LAC
ともに、イキル

JAPAN SECURITY OPERATION CENTER

INSIGHT

vol.17

December 22, 2017

JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER

JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol.17

1 Preface

The Japan Security Operation Center (JSOC) is a security monitoring center operated by LAC Co., Ltd. that provides security monitoring services, such as "JSOC Managed Security Services (MSS)" and the "24+ Series." The JSOC MSS maximizes the performance of security devices through unique signatures and tuning, and our security analysts, with their expert knowledge, analyze logs from security devices in real time, 24 hours a day, 365 days a year. In this real-time analysis, the security analysts study communication packets in detail, down to their content level, as well as diagnose whether monitored objects are affected and whether there are any vulnerabilities and other potential risks, for every occasion, all in order to minimize misreporting from security devices. We help our customers to improve their security level by reporting only critical incidents needing an emergency response in real time and by taking action against attacks in the shortest time possible.

This is an analysis report on the trend of security incidents, such as unauthorized access and malware infection, in Japan, based on the daily analysis results of our JSOC security analysts. As this report analyzes the trend of attacks, based on the data of incidents that JSOC customers have actually encountered, the report will aid the understanding of world trends, as well as the actual threats that Japanese users are currently facing.

We really hope that this report will provide our customers with useful information that can be made full use of when implementing countermeasures to improve security.

Japan Security Operation Center

Analysis Team

Data collection period

April 1, 2017 to June 30, 2017

Devices used

This report is based on data from security devices supported by the LAC-supplied JSOC Managed Security Services.

* This document is for information purposes only. LAC Co., Ltd. takes no responsibility for any loss resulting from using this document.
* When using data from this report, be sure to cite the source.
(For example, Source: "JSOC INSIGHT, vol. 17, from LAC Co., Ltd.")
* The information contained in this document is as of the initial publication of this document and may be changed by the time it is viewed or provided.

2 Executive Summary

This report illustrates an analysis of the trends in the incidents that occurred during the collection period and introduces some especially notable threats.

■ WannaCry infection incidents

WannaCry is a type of ransomware that encrypts document, image, video, or other types of files on a system, and that demands money in order to decrypt the encrypted files. We have found a severe incident likely to have occurred due to WannaCry infection. WannaCry is capable of attempting to spread the infection, and an infected terminal will attempt to expand the infection to a network internal or external to the organization. If a system on an internal network is infected, many files will be encrypted, and the infection will be spread to other systems, significantly affecting business activities.

WannaCry is known to target a vulnerability for which a security patch is released and to attempt to conduct infecting activities via "SMBv1," a feature of Windows, which was recommended to be disabled. The incident found this time gives us a renewed recognition of the importance of regular software updates and the review of various settings as being key to preventing such an incident.

■ Increasing traffic related to DDoS attacks

We regularly detect traffic that probes for services available as a stepping stone for DDoS attacks, such as SNMP, DNS, or NTP. If a service is found via the probe traffic to be available as a stepping stone for DDoS attack from an external network, the targeted server may be used for DDoS attack. The SOC saw a temporary surge in the number of incidents of NTP probe traffic and guessed that DDoS attacks were being prepared.

This type of probe traffic will continue also for other types of services. If a server under the control of an organization is exploited for DDoS attack, the organization might be held accountable in light of social responsibility. Thus, regular server security diagnoses and configuration reviews for servers are recommended.

3 Trends in Severe Incidents at the JSOC

3.1 Trends in severe incidents

Our security analysts at the JSOC analyze the logs detected by firewalls, IDS/IPS, and sandboxes, and assign one of four incident severity levels according to the nature of incident and the degree of impact that the incident has on monitored targets. Of these severity levels, "Emergency" and "Critical" indicate severe incidents for which a successful attack was confirmed or that the likelihood of damage was assessed to be high.

Table 1 Incident severity levels

Type	Severity	Description
Severe incident	Emergency	Incidents classified as an emergency: - When a customer system experiences an information leak or a Web alteration; or - When malware-infected traffic is confirmed and when the infection has been expanding.
	Critical	Incidents classified as where the likelihood of attack success is high: - When a successful attack against a vulnerability or malware infection is confirmed; or - When it is unknown whether the attack succeeded or not, but when it will cause serious impact at a high probability if successful.
Reference incident	Warning	Incidents classified as needing follow-up: - When the investigation of whether the attack succeeded or not showed no possibility of impact; or - When the possibility of an impact was low at the time of detection, but when follow-up is necessary.
	Informational	Incidents classified as a non-attack: - When audit traffic such as port scan traffic, or other traffic that does not cause any real damage, occurs; or - When security diagnosis or test traffic occurs.

Figure 1 shows the changes in the number of severe incidents during the collection period (from April to June 2017).

The number of severe intra-network incidents in total increased to 353 from the 332 of the previous collection period.

As a trend of severe incidents related to attacks from the Internet, attacks that exploited an OpenSSL vulnerability (Heartbleed)[1] occurred between late April and early May (① in Figure 1). The main reason why a large number of this type of severe incident occurred is because of continued attacks on our newly contracted customers due to the vulnerability. Three years have passed since information about the vulnerability was made available, but attacks related to the vulnerability have still occurred. There are likely to be still many OpenSSL users that are not aware of the existence of the vulnerability, as it is difficult to

[1] "4.1 Attacks that exploit encryption library (OpenSSL) vulnerabilities" in *JSOC INSIGHT* vol. 5
https://www.lac.co.jp/english/report/pdf/JSOC_INSIGHT_vol5_en.pdf

verify the existence of attacks via server logs, etc., and because the attacks do not directly affect servicing.

The middle of May saw many severe incidents that occurred in intra-networks (② in Figure 1). There were still many severe incidents likely to be due to Ursnif infection. Many emails with suspicious file attachments were found during the period, and users were likely to open such suspicious attached files and be infected. This is attributed to the increase in such severe incidents. A severe incident likely to be due to WannaCry infection was also found during this collection period.

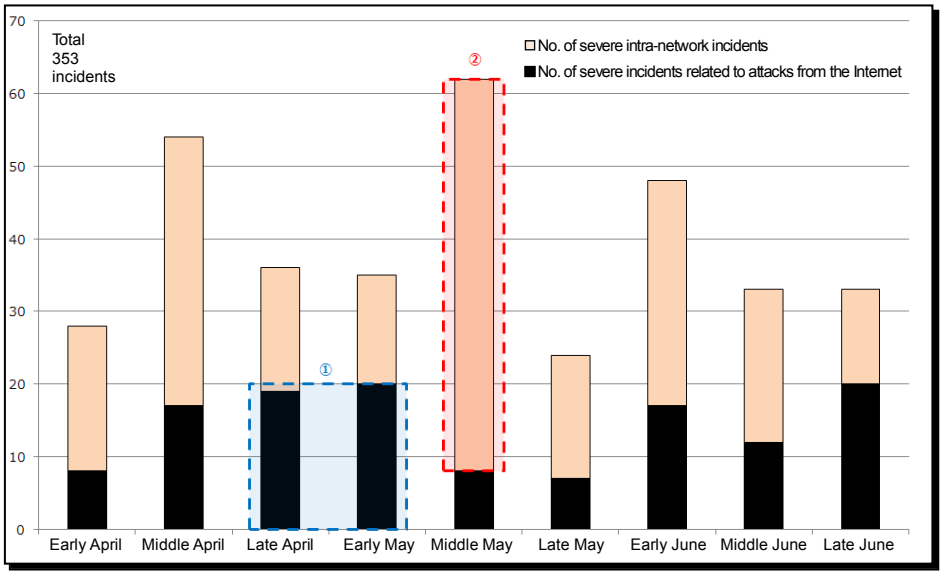
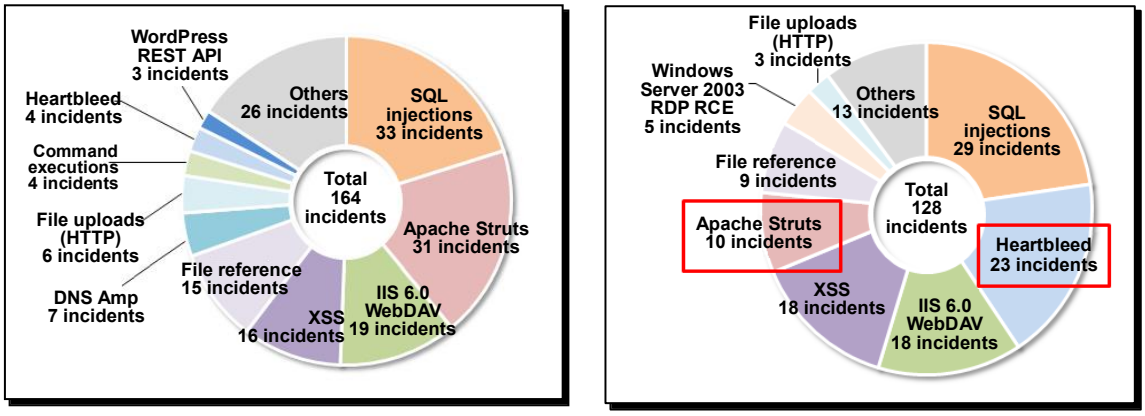


Figure 1 Changes in the number of severe incidents (April to June 2017)

Figure 2 shows a breakdown of the severe incidents related to attacks from the Internet.

The number of severe incidents related to attacks from the Internet decreased to 128 from the 164 of the previous collection period. While severe incidents due to attacks that exploited Apache Struts vulnerabilities decreased, those due to attacks that exploited Heartbleed increased. There was no notable increase or decrease observed for the other types of attacks, but the number of attacks in general was decreasing, which is attributed to the decreased severe incidents as compared to the previous collection period.

The cause of the decreased severe incidents related to Apache Struts is because of the lack of the occurrence of severe incidents of attacks that exploit the S2-045 vulnerability. While the previous collection had many such severe incidents, this collection period had none. The type of attacks that exploited the vulnerabilities themselves continued and was detected frequently, thus it may imply a complete countermeasure against the vulnerability in environments with Apache Struts.



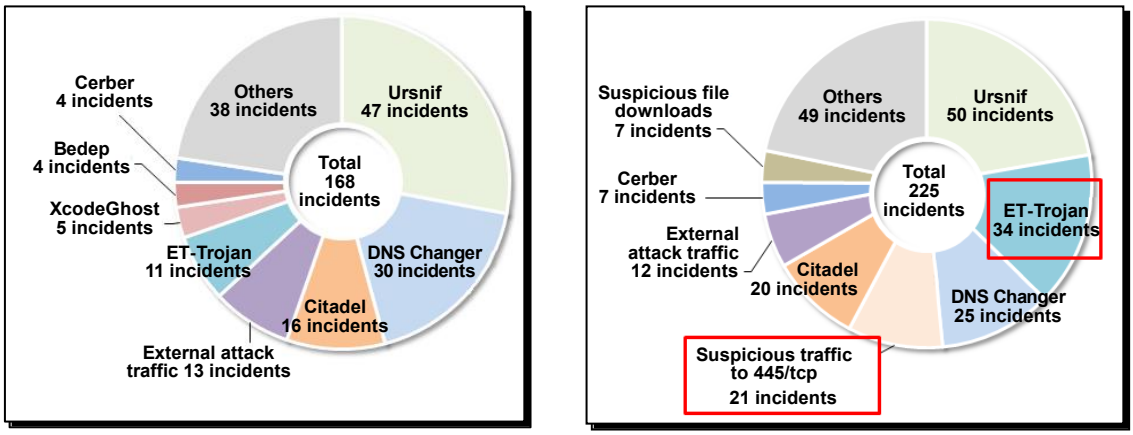
(a) January to March 2017 **(b) April to June 2017**

Figure 2 Breakdown of severe incidents related to attacks from the Internet

Figure 3 shows a breakdown of the severe incidents that occurred in intra-networks.

The number of severe intra-network incidents increased to 225 from the 168 of the previous collection period. Severe incidents due to ET-Trojan infection significantly increased, and they hold a large proportion in the breakdown. Severe incidents due to Ursnif or DNS Changer infections also still frequently occurred.

There was some suspicious traffic to 445/tcp that caused a severe incident likely to be due to infection with WannaCry, which is a type of ransomware. When the severe incident occurred, no signature designed to detect traffic that would occur due to infection with WannaCry had yet been released. However, a signature designed to detect a type of traffic that probes for hosts running a particular service was released and has detected many incidents of such a type of traffic, for a short period, between internal networks, or from an internal to an external network. We thus considered that a severe incident highly likely occurred due to WannaCry infection, taking into consideration the conditions of detection. WannaCry is detailed in Section 4.1.



(a) January to March 2017 **(b) April to June 2017**

Figure 3 Breakdown of severe incidents that occurred in intra-networks

3.2 Types of traffic to pay attention to

This section introduces the types of suspicious traffic found during this collection period that require attention, along with the types of attacks from the Internet that were detected frequently, although such did not cause serious damage.

Table 2 shows the types of traffic frequently detected during the collection period.

Table 2 Types of traffic frequently detected

Classification	JSOC observation	Observation period
Attacks from 110.85.4.102	These attacks continued from the previous collection period, and a vulnerability scan from 110.85.4.102 (China) was detected. Such a vulnerability scan stopped in the middle of April, but an attack attempt to upload a suspicious file from the same source was detected in early May.	Late January to middle April, early May
Attacks that exploited a buffer overflow vulnerability in Disk Sorter	An attack that exploited a buffer overflow vulnerability (CVE-2017-7230) in Disk Sorter Enterprise was detected in the middle of April. For the overflow vulnerability in the software, multiple PoC codes have already been released, and the same code as that in a PoC using the GET method[2] was detected. Many of the detected attacks originated from 79.135.55.204 (Italy), and they seemed to attack any IPv4 address available on the Internet.	Middle of April
SSH-related file access	In early May, suspicious file access was detected that targeted an SSH misconfiguration. Especially frequently accessed were paths like .ssh/id_rsa and .ssh/id_dsa that were generally known as locations of SSH private key storage.	Early May

[2] Disk Sorter Enterprise 9.5.12 – 'GET' Buffer Overflow (SEH)
https://www.exploit-db.com/exploits/41666/

Classification	JSOC observation	Observation period
Attacks from 183.129.160.229	In early May, attacks from 183.129.160.229 (China) were detected that exploited the S2-045 or Heartbleed vulnerability. Also, attacks that exploited the SQL injection vulnerability (CVE-2017-8917)[3] in Joomla! were detected immediately after information about the vulnerability was available in the middle of May. As with the above vulnerability, it should be noted that, if vulnerability information is available, offensive traffic that targets the vulnerability is detected immediately and frequently.	Early to the middle of May
Attacks from 185.22.187.227	In the middle of May, attacks from 185.22.187.227 (Turkey) were detected that exploited a WordPress REST API vulnerability.[4]	Middle of May
Attacks from 36.62.162.205	In late May, vulnerability scan attacks from 36.62.162.205 (China) were detected. The details of detection imply that a Web application vulnerability scanner, NetSparker, was used in these attacks.	Late May

[3] Joomla! Developer Network Security Announcements [20170501] – Core – SQL Injection
https://developer.joomla.org/security-centre/692-20170501-core-sql-injection.html

[4] "4.1 WordPress REST API Vulnerability" in *JSOC INSIGHT* vol. 16
https://www.lac.co.jp/english/report/pdf/JSOC_INSIGHT_vol16_en.pdf

4 Topics of This Volume

4.1 WannaCry infection incidents

Starting from May 12, 2017, we have been seeing infection with a malware type known as WannaCry[5] around the world.[6] WannaCry is a type of ransomware that has a worm-like characteristic of being able to expand the infection. The ransomware found so far was commonly infected via an email file attachment or invalid Web access (using an exploit kit, for example).[7] On the other hand, WannaCry exploits a vulnerability (CVE-2017-0144) in the Windows SMB service, and behaves like a worm to expand the infection over the network. This large-scale, worldwide infection is likely to have been caused by a terminal to which a patch against the MS17-010 vulnerabilities including this one was not applied, and was kept running and accessible from the Internet. The SOC also detected traffic that seemed to involve WannaCry infection activities and notified our customers of such as a severe incident.

4.1.1 Known WannaCry behavior

Various vendors have reported what WannaCry does and how it behaves, as described below.[8, 9]

- Circumvented dynamic analysis (such as a "sandbox")

To determine whether it is being executed in an analysis environment, WannaCry attempts to access a non-existing domain. This is because, in an analysis environment such as a "sandbox," a network may be configured to return a response if an attempt to access a non-existing domain occurs.

This behavior can be used to stop WannaCry, and it is possible if the domain can be accessed. Therefore, researchers attempted to obtain an unregistered domain that WannaCry communicated with and to "sinkhole" it. The domain "sinkholed" this time is also known as a kill switch domain of WannaCry.[10]

---

[5] Also known as Wana Decrypt0r, WannaCryptor, or WCRY, etc.

[6] Indicators Associated With WannaCry Ransomware
https://www.us-cert.gov/ncas/alerts/TA17-132A

[7] "4.2 Ransomware-infected traffic" in *JSOC INSIGHT* vol. 11
https://www.lac.co.jp/english/report/pdf/JSOC_INSIGHT_vol11_en.pdf

[8] Our Struggle with Malware Analysis - WannaCry Analysis (Japanese)
http://blog.macnica.net/blog/2017/05/wanacry-8ff1.html

[9] Guide to Protect Against the WannaCry Ransomware - Rev. 1 (Japanese)
https://www.lac.co.jp/lacwatch/report/20170519_001289.html

[10] Player 3 Has Entered the Game: Say Hello to 'WannaCry'
http://blog.talosintelligence.com/2017/05/wannacry.html

■ File encryption and ransom demand

WannaCry encrypts a document, image, video, database, or other type of file with any of over 170 different file extensions, and appends a character string of ".WNCRY" to the end of its filename.[11] Further, it displays a ransom demand screen (Figure 4).

Figure 4 Ransom demand screen displayed after WannaCry infection

■ Traffic hidden with Tor

WannaCry sends a file encryption key to a C2 server. As the WannaCry's C2 server is set up in a ".onion" domain, WannaCry makes access via Tor by downloading the Tor browser.

■ Infection expanded over the network

WannaCry uses the tool "ETERNALBLUE," released by The Shadow Brokers (TSB) on April 2017, and the backdoor "DoublePulsar," to expand the infection. ETERNALBLUE exploits the arbitrary code execution vulnerability CVE-2017-0144 in the Server Message Block (SMB) service implemented in Microsoft Windows. For more information about the tools and confidential information released by the TSB, see Appendix 1.

[11] WCry/WannaCry Ransomware Technical Analysis
https://www.endgame.com/blog/technical-blog/wcrywanacry-ransomware-technical-analysis

Figure 5[12] roughly shows how WannaCry infection is expanded.

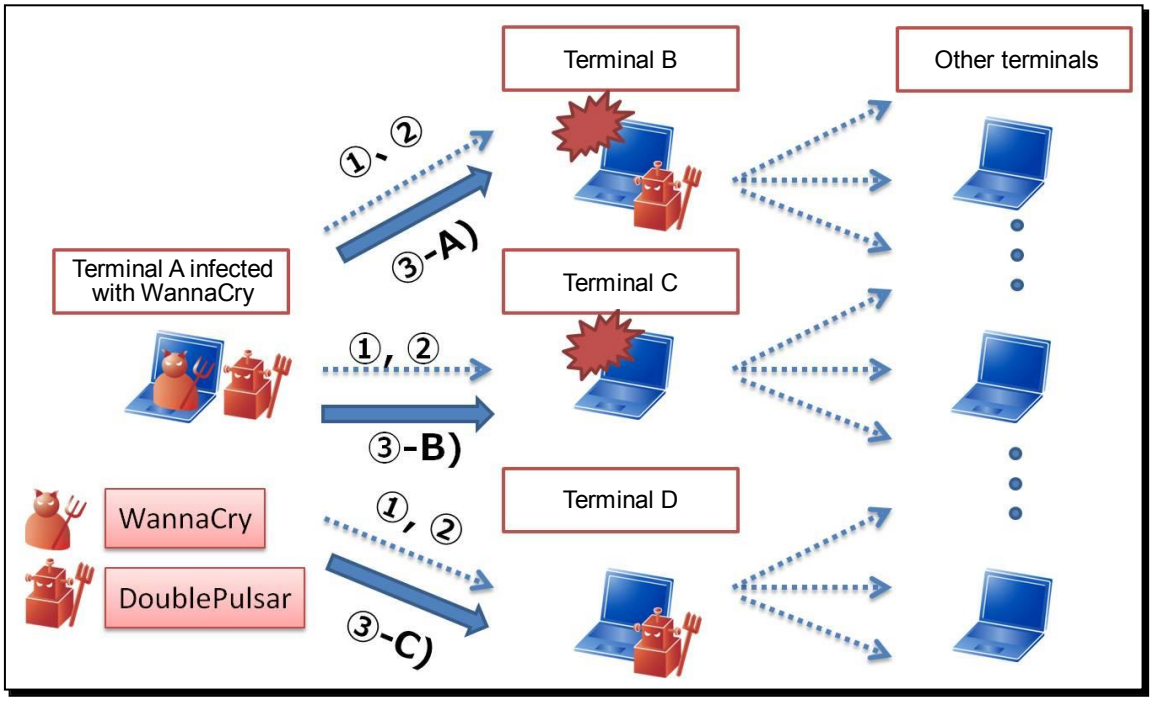


Figure 5 How WannaCry infection is expanded

① WannaCry checks whether it can connect to 445/tcp.

② If step ① can be carried out, WannaCry further checks the following:

- Whether the SMB service has the vulnerability (CVE-2017-0144); and
- Whether DoublePulsar exists.

③ WannaCry then performs the following according to the check results of step ②.

A) If the vulnerability exists and DoublePulsar is installed:
Creates and executes itself via DoublePulsar.

B) If the vulnerability exists and DoublePulsar is not installed:
Exploits the vulnerability to install DoublePulsar, and creates and executes itself.

C) If the vulnerability is already fixed and DoublePulsar is installed:
Creates and executes itself via DoublePulsar.
If the vulnerability is already fixed and DoublePulsar is not installed:
Does not infect the terminal and proceeds to another terminal to perform the checks (① and ②).

[12] Details about the Worm-Like Activities of WannaCry 2.0 (and its variants) and Remaining DoublePulsar (Japanese)
http://www.mbsd.jp/blog/20170629.html

A terminal infected with WannaCry uses ETERNALBLUE to expand the infection to other terminals over the network. The rapidly expanded infection is attributed to such a type of infection that occurs not only in the network of the organization but also over the external network.

4.1.2 WannaCry-infected traffic detected

Figure 6 shows changes in the number of 445/tcp port scans detected between April 1 and June 30. The port scans detected surged in number immediately after WannaCry information was reported on May 12. This is due to a WannaCry infection being expanded at a specific customer's site. Even after the customer completed protective measures, more port scans still occurred as compared to May 12 or earlier, which is attributed to WannaCry's variants or the attackers' increased investigative activities.

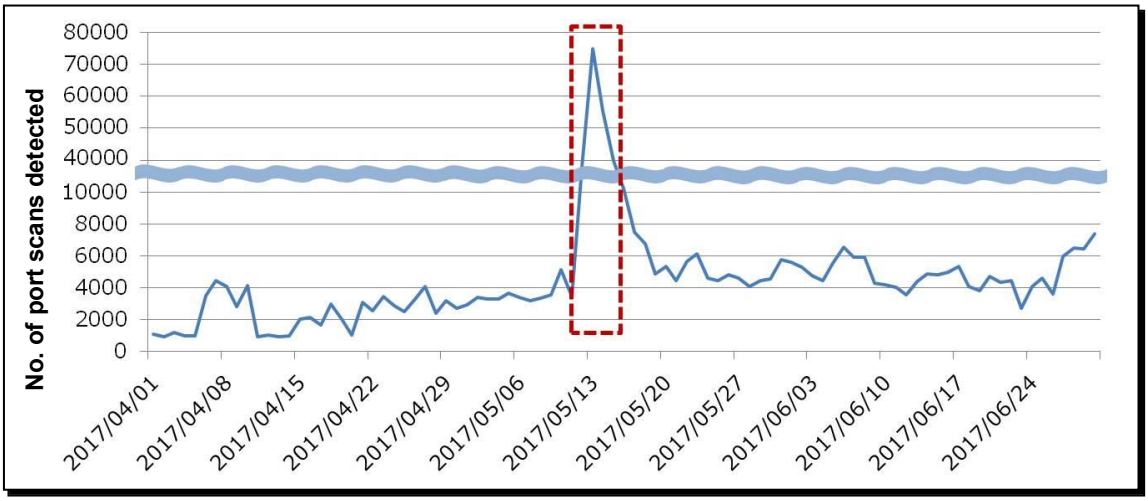
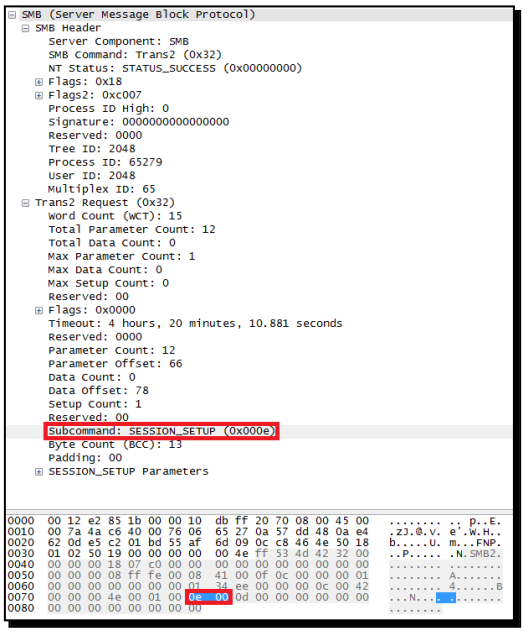
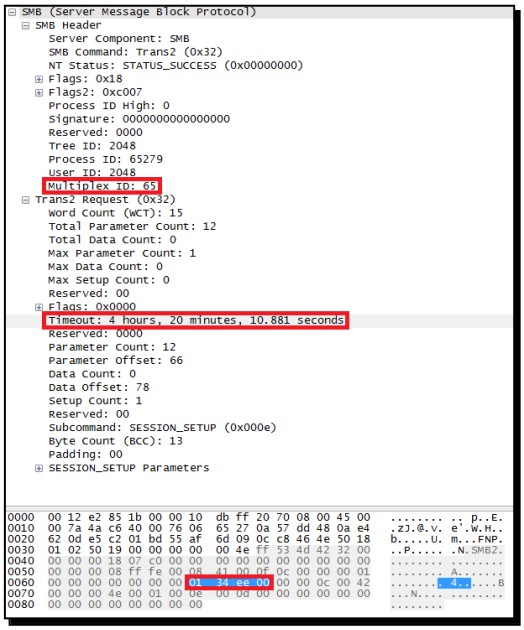


Figure 6 Changes in the number of 445/tcp port scans detected

In the customer's environment, suspicious traffic to 445/tcp for communication between internal networks, or from an internal network to an external network, was detected frequently for a short period. This type of suspicious traffic implied that malware infection was likely, thus we classified such traffic as a severe incident. After that, a signature was added that was designed to detect traffic when a WannaCry infection occurs or when ETERNALBLUE is executed. After the signature addition, suspicious traffic to 445/tcp as shown in Figure 7 was detected in the customer's environment.

Figure 7 shows part of traffic identified as ① in Figure 5, and the purpose of the traffic is to check whether DoublePulsar is installed. The traffic uses a command (TRANS2_SESSION_SETUP) that is not usually used in SMB communication[13] ((a) in Figure 7), and it uses the values of the Timeout and Multiplex ID fields ((b) in Figure 7) to send an instruction to a backdoor.





(a) SESSION_SETUP subcommand **(b) Multiplex ID and Timeout values**

Figure 7 TRANS2_SESSION_SETUP subcommand, used to check for a backdoor

The value written into the Timeout field is decoded to three different instructions with the following expression[14]:

$$\text{0xff \&}\ \big((x) + (x\text{>>}8) + (x\text{>>}16) + (x\text{>>}24)\big) = \begin{cases} \text{0x23} & \text{(to check for a backdoor)} \\ \text{0xc8} & \text{(to execute a code)} \\ \text{0x77} & \text{(to delete the backdoor)} \end{cases}$$

[13] 2.2.6.15 TRANS2_SESSION_SETUP (0x000E)
https://msdn.microsoft.com/en-us/library/ee441654.aspx

[14] BROKERS IN THE SHADOWS: Analyzing vulnerabilities and attacks spawned by the leaked NSA hacking tools
https://blog.checkpoint.com/2017/05/25/brokers-shadows-analyzing-vulnerabilities-attacks-spawned-leaked-nsa-hacking-tools/

When the value "01 34 ee 00" of the Timeout field shown in Figure 7 is applied to the above expression, it is evaluated to "0x23", which indicates that the purpose of the traffic is to check for the existence of a backdoor. If such traffic as shown in Figure 7 is originated from internal terminals in high volume, it is likely that a WannaCry infection is being expanded. In addition to such traffic between internal networks, the SOC also detected suspicious traffic to 445/tcp between internal networks, or from an internal to an external network frequently for a short period, thus we classified such a type of traffic as a severe incident.

The Multiplex ID field is used to obtain a response to an executed instruction code. If an instruction code having 0x41 as the value of the Multiplex ID field is sent, 0x51 will be returned if a backdoor exists. Otherwise, 0x41 will be returned.

4.1.3 Countermeasures against WannaCry

Table 3 shows what types of Windows systems are covered by MS17-010 that may be exploited when WannaCry infection is being expanded. Considering the large scale of possible impact by WannaCry, Microsoft has exceptionally released security updates for Windows XP and Windows Server 2003 for which support was already discontinued.[15] If any of these security updates are not applied, the system may be infected with WannaCry or its variants.

Table 3 Windows covered by MS17-010

Windows XP	Windows RT 8.1	Windows Server 2008 R2
Windows Vista	Windows 10	Windows Server 2012
Windows 7	Windows Server 2003	Windows Server 2012 R2
Windows 8	Windows Server 2008	Windows Server 2016

Countermeasures against WannaCry are described below. If you are using one of the Windows system types covered by MS17-010, you should take the following measures as early as possible.

[15] Customer Guidance for WannaCrypt attacks (Japanese)
https://blogs.technet.microsoft.com/jpsecurity/2017/05/14/ransomware-wannacrypt-customer-guidance/

To protect against WannaCry:

- Apply the MS17-010 security update[16] and restart the system.
- Keep the definition file for your anti-virus product up-to-date.
- Disable SMBv1.

WannaCry is a type of ransomware that attempts to expand the infection via DoublePulsar. If a system on an internal network is infected in an organization, the infection will be expanded internally and files on many systems will be encrypted, significantly affecting business activities. In addition, WannaCry's variants and a self-infecting type of ransomware have been identified,[17] and a new version of DoublePulsar was reported to have been used as a backdoor for malware infection.[18] Further, a type of backdoor that is different than the DoublePulsar might be installed. Therefore, the following fundamental measures against malware, including WannaCry, should be taken.

Fundamental measures against malware, including WannaCry

- Do not use any OS for which support is already discontinued.
- Use the latest version of all software.
- Monitor your network to check that no abnormal traffic occurs from an internal terminal.
- Perform regular checks via anti-virus software.
- Do not open an unnecessary service port.

Recommended countermeasures against WannaCry and fundamental countermeasures against malware in general are published as a guide.[19] Please refer to the guide along with this report.

---

[16] Microsoft Security Bulletin MS17-010 - Critical
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

[17] WannaCry Risk Again! A New Expansive Type of Ransomware, GoldenEye/Petya, is Expanding Over the World! (Japanese)
https://www.lac.co.jp/lacwatch/people/20170628_001319.html

[18] Analyzing Petya Version of DoublePulsar V2.0, Advanced Version of the Leaked NSA Backdoor (Japanese)
http://www.checkpoint.co.jp/threat-cloud/2017/07/brokers-shadows-part-2-analyzing-petyas-doublepulsarv2-0-backdoor.html

[19] Guide to Protect Against the WannaCry Ransomware - Rev. 1 (Japanese)
https://www.lac.co.jp/lacwatch/report/20170519_001289.html

4.2 Trend of traffic detected as related to DDoS attacks

The trend of traffic detected as related to DDoS attacks implies that, as preparation for using a UDP-based service as a stepping stone for DDoS attack, attackers were constantly probing for a host running a service, such as DNS, NTP, or SNMP, that is available for the purpose. Of the probe-type traffic, the collection period saw a sharp increase in the number of incidents of traffic for probing for a server where the monlist function of NTP was enabled. The collection period also saw an increase in attacks attempting to infect IoT devices with the Mirai malware that was capable of attacking DDoS and building a botnet through the infected devices.[20]

4.2.1 Overview of DDoS attacks that used a UDP-based service as a stepping stone

Figure 8 roughly shows an amp attack (or reflector attack), which is a type of DDoS attack using a UDP-based service as a stepping stone for it.[21]

As UDP communication does not establish a session, the source of the communication can be faked easily. That is, by using a fake source IP address as that targeted for DDoS attack in a request and by sending the request to a stepping-stone host, the attacker can make a reflector attack that attempts to have the stepping-stone host send a response to the targeted host.

Services typically used as a stepping stone for reflector attack include DNS, NTP, and SNMP. These services are often probed, as they mainly use UDP and are easily available as a stepping stone for reflector attack, and because they return a large amount of traffic in response to a request (high amplification rate). This type of DDoS attack where its efficiency is improved by using a service with a high amplification rate is also known as an "amp attack."

[20] "4.1 IoT device hijack attempts detected" in *JSOC INSIGHT* vol. 14
https://www.lac.co.jp/english/report/pdf/JSOC_INSIGHT_vol14_en.pdf

[21] Digging into How DNS Reflector Attacks Work (Japanese)
https://jprs.jp/tech/notice/2013-04-18-reflector-attacks.html

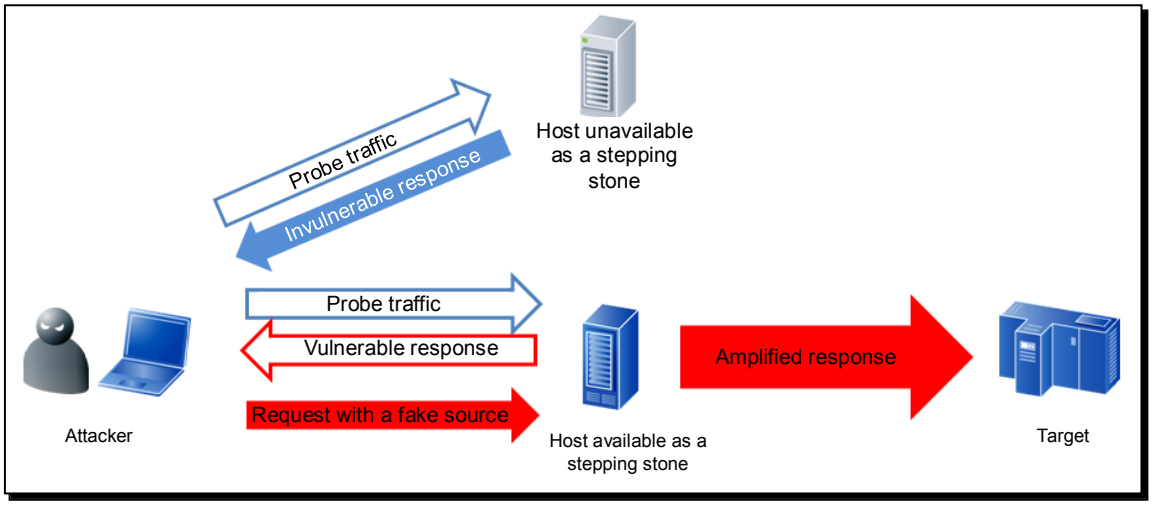


Figure 8 Amp attack using a UDP-based service as a stepping stone (reflector attack)

4.2.2 Incidents detected as being related to amp attacks

Table 4 shows incidents detected as being related to amp attacks.

The collection period saw no significant decrease or increase in the number of incidents of traffic related to amp attacks using a DNS or SNMP service. However, it saw a large increase in the number of incidents of probe traffic against the monlist function of the NTP service.

Table 4 Incidents detected as related to reflector and amp attacks

Service	Probe traffic overview with incidents detected	Amplification rate
DNS	Requests that externally attempt a recursive query; large-sized responses returned externally were detected. If the system is configured to allow external recursive query, a very highly amplified response may occur.	Several 10s to several 100s
NTP	Requests that targeted the monlist function implemented in ntpd were detected. monlist returns a list of past NTP communications. If this function is enabled, a very highly amplified response may occur.	Several 10s to several 100s
SNMP	Large-sized responses returned externally were detected. To use a service as a stepping stone, the service must be externally available, and its community name must be known as an additional condition. Further, they are often used as they are without changing their default settings. If such conditions are met, a very highly amplified response may occur.	Up to several 1,000s

Figure 9 shows the changes in the number of requests targeted for the monlist function of the NTP service.

The number of such requests increased only during the period from June 2 to June 3 (① in Figure 9).

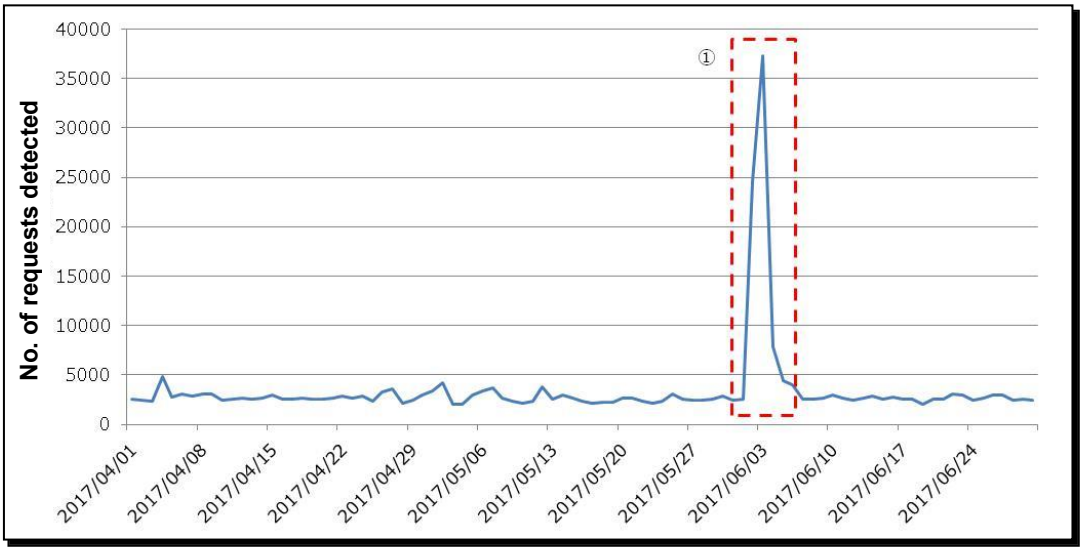


Figure 9 Changes in the number of requests targeted for the monlist function of the NTP service

Figure 10 shows the number of monlist-targeted requests detected during the period that saw the increase in such type of requests (① in Figure 9), for each country that owns the source IP address.

Over 90% of the requests detected during the period with the number increased originated from an IP address allocated to China, and the number of requests from China significantly increased only between June 2 and 3. However, these requests were from different sources and were not detected for an extended time, and no large-sized response was detected. This will imply that the requests attempted to probe for a host available as a stepping stone for DDoS attack, instead of attempting to use the host as a stepping stone for DDoS attack. The result of our investigation of the source IP addresses detected to have been used for the increased probe traffic will indicate that these requests probed for a host available as a stepping stone only during this short period, as no suspicious traffic was found in the past. For the other countries, there was no remarkable change in the number of requests detected between June 1 and 3 before that number increased. Depending on the situation of politics or any other major incident, such DDoS attacks or probe incidents may increase, but there has been no news, statistics, or other public information available as related to this increase incident.

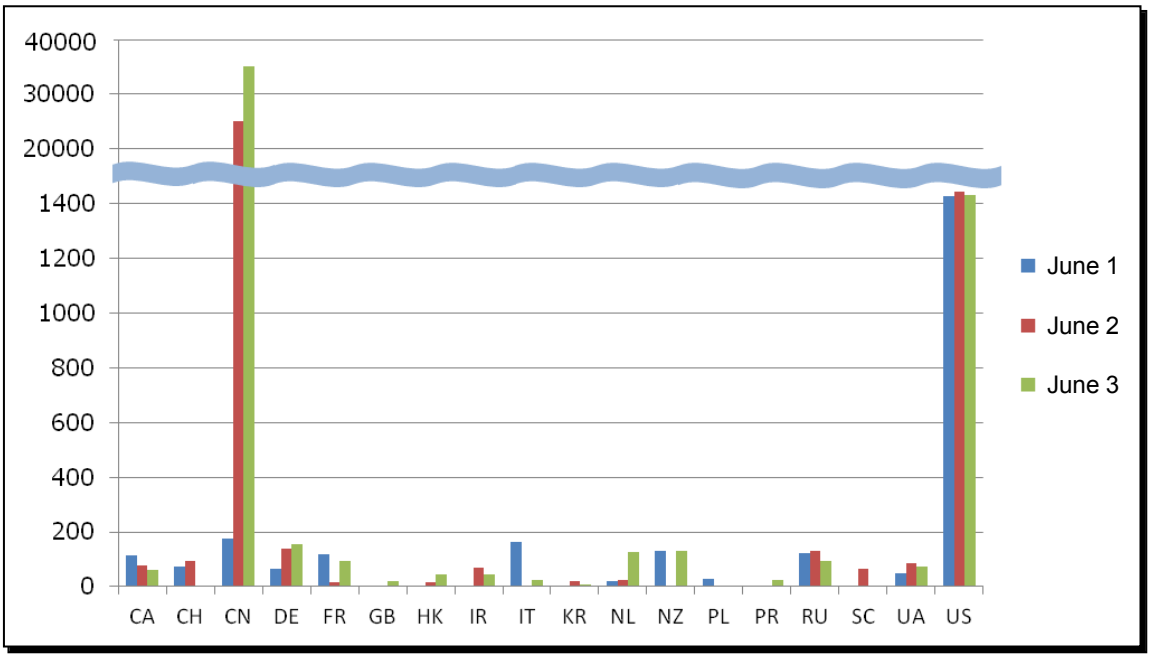


Figure 10 Number of requests detected during the period with an incident increase, by source IP address allocated by country

4.2.3 Trend of attacks detected as related to Mirai infection

The SOC found that the detected number of offensive attacks by the malware "Mirai" that exploits IoT devices increased from June 20. Over 90% of these were from IP addresses allocated to China, and the cause for such would be due to poorly secured Chinese products being widely available in the market in Japan. Figure 11 shows the number of attacks detected as related to Mirai.

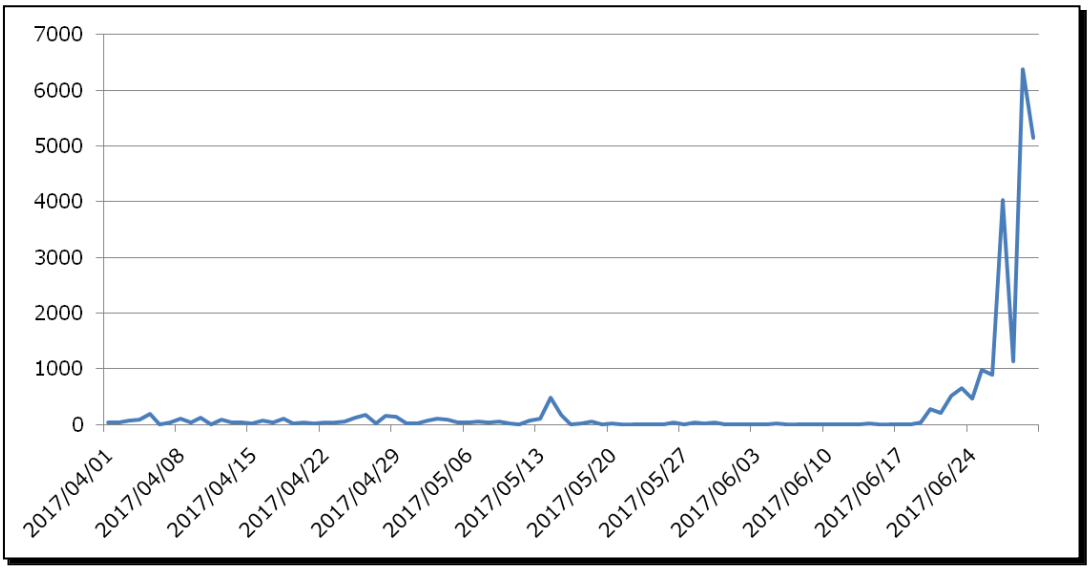


Figure 11 Changes in the number of attacks detected as related to Mirai

Traffic that attempts to expand Mirai infection has the characteristic that its target IP address is randomly selected and that the number of retries is relatively low. As a whole, the SOC concludes that the increased traffic this time consisted of attempts to expand the infection, as none of the sources attacked multiple destinations, and because there was no persistent attack detected that involved multiple attempts.

4.2.4 Countermeasures

A DDoS attack may make you a victim and then make you an attacker. To avoid this, it is necessary to take appropriate measures not to be involved in a DDoS attack. For information about the measures to be taken for using IoT devices, see *JSOC INSIGHT* vol. 14.

Countermeasures against DDoS attacks that use a UDP-based service as a stepping stone

- Check that no service is unintentionally open to the public.
  - Restrict access to any service that needs to be open to the public.
  - Configure authentication information that cannot be easily guessed if the service implements authentication.
- Check for vulnerability information available for a service open to the public.
- Check for increased suspicious traffic from an internal to an external network.

Appendix 1 Various Verification Codes Released by The Shadow Brokers

In August 2016, a hacker group calling itself "The Shadow Brokers" (TSB) disclosed a number of verification codes. The verification codes included a set of tools used by the National Security Agency (NSA) in the U.S., for hacking, and thus attracted attention. The SOC also issued an alert, as there was the concern that a code execution vulnerability (commonly known as EXTRABACON) in Cisco products might be exploited for a zero-day attack. [22, 23]

After disclosing EXTRABACON, the TSB divided and disclosed its obtained information in several batches. Table 5 shows the key information disclosed by the group.

Table 5 Information disclosed by The Shadow Brokers

Date disclosed	Title	Key verification code and disclosed information
8/13/2016	Equation Group Cyber Weapons Auction - Invitation	• EPICBANANA • EXTRABACON
10/31/2016	Message #5 - TrickOrTreat	• List of servers hacked by the NSA • Tools used for the hacking
12/14/2016	Message #6 - BLACK FRIDAY / CYBER MONDAY SALE	• Screenshot of the tools list
4/10/2017	Don't Forget Your Base	• Password available to extract the compressed tools released in August 2016
4/14/2017	Lost in Translation	• ETERNALBLUE • ESTEEMAUDIT • EXPLODINGCAN • DoublePulsar

The fifth disclosed information, titled "Lost in Translation," contains ETERNALBLUE used to expand WannaCry infection as described in 4.1. Table 6 lists the key verification codes made available in Lost in Translation.

[22] Alert: SNMP vulnerability (CVE-2016-6366) in Cisco products (Japanese)
https://www.lac.co.jp/lacwatch/people/20160823_000399.html

[23] "4.2 Regarding code execution vulnerability (CVE-2016-6366) in Cisco products" in *JSOC INSIGHT* vol. 14
https://www.lac.co.jp/english/report/pdf/JSOC_INSIGHT_vol14_en.pdf

Table 6 Key verification codes made available in Lost in Translation

Code name	Vulnerability exploited	Targeted service
ETERNALBLUE	MS17-010	SMB (445/tcp)
ETERNALCHAMPION		
ETERNALROMANCE		
ETERNALSYNERGY		
ESTEEMAUDIT	CVE-2017-9073	RDP (3389/tcp, udp)
EXPLODINGCAN[24]	CVE-2017-7269	WebDAV (80/tcp, 443/tcp)

Of the codes listed in Table 6, the SOC actually detected attacks that targeted the vulnerabilities covered by the three: ETERNALBLUE, ESTEEMAUDIT, and EXPLODINGCAN.

Figure 12 shows a detected example of traffic deemed to have used the ESTEEMAUDIT verification code.

Executing the verification code in an SOC verification environment also shows the same character strings enclosed by the red rectangle in Figure 12, thus we can safely say that the tool disclosed by the TSB was used in the traffic.

It is easily expected that, including WannaCry as described in 4.1 this time, offensive tools and types of malware based on these TSB verification codes and payloads will be rampant also in the future. From June 2017, the TSB started an information release service, named "TheShadowBrokers Monthly Dump Service," available on a monthly fee basis. As some users have subscribed to the service,[25] and as zero-day attacks based on the information available from the service are expected, the TSB will be one of the hacker groups that should be paid attention to, and information about the group should also be collected in the future.

[24] "4.3 Arbitrary code execution vulnerability in IIS 6.0 WebDAV" in *JSOC INSIGHT* vol. 16
https://www.lac.co.jp/english/report/pdf/JSOC_INSIGHT_vol16_en.pdf

[25] The Shadow Brokers are NOT Making America Great again!!!
https://steemit.com/shadowbrokers/@fsyourmoms/theshadowbrokers-are-not-making-america-great-again

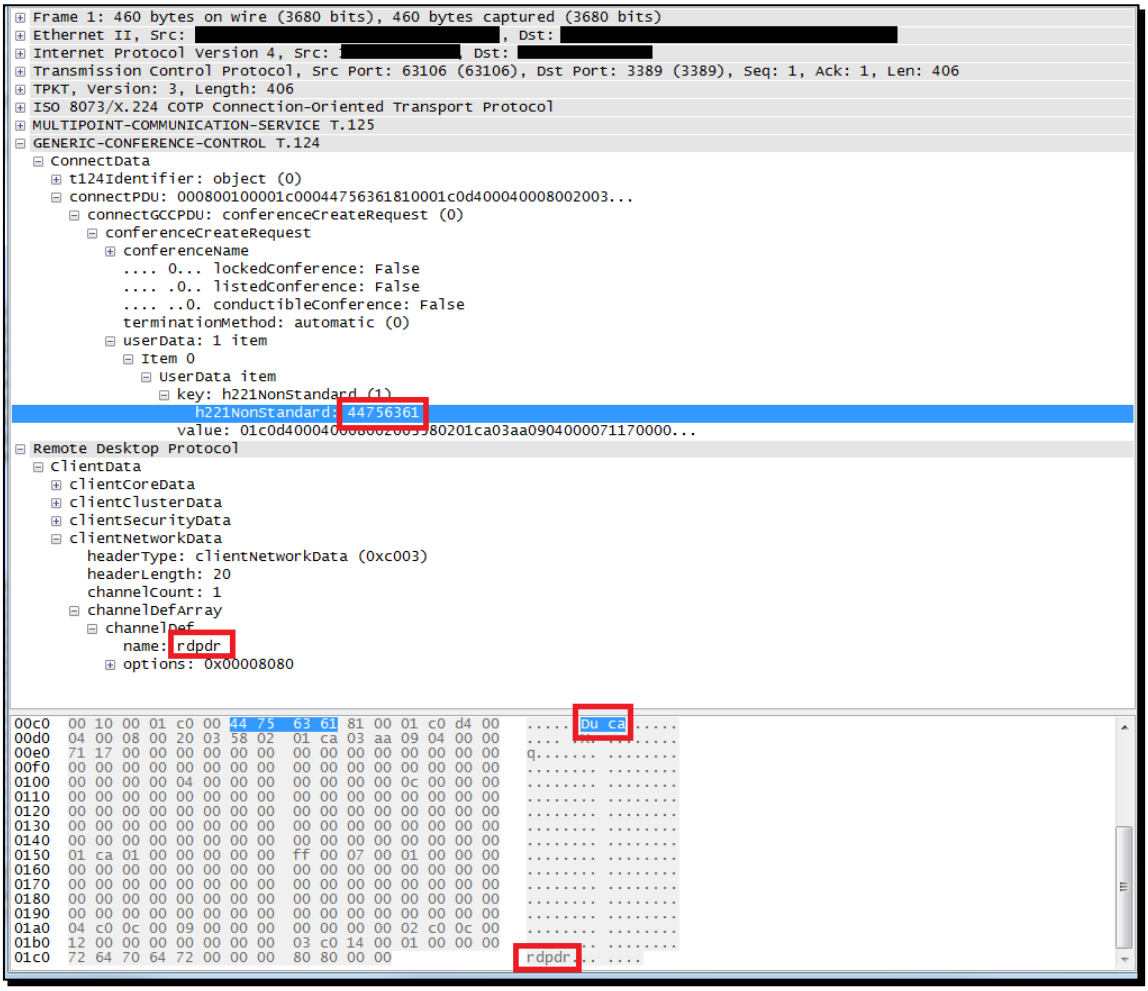


Figure 12　Detected example of traffic deemed to be ESTEEMAUDIT

Conclusion

Much like what the word "INSIGHT" itself implies, JSOC INSIGHT focuses on providing information on threats that our JSOC security analysts come across from time to time and believe to be worth noting.

Our security analysts are hard at work, carefully listening to customers in order to offer the most up-to-date information available. In our effort to provide vital information, the JSOC does not merely focus on the popular incidents that are discovered here and there, but also strives to draw attention to significant threats that can affect our now and tomorrow.

The JSOC's hope is to provide our customers with the safety and security that they need to conduct their business activities.

JSOC INSIGHT vol.17
Authors:
Junichiro Kume, Makoto Sonoda, Shohei Abe, Yusuke Takai
(alphabetical order)

JSOC

JAPAN
SECURITY OPERATION
CENTER

LAC ともに、イキル

LAC Co., Ltd.
Hirakawa-cho Mori Tower, 2-16-1, Hirakawa-cho, Chiyoda, Tokyo 102-0093
+81-3-6757-0113 (Sales)
E-MAIL: sales@lac.co.jp
https://www.lac.co.jp/english/