## **Regular Paper**

## Survey and Analysis on ATT&CK Mapping Function of Online Sandbox for Understanding and Efficient Using

Shota Fujii<sup>1,2,a)</sup> Rei Yamagishi<sup>1</sup> Toshihiro Yamauchi<sup>3</sup>

Received: March 8, 2022, Accepted: September 2, 2022

**Abstract:** Dynamic analysis that automatically analyzes malware has become the defacto standard for coping with the huge amount of current malware types. One analysis support is a function that maps the malware behavior to each element of the MITRE ATT&CK<sup>®</sup> Technique. This function has been adopted in many online sandboxes and contributes to the efficiency of analysis. On the other hand, this function depends on the implementation of the mapping rules, which may affect the analysis results. Therefore, we investigated the actual situation of online sandboxes that have a function for mapping to the attack technique. In this study, we analyzed a total of 26,078 malware analysis results from three online sandboxes, found that the characteristics for matching to each technique differed among the sandboxes, and clarified the ease of matching each technique. We also compared the mapping characteristics of techniques with those of static analysis-based techniques and manually written reports and showed that the mapping characteristics differed among the techniques. Furthermore, we derived best practices for utilization on the basis of each survey. We believe that these results will lead to a better understanding of online sandboxes and to more efficient malware analysis using online sandboxes.

Keywords: MITRE ATT&CK, malware, online sandbox

## 1. Introduction

Malware plays an important role in cyber attacks, and a large amount of new malware is being discovered every day [1]. To respond to such a large amount of malware, dynamic analysis, which automatically analyzes malware, has become the de facto standard. In addition, online services with dynamic analysis functions have become widespread as online sandboxes, and these are widely use because these do not require construction of an onpremise analysis environment and can be used through a Web interface. One support for analysis is a function to map the malware behavior to each element of the MITRE ATT&CK techniques [2] (hereinafter referred to as "technique").

The technique represents the attack function of the malware, and by referring to the mapping result, we can grasp the outline of the function of the malware. This function is particularly useful for malware analysts, because it enables identifying the characteristic functions of the malware even when analyzing it manually as well as automating the analysis. Because of its usefulness, the function for mapping malware activities onto techniques has been adopted in online sandboxes. For example, since around 2018, mapping functions have been implemented in JoeSandbox [3] and Hybrid Analysis [4], which have been widely used for a long time. The same feature has been implemented in

a) shota.fujii.xh@hitachi.com

Hatching Triage [5], an online sandbox released somewhat later on. Furthermore, the technique mapping function has been introduced into some commercial sandboxes [6], [7], and is expected to become a defacto standard for sandbox functions in the future.

General guidelines for mapping to techniques are given [8]. Detection methods are described in the "Detection" section of each technique. On the other hand, there are many techniques that do not provide specific detection rules or detection thresholds, so the mapping function to techniques in the online sandbox is implementation-dependent. Therefore, the actual situation of the mapping function of ATT&CK in various sandboxes needs to be understood to carry out security operations. However, to the best of our knowledge, no quantitative survey has been conducted on the actual status of this function and the existence of differences among online sandboxes.

Therefore, in this paper, we surveyed the online sandboxes with the ATT&CK mapping function. We quantified the differences among the online sandboxes and the differences with other methods such as static analysis and manual reporting. By doing so, we clarified the analysis capability of the current technique mapping function of online sandboxes and its limitations, in order to improve the usability. On the basis of the results of the survey, we also derived best practices for using the technique mapping function.

The contributions of this study are as follows:

- We obtained 26,078 analysis reports and 328,702 technique mapping results from multiple online sandboxes and performed the first quantitative research and analysis on them.
- We analyzed the differences in mapping tendencies of techniques among online sandboxes and discovered that the map-

<sup>&</sup>lt;sup>1</sup> Yokohama Research Laboratory, Hitachi, Ltd., Yokohama, Kanagawa 244–0817, Japan

<sup>&</sup>lt;sup>2</sup> Graduate School of Natural Science and Technology, Okayama University, Okayama 700–8530, Japan

<sup>&</sup>lt;sup>3</sup> Faculty of Natural Science and Technology, Okayama University, Okayama, 700–8530, Japan

ping consistency for the same sample was low, and those for 117 out of 153 techniques were significantly different.

- We compared the mapping results for malware with those for benign files and discovered that 32 techniques had no significant differences in their mapping tendencies. Because these techniques tend to be mapped to benign files, determining if their behavior is truly malicious or not is a high priority.
- For technique mapping, we compared the results with those of static analysis-based methods and manual reports, and discovered that there were differences in the extraction characteristics of these methods. Specifically, we quantitatively revealed that an online sandbox is not good at extracting tactical techniques outside its context, such as *Reconnaissance* and *Resource Development*. However, we showed that *Initial Access*, which appears to be outside the context of the sandbox, can be partially extracted. Furthermore, we quantitatively revealed that the extractions of techniques that have a specific and mechanically defined detection method are significantly better than those of other methods.
- Based on the survey and analysis conducted during the study, we derived the best practices, such as it is recommended to compare the mapping results with the analysis results of multiple online sandboxes and extraction methods as much as possible, substitute using mapping results for each task for which they are to be used, accounting for the possibility of false positives. We also discussed the effective usage of analysis report.

### 2. Background and Research Questions

### 2.1 Online Sandbox

A sandbox is a dynamic analysis environment in which malware is executed and its behavior is observed. As mentioned earlier, the currently existing amount of malware is enormous and many efforts have been made to improve efficiency through automatic dynamic analysis using sandboxes. For example, dynamic analysis is used to automate the generation of reports [9], the creation of malware detection rules [10], [11], and the identification of malware variants by clustering [12]. The results from dynamic analysis in sandboxes are used by analysts for analyzing malware [13].

Online services with dynamic analysis functions are widely used as online sandboxes because they do not require the construction of an on-premise analysis environment and can be used through a Web interface. In addition to conventional commercial sandboxes and the open source cuckoo sandbox [14], online sandboxes such as JoeSandbox [3] and any.run [15] are shown as sandboxes used by analysts [13].

### 2.2 MITRE ATT&CK

MITRE ATT&CK [2], which stands for Adversarial Tactics, Techniques, and Common Knowledge, is a knowledge base/framework that organizes and systematizes cyber attack tactics and techniques by attack lifecycle. ATT&CK is composed of tactics, which represent the goals to be achieved by an attack, and techniques, which are the attack techniques used to achieve the goals. The use of ATT&CK has attracted much attention in recent years because of its potential for various applications, since it enables cyber attacks to be described in a common language. For example, it can be used to simplify the understanding of the overall picture of cyber attacks, to standardize and improve the comprehensiveness of attack methods and detection/countermeasure techniques, and to facilitate information exchange through a common language. Moreover, clarifying attack methods (TTPs: Tactics, Techniques, and Procedures) is an important objective in malware analysis [13], and a survey revealed that analysts use MITRE ATT&CK to organize TTPs [13], [16]. Thus, the use of ATT&CK is expected to improve the efficiency of malware analysis.

### 2.3 Problems

As mentioned in Section 2.2, while ATT&CK has been utilized in many online sandboxes, there are still many implementation-dependent aspects of associating malware behavior with ATT&CK techniques. For example, *T1071 (Application Layer Protocol)* provides a detection method to analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). However, it is difficult to uniquely define *uncommon*; thus, whether the communication is *common* or *uncommon* depends on the threshold to be set and its implementation.

There are also some techniques which are difficult to detect in the online sandbox layer. For example, *T1195* (*Supply Chain Compromise*) means that the initial intrusion was caused by a supply chain attack, but it is difficult to detect because it occurs outside the context of the online sandbox analysis.

However, these ATT&CK techniques are difficult to detect because they occur outside the context of the analysis in the online sandboxes. Because the results of the analysis are affected by these features and have the potential to negatively impact the destination of the analysis results, the actual state of the mapping function to the technique in various online sandboxes needs to be understood to carry out security operations.

### 2.4 Research Questions

On the basis of the aforementioned issues, four RQs (Research Questions) were designed and a survey was conducted.

• RQ1: Are there differences in ATT&CK mapping capabilities between online sandboxes?

As mentioned in Section 2.3, the mapping function of techniques among online sandboxes have some differences. By quantitatively testing this hypothesis, we aim to understand the actual situation of this function.

• RQ2: Are there techniques that are easy or difficult to extract in online sandboxes?

Because the technique mapping function in the online sandbox requires mechanical mapping and there are out-ofcontext attacks, some techniques can be extracted and others cannot. Therefore, we examine this item in order to improve the usability of the technique mapping function in the online sandbox.

• RQ3: Are there techniques that tend to be mapped to benign files?

Some techniques, such as the aforementioned *T1071*, require a threshold to determine whether an observed potential attack is truly an attack. Depending on the rule settings, and not only the threshold, it is possible to map ATT&CK techniques even if the behavior is benign. Such incorrect mapping may induce false positives and have negative effects on the analysis results. Thus, it is examined whether any techniques tend to be mapped to benign files, and if this is the case, we try to determine which techniques are likely to be mapped to benign files and those that are not.

• RQ4: Are there differences in characteristic between other technique detection methods?

As mentioned in Sections 2.1 and 2.2, technique mapping is effective in security operations and is not just utilized in online sandboxes. For example, there are examples of mapping functions that use static analysis or manual mapping on the basis of various observation results which are published as threat reports. Each of these mapping methods has its own potential strengths and weaknesses, and there may be differences among them. By understanding these differences and the strengths and weaknesses of each method, we hope to obtain suggestions on which method should be used depending on the situation and analysis target.

## 3. Methodology

## 3.1 Design of Survey

First, to solve RQs1–3, we collected malware analysis reports from online sandboxes and obtained the mapping results to the ATT&CK technique. To solve RQ4, we also collected static analysis-based analysis results, manually generated threat reports for comparison, and extracted the mapping results to the ATT&CK technique. We then compared the results with those mapped automatically by an online sandbox.

#### 3.2 Survey Subjects

In this study, the following online sandbox services with the capability of mapping to technique were selected for the survey.

- JoeSandbox [3]
- Hybrid Analysis [4]
- Hatching Triage [5]

We also selected three threat information sites to collect human written reports related to RQ4.

- MANDIANT [17]
- Cisco Talos [18]
- Trend Micro [19]

These sites were selected as the target of this study because they provide the results of mapping to techniques in tabular form, etc., regarding threat information.

Additionally, we utilized capa [20] (v3.0.2) to obtain the results of static analysis-based analysis. Capa is a tool that takes the binary to be analyzed as the input and outputs the results of static analysis. The output includes the mapping result to technique, and we used this mapping result to compare with the mapping result of other methods.

Note that Intezer Analyze [21], which is a kind of online sandbox, has a mapping function to technique, but the documentation

Table 1	Data overview.	
	Number of reports	Number of techniques

Information source	Number of reports	I Number of	teeninques
information source	Number of reports         Inique           13,184         143           1,012         104           11,882         38	Total	
JoeSandbox	13,184	143	284,975
Hybrid Analysis	1,012	104	13,351
Hatching Triage	11,882	38	30,376
Total of online sandboxes	26,078	167	328,702
Static analysis (VirusTotal+capa)	3,918	64	19,291
Manual report	50	180	697

states that it uses capa. Therefore, although Intezer Analyze is an online sandbox, we judged that its technique mapping function is based on static analysis and excluded it from the verification in RQ1 to RQ3.

### 3.3 Dataset

In processing the online sandbox reports, we mainly collected those from JoeSandbox. Specifically, we collected 20,435 analysis reports of malware analyzed during the period of September 24, 2021 to October 23, 2021. From these reports, we extracted 13,184 malware analysis results, i.e., reports that analyzed files instead of URLs and were judged to be "malicious", and selected these as the target of our investigation. After that, we obtained the analysis results for the same samples from Hybrid Analysis and Hatching Triage on the basis of the hash values of the 13,184 samples extracted from JoeSandbox. However, not all the analysis reports for all the samples existed in each online sandbox, and only 1,012 out of 13,184 reports existed in Hybrid Analysis and 11,882 in Hatching Triage. The total number of reports was 26,078, and the number of analysis results of the same sample in all sandboxes was 1,012. After that, techniques were extracted from each report to form a dataset. Specifically, JoeSandbox and Hatching Triage extracted techniques by analyzing the structure of the reports, and Hybrid Analysis used techniques provided in csv format.

We selected 50 cases from threat information sites that contained mapping results to the ATT&CK technique and manually extracted the list of techniques summarized at the end of sentences, etc., to form a dataset.

Furthermore, the static analysis-based results were obtained by retrieving actual samples from VirusTotal on the basis of the hash values of 13,184 malware samples obtained from JoeSandbox and analyzing each sample with capa. However, only 11,973 samples actually existed in VirusTotal and could be obtained. Because capa supports only some file formats such as PE and ELF formats, and because obfuscated specimens are excluded from the analysis, static analysis was successful and techniques were extracted as datasets for 3,918 samples. These data are summarized in **Table 1**.

Here, MITRE ATT&CK is basically updated every six months, and the names of the techniques may change or be consolidated. To reduce the impact of these version differences on the analysis, we used the datasheet [22], which summarizes the correspondence of each technique with its predecessors, to assign names to the MITRE ATT&CK Technique v9. For example, the technique ID and its name are updated from *T1045 (Software Packing)* to *T1027.002 (Obfuscated Files or Information: Software Packing)*. The reason for the unification to v9 is that as of December 2021, the relevant datasheet is compatible with v9.

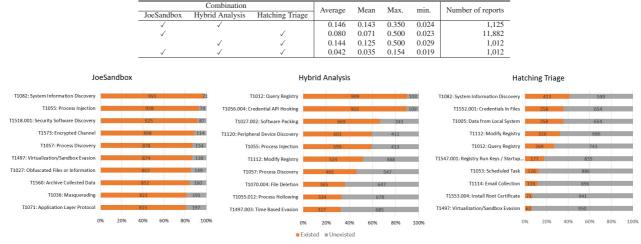


 Table 2
 Similarity of MITRE ATT&CK Technique mapping results between sandboxes by Eq. (1).

Fig. 1 Top 10 MITRE ATT&CK Technique for each sandbox.

 Table 3
 Analysis environment for each sandbox.

Analysis Environment	Online sandbox							
Analysis Environment	JoeSandbox	Hybrid Analysis	Hatching Triage					
Windows 7 (32-bit)	0	400	0					
Windows 7 (64-bit)	86	612	3					
Windows 10 (64-bit)	926	0	1,007					
Windows 11 (64-bit)	0	0	2					
Total	1,012	1,012	1,012					

## 4. Results

#### 4.1 Overview of Survey

In this section, we analyze the mapping results to ATT&CK collected from each online sandbox to derive the actual situation and best practices for its use.

First, we compare the mapping results of each sandbox to the same sample and resolve RQ1. Second, RQ2 is solved by measuring the coverage of all mapping results collected for all techniques. We also solve RQ3 by comparing the results of technique mappings to benign files with those to malware, and deriving the technique that tends to be mapped to both. Finally, we collect static analysis-based analysis results and manually written threat reports, and compare the ATT&CK mapping results performed by each of them with the results automatically mapped by the online sandbox to solve RQ4.

To solve the RQs, we used a statistical test method. The Yates' chi-square test was used as the test method because there were a few items with a small number of occurrences in all the test targets. The significance level was set at 0.05.

## 4.2 RQ1: Are There Differences in ATT&CK Mapping Capabilities between Online Sandboxes?

To answer this RQ, we utilized the reports that existed for the same sample in each sandbox. To measure the degree of consistency of the techniques in each sandbox, the set similarity of the techniques of each sample was calculated using a formula inspired by the Jaccard coefficient in Eq. (1) below.

$$Sim(S_1, S_2, \dots, S_n) = \frac{|S_1 \cap S_2 \dots \cap S_n|}{|S_1 \cup S_2 \dots \cup S_n|}$$
(1)

The calculation results are shown in **Table 2**. The analysis environment for each analysis sandbox is shown in **Table 3**. Each

environment includes a web browser, PDF viewer, Office software, etc. The mean values of the Jaccard coefficients were 0.146, 0.080, and 0.144 between the two sandboxes, and 0.042 between the three sandboxes, indicating a low degree of consistency. The top 10 techniques with the highest number among 1,012 cases in common for all sandboxes are shown in **Fig. 1**. Although all results are mapped to the same samples, the top 10 techniques and their percentages are all different. For example, *T1082 (System Information Discovery)* in JoeSandbox is mapped to 991 out of 1,012 specimens, which is almost all samples, while Hatching Triage is mapped to 413 samples, although these are in the same position. It can be confirmed that Hybrid Analysis is not even in the top 10.

A crosstabulation table was created for each technique, and a chi-square test was conducted to verify whether there was a significant difference between sandboxes for the 153 techniques detected in any of the sandboxes. As a result, we found that 36 techniques were not significantly different from each other (i.e., similar in all sandboxes), while 117 techniques were significantly different from each other. The results of the test for all 153 techniques are shown in Table A·1 in Appendix A.1. Table 4 shows the number of observations in each sandbox, the p-value of the chi-square test, and the presence or absence of a significant difference when the significance level is set to 0.05 for each of the 1,012 samples in all sandboxes. The table shows that there is a significant difference in the number of observations among the top 10 techniques in each sandbox. This indicates that there are differences in the ATT&CK mapping functions of the sandboxes surveyed in this study, and that there are techniques that are suitable for extraction.

In the above comparison, the v8 and earlier techniques were renamed as the v9 techniques as described in Section 3.3. **Table 5** shows the v8 and earlier techniques used in each sandbox extracted during this naming process. First, in the JoeSandbox, all techniques except *T1064* (*Scripting*) were v9 as far as we could confirm. Although *T1064* is deprecated, it is still available on the ATT&CK page as of December 2021, which means that JoeSandbox's technique mapping function is highly maintainable. On the other hand, there are 21 and 15 obsolete techniques remaining

TID	Technique	JoeSa	ndbox	Hybric	l Analysis	Hatch	ing Triage	p-value	Statistical
IID	Technique	exist	unexist	exist	unexist	exist	unexist	p-value	significance
T1082	System Information Discovery	991	21	207	805	413	599	2.29E-285	$\checkmark$
T1055	Process Injection	938	74	598	414	0	1,012	0	$\checkmark$
T1518.001	Security Software Discovery	925	87	53	959	3	1,009	0	$\checkmark$
T1573	Encrypted Channel	898	114	223	789	0	1,012	0	$\checkmark$
T1057	Process Discovery	878	134	465	547	0	1,012	0	$\checkmark$
T1497	Virtualization/Sandbox Evasion	874	138	241	771	62	950	0	$\checkmark$
T1027	Obfuscated Files or Information	863	149	7	1,005	0	1,012	0	$\checkmark$
T1560	Archive Collected Data	852	160	3	1,009	0	1,012	0	√ √
T1036	Masquerading	821	191	89	923	0	1,012	0	$\checkmark$
T1071	Application Layer Protocol	815	197	0	1,012	0	1,012	0	$\checkmark$
T1012	Query Registry	289	723	909	103	269	743	2.94E-228	√ -
T1056.004	Credential API Hooking	57	955	902	110	0	1,012	0	$\checkmark$
T1027.002	Software Packing	769	243	669	343	0	1,012	1.18E-301	$\checkmark$
T1120	Peripheral Device Discovery	9	1,003	601	411	38	974	1.95E-285	√ √
T1112	Modify Registry	39	973	524	488	326	686	5.78E-124	$\checkmark$
T1070.004	File Deletion	133	879	365	647	9	1,003	1.81E-101	$\checkmark$
T1055.012	Process Hollowing	0	1,012	333	679	0	1,012	3.66E-163	√ √
T1497.003	Time Based Evasion	0	1,012	326	686	0	1,012	2.45E-159	$\checkmark$
T1552.001	Credentials In Files	58	954	2	1,010	358	654	3.48E-133	$\checkmark$
T1005	Data from Local System	453	559	84	928	358	654	1.66E-76	√ √
T1547.001	Registry Run Keys / Startup Folder	208	804	162	850	177	835	0.025182647	$\checkmark$
T1053	Scheduled Task/Job	183	829	115	897	126	886	1.74E-05	√
T1114	Email Collection	322	690	122	890	116	896	6.13E-40	√ -
T1553.004	Install Root Certificate	2	1,010	0	1,012	71	941	1.29E-30	$\checkmark$

Table 4	Number of observations and presence of significant differences among sandboxes for each
	MITRE ATT&CK Technique (top 10 observations for each sandbox).

 Table 5
 Usage of the deprecated MITRE ATT&CK Technique per sandbox.

#	Deprecated TID	Deprecated technique	Updated TID	Updated technique	JoeSandbox	Hybrid Analysis	Hatching Triage
1	T1215	Kernel Modules and Extensions	T1547.006	Kernel Modules and Extensions		$\checkmark$	
2	T1179	Hooking	T1056.004	Credential API Hooking		$\checkmark$	
3	T1168	Local Job Scheduling	T1053	Scheduled Task/Job		$\checkmark$	
4	T1158	Hidden Files and Directories	T1564.001	Hidden Files and Directories			$\checkmark$
5	T1130	Install Root Certificate	T1553.004	Install Root Certificate			$\checkmark$
6	T1116	Code Signing	T1553.002	Code Signing		$\checkmark$	
7	T1107	File Deletion	T1070.004	File Deletion		$\checkmark$	$\checkmark$
8	T1094	Custom Command and Control Protocol	T1095	NonApplication Layer Protocol		$\checkmark$	
9	T1089	Disabling Security Tools	T1562.001	Disable or Modify Tools		$\checkmark$	$\checkmark$
10	T1088	Bypass User Account Control	T1548.002	Bypass User Access Control		$\checkmark$	$\checkmark$
11	T1086	PowerShell	T1059.001	PowerShell		$\checkmark$	
12	T1085	Rundll32	T1218.011	Rundl132		$\checkmark$	
13	T1081	Credentials in Files	T1552.001	Credentials In Files			$\checkmark$
14	T1076	Remote Desktop Protocol	T1021.001	Remote Desktop Protocol		$\checkmark$	$\checkmark$
15	T1067	Bootkit	T1542.003	Bootkit			$\checkmark$
16	T1065	Uncommonly Used Port	T1571	NonStandard Port		$\checkmark$	
17	T1064	Scripting	N/A	N/A	1	$\checkmark$	$\checkmark$
18	T1063	Security Software Discovery	T1518.001	Security Software Discovery		$\checkmark$	$\checkmark$
19	T1060	Registry Run Keys/Startup Folder	T1547.001	Registry Run Keys/Startup Folder		$\checkmark$	$\checkmark$
20	T1050	New Service	T1543.003	Windows Service		$\checkmark$	$\checkmark$
21	T1045	Software Packing	T1027.002	Software Packing		$\checkmark$	
22	T1044	File System Permissions Weakness	T1574.010	Services File Permissions Weakness		$\checkmark$	
23	T1043	Commonly Used Port	N/A	N/A		$\checkmark$	
24	T1042	Change Default File Association	T1546.001	Change Default File Association			$\checkmark$
25	T1035	Service Execution	T1569.002	Service Execution		$\checkmark$	
26	T1031	Modify Existing Service	T1543.003	Windows Service			$\checkmark$
27	T1004	Winlogon Helper DLL	T1547.004	Winlogon Helper DLL			$\checkmark$
28	T1002	Data Compressed	T1560	Archive Collected Data		$\checkmark$	
Tota	1	*			1	21	15

in Hybrid Analysis and Hatching Triage, respectively. These are not necessarily undesirable because they are useful in terms of consistency with the mapping results before the revision in the same sandbox. However, if the mapping results are to be compared with those of other sandboxes or other methods, or if the mapping results are to be used in reports, etc., it is assumed that adverse effects due to the difference in versions may occur, and therefore, it is necessary to perform name matching, etc.

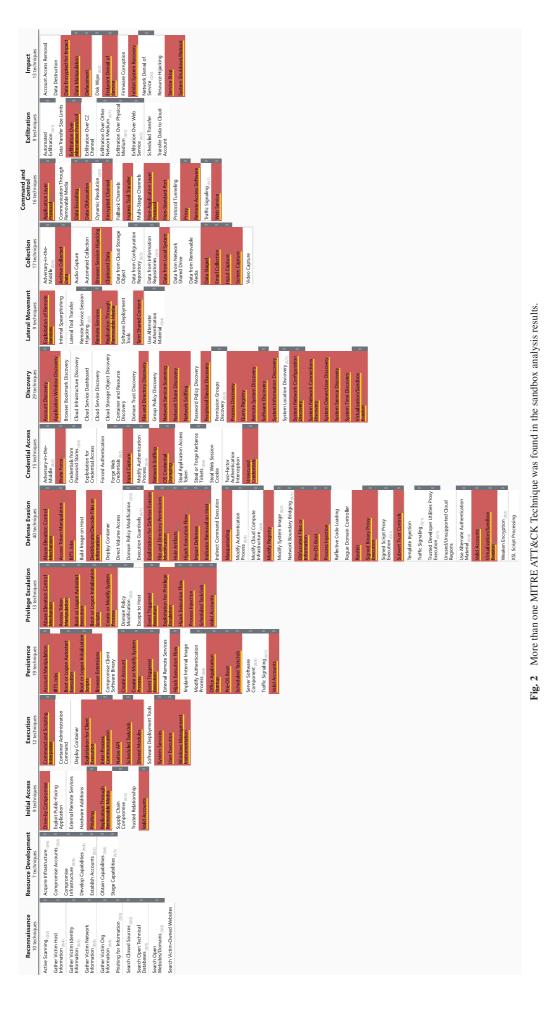
In conclusion, the ATT&CK mapping function can be said to differ among the online sandboxes.

## 4.3 RQ2: Are There Techniques that are Easy or Difficult to extract in Online Sandboxes?

To answer this RQ, we utilized 26,078 reports from all sandboxes. First, we extracted the techniques from all the reports and performed a chi-square test to confirm that there was a significant difference between the extracted techniques. Then we calculated the number of techniques that existed in more than one case and those that did not. **Figure 2** shows a visualization of the techniques that existed in more than one case using ATT&CK Navigator [23] only at the granularity of techniques (not including sub-techniques). Among the total of 568 techniques, only 175 (29.40%) were found to exist, while the remaining 70.60% did not. Particularly noteworthy were *Reconnaissance* and *Resource Development*, which are the preliminary stages of an attack, both of which had zero cases. These are techniques applied before the malware is executed and it was confirmed that it is difficult to extract techniques with the online sandbox function that extracts techniques from the analysis log after the malware is basically executed.

**Table 6** shows the values aggregated for each tactic. Excluding *Reconnaissance* and *Resource Development*, the coverage rates for *Exfiltration* (11.76%) and *Impact* (23.08%) are low.

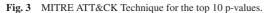
This may be partly because these techniques are related to data removal and system destruction, which are outside the context of online sandboxes and include a relatively high level of abstrac-



Electronic Preprint for Journal of Information Processing Vol.30

Tactic	Number of existing techniques To	otal number of techniques	ratio (%)
Reconnaissance	0	41	0.00
Resource Development	0	32	0.00
Initial Access	4	15	26.67
Execution	15	44	34.09
Persistence	28	83	33.73
Privilege Escalation	25	69	36.23
Defense Evasion	42	121	34.71
Discovery	18	35	51.43
Lateral Movement	7	25	28.00
Collection	7	27	25.93
Command and Control	13	33	39.39
Exfiltration	2	17	11.76
Impact	6	26	23.08
Total	167	568	29.40
malicious		benign	
malicious	144 T1574.010: Services File Permissions Weakness [0		_
	144 T1574.010: Services File Permissions Weakness ( 997 T1068: Exploitation for Privilege Escalation (0.87)	.93] 17 1516	
12971		1.93] 17 1516 68 1465	
12971 12518	597 T1068: Exploitation for Privilege Escalation [0.87]	1.93] 17 1516 68 1465	
12971 12518 13006	<ul> <li>597 T1068: Exploitation for Privilege Escalation [0.87]</li> <li>109 T1055.011: Extra Window Memory Injection [0.22]</li> </ul>	193] 17 1516 68 1465 2] 18 1515 194 1339	
12971 12518 13006 11622	537         T1068: Exploitation for Privilege Escalation [0.87]           109         T1055.011: Extra Window Memory Injection [0.22]           1283         T1574.002: DLL Side-Loading [0.15]	193] 17 1516 68 1465 2] 18 1515 194 1339	
12971 12518 13006 11622 12927	<ol> <li>T1088: Exploitation for Privilege Escalation (0.87)</li> <li>T1055.011: Extra Window Memory Injection (0.22)</li> <li>T1574.002: DLL Side-Loading (0.15)</li> <li>T18571421: System Network Connections Discovery (0.15)</li> </ol>	193] 17 1516 68 1465 18 1515 194 1339 80] 18 1520	
12971 12518 13006 11622 12927 12927	39         T1068: Exploitation for Privilege Exabition (0.87)           19         T1055.011: Extra Window Memory Injection (0.22)           100         T1574.002: DLL Side Loading (0.15)           18         T14274.22: System Network Connections Discovery (0.06)           19         T1577. Network Information Discovery (0.06)	193] 10 1516 10 1465 10 1515 10 1339 10 1339 13 1520	395
12971 12518 1006 11622 12927 12927 12929 11939	39         T1068: Exploritation for Privilege Exalation (0.27)           189         T1055.011: Estra Window Memory Injection (0.22)           193         T157.4002: 0LL Side Loading (0.15)           188         T1421: System Network Connections Discovery (0.19)           195         T15729: Network Information Discovery (0.04)           19         T1529: System Network Information Discovery (0.04)	193] 10 1516 10 1465 10 1515 10 1339 10 1339 13 1520	395

 Table 6
 Number and percentage of each MITRE ATT&CK Tactic present.



tion. Note that although *Initial Access* appears to be undetectable because it is intuitively outside the context of the online sandbox, it was partially detected (4/15). We confirmed that *Initial Access* was associated with, for example, a PDF file sample. For *Drive-by Compromise* among *Initial Access*, the URL included in the PDF file was the starting point of *Drive-by Compromise*, and there were several cases wherein the infection started from this point. The online sandbox identifies it by finding iframes.

From these results, we can confirm that in current online sandboxes, there are differences in the extraction tendencies for each technique and tactic. This suggests that some techniques are relatively easy to extract, and those that are currently extractable account for most of them. Furthermore, it infers that some techniques are potentially difficult to extract.

## 4.4 RQ3: Are There Techniques that Tend to be Mapped to Benign Files?

As mentioned in Section 3.3, the reports obtained from Joe-Sandbox include non-malicious files. Therefore, for this RQ, we utilized the reports obtained from JoeSandbox for benign files and for malware. Specifically, we compared 1,533 reports labelled as "clean" with 13,184 reports on malware. For each technique, we tested whether there was a significant difference between benign files and malware, and extracted them without a significant difference.

As a result, it was discovered that 32 techniques were not significantly different. The butterfly chart of the techniques with high p-values is shown in **Fig. 3**. For design reasons, techniques with less than 100 occurrences are omitted from the figure, and the values in square brackets denote the p-values. Figure 3 infers that all the techniques are present in a similar percentage for both benign files and malware, and it should be verified whether these techniques are truly related to malicious activity. The butterfly charts of the techniques with low p-values are shown in **Fig. 4**, wherein it is indicated that these techniques have high true positives. The number of observations and test results for all the techniques are shown in Table A·2 presented in Appendix A.1.



Fig. 4 MITRE ATT&CK Technique for the lower 10 p-values.

Techniques such as T1027.002 Software Packing, T1018 Remote Service Discovery, and T1003 OS Credential Discovery, which can be expressed by the binary values of "executed" or "not executed" and are not easily found in benign files, tend to have high true positives. On the other hand, behaviors such as T1447 Delete Device Data and T1426 Process Injection, which are easily performed even in benign files and can be benign or malicious depending on the context, are difficult to definitively distinguish by means of rules and tend to cause false positives.

In summary, some techniques are prone to be assigned not only to malwares but also to benign files.

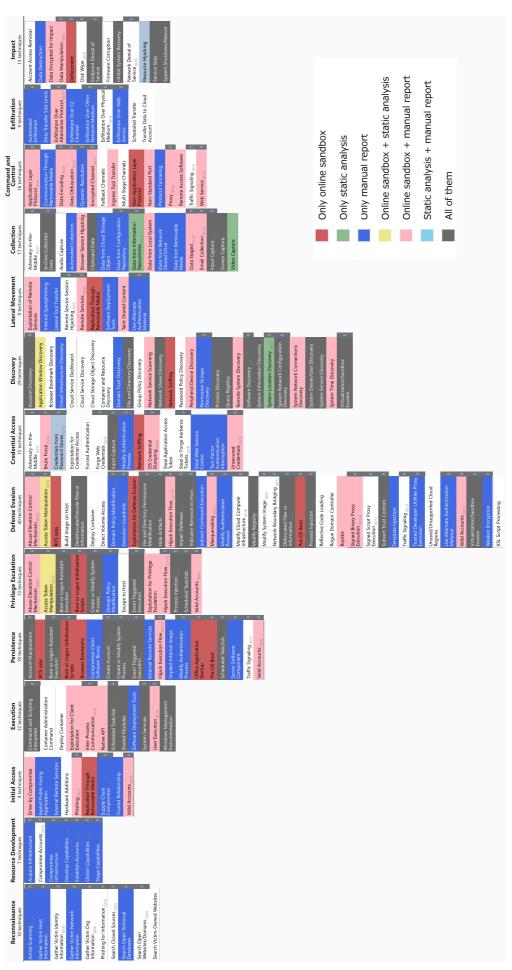
# 4.5 RQ4: Are There Differences in Characteristic between Other Technique Detection Methods?

To answer this RQ, we utilized 26,078 reports from all online sandboxes, 50 manual reports, and 3,918 static analysis results extracted by capa. In all of the reports, we counted the number of techniques that were found only in each method and the techniques that were found in multiple methods. The results of this analysis are shown in **Fig. 5** and **Table 7**.

The number of techniques confirmed by all the methods was 38, which is only 18.10% of the total techniques confirmed. On the other hand, some techniques were confirmed only by specific methods. Techniques of 54.29% in total were confirmed; 3 (1.43%) by static analysis only, 25 (11.91%) by online sandbox and 86 (40.95%) by manual report. First, it can be seen that the manual report covers techniques that are difficult to extract with the online sandbox and static analysis, focusing on the techniques of Reconnaissance and Resource Development. Furthermore, *T1040* (*Network Sniffing*), *T1091* (*Replication Through Removable Media*), *T1137* (*Office Application Startup*), and *T1197* (*BITS Jobs*) etc. were confirmed only in the online sandbox.

The common features of these techniques are that the detection methods are specifically described in the "Detection" section of each technique, such as executing a specific API, executing a specific command, modifying a specific registry, etc., and that these can be detected mechanically. These behaviors are likely to be manifested by actually executing the malware, and it is inferred that they are detected in online sandboxes. Although these features are difficult to detect by static analysis, these can potentially be detected manually. However, we believe that this result was obtained because it is more likely to be observed in the online sandbox which can be executed mechanically and the number of observations can be scaled.

To verify the RQ4 quantitatively, a chi-square test was conducted on the techniques confirmed by multiple methods, between two methods for those confirmed by two methods, and





TID	Technique	JoeSand			Analysis		ng Triage	Combination	p-value	Statistical
T1497	*	exist	unexist	exist	unexist	exist	unexist		0	significance
Г1497 Г1497	Virtualization/Sandbox Evasion	9,577	16,501 16,501	2	3,916 3,916	4	46 46	(all) sandbox+static	5.99E-06	1
Г 1497 Г 1497	Virtualization/Sandbox Evasion Virtualization/Sandbox Evasion	9,577 9,577	16,501	22	3,916	4	40 46	(all) sandbox+report (all) static+report	4.36E-36	
T1027.002	Software Packing	8,649	17,429	4	3,910	2	40	(all) sandbox+static	4.50E-50	$\checkmark$
Г1027.002	Software Packing	8,649	17,429	4	3,914	2	48	(all) sandbox+report	0.000175584	× 1
T1027.002	Software Packing	8,649	17,429	4	3,914	2	48	(all) static+report	1.82E-07	l v
T1027.002	Obfuscated Files or Information	9,530	16,548	1,412	2,506	15	35	(all) sandbox+static	0.551849477	-
T1027	Obfuscated Files or Information	9,530	16,548	1,412	2,500	15	35	(all) sandbox+static	0.551049477	- -
T1027	Obfuscated Files or Information	9,530	16,548	1,412	2,506	15	35	(all) static+report	0.46179638	-
T1518.001	Security Software Discovery	11,428	14,650	3	3,915	2	48	(all) sandbox+static	0.40175050	
T1518.001	Security Software Discovery	11,428	14,650	3	3,915	2	48	(all) sandbox+report	1.07E-07	l v
T1518.001	Security Software Discovery	11,428	14,650	3	3,915	2	48	(all) static+report	8.17E-09	j j
T1057	Process Discovery	9,569	16,509	99	3,819	7	43	(all) sandbox+static	0.172 09	$\checkmark$
T1057	Process Discovery	9,569	16,509	99	3.819	7	43	(all) sandbox+report	8.45E-16	l v
T1057	Process Discovery	9,569	16,509	99	3.819	7	43	(all) static+report	5.16E-06	l v
T1082	System Information Discovery	15,879	10,309	2,416	1.502	11	39	(all) sandbox+static	0.363771896	-
T1082	System Information Discovery	15,879	10,199	2,416	1,502	11	39	(all) sandbox+report	3.48E-300	1
T1082	System Information Discovery	15,879	10,199	2,416	1,502	11	39	(all) static+report	2.51E-08	ý 1
T1569.002	Service Execution	858	25,220	125	3,793	5	45	(all) sandbox+static	0.78040016	-
T1569.002	Service Execution	858	25,220	125	3,793	5	45	(all) sandbox+report	0.78040010	-
T1569.002	Service Execution	858	25,220	125	3,793	5	45	(all) static+report	0.022133283	l v
T1083	File and Directory Discovery	6,818	19,260	1,748	2,170	12	38	(all) sandbox+static	1.11E-125	
T1083	File and Directory Discovery	6,818	19,260	1,748	2,170	12	38	(all) sandbox+static	0	↓ <i>↓</i>
Г1083 Г1083	File and Directory Discovery	6.818	19,260	1,748	2,170	12	38	(all) static+report	0.005565762	l v
T1012	Query Registry	7,460	19,200	724	3,194	4	46	(all) sandbox+static	4.45E-40	 ✓
Г1012 Г1012	Query Registry	7,460	18,618	724	3,194	4	40	(all) sandbox+report	4.451-40	×
T1012	Query Registry	7,460	18,618	724	3,194	4	46	(all) static+report	0.085716776	, v
T1012	System Owner/User Discovery	2.845	23.233	201	3,174	5	45	(all) sandbox+static	8.13E-29	-
T1033	System Owner/User Discovery	2,845	23,233	201	3,717	5	45	(all) sandbox+static	4.35E-260	ý 1
T1033	System Owner/User Discovery	2,845	23,233	201	3,717	5	45	(all) static+report	0.221871132	
T1115	Clipboard Data	1,955	24,123	238	3.680	1	49	(all) sandbox+static	0.001601174	-
T1115	Clipboard Data	1,955	24,123	238	3,680	1	49	(all) sandbox+report	0.001001174	ý 1
T1115	Clipboard Data	1,955	24,123	238	3,680	1	49	(all) static+report	0.365872328	, v
T1059	Command and Scripting Interpreter	3,122	22,956	1,801	2,117	11	39	(all) sandbox+static	0.505072520	
T1059	Command and Scripting Interpreter	3,122	22,956	1.801	2,117	11	39	(all) sandbox+report	0	l v
T1059	Command and Scripting Interpreter	3,122	22,956	1,801	2,117	11	39	(all) static+report	0.001203964	× 1
T1113	Screen Capture	664	25,414	403	3,515	3	47	(all) sandbox+static	7.12E-131	 √
T1113	Screen Capture	664	25,414	403	3,515	3	47	(all) sandbox+report	0	× 1
T1113	Screen Capture	664	25,414	403	3,515	3	47	(all) static+report	0.447946249	× ·
T1222	File and Directory Permissions Modification	628	25,450	237	3,681	1	49	(all) sandbox+static	1.17E-36	-
T1222 T1222	File and Directory Permissions Modification	628	25,450	237	3,681	1	49	(all) sandbox+static (all) sandbox+report	1.1/E-30	↓ ✓
T1222	File and Directory Permissions Modification	628	25,450	237	3.681	1	49	(all) static+report	0.368942641	×
Г1222 Г1129	Shared Modules	920	25,450	3.392	526	1	49	(all) sandbox+static	0.308942041	-
Г1129 Г1129	Shared Modules	920	25,158	3,392	526	1	49	(all) sandbox+static	0	l v
T1129	Shared Modules	920	25,158	3,392	526	1	49	(all) static+report	1.84E-62	×
T1564.003		26	26.052		3.402	0	50			-
T11364.003 T1135	Hidden Window	26	26,052	516 21	3,402	3	47	sandbox+static (all) sandbox+static	0 6.00E-12	∕
T1135 T1135	Network Share Discovery	21	26,057	21	3,897	3	47		6.00E-12 0	<b>√</b>
T1135 T1135	Network Share Discovery Network Share Discovery	21	26,057	21	3,897	3	47	(all) sandbox+report (all) static+report	5.49E-05	
T1489		21	26,057	21	3,897	7	47		1.81E-15	
	Service Stop					7		(all) sandbox+static		✓ _
Г1489 Г1489	Service Stop Service Stop	22 22	26,056 26,056	25 25	3,893 3,893	7	43 43	(all) sandbox+report	0 2.97E-22	
Г 1489 Г 1402							43	(all) static+report	2.9/E-22 0	
	Broadcast Receivers	1	26,077	0	3,918	5		sandbox+report		✓ ✓
T1566.001	Spearphishing Attachment	3	26,075	0	3,918	4	46	sandbox+report	8.54E-200	√
T1560.002	Archive via Library	3	26,075	9	3,909	1	49	(all) sandbox+static	2.85E-09	✓
F1560.002	Archive via Library	3	26,075	9	3,909	1	49	(all) sandbox+report	0	√
T1560.002	Archive via Library	3	26,075	9	3,909	1	49	(all) static+report	0.288413195	
T1056.001	Keylogging	4	26,074	532	3,386	1	49	(all) sandbox+static	0	1
T1056.001	Keylogging	4	26,074	532	3,386	1	49	(all) sandbox+report	0	✓
Г1056.001	Keylogging	4	26,074	532	3,386	1	49	(all) static+report	0.029476232	√

Table 8	Technique observed in multiple methods and presence/absence of significant differences between
	methods (excerpt).

 Table 7
 Extraction trend of MITRE ATT&CK Technique by each method.

Combination			Number	Ratio (%)
Online sandbox	Static analysis	Manual report	Number	Katio (70)
$\checkmark$			25	11.91
$\checkmark$	$\checkmark$		2	0.95
$\checkmark$		$\checkmark$	54	25.71
	$\checkmark$		3	1.43
	$\checkmark$	$\checkmark$	2	0.95
		$\checkmark$	86	40.95
$\checkmark$	$\checkmark$	$\checkmark$	38	18.10
Total			210	100.00

between all combinations of methods ( $_{3}C_{2} = 3$  methods) for those confirmed by three methods, to verify the significant difference between methods for each technique. As a result, out of 193 combinations tested, 141 combinations had significant differences. Of these, a selection of techniques including those with significant differences is shown in **Table 8**. For example, although *T1566.001* (*Spearphishing Attachment*) was found in both the online sandbox and the manual report, it is basically outside the context of the online sandbox, so intuitively it is easier to detect in the manual report. In fact, it was found in a small number of cases (3 out of 26,075) in the online sandbox, while it was found in 4 out of 46 cases in the manual report. The results of both tests are "significantly different", indicating that the detection is significant in the manual reports, as assumed.

Therefore, it can be said that the tendency to extract techniques differs depending on the extraction method. The details of the test results can be found in Table A $\cdot$ 3 in Appendix A.1.

### 5. Discussion

## 5.1 Best Practice

As shown in RQ1, there are differences in the ATT&CK mapping function among online sandboxes. RQ4 shows that differences can also occur depending on the extraction method. Therefore, it is recommended to compare the analysis and mapping results of multiple online sandboxes and extraction methods as much as possible and use these in a way so that these comple-

### ment each other.

Moreover, as described in RQs2-4, some techniques are difficult to extract mechanically via the online sandbox and conversely, some techniques are prone to be false positives. Particularly, as shown in RQ3, some ATT&CK techniques tend to be mapped to benign files. These ATT&CK techniques are defined as techniques used in attacks and should not be mapped to the behavior of benign files. As a side effect of the emphasis on coverage, the mapping of ATT&CK techniques with benign files can result in false positives and should be handled cautiously. By understanding the characteristics of each technique, those that are prone to false positives can be more effectively used, for example, by manually confirming their authenticity, even if they are automatically mapped. It would also be effective to change the way the technique mapping function is used based on the task to be performed. For example, if a researcher wants to comprehend the bigger picture of an attack, completely discarding false positives may have negative effects such as making it difficult to understand the flow of the attack. In such cases, false positives can be allowed to some extent, and such techniques can be presented with a message stating that the technique has a high number of false positives, or the log of the technique mapping can be presented as well, and the final judgment can be left to the analyst. In contrast, for a task that requires true positives such as creating detection rules along with mapping results, techniques with high false positives can be rejected.

However, collecting several reports for a single sample is not always desirable from the viewpoint of efficiency. As mentioned in Section 4.2, there are differences in the ATT&CK mapping function; hence, it is considered that efficient analysis can be achieved by collecting at least two reports, manually verifying the authenticity of only those techniques that can be easily mapped to benign files, focusing only on the more important techniques [24] among the extracted ones, and so on.

As shown in the section on RQ1, there are cases wherein the mapping is done on an older version of the technique. This may be because the mapping was done before technique revision, or the mapping function does not support the latest techniques. However, it is crucial to identify whether the data are mapped to the latest version of the technique and read the data accordingly.

### 5.2 Limitation

This study has some limitations. First, the reports collected in this study are primarily those analyzed by JoeSandbox from September 24 to October 23, 2021 and do not include all malware analysis results. Next, there is evasive malware that detects the analysis environment and then avoids malicious behavior. Therefore, even if the samples were identical, these do not always behave maliciously in all sandboxes. Even if these exhibit malicious behavior it is not always identical. In fact, as presented in Table 3, different versions of the OS were used among the sandboxes in some cases and this possibly affected the analysis results. However, it was confirmed that in several cases, the samples common to all sandboxes were judged as "malicious" or assigned a high maliciousness level by the judgment mechanism of each sandbox. If evasive malware is mostly found in a particular sandbox, the number of "malicious" samples in that sandbox should be high, whereas the number of "benign" samples in another sandbox should be high. Therefore, it is unlikely that the ATT&CK mapping function would have been different in one sandbox, but not in another owing to detection of the analysis environment or other accidental factors. However, it is possible that there are some samples that behave maliciously in all sandboxes but change their behavior significantly to confuse the analyst. A limitation of this study is that the presence of such samples was not considered.

In the RQ3 survey, we found that *Exfiltration* and *Impact*, which are the latter stages of malware behavior, were less common. There is malware that bypasses the sandbox and malware that finishes its attack when the C2 server is closed. One reason for this may be that the more advanced the tactics are, the more difficult it is for the malware to perform the technique that corresponds to the tactics. This is a factor that depends only on the detection evasion function of malware, not on the ease of extracting the technique and may appear as noise in this study. Additionally, the collection of benign files is difficult except for Joe-Sandbox, and as a result, the verification of RQ3 is limited to the JoeSandbox results only.

Manual reports may also contain larger sample errors, since the absolute number of such reports is smaller than that of the online sandbox analysis reports. There are reports that there are omissions in the technique mentioned in the report [25], which may also have an impact. In addition, the granularity of the targets of online sandboxes and static analysis is different from that of publicly available manually written reports, as most of them target entire attack campaigns or threats, while online sandboxes and static analysis target a single malware sample. This difference in the granularity of the target may have affected the results of the survey described in this paper.

Because the number of online sandboxes that we covered in this study was three, the results described in this paper may not fully include the nature of online sandboxes as a whole. For example, SandPrint [26], which investigated the fingerprinting potential of online sandboxes, covered 20 services. One reason for the small number of surveyed services is that not all sandboxes are equipped with the technique mapping function, which is the subject of this paper's survey.

In this paper, we have tried to keep the number of survey targets as large as possible in order to control each limitation.

#### 5.3 Research Ethics

In this study, when collecting analysis reports of malware, a certain interval was set for each access when information was obtained from the same site. By applying this measure, the load on each service was reduced, and the survey was conducted.

### 6. Related Work

As mentioned in Section 2.2, various online sandboxes have implemented functions for mapping malware to technique. In this paper, we investigate the features of this function and derive the best practices for using it, with the aim of making it more efficient and effective. Some studies have attempted to analyze technique. Reference [27] uses hierarchical clustering to derive correlations between APTs and software reported in ATT&CK. Reference [28] proposes a method and tool to analyze the correlation between MITRE ATT&CK, CAPEC, CWE and CVE. On the basis of the findings of this paper, it can be inferred that these methods can be used more effectively by improving the true positives of the techniques that are the inputs to each method.

Although the present study focused on a technique related functions of online sandboxes, other studies have been conducted from other perspectives. For example, the developers of Sand-Print [26] investigated and demonstrated whether various online sandboxes can be detected by fingerprinting technology. Another study investigated and verified whether online sandboxes can be detected [29], [30]. On the other hand, to the best of our knowledge, no research has been conducted on the mapping function of ATT&CK in online sandboxes as described in this paper. We believe that the combination of these research results and this survey will lead to online sandboxes being better understood and more effectively used.

### 7. Conclusion

In this study we investigate the function for mapping malware analysis results to the relevant ATT&CK techniques in three online sandboxes.

Analysis of survey results reveals that the mapping characteristics differ among the sandboxes. We also compared the results with those of static analysis-based techniques and manually written reports, and showed that there were differences in the mapping tendencies among the techniques. Specifically, we quantitatively revealed that the online sandbox is not good at extracting tactical techniques outside the context of the sandbox. On the other hand, the online sandbox is significantly better than other methods at extracting techniques where the detection method is specific and mechanically defined.

We can therefore infer that malware analysis can be performed more efficiently and reliably by being aware of these factors when using the online sandbox. For example, best practices may include it is desirable to compare the mapping results with the analysis results of multiple online sandboxes and extraction methods as much as possible, and to use them in a way that complements each other, or to use the mapping results in different ways for different tasks, considering the possibility of false positives.

Future work includes expanding the scope of the survey and investigating more efficient ways to use the technique mapping function on the basis of the survey results.

#### References

- [1] AV-TEST: Malware Statistics & Trends Report, available from (https://www.av-test.org/en/statistics/malware/) (accessed 2022-02-24).
- [2] MITRE: ATT&CK, available from (https://attack.mitre.org/) (accessed 2022-02-24).
- [3] JoeSandbox: Automated Malware Analysis Joe Sandbox Cloud Basic, available from (https://www.joesandbox.com/) (accessed 2022-

All named products and descriptions are trademarks and/or registered trademarks of the respective manufacturers and are accepted as protected.

02-24).

- [4] Hybrid Analysis: Free Automated Malware Analysis Service powered by Falcon Sandbox, available from (https://www.hybridanalysis.com/) (accessed 2022-02-24).
- [5] Hatching Triage: Hatching Triage Sandbox for High-Volume Automated Malware Analysis, available from (https://tria.ge/) (accessed 2022-02-24).
- [6] McAfee: McAfee Advanced Threat Defense Leverages MITRE ATT&CK Framework, available from (https://www.mcafee.com/ enterprise/en-us/assets/solution-briefs/sb-atd-leverages-mitre.pdf) (accessed 2022-02-24).
- Trend Micro: TREND MICRO VISION ONE, available from 
   (https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-ca/ brand/trend-micro/trendmicro-vision-one-solution-brief-aoda-v2.pdf) (accessed 2022-02-24).
- CISA: Best Practices for MITRE ATT&CK Mapping, available from (https://www.cisa.gov/uscert/sites/default/files/publications/ Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf (accessed 2022-02-24).
- [9] Sun, B. et al.: Automatically Generating Malware Analysis Reports Using Sandbox Logs, *IEICE Trans. Information and Systems*, Vol.E101.D, No.11, pp.2622–2632 (2018).
- [10] Paleari, R. et al.: Automatic Generation of Remediation Procedures for Malware Infections, *The 19th USENIX Conference on Security* (SEC '10) (2010).
- [11] Kirat, D. et al.: MalGene: Automatic Extraction of Malware Analysis Evasion Signature, *The 2015 ACM SIGSAC Conference on Computer* and Communications Security (CCS '15), pp.768–780 (2015).
- [12] Rieck, K. et al.: Automatic analysis of malware behavior using machine learning, *Journal of Computer Security*, Vol.19, No.4, pp.639– 668 (2011).
- [13] Wong, M.Y. et al.: An Inside Look into the Practice of Malware Analysis, *The 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21)*, pp.3053–3069 (2021).
- [14] Stichting Cuckoo Foundation: Cuckoo Sandbox Automated Malware Analysis, available from (https://cuckoosandbox.org/) (accessed 2022-02-24).
- [15] any.ryn: ANY.RUN Interactive Online Malware Sandbox, available from (https://any.run) (accessed 2022-02-24).
- [16] Yamagishi, R. et al.: Clarification of Malware Dynamic Analysis Tasks by User Investigation, *Computer Security Symposium 2021* (*CSS '21*), pp.112–119 (2021) (in Japanese).
- [17] Mandiant: Cyber Security & Threat Intelligence Resources, available from (https://www.mandiant.com/resources?f[0]=layout:article\_ report) (accessed 2022-02-24).
- [18] Cisco Talos: Cisco Talos Intelligence Group Comprehensive Threat Intelligence, available from (https://talosintelligence.com/) (accessed 2022-02-24).
- [19] Trend Micro: Research, News, and Perspectives, available from (https://www.trendmicro.com/en\_us/research.html) (accessed 2022-02-24).
- [20] Mandiant: GitHub mandiant/capa: The FLARE team's opensource tool to identify capabilities in executable files, available from (https://github.com/mandiant/capa) (accessed 2022-02-24).
- [21] Intezer Analyze: Intezer Analyze All-In-One Malware Analysis Platform, available from (https://analyze.intezer.com/) (accessed 2022-02-24).
- [22] MITRE: subtechniques-csv.zip, available from (https://attack.mitre. org/docs/subtechniques/subtechniques-csv.zip) (accessed 2022-02-24).
- [23] MITRE: MITRE ATT&CK Navigator, available from (https://mitreattack.github.io/attack-navigator/) (accessed 2022-02-24).
- [24] MITRE: Sightings Ecosystem: A Data-driven Analysis of ATT&CK in the Wild, available from (https://web.mitre-engenuity.org/hubfs/ Center%20for%20Threat%20Informed%20Defense/CTID-Sightings-Ecosystem-Report.pdf) (accessed 2022-07-26).
- [25] Takahashi, Y. et al.: APTGen: An Approach towards Generating Practical Dataset Labelled with Targeted Attack Sequences, 13th USENIX Workshop on Cyber Security Experimentation and Test (CSET '20), (2020).
- [26] Yokoyama, A. et al.: SandPrint: Fingerprinting Malware Sandboxes to Provide Intelligence for Sandbox Evasion, *The 19th International Symposium on Research in Attacks*, Intrusions and Defenses (RAID '16), pp.165–187 (2016).
- [27] Al-Shaer, R. et al.: Eliana Christou: Learning the Associations of MITRE ATT & CK Adversarial Techniques, 2020 IEEE Conference on Communications and Network Security (CNS '20), pp.1–9 (2020).
- [28] Hemberg, E. et al.: Linking Threat Tactics, Techniques, and Patterns with Defensive Weaknesses, Vulnerabilities and Affected Platform Configurations for Cyber Hunting, arXiv (2020).
- [29] Bulazel, A. et al.: A Survey On Automated Dynamic Malware Anal-

ysis Evasion and Counter-Evasion: PC, Mobile, and Web, Proc. 1st Reversing and Offensive-oriented Trends Symposium (ROOTS '17), pp.1–21 (2017).

[30] Nappa, A. et al.: PoW-How: An Enduring Timing Side-Channel to Evade Online Malware Sandboxes, *European Symposium on Research* in Computer Security (ESORICS '21), pp.86–109 (2021).

## Appendix

## A.1 Detailed Information on the Validation of the ATT&CK Technique Mapping Function

This section shows detail of statistical tests of each RQ.

First, **Table A**·1 shows the results for all techniques for the number of techniques observed and the presence of significant differences in each sandbox as described in RQ1. As in Table 4, the number of observations in each sandbox, the p-value of the chi-square test, and the presence of significant differences at a significance level of 0.05 are shown for each technique for the 1,012 samples in all sandboxes.

Next, **Table A** $\cdot$ **2** shows the significant difference between malware and benign files for each technique described in RQ3. This table shows the number of observations, the p-value of the chisquare test, and the presence or absence of a significant difference when the significance level is set to 0.05 for each technique for the 13,115 malware and 1,531 benign files that existed in Joe-Sandbox.

**Table A** $\cdot$ **3** shows the techniques observed in the multiple methods described in RQ4 and whether there are significant differences between methods. The table shows the number of observations per method, the p-value of the chi-square test, and the presence of significant differences when the significance level is set to 0.05 for the techniques observed in the online sandbox, static analysis, and reports.

TID	Technique	JoeSat	unexist	Hybrid exist	I Analysis unexist		unexist	p-value	Statistical significance
T1055 T1497	Process Injection Virtualization/Sandbox Evasion	938 874	74 138	598 241	414 771	0 62	1,012 950	0	1
T1027.002 T1027	Software Packing Obfuscated Files or Information	769 863	243 149	669	343 1,005	0	1,012 1,012	1.18E-301	4
T1518.001	Security Software Discovery	925	87	53	959	3	1,009	0	v v
T1057 T1082	Process Discovery System Information Discovery	878 991	134 21	465 207	547 805	0 413	1,012 599	0 2.29E-285	1
T1560 T1573	Archive Collected Data Encrypted Channel	852 898	160 114	3 223	1,009 789	0	1,012 1,012	0	4
T1071 T1036	Application Layer Protocol Masquerading	815 821	197 191	0 89	1,012 923	0	1,012 1,012	0	*****
T1095	Non-Application Layer Protocol	744	268	3	1,009	0	1,012	0	1
T1105 T1078	Ingress Tool Transfer Valid Accounts	540 30	472 982	47 0	965 1,012	0	1,012 1,012	6.30E-247 6.94E-14	1
T1106 T1203	Native API Exploitation for Client Execution	293 65	719 947	4 34	1,008 978	0 32	1,012 980	5.33E-138 0.000276521	4
T1569.002 T1574.002	Service Execution	47	965	5	1,007	0	1,012	1.03E-17	V.
T1546.011	DLL Side-Loading Application Shimming	110 124	902 888	0	1,012 1,012	0	1,012 1,012	2.70E-50 7.15E-57	1
T1543.003 T1068	Windows Service Exploitation for Privilege Escalation	69 27	943 985	15 0	997 1,012	23 0	989 1,012	1.91E-11 1.48E-12	1
T1134 T1140	Access Token Manipulation Deobfuscate/Decode Files or Information	172 579	840 433	0	1,012	0	1,012	6.54E-80 9.15E-307	,
T1070.006	Timestomp	180	832	0	1,012	0	1,012	7.95E-84	ž.
T1218.010 T1218.011	Regsvr32 Rundll32	3 48	1,009 964	5 7	1,007 1,005	0	1,012 1,012	0.092432672 6.02E-17	-
T1056 T1124	Input Capture System Time Discovery	379 271	633 741	2 11	1,010 1,001	0	1,012 1,012	5.66E-187 1.48E-120	********
T1120	Peripheral Device Discovery	9 581	1,003	601 18	411 994	38 0	974	1.95E-285 1.80E-296	- -
T1083 T1012	File and Directory Discovery Query Registry	289	431 723	909	103	269	1,012 743	2.94E-228	1
T1070.004 T1087	File Deletion Account Discovery	133 227	879 785	365 0	647 1,012	9 0	1,003 1,012	1.81E-101 2.81E-107	
T1033 T1018	System Owner/User Discovery Remote System Discovery	227 691	785 321	16 14	996 998	0 14	1,012 998	2.83E-94 0	1
T1115	Clipboard Data	196	816	3	1,009	0	1,012	4.29E-89	2
T1529 T1070	System Shutdown/Reboot Indicator Removal on Host	103	909 1,009	0	1,012 1,011	0	1,012 1,012	4.97E-47 0.173373213	-
T1003 T1571	OS Credential Dumping Non-Standard Port	478 367	534 645	52 256	960 756	0	1,012 1,012	1.48E-205 6.16E-94	4
T1059	Command and Scripting Interpreter	222	790	4	1,008	13	999	9.41E-91	V.
T1547.001 T1574.010 T1010	Registry Run Keys / Startup Folder Services File Permissions Weakness	208 5	804 1,007	162 3	850 1,009	177 0	835 1,012	0.025182647 0.092432672	-
T1016	Application Window Discovery System Network Configuration Discovery	501 118	511 894	148 59	864 953	0	1,012 1,012	6.83E-170 6.17E-28	1
T1113 T1486	Screen Capture Data Encrypted for Impact	34 19	978 993	6 19	1,006	0	1,012 1,012	1.35E-11 6.64E-05	1
T1053	Scheduled Task/Job	183	829	115	897	126	886	1.74E-05	Ž,
T1562.001 T1112	Disable or Modify Tools Modify Registry	695 39	317 973	11 524	1,001 488	13 326	999 686	0 5.78E-124	1
T1005 T1114	Data from Local System Email Collection	453 322	559 690	84 122	928 890	358 116	654 896	1.66E-76 6.13E-40	1
T1047	Windows Management Instrumentation	422	590 948	42	970	0	1,012	7.58E-180	****
T1222 T1564.001	File and Directory Permissions Modification Hidden Files and Directories	64 133	879	0 4	1,012 1,008	3	1,009 1,007	1.16E-26 1.04E-53	×.
T1552.002 T1037.005	Credentials in Registry Startup Items	232 33	780 979	0	1,012	0	1,012 1.012	8.08E-110 3.24E-15	1
T1189 T1102	Drive-by Compromise Web Service	1 22	1,011 990	0	1,012 1,012	0 32	1,012 980	0.367758249 2.61E-07	-
T1014	Rootkit	39	973	0	1,012	0	1,012	6.95E-18	1
T1056.004 T1059.001	Credential API Hooking PowerShell	57 22	955 990	902 94	110 918	0	1,012 1,012	0 5.90E-29	~~~
T1197 T1552.001	BITS Jobs Credentials In Files	58	1,011 954	0	1,012 1,010	1 358	1,011 654	0.606330781 3.48E-133	-
T1007 T1219	System Service Discovery	33	979	0	1,012	0	1,012	3.24E-15	V.
T1406	Remote Access Software Obfuscated Files or Information	54 6	958 1,006	0	1,012 1,012	0	1,012 1,012	1.33E-24 0.002449476	1
T1523 T1412	Evade Analysis Environment Capture SMS Messages	1	1,011 1,009	0	1,012	0	1,012 1,012	0.367758249 0.173373213	1
T1426 T1449	System Information Discovery Exploit SS7 to Redirect Phone Calls/SMS	3	1,009 1,008	0	1,012 1,012	0	1,012 1,012	0.049639551 0.018219241	
T1448	Carrier Billing Fraud	4	1,008	0	1,012	0	1,012	0.018219241	4 - 4 - 4
T1418 T1409	Application Discovery Access Stored Application Data	5	1,007 1,011	1	1,011 1,012	0	1,012 1,012	0.029988818 0.367758249	√ -
T1421 T1422	Access Stored Application Data System Network Connections Discovery System Network Configuration Discovery	3 2	1,009 1,010	1	1,011 1,012	0	1,012 1,012	0.173373213 0.135156976	
T1430 T1424	Location Tracking Process Discovery	5	1,007	1	1,011	0	1,012	0.029988818 0.049639551	4
T1432	Access Contact List	2	1,010	0	1,012	0	1,012	0.135156976	- -
T1433 T1507	Access Call Log Network Information Discovery	1 5	1,011 1,007	0	1,012 1,012	0	1,012 1,012	0.367758249 0.0066826	-
T1439 T1472	Eavesdrop on Insecure Network Communication Generate Fraudulent Advertising Revenue	2	1,010 1,011	0	1,012 1,012	0	1,012 1,012	0.135156976 0.367758249	-
T1447	Delete Device Data	4	1,008	0	1,012	0	1,012	0.018219241	1
T1129 T1136	Shared Modules Create Account	90 16	922 996	0	1,012 1,012	0	1,012 1,012	5.24E-41 1.03E-07	~~~~
T1564.002 T1049	Hidden Users System Network Connections Discovery	12 5	1,000 1,007	0	1,012 1,012	0	1,012 1,012	5.86E-06 0.0066826	4
T1499	Endpoint Denial of Service	11	1,001	0	1,012	0	1,012	1.60E-05 0.029988818	
T1566.002 T1429	Spearphishing Link Capture Audio	5	1,007 1,010	0	1,011 1,012	0	1,012 1,012	0.135156976	-
T1080 T1055.011	Taint Shared Content Extra Window Memory Injection	7	1,005 1,004	0 31	1,012 981	0	1,012 1,012	0.000897249 1.72E-09	4
T1547.008 T1021.001	LSASS Driver Remote Desktop Protocol	5	1,007	0 230	1,012 782	0	1,012 1.011	0.0066826 5.13E-107	√ √ -
T1574.001 T1490	DLL Search Order Hijacking	1	1,011 1,009	0	1,012 1,006	0	1,012 1,003	0.367758249 0.221142869	-
T1185	Inhibit System Recovery Man in the Browser	18	994	0	1,012	0	1,012	1.37E-08	-
T1048 T1091	Exfiltration Over Alternative Protocol Replication Through Removable Media	5	1,007 1,003	0	1,012 1,012	0	1,012 1,009	0.0066826 0.005139326	4 4 4
T1090.003 T1090	Multi-hop Proxy Proxy	8 24	1,004 988	0	1,012 1,010	0 10	1,012 1,002	0.000328447 2.87E-05	1
T1564.003	Hidden Window	0	1,012	3	1,009	0	1,012	0.049639551	✓
T1542.003 T1053.001	Bootkit At (Linux)	8 2	1,004 1,010	9 0	1,003 1,012	8 0	1,004 1,012	0.960470399 0.135156976	1
T1547.006 T1553.004	Kernel Modules and Extensions Install Root Certificate	1 2	1,011 1,010	30 0	982 1,012	0 71	1,012 941	4.70E-13 1.29E-30	1
T1001 T1562.004	Data Obfuscation Disable or Modify System Firewall	5	1,007 1,012	0	1,012 1,005	0	1,012 1,012	0.0066826 0.000897249	
T1548.002	Bypass User Access Control	4	1,008	1	1,011 1,010	2	1,010	0.367030256	1
T1491 T1564.004	Defacement NTFS File Attributes	10	1,002 1,011	2 163	849	0	1,003 1,012	0.065011494 1.20E-74	~
T1135 T1553.002	Network Share Discovery Code Signing	3	1,009 1,012	1 45	1,011 967	0	1,012 1,012	0.173373213 1.45E-20	-
T1046 T1176	Network Service Scanning Browser Extensions	0	1,012	1 0	1,011	0	1,012	0.367758249	
T1218.005	Mshta	0	1,012	7	1,005	0	1,012	0.000897249	1
T1413 T1547.004	Access Sensitive Data in Device Logs Winlogon Helper DLL	3	1,009 1,012	0	1,012 1,011	0 7	1,012 1,005	0.049639551 0.004565621	1
T1546.001 T1098	Change Default File Association Account Manipulation	0	1,012	0	1,012	2	1,010 1,011	0.135156976 0.367758249	
T1489	Service Stop	0	1,012	17	995	2	1,010	1.10E-06	1
T1055.012 T1055.003	Process Hollowing Thread Execution Hijacking	0	1,012 1,012	333 39	679 973	0	1,012 1,012	3.66E-163 6.95E-18	1
T1497.003 T1071.001	Time Based Evasion Web Protocols	0	1,012 1,012	326 161	686 851	0	1,012 1,012	2.45E-159 1.46E-74	· · · · · · · · · · · · · · · · · · ·
T1204 T1137	User Execution	0	1,012	41	971	0	1,012 1,012	8.92E-19 4.19E-16	5
T1074.001	Office Application Startup Local Data Staging	0	1,012	83	929	0	1,012	8.72E-38	ž
T1053.005 T1059.003	Scheduled Task Windows Command Shell	0	1,012 1,012	115 103	897 909	0	1,012 1,012	1.23E-52 4.97E-47	1
T1036.005 T1565	Match Legitimate Name or Location Data Manipulation	0	1,012	12 50	1,000 962	0	1,012	5.86E-06 8.35E-23	1
T1218.007	Msiexec	0	1,012	7	1,005	0	1,012	0.000897249	· ·
T1132.001 T1402	Standard Encoding Broadcast Receivers	0	1,012 1,012	28 1	984 1,011	0	1,012 1,012	5.33E-13 0.367758249	-
T1420 T1582	File and Directory Discovery SMS Control	0	1,012	1	1,011	0	1,012	0.367758249 0.367758249	1
T1204.002 T1070.001	Malicious File Clear Windows Event Logs	0	1,012	15 20	997 992	0	1,012 1,012	2.84E-07 1.81E-09	4
T1559.001	Component Object Model	0	1,012	16	996	0	1,012	1.03E-07	ž.
T1218 T1059.005	Signed Binary Proxy Execution Visual Basic	0	1,012 1,012	1 14	1,011 998	0	1,012 1,012	0.367758249 7.79E-07	-
T1114.001 T1222.001	Local Email Collection Windows File and Directory Permissions Modification	0	1,012 1,012	3	1,009 1,009	0	1,012 1,012	0.049639551 0.049639551	4
T1546.007	Netsh Helper DLL	0	1,012	2	1,010	0	1,012	0.049639331 0.135156976 0.367758249	-
T1566.001 T1560.002	Spearphishing Attachment Archive via Library	0	1,012 1,012	1	1,011 1,011	0	1,012 1,012	0.367758249	
T1056.001 T1048.003	Keylogging Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	0	1,012 1,012	4	1,008 1,011	0	1,012 1,012	0.018219241 0.367758249	- -
T1059.007 T1055.001	JavaScript Dynamic-link Library Injection	0	1,012	1	1,011	0	1,012	0.367758249 0.367758249	-
	, manual mpenna		1,012		-,311	0	1,012		

 
 Table A·1
 Number of observations and presence of significant differences among sandboxes for each MITRE ATT&CK Technique (RQ1).

Techniqu

JoeSandbox Hybrid Analysis Hatching Triage p-value Statistical

ID	Technique	Maliciou exist	unexist	Clean exist	unexist	p-value	Statistical significance
1573 1518.001	Encrypted Channel Security Software Discovery	11,855 11,364	1,260 1,751	678 508	855 1,025	0	1
1071	Application Layer Protocol	10,920	2,195	382	1,151	0	1
1082 1055	System Information Discovery Process Injection	10,352 10,055	2,763 3,060	919 1,138	614 395	2.26E-62 0.036382082	-
1027	Obfuscated Files or Information	9,523	3,592	385	1,148	0.00E+00	1
057	Process Discovery Masquerading	9,081 8,760	4,034 4,355	529 948	1,004 585	2.80E-161 0.000116312	1
560	Archive Collected Data	8,741	4,374	394	1,139	7.43E-215	1
497	Virtualization/Sandbox Evasion Non-Application Layer Protocol	8,637 8,310	4,478 4,805	272 285	1,261 1,248	1.75E-291 2.40E-248	1
027.002	Software Packing	7,930	5,185	88	1,445	0	1
018	Remote System Discovery File and Directory Discovery	7,676 6,796	5,439 6,319	155 958	1,378 575	8.76E-283 2.90E-15	
562.001	Disable or Modify Tools	6,406	6,709	187	1,346	1.17E-163	1
105 140	Ingress Tool Transfer Deobfuscate/Decode Files or Information	6,352 6,332	6,763 6,783	347 203	1,186 1,330	8.29E-82 5.11E-150	1
003	OS Credential Dumping	4,941	8,174	1	1,532	1.66E-190	1
571 010	Non-Standard Port Application Window Discovery	4,940 4,719	8,175 8,396	27 123	1,506 1,410	2.21E-173 3.57E-107	1
005	Data from Local System	4,171	8,944	8	1,525	6.19E-145	1
106 124	Native API System Time Discovery	4,152 4,085	8,963 9,030	232 268	1,301 1,265	1.37E-40 2.23E-28	1
056	Input Capture	3,996	9,119	129	1,404	1.67E-73	1
047 059	Windows Management Instrumentation Command and Scripting Interpreter	3,491 3,015	9,624 10,100	17 243	1,516 1,290	2.36E-108 2.51E-10	1
012	Query Registry	2,958	10,157	229	1,304	1.00E-11	1
033	System Owner/User Discovery Email Collection	2,828 2,761	10,287 10,354	82	1,451 1,525	5.30E-51 9.05E-84	1
087	Account Discovery	2,730	10,385	55	1,478	3.03E-59	1
070.006	Timestomp File Deletion	2,183 2,138	10,932 10,977	46	1,487 1,456	9.40E-45 3.03E-31	1
1134	Access Token Manipulation	1,984	11,131	133	1,400	1.38E-11	1
1115 1203	Clipboard Data Exploitation for Client Execution	1,950 1,823	11,165 11,292	63 80	1,470 1,453	8.49E-31 1.63E-21	1
1547.001	Registry Run Keys / Startup Folder	1,823	11,292	84	1,449	2.69E-20	1
1552.002 1546.011	Credentials in Registry	1,741	11,374 11,380	0 83	1,533	6.97E-52	1
1574.002	Application Shimming DLL Side-Loading	1,735 1,493	11,380	194	1,450 1,339	2.32E-18 0.151912084	-
053	Scheduled Task/Job	1,400	11,715	12	1,521	3.72E-35	1
564.001 016	Hidden Files and Directories System Network Configuration Discovery	1,384 1,232	11,731 11,883	10	1,523 1,533	1.34E-35 8.40E-36	1
529 218.011	System Shutdown/Reboot	1,176	11,939	113	1,420	0.041438039	-
543.003	Rundl132 Windows Service	1,169 930	11,946 12,185	72	1,461 1,460	2.67E-08 0.000770065	1
129	Shared Modules	920	12,195	0	1,533	1.63E-26	1
569.002 113	Service Execution Screen Capture	845 658	12,270 12,457	27	1,506 1,514	3.50E-13 4.06E-11	1
068	Exploitation for Privilege Escalation	597	12,518	68	1,465	0.886976911	
552.001 112	Credentials In Files Modify Registry	564 557	12,551 12,558	0	1,533 1,524	2.21E-16 3.28E-12	1
078	Valid Accounts	529	12,586	11	1,522	1.13E-10	1
219 056.004	Remote Access Software Credential API Hooking	526 521	12,589 12,594	0	1,533 1,533	2.51E-15 3.45E-15	1
222	File and Directory Permissions Modification	470	12,645	5	1,528	1.62E-11	1
014 037.005	Rootkit Startup Items	399 323	12,716 12,792	0 2	1,533 1,531	7.85E-12 7.70E-09	1
007	System Service Discovery	320	12,795	4	1,529	6.76E-08	√
1120 1059.001	Peripheral Device Discovery PowerShell	305 289	12,810 12,826	90	1,443 1,533	1.01E-15 7.77E-09	1
070	Indicator Removal on Host	286	12,829	8	1,525	1.82E-05	<i>v</i> .
1486 1102	Data Encrypted for Impact Web Service	271 252	12,844 12,863	5	1,528 1,533	3.44E-06 7.84E-08	1
1218.010	Regsvr32	241	12,874	18	1,515	0.077975619	-
1091 1406	Replication Through Removable Media Obfuscated Files or Information	225 201	12,890 12,914	86	1,447 1,522	3.59E-23 0.015720353	-
1507	Network Information Discovery	195	12,920	13	1,520	0.059249023	-
1426 1421	System Information Discovery System Network Connections Discovery	194 188	12,921 12,927	11	1,522 1,520	0.022177882 0.080383406	-
1447	Delete Device Data	184	12,931	10	1,523	0.020631478	-
1424 1185	Process Discovery Man in the Browser	163 150	12,952 12,965	9	1,524 1,532	0.033169614 0.000132267	-
1418	Application Discovery	147	12,968	2	1,531	0.000427987	1
1574.010 1136	Services File Permissions Weakness Create Account	144 140	12,971 12,975	17	1,516 1,531	0.927883606 0.000660962	-
564.002	Hidden Users	116	12,999	0	1,533	0.000393093	1
055.011 499	Extra Window Memory Injection Endpoint Denial of Service	109 101	13,006 13,014	18	1,515 1,533	0.220443697 0.001020654	-
422	System Network Configuration Discovery	97	13,018	2	1,531	0.009605471	1
090 523	Proxy Evade Analysis Environment	97 95	13,018 13,020	0	1,533 1,533	0.001317978 0.00149803	
080	Taint Shared Content	81	13,034	0	1,533	0.003689418	<i>v</i> .
548.002 547.008	Bypass User Access Control LSASS Driver	77 75	13,038 13,040	0	1,533 1,533	0.004782079 0.005446388	1
429	Capture Audio	71	13,044	3	1,530	0.10609741	-
491 048	Defacement Exfiltration Over Alternative Protocol	69 61	13,046 13,054	03	1,533 1,530	0.008059561 0.190616084	-
001	Data Obfuscation	48	13,067	0	1,533	0.032644518	-
542.003 049	Bootkit System Network Connections Discovery	48 46	13,067 13,069	1	1,532 1,532	0.089877812 0.102735537	-
564.004	NTFS File Attributes	43	13,072	0	1,533	0.045959464	-
090.003 566.002	Multi-hop Proxy Spearphishing Link	41 39	13,074 13,076	0 84	1,533 1,449	0.052771664 6.37E-97	-
490	Inhibit System Recovery	29	13,086	0	1,533	0.123719937	-
021.001	Remote Desktop Protocol Drive-by Compromise	28 26	13,087 13,089	0 45	1,533 1,488	0.133131673 4.70E-47	-
553.004	Install Root Certificate	25	13,090	1	1,532	0.433632044	-
564.003 547.006	Hidden Window Kernel Modules and Extensions	23 22	13,092 13,093	0	1,533 1,533	0.19357285 0.20900378	-
1135	Network Share Discovery	20	13,095	0	1,533	0.244206902	-
562.004 574.001	Disable or Modify System Firewall DLL Search Order Hijacking	16 15	13,099 13,100	0 33	1,533 1,500	0.337188376 1.65E-38	-
1433	Access Call Log	14	13,101	0	1,533	0.399175466	-
564 543.002	Hide Artifacts Systemd Service	11 10	13,104 13,105	0	1,533 1,533	0.521084905 0.572197451	-
176	Browser Extensions	7	13,108	1	1,532	0.69681483	-
110	Brute Force Image File Execution Options Injection	6	13,109	0	1,533	0.864492365	-
1546.012 1046	Image File Execution Options Injection Network Service Scanning	5 5	13,110 13,110	0	1,533 1,533	0.972864077 0.972864077	-
1197	BITS Jobs	3	13,112	0	1,533	0.72565624	-
1546.006 1543.001	LC_LOAD_DYLIB Addition Launch Agent	3	13,112 13,112	0	1,533 1,533	0.72565624 0.72565624	-
1547.011	Plist Modification	3	13,112	5	1,528	2.32E-05	1
1040 1211	Network Sniffing Exploitation for Defense Evasion	3 2	13,112 13,113	0	1,533 1,533	0.72565624 0.501883284	-
1056.002	GUI Input Capture	2	13,113	0	1,533	0.501883284	-
1532 1218.005	Data Encrypted Mshta	2 2	13,113 13,113	0	1,533 1,533	0.501883284 0.501883284	-
1553.002	Code Signing	2	13,113	1	1,532	0.72565624	-
1132	Data Encoding	1	13,114 13,114	2	1,531 1,533	0.025273731 0.196511029	-
573.002	Asymmetric Cryptography						

 Table A-2
 Presence of significant differences between malware and benign files for each technique (RQ3).

1055 1497 1497	Technique	JoeSand		cxist	Analysis unexist	Hatch	ing Triage unexist	Combination	p-value	Statistica
	Process Injection Virtualization/Sandbox Evasion Virtualization/Sandbox Evasion	10,690	unexist 15,388 16,501	0	unexist 3,918 3,916	exist 16 4	34 46	sandbox+report (all) sandbox+static	0.251052825	
1497 1497	Virtualization/Sandbox Evision Virtualization/Sandbox Evision	9,577 9,577 9,577	16,501 16,501 16,501	2 2	3,916 3,916 3,916	4	40 46 46	(all) sandbox+static (all) sandbox+report (all) static+report (all) sandbox+static	5.99E-06 4.36E-36	
1497 1027.002 1027.002	Software Packing Software Backing	8,649 8,649	17,429	4	3,914 3,914	2 2	48 48	(all) sandbox+static (all) sandbox + static	0 0.000175584	
1027.002	Software Facking Obfuscated Files or Information Obfuscated Files or Information	8,649	17,429 17,429	4 4	3,914 3,914 2,506	2	48	(all) sandbox+report (all) static+report (all) sandbox+static (all) sandbox+report	1.82E-07 0.551849477	~
1027 1027	Obfuscated Files or Information Obfuscated Files or Information	9,530	16,548 16,548	1,412	2,506	15	35	(all) sandbox+report (all) statio report	0.46179638	1
1518.001	Security Software Discovery Security Software Discovery	11,428	16,548 14,650 14,650	3	3,915 3,915	2	48 48	(all) static+report (all) sandbox+static (all) sandbox+report	0 1.07E-07	
1518.001		11.428	14,650	3 3 99	3,915	2 2 7	48	(all) static+report	8.17E-09	1
1057 1057 1057	Process Discovery Process Discovery Broomer Discovery	9569 9569 9569	16,509 16,509 16,509	99 99 99	3,819 3,819 2,819	7	43 43 43	(all) sandbox+static (all) sandbox+report (all) static+report	0 8.45E-16 5.16E.06	1
1082	Process Discovery System Information Discovery	15 870	10 100	2.416	3,819	11	39	(all) static+report (all) sandbox+static	5.16E-06 0.363771896	2
1082 1082 1560	System Information Discovery System Information Discovery Archive Collected Data	15,879 15,879 15,879 8,750	10,199 10,199 10,199	2,416 2,416 0	1,502 1,502 3,918	11	39 39	(all) sandbox+report (all) static+report sandbox+report	3.48E-300 2.51E-08 7.07E-05 8.02E-10	,
1573	Encline Connect International	12,093	13,985	0	3,918	1	49 40		8.02E-10 0.002797683	1
1071 1036 1105	Encrypted Channel Application Layer Protocol Misequerading Ingress Tool Transfer	8,851	17,227	0	3,918	10 5 15	40 45 35	sandbox+report sandbox+report	0.000618542 0.464919838	7
1078	Ingress tool transfer Valid Accounts	6,401 529	19,6/7 25,549 21,922	0	3,918 3,918 3,918	15	39	sandbox+report sandbox+report	0.464919838 4.54E-21 0.034712164	
1106 1203 1569.002	Masqueraling Ingress Tool Transfer Vild Accounts Naive API Exploitation for Client Execution Service Execution Service Execution Service Incountion DIT Stol-Londone	4,156 2,415 858	21,922 23,663 25,220	0	3,918 3,918 3,793	2	48 48	sandbox+report sandbox+report sandbox+report	0.034712164 0.299105373 0.78040016	
1569.002	Service Execution Service Execution	858	25,220	125 125	3,793	5	45 45	(all) sandbox+static (all) sandbox+report	0	2
1569.002 1574.002	Service Execution DEL Side-Loading	858	25,220 24,585	125	3,793 3,918	3	45 49 48	(all) static+report sandbox+report	0.022133283 0.407363774	
1543.003 1543.003 1543.003	Windows Service Windows Service	1,338 1,338	24,740 24,740 24,740	42 42 42	3,918	2 2 2	48 48 48	sandbox+report (all) sandbox+static (all) sandbox+report (all) static+report	1.93E-29 1.56E-67 0.198753535	1
	Windows Service Exploitation for Privilege Escalation	1,338		0	3,870	2	48	(all) static+report sandbox+report		
1134 1140	Access Token Manipulation Deobfuscate/Decode Files or Information	1,985	24,093 19,741	144	3,774 3,796	0	50 39	sandbox+report sandbox+static (all) sandbox+static (all) sandbox+report	4.94E-19 1.59E-198	
1140 1140	Windows Service Exploritation for Privilege Escalation Access Token Manipulation Deoblisus:etgDecode Files or Information Deoblisus:etgDecode Files or Information Deoblisus:etgDecode Files or Information Timestomp	6,337 6,337	19,741 19,741 19,741	122 122 122 122	3,796	11 11 11	39 39	(all) sandbox+report (all) static+report (all) sandbox+static	5.10E-51 3.00E-12	1
1070.006		2,183	23,895	17	3,901 3,901	2	48 48	(oII) sandbox arenort	2.21E-70 8.05E-07	1
1070.006 1056	Timestomp Input Capture System Time Discovery	2,183	23,895	17	3,901 3,918	2	48 45	(all) static+report sandbox+report	0.009351916 0.395487368	
1124 1120	System Time Discovery Peripheral Device Discovery	4,099 1,687	21,979 24,391	0	3,918 3,918	2	48 48	sandbox+report sandbox+report	0.037422522 0.673395827	
1120 1083 1083	Peripheral Device Discovery File and Directory Discovery File and Directory Discovery File and Directory Discovery	1,687 6,818 6,818 6,818	24,391 19,260 19,260	0 1,748 1,748 1,748	3,918 2,170 2,170 2,170	12 12 12	48 38 38 38	sandbox+report (all) sandbox+static (all) sandbox+report (all) static+report	1.11E-125 0	1
1083		6,818 7,460 7,460	19,260	1,748 724 724	2,170 3,194 3,194		38 46	(all) sandbox+static	0.005565762 4.45E-40	1
1012 1012	Query Registry Query Registry File Deletion	7,460	18,618 18,618	724 724		4 4 4	46 46		0 0.085716776	Ľ.
1070.004 1070.004 1070.004	File Deletion File Deletion	2,550 2,550 2,550	23,528 23,528 23,528	1	3,917 3,917 3,917 3,917 3,783	7	43 43	(all) sandbox+static (all) sandbox+report (all) static+report (all) sandbox+static	2.81E-92 0.155138889 1.20E-91 5.06E-44	
	File Deletion File Deletion Account Discovery	2,730	23,348	135	3,917 3,783	7	43	(all) static+report (all) sandbox+static	1.20E-91 5.06E-44	
1087 1087		2,730 2,730	23,348	135	3,783	9	41 41		4.16E-172	1
1033 1033	Account Discovery Account Discovery System Owner/User Discovery System Owner/User Discovery System Owner/User Discovery	2,845 2,845 2,845	23,233 23,233 23,233	201 201	3,717	5	45	(all) static+report (all) static+report (all) sandbox+static (all) sandbox+report (all) static+report	8.13E-29 4.35E-260 0.221871132	1
1033 1018	System Owner/User Discovery Remote System Discovery	7,846		201	3,717 3,717 3,918	5 5 5	45 45 45	(all) static+report sandbox+report		
1115	Remote System Discovery Clipboard Data Clipboard Data	1,955 1,955	24122	729	3,680 3,680	1	49	sandbox+report (all) sandbox+static (all) sandbox+report	0.001601174	1
1115 1115 1529	Clipboard Data System Shutdown/Reboot	1,955	24,123 24,123 24,902	238 238 41	3,680	1	49 49 48	(all) static+report	0.365872328	<u> </u>
1529 1529 1529	System Shutdown/Reboot	1,176 1,176 1,176	24,902 24,902 24,902	41 41 41	3,877 3,877 3,877	2 2 2	48 48	(all) sandbox+static (all) sandbox+report (all) static+report	1.96E-24 4.45E-75 0.187797059	1.
1529 1070 1003	System Smallowigheesson Indicator Removal on Host OS Credential Dumping	290	24,902 25,788 21,084	41 0 0	3,918	6 10	40	(all) static+report sandbox+report sandbox+report	0.187797059 4.14E-11 0.978207255	Ż
1003 1571 1059		4,994 5,205 3,122	21,084 20,873 22,956	0	3,918	3	40 47 39	sandbox+report sandbox+report (all) sandbox+static (all) sandbox+report	0.978207255 0.02194729	Ż
1059 1059 1059	Non-Standard Port Command and Scripting Interpreter Command and Scripting Interpreter Command and Scripting Interpreter	3,122	22,956	1,801 1,801 1,801	2,117 2,117 2,117	11	39 39 39	(all) sandbox+report	0 001203964	1
1059 1547.001 1547.001	Command and scripting interpreter Registry Run Keys / Startup Folder	3,122 4,302 4,302	22,956 21,776 21,776	1,801 104 104	2,117 3,814 3,814	11 5 5	39 45 45	(all) static+report (all) sandbox+static (all) sandbox+report	0.001203964 4.84E-115 1.25E-66	
1547.001 1547.001 1010	Registry Run Keys / Startup Folder Registry Run Keys / Startup Folder	4,302 4,302 4,897	21,776 21,181	104 104 1.096	3,814 3,814 2,822	5	45 45 50	(all) static+report (all) static+report	0.006481233 6.03E-41	1
1016	Regiony Ruin Reys / Stating Polder Regions Run Reys / Stating Polder Application Window Discovery System Network Configuration Discovery System Network Configuration Discovery System Network Configuration Discovery System Network Configuration Discovery	4,897	21,181 24,595 24,595	1,096 89 89	2,822 3,829 3,829	0	47	(all) static+report sandbox+static (all) sandbox+static (all) sandbox+report	6.0.5E-41 5.29E-19 4.44E-186	1
1016 1016	System Network Configuration Discovery System Network Configuration Discovery	1,483 1,483 1,483 1,483 664	24,595 24,595 25,414	89 89 403	3,829 3,829 3,515	3	47 47 47 47	(all) sandbox+report (all) static+report (all) sandbox+static	4.44E-186 0.204823814 7.12E-131	
1113	Screen Capture Screen Capture Screen Capture		25,414 25,414 25,414	403	3,515 3,515 3,515	3	47 47 47	(all) sandbox+static (all) sandbox+report (all) static+report		1
1113 1486	Screen Capture Data Encrypted for Impact Scheduled Task/Job	664 290	25788	403	3,515 3,918 3,918	3 11 12	30	(all) static+report sandbox+report sandbox+report	0.447946249 1.41E-39	- 7
1053 1562.001	Scheduled Task/Job Disable or Modify Tools	2,787 6,784	23,291 19,294	0	3,918	9	38 41	sandbox+report sandbox+report	0.004923383 0.258742312	
1112 1112 1112	Sententice task/160 Disable of Modify Tools Modify Registry Modify Registry Modify Registry Data from Local System	4,886	21,192 21,192	195	3,723 3,723	6	44 44 44	sandbox+report (all) sandbox+report (all) sandbox+static (all) static+report sandbox+report sandbox+report	1.82E-101 9.55E-132	1
1112	Modify Registry Data from Local System	4,886 4,886 8,036	21,192 21,192 21,192 18,042	193 195 195 0	3,723 3,723 3,723 3,918	6 6 3	44	(all) static+report sandbox+report	9.55E-132 0.054137315 0.000267483	· ·
1114	Window Management Instrumentation	3,995	22,083	0	3,918	2	48	sandbox+report (all) sandbox+static	0.042887734 8.44E 120	- /
1047	Windows Management Instrumentation Windows Management Instrumentation	3,542 3,542	22,536 22,536	8	3,910 3,910	3	47	(all) sandbox+report (all) static+report	0.991008892 1.64E-10 1.17E-36	
1047 1047 1047 1222 1222	File and Directory Permissions Modification File and Directory Permissions Modification	628 628	25,450 25,450	237 237	3,681 3,681	1	49 49	(all) sandbox+static (all) sandbox+report	1.17E-36 0	1
1222	File and Directory Permissions Modification File and Directory Permissions Modification Drive-by Compromise	628 628 76	25,450	237	3,681 3,681 3,918	i	49 49 48	(all) static+report	0.368942641 3.90E-10	Ľ.
1102	Web Service	588	25,450 26,052 25,490	0	3,918	2	48	sandbox+report sandbox+report	0.72375299	
1014 1059.001	Rootkit PowerShell	399 386		0	3,918 3,918	1 14	49 36	sandbox+report sandbox+report	0.759558725 8.40E-49	
1007 1007 1007	System Service Discovery System Service Discovery System Service Discovery	320 320 320	25,692 25,758 25,758 25,758 25,758	26 26 26	3,892 3,892 3,892	2 2 2	48 48 48	(all) sandbox+static (all) sandbox+report (all) static+report	0.002703009 9.37E-138 0.051117737	1
	System Service Discovery Remote Access Software Obfuscated Files or Information	526	25,758 25,552	0	3,892 3,918	6	44	(all) static+report sandbox+report		
1406 1523	Evade Analysis Environment	201	25,552 25,877 25,983	0	3,918 3,918 3,918 3,918 3,918	3	47 49	sandbox+report sandbox+report	0.00069151 0.459299844	
1426 1448	System Information Discovery	194 140	25,884 25,938	0		1	49 49	sandbox+report sandbox+report	0.834750965 0.656507257	
1418 1409	Carrier Billing Fraud Application Discovery Access Stored Application Data	148 68	25,930 26,010	0	3,918 3,918	1	49 49	sandbox+report sandbox+report	0.686269057 0.310144153	
1422 1430	System Network Configuration Discovery	97	25,981 25,906	0	3,918 3,918	1	49 49	sandbox+report sandbox+report	0.469326426 0.768093651	
1507 1472	Network Information Discovery Generate Frandulent Advertising Revenue Shared Modules Shared Modules	195	25,883 25,978	0	3,918 3,918	1	49	sandbox+report	0.837615936 1.97E-07	
1129 1129	Shared Modules	920 920	25,158 25,158	3,392 3,392	526 526	1	49 49	(all) sandbox+static (all) sandbox+report	0	
1129		920 920 140	25,158 25,938	3,392	526 3.917	i	49 49 49	(all) static+report	1.84E-62 2.26E-05	1
1136 1136 1136	Create Account Create Account	140 140 140	25,938 25,938 25,938		3,917 3,917 3,917		49 49 49	(all) sandbox+report	2.26E-05 0.656507257 0.002607017 0.000558551	L É
1136 1049 1499	Create Account System Network Connections Discovery Endpoint Denial of Service	140 78 101	25,938 26,000 25,977	0					0.00/200/017	
	Endpoint Denial of Service	101			3,918	2	48		0.000338331	,
1499	Endpoint Denial of Service	101	25,977	6	3,918 3,912 3,912	2	48 49 49 49	sandbox+report (all) sandbox+static (all) sandbox+report (all) static + senser	0.031667893 7.16E-29	
1499 1499	Spearphisning Link	101	25,977 25,977 26,036	6	3,918 3,912 3,912 3,912 3,912		48 49 49 49 46 40	(all) sandbox+static (all) sandbox+report (all) static+report sandbox+report candbox+senort	0.031667893 7.16E-29 0.162536612	- V - V - V - V
1499 1499 1566.002 1513 1080	Spearphisting Link Spearphisting Link Screen Capture Taint Shared Content	101 42 26 81	25,977 25,977 26,036 26,052	6 6 0 0	3,918 3,912 3,912 3,912 3,918 3,918	1 4 1	49 49 46 49 49	(all) sandbox+report (all) static+report sandbox+report sandbox+report sandbox+report	0.031667893 7.16E-29 0.162536612 1.03E-30 0.048237909 0.385245941	
1499 1499 1566.002 1513 1080 1021.001 1490	Taint Shared Content Remote Desktop Protocol Inhibit System Recovery	101 42 26 81 309 61	25,977 25,977 26,036 26,052 25,997 25,769 26,017	6 6 0	3,918 3,912 3,912 3,912 3,912	1 4 1 1 8 6	49 49 46 49 49 42 42 44	(all) sandbox+report (all) static+report sandbox+report sandbox+report sandbox+report sandbox+report (all) sandbox+static	0.031667893 7.16E-29 0.162536612 1.03E-30 0.048237909 0.385245941 4.96E-19 0.0127993	
1499 1499 1566.002 1513 1080 1021.001 1490	Taint Shared Content Remote Desktop Protocol Inhibit System Recovery Inhibit System Recovery	101 42 26 81 309 61 61 61 61	25,977 25,977 26,036 26,052 25,997 25,769 26,017	6 6 0 0 1 1 1	3,918 3,912 3,912 3,912 3,918 3,918 3,918 3,918 3,918 3,918 3,917 3,917 3,917	1 4 1	49 49 46 49 49 42 42 44	(all) sandbox+report (all) static+report sandbox+report sandbox+report sandbox+report (all) sandbox+report (all) sandbox+report (all) sandbox+report	0.031667893 7.16E-29 0.162536612 1.03E-30 0.048237909 0.385245941 4.96E-19 0.0127993	
1499 1499 1566.002 1513 1080 1021.001 1490 1490 1490 1183 1049	Tain's Shared Contest Remote Desktop Protocol Inhibit System Recovery Inhibit System Recovery Inhibit System Recovery Main in the Browser Extiliation Over Alternative Protocol	101 42 26 81 309 61 61 61 61 150 61	25,977 25,977 26,036 26,052 25,997 25,769 26,017 26,017 26,017 25,928 26,017	6 6 0 0 1 1 1 1 0 0	3,918 3,912 3,912 3,912 3,918 3,918 3,918 3,918 3,918 3,918 3,917 3,917 3,917 3,917 3,917 3,918	1 4 1 1 8 6 6	49 49 49 49 49 42 44 44 44 44 44 48 46	(all) sandbox+report (all) static+report sandbox+report sandbox+report sandbox+report (all) sandbox+static (all) sandbox+static (all) sandbox+report (all) sattic+report	0.031667893 7.16E-29 0.162536612 1.03E-30 0.048237909 0.048237909 0.048237909 0.0127993 0.02796386 3.07E-75 0.024410287 8.65E-22	
1499 1499 1566.002 1513 1080 1021.001 1490 1490 1490 1183 1048 1050.003 1050	Taint Shared Content Remote Desktop Protocol Inhibit System Recovery Inhibit System Recovery Mas in the Browser Ecliftratisa Over Alternative Protocol Multi-hop Proxy Poroc	101 42 26 81 309 61 61 61 61 150 61 150 61 41 116	25,977 25,977 26,036 26,052 25,997 26,017 26,017 26,017 26,017 25,928 26,017 25,928 26,017 25,928 26,017 25,928	6 6 0 0 1 1 1 1 0 0 0 0 0 0	3,918 3,912 3,912 3,918 3,918 3,918 3,918 3,918 3,917 3,917 3,917 3,917 3,917 3,918 3,918 3,918	1 1 1 1 1 8 6 6 6 6 6 6 2 2 4 1 5	49 49 49 49 49 42 44 44 44 44 44 48 46 49 45	(all) siandbox+report sandbox+report sandbox+report sandbox+report sandbox+report (all) sandbox+report (all) sandbox+report sandbox+report sandbox+report sandbox+report	0.031667893 7.16629 0.162536612 1.03E30612 0.0385245941 4.966219 0.0127993 0.022796386 3.07E-75 0.024410287 8.62E-22 0.138137537 5.61E-19	
1499 1499 1566.002 1513 1080 1021.001 1490 1490 1490 1490 1490 1490 1490 1	Third Shared Contest Remote Decktop Potocol Inhibit System Recovery Inhibit System Recovery Mas in the Browser Exfiltration Over Alternative Protocol Multi-kop Proxy Proxy Proxy Hidden Window	101 42 26 81 309 61 61 61 61 41 150 61 41 116 26 2	25,977 25,977 25,977 25,036 25,599 25,569 26,017 26,017 26,017 26,017 25,928 26,017 25,928 26,017 25,962 26,037 25,962 26,052	6 6 0 0 1 1 1 1 1 0 0 0 0 0 0 516	3,918 3,912 3,912 3,912 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,918	1 1 1 1 8 6 6 6 6 6 6 6 4 1 1 3 5 0 2	49 49 49 49 42 44 44 44 44 44 44 44 44 45 46 49 45 50 48	(all) siandbox+report (all) statis-report sandbox+report sandbox+report sandbox+report (all) sandbox+report (all) sandbox+report sandbox+report sandbox+report sandbox+report sandbox+report sandbox+report	0.031667893 7.168-29 0.162536612 1.038-30 0.048237509 0.385245941 4.968-19 0.0127993 0.22796386 3.07E-75 0.024410287 8.62E-22 0.138137537 5.61E-19 0 0.2278645	
1499 1499 1566.002 1513 1080 1021.001 1490 1490 1490 1490 1185 1048 1090.003 1056.003 1185 1553.004 1001	Tair Shared Contest Faurt Enclose Protocol Lability System Recovery Lability System Recovery Lability System Recovery Lability System Recovery Man in the Recovery Lability System Recovery Man in the Recovery Lability System Recovery Reco	101 42 26 81 61 61 150 61 41 116 26 26 28 907 48	25,977 25,977 25,036 26,032 25,997 25,997 25,979 26,017 26,017 25,928 25,017 25,928 25,017 25,928 25,017 25,928 25,017 25,928 25,017 25,9200 25,9200 25,9200 25,9200 25,9200 25,9200 25,9200 25,9200 25,9200	6 6 0 0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0	3,918 3,912 3,912 3,918 3,918 3,918 3,918 3,918 3,918 3,917 3,917 3,917 3,917 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,918	1 1 1 8 6 6 6 6 2 2 4 1 5 0 2 1 3	49 49 49 49 49 49 42 44 44 44 44 44 44 44 45 50 50 45 50 48 48 49 47	(all) similax+report annihax+report annihax+report annihax+report annihax+report (all) annihax+report (all) annihax+report annihax+report annihax+report annihax+report annihax+report annihax+report annihax+report annihax+report annihax+report annihax+report	0.031667893 7.168-29 0.162536612 1.038-30 0.048237909 0.385245941 4.968-19 0.0127993 0.22796386 3.07E-75 0.024410287 8.62E-22 0.138137537 5.61E-19 0 2.28E-65 0.969842287	
1499 1499 1556.002 1513 1080 1021.001 1490 1490 1490 1490 1490 1490 1490 1	Tairi Sharid Cantari Renard Disking Protocid Lahki Sytan Recovery Lahki Sytan Recovery Lahki Sytan Recovery Man in the Browsre Echlimatic Ore Network Protocid Mali Sang Proxy Proxy Proxy Proxy Proxy Proxy Data Brooding Land Record Conflocat Data Checkang Lahki Andrea Data Checkang Data Checkang	101 42 26 81 61 61 61 61 41 41 66 26 2 807 48 807 48 11 25	25,977 25,977 26,036 26,052 25,997 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,016 26,052 26,052 26,056 25,271 26,030 25,261 26,036 25,271 26,036 26,037 25,962 26,036 26,037 26,036 26,037 26,036 26,037 26,036 26,037 26,036 26,037 26,036 26,037 26	6 6 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0	3,918 3,912 3,912 3,912 3,918 3,918 3,918 3,918 3,918 3,918 3,917 3,917 3,917 3,917 3,917 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,912 3,918 3,912 3,918 3,	1 1 1 8 6 6 6 6 7 2 4 4 1 5 0 2 2 1 3 0 0 2 2	49 49 49 49 49 49 49 44 44 44 44 44 44 4	(all) sandbox+report sandbox+report sandbox+report sandbox+report (all) sandbox+report (all) sandbox+static (all) sandbox+static (all) sandbox+report sandbox+report sandbox+report sandbox+static sandbox+static sandbox+static sandbox+report sandbox+report	0.031667893 7.168-29 0.162536612 1.038-30 0.048237509 0.048237509 0.0127993 0.022796386 3.07E-75 0.024410287 8.62E-22 0.138137537 5.61E-19 0 0 2.28E-65 0.969842387 0 0.02825449 0.0122249 0.0122249 0.0122249 0.0122249 0.0122249 0.0122249 0.01229 0.	
1499 1499 1556.002 1513 1080 1021.001 1490 1490 1490 1490 1490 1490 1490 1	Tairi Sharid Cantari Renard Disking Protocid Lahki Sytan Recovery Lahki Sytan Recovery Lahki Sytan Recovery Man in the Browsre Echlimatic Ore Network Protocid Mali Sang Proxy Proxy Proxy Proxy Proxy Proxy Data Brooding Land Record Conflocat Data Checkang Lahki Andrea Data Checkang Data Checkang	101 422 26 81 309 61 61 61 61 41 41 41 41 26 26 280 7 48 11 25 25 525	25,977 25,977 26,036 26,052 25,997 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,016 26,052 26,052 26,056 25,271 26,030 25,261 26,030 25,261 26,030 26	6 6 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0	3,918 3,912 3,912 3,912 3,918 3,918 3,918 3,918 3,918 3,918 3,917 3,917 3,917 3,917 3,917 3,918 3,918 3,918 3,918 3,918 3,918 3,918 3,912 3,918 3,912 3,918 3,	1 1 1 8 6 6 6 6 6 6 6 2 2 4 1 5 0 2 2 1 3 0 0	49 49 49 49 49 49 49 44 44 44 44 44 44 4	(all) sandbox-report sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport (all) sandbox-sreport (all) sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport (all) sandbox-sreport (all) sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport sandbox-sreport	0.031667893 7.168-29 0.162536612 1.038-30 0.048237509 0.048237509 0.0127993 0.022796386 3.07E-75 0.024410287 8.62E-22 0.138137537 5.61E-19 0 0 2.28E-65 0.969842387 0 0.02825449 0.0122249 0.0122249 0.0122249 0.0122249 0.0122249 0.0122249 0.01229 0.	
1499 1499 1499 1499 1566.002 1513 1080 1021.001 1490 1490 1490 1490 1490 1490 1564.003 1554.003 1554.003 1554.004 1554.004 1556.004 1562.004 1562.004 1562.004 1562.004	Tatri Shard Contant Fanti Shard Contant Renover Dekking Postcol Labels System Recovery Labels System Recovery Man in the Bower Mark Shard Shard Shard Shard Shard Proxy Proxy Proxy Data Bog Proxy Proxy Data Bog Postcol Proxy Data Bog Postcol Data Bog Postcol Dat	101 42 26 81 61 61 61 61 41 41 66 26 2 807 48 807 48 11 25	25,977 25,977 26,035 26,035 25,769 26,017 26,017 26,017 26,017 25,928 26,017 25,928 26,037 25,962 26,037 25,965 25,051 25,053 26,053 26,053 26,053	6 6 0 0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0	3.918 3.912 3.912 3.912 3.918 3.918 3.918 3.918 3.918 3.917 3.917 3.917 3.917 3.917 3.918 3.915 3.	1 1 1 1 1 1 1 1 8 6 6 6 6 6 2 2 4 1 1 3 0 2 2 2 2 2 2 2 2 1 1 3 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	49 40 49 49 42 42 44 44 44 44 44 44 44 44 44 45 50 50 50 48 48 48 48 48 48 48 48 49 49 49 40	(all) sandievsergort sandlitos sergort sandlitos sergort sandlitos sergort sandlitos sergort (all) sandibos sergort (all) sandhos sergort sandhos sergort sandhos sergort sandhos sergort sandhos sergort sandhos sergort sandhos sergort sandhos sergort anndhos sergort anndhos sergort sandhos sergort sandhos sergort sandhos sergort sandhos sergort sandhos sergort	0.031667893 7.662-29 0.162536612 1.038-30 0.048273909 0.385235941 4.9662-19 0.0127993 0.22796386 3.0727-55 0.024110287 8.662-22 0.024410287 1.3182-14 0.018127449 0.018127449 0.01822449 0.01822449 0.01822449 0.01822449 0.059678359 1.118-25 8.17E-09 0.559412263	
1499 1499 1499 1499 1499 1562.002 1513 1080 1021.001 1490 1490 1490 1183 1090 1184 1090 11553.004 1552.004 1562	Tarit Shard Content Tarit Shard Content Research Tokish Photod Ishiha System Recovery Ishiha System Recovery Ishiha System Recovery Tellination Ore and Party Part	101 422 26 81 309 61 61 61 150 61 41 116 26 6 2 80 7 80 80 81 81 81 82 5 25 25 25 22 100 5 9 21	25,977 25,977 26,036 26,036 25,769 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,017 26,037 26,030 26,053 26,055 25,566 25,566 25,568 26,055 25,566 25,566 25,576 26,057 26,057 26,017 26	6 6 0 0 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0	3.918 3.912 3.912 3.912 3.918 3.918 3.918 3.918 3.918 3.917 3.917 3.917 3.917 3.917 3.918 3.	1 1 1 1 8 6 6 6 6 6 7 2 4 1 1 5 0 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1	49 40 40 49 49 49 42 44 44 44 44 44 44 44 45 50 49 49 47 50 47 50 48 48 48 48 49 49 49 49 49 49 49 49 49 49 49 49 49	(all) sandbox-report sindbox-report sindbox-report sindbox-report sindbox-report (all) sandbox-report (all) sandbox-report (all) sandbox-report sandbox-report sandbox-report sandbox-report sindbox-report sindbox-report sindbox-static (all) sandbox-static (all) sandbox-static	0.031667383 7.165:29 0.162536612 1.038:36 0.048237360 0.0385245941 4.058524594 0.0385245941 4.058524594 0.038524594 0.038524594 0.03852459 0.03852550 0.03852550 0.03852550 0.038525550 0.03852550 0.03855550000000000000000000000000000000	
1499 1499 1499 1499 1490 1556.002 1513 1080 1021.001 1490 1490 1490 1490 1490 1185 1090.003 1090 1554.003 1132 1552.004 1562.004	Taris Sharka Content Concerne Disking Protection Linksh System Recovery Linksh System Recovery Linksh System Recovery Tellinarian Orer Ammunic Protocol Malik Sop Process Proceedings of the Content of the Content Process Proceedings Process Proceedings Process Process Proceedings Process Process Proceedings Process Process Process Proceedings Process Process Process Proceedings Process Process Process Proceedings Process Process Process Process Process Process Process Process Process Proces	101           42           26           81           309           61           61           61           61           150           61           150           61           150           61           61           150           61           116           26           27           2807           240           25           25           25           25           25           25           25           25           25           21           21           21	25,977 25,977 25,977 25,977 25,977 25,979 25,017 26	6 0 0 0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0	3.918 3.912 3.912 3.912 3.913 3.918 3.897 3.	1 1 1 1 1 1 1 1 8 6 6 6 6 6 2 2 4 1 1 3 0 2 2 2 2 2 2 2 2 1 1 3 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	49 49 49 46 49 42 42 44 44 44 44 48 46 49 45 50 48 48 49 47 50 48 48 48 49 49 49 49 49 49 49 49 49 49	(all) sandbox-report and/box-report and/box-report and/box-report and/box-report and/box-report (all) sandbox-report and/box-report	0.031667383 7.165:39 0.162536612 0.0382536612 0.038253780 0.0383254814 0.0383254814 0.0383254814 0.0383254814 0.0383254814 0.0383254814 0.038325481 0.039455556 0.039455556 0.03545565665656565656565656565656565656565	
1499 1499 1499 1499 1566.002 1513 1080 1021.001 1490 1490 1490 1490 1490 1490 1564.003 1564.003 1564.003 1553.004 1562.0	Taris Sharka Content Concerne Disking Protection Linksh System Recovery Linksh System Recovery Linksh System Recovery Tellinarian Orer Ammunic Protocol Malik Sop Process Proceedings of the Content of the Content Process Proceedings Process Proceedings Process Process Proceedings Process Process Proceedings Process Process Process Proceedings Process Process Process Proceedings Process Process Process Proceedings Process Process Process Process Process Process Process Process Process Proces	101           42           26           81           309           61           62           26           25           25           25           25           25           25           25           25           21           21     21     21     <	25,977 25,977 25,977 25,977 25,977 25,977 25,979 25,017 25,928 26,017 25,928 26,017 25,928 26,017 25,928 26,017 25,928 26,017 25,926 25,976 25,976 25,966 25,271 25,956 25,956 25,956 25,956 25,957 26,057 25,976 26,057 25,976 25,976 25,976 25,976 25,976 25,976 25,976 25,976 25,976 25,976 25,977 25,978 25,977 25,977 25,977 25,978 25,977 26,077 26	6 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 516 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	3.918 3.912 3.912 3.912 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.915 3.915 3.915 3.915 3.915 3.915 3.915 3.918 3.918 3.918 3.918 3.915 3.917 3.917 3.918	1 1 1 1 1 1 1 1 1 1 1 1 1 1	49 49 49 46 49 49 42 42 44 44 44 44 48 46 49 45 50 50 50 48 48 48 49 49 47 50 49 49 49 49 49 49 49 49 49 49	(all) sandbox-report and/box-report and/box-report and/box-report and/box-report and/box-report (all) sandbox-report and/box-report	0.031667393 7.162.29 0.162536612 1.0382536712 0.0382538700 0.0382538700 0.0382538700 0.0382538700 0.0382538700 0.0382538700 0.0382538700 0.0238102580 0.023810258 0.0398412585 0.0398412555 0.03984125555 0.03984125555 0.0398412555555555555555555555555555	
1499 1499 1499 1499 1566.002 1513 1080 1021.001 1490 1490 1490 1490 1490 1490 1564.003 1564.003 1564.003 1553.004 1562.0	Taris Wand Conner Taris Wand Conner Kenner Dicking Parcel Label System Recovery Habita System Recovery Habita System Recovery Eclimation Our Alexandre Potocol Malita System Fachar Wandow Label Tario (1998) Redder Wandow Label Tario	101           42           26           81           309           61           61           61           61           150           61           150           61           150           61           61           150           61           116           26           27           2807           240           25           25           25           25           25           25           25           25           25           21           21           21           21	25,977 25,977 25,977 25,977 25,977 25,977 25,979 25,017 25,928 26,017 25,928 26,017 25,928 26,017 25,928 26,017 25,928 26,017 25,926 25,976 25,976 25,966 25,271 25,956 25,956 25,956 25,956 25,957 26,057 25,976 26,057 25,976 25,976 25,976 25,976 25,976 25,976 25,976 25,976 25,976 25,976 25,977 25,978 25,977 25,977 25,977 25,978 25,977 26,077 26	6 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 516 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	3.918 3.912 3.912 3.912 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.915 3.915 3.915 3.915 3.915 3.915 3.915 3.918 3.918 3.918 3.918 3.915 3.917 3.917 3.918	1 1 1 4 4 4 1 1 8 6 6 6 6 6 6 6 6 6 6 6 6 2 2 4 4 1 1 3 3 0 0 2 2 2 2 1 1 3 3 3 3 3 3	49 49 49 49 40 40 44 44 44 44 44 44 44 44	(all) static-separt (all) static-separt	0.031667393 7.165:29 0.162536612 1.038-30 0.0482137800 0.0482137800 0.0482137800 0.04852437800 0.0127993 0.0127993 0.0127993 0.0127937 0.038524591 0.0127947 0.02410257 0.024410257 0.024410257 0.038242450 0.03949421357 0.038242450 0.03824450 0.038245000000000000000000000000000000000000	
1499 1566.002 1513 1513 1000 1000 1000 1000 11400 1490 1	Taris Sharia Contan Concern Exclare Protocol Indust System Recovery Indust System Recovery Indust System Recovery Exclusions Over Alexandre Vennool Markin Sop Prays Pray Pray Pray Pray Device Protocol Pray Device Protocol Pray Device Protocol Pray Device Protocol Pray Device Protocol Pray Device Protocol Pro	101           42           26           81           309           61           62           26           27           28           25           25           25           25           25           25           21           21     21     21     <	25,977 25,036 25,977 25,036 25,997 25,799 25,799 25,799 25,792 25,029 26,037 25,928 26,037 25,928 26,037 25,908 25,908 25,907 25,908 25,907 25,908 25,907 25,908 25,907 25,007 25,007 26,007 25,007 26	66000000000000000000000000000000000000	3.018 3.012 3.012 3.012 3.012 3.012 3.018 3.019 3.018 3.019 3.018 3.019 3.019 3.019 3.009 3.019 3.0090	1 1 1 1 1 1 1 1 1 1 1 5 6 6 6 6 6 6 7 2 2 1 1 1 3 3 3 3 3 3 3 1 1 1 1 1 1 1 1 1 1 1 1 1	499 499 499 499 494 444 444 444 444 444	(Ld):udioscrepti (Ld):udioscrepti udioscrepti udioscrepti udioscrepti (Ld):udioscrepti (Ld):udioscrepti (Ld):udioscrepti (Ld):udioscrepti (Ld):udioscrepti udioscrepti udioscrepti (Ld):udioscrep	0.031667393 7.162.29 0.162536614 0.0425736614 0.048237390 0.048237390 0.048237390 0.048237390 0.048237390 0.048237390 0.048237390 0.04823740 0.04823740 0.04823740 0.04825444 0.02416237 0.024161237 0.024161237 0.024161237 0.024161237 0.024161237 0.024161237 0.024161237 0.024161237 0.024161237 0.024161237 0.024161237 0.024161237 0.024161237 0.024161237 0.024161237 0.02461237 0.02461237 0.025675139 0.025675519 0.025675139 0.025675150000000000000000000000000000000000	
1499 1566.002 1513 1513 1000 1000 1000 1000 11400 1490 1	Taris Sharia Contan Concern Exclare Protocol Indust System Recovery Indust System Recovery Indust System Recovery Exclusions Over Alexandre Vennool Markin Sop Prays Pray Pray Pray Pray Device Protocol Pray Device Protocol Pray Device Protocol Pray Device Protocol Pray Device Protocol Pray Device Protocol Pro	101           42           26           81           309           61           61           61           41           116           25           22           25           22           210           211           21           21           21           21           21           3           6           7           8           3           6           7           2	25,977 26,036 26,052 25,977 25,977 25,977 25,979 25,979 25,979 25,979 25,979 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,977 25,978 25,978 25,978 25,978 25,977 25,978 25,978 25,978 25,978 25,978 25,977 25,978 26,977 26,977 26,979 26,977 26	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3.918 3.912 3.912 3.912 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.915 3.915 3.915 3.915 3.915 3.915 3.915 3.918 3.918 3.918 3.917 3.918	1 1 1 1 1 1 1 1 1 1 1 1 1 1	499 499 461 462 463 464 464 464 464 464 464 464 464 464	(Ld):uddesrepet (Ld):uddesrepet uddesrepet uddesrepet uddesrepet (Ld):uddesrepet (Ld):uddesrepet uddesrepet (Ld):uddesrepet uddesrepet	0.031667393 7.16529 0.1025306116 0.0125306116 0.048237390 0.048237900 0.048237900 0.024812390 0.024812390 0.024810390 0.02481039 0.0	
1499 1566.002 1513 1513 1513 1513 1513 151 151 151 15	Taris Shork Conner Facts Shork Conner Kenner Dekking Parked Hahdt System Recovery Hahdt System Recovery Hahdt System Recovery Estimation Dora Abensity Parked Haldt Say Press Data Bacoling Handt Rock Conference Data Bacoling Handt Rock Conference Handt Rock Conference Handt Rock Addition Handt Rock Addition Handt Rock Mathy System Forend Handt Rock Mathy Network Many Disource Forent Handt Rock Mathy Network Many Disource Forent Handt Rock Mathy Network Many Disource Forent Handt Rock Mathy Network Many Disource Forent Network Many Disource Cock Signing Network Many Disource Network Many D	$\begin{array}{c} 101\\ 412\\ 26\\ 811\\ 309\\ 61\\ 150\\ 61\\ 150\\ 61\\ 41\\ 116\\ 26\\ 22\\ 20\\ 807\\ 48\\ 111\\ 25\\ 25\\ 122\\ 210\\ 6\\ 5\\ 21\\ 12\\ 21\\ 21\\ 21\\ 21\\ 21\\ 21\\ 21\\ 21$	25,977 25,036 25,977 25,036 25,997 25,799 25,799 25,799 25,792 25,029 26,037 25,928 26,037 25,928 26,037 25,908 25	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3018 3012 3012 3012 3012 3012 3012 3018 3017 3017 3017 3017 3017 3017 3017 3017	1 1 1 4 1 1 8 6 6 6 6 6 6 6 6 6 6 6 7 2 2 2 2 2 2 2 2 2 2 2 2 2	40 49 49 49 49 49 49 49 49 44 44 44 44 44	(d)) undersrepert (undersrepert undersrepert (d)) undersrepert (d)) undersrepert (d)	0.031667383 7.166239 0.10103824 0.01203824 0.01823790 0.01823790 0.01823790 0.01827993 0.01827993 0.01827993 0.01827993 0.01827993 0.012793 0.012	
1499 1556.002 1513 1080 1071.001 1490 1490 1490 1490 1490 1490 1490 1	Taris Shork Conner Facts Shork Conner Kenner Dekking Parked Hahdt System Recovery Hahdt System Recovery Hahdt System Recovery Estimation Dora Abensity Parked Haldt Say Press Data Bacoling Handt Rock Conference Data Bacoling Handt Rock Conference Handt Rock Conference Handt Rock Addition Handt Rock Addition Handt Rock Mathy System Forend Handt Rock Mathy Network Many Disource Forent Handt Rock Mathy Network Many Disource Forent Handt Rock Mathy Network Many Disource Forent Handt Rock Mathy Network Many Disource Forent Network Many Disource Cock Signing Network Many Disource Network Many D	101           422           26           81           309           61           61           41           16           22           22           22           22           2307           441           116           25           25           6           70           7           7           7           7           7           7           70           70	25,977 25,076 25,077 25,076 25,997 25,998 25,997 25,998 25,997 25,998 25,997 25,998 25,997 25,998 25,997 25,998 25,997 25,998 25,997 25,988 25,997 25,988 25,997 25,988 25,997 25,988 25,997 25,988 25,997 25,988 25,997 25,998 25,997 25,988 25,997 25,988 25,997 25,988 25,997 25,999 25,997 25,998 25,997 25,998 25,997 25,998 25,997 25,999 25,997 25,999 25,997 25,998 25,997 25,998 25,997 25,999 25,999 25,999 25,999 25,997 25,998 25,997 25,999 25,997 25,999 25,99	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3018 3012 3012 3012 3012 3012 3018 3018 3018 3018 3018 3018 3018 3018	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	49 49 49 46 49 42 44 44 44 44 44 44 44 45 50 50 40 40 40 40 40 40 40 40 40 4	(d)) undersrepert (undersrepert sundersrepert undersrepert (d)) undersrepert (d))	0.011667393 7.1662-397 7.1662-397 1.0082-30 0.018237509 0.0382354841 4.5621-398 4.5621-399 0.018237509 0.018237509 4.5621-399 5.0121-109 5.0121-109 5.0121-109 0.022246 0.01822440 0.0182440 0.0184400 0.0184400 0.0184400 0.0184400 0.0184400 0.0184400 0.0184400 0.0184400 0.0184400 0.0184400 0.0184000 0.0184000 0.0184000 0.01840000 0.01840000 0.01840000000000000000000000000000000000	
1499 1566.002 151 151 160 1621.001 1621.001 1621.001 164 164 164 164 164 164 164 164 164 16	Taris Wards Consur Taris Wards Consur Kenner Tecking Pracead Landa Cystera Recovery Handa System Recovery Handa System Recovery Fellmanne Our Alexandre Protected Pellmanne Our Alexandre Protected Wardsong Protection Technic Markow Data Electronic Markow Data Stream Stream Data Stream Dat	101           422           26           81           64           61           61           61           61           11           25           27           2807           441           111           25           122           210           5           21           22           23           36           21           22	25977 25077 25076 25977 25077 25	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3018 3012 3012 3012 3012 3012 3018 3018 3018 3018 3018 3018 3018 3018	1 1 1 4 1 1 8 6 6 6 6 6 6 6 6 6 6 6 7 2 2 2 2 2 2 2 2 2 2 2 2 2	40 40 40 40 40 40 40 40 40 40 40 40 40 4	(d)) under sepert (d)) under sepert subserverport ausback report (d)) under sepert (d)) under seper	0.011667393 1.1462-39 1.1462-39 1.0382-39 0.038234941 0.038234941 0.038234941 0.038234941 0.038234941 0.038234941 0.038234941 0.02796386 0.02796386 0.02796386 0.02796386 0.02967310 0.0296730 0.0296730 0.0296730 0.0296730 0.0296730 0.0296730 0.0296730 0.0296730 0.0296730 0.029730 0.02967300 0.02967300 0.02967300 0.02967300 0.02967300 0.0296730	
1499 1566.002 1513 1080 1071.001 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1554.004 1554.004 1554.004 1554.004 1554.004 1554.004 1554.004 1554.004 1554.004 1554.004 1554.004 1554.004 1554.004 1554.004 1554.004 1554.004 1555.004 1557.002 1557.002 1573	Taris Wards Consur Taris Wards Consur Kenner Tecking Parker Lahak System Recovery Hahak System Recovery Hahak System Recovery Heat and Barrier Heat and Barrier Heat and Barrier Heat and Barrier Heat and Barrier Heat and Barrier Heat And System Frenzil Dan de Kenzins Heat Andrey System Frenzil Dander & Madh System Frenzil Dander & Mathematica Network Naur Decorery Color Spring Data Angemetric Copyneght Data Account Mangelation Account Mangelation Account Mangelation Account Mangelation	$\begin{array}{c c c c c c c c c c c c c c c c c c c $	254977 254977 254976 254977 254976 254977 254978 25497 254978 254998 254978 254998 254978 254998 25499 254998 254998 25499 254998 254998 254998 254998 254998 254998 25499 254998 25499 254998 25499 254998 25499 254998 25499 254998 25499 254998 254998 25499 25	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3.012 3.012 3.012 3.012 3.012 3.012 3.012 3.012 3.012 3.012 3.018 3.018 3.017 3.007 3.007 3.007 3.007 3.007 3.007 3.007 3.007 3.007 3.007 3.	1 1 1 1 4 4 4 1 1 1 4 4 1 1 1 1 4 4 1	40 40 40 40 40 40 40 40 40 40 40 40 40 4	(d)) under sepert authors report authors report (d)) under sepert (d)) under sepert	0.0014627893 1.1462.200 1.0382.3760 0.038237890 0.038237890 0.038237890 0.038237890 0.038237890 0.02790386 0.02790386 0.02791208 1.111124 0.018278 0.029078159 0.0290780 0.029078159 0.02907859 0.02907859 0.02907859 0.02907859 0.02907	
1499 1556.002 1513 1080 1021.001 1021.001 1021.001 1490 1490 1490 1490 1490 1490 1490 1	Taris Bande Cassar Taris Bande Cassar Kanon Factor Parkar Lahak System Recovery Lahak System Recovery Harding Wang Sin Bander Erffinnten Oer Alternative Protected Herding Wang Sin Bander Herding Wang Sin Bander Harding Wang Sin Bander Haritton Bander Harding W	$\begin{array}{c c} 101\\ 42\\ 2\\ 3\\ 6\\ 8\\ 9\\ 9\\ 9\\ 9\\ 9\\ 9\\ 9\\ 9\\ 9\\ 9\\ 9\\ 9\\ 9\\$	25,977 25,977 26,035 25,977 25,977 25,077 25	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3018 3012 3012 3012 3012 3012 3012 3018 3018 3018 3018 3018 3018 3018 3018	1 1 1 1 1 1 1 1 1 1 1 1 1 1	40 40 40 40 40 40 40 40 40 40 40 40 40 4	(d)) under separation of the s	0.011467393 1.1462-39 1.1462-39 1.0382-30 0.04827399 0.038234841 0.04827399 0.038234841 0.04827399 0.038234841 0.04827399 0.038234841 0.04827399 0.03824841 0.03824841 0.038424734 0.038441257 0.038741257 0.039744019574 0.03974401957 0.03974401957 0.03974400	
1499 1556:002 1533 1080 1071.001 1071.001 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1490 1535 1037 1535 1037 1555 1037 1555 1037 1555 1037 1555 1037 1555 1037 1555 1037 1555 1037 1555 1037 1135	Taris Nonie Comer Taris Nonie Comer Recent Postej Pracod Label System Recovery Habel System Recovery Habel System Recovery Heat System Recovery Heat System Recovery Heat System Present Comerce System Present Data Recovery Heat		259773 25977 26036 25977 26036 25987 2508 2508 2508 2508 2508 2508 2508 2508	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3018 3012 3012 3012 3012 3012 3018 3018 3018 3018 3018 3018 3018 3018	1 1 1 4 1 1 4 4 1 1 8 6 6 6 6 6 6 6 7 2 2 2 2 2 2 1 1 3 3 3 3 3 3 3 3 3 3 3 3 3	49 49 40 40 40 40 40 40 40 40 40 40 40 40 40		0.0014627893 0.0014627893 0.12356212 10382-30 0.048237800 0.048237800 0.048237800 0.048237800 0.048237800 0.0229931 0.2294386 0.0122993 0.022993 0.022993 0.022993 0.022993 0.022993 0.022993 0.022993 0.0229438 0.0012293 0.0229438 0.0012293 0.0229438 0.0012293 0.0229438 0.0012293 0.001299 0.001299 0.001299 0.001299 0.001299 0.00129 0.001299 0.001299 0.001299 0.00129 0.001299 0.001299 0.001299 0.00129 0.00129 0.001299 0.00129 0.00129 0.00129 0.001299 0.00129	
1499 1499 1556.002 153 1080 1071.001 1490 1490 1490 1490 1490 1490 1490 1	Taris Back Consul Taris Back Consul Consult Science Package Labels System Recovery Labels System Recovery Labels System Recovery Labels System Recovery Labels System Recovery Labels System Recovery Holdse Workshow Handle Star Star Star Handle Sta	101           446           3           361           509           61           61           61           61           61           61           61           61           61           61           61           62           307           307           31           21           22           210           50           51           31           21           22           230           30           7           29           29           20           22           22           22           22           22           22           22           230           301           302           303           304           408           120           120	25,977 25,977 25,077 25,077 25,077 25,077 25,077 25,077 25,077 25,027 25,007	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3018 3012 3012 3012 3012 3018 3012 3018 3018 3018 3018 3018 3018 3018 3018	1 1 1 1 4 4 4 1 1 1 4 4 1 1 1 1 4 4 1	49 49 49 49 49 49 49 49 49 40 44 44 44 44 44 44 44 46 6 49 49 47 47 47 47 47 47 47 47 47 47 47 47 47		0.0016021991 0.0012621991 0.102316612 1.02316612 0.048237900 0.048237900 0.048237900 0.04823790 0.0127993 0.0219032 0.0127993 0.02191032 0.0121993 0.0121993 0.0121993 0.0121993 0.0121993 0.0121993 0.0121917 0.0121917 0.0121920 0.0121917 0.012219200 0.01221920 0.01221920	
1499 1566:002 1573 1080 1080 1080 1080 1080 1080 1087 10	Taris Bande Consur Taris Bande Consur Kenner Tecking Parker Lahde System Recovery Lahde System Recovery Harde System Recovery Header Wender Berlinstein Ger Alternative Protocol Wender State System Freedul Data (State State State State State State Data (State State State State State State State Data (State State State State State State State State Data (State State State State State State State State Data (State State State State State State State State State Data (State State State State State State State State Data (State State State State State State State State Data) (State State State State State State State State Data) (State State	101           436           436           367           369           61           61           61           61           61           61           61           61           61           61           61           61           61           61           61           61           61           70           71           71           72           73           74           75           71           71           73           74           75           71           73           74           75           71           73           74           75           75           71           75           75           76           79           79           70           70           70	25,977 36,056 25,977 36,052 25,977 36,052 25,970 36,057	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3018 3012 3012 3012 3012 3018 3012 3018 3018 3018 3018 3018 3018 3018 3018	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	40 40 40 40 40 40 40 40 40 40 40 40 40 4		0.0164200 0.01164200 0.015254642 0.015254642 0.015254642 0.015256642 0.01525664 0.0152566 0.01526 0.015266 0.015266 0.015266 0.01526 0.0	
1499 1499 1566.002 153 153 153 153 153 153 153 153 153 160 160 160 164 169 164 169 164 169 164 169 164 164 164 164 164 164 164 164 164 164	Taris Wards Consur Taris Wards Consur Research Texts proceedings of the second label System Recovery Habits System Recovery Habits System Recovery Habits System Recovery Habits System Recovery Habits System Forward Data Theorem System Forward Data Theorem System Forward Data System System Forward Data System System Forward Data System Forward D	101         101           3         342           4         42           4         42           4         42           4         42           4         42           4         42           5         309           5         309           4         44           4         44           4         44           4         46           4         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           47         7           47         7           49         7           40         7           41         41           42         22           43         44           44         44           44         44	25977 26076 25977 250777 250777 250777 250777 250777 250777 250777 250777 250777	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3018 3012 3012 3012 3012 3012 3012 3012 3018 3018 3018 3018 3018 3018 3018 3018	1 1 1 4 1 1 4 4 1 1 8 6 6 6 6 6 6 6 7 2 2 2 2 2 2 1 1 3 3 3 3 3 3 3 3 3 3 3 3 3	40 40 40 40 40 40 40 40 40 40 40 40 40 4		0.0116/2709 0.0116/2709 0.01253/06/2 0.01253/06/2 0.01253/06/2 0.01253/06/2 0.01253/06/2 0.01259/07 0.0125	
1499 1556-002 1533 1533 1533 1533 1535 1535 1535 1535 1535 1490 1490 1490 1490 1490 1490 1490 1490 1545 1645 1552 1545 1552 1545 1552 1545 1555 15	Taris Wards Consur Taris Wards Consur Consure Textury Protocol Labels System Recovery Labels System Recovery Market System Recovery Heads Wards Consure Federation Orer Alements Heads Wards Consult Data (Stematistic Constitution) Heads Wards Constitution) Data (Stematistic Constitution)	101         101           4         101           5         101           5         101           105         101           106         101           107         101           108         101           109         101           100         101           101         101           102         101           103         102           104         101           105         101           105         101           105         101           106         101           107         101           108         101           109         101           100         101           101         101           101         101           101         101           101         101           102         101           103         101           104         101           105         101           106         101           107         101	25977 26036 25977 26036 25977 26037 25970 25077 25027 25077 25075 25	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3.018 3.012 3.002 3.	1   1   1   1   1   1   1   1   1   1	40 40 40 40 40 40 40 40 40 40 40 40 40 4		0.3164709 0.3153462 0.3153462 0.3153462 0.3153462 0.3153462 0.3153462 0.3153462 0.315346 0.315346 0.315346 0.315476 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576 0.315576	
1499 1499 1556,002 155 155 155 169 169 169 169 169 169 169 169 169 169	Taris Nonie Conner Taris Nonie Conner Kenner Tockie Protecki Label System Recovery Halak System Recovery Halak System Recovery Halak System Recovery Heat System Recovery Heat System Recovery Heat System System Frenzel Data Recovery Heat Recovery Heat System System Frenzel Data Recovery Heat System Recovery Heat System Heat System Heat System Heat System Heat System Heat System Heat System Heat System	100         100           101         14           102         16           103         10           104         11           105         10           106         10           107         10           108         10           109         10           100         10           101         11           101         11           101         11           101         11           101         11           101         11           101         11           101         11           101         11           102         101           103         101           104         101           105         101           104         101           105         101           106         101           107         101           108         101           108         101	25,977 25,070 25,077 25,770 25,770 25,770 25,770 25,770 25,770 25,770 25,077 25,077 25,077 25,077 25,077 25,077 25,077 25,077 25,077 25,076 25,077 25	66 67 67 67 67 67 67 67 67 67 67 67 67 6	3.018 3.012 3.003 3.0000 3.0000 3.0000 3.0000 3.0000 3.0000 3.0000 3.0000 3.00000 3.00000 3.00000 3.00000000	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	40 40 40 40 40 40 40 40 40 40		0.0114270 1.01253412 1.01253412 1.01253412 1.01253412 1.01253412 1.0125341 1.0125	
1499 1499 1566.002 151 150 151 151 151 152 160 160 160 160 160 160 160 160 160 160	Taris Banka Cassar Taris Banka Cassar Banka December 2014 (1997) Annual Cassar Cassar Cassar Estimated December 2014 (1997) Annual Person Estimated December 2014 (1997) Annual Person Hada Wardsan Banka Cassar Hada Wardsan Banka Cassar Hada Wardsan Hada	100         100           101         100           103         100           104         100           105         100           106         100           107         100           108         100           109         100           100         100           101         100           102         100           103         100           104         100           105         100           107         100           108         100           109         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100	25,977 26,036 26,057 25,077 25,770 25,770 25,770 25,770 25,770 25,770 25,770 25,770 25,077 25	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3.018 3.012 3.012 3.012 3.012 3.012 3.012 3.012 3.018 3.009 3.	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	40 40 40 40 40 40 40 40 40 40 40 40 40 4		0.0116/2002 0.0115/2002 0.01523/06/2 0.01	
1499 1499 155:500 155:	Taris Bande Cassar Taris Bande Cassar Kenner Tecking Package Lahak System Recovery Hahak System Recovery Hahak System Recovery Heat System Recovery Heat System Recovery Heat System Recovery Heat System System Heat System System Heat System System Heat System System Heat System System Heat	101         101           101         101           102         101           103         101           104         101           105         101           106         101           107         101           108         101           108         101           108         101           108         101           108         101           108         101           108         101           108         101           108         101           108         101           108         101           109         101           100         101           101         101           102         101           103         101           104         101           105         101           108         101           109         101           101         11           101         11           101         11	25,977 36,000 35,007 35,000 35,007 35,000 35,007	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3018 3012 3012 3012 3012 3012 3012 3012 3012	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	40 40 40 40 40 40 40 40 40 40		0.0114/2004 0.0114/2004 0.01253/04/200	
1499 1499 153 154 154 154 155 155 165 165 165 165 165 165 165 165	Taris Back Consul Taris Back Consul Consult Factor Packet (1999) A second factor of the second table System Recovery (1990) A second factor of the second Endination Orex Aleman's Packet Endination Orex Aleman's Packet Head Start Constant Back Constant Orex Aleman's Constant Back Constant Back Constant Databack (1990) A second factor of the Databack (1990) A second fa	100         100           101         100           103         100           104         100           105         100           106         100           107         100           108         100           109         100           100         100           101         100           102         100           103         100           104         100           105         100           107         100           108         100           109         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100         100           100	25,977 26,000 25,977 25,007	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3.012 3.	1 1 1 1 1 4 4 4 6 6 6 6 6 6 7 7 7 7 7 7 7 7 7 7 7 7 7	40 40 40 40 40 40 40 40 40 40 40 40 40 4		0.1125002 0.11253022 1.1253022 1.1253022 1.1253022 1.1253022 1.1253022 1.1253022 1.1253022 1.125202 1.12520 1.12520 1.12520 1.12520 1.12520 1.12520 1.111252 1.	
1499 1499 153 154 154 154 155 155 164 155 165 165 165 165 165 165 165 165 165	Taris Back Consur Taris Back Consur Consure Texting Packer Labels System Recovery Labels System Recovery Labels System Recovery Labels System Recovery Labels System Recovery Labels System Recovery Labels Works Labels System System Labels Works Labels Works Labels Labels Works Labels Labels Works Labels La	101         101           111         11           112         111           113         111           114         111           115         111           115         111           115         111           115         111           115         111           115         111           115         111           115         111           115         111           115         111           116         111           117         111           118         111           119         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111	55,977 55,977 55,978	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3.918 3.912 3.912 3.912 3.912 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.917 3.	1           1           4           1           4           1           8           6           6           6           7           1           1           1           1	40         40           40         40           40         40           40         40           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           46         45           47         77           47         77           47         77           43         44           44         44           43         43           44         44           45         45           46         45           47         47           47         47           47         47           48         <		0.0112/070 0.01233/022 0.023	
1499 1499 1499 15 15 15 15 15 15 15 15 15 15 15 15 15	Taris Back Consul Taris Back Consul Consult Science (Consult Parker) Label System Recovery Label System Recovery Editoria Ora (Nematic Forceal Editoria Ora (Nematic Forceal) Editoria Ora (Nematic Forceal) Editoria (Nematic Forceal) Edito	101         101           313         32           324         33           325         34           326         35           327         36           328         36           329         36           329         36           329         37           320         37           321         32           321         32           321         32           321         32           321         32           321         32           321         32           321         32           322         32           323         32           324         32           325         32           326         32           327         32           328         32           329         32           320         32           320         32           320         32           320         32           320         32           320         32           320         32	55,977 55,977 55,977 55,977 55,977 55,977 55,977 55,977 55,977 55,977 55,977 55,977 55,977 55,978 55,977 55,978	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3.918 3.912 3.912 3.912 3.912 3.918 3.917 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	49         49           49         44           44         44           44         44           44         44           44         44           44         44           44         44           44         44           46         48           46         48           47         14           48         48           49         99           90         77           47         77           47         77           47         77           47         77           47         77           47         77           50         50           50         50           50         50           50         50           50         50           50         50           50         50           50         50           50         50           50         50           50         50           50         50           50         50           40         <		0.112/00/01 0.112336/2 1.012336/2 1.012336/2 1.012336/2 1.012336/2 0.02356/2 0.02566/2 0.02	
1499 1499 153 154 154 154 155 155 165 165 165 165 165 165 165 165	Taris Back Consur Taris Back Consur Consure Texting Packer Labels System Recovery Labels System Recovery Labels System Recovery Labels System Recovery Labels System Recovery Labels System Recovery Labels Works Labels System System Labels Works Labels Works Labels Labels Works Labels Labels Works Labels La	101         101           111         11           112         111           113         111           114         111           115         111           115         111           115         111           115         111           115         111           115         111           115         111           115         111           115         111           115         111           116         111           117         111           118         111           119         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111         111           111	55,977 55,978 55,978	6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	3.918 3.912 3.912 3.912 3.912 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.918 3.917 3.	1           1           4           1           4           1           8           6           6           6           7           1           1           1           1	49         49           49         49           49         49           46         49           42         44           44         44           44         44           44         44           44         44           48         50           97         77           47         47           48         49           49         <		0.0112/070 0.01233/022 0.023	

 Table A·3
 Technique observed in multiple methods and presence/absence of significant differences between methods (RQ4).



Shota Fujii received his B.E. and M.E. degrees from Okayama University, Japan in 2014 and 2016 respectively. He has been a doctoral student of Graduate School of Natural Science and Technology at Okayama University since 2020. He is working for Hitachi since 2016. His research interests include computer secu-

rity and virtualization technology. He is a member of IPSJ.



**Rei Yamagishi** received his B.E. and M.E. degrees from The University of Electro-Communications in 2017 and 2019 respectively. He is working for Hitachi since 2019. His research interests include computer security and usable security. He is a member of IPSJ.



**Toshihiro Yamauchi** received his B.E., M.E., and Ph.D. degrees in computer science from Kyushu University, Japan, in 1998, 2000, and 2002, respectively. In 2001, he was a Research Fellow with Japan Society for the Promotion of Science. In 2002, he became a Research Associate with the Faculty of Information

Science and Electrical Engineering, Kyushu University. In 2005, he became an Associate Professor with the Graduate School of Natural Science and Technology, Okayama University. Since 2021, he has been serving as a Professor with Okayama University. His research interests include operating systems and computer security. He is a member of IPSJ, IEICE, ACM, IEEE, and USENIX.