Electronic Preprint for Journal of Information Processing Vol.30

Regular Paper

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

Shota Fujii[1,2,a)] Rei Yamagishi[1] Toshihiro Yamauchi[3]

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® 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 on-premise 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 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-

1 Yokohama Research Laboratory, Hitachi, Ltd., Yokohama, Kanagawa 244–0817, Japan
2 Graduate School of Natural Science and Technology, Okayama University, Okayama 700–8530, Japan
3 Faculty of Natural Science and Technology, Okayama University, Okayama, 700–8530, Japan
a) shota.fujii.xh@hitachi.com

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-of-context 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 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.

Table 1 Data overview.

Information source	Number of reports	Number of techniques	
		Unique	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

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).

Combination			Average	Mean	Max.	min.	Number of reports
JoeSandbox	Hybrid Analysis	Hatching Triage					
✓	✓		0.146	0.143	0.350	0.024	1,125
✓		✓	0.080	0.071	0.500	0.023	11,882
	✓	✓	0.144	0.125	0.500	0.029	1,012
✓	✓	✓	0.042	0.035	0.154	0.019	1,012

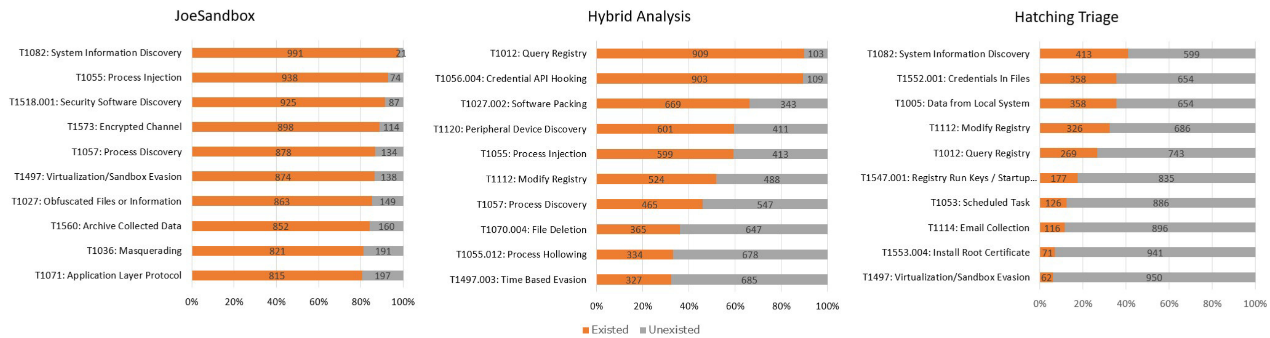

Fig. 1 Top 10 MITRE ATT&CK Technique for each sandbox.

Table 3 Analysis environment for each sandbox.

Analysis Environment	Online sandbox		
	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.

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

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

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

TID	Technique	JoeSandbox		Hybrid Analysis		Hatching Triage		p-value	Statistical significance
		exist	unexist	exist	unexist	exist	unexist		
T1082	System Information Discovery	991	21	207	805	413	599	2.29E-285	✓
T1055	Process Injection	938	74	598	414	0	1,012	0	✓
T1518.001	Security Software Discovery	925	87	53	959	3	1,009	0	✓
T1573	Encrypted Channel	898	114	223	789	0	1,012	0	✓
T1057	Process Discovery	878	134	465	547	0	1,012	0	✓
T1497	Virtualization/Sandbox Evasion	874	138	241	771	62	950	0	✓
T1027	Obfuscated Files or Information	863	149	7	1,005	0	1,012	0	✓
T1560	Archive Collected Data	852	160	3	1,009	0	1,012	0	✓
T1036	Masquerading	821	191	89	923	0	1,012	0	✓
T1071	Application Layer Protocol	815	197	0	1,012	0	1,012	0	✓
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	✓
T1027.002	Software Packing	769	243	669	343	0	1,012	1.18E-301	✓
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	✓
T1070.004	File Deletion	133	879	365	647	9	1,003	1.81E-101	✓
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	✓
T1552.001	Credentials In Files	58	954	2	1,010	358	654	3.48E-133	✓
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	✓
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	✓

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

Fig. 2 More than one MITRE ATT&CK Technique was found in the sandbox analysis results.

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

Tactic	Number of existing techniques	Total 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

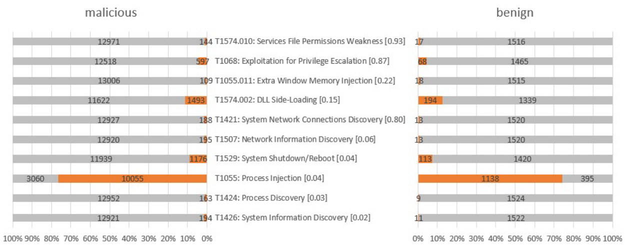

Fig. 3 MITRE ATT&CK Technique for the top 10 p-values.

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 JoeSandbox 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.

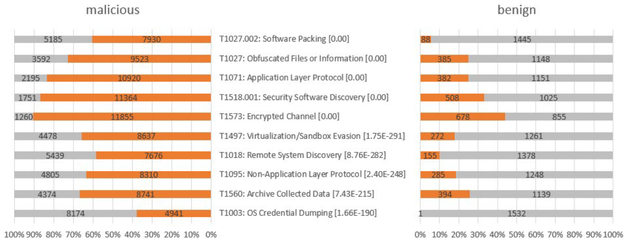

Fig. 4 MITRE ATT&CK Technique for the lower 10 p-values.

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

Fig. 5 MITRE ATT&CK Technique mapped by each technique.

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

TID	Technique	JoeSandbox		Hybrid Analysis		Hatching Triage		Combination	p-value	Statistical significance
		exist	unexist	exist	unexist	exist	unexist			
T1497	Virtualization/Sandbox Evasion	9,577	16,501	2	3,916	4	46	(all) sandbox+static	0	✓
T1497	Virtualization/Sandbox Evasion	9,577	16,501	2	3,916	4	46	(all) sandbox+report	5.99E-06	✓
T1497	Virtualization/Sandbox Evasion	9,577	16,501	2	3,916	4	46	(all) static+report	4.36E-36	✓
T1027.002	Software Packing	8,649	17,429	4	3,914	2	48	(all) sandbox+static	0	✓
T1027.002	Software Packing	8,649	17,429	4	3,914	2	48	(all) sandbox+report	0.000175584	✓
T1027.002	Software Packing	8,649	17,429	4	3,914	2	48	(all) static+report	1.82E-07	✓
T1027	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	2,506	15	35	(all) sandbox+report	0	✓
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	✓
T1518.001	Security Software Discovery	11,428	14,650	3	3,915	2	48	(all) sandbox+report	1.07E-07	✓
T1518.001	Security Software Discovery	11,428	14,650	3	3,915	2	48	(all) static+report	8.17E-09	✓
T1057	Process Discovery	9,569	16,509	99	3,819	7	43	(all) sandbox+static	0	✓
T1057	Process Discovery	9,569	16,509	99	3,819	7	43	(all) sandbox+report	8.45E-16	✓
T1057	Process Discovery	9,569	16,509	99	3,819	7	43	(all) static+report	5.16E-06	✓
T1082	System Information Discovery	15,879	10,199	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	✓
T1082	System Information Discovery	15,879	10,199	2,416	1,502	11	39	(all) static+report	2.51E-08	✓
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	✓
T1569.002	Service Execution	858	25,220	125	3,793	5	45	(all) static+report	0.022133283	✓
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+report	0	✓
T1083	File and Directory Discovery	6,818	19,260	1,748	2,170	12	38	(all) static+report	0.005565762	✓
T1012	Query Registry	7,460	18,618	724	3,194	4	46	(all) sandbox+static	4.45E-40	✓
T1012	Query Registry	7,460	18,618	724	3,194	4	46	(all) sandbox+report	0	✓
T1012	Query Registry	7,460	18,618	724	3,194	4	46	(all) static+report	0.085716776	-
T1033	System Owner/User Discovery	2,845	23,233	201	3,717	5	45	(all) sandbox+static	8.13E-29	✓
T1033	System Owner/User Discovery	2,845	23,233	201	3,717	5	45	(all) sandbox+report	4.35E-260	✓
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	✓
T1115	Clipboard Data	1,955	24,123	238	3,680	1	49	(all) static+report	0.365872328	-
T1059	Command and Scripting Interpreter	3,122	22,956	1,801	2,117	11	39	(all) sandbox+static	0	✓
T1059	Command and Scripting Interpreter	3,122	22,956	1,801	2,117	11	39	(all) sandbox+report	0	✓
T1059	Command and Scripting Interpreter	3,122	22,956	1,801	2,117	11	39	(all) static+report	0.001203964	✓
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	✓
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	File and Directory Permissions Modification	628	25,450	237	3,681	1	49	(all) sandbox+report	0	✓
T1222	File and Directory Permissions Modification	628	25,450	237	3,681	1	49	(all) static+report	0.368942641	-
T1129	Shared Modules	920	25,158	3,392	526	1	49	(all) sandbox+static	0	✓
T1129	Shared Modules	920	25,158	3,392	526	1	49	(all) sandbox+report	0	✓
T1129	Shared Modules	920	25,158	3,392	526	1	49	(all) static+report	1.84E-62	✓
T1564.003	Hidden Window	26	26,052	516	3,402	0	50	sandbox+static	0	✓
T1135	Network Share Discovery	21	26,057	21	3,897	3	47	(all) sandbox+static	6.00E-12	✓
T1135	Network Share Discovery	21	26,057	21	3,897	3	47	(all) sandbox+report	0	✓
T1135	Network Share Discovery	21	26,057	21	3,897	3	47	(all) static+report	5.49E-05	✓
T1489	Service Stop	22	26,056	25	3,893	7	43	(all) sandbox+static	1.81E-15	✓
T1489	Service Stop	22	26,056	25	3,893	7	43	(all) sandbox+report	0	✓
T1489	Service Stop	22	26,056	25	3,893	7	43	(all) static+report	2.97E-22	✓
T1402	Broadcast Receivers	1	26,077	0	3,918	5	45	sandbox+report	0	✓
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	✓
T1560.002	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	✓
T1056.001	Keylogging	4	26,074	532	3,386	1	49	(all) sandbox+report	0	✓
T1056.001	Keylogging	4	26,074	532	3,386	1	49	(all) static+report	0.029476232	✓

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

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

between all combinations of methods ($_3C_2 = 3$ 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·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 complement 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 JoeSandbox, 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 SandPrint [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.

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

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 2022-02-24).

[4] Hybrid Analysis: Free Automated Malware Analysis Service - powered by Falcon Sandbox, available from ⟨https://www.hybrid-analysis.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).

[7] 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).

[8] 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 open-source 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://mitre-attack.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·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 chi-square 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 JoeSandbox.

Table A·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.

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

TID	Technique	JoeSandbox		Hybrid Analysis		Hatching Triage		p-value	Statistical significance
		exist	unexist	exist	unexist	exist	unexist		
T1055	Process Injection	938	74	598	414	0	1,012	0	✓
T1497	Virtualization/Sandbox Evasion	874	138	241	771	62	950	0	✓
T1027.002	Software Packing	769	243	669	343	0	1,012	1.18E-301	✓
T1027	Obfuscated Files or Information	863	149	7	1,005	0	1,012	0	✓
T1518.001	Security Software Discovery	925	87	53	959	3	1,009	0	✓
T1057	Process Discovery	878	134	465	547	0	1,012	0	✓
T1082	System Information Discovery	991	21	207	805	413	599	2.29E-285	✓
T1560	Archive Collected Data	852	160	3	1,009	0	1,012	0	✓
T1573	Encrypted Channel	898	114	223	789	0	1,012	0	✓
T1071	Application Layer Protocol	815	197	0	1,012	0	1,012	0	✓
T1036	Masquerading	821	191	89	923	0	1,012	0	✓
T1095	Non-Application Layer Protocol	744	268	3	1,009	0	1,012	0	✓
T1105	Ingress Tool Transfer	540	472	47	965	0	1,012	6.30E-247	✓
T1078	Valid Accounts	30	982	0	1,012	0	1,012	6.94E-14	✓
T1106	Native API	293	719	4	1,008	0	1,012	5.33E-138	✓
T1203	Exploitation for Client Execution	65	947	34	978	32	980	0.000276521	✓
T1569.002	Service Execution	47	965	5	1,007	0	1,012	1.03E-17	✓
T1574.002	DLL Side-Loading	110	902	0	1,012	0	1,012	2.70E-50	✓
T1546.011	Application Shimming	124	888	0	1,012	0	1,012	7.15E-57	✓
T1543.003	Windows Service	69	943	15	997	23	989	1.91E-11	✓
T1068	Exploitation for Privilege Escalation	27	985	0	1,012	0	1,012	1.48E-12	✓
T1134	Access Token Manipulation	172	840	0	1,012	0	1,012	6.54E-80	✓
T1140	Deobfuscate/Decode Files or Information	579	433	5	1,007	0	1,012	9.15E-307	✓
T1070.006	Timestomp	180	832	0	1,012	0	1,012	7.95E-84	✓
T1218.010	Regsvr32	3	1,009	5	1,007	0	1,012	0.092432672	-
T1218.011	Rundll32	48	964	7	1,005	0	1,012	6.02E-17	✓
T1056	Input Capture	379	633	2	1,010	0	1,012	5.66E-187	✓
T1124	System Time Discovery	271	741	11	1,001	0	1,012	1.48E-120	✓
T1120	Peripheral Device Discovery	9	1,003	601	411	38	974	1.95E-285	✓
T1083	File and Directory Discovery	581	431	18	994	0	1,012	1.80E-296	✓
T1012	Query Registry	289	723	909	103	269	743	2.94E-228	✓
T1070.004	File Deletion	133	879	365	647	9	1,003	1.81E-101	✓
T1087	Account Discovery	227	785	0	1,012	0	1,012	2.81E-107	✓
T1033	System Owner/User Discovery	227	785	16	996	0	1,012	2.83E-94	✓
T1018	Remote System Discovery	691	321	14	998	14	998	0	✓
T1115	Clipboard Data	196	816	3	1,009	0	1,012	4.29E-89	✓
T1529	System Shutdown/Reboot	103	909	0	1,012	0	1,012	4.97E-47	✓
T1070	Indicator Removal on Host	3	1,009	1	1,011	0	1,012	0.173373213	-
T1003	OS Credential Dumping	478	534	52	960	0	1,012	1.48E-205	✓
T1571	Non-Standard Port	367	645	256	756	0	1,012	6.16E-94	✓
T1059	Command and Scripting Interpreter	222	790	4	1,008	13	999	9.41E-91	✓
T1547.001	Registry Run Keys / Startup Folder	208	804	162	850	177	835	0.025182647	✓
T1574.010	Services File Permissions Weakness	5	1,007	3	1,009	0	1,012	0.092432672	-
T1010	Application Window Discovery	501	511	148	864	0	1,012	6.83E-170	✓
T1016	System Network Configuration Discovery	118	894	59	953	0	1,012	6.17E-28	✓
T1113	Screen Capture	34	978	6	1,006	0	1,012	1.35E-11	✓
T1486	Data Encrypted for Impact	19	993	19	993	0	1,012	6.64E-05	✓
T1053	Scheduled Task/Job	183	829	115	897	126	886	1.74E-05	✓
T1562.001	Disable or Modify Tools	695	317	11	1,001	13	999	0	✓
T1112	Modify Registry	39	973	524	488	326	686	5.78E-124	✓
T1005	Data from Local System	453	559	84	928	358	654	1.66E-76	✓
T1114	Email Collection	322	690	122	890	116	896	6.13E-40	✓
T1047	Windows Management Instrumentation	422	590	42	970	0	1,012	7.58E-180	✓
T1222	File and Directory Permissions Modification	64	948	0	1,012	3	1,009	1.16E-26	✓
T1564.001	Hidden Files and Directories	133	879	4	1,008	5	1,007	1.04E-53	✓
T1552.002	Credentials in Registry	232	780	0	1,012	0	1,012	8.08E-110	✓
T1037.005	Startup Items	33	979	0	1,012	0	1,012	3.24E-15	✓
T1189	Drive-by Compromise	1	1,011	0	1,012	0	1,012	0.367758249	-
T1102	Web Service	22	990	0	1,012	32	980	2.61E-07	✓
T1014	Rootkit	39	973	0	1,012	0	1,012	6.95E-18	✓
T1056.004	Credential API Hooking	57	955	902	110	0	1,012	0	✓
T1059.001	PowerShell	22	990	94	918	0	1,012	5.90E-29	✓
T1197	BITS Jobs	1	1,011	0	1,012	1	1,011	0.606330781	-
T1552.001	Credentials In Files	58	954	2	1,010	358	654	3.48E-133	✓
T1007	System Service Discovery	33	979	0	1,012	0	1,012	3.24E-15	✓
T1219	Remote Access Software	54	958	0	1,012	0	1,012	1.33E-24	✓
T1406	Obfuscated Files or Information	6	1,006	0	1,012	0	1,012	0.002449476	✓
T1523	Evade Analysis Environment	1	1,011	0	1,012	0	1,012	0.367758249	-
T1412	Capture SMS Messages	3	1,009	1	1,011	0	1,012	0.173373213	-
T1426	System Information Discovery	3	1,009	0	1,012	0	1,012	0.049639551	✓
T1449	Exploit SS7 to Redirect Phone Calls/SMS	4	1,008	0	1,012	0	1,012	0.018219241	✓
T1448	Carrier Billing Fraud	4	1,008	0	1,012	0	1,012	0.018219241	✓
T1418	Application Discovery	5	1,007	1	1,011	0	1,012	0.029988818	✓
T1409	Access Stored Application Data	1	1,011	0	1,012	0	1,012	0.367758249	-
T1421	System Network Connections Discovery	3	1,009	1	1,011	0	1,012	0.173373213	-
T1422	System Network Configuration Discovery	2	1,010	0	1,012	0	1,012	0.135156976	-
T1430	Location Tracking	5	1,007	1	1,011	0	1,012	0.029988818	✓
T1424	Process Discovery	3	1,009	0	1,012	0	1,012	0.049639551	✓
T1432	Access Contact List	2	1,010	0	1,012	0	1,012	0.135156976	-
T1433	Access Call Log	1	1,011	0	1,012	0	1,012	0.367758249	-
T1507	Network Information Discovery	5	1,007	0	1,012	0	1,012	0.0066826	✓
T1439	Eavesdrop on Insecure Network Communication	2	1,010	0	1,012	0	1,012	0.135156976	-
T1472	Generate Fraudulent Advertising Revenue	1	1,011	0	1,012	0	1,012	0.367758249	-
T1447	Delete Device Data	4	1,008	0	1,012	0	1,012	0.018219241	✓
T1129	Shared Modules	90	922	0	1,012	0	1,012	5.24E-41	✓
T1136	Create Account	16	996	0	1,012	0	1,012	1.03E-07	✓
T1564.002	Hidden Users	12	1,000	0	1,012	0	1,012	5.86E-06	✓
T1049	System Network Connections Discovery	5	1,007	0	1,012	0	1,012	0.0066826	✓
T1499	Endpoint Denial of Service	11	1,001	0	1,012	0	1,012	1.60E-05	✓
T1566.002	Spearphishing Link	5	1,007	1	1,011	0	1,012	0.029988818	✓
T1429	Capture Audio	2	1,010	0	1,012	0	1,012	0.135156976	-
T1080	Taint Shared Content	7	1,005	0	1,012	0	1,012	0.000897249	✓
T1055.011	Extra Window Memory Injection	8	1,004	31	981	0	1,012	1.72E-09	✓
T1547.008	LSASS Driver	5	1,007	0	1,012	0	1,012	0.0066826	✓
T1021.001	Remote Desktop Protocol	1	1,011	230	782	1	1,011	5.13E-107	✓
T1574.001	DLL Search Order Hijacking	1	1,011	0	1,012	0	1,012	0.367758249	-
T1490	Inhibit System Recovery	3	1,009	6	1,006	9	1,003	0.221142869	-
T1185	Man in the Browser	18	994	0	1,012	0	1,012	1.37E-08	✓
T1048	Exfiltration Over Alternative Protocol	5	1,007	0	1,012	0	1,012	0.0066826	✓
T1091	Replication Through Removable Media	9	1,003	0	1,012	3	1,009	0.005139326	✓
T1090.003	Multi-hop Proxy	8	1,004	0	1,012	0	1,012	0.000328447	✓
T1090	Proxy	24	988	2	1,010	10	1,002	2.87E-05	✓
T1564.003	Hidden Window	0	1,012	3	1,009	0	1,012	0.049639551	✓
T1542.003	Bootkit	8	1,004	9	1,003	8	1,004	0.960470399	-
T1053.001	At (Linux)	2	1,010	0	1,012	0	1,012	0.135156976	-
T1547.006	Kernel Modules and Extensions	1	1,011	30	982	0	1,012	4.70E-13	✓
T1553.004	Install Root Certificate	2	1,010	0	1,012	71	941	1.29E-30	✓
T1001	Data Obfuscation	5	1,007	0	1,012	0	1,012	0.0066826	✓
T1562.004	Disable or Modify System Firewall	0	1,012	7	1,005	0	1,012	0.000897249	✓
T1548.002	Bypass User Access Control	4	1,008	1	1,011	2	1,010	0.367030256	-
T1491	Defacement	10	1,002	2	1,010	9	1,003	0.065011494	-
T1564.004	NTFS File Attributes	1	1,011	163	849	0	1,012	1.20E-74	✓
T1135	Network Share Discovery	3	1,009	1	1,011	0	1,012	0.173373213	-
T1553.002	Code Signing	0	1,012	45	967	0	1,012	1.45E-20	✓
T1046	Network Service Scanning	0	1,012	1	1,011	0	1,012	0.367758249	-
T1176	Browser Extensions	1	1,011	0	1,012	0	1,012	0.367758249	-
T1218.005	Mshta	0	1,012	7	1,005	0	1,012	0.000897249	✓
T1413	Access Sensitive Data in Device Logs	3	1,009	0	1,012	0	1,012	0.049639551	✓
T1547.004	Winlogon Helper DLL	0	1,012	1	1,011	7	1,005	0.004565621	✓
T1546.001	Change Default File Association	0	1,012	0	1,012	2	1,010	0.135156976	-
T1098	Account Manipulation	0	1,012	0	1,012	1	1,011	0.367758249	-
T1489	Service Stop	0	1,012	17	995	2	1,010	1.10E-06	✓
T1055.012	Process Hollowing	0	1,012	333	679	0	1,012	3.66E-163	✓
T1055.003	Thread Execution Hijacking	0	1,012	39	973	0	1,012	6.95E-18	✓
T1497.003	Time Based Evasion	0	1,012	326	686	0	1,012	2.45E-159	✓
T1071.001	Web Protocols	0	1,012	161	851	0	1,012	1.46E-74	✓
T1204	User Execution	0	1,012	41	971	0	1,012	8.92E-19	✓
T1137	Office Application Startup	0	1,012	35	977	0	1,012	4.19E-16	✓
T1074.001	Local Data Staging	0	1,012	83	929	0	1,012	8.72E-38	✓
T1053.005	Scheduled Task	0	1,012	115	897	0	1,012	1.23E-52	✓
T1059.003	Windows Command Shell	0	1,012	103	909	0	1,012	4.97E-47	✓
T1036.005	Match Legitimate Name or Location	0	1,012	12	1,000	0	1,012	5.86E-06	✓
T1565	Data Manipulation	0	1,012	50	962	0	1,012	8.35E-23	✓
T1218.007	Msiexec	0	1,012	7	1,005	0	1,012	0.000897249	✓
T1132.001	Standard Encoding	0	1,012	28	984	0	1,012	5.33E-13	✓
T1402	Broadcast Receivers	0	1,012	1	1,011	0	1,012	0.367758249	-
T1420	File and Directory Discovery	0	1,012	1	1,011	0	1,012	0.367758249	-
T1582	SMS Control	0	1,012	1	1,011	0	1,012	0.367758249	-
T1204.002	Malicious File	0	1,012	15	997	0	1,012	2.84E-07	✓
T1070.001	Clear Windows Event Logs	0	1,012	20	992	0	1,012	1.81E-09	✓
T1559.001	Component Object Model	0	1,012	16	996	0	1,012	1.03E-07	✓
T1218	Signed Binary Proxy Execution	0	1,012	1	1,011	0	1,012	0.367758249	-
T1059.005	Visual Basic	0	1,012	14	998	0	1,012	7.79E-07	✓
T1114.001	Local Email Collection	0	1,012	3	1,009	0	1,012	0.049639551	✓
T1222.001	Windows File and Directory Permissions Modification	0	1,012	3	1,009	0	1,012	0.049639551	✓
T1546.007	Netsh Helper DLL	0	1,012	2	1,010	0	1,012	0.135156976	-
T1566.001	Spearphishing Attachment	0	1,012	1	1,011	0	1,012	0.367758249	-
T1560.002	Archive via Library	0	1,012	1	1,011	0	1,012	0.367758249	-
T1056.001	Keylogging	0	1,012	4	1,008	0	1,012	0.018219241	✓
T1048.003	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	0	1,012	1	1,011	0	1,012	0.367758249	-
T1059.007	JavaScript	0	1,012	1	1,011	0	1,012	0.367758249	-
T1055.001	Dynamic-link Library Injection	0	1,012	1	1,011	0	1,012	0.367758249	-

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

TID	Technique	Malicious		Clean		p-value	Statistical significance
		exist	unexist	exist	unexist		
T1573	Encrypted Channel	11,855	1,260	678	855	0	✓
T1518.001	Security Software Discovery	11,364	1,751	508	1,025	0	✓
T1071	Application Layer Protocol	10,920	2,195	382	1,151	0	✓
T1082	System Information Discovery	10,352	2,763	919	614	2.26E-62	✓
T1055	Process Injection	10,055	3,060	1,138	395	0.036382082	-
T1027	Obfuscated Files or Information	9,523	3,592	385	1,148	0.00E+00	✓
T1057	Process Discovery	9,081	4,034	529	1,004	2.80E-161	✓
T1036	Masquerading	8,760	4,355	948	585	0.000116312	✓
T1560	Archive Collected Data	8,741	4,374	394	1,139	7.43E-215	✓
T1497	Virtualization/Sandbox Evasion	8,637	4,478	272	1,261	1.75E-291	✓
T1095	Non-Application Layer Protocol	8,310	4,805	285	1,248	2.40E-248	✓
T1027.002	Software Packing	7,930	5,185	88	1,445	0	✓
T1018	Remote System Discovery	7,676	5,439	155	1,378	8.76E-283	✓
T1083	File and Directory Discovery	6,796	6,319	958	575	2.90E-15	✓
T1562.001	Disable or Modify Tools	6,406	6,709	187	1,346	1.17E-163	✓
T1105	Ingress Tool Transfer	6,352	6,763	347	1,186	8.29E-82	✓
T1140	Deobfuscate/Decode Files or Information	6,332	6,783	203	1,330	5.11E-150	✓
T1003	OS Credential Dumping	4,941	8,174	1	1,532	1.66E-190	✓
T1571	Non-Standard Port	4,940	8,175	27	1,506	2.21E-173	✓
T1010	Application Window Discovery	4,719	8,396	123	1,410	3.57E-107	✓
T1005	Data from Local System	4,171	8,944	8	1,525	6.19E-145	✓
T1106	Native API	4,152	8,963	232	1,301	1.37E-40	✓
T1124	System Time Discovery	4,085	9,030	268	1,265	2.23E-28	✓
T1056	Input Capture	3,996	9,119	129	1,404	1.67E-73	✓
T1047	Windows Management Instrumentation	3,491	9,624	17	1,516	2.36E-108	✓
T1059	Command and Scripting Interpreter	3,015	10,100	243	1,290	2.51E-10	✓
T1012	Query Registry	2,958	10,157	229	1,304	1.00E-11	✓
T1033	System Owner/User Discovery	2,828	10,287	82	1,451	5.30E-51	✓
T1114	Email Collection	2,761	10,354	8	1,525	9.05E-84	✓
T1087	Account Discovery	2,730	10,385	55	1,478	3.03E-59	✓
T1070.006	Timestomp	2,183	10,932	46	1,487	9.40E-45	✓
T1070.004	File Deletion	2,138	10,977	77	1,456	3.03E-31	✓
T1134	Access Token Manipulation	1,984	11,131	133	1,400	1.38E-11	✓
T1115	Clipboard Data	1,950	11,165	63	1,470	8.49E-31	✓
T1203	Exploitation for Client Execution	1,823	11,292	80	1,453	1.63E-21	✓
T1547.001	Registry Run Keys / Startup Folder	1,823	11,292	84	1,449	2.69E-20	✓
T1552.002	Credentials in Registry	1,741	11,374	0	1,533	6.97E-52	✓
T1546.011	Application Shimming	1,735	11,380	83	1,450	2.32E-18	✓
T1574.002	DLL Side-Loading	1,493	11,622	194	1,339	0.151912084	-
T1053	Scheduled Task/Job	1,400	11,715	12	1,521	3.72E-35	✓
T1564.001	Hidden Files and Directories	1,384	11,731	10	1,523	1.34E-35	✓
T1016	System Network Configuration Discovery	1,232	11,883	0	1,533	8.40E-36	✓
T1529	System Shutdown/Reboot	1,176	11,939	113	1,420	0.041438039	-
T1218.011	Rundll32	1,169	11,946	72	1,461	2.67E-08	✓
T1543.003	Windows Service	930	12,185	73	1,460	0.000770065	✓
T1129	Shared Modules	920	12,195	0	1,533	1.63E-26	✓
T1569.002	Service Execution	845	12,270	27	1,506	3.50E-13	✓
T1113	Screen Capture	658	12,457	19	1,514	4.06E-11	✓
T1068	Exploitation for Privilege Escalation	597	12,518	68	1,465	0.886976911	-
T1552.001	Credentials In Files	564	12,551	0	1,533	2.21E-16	✓
T1112	Modify Registry	557	12,558	9	1,524	3.28E-12	✓
T1078	Valid Accounts	529	12,586	11	1,522	1.13E-10	✓
T1219	Remote Access Software	526	12,589	0	1,533	2.51E-15	✓
T1056.004	Credential API Hooking	521	12,594	0	1,533	3.45E-15	✓
T1222	File and Directory Permissions Modification	470	12,645	5	1,528	1.62E-11	✓
T1014	Rootkit	399	12,716	0	1,533	7.85E-12	✓
T1037.005	Startup Items	323	12,792	2	1,531	7.70E-09	✓
T1007	System Service Discovery	320	12,795	4	1,529	6.76E-08	✓
T1120	Peripheral Device Discovery	305	12,810	90	1,443	1.01E-15	✓
T1059.001	PowerShell	289	12,826	0	1,533	7.77E-09	✓
T1070	Indicator Removal on Host	286	12,829	8	1,525	1.82E-05	✓
T1486	Data Encrypted for Impact	271	12,844	5	1,528	3.44E-06	✓
T1102	Web Service	252	12,863	0	1,533	7.84E-08	✓
T1218.010	Regsvr32	241	12,874	18	1,515	0.077975619	-
T1091	Replication Through Removable Media	225	12,890	86	1,447	3.59E-23	✓
T1406	Obfuscated Files or Information	201	12,914	11	1,522	0.015720353	-
T1507	Network Information Discovery	195	12,920	13	1,520	0.059249023	-
T1426	System Information Discovery	194	12,921	11	1,522	0.022177882	-
T1421	System Network Connections Discovery	188	12,927	13	1,520	0.080383406	-
T1447	Delete Device Data	184	12,931	10	1,523	0.020631478	-
T1424	Process Discovery	163	12,952	9	1,524	0.033169614	-
T1185	Man in the Browser	150	12,965	1	1,532	0.000132267	✓
T1418	Application Discovery	147	12,968	2	1,531	0.000427987	✓
T1574.010	Services File Permissions Weakness	144	12,971	17	1,516	0.927883606	-
T1136	Create Account	140	12,975	2	1,531	0.000660962	✓
T1564.002	Hidden Users	116	12,999	0	1,533	0.000393093	✓
T1055.011	Extra Window Memory Injection	109	13,006	18	1,515	0.220443697	-
T1499	Endpoint Denial of Service	101	13,014	0	1,533	0.001020654	✓
T1422	System Network Configuration Discovery	97	13,018	2	1,531	0.009605471	✓
T1090	Proxy	97	13,018	0	1,533	0.001317978	✓
T1523	Evade Analysis Environment	95	13,020	0	1,533	0.00149803	✓
T1080	Taint Shared Content	81	13,034	0	1,533	0.003689418	✓
T1548.002	Bypass User Access Control	77	13,038	0	1,533	0.004782079	✓
T1547.008	LSASS Driver	75	13,040	0	1,533	0.005446388	✓
T1429	Capture Audio	71	13,044	3	1,530	0.10609741	-
T1491	Defacement	69	13,046	0	1,533	0.008059561	✓
T1048	Exfiltration Over Alternative Protocol	61	13,054	3	1,530	0.190616084	-
T1001	Data Obfuscation	48	13,067	0	1,533	0.032644518	-
T1542.003	Bootkit	48	13,067	1	1,532	0.089877812	-
T1049	System Network Connections Discovery	46	13,069	1	1,532	0.102735537	-
T1564.004	NTFS File Attributes	43	13,072	0	1,533	0.045959464	-
T1090.003	Multi-hop Proxy	41	13,074	0	1,533	0.052771664	-
T1566.002	Spearphishing Link	39	13,076	84	1,449	6.37E-97	✓
T1490	Inhibit System Recovery	29	13,086	0	1,533	0.123719937	-
T1021.001	Remote Desktop Protocol	28	13,087	0	1,533	0.133131673	-
T1189	Drive-by Compromise	26	13,089	45	1,488	4.70E-47	✓
T1553.004	Install Root Certificate	25	13,090	1	1,532	0.433632044	-
T1564.003	Hidden Window	23	13,092	0	1,533	0.19357285	-
T1547.006	Kernel Modules and Extensions	22	13,093	0	1,533	0.20900378	-
T1135	Network Share Discovery	20	13,095	0	1,533	0.244206902	-
T1562.004	Disable or Modify System Firewall	16	13,099	0	1,533	0.337188376	-
T1574.001	DLL Search Order Hijacking	15	13,100	33	1,500	1.65E-38	✓
T1433	Access Call Log	14	13,101	0	1,533	0.399175466	-
T1564	Hide Artifacts	11	13,104	0	1,533	0.521084905	-
T1543.002	Systemd Service	10	13,105	0	1,533	0.572197451	-
T1176	Browser Extensions	7	13,108	1	1,532	0.69681483	-
T1110	Brute Force	6	13,109	0	1,533	0.864492365	-
T1546.012	Image File Execution Options Injection	5	13,110	0	1,533	0.972864077	-
T1046	Network Service Scanning	5	13,110	0	1,533	0.972864077	-
T1197	BITS Jobs	3	13,112	0	1,533	0.72565624	-
T1546.006	LC_LOAD_DYLIB Addition	3	13,112	0	1,533	0.72565624	-
T1543.001	Launch Agent	3	13,112	0	1,533	0.72565624	-
T1547.011	Plist Modification	3	13,112	5	1,528	2.32E-05	✓
T1040	Network Sniffing	3	13,112	0	1,533	0.72565624	-
T1211	Exploitation for Defense Evasion	2	13,113	0	1,533	0.501883284	-
T1056.002	GUI Input Capture	2	13,113	0	1,533	0.501883284	-
T1532	Data Encrypted	2	13,113	0	1,533	0.501883284	-
T1218.005	Mshta	2	13,113	0	1,533	0.501883284	-
T1553.002	Code Signing	2	13,113	1	1,532	0.72565624	-
T1132	Data Encoding	1	13,114	2	1,531	0.025273731	-
T1573.002	Asymmetric Cryptography	1	13,114	0	1,533	0.196511029	-
T1210	Exploitation of Remote Services	0	13,115	2	1,531	0.00286684	✓

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

TID	Technique	JoeSandbox		Hybrid Analysis		Hatching Triage		Combination	p-value	Statistical significance
		exist	unexist	exist	unexist	exist	unexist			
T1055	Process Injection	10,690	15,388	0	3,918	16	34	sandbox+report	0.251052825	-
T1497	Virtualization/Sandbox Evasion	9,577	16,501	2	3,916	4	46	(all) sandbox+static	0	✓
T1497	Virtualization/Sandbox Evasion	9,577	16,501	2	3,916	4	46	(all) sandbox+report	5.99E-06	✓
T1497	Virtualization/Sandbox Evasion	9,577	16,501	2	3,916	4	46	(all) static+report	4.36E-36	✓
T1027.002	Software Packing	8,649	17,429	4	3,914	2	48	(all) sandbox+static	0	✓
T1027.002	Software Packing	8,649	17,429	4	3,914	2	48	(all) sandbox+report	0.000175584	✓
T1027.002	Software Packing	8,649	17,429	4	3,914	2	48	(all) static+report	1.82E-07	✓
T1027	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	2,506	15	35	(all) sandbox+report	0	✓
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	✓
T1518.001	Security Software Discovery	11,428	14,650	3	3,915	2	48	(all) sandbox+report	1.07E-07	✓
T1518.001	Security Software Discovery	11,428	14,650	3	3,915	2	48	(all) static+report	8.17E-09	✓
T1057	Process Discovery	9569	16,509	99	3,819	7	43	(all) sandbox+static	0	✓
T1057	Process Discovery	9569	16,509	99	3,819	7	43	(all) sandbox+report	8.45E-16	✓
T1057	Process Discovery	9569	16,509	99	3,819	7	43	(all) static+report	5.16E-06	✓
T1082	System Information Discovery	15,879	10,199	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	✓
T1082	System Information Discovery	15,879	10,199	2,416	1,502	11	39	(all) static+report	2.51E-08	✓
T1560	Archive Collected Data	8,750	17,328	0	3,918	3	47	sandbox+report	7.07E-05	✓
T1573	Encrypted Channel	12,093	13,985	0	3,918	1	49	sandbox+report	8.02E-10	✓
T1071	Application Layer Protocol	10,920	15,158	0	3,918	10	40	sandbox+report	0.002797683	✓
T1036	Masquerading	8,851	17,227	0	3,918	5	45	sandbox+report	0.000618542	✓
T1105	Ingress Tool Transfer	6,401	19,677	0	3,918	15	35	sandbox+report	0.464919838	-
T1078	Valid Accounts	529	25,549	0	3,918	11	39	sandbox+report	4.54E-21	✓
T1106	Native API	4,156	21,922	0	3,918	2	48	sandbox+report	0.034712164	✓
T1203	Exploitation for Client Execution	2,415	23,663	0	3,918	2	48	sandbox+report	0.299105373	-
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	✓
T1569.002	Service Execution	858	25,220	125	3,793	5	45	(all) static+report	0.022133283	✓
T1574.002	DLL Side-Loading	1,493	24,585	0	3,918	1	49	sandbox+report	0.407363774	-
T1543.003	Windows Service	1,338	24,740	42	3,876	2	48	(all) sandbox+static	1.93E-29	✓
T1543.003	Windows Service	1,338	24,740	42	3,876	2	48	(all) sandbox+report	1.56E-67	✓
T1543.003	Windows Service	1,338	24,740	42	3,876	2	48	(all) static+report	0.198753535	-
T1068	Exploitation for Privilege Escalation	597	25,481	0	3,918	2	48	sandbox+report	0.737961337	-
T1134	Access Token Manipulation	1,985	24,093	144	3,774	0	50	sandbox+static	4.94E-19	✓
T1140	Deobfuscate/Decode Files or Information	6,337	19,741	122	3,796	11	39	(all) sandbox+static	1.59E-198	✓
T1140	Deobfuscate/Decode Files or Information	6,337	19,741	122	3,796	11	39	(all) sandbox+report	5.10E-51	✓
T1140	Deobfuscate/Decode Files or Information	6,337	19,741	122	3,796	11	39	(all) static+report	3.00E-12	✓
T1070.006	Timestomp	2,183	23,895	17	3,901	2	48	(all) sandbox+static	2.21E-70	✓
T1070.006	Timestomp	2,183	23,895	17	3,901	2	48	(all) sandbox+report	8.05E-07	✓
T1070.006	Timestomp	2,183	23,895	17	3,901	2	48	(all) static+report	0.009351916	✓
T1056	Input Capture	3,999	22,079	0	3,918	5	45	sandbox+report	0.395487368	-
T1124	System Time Discovery	4,099	21,979	0	3,918	2	48	sandbox+report	0.037422522	✓
T1120	Peripheral Device Discovery	1,687	24,391	0	3,918	2	48	sandbox+report	0.673395827	-
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+report	0	✓
T1083	File and Directory Discovery	6,818	19,260	1,748	2,170	12	38	(all) static+report	0.005565762	✓
T1012	Query Registry	7,460	18,618	724	3,194	4	46	(all) sandbox+static	4.45E-40	✓
T1012	Query Registry	7,460	18,618	724	3,194	4	46	(all) sandbox+report	0	✓
T1012	Query Registry	7,460	18,618	724	3,194	4	46	(all) static+report	0.085716776	-
T1070.004	File Deletion	2,550	23,528	1	3,917	7	43	(all) sandbox+static	2.81E-92	✓
T1070.004	File Deletion	2,550	23,528	1	3,917	7	43	(all) sandbox+report	0.155138889	-
T1070.004	File Deletion	2,550	23,528	1	3,917	7	43	(all) static+report	1.20E-91	✓
T1087	Account Discovery	2,730	23,348	135	3,783	9	41	(all) sandbox+static	5.06E-44	✓
T1087	Account Discovery	2,730	23,348	135	3,783	9	41	(all) sandbox+report	4.16E-172	✓
T1087	Account Discovery	2,730	23,348	135	3,783	9	41	(all) static+report	3.62E-07	✓
T1033	System Owner/User Discovery	2,845	23,233	201	3,717	5	45	(all) sandbox+static	8.13E-29	✓
T1033	System Owner/User Discovery	2,845	23,233	201	3,717	5	45	(all) sandbox+report	4.35E-260	✓
T1033	System Owner/User Discovery	2,845	23,233	201	3,717	5	45	(all) static+report	0.221871132	-
T1018	Remote System Discovery	7,846	18,232	0	3,918	5	45	sandbox+report	0.003275006	✓
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	✓
T1115	Clipboard Data	1,955	24,123	238	3,680	1	49	(all) static+report	0.365872328	-
T1529	System Shutdown/Reboot	1,176	24,902	41	3,877	2	48	(all) sandbox+static	1.96E-24	✓
T1529	System Shutdown/Reboot	1,176	24,902	41	3,877	2	48	(all) sandbox+report	4.45E-75	✓
T1529	System Shutdown/Reboot	1,176	24,902	41	3,877	2	48	(all) static+report	0.187797059	-
T1070	Indicator Removal on Host	290	25,788	0	3,918	6	44	sandbox+report	4.14E-11	✓
T1003	OS Credential Dumping	4,994	21,084	0	3,918	10	40	sandbox+report	0.978207255	-
T1571	Non-Standard Port	5,205	20,873	0	3,918	3	47	sandbox+report	0.02194729	✓
T1059	Command and Scripting Interpreter	3,122	22,956	1,801	2,117	11	39	(all) sandbox+static	0	✓
T1059	Command and Scripting Interpreter	3,122	22,956	1,801	2,117	11	39	(all) sandbox+report	0	✓
T1059	Command and Scripting Interpreter	3,122	22,956	1,801	2,117	11	39	(all) static+report	0.001203964	✓
T1547.001	Registry Run Keys / Startup Folder	4,302	21,776	104	3,814	5	45	(all) sandbox+static	4.84E-115	✓
T1547.001	Registry Run Keys / Startup Folder	4,302	21,776	104	3,814	5	45	(all) sandbox+report	1.25E-66	✓
T1547.001	Registry Run Keys / Startup Folder	4,302	21,776	104	3,814	5	45	(all) static+report	0.006481233	✓
T1010	Application Window Discovery	4,897	21,181	1,096	2,822	0	50	sandbox+static	6.03E-41	✓
T1016	System Network Configuration Discovery	1,483	24,595	89	3,829	3	47	(all) sandbox+static	5.29E-19	✓
T1016	System Network Configuration Discovery	1,483	24,595	89	3,829	3	47	(all) sandbox+report	4.44E-186	✓
T1016	System Network Configuration Discovery	1,483	24,595	89	3,829	3	47	(all) static+report	0.204823814	-
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	✓
T1113	Screen Capture	664	25,414	403	3,515	3	47	(all) static+report	0.447946249	-
T1486	Data Encrypted for Impact	290	25788	0	3,918	11	39	sandbox+report	1.41E-39	✓
T1053	Scheduled Task/Job	2,787	23,291	0	3,918	12	38	sandbox+report	0.004923383	✓
T1562.001	Disable or Modify Tools	6,784	19,294	0	3,918	9	41	sandbox+report	0.258742312	-
T1112	Modify Registry	4,886	21,192	195	3,723	6	44	(all) sandbox+static	1.82E-101	✓
T1112	Modify Registry	4,886	21,192	195	3,723	6	44	(all) sandbox+report	9.55E-132	✓
T1112	Modify Registry	4,886	21,192	195	3,723	6	44	(all) static+report	0.054137315	-
T1005	Data from Local System	8,036	18,042	0	3,918	3	47	sandbox+report	0.000267483	✓
T1114	Email Collection	3,995	22,083	0	3,918	2	48	sandbox+report	0.042887734	✓
T1047	Windows Management Instrumentation	3,542	22,536	8	3,910	3	47	(all) sandbox+static	8.44E-129	✓
T1047	Windows Management Instrumentation	3,542	22,536	8	3,910	3	47	(all) sandbox+report	0.991008892	-
T1047	Windows Management Instrumentation	3,542	22,536	8	3,910	3	47	(all) static+report	1.64E-10	✓
T1222	File and Directory Permissions Modification	628	25,450	237	3,681	1	49	(all) sandbox+static	1.17E-36	✓
T1222	File and Directory Permissions Modification	628	25,450	237	3,681	1	49	(all) sandbox+report	0	✓
T1222	File and Directory Permissions Modification	628	25,450	237	3,681	1	49	(all) static+report	0.368942641	-
T1189	Drive-by Compromise	26	26,052	0	3,918	2	48	sandbox+report	3.90E-10	✓
T1102	Web Service	588	25,490	0	3,918	2	48	sandbox+report	0.72375299	-
T1014	Rootkit	399	25,679	0	3,918	1	49	sandbox+report	0.759558725	-
T1059.001	PowerShell	386	25,692	0	3,918	14	36	sandbox+report	8.40E-49	✓
T1007	System Service Discovery	320	25,758	26	3,892	2	48	(all) sandbox+static	0.002703009	✓
T1007	System Service Discovery	320	25,758	26	3,892	2	48	(all) sandbox+report	9.37E-138	✓
T1007	System Service Discovery	320	25,758	26	3,892	2	48	(all) static+report	0.051117737	-
T1219	Remote Access Software	526	25,552	0	3,918	6	44	sandbox+report	7.05E-06	✓
T1406	Obfuscated Files or Information	201	25,877	0	3,918	3	47	sandbox+report	0.00069151	✓
T1523	Evade Analysis Environment	95	25,983	0	3,918	1	49	sandbox+report	0.459299844	-
T1426	System Information Discovery	194	25,884	0	3,918	1	49	sandbox+report	0.834750965	-
T1448	Carrier Billing Fraud	140	25,938	0	39,18	1	49	sandbox+report	0.656507257	-
T1418	Application Discovery	148	25,930	0	3,918	1	49	sandbox+report	0.686269057	-
T1409	Access Stored Application Data	68	26,010	0	3,918	1	49	sandbox+report	0.310144153	-
T1422	System Network Configuration Discovery	97	25,981	0	3,918	1	49	sandbox+report	0.469326426	-
T1430	Location Tracking	172	25,906	0	3,918	1	49	sandbox+report	0.768093651	-
T1507	Network Information Discovery	195	25,883	0	3,918	1	49	sandbox+report	0.837615936	-
T1472	Generate Fraudulent Advertising Revenue	100	25,978	0	3,918	3	47	sandbox+report	1.97E-07	✓
T1129	Shared Modules	920	25,158	3,392	526	1	49	(all) sandbox+static	0	✓
T1129	Shared Modules	920	25,158	3,392	526	1	49	(all) sandbox+report	0	✓
T1129	Shared Modules	920	25,158	3,392	526	1	49	(all) static+report	1.84E-62	✓
T1136	Create Account	140	25,938	1	3,917	1	49	(all) sandbox+static	2.26E-05	✓
T1136	Create Account	140	25,938	1	3,917	1	49	(all) sandbox+report	0.656507257	-
T1136	Create Account	140	25,938	1	3,917	1	49	(all) static+report	0.002607017	✓
T1049	System Network Connections Discovery	78	26,000	0	3,918	2	48	sandbox+report	0.000558551	✓
T1499	Endpoint Denial of Service	101	25,977	6	3,912	1	49	(all) sandbox+static	0.031667893	✓
T1499	Endpoint Denial of Service	101	25,977	6	3,912	1	49	(all) sandbox+report	7.16E-29	✓
T1499	Endpoint Denial of Service	101	25,977	6	3,912	1	49	(all) static+report	0.162536612	-
T1566.002	Spearphishing Link	42	26,036	0	3,918	4	46	sandbox+report	1.03E-30	✓
T1513	Screen Capture	26	26,052	0	3,918	1	49	sandbox+report	0.048237909	✓
T1080	Taint Shared Content	81	25,997	0	3,918	1	49	sandbox+report	0.385245941	-
T1021.001	Remote Desktop Protocol	309	25,769	0	3,918	8	42	sandbox+report	4.96E-19	✓
T1490	Inhibit System Recovery	61	26,017	1	3,917	6	44	(all) sandbox+static	0.0127993	✓
T1490	Inhibit System Recovery	61	26,017	1	3,917	6	44	(all) sandbox+report	0.22796386	-
T1490	Inhibit System Recovery	61	26,017	1	3,917	6	44	(all) static+report	3.07E-75	✓
T1185	Man in the Browser	150	25,928	0	3,918	2	48	sandbox+report	0.024410287	✓
T1048	Exfiltration Over Alternative Protocol	61	26,017	0	3,918	4	46	sandbox+report	8.62E-22	✓
T1090.003	Multi-hop Proxy	41	26,037	0	3,918	1	49	sandbox+report	0.138137537	-
T1090	Proxy	116	25,962	0	3,918	5	45	sandbox+report	5.61E-19	✓
T1564.003	Hidden Window	26	26,052	516	3,402	0	50	sandbox+static	0	✓
T1132	Data Encoding	2	26,076	0	3,918	2	48	sandbox+report	2.28E-65	✓
T1553.004	Install Root Certificate	807	25,271	0	3,918	1	49	sandbox+report	0.969842387	-
T1001	Data Obfuscation	48	26,030	0	3,918	3	47	sandbox+report	1.31E-14	✓
T1564	Hide Artifacts	11	26,067	6	3,912	0	50	sandbox+static	0.018224449	✓
T1562.004	Disable or Modify System Firewall	25	26,053	3	3,915	2	48	(all) sandbox+static	0.929678359	-
T1562.004	Disable or Modify System Firewall	25	26,053	3	3,915	2	48	(all) sandbox+report	1.11E-25	✓
T1562.004	Disable or Modify System Firewall	25	26,053	3	3,915	2	48	(all) static+report	8.17E-09	✓
T1548.002	Bypass User Access Control	122	25,956	0	3,918	1	49	sandbox+report	0.584212563	-
T1564.004	NTFS File Attributes	210	25,868	0	3,918	1	49	sandbox+report	0.879043574	-
T1546.012	Image File Execution Options Injection	5	26,073	0	3,918	1	49	sandbox+report	5.02E-06	✓
T1135	Network Share Discovery	21	26,057	21	3,897	3	47	(all) sandbox+static	6.00E-12	✓
T1135	Network Share Discovery	21	26,057	21	3,897	3	47	(all) sandbox+report	0	✓
T1135	Network Share Discovery	21	26,057	21	3,897	3	47	(all) static+report	5.49E-05	✓
T1553.002	Code Signing	58	26,020	0	3,918	3	47	sandbox+report	2.74E-12	✓
T1546.004	.bash_profile and .bashrc	3	26,075	1	3,917	0	50	sandbox+static	0.973401992	-
T1110	Brute Force	6	26,072	0	3,918	1	49	sandbox+report	2.57E-05	✓
T1046	Network Service Scanning	7	26,071	0	3,918	3	47	sandbox+report	4.44E-72	✓
T1532	Data Encrypted	2	26,076	0	3,918	1	49	sandbox+report	6.58E-11	✓
T1218.005	Mshta	9	26,069	0	3,918	2	48	sandbox+report	1.87E-24	✓
T1573.002	Asymmetric Cryptography	1	26,077	0	3,918	3	47	sandbox+report	7.32E-179	✓
T1547.004	Winlogon Helper DLL	79	25,999	6	3,912	0	50	sandbox+static	0.137936971	-
T1098	Account Manipulation	29	26,049	1	3,917	3	47	(all) sandbox+static	0.189859721	-
T1098	Account Manipulation	29	26,049	1	3,917	3	47	(all) sandbox+report	0.057723068	-
T1098	Account Manipulation	29	26,049	1	3,917	3	47	(all) static+report	4.46E-28	✓
T1489	Service Stop	22	26,056	25	3,893	7	43	(all) sandbox+static	1.81E-15	✓
T1489	Service Stop	22	26,056	25	3,893	7	43	(all) sandbox+report	0	✓
T1489	Service Stop	22	26,056	25	3,893	7	43	(all) static+report	2.97E-22	✓
T1055.012	Process Hollowing	349	25,729	18	3,900	0	50	sandbox+static	4.48E-06	✓
T1055.003	Thread Execution Hijacking	41	26,037	24	3,894	0	50	sandbox+static	3.19E-08	✓
T1071.001	Web Protocols	173	25,905	0	3,918	7	43	sandbox+report	5.99E-26	✓
T1204	User Execution	48	26,030	0	3,918	7	43	sandbox+report	7.90E-87	✓
T1053.005	Scheduled Task	120	25,958	9	3,909	3	47	(all) sandbox+static	0.054301071	-
T1053.005	Scheduled Task	120	25,958	9	3,909	3	47	(all) sandbox+report	1.59E-55	✓
T1053.005	Scheduled Task	120	25,958	9	3,909	3	47	(all) static+report	1.14E-09	✓
T1059.003	Windows Command Shell	108	25,970	16	3,902	5	45	(all) sandbox+static	0.935416564	-
T1059.003	Windows Command Shell	108	25,970	16	3,902	5	45	(all) sandbox+report	3.97E-177	✓
T1059.003	Windows Command Shell	108	25,970	16	3,902	5	45	(all) static+report	9.74E-17	✓
T1036.005	Match Legitimate Name or Location	13	26,065	0	3,918	1	49	sandbox+report	0.003796366	✓
T1565	Data Manipulation	51	26,027	0	3,918	1	49	sandbox+report	0.203352928	-
T1132.001	Standard Encoding	31	26,047	0	3,918	6	44	sandbox+report	7.77E-93	✓
T1402	Broadcast Receivers	1	26,077	0	3,918	5	45	sandbox+report	0	✓
T1420	File and Directory Discovery	1	26,077	0	3,918	1	49	sandbox+report	9.89E-16	✓
T1204.002	Malicious File	18	26,060	0	3,918	4	46	sandbox+report	6.76E-64	✓
T1070.001	Clear Windows Event Logs	23	26,055	0	3,918	3	47	sandbox+report	3.79E-28	✓
T1218	Signed Binary Proxy Execution	1	26,077	0	3,918	2	48	sandbox+report	9.54E-87	✓
T1059.005	Visual Basic	14	26,064	0	3,918	3	47	sandbox+report	1.05E-42	✓
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	✓
T1560.002	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	✓
T1056.001	Keylogging	4	26,074	532	3,386	1	49	(all) sandbox+report	0	✓
T1056.001	Keylogging	4	26,074	532	3,386	1	49	(all) static+report	0.029476232	✓
T1048.003	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	1	26,077	0	3,918	1	49	sandbox+report	9.89E-16	✓
T1059.007	JavaScript	1	26,077	0	3,918	2	48	sandbox+report	9.54E-87	✓
T1055.001	Dynamic-link Library Injection	1	26,077	4	3,914	0	50	sandbox+static	0.000157776	✓

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 security 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.