alpha = 0.5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	18	0	0	590	0.0296	0.0000	0.0296
FAREIT	68	47	0	0	21	0.6912	0.0000	0.6912
FTPINFOSTEAL	3	3	0	0	0	1.0000	0.0000	1.0000
SHAKTI	398	333	0	0	65	0.8367	0.0000	0.8367
SPYWARE	1241	1226	0	0	15	0.9879	0.0000	0.9879
TIM	67	61	0	0	6	0.9104	0.0000	0.9104
URSNIF	2472	1601	0	0	871	0.6477	0.0000	0.6477
Total	4857	3289	0	0	1568	0.6772	0.0000	0.6772

Table 273: DUMONT - Analysis exfiltration dataset - Alpha = 0.6

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	34	0	0	574	0.0559	0.0000	0.0559
FAREIT	68	47	0	0	21	0.6912	0.0000	0.6912
FTPINFOSTEAL	3	3	0	0	0	1.0000	0.0000	1.0000
SHAKTI	398	375	0	0	23	0.9422	0.0000	0.9422
SPYWARE	1241	1226	0	0	15	0.9879	0.0000	0.9879
TIM	67	65	0	0	2	0.9701	0.0000	0.9701
URSNIF	2472	1906	0	0	566	0.7710	0.0000	0.7710
Total	4857	3656	0	0	1201	0.7527	0.0000	0.7527

Table 274: DUMONT - Analysis exfiltration dataset - Alpha = 0.7

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	131	0	0	477	0.2155	0.0000	0.2155
FAREIT	68	47	0	0	21	0.6912	0.0000	0.6912
FTPINFOSTEAL	3	3	0	0	0	1.0000	0.0000	1.0000
SHAKTI	398	375	0	0	23	0.9422	0.0000	0.9422
SPYWARE	1241	1226	0	0	15	0.9879	0.0000	0.9879
TIM	67	65	0	0	2	0.9701	0.0000	0.9701
URSNIF	2472	1925	0	0	547	0.7787	0.0000	0.7787
Total	4857	3772	0	0	1085	0.7766	0.0000	0.7766

Table 275: DUMONT - Analysis exfiltration dataset - Alpha = 0.8

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	195	0	0	413	0.3207	0.0000	0.3207
FAREIT	68	47	0	0	21	0.6912	0.0000	0.6912
FTPINFOSTEAL	3	3	0	0	0	1.0000	0.0000	1.0000
SHAKTI	398	375	0	0	23	0.9422	0.0000	0.9422
SPYWARE	1241	1226	0	0	15	0.9879	0.0000	0.9879
TIM	67	66	0	0	1	0.9851	0.0000	0.9851
URSNIF	2472	2119	0	0	353	0.8572	0.0000	0.8572
Total	4857	4031	0	0	826	0.8299	0.0000	0.8299

Table 276: DUMONT - Analysis exfiltration dataset - Alpha = 0.9

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	68	0	0	0	1.0000	0.0000	1.0000
FTPINFOSTEAL	3	3	0	0	0	1.0000	0.0000	1.0000
SHAKTI	398	375	0	0	23	0.9422	0.0000	0.9422
SPYWARE	1241	1236	0	0	5	0.9960	0.0000	0.9960
TIM	67	66	0	0	1	0.9851	0.0000	0.9851
URSNIF	2472	2119	0	0	353	0.8572	0.0000	0.8572
Total	4857	4475	0	0	382	0.9214	0.0000	0.9214

Table 277: DUMONT - Analysis exfiltration dataset - Alpha = 1.0

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	68	0	0	0	1.0000	0.0000	1.0000
FTPINFOSTEAL	3	3	0	0	0	1.0000	0.0000	1.0000
SHAKTI	398	398	0	0	0	1.0000	0.0000	1.0000
SPYWARE	1241	1241	0	0	0	1.0000	0.0000	1.0000
TIM	67	67	0	0	0	1.0000	0.0000	1.0000
URSNIF	2472	2469	0	0	3	0.9988	0.0000	0.9988
Total	4857	4854	0	0	3	0.9994	0.0000	0.9994

Table 278: Dumont - Analysis exfiltration dataset - σ = 10000 - Alpha = 0.1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	0	0	0	608	0.0000	0.0000	0.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	377	0	0	21	0.9472	0.0000	0.9472
SPYWARE	1241	0	0	0	1241	0.0000	0.0000	0.0000
TIM	67	0	0	0	67	0.0000	0.0000	0.0000
URSNIF	2472	780	0	0	1692	0.3155	0.0000	0.3155
Total	4857	1157	0	0	3700	0.2382	0.0000	0.2382

Table 279: Dumont - Analysis exfiltration dataset - σ = 10000 - Alpha = 0.2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	0	0	0	608	0.0000	0.0000	0.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	377	0	0	21	0.9472	0.0000	0.9472
SPYWARE	1241	0	0	0	1241	0.0000	0.0000	0.0000
TIM	67	0	0	0	67	0.0000	0.0000	0.0000
URSNIF	2472	780	0	0	1692	0.3155	0.0000	0.3155
Total	4857	1157	0	0	3700	0.2382	0.0000	0.2382

Table 280: Dumont - Analysis exfiltration dataset - σ = 10000 - Alpha = 0.3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	0	0	0	608	0.0000	0.0000	0.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	377	0	0	21	0.9472	0.0000	0.9472
SPYWARE	1241	0	0	0	1241	0.0000	0.0000	0.0000
TIM	67	0	0	0	67	0.0000	0.0000	0.0000
URSNIF	2472	780	0	0	1692	0.3155	0.0000	0.3155
Total	4857	1157	0	0	3700	0.2382	0.0000	0.2382

Table 281: Dumont - Analysis exfiltration dataset - σ = 10000 - Alpha = 0.4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	377	0	0	21	0.9472	0.0000	0.9472
SPYWARE	1241	354	0	0	887	0.2853	0.0000	0.2853
TIM	67	0	0	0	67	0.0000	0.0000	0.0000
URSNIF	2472	780	0	0	1692	0.3155	0.0000	0.3155
Total	4857	2119	0	0	2738	0.4363	0.0000	0.4363

Table 282: Dumont - Analysis exfiltration dataset - σ = 10000 - Alpha = 0.5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	377	0	0	21	0.9472	0.0000	0.9472
SPYWARE	1241	977	0	0	264	0.7873	0.0000	0.7873
TIM	67	0	0	0	67	0.0000	0.0000	0.0000
URSNIF	2472	867	0	0	1605	0.3507	0.0000	0.3507
Total	4857	2829	0	0	2028	0.5825	0.0000	0.5825

Table 283: Dumont - Analysis exfiltration dataset - σ = 10000 - Alpha = 0.6

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	377	0	0	21	0.9472	0.0000	0.9472
SPYWARE	1241	977	0	0	264	0.7873	0.0000	0.7873
TIM	67	0	0	0	67	0.0000	0.0000	0.0000
URSNIF	2472	876	0	0	1596	0.3544	0.0000	0.3544
Total	4857	2838	0	0	2019	0.5843	0.0000	0.5843

Table 284: Dumont - Analysis exfiltration dataset - σ = 10000 - Alpha = 0.7

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	377	0	0	21	0.9472	0.0000	0.9472
SPYWARE	1241	977	0	0	264	0.7873	0.0000	0.7873
TIM	67	0	0	0	67	0.0000	0.0000	0.0000
URSNIF	2472	973	0	0	1499	0.3936	0.0000	0.3936
Total	4857	2935	0	0	1922	0.6043	0.0000	0.6043

Table 285: Dumont - Analysis exfiltration dataset - σ = 10000 - Alpha = 0.8

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	377	0	0	21	0.9472	0.0000	0.9472
SPYWARE	1241	977	0	0	264	0.7873	0.0000	0.7873
TIM	67	0	0	0	67	0.0000	0.0000	0.0000
URSNIF	2472	973	0	0	1499	0.3936	0.0000	0.3936
Total	4857	2935	0	0	1922	0.6043	0.0000	0.6043

Table 286: Dumont - Analysis exfiltration dataset - σ = 10000 - Alpha = 0.9

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	377	0	0	21	0.9472	0.0000	0.9472
SPYWARE	1241	977	0	0	264	0.7873	0.0000	0.7873
TIM	67	0	0	0	67	0.0000	0.0000	0.0000
URSNIF	2472	973	0	0	1499	0.3936	0.0000	0.3936
Total	4857	2935	0	0	1922	0.6043	0.0000	0.6043

Table 287: Dumont - Analysis exfiltration dataset - σ = 10000 - Alpha = 1.0

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
COSMIC_DUKE	608	608	0	0	0	1.0000	0.0000	1.0000
FAREIT	68	0	0	0	68	0.0000	0.0000	0.0000
FTPINFOSTEAL	3	0	0	0	3	0.0000	0.0000	0.0000
SHAKTI	398	377	0	0	21	0.9472	0.0000	0.9472
SPYWARE	1241	977	0	0	264	0.7873	0.0000	0.7873
TIM	67	0	0	0	67	0.0000	0.0000	0.0000
URSNIF	2472	987	0	0	1485	0.3993	0.0000	0.3993
Total	4857	2949	0	0	1908	0.6072	0.0000	0.6072

Table 288: DUMONT - Analysis user dataset - Alpha = 0.1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	1544	2413	0	0.0000	0.6098	0.3902
User 2	243	0	22	221	0	0.0000	0.9095	0.0905
User 3	17210	0	8936	8274	0	0.0000	0.4808	0.5192
User 4	9011	0	8106	905	0	0.0000	0.1004	0.8996
Total	30421	0	18608	11813	0	0.0000	0.3883	0.6117

Table 289: DUMONT - Analysis user dataset - Alpha = 0.2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	1013	2944	0	0.0000	0.7440	0.2560
User 2	243	0	22	221	0	0.0000	0.9095	0.0905
User 3	17210	0	8111	9099	0	0.0000	0.5287	0.4713
User 4	9011	0	8056	955	0	0.0000	0.1060	0.8940
Total	30421	0	17202	13219	0	0.0000	0.4345	0.5655

Table 290: DUMONT - Analysis user dataset - Alpha = 0.3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	978	2979	0	0.0000	0.7528	0.2472
User 2	243	0	5	238	0	0.0000	0.9794	0.0206
User 3	17210	0	5392	11818	0	0.0000	0.6867	0.3133
User 4	9011	0	5110	3901	0	0.0000	0.4329	0.5671
Total	30421	0	11485	18936	0	0.0000	0.6225	0.3775

Table 291: DUMONT - Analysis user dataset - Alpha = 0.4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	314	3643	0	0.0000	0.9206	0.0794
User 2	243	0	5	238	0	0.0000	0.9794	0.0206
User 3	17210	0	1518	15692	0	0.0000	0.9118	0.0882
User 4	9011	0	4225	4786	0	0.0000	0.5311	0.4689
Total	30421	0	6062	24359	0	0.0000	0.8007	0.1993

Table 292: DUMONT - Analysis user dataset - Alpha = 0.5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	278	3679	0	0.0000	0.9297	0.0703
User 2	243	0	5	238	0	0.0000	0.9794	0.0206
User 3	17210	0	1427	15783	0	0.0000	0.9171	0.0829
User 4	9011	0	3788	5223	0	0.0000	0.5796	0.4204
Total	30421	0	5498	24923	0	0.0000	0.8193	0.1807

Table 293: DUMONT - Analysis user dataset - Alpha = 0.6

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	209	3748	0	0.0000	0.9472	0.0528
User 2	243	0	2	241	0	0.0000	0.9918	0.0082
User 3	17210	0	1413	15797	0	0.0000	0.9179	0.0821
User 4	9011	0	3410	5601	0	0.0000	0.6216	0.3784
Total	30421	0	5034	25387	0	0.0000	0.8345	0.1655

Table 294: DUMONT - Analysis user dataset - Alpha = 0.7

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	120	3837	0	0.0000	0.9697	0.0303
User 2	243	0	0	243	0	0.0000	1.0000	0.0000
User 3	17210	0	469	16741	0	0.0000	0.9727	0.0273
User 4	9011	0	777	8234	0	0.0000	0.9138	0.0862
Total	30421	0	1366	29055	0	0.0000	0.9551	0.0449

Table 295: DUMONT - Analysis user dataset - Alpha = 0.8

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	38	3919	0	0.0000	0.9904	0.0096
User 2	243	0	0	243	0	0.0000	1.0000	0.0000
User 3	17210	0	107	17103	0	0.0000	0.9938	0.0062
User 4	9011	0	184	8827	0	0.0000	0.9796	0.0204
Total	30421	0	329	30092	0	0.0000	0.9892	0.0108

Table 296: DUMONT - Analysis user dataset - Alpha = 0.9

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	1	3956	0	0.0000	0.9997	0.0003
User 2	243	0	0	243	0	0.0000	1.0000	0.0000
User 3	17210	0	15	17195	0	0.0000	0.9991	0.0009
User 4	9011	0	184	8827	0	0.0000	0.9796	0.0204
Total	30421	0	200	30221	0	0.0000	0.9934	0.0066

Table 297: DUMONT - Analysis user dataset - Alpha = 1.0

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	0	3957	0	0.0000	1.0000	0.0000
User 2	243	0	0	243	0	0.0000	1.0000	0.0000
User 3	17210	0	4	17206	0	0.0000	0.9998	0.0002
User 4	9011	0	16	8995	0	0.0000	0.9982	0.0018
Total	30421	0	20	30401	0	0.0000	0.9993	0.0007

Table 298: DUMONT - Analysis user dataset - σ = 10000 - Alpha = 0.1

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3456	501	0	0.0000	0.1266	0.8734
User 2	243	0	243	0	0	0.0000	0.0000	1.0000
User 3	17210	0	12625	4585	0	0.0000	0.2664	0.7336
User 4	9011	0	9011	0	0	0.0000	0.0000	1.0000
Total	30421	0	25335	5086	0	0.0000	0.1672	0.8328

Table 299: DUMONT - Analysis user dataset - σ = 10000 - Alpha = 0.2

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3304	653	0	0.0000	0.1650	0.8350
User 2	243	0	243	0	0	0.0000	0.0000	1.0000
User 3	17210	0	12045	5165	0	0.0000	0.3001	0.6999
User 4	9011	0	7013	1998	0	0.0000	0.2217	0.7783
Total	30421	0	22605	7816	0	0.0000	0.2569	0.7431

Table 300: DUMONT - Analysis user dataset - σ = 10000 - Alpha = 0.3

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3304	653	0	0.0000	0.1650	0.8350
User 2	243	0	243	0	0	0.0000	0.0000	1.0000
User 3	17210	0	10857	6353	0	0.0000	0.3691	0.6309
User 4	9011	0	5154	3857	0	0.0000	0.4280	0.5720
Total	30421	0	19558	10863	0	0.0000	0.3571	0.6429

Table 301: DUMONT - Analysis user dataset - σ = 10000 - Alpha = 0.4

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3304	653	0	0.0000	0.1650	0.8350
User 2	243	0	243	0	0	0.0000	0.0000	1.0000
User 3	17210	0	9189	8021	0	0.0000	0.4661	0.5339
User 4	9011	0	4911	4100	0	0.0000	0.4550	0.5450
Total	30421	0	17647	12774	0	0.0000	0.4199	0.5801

Table 302: DUMONT - Analysis user dataset - σ = 10000 - Alpha = 0.5

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3304	653	0	0.0000	0.1650	0.8350
User 2	243	0	243	0	0	0.0000	0.0000	1.0000
User 3	17210	0	9189	8021	0	0.0000	0.4661	0.5339
User 4	9011	0	4572	4439	0	0.0000	0.4926	0.5074
Total	30421	0	17308	13113	0	0.0000	0.4311	0.5689

Table 303: DUMONT - Analysis user dataset - σ = 10000 - Alpha = 0.6

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3304	653	0	0.0000	0.1650	0.8350
User 2	243	0	243	0	0	0.0000	0.0000	1.0000
User 3	17210	0	9189	8021	0	0.0000	0.4661	0.5339
User 4	9011	0	4572	4439	0	0.0000	0.4926	0.5074
Total	30421	0	17308	13113	0	0.0000	0.4311	0.5689

Table 304: DUMONT - Analysis user dataset - σ = 10000 - Alpha = 0.7

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3115	842	0	0.0000	0.2128	0.7872
User 2	243	0	243	0	0	0.0000	0.0000	1.0000
User 3	17210	0	8460	8750	0	0.0000	0.5084	0.4916
User 4	9011	0	3784	5227	0	0.0000	0.5801	0.4199
Total	30421	0	15602	14819	0	0.0000	0.4871	0.5129

Table 305: DUMONT - Analysis user dataset - σ = 10000 - Alpha = 0.8

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3115	842	0	0.0000	0.2128	0.7872
User 2	243	0	243	0	0	0.0000	0.0000	1.0000
User 3	17210	0	8460	8750	0	0.0000	0.5084	0.4916
User 4	9011	0	3532	5479	0	0.0000	0.6080	0.3920
Total	30421	0	15350	15071	0	0.0000	0.4954	0.5046

Table 306: DUMONT - Analysis user dataset - σ = 10000 - Alpha = 0.9

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3115	842	0	0.0000	0.2128	0.7872
User 2	243	0	243	0	0	0.0000	0.0000	1.0000
User 3	17210	0	8460	8750	0	0.0000	0.5084	0.4916
User 4	9011	0	3532	5479	0	0.0000	0.6080	0.3920
Total	30421	0	15350	15071	0	0.0000	0.4954	0.5046

Table 307: DUMONT - Analysis user dataset - σ = 10000 - Alpha = 1.0

Dataset	Packets	TP	TN	FP	FN	TPR	FPR	Accuracy
User 1	3957	0	3115	842	0	0.0000	0.2128	0.7872
User 2	243	0	243	0	0	0.0000	0.0000	1.0000
User 3	17210	0	8460	8750	0	0.0000	0.5084	0.4916
User 4	9011	0	3490	5521	0	0.0000	0.6127	0.3873
Total	30421	0	15308	15113	0	0.0000	0.4968	0.5032