NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends

3rd Quarter of 2021

NTT DATA
Trusted Global Innovator

Table of Contents

1. Executive Summary

This report is the result of surveys and analysis by NTTDATA-CERT on quarterly global trends from its own perspective based on cybersecurity-related information collected during the period.

"Log4Shell," a serious vulnerability in Apache Log4j

In December 2021, information was released about Log4Shell (CVE-2021-44228), a vulnerability in Apache Log4j. It made headlines because Log4j is a widely used library in Java-based systems and because the CVSS score, an indicator of the severity of the vulnerability, was 10.0, the most severe. It is difficult to take countermeasures against every single system subject to the Log4j vulnerability, and we expect that there will be no end to the number of damage reports in the future.

To prepare against software and library vulnerabilities with significant impact, such as Log4Shell, system operators need to manage their architecture with an awareness of the software supply chain. As a method that can be used for that purpose, we introduce the creation and operation of a Software Bill of Materials (SBOM).

"Minimum Viable Security Product (MVSP)," a minimum security baseline, established

A vendor-neutral minimum security baseline, Minimum Viable Security Product (hereinafter referred to as "MVSP"), has been established by companies such as Google and Salesforce. The MVSP is the minimum security requirement that companies providing B2B software and business process outsourcing services should meet. While supply chain attacks are becoming more active and risk assessment of the entire supply chain is becoming more important, the risk assessment process is complex, time-consuming, and burdensome for both the assessor and the assessed. The MVSP was developed to address this issue and is presented as a simplified checklist focused on the minimum acceptable security requirements. In order to eliminate any ambiguities in interpretation, the implementation methods and standards of security measures as well as the importance of the measures are clearly stated. Utilizing the MVSP for contractors' risk assessment at the time of contracting or on a regular basis, or as a security requirement in RFPs, would simplify the review process. It should be noted that the MVSP is only a minimum security requirement, and in some cases, customization is required, such as adding additional requirements. If more companies adopt the MVSP in the future, it may become the de facto standard.

Vulnerabilities in Zoho's UEM products

Zoho Corporation's ManageEngine-related products are Unified Endpoint Management (UEM) products that allow system administrators to remotely manage employee terminals and servers by installing an agent in the machines. When connecting to agents of these ManageEngine-related products and remotely managing the end user devices, authentication could be bypassed, thus creating a vulnerability. An APT attack group exploited this vulnerability to conduct a zero-day attack. Once an attacker hijacks a UEM product, the product that was designed to protect your information and assets is transformed into a product that aids attackers. Software that integrates and centrally manages large numbers of machines, such as UEM products, must be protected by stronger security measures to prevent attackers from exploiting them.

EMOTET resumed attack activities

EMOTET, which was believed to have been taken down in January 2021, resumed its attack activities around November 14, 2021. A group that had organized a Conti ransomware attack using EMOTET prior to the takedown used the TrickBot/Qbot attack group to rebuild the EMOTET botnet in order to resume their ransomware attack activities. As a result, the Conti attack group and the TrickBot/Qbot attack group have resumed their ransomware attack activities using the rebuilt EMOTET botnet.

After the resumption of attack activities, EMOTET infection methods have changed, and it has become difficult to prevent infection through human measures alone. Therefore, instead of relying on personal security awareness, we should strengthen our systems, i.e., quickly obtain IoC (Indicator of Compromise) information on EMOTET and apply it to security devices such as firewalls and SIEMs, in order to prevent or detect EMOTET infection at an early stage.

Outlook

More and more organizations are not paying ransoms to ransomware attack groups after the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and police issued orders regulating ransom payments. Therefore, we predict that ransomware attack groups will increasingly try to secure revenue by means other than ransom demands. In the future, it is quite possible that ransomware attack groups will develop subplans other than ransom demands, such as the sale of stolen information, or develop new means of attack based on new revenue models that circumvent security measures. We are now in a time of transition.

Having said that, not all organizations refuse to pay ransoms. One reason for this is that organizations that have cyber insurance for ransom choose to pay a ransom, as this can resolve the issue quickly and inexpensively. However, four of the top 10 cyber insurers in the U.S., where cyber attacks are on the rise, are in the red, and if the losses continue to grow, these insurers may stop offering insurance riders for ransomware-related ransom payments. In that case, we expect ransom payments to decrease, and if they do, ransomware attacks may also decrease.

In addition, with the increase in remote work due to the coronavirus pandemic, opportunities for VPN connections from outside the company to internal systems via the Internet and the use of cloud services have increased, and phishing attacks aimed at infiltrating internal systems have become widespread. Phishing as a Service (PHaaS), which provides the work required for phishing attacks as-a-Service for a fee, exists, and the more the PHaaS business is active, the more phishing damage is estimated to increase.

2. Featured Topics

2.1. "Log4Shell," a serious vulnerability in Apache Log4j

2.1.1. What is Log4Shell?

The Apache Software Foundation disclosed vulnerability CVE-2021-44228 in December 2021. [1] CVE-2021-44228 is a vulnerability in the Java library Log4j, commonly known as “Log4Shell.” Arbitrary code can be executed remotely on a system running Log4j at a low level of execution difficulty, which makes this vulnerability extremely easy to exploit. The CVSS score, an indicator of vulnerability severity, was also 10.0, the most severe.

The fact that Log4j is widely used in Java-based systems also adds to the severity of the situation. Google's investigation revealed that more than 35,000 libraries in the Maven Central Repository1 depend on a vulnerable version of the Log4j library. [2] The Apache Software Foundation already released Log4j 2.15, a new version that fixed the vulnerability, in January 2022, but libraries that depend on Log4j must also be upgraded to a version that includes Log4j 2.15. In addition, libraries have complex dependencies on each other, and sometimes it is not possible to start fixing one's own libraries until after other libraries that have Log4j have been fixed. As shown in Figure 2-1, there are cases in which a library is blocked waiting for a fix for a vulnerable lower-level library that depends Log4j.

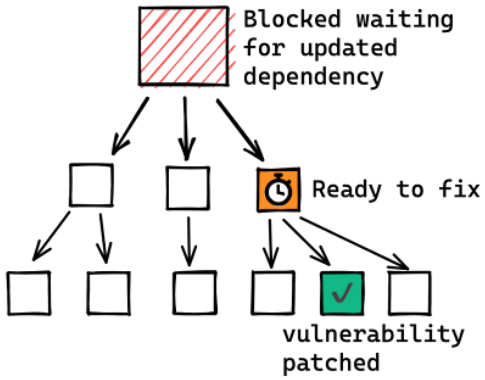


Figure 2-1: Conceptual diagram of library dependencies (taken from Google Security Blog)

[1]One of the sites where Java libraries are available. Many libraries are publicly available, and Java developers can download and use the necessary libraries from here. The site is operated by The Apache Software Foundation.

It is said that even fixing all the Log4j-dependent libraries that exist on the Maven Central Repository alone would be difficult in a short period of time. In addition, if we extend the scope of the investigation of the impact to the group of Java systems that use the aforementioned Log4j-dependent libraries, the number of affected systems is much larger. It is quite difficult to fix every single system affected by the Log4j vulnerability without omission. We expect that the Log4Shell vulnerability will remain in some libraries or systems and cause damage somewhere in the world in the future.

2.1.2. The vulnerability's mechanism, workarounds

(1) The vulnerability's mechanism

Log4j is a library for outputting system logs. Log4j implements a function called JNDI Lookup for referencing objects and resources outside the system. This JNDI Lookup function allows you to specify an external object reference using a specific format and then read that object. Log4j was implemented in such a vulnerable way that if the log contained the same string as in this particular format, the JNDI Lookup function would refer to an external object or resource according to the instructions in that string.

An attacker could exploit this vulnerable implementation of the JNDI Lookup function to make the target system access a server prepared by the attacker and refer to an external object, thereby executing an arbitrary Java object on the system. In addition, because this JNDI Lookup was enabled as the default setting, many systems using Log4j were forced to take countermeasures.

The prerequisite for the attack is that the attacker must interfere with the contents of the system's log output, which in many cases is not too difficult. For example, in the case of web servers, it is common to output the "User-Agent" parameter of the accessing user in the log, but this "User-Agent" can be specified by the attacker as desired.

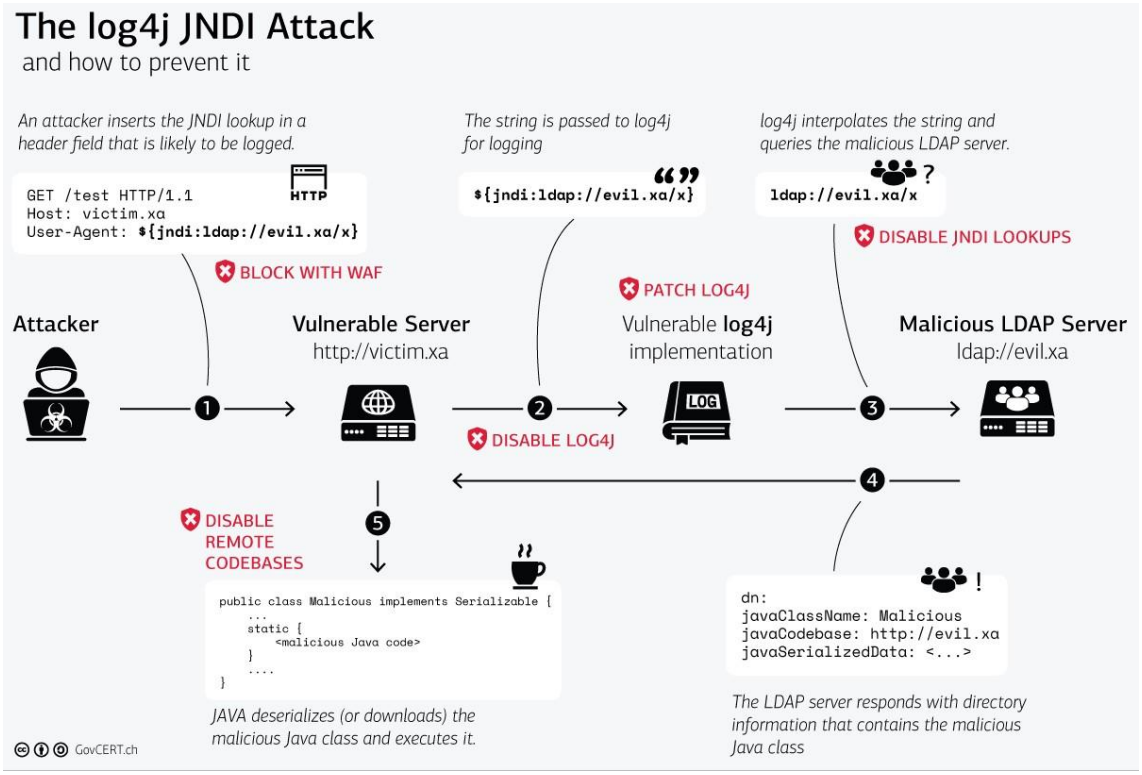


Figure 2-2: Example of attack via LDAP (taken from a commentary page on GovCERT.ch) [3]

Figure 2-2 shows the flow of an attacker remotely executing arbitrary Java code via LDAP.

1. The attacker sets the address information of the LDAP server prepared by themselves to the "User-Agent" which is the client environment parameter for HTTP protocol.
2. When the attacker accesses the target web server, the web server records logs related to this access. At this time, if the "User-Agent" information of the client environment of the visitor is designed to be output to the log, the above LDAP server address information set by the attacker will be logged as it is.
3. When outputting LDAP server address information in JNDI format to the log, Log4j's JNDI Lookup function is enabled as default, so the function interprets the JNDI format in the log and extracts LDAP server address information.
4. Log4j send lookup request to the LDAP server of the acquired address.
5. The LDAP server returns address information for another server.
6. The target web server accesses the server of the above returned address information, and then downloads and executes a malicious code.

(2) Measures to address the vulnerability

Implement the full-scale measures described in (1) below. If (1) is difficult to implement, implement the provisional measures in (2).

(1) Full-scale measures: upgrading Log4j version

Upgrade to a version of Log4j that has fixed vulnerability CVE-2021-44228. The fixed versions are shown in Table 2-1. Vendor support for Java 6 and 7 series is no longer available, so please switch to Java 8 series or later if possible.

Table 2-1: Fixed Log4j versions (as of 2022.1)

Java versions	Fixed Log4j versions
6 series	2.3.2 or later
7 series	2.12.4 or later
8 series	2.16.0 or later

(2) Provisional measures: disabling the JNDI Lookup function

If upgrading is difficult, consider disabling the JNDI Lookup function. Specifically, remove the JNDI Lookup class from the classpath. [4] In addition to the measures listed above, restricting access from the system to the outside is also an effective measure. [4] However, for systems that use DNS, DNS access cannot be restricted.

2.1.3. Software supply chain issues in vulnerability response

Log4j is so-called open source software, belonging to the Apache Software Foundation. Open source software permits its use free of charge under the conditions set forth in the software's license. For Log4j, the Apache License 2.0 is applied. [5] The Apache License 2.0 makes it free to copy the software and to create, run, and publish derivative software, and has been adopted in many system development sites because of its ease of use.

When system developers develop a system, in some cases they themselves incorporate Log4j, while in other cases Log4j is already embedded in the software or libraries they have adopted. In the latter case, where Log4j is already embedded in the software or libraries that make up a system, it is difficult to know that Log4j has been embedded in the system when the system has been developed. Log4j provides the general-purpose functionality of outputting logs, and is among the most widely used open-source software. This makes it very time-consuming and demanding to grasp the actual situation, i.e., which systems have Log4j embedded, what version it is, and whether or not it can be affected by Log4Shell. The Log4Shell vulnerability turned out to be quite dangerous and also difficult to address because of such difficulty in understanding the actual usage and impact.

Besides Log4j, if there is any other software embedded in the system in a similar manner and a serious vulnerability is found, it will be a serious risk to the system. It would be reassuring to have a prior grasp of what software is embedded in the system, and if a serious vulnerability is discovered, to have a way to quickly identify the software containing the vulnerability and assess its impact. One means of achieving this is the Software Bill of Materials (SBOM). SBOM is a method of describing software components and the relationships among them.

(2) Software Bill of Materials (SBOM)

Software supply chain attacks, such as the incident in which multiple companies were compromised through the exploitation of a vulnerability at Solarwinds, have become a serious problem, and discussion is underway regarding the usefulness of the SBOM. Software supply chain attacks were also included in the report for the third quarter of FY2020. [6] An SBOM is like a bill of materials in an industrial product, such as an automobile or household appliance, and is a document that shows the software incorporated in a system. According to the U.S. NTIA definition [7], an SBOM consists of the elements listed in Table 2-2.

Table 2-2: Elements of Software Bill of Materials (SBOM)

Element	Overview
Author Name	Name of the creator of the Software Bill of Materials (SBOM)
Timestamp	Last update date of the Software Bill of Materials (SBOM)
Supplier Name	Name of the software supplier
Component Name (Software Name)	Name of the software
Version String	Version information of the software
Component Hash	Hash value of the software An identifier that uniquely identifies the software version, etc., in use. In addition to the hash value, its generation method must also be defined in order to reproduce the hash.
ID	Unique identifier
Relationship	Relationship of different software. If the software includes or depends on another piece of software, their relationship is indicated.

The concept of SBOM is shown in Table 2-3. The SBOM represents the relationship between the system, software, and libraries in a nested structure. In Table 2-3, for example, the component "Foo Application" includes two components: "foo-framework-logger" and "bar-framework-http." One of the components, "foo-framework-logger", includes "log4j-api." If a serious vulnerability is announced in version 2.14.0 of log4j-api, the SBOM of the Foo Application will show that there is a dependency between the Foo Application and log4j-api. In addition, we can immediately determine that the version of log4j-api on which the dependency exists is 2.14.0.

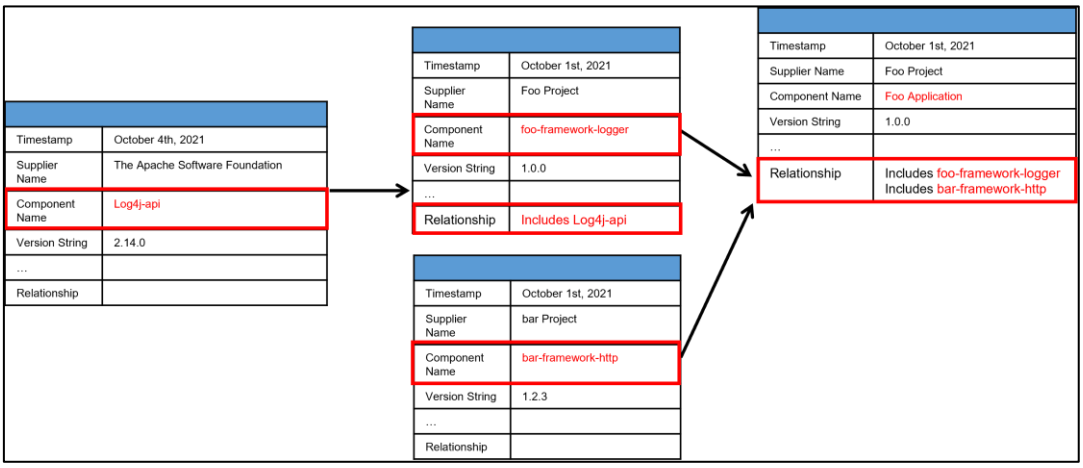


Table 2-3: Conceptual diagram of Software Bill of Materials (SBOM)

By creating and maintaining such an SBOM, it is possible to instantly determine whether any software with disclosed vulnerabilities is embedded in the system in operation, and if so, which other software is dependent on the software in question. SBOMs are expected to reduce the time required to identify systems affected by vulnerabilities and prevent such systems from being unidentified, as shown in Figure 2-4 [8].

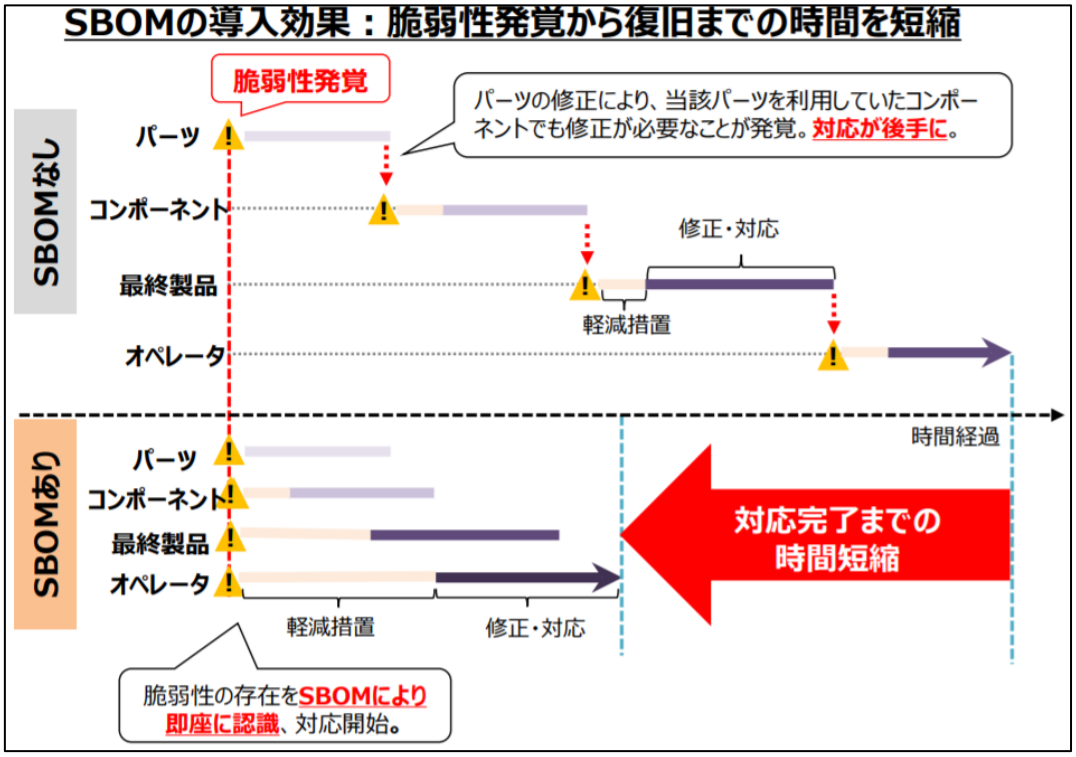


Figure 2-4: Benefits of Software Bill of Materials (SBOM)

2.1.4. Conclusion

Log4j's vulnerability, Log4Shell (CVE-2021-44228), is a very serious vulnerability. It makes it easy to remotely execute arbitrary code, and any Java system embedded with a vulnerable Log4j could be attacked, whether on the server or the client. Because Log4j is widely used, there is a risk that some software still contains vulnerable Log4j without resolving the vulnerability. In the future, we expect that various kinds of damage will be reported due to the remaining vulnerable Log4j. Thus, it has been found that when a vulnerability exists in the software or libraries included in a system, only the manufacturer of the system can investigate the risk of the vulnerability, so the vulnerability is likely to persist.

Leaving vulnerabilities unaddressed can lead to immediate and serious security breaches. Organizations that operate multiple large systems are especially burdened with the task of investigating vulnerabilities in widely used libraries. This is why a Software Bill of Materials (SBOM), which enables to manage the configuration of a software supply chain, has been attracting attention. The creation and operation of SBOMs can be very effective because vulnerability responses can be executed more accurately and in less time.

2.2. "Minimum Viable Security Product (MVSP)," a minimum security baseline, established

In October 2021, a vendor-neutral minimum security baseline, Minimum Viable Security Product (hereinafter referred to as "MVSP"), was established by companies such as Google and Salesforce. The MVSP was developed as the minimum security requirement that companies providing B2B software and business process outsourcing services should meet. The MVSP is a simplified checklist that focuses on the minimum acceptable security requirements to save companies that provide the above software and services from the complexity of security assessment processes and the resulting overhead [9]. This section provides the background of the MVSP's formulation, an overview of the MVSP, and how to use it.

2.2.1. Background of the MVSP’s formulation

(3) Importance of assessing risk across the supply chain

The supply chain related to IT is expanding as more companies utilize cloud services or outsource IT operations and system development, operation, and maintenance in an effort to reduce costs and focus on core operations. As a result, even though companies may have strong security measures in place, there have been an increasing number of cases of cyber-attacks exploiting weak points in their supply chains, such as contractors with inadequate security measures. While it is difficult to completely prevent damage from supply chain attacks on the chain of organizations that spread over the commercial distribution channels, the entire supply chain should be understood and appropriate risk mitigation measures should be taken to minimize the damage in the event of an attack. This risk mitigation measures include managing contractors collectively by applying the security measures of the owner, i.e., the company that seeks to outsource its operation(s) from the contractors, to all of its contractors, as well as ensuring that contractors have sufficient measures in place to prevent supply chain attacks before signing a contract [10]. In either of these methods, the first step that must be taken is to understand the status of security measures across the entire supply chain, including contractors, and to assess the risks appropriately.

(4) Challenges in assessing supply chain risk

When an owner conducts a risk assessment of its contractors, it generally uses either (1) a security baseline established by the owner itself to assess the status of security measures, or (2) a risk assessment service provided by a security company.

In the case of (1), not only does the owner have to establish its own security baseline, but it also takes time to check and compile the responses of the contractors, which can slow down the process of determining the security of the contractors. At a time when technological

and social trends are changing rapidly, if entering into a contract takes longer due to delays in decision-making, it will delay the launch of the business and lead to lost business opportunities.

In either case of (1) or (2), a contractor needs to go through a risk assessment a number of times, if the contractor seeks to do business with multiple owners. In many cases, the assessment items vary depending on the owner or the risk assessment service, and as a result, contractors need to meet an enormous number of security requirements, which is a heavy burden for them.

2.2.2. What is the MVSP?

(1) The MVSP overview

The MVSP was developed by several companies across industries, including Google, Salesforce, Okta, and Slack, to ease the burden of assessing risks in a supply chain, including contractors as mentioned above [9]. The MVSP is a checklist consisting of 24 controls that should be implemented at a minimum. The MVSP covers most of the requirements identified from analyzing security assessment items used by several companies, such as Google [11]. The 24 controls can be divided into four categories: business controls, application design controls, application implementation controls, and operational controls. The checklist provides specific details that should be implemented for each control. In addition to the checklist, an FAQ section is provided, presenting a detailed description of each control and the reasons why each control is important for security measures [12]. Below is an excerpt from the MVSP checklist.

Table 2-3: MVSP checklist (excerpt) [13]

Control category name	Control name	Control description
1 Business controls	1.4 External testing	Contract a security vendor to perform annual, comprehensive penetration tests on your systems
	1.7 Incident handling	Notify your customers about a breach without undue delay, no later than 72 hours upon discovery. Include the following information in the notification: ・ Relevant point of contact ・ Preliminary technical analysis of the breach ・ Remediation plan with reasonable timelines
2 Application design controls	2.1 Single Sign-On	Implement single sign-on using modern and industry standard protocols
	2.4 Password policy	If password authentication is used in addition to single sign-on: ・ Do not limit the permitted characters that can be used ・ Do not limit the length of the password to anything

		below 64 characters ・Do not use secret questions as a sole password reset requirement ・Require email verification of a password change request ・Require the current password in addition to the new password during password change ・Verify newly created passwords against common passwords lists or leaked passwords databases ・Check existing user passwords for compromise regularly ・Store passwords in a hashed and salted format using a memory-hard or CPU-hard one-way hash function ・Enforce appropriate account lockout and brute-force protection on account access
	2.6 Dependency Patching	Apply security patches with a severity score of "medium" or higher, or ensure equivalent mitigations are available for all components of the application stack within one month of the patch release
3 Application implementation controls	3.3 Vulnerability prevention	Train your developers and implement development guidelines to prevent at least the following vulnerabilities: ・Authorization bypass. Example: Accessing other customers' data or admin features from a regular account ・Insecure session ID. Examples: Guessable token; a token stored in an insecure location (e.g., cookie without secure and httpOnly flags set) ・Injections. Examples: SQL injection, NoSQL injection, XXE, OS command injection ・Cross-site scripting. Examples: Calling insecure JavaScript functions, performing insecure DOM manipulations, echoing back user input into HTML without escaping ・Cross-site request forgery. Example: Accepting requests with an Origin header from a different domain ・Use of vulnerable libraries. Example: Using server-side frameworks or JavaScript libraries with known vulnerabilities
	3.4 Time to fix vulnerabilities	Produce and deploy patches to address application vulnerabilities that materially impact security within 90 days of discovery.

4 Operational controls	4.1 Physical access	Validate the physical security of relevant facilities by ensuring the following controls are in place: ・ Layered perimeter controls and interior barriers ・ Managed access to keys ・ Entry and exit logs ・ Appropriate response plan for intruder alerts

(2) Comparison with existing security baselines

Well-known security baselines include "CIS Controls" managed by the Center for Internet Security (CIS), a U.S. non-profit organization, and "Non-Functional Requirements Grades" released by the Information-technology Promotion Agency, Japan (IPA).

The CIS Controls are renowned globally, and many companies refer to this security baseline to formulate their own rules and implement security measures. The CIS Controls are a list of countermeasures that describes best practices of technical countermeasures against cyber attacks, categorized into 18 controls. The CIS Controls show Implementation Groups (IGs) for each control, enabling users to prioritize implementation according to the size and maturity of their organizations. The CIS Controls also list 153 specific measures an organization should take to implement the controls, and present a glossary of terms, the importance of each control, implementation procedures, and information on tools and other resources [14]. The CIS Controls are designed with an emphasis on the feasibility of individual measures and provide specific procedures and tools for implementing controls. In addition, the CIS Controls do not use ambiguous language to avoid different interpretations by different people, and define threshold values for some measures so that the level of implementation of measures, etc., can be measured.

The Non-Functional Requirements Grades provide an exhaustive list of non-functional requirement items for system infrastructure. They are formulated for the purpose of ensuring a common understanding between the client and the vendor when presenting and proposing non-functional requirements during requirement definition and other phases of system development. Requirement items are classified into six categories: availability, performance/scalability, operation/maintainability, migratability, security, and system environment/ecology, with 37 requirements related to security. The requirement levels are shown in phases according to the importance of the system. In addition to the list of requirement items, a user's guide is available that includes a glossary of terms and instructions for use [15].

Below is a summary of the features and advantages/disadvantages of the MVSP and existing security baselines.

Table 2-4: Features and advantages/disadvantages of security baselines

Security baselines	Features	Advantages	Disadvantages
MVSP	・Limited to security requirements to assess the security of targeted companies and fewer items in the checklist ・Specifically shows how to achieve the controls, and clearly indicates the decision criteria and importance of the controls	・Can simplify the risk assessment process ・Less likely to cause discrepancies in perception	・Less comprehensive in security requirements ・Applicable to only limited types of organizations
CIS Controls	・Offers comprehensive technical countermeasures that are practical and based on trends in cyber-attacks ・Specifically shows how to achieve the controls, and clearly indicates the decision criteria and importance of the controls ・Compatible with other security frameworks ・Can prioritize implementation according to the size and maturity of the organization ・Popular globally	・Applicable to organizations of all sizes and maturity levels ・Less likely to cause discrepancies in perception ・Strong affinity with global companies	・Costly to address all the numerous security requirements
Non-Functional Requirements Grades	・Limited to security requirements for system infrastructure ・Distinguishes between critical and non-critical items ・Shows the quantitative requirement level for each requirement item ・User's guide with extensive information	・Easy to prioritize measures ・Can make quantitative assessment	・Does not include security requirements to be realized outside of the system infrastructure ・Used only in Japan

Of the three baselines, the CIS Controls offer the most comprehensive security requirements. The CIS Controls may be a good choice when the comprehensiveness of security requirements is more important than monetary and time costs, such as when

developing rules for your own company or when conducting risk assessments for systems and companies that handle highly important information. On the other hand, when an owner performs risk assessments for a large number of contractors, the budget allocated to each contractor may be limited, or the emphasis may be on speed. In such cases, it may be a good idea to utilize the MVSP, which is focused on minimum security requirements. The Non-Functional Requirements Grades may be a better fit for requirement definition and other phases of system development, as they focus on security requirements to be realized in system infrastructure and indicate requirement levels according to the system's importance. As described above, different security baselines have different features and advantages/disadvantages, so it is recommended to pick the one suitable for your purpose.

2.2.3. Advantages and cautions when using the MVSP

While risk assessment of contractors is critical to reducing risk across the supply chain, the more complex the supply chain becomes, the greater the burden on both the owner and the contractors. By using the MVSP for risk assessment of contractors in the supply chain, the owner and the contractors can benefit the following advantages listed in Table 2-5.

Table 2-5: Advantages of using the MVSP for owners and contractors

Owners	Contractors
No need to develop their own security baseline	No need to deal with the unique requirements of each owner just by meeting the MVSP requirements
Less time required for risk assessment of contractors (checking and analyzing their responses, etc.)	Less time required to answer a checklist
Can shorten the contract review process by selecting a contractor that complies with the MVSP	Compliance with the MVSP appeals to customers

The MVSP can be used for risk assessment of contractors at the time of contracting and on a regular basis. Since the contents and standards of security measures and the reasons why they should be implemented are clearly indicated, there is less likelihood of discrepancies in perception of the contents of the measures between the owner and the contractors at the time of contracting. In addition, because the checklist contains only 24 items, the burden on both the contractors who answer the questions and the owner who assesses and analyzes the answers is minimized. The MVSP can also be used to develop a Request for Proposal (RFP). By designating the MVSP as security requirements in the RFP, the owner can ensure a minimum level of security with a simple review process.

Note, however, that in all of the above cases, the MVSP provides only minimal security. Companies that require a high level of security measures to handle large amounts of credit card information or sensitive information such as genetic information are recommended to implement industry standard security measures and additional measures on top of the MVSP.

2.2.4. Conclusion

We expect supply chains to become increasingly complex as globalization and diversification of business models continue. It will be more difficult to accurately identify risks across the supply chain, and measures will most likely be deficient. As a result, we can expect to see more companies with inadequate security measures in their supply chains and more companies falling victim to supply chain attacks in the future. Since there is no definitive countermeasure against supply chain attacks, it is important not to create vulnerabilities in any part of the supply chain. To achieve this, risks in the entire supply chain must be properly assessed and measures must be taken from areas of high risk. However, traditional risk assessment processes are complex, time-consuming, and burdensome for both the assessor and the assessed, making it difficult to assess risk for all organizations in the supply chain. Since the MVSP offers a simplified risk assessment process and helps to ensure a minimum level of security, we expect more companies to adopt it for risk assessment across their supply chains. If more companies adopt the MVSP in the future, it may become the de facto standard. It may be a good idea for potential owners and contractors to be prepared to use the MVSP.

3. Data breach, “EC-CUBE vulnerability-related incidents continue”

On May 7, 2021, EC-CUBE Co., Ltd. released an awareness raising article regarding EC-CUBE’s cross-site scripting (XSS) vulnerabilities. [16] In the previous reports for the first and second quarters of FY2021, we discussed the incidents that had occurred due to these vulnerabilities and the countermeasures against them [17] [18]. In the third quarter as well, there were still cases of credit card information and other data being leaked from EC sites due to attacks that exploited the said EC-CUBE vulnerabilities.

This section discusses the reasons for the delay in addressing vulnerabilities and how to properly take countermeasures, based on past incidents.

3.1. EC-CUBE vulnerabilities released in May 2021

(3) Explanation of vulnerabilities in the main body and a plug-in

EC-CUBE has two vulnerabilities released in May 2021 that make an XSS attack possible. Normally, web pages where users enter text strings will take measures so that if a script is entered instead of the expected string, the script will not be executed. However, the EC-CUBE 4.0 series deactivated the process of sanitizing entered scripts. This is the first vulnerability, CVE-2021-20727. In addition, the EC-CUBE 3.0 series had a sanitizing process in place, but a certain plug-in implemented a process to restore sanitized scripts to an executable state. This is the second vulnerability, CVE-2021-20735.

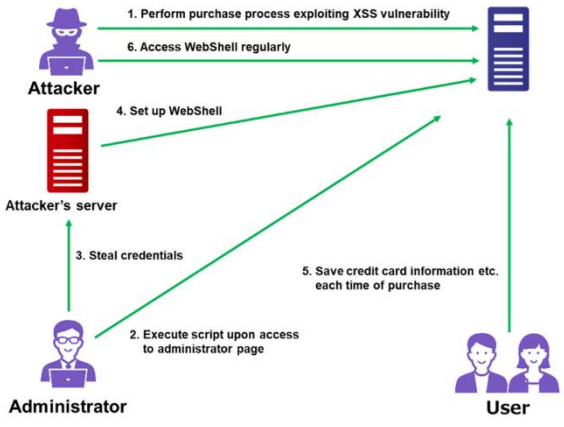


Figure 3-1: Flowchart of XSS attack on EC-CUBE vulnerabilities [19]

Attacks that exploit these vulnerabilities follow the sequence shown in Figure 3-1. An attacker enters a string containing a malicious script into an order form on an EC site. The malicious script entered by the attacker is stored in the EC site's database ((1) in Figure 3-1). In this state, if the administrator of the EC site opens the EC-CUBE administration screen with a browser and views the above order information, the browser will load and execute the malicious script ((2) in Figure 3-1). The attacker's malicious script steals credentials from the administrator's machine and sends them to the server managed by the attacker ((3) in Figure 3-1). The attacker uses the stolen credentials to illegally log in to the EC site and installs a webshell ((4) in Figure 3-1). The attacker can use the installed webshell to steal information whenever a user enters information such as a credit card number into the EC site ((5) and (6) in Figure 3-1).

(4) Cases of damage from XSS attacks on EC-CUBE vulnerabilities

In the second quarter report for FY2021, we presented cases of damage caused by attacks on EC-CUBE that had occurred at that time [18]. The trend continued in the third quarter as well and as shown in Table 3-1 below, cases of damage caused by the same vulnerabilities have been reported.

Table 3-1: Cases of damage to EC sites using EC-CUBE (Q2 and Q3 of FY2021)

#	Date Released	EC Site Name	EC Site Operating Company
1	7/6/2021	Hoick [20]	Songbookcafe Inc.
2	7/12/2021	Cosmos Online Store [21]	Cosmos Pharmaceutical Corporation
3	7/13/2021	TRANSIC [22]	Transic Co., Ltd.
4	7/14/2021	Yomifa Net [23]	Yomiuri Joho Kaihatsu Osaka Co., Ltd.
5	7/20/2021	EC Site Pro Shop Takumi [24]	Candeal Design Co., Ltd.
6	7/21/2021	Mainichigenki Official Shopping Site [25]	Mainichigenki Co., Ltd.
7	7/26/2021	KQLFT TOOLS [26]	Sons-Market Inc.
8	8/16/2021	FUKUYAONLINE [27]	Fukuya Co., Ltd.
9	8/18/2021	The Hair Bar Tokyo Online Store [28]	Gap International Inc.
10	8/23/2021	Komaki Music website [29]	Komaki Music Inc.
11	9/7/2021	Tachikichi Online Shop [30]	Tachikichi Corp.
12	9/14/2021	Ise Sekiya Online Shop [31]	Sekiya Co., Ltd.
13	9/16/2021	Omni EC System [32]	GR Inc.
14	10/21/2021	ALPHAICON [33]	Icons Co., Ltd.
15	10/26/2021	www.tapiocaworld.jp [34]	Nettower Co., Ltd.

16	10/28/2021	Tanax Online Shop [35]	Tanax Co., Ltd.
17	11/2/2021	Beisia Net Shopping [36]	Beisia Co., Ltd.
18	11/2/2021	Parts Club Online [37]	Endless Co., Ltd.
19	11/2/2021	Roomdeco Online Shop [38]	Kanetaya Co., Ltd.
20	11/9/2021	LINK IT MALL [39]	Link It Co., Ltd.
21	11/16/2021	Kyorindo Online Shop [40]	Kyorindo Pharmacy Co., Ltd.
22	11/18/2021	Grantomato Online Shop [41]	Grantomato Co., Ltd.
23	11/18/2021	tocochan.com EC site[42]	tocochan.com, Ltd.
24	12/2/2021	Shibazushi Online Shop [43]	Shibazushi Co., Ltd.
25	12/2/2021	EVANGELION STORE [44]	GroundWorks Co., Ltd.

3.2. Trends of companies that disclosed their damage from incidents

Analysis of information and reports from companies that have suffered damage from incidents in Table 3-1 reveals the following trends:

(1) Industry and size

Table 3-1 shows that companies in a wide variety of industries were affected by attacks targeting the vulnerabilities in question. In addition, many of the companies that disclosed their damage are small and medium-sized enterprises, relatively speaking. While recognizing the importance of security measures, these companies might have been unable to allocate sufficient budgets and personnel to fully investigate and address the vulnerabilities, resulting in damage from the said vulnerabilities.

(2) Time of incident discovery

Analysis of the damage reports of the companies listed in Table 3-1 reveals that most of the operators became aware of the incidents after they were contacted by credit card companies or customers about fraudulent credit card use. We surmise why the operators were unaware of the incidents until they were contacted by an outside party, as follows.

- Unable to take action using security products.
  - Security products were not installed.
  - Poorly installed, security products did not detect fraudulent activities.
  - Security products detected fraudulent activities but people made a bad call.
- No monitoring of breaches or regular examination of logs.
  - Web access logs for EC sites were not monitored.
  - Logs of administrator logins and operations were not regularly audited.
- Problems with the implementation of a vulnerability countermeasure cycle.
  - Did not implement configuration management and vulnerability information collection.
  - Did not conduct vulnerability risk assessments.
  - Did not or could not conduct a breach investigation.

3.3. Vulnerability countermeasures to be taken by affected companies.

In the report for the second quarter of FY2021, we highlighted incidents caused by FortiGate vulnerabilities to illustrate the importance of properly implementing a vulnerability countermeasure cycle. [18] From the results of the analysis in 3.2, we surmise that most of the EC sites that suffered damage due to EC-CUBE vulnerabilities did not implement sufficient “(1) configuration management” and “(2) vulnerability collection” in their vulnerability countermeasure cycles. We suspect that this is why the vulnerabilities were left unchecked until receiving damage reports from credit card companies or customers. The first step in vulnerability countermeasures is to ensure that (1) configuration management and (2) vulnerability collection are conducted.

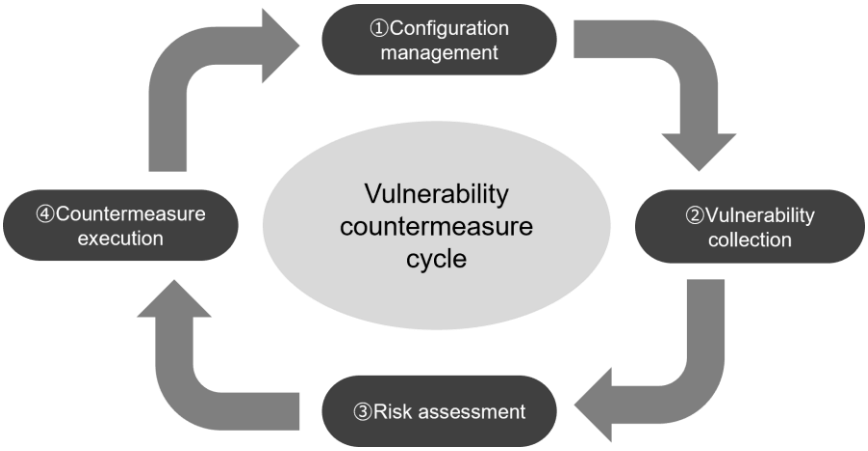


Figure 3-2: Vulnerability countermeasure cycle [18]

In addition, EC-CUBE disclosed an improper access control vulnerability, CVE-2021-20841, and a cross-site request forgery vulnerability, CVE-2021-20842 in November 2021, although the impacts were less severe than those of the May 2021 vulnerabilities. [45] [46] Like in this case, sometimes multiple vulnerabilities can be found one after another in a single product. In the article on the FortiGate incident case, we proposed that organizations should develop their own security systems to ensure that a vulnerability countermeasure cycle is implemented in them. However, as mentioned in 3.2, the affected companies in Table 3-1 include many small and medium-sized enterprises that would have difficulty establishing and operating security systems on their own. These small and medium-sized companies commonly outsource the entire construction and operation of their EC sites from outside vendors. Therefore, they should outsource the maintenance and operation of their EC sites from contractors that meet the following conditions:

- Able to implement a vulnerability countermeasure cycle
  - Able to manage configurations
  - Able to collect vulnerability information, able to perform risk assessment and impact analysis of vulnerabilities
  - Able to apply patches and take provisional measures
  - Able to investigate breaches
- Has obtained ISMS, PrivacyMark, or other third-party certification.

If it is difficult to outsource the maintenance and operation of your EC site from a contractor that meets the above conditions, consider using a SaaS-type cloud service. When using such a service, you would feel more reassured with a cloud service that has a track record of proactively disclosing information or responding promptly when vulnerabilities are found. If you are unsure of how cloud services address vulnerabilities, choose a service that has obtained third-party certification, such as ISO/IEC 27017 or ISMS cloud security certification.

3.4. Conclusion

Reports of damage from attacks exploiting the XSS vulnerabilities in EC-CUBE continued even in December 2021, more than six months after the public announcement. As mentioned in 3.2, it seems that many of the affected companies were unaware of the disclosed vulnerabilities and were attacked without taking effective countermeasures. Therefore, leaving disclosed vulnerabilities unattended will most likely result in being attacked and suffering damage. Introducing and continuously implementing a vulnerability countermeasure cycle, including the collection of vulnerability information, is an effective countermeasure. However, small and medium-sized companies that do not have an adequate information security system will find it difficult to implement a vulnerability countermeasure cycle on their own. When outsourcing system development and operation, these companies should hire contractors that can reliably handle a vulnerability countermeasure cycle, or proactively utilize SaaS-type cloud services.

4. Vulnerabilities, “vulnerabilities in Zoho's UEM products”

This chapter explains several vulnerabilities in Zoho Corporation's ManageEngine Desktop Central. The National Institute of Standards and Technology (NIST) has listed these vulnerabilities in its National Vulnerability Database (NVD), rating them critical vulnerabilities with a CVSS score of 9.8. Companies and organizations using the said product must apply the relevant patch as soon as possible.

4.1. Vulnerabilities in Zoho's UEM products

4.1.1. Overview of the vulnerabilities

On December 3, 2021, Zoho Corporation released a security advisory and patch for vulnerability CVE-2021-44515 in ManageEngine Desktop Central and vulnerability CVE-2021-44526 in ManageEngine ServiceDesk Plus. [47] CVE-2021-44515 is a vulnerability that makes it possible to bypass authentication when connecting to the ManageEngine Desktop Central agent remotely. An attacker could send a crafted request to the agent to bypass authentication and remotely execute arbitrary code. CVE-2021-44526 is another vulnerability that allows bypassing authentication. By sending a crafted request targeting an application filter vulnerability, an attacker could bypass authentication and gain access to functions that are only available to authenticated users. These vulnerabilities are zero-day vulnerabilities with attacks occurring prior to patch release. State-sponsored attack groups are exploiting these vulnerabilities in their attacks.

According to an FBI report, an APT (Advanced Persistent Threat) attack group has been conducting zero-day attacks exploiting these vulnerabilities since as early as late October 2021. [48] This APT attack group has launched three attack campaigns since August, compromising at least 13 organizations. First, on September 16, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. warned that an APT attack group was carrying out Campaign 1 in Figure 4-1 by exploiting a vulnerability in ManageEngine's ADSelfService Plus, a self-service password management and single sign-on solution. On November 7, Palo Alto Networks announced that at least nine organizations had been compromised in Campaign 2. The APT attack group then changed the target to another ManageEngine product, ServiceDesk Plus, in Campaign 3 and compromised multiple organizations by exploiting the vulnerabilities between October 25 and November 8.

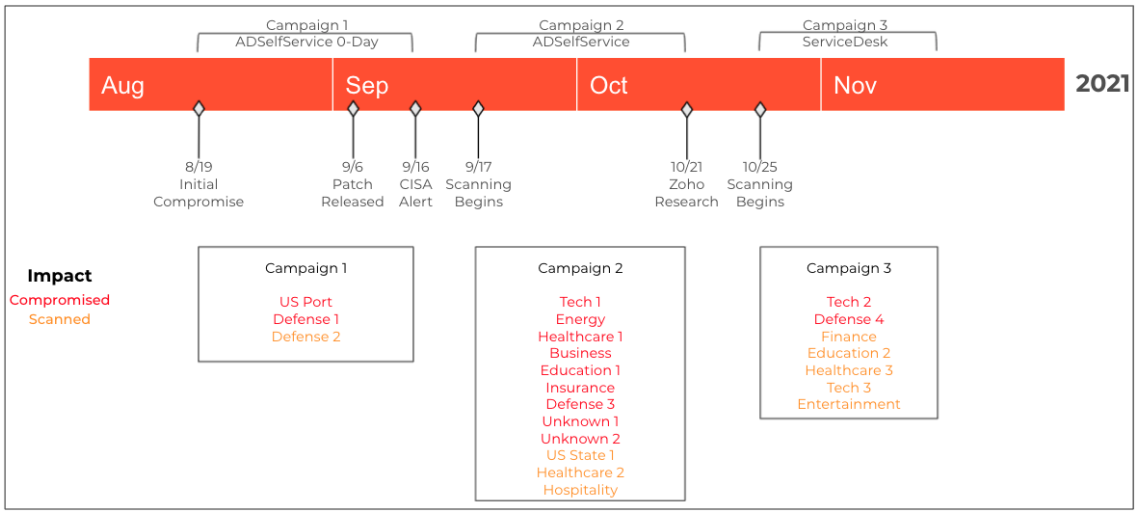


Figure 4-1: Campaign timeline and impact [49]

4.1.2. Overview of ManageEngine products

ManageEngine Desktop Central is a software product called Unified Endpoint Management (UEM) that allows system administrators to provide centralized control from a unified console over patch management for employee terminals, software installation, license management, connection control for various external devices, and mobile device management. [50] Once an agent is installed on the device to be managed, be it a Windows, Mac, or Linux device, system administrators can access the device from anywhere via the network and perform various types of management and remote control. Whether the device is in another building or overseas, it can be efficiently managed remotely as long as it is connected to the network.

ManageEngine ServiceDesk Plus is a web-based IT service management tool with abundant functions including incident management, problem management, change management, CMDB, asset management, and customer satisfaction surveys.

4.1.3. Description of vulnerabilities CVE-2021-44515 and CVE-2021-44526

As discussed in 4.1.1, CVE-2021-44515 is a vulnerability in which authentication can be bypassed. By sending a specially crafted request to a vulnerable agent, an attacker can exploit CVE-2021-44515 to bypass authentication to ManageEngine Desktop Central and execute arbitrary code remotely. We surmise that the vulnerability can be exploited to remotely install software on the machine where the agent is running, or to directly manipulate the command prompt. An APT attack group exploits vulnerability CVE-2021-44515 to upload a webshell without authentication via the API of ManageEngine Desktop Central. This webshell overrides the legitimate ManageEngine Desktop Central API functionality. The webshell retrieves request communications delivered to ManageEngine Desktop Central, extracts the attacker's instructions from them, and uses the system user authority to execute

commands. The APT attack group uses the machine compromised using the above webshell as a launching pad to launch the next attack. The APT attack group attacks a domain controller to gain entry and obtains credentials using Mimikatz, or retrieves passwords from the LSASS process memory with pwdump or ProcDump.

CVE-2021-44526 is a vulnerability in which a servlet program can be accessed without authentication by sending a crafted URL and exploiting an issue of incorrectly configured application filters. According to Palo Alto Networks, the vulnerability exists in the REST API for remotely managing ManageEngine ServiceDesk Plus. An APT attack group first uses a crafted URL to request a malware (dropper) file named “msiexec.exe” to be uploaded to the REST API of the ManageEngine ServiceDesk Plus server. Authentication is not required at this time. The APT attack group then requests the REST API to activate this msiexec.exe using the same procedure. At this point, the APT attack group configures ManageEngine ServiceDesk Plus to execute malware instead of the legitimate msiexec.exe. After successful execution of the malware, a mutex is created, which is an exclusive control mechanism to prevent multiple malware programs from running on the same machine. Since this mutex was the same as the mutex of the malware found in Attack Campaigns 1 and 2, we surmise that the attacks are from the same APT attack group. This malware downloads a webshell from the APT attack group's server, loads it into memory, and executes it. This webshell works by using the Java Servlet Filter function of Apache Tomcat. During the filtering process, only instruction communication from the APT Attack Group to the webshell is extracted, so the extracted information is passed to the webshell without the need to designate a specific destination URL. Therefore, security filters are also bypassed. The APT attack group can remotely control the ManageEngine ServiceDesk Plus server using the webshell installed by exploiting this vulnerability. [51]

4.1.4. Danger of the vulnerabilities

These vulnerabilities in UEM products present different kinds of dangers than vulnerabilities in products that allow remote connectivity. What would be the impact if an attacker attacked and hijacked a UEM product?

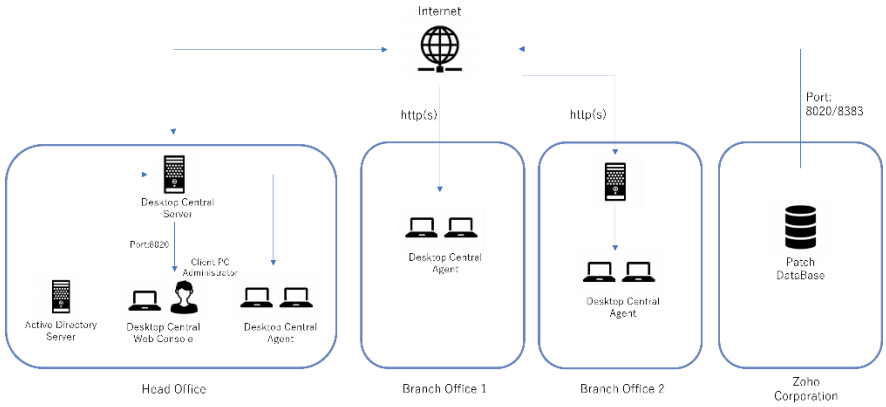


Figure 4-2: Architecture of ManageEngine Desktop Central [50]

If an APT attack group is able to attack and remotely control the ManageEngine Desktop Central or ServiceDesk Plus servers located in the headquarters shown in Figure 4-2, the server management functions of a ManageEngine application can be used. As described in 4.1.2, ManageEngine Desktop Central allows users to remotely install software and execute commands on all agents-installed terminals. An APT attack group can install malware on all terminals, or can steal information on the terminals.

ManageEngine ServiceDesk Plus is a web-based IT service management tool and does not provide the ability to remotely control terminals. However, an APT attack group can use the ManageEngine ServiceDesk Plus server as a launching pad to attack adjacent Active Directory servers. If an APT attack group succeeds in penetrating an Active Directory server and gains administrative privileges for a Windows domain, it may compromise terminals participating in the Windows domain or expand the scope of compromise to trusted domains (lateral movement).

4.2. Conclusion

Compared to cases where an attacker compromises a terminal within an organization or system and uses it as a launching pad to expand the scope of the compromise, an attacker who compromises a UEM product and obtains administrative privileges can easily infect a large number of machines with malware, steal confidential information, or expand the scope of the compromise. The UEM product that was originally designed to protect your information and assets is transformed into a product that aids attackers. Software that integrates and centrally manages large numbers of machines, such as UEM products, must be protected by stronger security measures to prevent attackers from exploiting them. If a breach occurs, the impact can spread over a wide area in a short period of time, making it difficult to take provisional measures and restore the system. Be prepared for emergencies by considering in advance how to identify the scope of impact, how to prevent the spread of damage, e.g., through network shutdown or system shutdown, and how to restore the system.

5. Malware/ransomware, “EMOTET resumed attack activities”

According to a report by the Record by Recorded Future, EMOTET, which was taken down in January 2021, resumed its attack activities around November 14, 2021. [52] Later, on November 16, 2021, the IPA issued an alert regarding attack e-mails, titled “Resumption of EMOTET Attack Activities”. [53]

This section discusses the background and purpose behind the resumption of EMOTET's attack activities, describes the characteristics of the resumed EMOTET attacks, and provides alerts.

5.1. History of EMOTET

EMOTET infects users when they click on attachments or links in attack e-mails that are disguised as legitimate e-mails, causing theft of confidential information or secondary infection with other malware. EMOTET communicates with a command and control server (hereinafter referred to as “C2 server”) prepared by the attacker on the Internet. The main body of EMOTET malware is highly flexible and modular, characterized by the ability to easily add functions and form a large botnet with a C2 server. After its first appearance around 2014, EMOTET caused massive damage around the world. However, on January 27, 2021, under the orchestration of EUROPOL and EUROJUST, the police of eight countries, including the Netherlands and Germany, cooperated to carry out Operation LadyBird, and EMOTET's operational infrastructure was shut down (taken down). Please refer to our “Quarterly Report on Global Security Trends, 4th Quarter of 2020” for a detailed description of the takedown process from start to finish.

According to the IPA, after the takedown, information and observations of EMOTET gradually decreased, and EMOTET attacks and damage either stopped or decreased significantly. [53] In addition, according to a report by JPCERT/CC, the EMOTET program was to update itself automatically to a detoxified program and stop working when the infected terminal's clock struck 12:00 on April 25, 2021. As a result, almost no EMOTET infections were observed in Japan after April 26, 2021. [55]

However, around November 14, 2021, the Record by Recorded Future announced that it had confirmed the resumption of EMOTET's attack activities. [52] The IPA has also provided information on EMOTET attack e-mails that were actually received. [53] After the attack has resumed, the scale of infection is no less than before the takedown. In December 2021, the number of malicious URLs related to EMOTET that were reported to URLhaus, a project for eradicating malicious sites, was almost double the number of malicious URLs reported in

December 2020.

So, why did EMOTET resume its attack activities? The following section provides possible background and objectives.

5.2. Explaining the resumption of EMOTET attack activities

5.2.1. Background of resumed attack activities

Prior to the takedown, EMOTET attack groups were infecting computers with various malware, including TrickBot/Qbot, via EMOTET (secondary infection). TrickBot/Qbot attack groups were infecting computers with and executing Conti (formerly Ryuk), DoppelPaymer, Darkside, Revil and other ransomware via TrickBot and other means (tertiary infection).

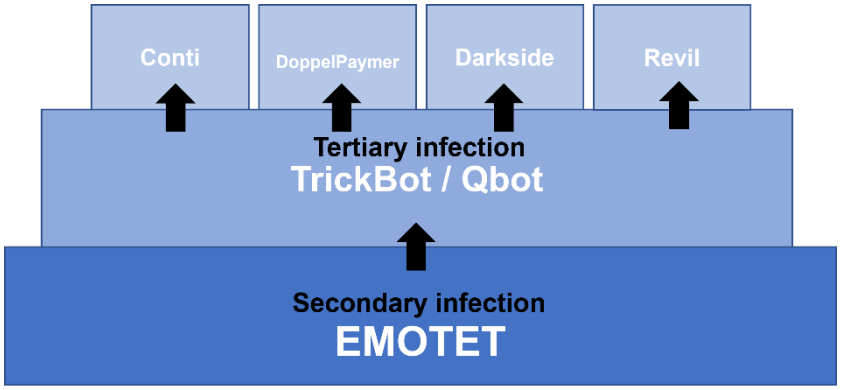


Figure 5-1: Image of other malware infection using the EMOTET platform

When the police took down the EMOTET botnet in January 2021, these ransomware attack groups were no longer able to attack using the EMOTET botnet. As a result, several attack groups that had been using the EMOTET botnet stopped their ransomware attack activities.

However, of these attack groups, only the Conti ransomware attack group began to gather human resources from other inactive ransomware attack groups and work toward rebuilding the EMOTET botnet. The Conti ransomware attack group was spreading its own malware using the EMOTET botnet platform and is believed to have approached a TrickBot attack group, with which it had previously partnered, to initiate rebuilding of EMOTET. [57] According to reports from Bleeping Computer and BlackBerry, the TrickBot/Qbot attack group sent an EMOTET loader (a program responsible for infecting machines by downloading EMOTET to them) to TrickBot malware-infected devices by using the TrickBot malware and executed it, thus rebuilding the EMOTET botnet. [57] [58] It is believed that this is how the Conti ransomware attack group and the TrickBot/Qbot attack group rebuilt the EMOTET botnet in order to resume their ransomware attack activities.

The above view is a hypothesis by Bleeping Computer and others, but if this is true, the resumption of sending EMOTET attack emails is not aimed at the spread of EMOTET infection, but at the resumption of attack activities by the Conti ransomware attack group.

In the future, if the police again succeed in taking down the EMOTET botnet and arrest members of the attack group running the EMOTET botnet, other attack groups that are also using the EMOTET botnet now are likely to rebuild the EMOTET botnet and resume their ransomware attacks. In this light, the root cause of the problem can only be eliminated through the arrest of or suspension of activities by a broad range of people, including not only EMOTET attack group members, but also the members of the ransomware attack groups with which the EMOTET attack group is affiliated.

5.2.2. Characteristics of resumed attacks

Now, this section describes the differences in characteristics of EMOTET before the takedown and after the resumption of attack activities. It focused on the following two aspects.

(1) Differences in infection methods

The differences in infection methods are the following two points.

The first is the use of new Office files. EMOTET infection methods after the resumption of attack activities are the same as before the takedown, using attack e-mails disguised as replies to legitimate e-mails or cleverly worded attack e-mails that are likely to be opened in the course of business. Attack e-mails have files attached to them. Before the takedown, Microsoft Word macro-enabled document files (with extension “.docm”) were used frequently, but after the resumption, Microsoft Excel macro-enabled documents (“.xlsm”) are used. [59] Office files containing macros may be directly attached to e-mail just as before the takedown, or in some cases they may be attached as zip files. As before the takedown, there are also cases with no attachments. In such cases, a URL is provided in the e-mail. A link is designed so that when the URL is accessed, an Office file containing a macro or an app installer file described below will be downloaded. This URL is called a “Cushion Page.” [60] The macro in this Office file calls PowerShell from the command prompt to retrieve and execute the files necessary to infect the machine with EMOTET.

Next, new cases have been found where PowerShell is attached or an app installer is used. App installer files have been distributed on the aforementioned Cushion Page. The app installer reads an app installer file with the extension “.appinstaller” and launches the installation program. In the case of app installer files distributed on the Cushion Page, an EMOTET dropper disguised as an Adobe PDF is installed, and when the user logs on to Windows, it is launched and downloads EMOTET to infect the machine. [60]

(2) Functional changes in the EMOTET main body

The main body of EMOTET has been functionally changed in the following four points.

First, as a major change, the EMOTET main body now communicates with a C2 server using encrypted communication such as HTTPS. [59] As a result, the method of detecting C2 communication based on communication characteristics is no longer viable for detecting EMOTET's C2 communication on communication paths such as proxies that cannot decrypt

communication contents. Also, HTTP requests have changed from the POST method to the GET method. [59] Detecting methods may need to be reviewed if they are based on the characteristic of EMOTET communication before the takedown, namely, that the destination URL and the referrer are the same URL in the POST method.

In addition, after resuming attack activities, EMOTET contains a randomly generated key name and base64-encoded key value in the cookie header. [59] [61] Also, the address information of the C2 server is hard-coded into the EMOTET main body as it was before the takedown, but after the resumption of attack activities, EMOTET uses an XOR-based algorithm to encrypt the information. [61]

5.3. Countermeasures against EMOTET and Conti ransomware

Just as before the takedown, the EMOTET infection spreads via e-mail after the resumption of attack activities. Therefore, as in the past, it is important to take basic measures such as being vigilant against attack e-mails and their attachments, and not opening suspicious attachments or links. However, as mentioned in the previous section, after the resumption of attack activities, EMOTET uses a wide variety of infection methods, as well as attack e-mails that are disguised as replies or cleverly written as if they were related to business, making it more difficult to prevent infection by determining whether the e-mails are legitimate or not. Therefore, apart from measures that rely on the security awareness of each individual as described above, it is important for organizations to take measures to strengthen their systems in order to prevent or detect EMOTET infection at an early stage. This can be achieved if IoC (Indicator of Compromise) information on EMOTET can be quickly obtained and reflected in security devices such as firewalls and SIEMs. One specific way to achieve this would be to use Malware Information Sharing Platform (MISP). [62] MISP can automatically collect IoC information with the feed function and easily share IoC with other organizations' MISPs using the synchronization function.

In addition, as noted in “6.2.1. Background of resumed attack activities,” the Conti attack group used Trickbot's infrastructure to rebuild the EMOTET botnet. Conti ransomware is “double-extortion ransomware” that not only encrypts, but also steals and discloses information. The ransomware was first discovered only in May 2020, but its attack activities have increased in recent years. According to darkfeed.io, a system that monitors the darknet in real time, Conti accounted for about 24% of all ransomware damage in December 2021, just after EMOTET resumed its activities. [63] The Conti ransomware not only encrypts files on the infected terminal, but also explores accessible shared folders and attempts to encrypt files on other terminals . [64] The Conti ransomware has a short development cycle and is upgraded in a short period of time. Newer versions of Conti ransomware are fileless, meaning that the loader is first infected, and then the loader downloads a DLL, loads it into memory, and executes it. This way, they can avoid Conti ransomware analysis by antivirus software vendors and security experts. [64] Therefore, if we can obtain the IoC information of the Conti ransomware download location and reflect it in the security devices, we can mitigate the

damage.

5.4. Conclusion

This chapter focused on EMOTET, which has resumed its attack activities, and explained the background that led to its resumption and its characteristics. As the background, it is believed that a group that had organized a Conti ransomware attack using EMOTET prior to the takedown used a TrickBot/Qbot attack group to rebuild the EMOTET botnet in order to resume their ransomware attack activities. Compared to before the takedown, the infection methods of EMOTET have changed since the resumption of attacks, and in some cases, conventional methods of detection and identification are no longer applicable. In addition, the infection methods are becoming increasingly sophisticated, making it difficult to prevent infection through human measures alone. Therefore, instead of relying on personal security awareness, we should strengthen our systems, i.e., quickly obtain IoC (Indicator of Compromise) information on EMOTET and apply it to security devices such as firewalls and SIEMs, in order to prevent or detect EMOTET infection at an early stage.

6. Outlook

Changing revenue models of ransomware attack groups

We are seeing a new change in the way ransomware attack groups attack. As typified by the WannaCry outbreak in 2017, the modus operandi of traditional ransomware attack groups was mainly based on a revenue model of encrypting organizational or personal data and charging a ransom in exchange for decrypting the data. In the third quarter of FY2021, cases of ransomware attacks were reported in which the ransomware attack groups did not encrypt the data.

Volvo, a Swedish car manufacturer, fell victim to an attack by the ransomware attack group “Snatch.” Snatch published some of the data stolen from Volvo on its own leak site. A Bleeping Computer article speculates that the Volvo incident also did not involve data encryption, since Snatch has stated that it “does not encrypt data.” [65] Snatch may sell the stolen data to third parties if the victim does not pay the ransom.

More and more organizations are not paying ransoms to ransomware attack groups, partly because the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) issued an advisory regulating ransom payments in 2020. [66] In Japan as well, there have been cases of organizations refusing to pay ransoms. Tsurugi municipal Handa Hospital in Tokushima Prefecture became a victim of ransomware in October 2021 and had its electronic medical records encrypted, but it refused to pay the ransom and chose to recover the records on its own. [67] In the case of blackmailing with encrypted information, ransomware attack groups cannot make a profit if the ransom payment is refused. As a result, it is becoming increasingly difficult to profit from traditional ransomware attacks that demand a ransom.

Therefore, we predict that ransomware attack groups will increasingly try to secure revenue by means other than ransom demands in order to secure profits even if ransoms are not paid. For example, if an attack group like Snatch has stolen a large amount of information from a company, it may be able to redeem that information for cash. If the information stolen is payment information such as credit card numbers or highly redeemable information such as ID/password lists, the ransomware attack group may be able to make money without relying on ransom. In the future, it is quite possible that ransomware attack groups will develop subplans other than ransom demands, such as the sale of stolen information, or develop new means of attack based on new revenue models that circumvent security measures. We are now in a time of transition.

Trends in ransom payments upon ransomware infection

In a ransomware attack, the attacker encrypts files containing information that are company assets and demands a ransom payment for decryption. Despite regulations and instructions from various organizations, such as the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and the police, there is no end to the number of companies that pay the ransom. [68] One of the reasons why cases of ransom payments have not disappeared is that there is cyber insurance that covers ransom payments. Organizations that have this insurance will choose to pay the ransom because it is a quicker and cheaper solution than trying to recover the system themselves at their own expense.

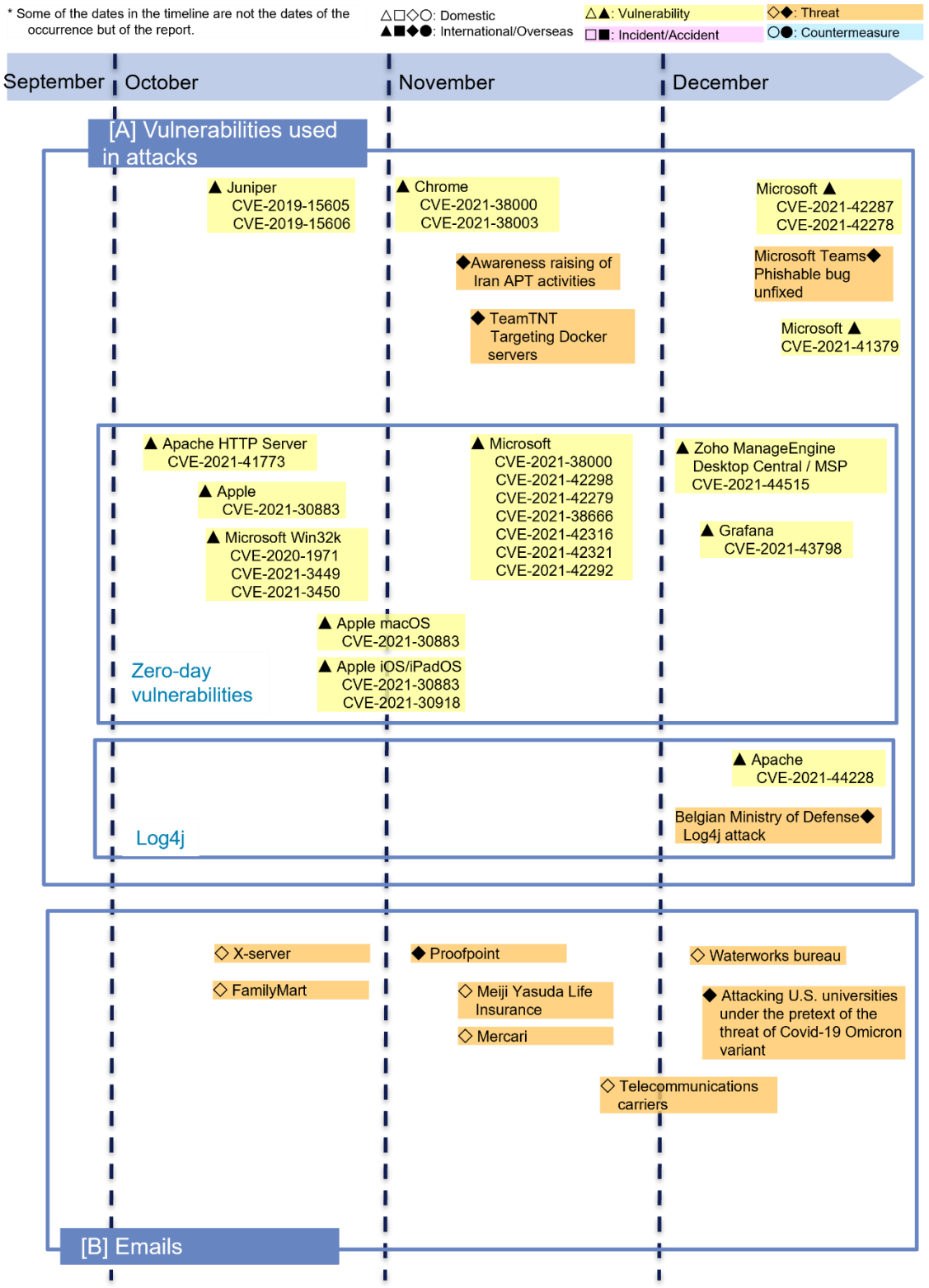
However, this method of paying ransom through cyber insurance may become unusable. Of the top 10 cyber insurers in the U.S. in 2020, four were in the red. [69] We can assume that insurance payouts related to ransomware are increasing, especially in the U.S., where cyber attacks, including ransomware attacks, are more frequent. In fact, ransomware attackers say they are stealing lists of cyber insurance customers from insurance companies and targeting their attacks on companies that can pay the ransom with insurance proceeds. [70] If the insurers' losses continue to grow, they may stop offering insurance riders for ransomware-related ransom payments. If this happens, we expect that many companies that have fallen victim to ransomware will choose not to pay the ransom. If ransom payments are significantly reduced, ransomware attacks could also be significantly reduced.

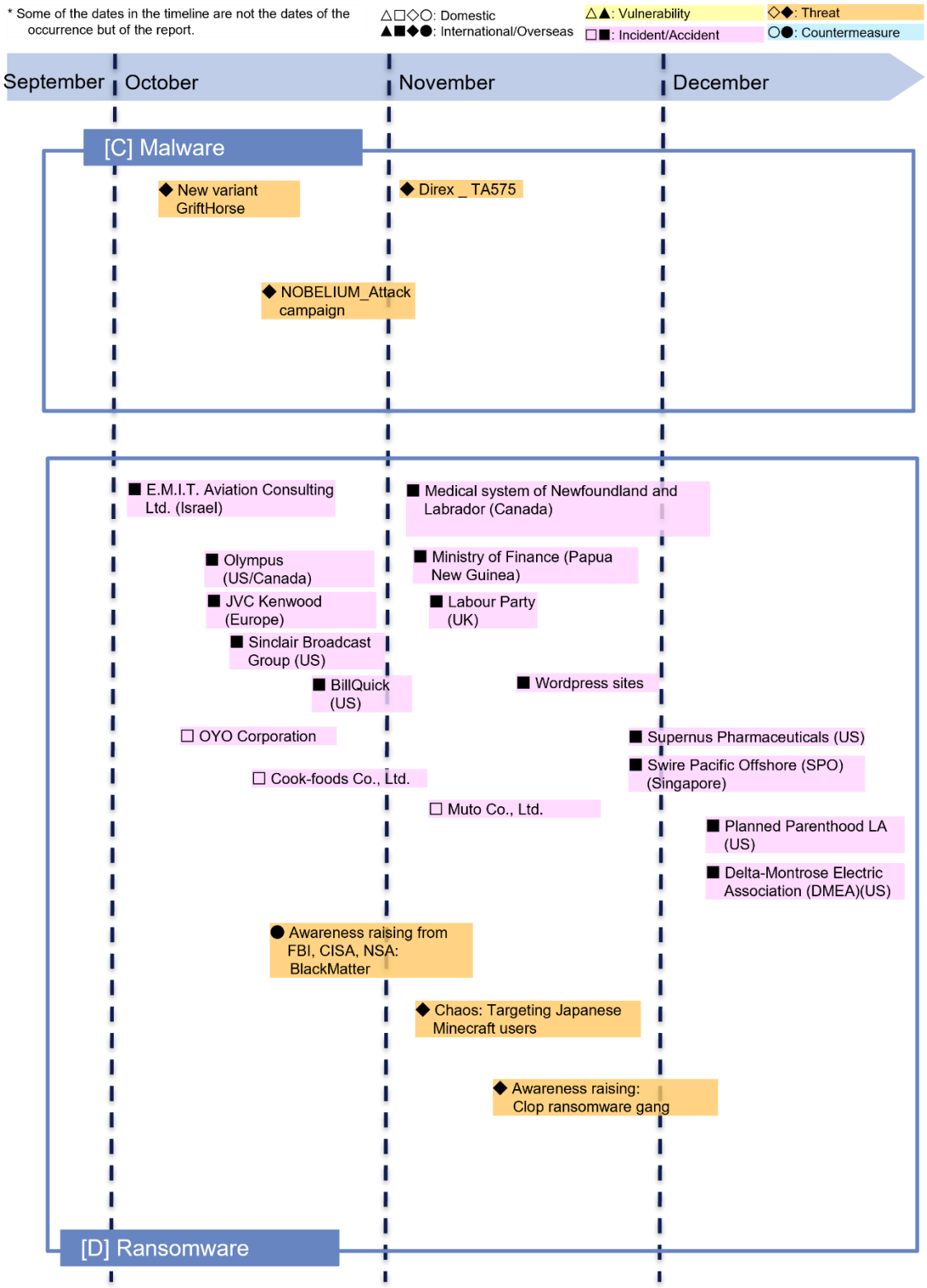
Flourishing of Phishing as a Service (PHaaS)

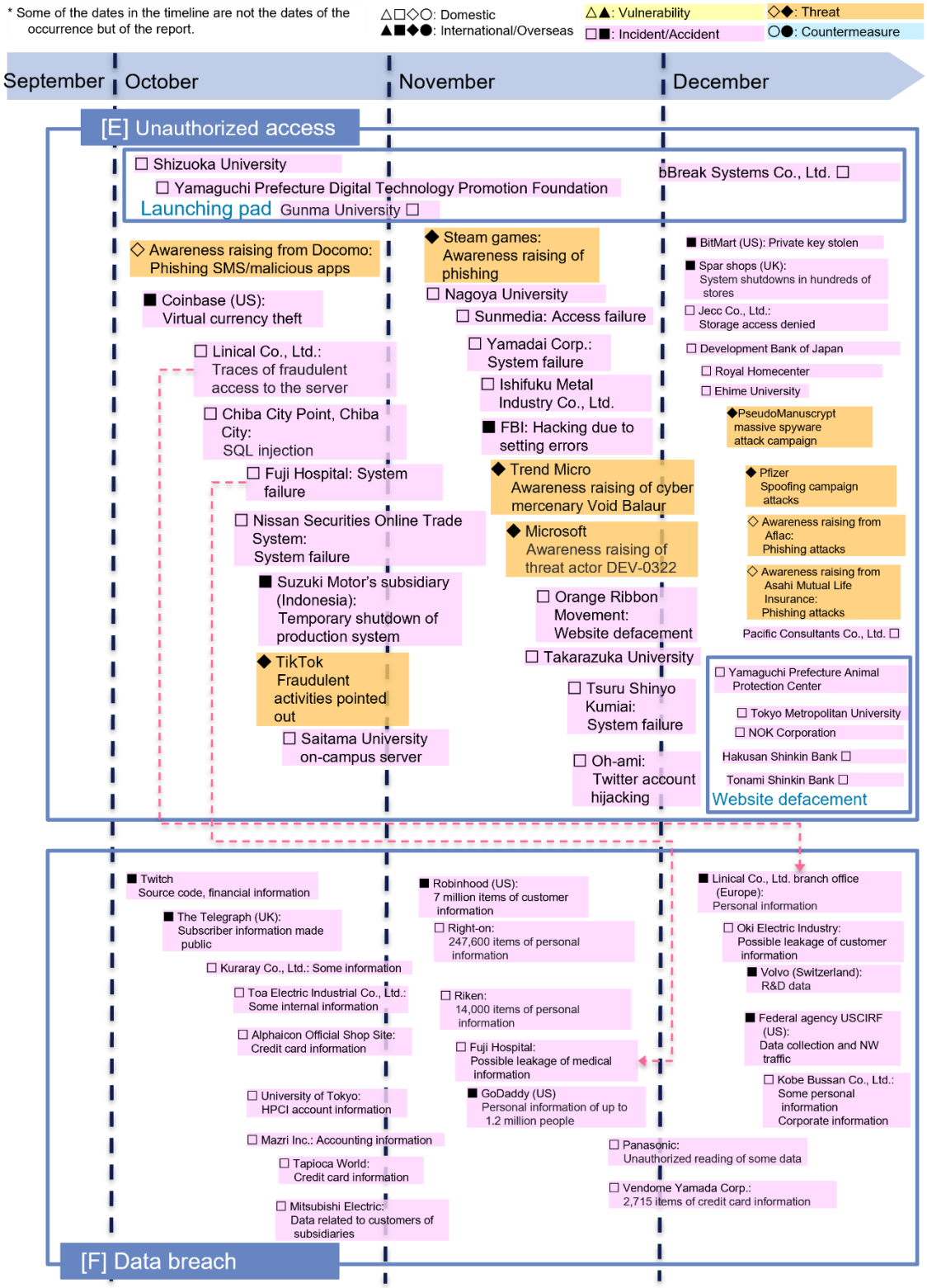
With the increase in remote work due to the coronavirus pandemic, there are more opportunities to connect to internal systems via VPN over the Internet from home or outside the office, or to use cloud services such as Microsoft 365. In response to this situation, phishing attacks aimed at infiltrating internal systems have become widespread. If a phishing attack succeeds in stealing IDs and passwords for company-related accounts, the attacker may, for example, illegally log into a critical system to launch a ransomware attack, which could cause far more damage than if a phishing attack is directed at an individual.

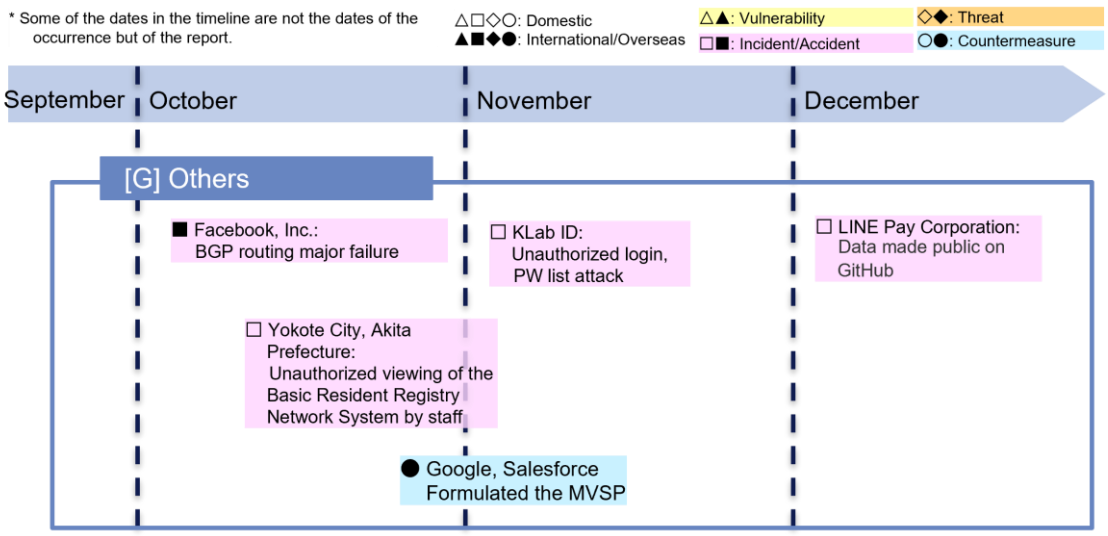
Preparing for executing a phishing attack takes time and effort, including creating a phishing site to steal IDs/passwords, creating phishing e-mails to direct users to the site, collecting addresses to send the e-mails to, and sending a large number of e-mails. Such tasks required for phishing attacks are being provided as a service for a fee and called "Phishing as a Service (PHaaS)." In the underground world, some vendors specializing in PHaaS have emerged. Some of these PHaaS vendors, as the name implies, provide phishing-related services by dividing up each process required for phishing into smaller functional units and offering them on a subscription basis, depending on the needs of the attacker. There is an ecosystem already in place that allows attackers to efficiently conduct sophisticated phishing attacks. As the PHaaS business flourishes, phishing attacks are expected to increase.

7. Timeline









References

[1] The Apache Software Foundation, “Apache Log4j Security Vulnerabilities,” [オンライン]. Available: https://logging.apache.org/log4j/2.x/security.html#CVE-2021-44832.

[2] Google, “Google Online Security Blog: Understanding the Impact of Apache Log4j Vulnerability,” 17 12 2021. [オンライン]. Available: https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html.

[3] Swiss Government Computer Emergency Response Team, “Zero-Day Exploit Targeting Popular Java Library Log4j,” 12 12 2021. [オンライン]. Available: https://www.govcert.admin.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/.

[4] Japan Vulnerability Notes(JVN), “Apache Log4jにおける任意のコードが実行可能な脆弱性,” 13 12 2021. [オンライン]. Available: https://jvn.jp/vu/JVNVU96768815/.

[5] The Apache Software Foundation, “APACHE LICENSE, VERSION 2.0,” 1 2004. [オンライン]. Available: https://www.apache.org/licenses/LICENSE-2.0.

[6] NTTデータ, “サイバーセキュリティに関するグローバル動向四半期レポート（2020年10月～12月）,” 16 3 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/news/information/2021/031600/.

[7] National Telecommunications and Information Administration(United States Department of Commerce), “SOFTWARE BILL OF MATERIALS,” [オンライン]. Available: https://www.ntia.gov/SBOM.

[8] 経済産業省, “『第３層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性,” 13 12 2021. [オンライン]. Available: https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/daisanso/pdf/005_03_00.pdf.

[9] R. Hansen, “Google Security Blog,” Google, 27 10 2021. [オンライン]. Available: https://security.googleblog.com/2021/10/launching-collaborative-minimum.html.

[10] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート（2020年度第3四半期）,” 16 3 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2020_3q_securityreport.pdf.

[11] MVSP, “Minimum Viable Secure Product,” 27 10 2021. [オンライン]. Available: https://mvsp.dev/.

[1 MVSP, “MVSP FAQ,” MVSP, 27 10 2021. [オンライン]. Available:
2] https://mvsp.dev/faq.en/index.html.

[1 MVSP, “MVSP Checklist,” MVSP, 27 10 2021. [オンライン]. Available:
3] https://mvsp.dev/mvsp.en/index.html.

[1 Center for Internet Security, “CIS Critical Security Controls Version 8,” Center for
4] Internet Security, 18 5 2021. [オンライン]. Available:
https://www.cisecurity.org/controls/v8.

[1 独立行政法人情報処理推進機構, “システム構築の上流工程強化（非機能要求グレー
5] ド）,” 独立行政法人情報処理推進機構, 18 9 2019. [オンライン]. Available:
https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html.

[1 株式会社イーシーキューブ, “EC-CUBE 4.0系: クロスサイトスクリプティング 脆
6] 弱性 (JVN#97554111) について,” 7 5 2021. [オンライン]. Available:
https://www.ec-cube.net/info/weakness/20210507/.

[1 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2021 年度 第
7] 1 四半期,” 2 11 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-
/media/nttdatajapan/files/services/security/nttdata_fy2021_1q_securityreport.pdf.

[1 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2021 年度 第
8] 2 四半期,” 18 1 2022. [オンライン]. Available: https://www.nttdata.com/jp/ja/-
/media/nttdatajapan/files/services/security/nttdata_fy2021_2q_securityreport.pdf.

[1 JPCERT/CC, “ECサイトのクロスサイトスクリプティング脆弱性を悪用した攻撃,”
9] 6 7 2021. [オンライン]. Available:
https://blogs.jpcert.or.jp/ja/2021/07/water_pamola.html.

[2 ニュースガイア株式会社, “保育関係者向けサイトに不正アクセス - クレカやアカ
0] ウント情報が流出,” 6 7 2021. [オンライン]. Available: https://www.security-
next.com/127865.

[2 株式会社コスモス薬品, “弊社が運営する「コスモスオンラインストア」への不正ア
1] クセスによるお客様情報流出に関するお詫びとお知らせ,” 12 7 2021. [オンライン].
Available:
https://www.cosmospc.co.jp/notice/upload/ed661581b067c469eb29047679fa8a86e
6446fe7.pdf.

[2 ニュースガイア株式会社, “革製品通販サイトに不正アクセス - クレカ情報流出の
2] 可能性,” 13 7 2021. [オンライン]. Available: https://www.security-next.com/128099.

[2 ニュースガイア株式会社, “読売関連会社のネットショップに不正アクセス - クレ
3] カ情報が被害,” ニュースガイア株式会社, 14 7 2021. [オンライン]. Available:
https://www.security-next.com/128114.

[2 株式会社キ ャ ン デ ィ ル, “当社子会社が運営するオンラインショップへの不正

4] アクセスによる個人情報漏洩に関するお詫びとお知らせ," 20 7 2021. [オンライン]. Available: http://fs.magicalir.net/tdnet/2021/1446/20210719469018.pdf.

[2 有限会社毎日元気 , "弊社が運営する「毎日元気公式ショッピングサイト」への不
5] 正アクセスによる個人情報漏えいに関するお詫びとお知らせ," 21 7 2021. [オンライン]. Available: https://www.mainichigenki.co.jp/210721.pdf.

[2 株式会社 SONS-MARKET, "弊社が運営する「KQLFT TOOLS」への不正アクセス
6] による個人情報漏えいに関するお詫びとお知らせ," 26 7 2021. [オンライン]. Available: https://kqlft.com/card.pdf.

[2 株式会社フクヤ, "弊社が運営するオンラインショップへの不正アクセスによる 個
7] 人情報流出に関するお詫びとご報告," 株式会社フクヤ, 16 8 2021. [オンライン]. Available: https://www.fancy-fukuya.co.jp/topics/news20210816/.

[2 ギャップインターナショナル株式会社, "クレジットカード情報流出に関するお詫び
8] とお知らせ," ギャップインターナショナル株式会社, 18 8 2021. [オンライン]. Available: https://thehairbar.jp/blogs/news/information001.

[2 株式会社コマキ楽器, "弊社が運営する「コマキ楽器WEBサイト」への不正アクセ
9] スによる個人情報漏えいに関するお詫びとお知らせ," 株式会社コマキ楽器, 23 8 2021. [オンライン]. Available: https://komakimusic.co.jp/pages/important-notices.

[3 株式会社たち吉, "お詫びとお知らせ 「たち吉オンラインショップ」への不正アク
0] セスによる個人情報漏えいについて," 株式会社たち吉, 7 9 2021. [オンライン]. Available: https://www.tachikichi.co.jp/2021/09/07/%e3%81%8a%e8%a9%ab%e3%81%b3%e3%81%a8%e3%81%8a%e7%9f%a5%e3%82%89%e3%81%9b/.

[3 株式会社関谷食品, "弊社が運営する「伊勢せきやオンラインショップ」への不正ア
1] クセスによる個人情報漏えいに関するお詫びとお知らせ," 株式会社関谷食品, 14 9 2021. [オンライン]. Available: https://www.sekiya.com/notice/.

[3 東芝テック株式会社, "株式会社ジーアールが運営する「オムニＥＣ」への不正アク
2] セスについて," 東芝テック株式会社, 16 9 2021. [オンライン]. Available: https://www.toshibatec.co.jp/information/20210916_01.html.

[3 株式会社アイコンズ, "弊社が運営する「アルファアイコンオフィシャルショップサ
3] イト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ," 20 10 2021. [オンライン]. Available: https://alphaicon.com/uploads/news/file/00000/131/691ecdadfd5530d9f1e034aed6e4532a.pdf.

[3 株式会社ネットタワー, "弊社が運営する「www.tapiocaworld.jp」への不正アクセス
4] による個人情報漏えいに関するお詫びとお知らせ," 25 10 2021. [オンライン].

Available: https://www.tapiocaworld.jp/topics_detail.html?info_id=29.

[35] タナックス株式会社, “弊社が運営する「TANAXオンラインショップ」への不正アクセスによる 個人情報漏えいに関するお詫びとお知らせ,” 27 10 2021. [オンライン]. Available: https://www.tanax.co.jp/motorcycle/topics/900.html.

[36] 株式会社ベイシア, “弊社「ベイシアネットショッピング」委託先への不正アクセスによるお客様情報流出に関するお詫びとお知らせ,” 1 11 2021. [オンライン]. Available: https://www.beisia.co.jp/wp-content/uploads/2021/11/c9f3e8b196c27d7f25d6e823c664f247-1.pdf.

[37] 株式会社エンドレス, “弊社が運営する「パーツクラブ オンライン」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 1 11 2021. [オンライン]. Available: https://cdn.shopify.com/s/files/1/0554/1009/8341/files/211101.pdf?v=1637726561.

[38] 株式会社かねたや家具店, “弊社が運営する「オンラインショップ」への不正アクセスによる個人情報漏洩に関するお詫びとお知らせ,” 28 10 2021. [オンライン]. Available: https://www.kanetaya.com/infomation2021.pdf.

[39] 株式会社リンクイット, “弊社が運営する「LINK IT MALL」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 4 11 2021. [オンライン]. Available: https://www.boujeloud.com/c/information/card.

[40] 株式会社杏林堂薬局, “「杏林堂（公式）オンラインショップおよび「店頭予約者情報」への不正アクセスによるお客様情報漏えいに関するお詫びとお知らせ,” 10 11 2021. [オンライン]. Available: https://www.kyorindo.co.jp/news/pdf/kyorindo_online_news.pdf.

[41] グラントマト株式会社, “不正アクセスによる個人情報流出の可能性に関する調査結果のご報告,” 15 11 2021. [オンライン]. Available: https://www.grantomato.jp/topics/topics.php?id=687.

[42] 有限会社トコちゃんドットコム, “弊社が運営する「トコちゃんドットコムＥＣサイト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 15 11 2021. [オンライン]. Available: https://tocochan.com/info/information.pdf.

[43] 株式会社芝寿し, “弊社「芝寿しオンラインショップ」委託先への不正アクセスによる お客様情報流出に関するお詫びとお知らせ,” 30 11 2021. [オンライン]. Available: https://www.online-shibazushi.com/user_data/20211130_oshirase.pdf.

[44] 株式会社グラウンドワークス, “弊社株式会社グラウンドワークスが運営す「EVANGELION STORE(オンライン)」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 30 11 2021. [オンライン]. Available: https://www.evastore.jp/.

[45] 株式会社イーシーキューブ, “EC-CUBE 2系における複数の脆弱性

5] (JVN#75444925),” 11 11 2021. [オンライン]. Available: https://www.ec-cube.net/info/weakness/20211111/.

[4 JVN, “EC-CUBE 2系における複数の脆弱性,” 11 11 2021. [オンライン]. Available:
6] https://jvn.jp/jp/JVN75444925/.

[4 E. V. Kumar, “[Security advisory for CVE-2021-44526 and CVE-2021-44515]
7] Authentication bypass vulnerabilities in ServiceDesk Plus and Desktop Central,” Zoho ManageEngine, 6 12 2021. [オンライン]. Available: https://pitstop.manageengine.com/portal/en/community/topic/security-advisory-for-cve-2021-44526-and-cve-2021-44515-authentication-bypass-vulnerabilities-in-servicedesk-plus-and-desktop-central.

[4 “FBI、Zoho ManageEngine Desktop Centralのゼロデイ脆弱性狙う攻撃を警告,”
8] TECH+, 22 12 2021. [オンライン]. Available: https://news.mynavi.jp/techplus/article/20211222-2234822/.

[4 Robert Falcone, Peter Renals, PaloAlto, “APT攻撃グループ ManageEngine への攻
9] 撃をさらに拡大 ServiceDesk Plus も攻撃の対象に,” 2 12 2021. [オンライン]. Available: https://unit42.paloaltonetworks.jp/tiltedtemple-manageengine-servicedesk-plus/.

[5 “統合エンドポイント管理（UEM）ソフト | Desktop Central (manageengine.jp),”
0] Zoho ManageEngine, [オンライン]. Available: https://www.manageengine.jp/products/Desktop_Central/features.html?utm_source=DC-index-page-cta.

[5 FBI, “APT Actors Exploiting Newly-Identified Zero Day in ManageEngine Desktop
1] Central,” FBI, 17 12 2021. [オンライン]. Available: https://www.ic3.gov/Media/News/2021/211220.pdf.

[5 The Record by Recorded Future, “Emotet botnet returns after law enforcement
2] mass-uninstall operation,” 15 11 2021. [オンライン]. Available: https://therecord.media/emotet-botnet-returns-after-law-enforcement-mass-uninstall-operation/.

[5 独立行政法人情報処理推進機構, “「Emotet（エモテット）」と呼ばれるウイルスへ
3] の感染を狙うメールについて,” 12 9 2021. [オンライン]. Available: https://www.ipa.go.jp/security/announce/20191202.html.

[5 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2020 年度 第
4] 4 四半期,” 18 6 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2020_4q_securityreport.pdf.

[5 一般社団法人JPCERTコーディネーションセンター, “マルウェアEmotetのテイクダ
5] ウンと感染端末に対する通知,” 22 2 2021. [オンライン]. Available: https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.html.

[56] abuse.ch, “URLhaus,” 12 2021. [オンライン]. Available: https://urlhaus.abuse.ch/.

[57] Bleeping Computer LLC, “Emotet botnet comeback orchestrated by Conti ransomware gang,” 19 11 2021. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/emotet-botnet-comeback-orchestrated-by-conti-ransomware-gang/.

[58] BLACKBERRY.COM, “Threat Thursday: Emotet Update,” 6 1 2022. [オンライン]. Available: https://blogs.blackberry.com/en/2022/01/threat-thursday-emotet-update.

[59] 株式会社ラック, “【注意喚起】マルウェアEmotetが10カ月ぶりに活動再開、日本も攻撃対象に,” 19 11 2021. [オンライン]. Available: https://www.lac.co.jp/lacwatch/alert/20211119_002801.html.

[60] デジタルアーツ株式会社, “復活したEmotetの1か月,” 2 2 2022. [オンライン]. Available: https://www.daj.jp/security_reports/220202_1/.

[61] Zscaler, Inc., “Return of Emotet: Malware Analysis,” 13 12 2021. [オンライン]. Available: https://www.zscaler.com/blogs/security-research/return-emotet-malware-analysis.

[62] MISP Project, [オンライン]. Available: https://www.misp-project.org/.

[63] darkfeed.io, “DarkFeed DeepWeb Intelligence Feed,” [オンライン]. Available: https://darkfeed.io/.

[64] Cybereason Inc., “サイバーリーズン vs. Contiランサムウェア,” 16 02 2021. [オンライン]. Available: https://www.cybereason.co.jp/blog/ransomware/5760/.

[65] “BleepingComputer,” 10 12 2021. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/volvo-cars-discloses-security-breach-leading-to-randd-data-theft/.

[66] 米国財務省外国資産管理局(OFAC), “Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” 1 10 2020. [オンライン]. Available: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[67] 時事通信社, “サイバー攻撃で診療停止　電子カルテ、２カ月使えず―病院に「身代金ウイルス」・徳島,” 24 1 2022. [オンライン]. Available: https://www.jiji.com/jc/article?k=2022012400094.

[68] “サイバー攻撃、半数が要求応じる,” 共同通信社, 18 6 2021. [オンライン]. Available: https://nordot.app/778459067998420992.

[69] “7 Major Cyber Insurers Form Company to Coordinate Cyber Analysis, Risk Mitigation,” INSURANCE JOURNAL, 21 6 2021. [オンライン]. Available:

https://www.insurancejournal.com/news/national/2021/06/21/619446.htm.

[70] "'I scrounged through the trash heaps… now I'm a millionaire:' An interview with REvil's Unknown," The Record, [オンライン]. Available: https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/.

[71] C. Tills, "CVE-2021-44515: ZoHo Patches ManageEngine Zero-Day Exploited in the Wild," tenable, 6 12 2021. [オンライン]. Available: https://www.tenable.com/blog/cve-2021-44515-zoho-patches-manageengine-zero-day-exploited-in-the-wild.

[72] "APT Expands Attack on ManageEngine With Active Campaign Against ServiceDesk Plus," palo alto networks, 2 12 2021. [オンライン]. Available: https://unit42.paloaltonetworks.jp/tiltedtemple-manageengine-servicedesk-plus/.

[73] Robert Falcone, Peter Renals(paloaltonetworks), "APT攻撃グループ ManageEngine への攻撃をさらに拡大 ServiceDesk Plus も攻撃の対象に (paloaltonetworks.jp)," 2 12 2021. [オンライン]. Available: https://unit42.paloaltonetworks.jp/tiltedtemple-manageengine-servicedesk-plus/.

NTT DATA
Trusted Global Innovator

Published on March 15, 2022

NTT Data Corporation
Security Engineering Department
Hisamichi Ohtani / Yoshinori Kobayashi / Masao Oishi / Daisuke Yamashita
Chihiro Oyama / Tomohiro Ito / Kanako Sato / Daiki Nishizuka / Kazuki Shimizu / Daisuke Miyazaki
nttdata-cert@kits.nttdata.co.jp