SOC Report

1.1 Introduction

IIJ maintains the wizSafe security brand 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.

Section 1.2 of this report looks back at major security topics in 2022, and Section 1.3 discusses threats related to the topics covered, with a focus on those observed on our data analytics platform.

1.2 2022 Security Summary

Tables 1 and 2 show the security incidents that the SOC focused on from among those that rose to prominence in 2022.

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

Table 1: Incident Calendar (January–May)

Month	Summary
January	**A software developer announced it had been compromised by ransomware in the early hours of December 31, 2021. It was found not only that files had been encrypted in the attack but also that the attacker had stolen customer transaction and other data, which was published twice on data leak sites.** (Tokyo Computer Service Co., Ltd.) https://www.to-kon.co.jp/ja/topics/topics20220411103030/main/0/teaserItems1/0/linkList/0/link/letter.pdf https://www.to-kon.co.jp/ja/topics/topics20220411103030/main/0/teaserItems1/0/linkList/00/link/letter2.pdf https://www.to-kon.co.jp/ja/topics/topics20220411103030/main/0/teaserItems1/0/linkList/01/link/letter3.pdf https://www.to-kon.co.jp/ja/topics/topics20220411103030/main/0/teaserItems1/0/linkList/02/link/letter4.pdf
January	**A payment service provider announced that it had been subject to unauthorized access between August 2, 2021 and January 25, 2022. The attacks were complex and included unauthorized logins to internal management systems, SQL injection attacks into some applications, and the installation of backdoors, and it was revealed that personal information had been leaked.** (Metaps Payment Inc.) https://www.metaps-payment.com/company/20220125.html https://www.metaps-payment.com/company/20220228.html
February	**The JPCERT Coordination Center (JPCERT/CC) issued an alert on Emotet infections spreading rapidly since February. In March, the number of Emotet-compromised .jp email addresses that could be exploited to send emails surged to over five-fold the 2020 wave peak, and while these observations eased off in mid July, mailouts were again observed from November 2.** (JPCERT/CC) https://www.jpcert.or.jp/english/at/2022/at220006.html
March	**A major automaker announced it had suspended operations at all of its domestic plants (28 lines across 14 plants) on March 1. This was attributed to a system failure at a domestic supplier, which disclosed that this involved file server virus infections.** (Kojima Industries Corporation) https://www.kojima-tns.co.jp/wp-content/uploads/2022/03/20220331_%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E9%9A%9C%E5%AE%B3%E8%AA%BF%E6%9F%BB%E5%A0%B1%E5%91%8A%E6%9B%B8%EF%BC%88%E7%AC%AC1%E5%A0%B1%EF%BC%89.pdf https://www.kojima-tns.co.jp/wp-content/uploads/2022/08/%E3%82%A6%E3%82%A3%E3%83%AB%E3%82%B9%E6%84%9F%E6%9F%93%E8%A2%AB%E5%AE%B3%E3%81%AB%E3%82%88%E3%82%8B%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E5%81%9C%E6%AD%A2%E4%BA%8B%E6%A1%88%E7%99%BA%E7%94%9F%E3%81%AE%E3%81%8A%E7%9F%A5%E3%82%89%E3%81%9B-2.pdf
March	**An auto parts manufacturer announced on March 10 that a third party had illegally accessed the network at one of its overseas group companies.** (Denso Corporation) https://www.denso.com/global/en/news/newsroom/2022/20220314-g01/
March	**VMware announced on March 31 that the Spring Framework had a vulnerability (CVE-2022-22965) that was leaked out ahead of the CVE being published. If exploited, the vulnerability could allow remote arbitrary code execution. In addition to VMware products, this also impacts other products using the Spring Framework. The vulnerability is known as Spring4Shell.** (VMware) https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
April	**VMware announced on April 6 that multiple vulnerabilities were present in some of its products, including VMware Workspace ONE Access and VMware Identity Manager. VMware also confirmed that, of these, a remote code execution vulnerability (CVE-2022-22954) and a local privilege escalation vulnerability (CVE-2022-22960) were being exploited in the wild.** (VMware) https://www.vmware.com/security/advisories/VMSA-2022-0011.html
April	**An industrial parts manufacturer announced on April 8 that a third party had illegally accessed the network at an overseas plant of one of its group companies. It reported that the intruder had likely exploited a VPN device vulnerability.** (Nippo Ltd.) https://www.nip.co.jp/news/.assets/20220408-1.pdf https://www.nip.co.jp/news/.assets/20220422-1.pdf
May	**On May 4, F5 Networks disclosed a vulnerability (CVE-2022-1388) in F5 BIG-IP that may allow iControl REST authentication to be bypassed. By exploiting this vulnerability, an unauthenticated attacker could execute arbitrary system commands, create or delete files, or disable services.** (F5 Networks) https://support.f5.com/csp/article/K23605346
May	**A cloud service provider announced that unauthorized access had been gained to some of the load balancers provided on its services between May 7 and 11.** (Fujitsu Cloud Technologies Limited) https://pfs.nifcloud.com/cs/catalog/cloud_news/catalog_202205161000_1.htm https://pfs.nifcloud.com/cs/catalog/cloud_news/catalog_202205311000_1.htm https://pfs.nifcloud.com/cs/catalog/cloud_news/catalog_202206071000_1.htm https://pfs.nifcloud.com/cs/catalog/cloud_news/catalog_202206291000_1.htm
May	**Microsoft announced on May 30 that a remote code execution vulnerability (CVE-2022-30190) was present in Microsoft Support Diagnostic Tool (MSDT). This zero-day vulnerability is known as Follina.** (Microsoft) https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

Table 2: Incident Calendar (June–December)

Month	Summary
June	**Atlassian announced on June 2 that an unauthenticated remote code execution vulnerability (CVE-2022-26134) was present in its Confluence Server and Confluence Data Center products.** (Atlassian) https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html
June	**A local government announced that a USB flash drive containing personal information had been lost on June 21. The USB flash drive was found on June 24, and an investigative report released on November 28 said there was no evidence any personal information had been leaked.** (City of Amagasaki) https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html
July	**A hotel chain announced on July 27 that 11,961 personal information records had been breached owing to Emotet infecting a computer at one of its outsourcing contractors.** contractors. (APA Group) https://www.apa.co.jp/newsrelease/164149
September	**Access was disabled to 23 websites of four Japanese ministries/agencies (Digital Agency, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology, and Imperial Household Agency) as well as websites of a number of private-sector companies. The attack is believed to have been carried out by the pro-Russia hacking group Killnet, which posted a video to its Telegram channel declaring war against the Japanese government.**
October	**On October 10, Fortinet disclosed a vulnerability (CVE-2022-40684) in the administrative interface of its FortiOS, FortiProxy, and FortiSwitchManager products. By exploiting this vulnerability, an attacker could bypass authentication and perform arbitrary operations on the interface.** (Fortinet) https://www.fortiguard.com/psirt/FG-IR-22-377
October	**It was disclosed on October 19 that over 65,000 company data records had been potentially exposed by the misconfiguration of an object storage service provided by a software developer. After a foreign security firm notified Microsoft of the issue, the misconfiguration was rectified and affected customers were notified.** (Microsoft) https://msrc-blog.microsoft.com/2022/10/19/investigation-regarding-misconfigured-microsoft-storage-location-2/
October	**The National Institute of Information and Communications Technology (NICT) announced that DDoS bot infections targeting DVRs manufactured by Focus H&S were increasing, with 17,489 attacks observed between June 1 and August 31. As the products are also sold in Japan, NICT is calling on users to update the firmware as soon as possible.** (National Institute of Information and Communications Technology) https://blog.nicter.jp/2022/10/analysis-of-ddos-bot-targeting-dvrs/
October	**A medical center disclosed on October 31 that it had received what was apparently a ransomware attack. The attack caused a failure in the center's electronic medical record system, making it impossible to perform regular consultations and also causing the suspension of general outpatient services.** (Osaka General Medical Center) https://www.gh.opho.jp/pdf/obstacle20221031.pdf
November	**A PC peripherals manufacturer disclosed on November 21 that a third party had gained unauthorized access to a website it operates, and that tampering with its payment application had resulted in the personal information of up to 147,545 people and 1,938 credit card records being breached.** (Wacom) https://www.wacom.com/ja-jp/about-wacom/news-and-events/2022/1484
December	**On December 12, Fortinet disclosed a vulnerability (CVE-2022-42475) in FortiOS SSL-VPN that, if exploited, could allow a remote unauthenticated attacker to execute arbitrary code or commands.** (Fortinet) https://www.fortiguard.com/psirt/FG-IR-22-398
December	**On December 14, Citrix disclosed a vulnerability (CVE-2022-27518) in Citrix Gateway and Citrix ADC that, if exploited, could allow an unauthenticated remote attacker to execute arbitrary code.** (Citrix) https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518
December	**A password management software provider disclosed on December 22 that an unauthorized party had gained access to the cloud storage it uses to store production data backups. The attack resulted in customer information and encrypted sensitive information, including information generated when customers use the service, being breached.** (LastPass) https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/

1.3 Security Topics

This section discusses the SOC's observations on the key topics our analysts were focused on from among the 2022 security incidents covered in Section 1.2.

1.3.1 Emotet in 2022

■ Emotet Overview

Emotet activity rose to the fore again in 2022, after a quiet period in 2021 following the high volume of observations back in 2019 and 2020. Emotet was first reported in 2014, and at the time was known as a type of malware called a banking trojan, which steals financial details and the like. Added functionality subsequently saw Emotet transform, and it increasingly began to infect other devices. Starting with its observations in September 2019, in 2019 and 2020 our SOC observed many Emotet-related emails and C&C server communications. With Europol taking down Emotet's attack infrastructure on January 27, 2021[*2], Emotet infections disappeared for a time from January 26, 2021. But on November 14, 2021, Emotet was able to compromise systems via another malware named Trickbot[*3], and Emotet file downloads via email were detected. In 2022, the JPCERT Coordination Center (JPCERT/CC) reported that the Emotet infections were greater in scale than those in 2020, and as illustrated by examples given in the previous section's incident calendar, this rampancy did lead to some damage (Tables 1 and 2).

Emotet has functionality for stealing information and spreading itself, as well as loader and botnet functionality allowing it to download and execute other malware. Once it infiltrates a device, Emotet steals information like email addresses, account information, and email text. It also creates emails using stolen email text and subject lines, to which it attaches a file that downloads Emotet before sending out. It is known that it attaches VBA macro-containing Microsoft Office Word/Excel files and password-protected ZIP files that contain such Word/Excel files in compressed form. The password-protected ZIP files are encrypted, so the contents cannot be examined if they cannot be decrypted by security products such as antivirus or sandbox systems. Files that cannot be inspected can circumvent security products, so there is a good probability of them making it to the end user. A new approach was also observed in April 2022, whereby Emotet attaches a shortcut file (LNK file) or a password-protected ZIP containing a shortcut[*4], so care must be taken with other file formats, not just the conventionally used Word and Excel formats.

And Emotet's loader functionality, mentioned above, means it can also serve as an entry point for other malware. In 2022, Palo Alto Networks confirmed that devices compromised by Emotet also contained malware known as IcedID and Bumblebee[*5]. Cybereason also reported on attacks in which Emotet was used to deploy the Cobalt Strike framework, which is used in penetration testing[*6]. So if Emotet infections are left unaddressed, the damage caused can become even more serious. These attributes make Emotet one of the more infectious and threatening malware programs out there.

[*2] Europol (European Union Agency for Law Enforcement Cooperation), "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).

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

[*4] Information-technology Promotion Agency (IPA), "Emails designed to cause Emotet malware infections" (https://www.ipa.go.jp/security/announce/20191202.html#L20, in Japanese).

[*5] Twitter (@Unit42_Intel) (https://twitter.com/Unit42_Intel/status/1590002190298804225).

[*6] Cybereason, "Threat analysis report: All roads lead to Cobalt Strike—IcedID, Emotet, QBot" (https://www.cybereason.co.jp/blog/malware/7797/).

Emotet Observations

Here, we report on Emotet observations by our SOC.

Figure 1 shows the number of Emotet emails over the course of a year. Date is on the horizontal axis. The detection count is on the vertical axis, normalized so that the total number of detections over the period corresponds to 100%.

Broadly speaking, Emotet was detected during three periods. The first was January 21 – April 5, which saw the highest detection count. Detections increased from February 2 and peaked on March 2. This corresponds to when JPCERT/CC reported a rapid increase in the number of Japanese email addresses possibly compromised and being abused by Emotet to send emails (Tables 1 and 2), and our SOC observed a similar trend.

The second period was April 21 – July 14, with observations increasing from June 4 and peaking on June 14. In addition to macro-bearing Excel files, detections from April 30 showed that Emotet was also attaching shortcuts and ZIP files containing shortcuts.

The third period was November 2–12, which saw the fewest detections. The shortcut files detected in the second period were not detected during this period; only macro-bearing Excel files were detected.

Even during the periods when attack emails were not observed (April and July–November), it was reported that Emotet itself had been changed[*7], so it would seem that activity is ongoing even during times when conspicuous attacks are not being observed.

Next, Figure 2 shows Emotet device infections on each date as a percentage of the year's total. Date is on the horizontal axis. The number of devices infected by Emotet is on the vertical axis, normalized so that the total

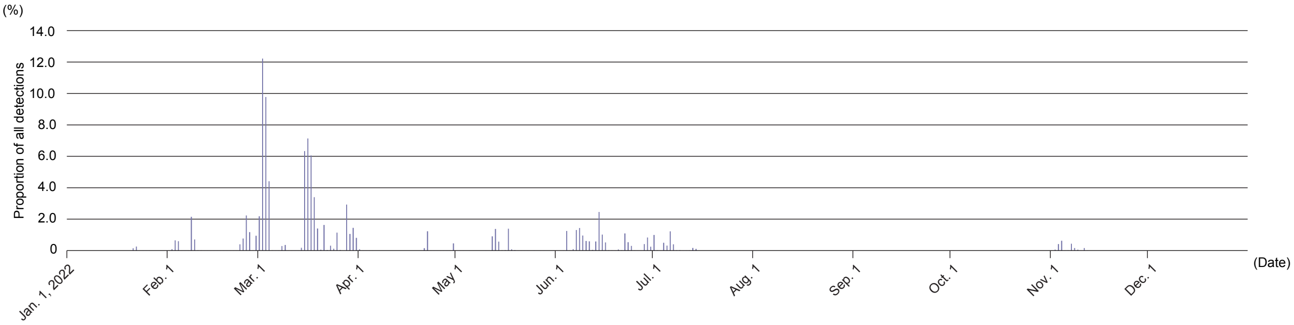


Figure 1: Number of Emails in which Emotet was Detected

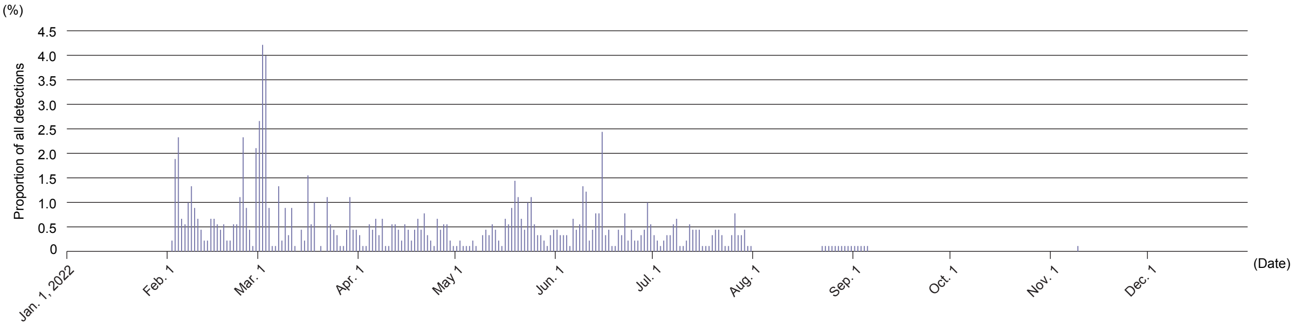


Figure 2: Devices infected by Emotet as Proportion of Annual Total

[*7] Proofpoint, "A Comprehensive Look at Emotet Malware's Fall 2022 Return" (https://www.proofpoint.com/au/blog/threat-insight/comprehensive-look-emotets-fall-2022-return).

corresponds to 100%. Each IP address that engages in communications with a C&C server is counted as one device.

As with the Emotet emails, the observations began on February 2 and peaked on March 2. From April to May, the number of devices infected tended to be lower than in March, but a large number of devices was again observed on June 15.

Periods of high device observations coincide with periods when a high number of emails in which Emotet was detected were received, but there are also periods in which infection traffic continued to appear despite no Emotet emails being received. This is probably because Emotet infections went unnoticed for some time after occurring, which suggests insufficient early detection measures. Emotet has loader functionality, and failure to detect an infection can result in other malware being let in, possibly resulting in serious damage, so you have to take steps to detect it early.

■ Countermeasures

Emotet infection activity has stopped as of end-December 2022, but it could resume, so Emotet is one form of malware that we should continue to keep a close eye on. Emotet infiltrates systems when users open VBA macro-containing Microsoft Office files and shortcut files (LNK files). A method of limiting the damage caused by infections is to disable the automatic execution of macros so that macros are not executed when a file is opened. Both the Microsoft Office files and the shortcut files execute PowerShell to download Emotet, so disabling PowerShell from running, if you are not using it in your operations, is one possible countermeasure. If possible, ending the practice of using password-protected ZIP archives to share files and changing your operations to block password-protected ZIP files across the board when emails are received is also an effective step. To spread itself, Emotet will also regurgitate actual legitimate emails, so it can be difficult for humans to spot Emotet-related emails. If you suspect that you have been infected with Emotet by executing a macro or following a shortcut, you can use EmoCheck, a tool released by JPCERT/CC, to check for this[*8]. Making sure you are set up to enable early detection and a rapid initial response is also key, and this can be achieved through monitoring by a SOC or EDR and installing antivirus software.

1.3.2 VPN Device Vulnerabilities that Expose Corporate Networks

Stories of major corporations, hospitals, and other Japanese entities suffering damage from ransomware infections appeared frequently in the news in 2022 (Tables 1 and 2). Businesses had to temporarily shut down in some cases depending on the damage caused, resulting in product deliveries being delayed, hospitals pausing patient intake, and so forth, so the impact of infections rippled through to customers and local communities.

The main triggers of ransomware damage are systems being infected by malware from suspicious emails or suspicious sites and attackers infiltrating organizations' networks. The rise of telework in recent years has led an increasing number of companies to install VPN devices so that workers can connect to internal networks via the Internet, and so instances of attackers exploiting VPN device vulnerabilities to infiltrate networks are becoming quite prevalent. According to a survey by Japan's National Police Agency, 68% of companies that suffered ransomware damage in the first half of 2022 cited VPN devices as the intrusion route[*9].

In this section, we look at known VPN device vulnerabilities and discuss our SOC's observations of attacks targeting those vulnerabilities.

[*8] GitHub (@JPCERTCC) (https://github.com/JPCERTCC/EmoCheck).

[*9] National Policy Agency, "Information on cyberspace threats in 1H of 2022" (https://www.npa.go.jp/news/release/2022/20220914001.html, in Japanese).

VPN Device Vulnerabilities

Table 3 lists 14 VPN device-related vulnerabilities mentioned in alerts[*10] issued by JPCERT/CC during 2018–2022. “CVE ID” is the Common Vulnerabilities and Exposures Identifier managed by the US-based MITRE Corporation, and “CVSS v3 base score” is a gauge of the severity of the vulnerability, ranging from 0.0 to 10.0, as assessed by the US National Institute of Standards and Technology (NIST) under the Common Vulnerability Scoring System.

SOC’s Observations of Attacks Targeting the Vulnerabilities

Attack activity aimed at discovering and exploiting vulnerable VPN devices is relentless on the Internet. Figure 3 graphs the number (as a percentage) of attacks targeting the VPN device vulnerabilities shown in Table 3 observed by our SOC in 2022. The data are normalized so that the total number of attacks detected during the period sums to 100% on the vertical axis.

Table 3: Main VPN Device-Related Vulnerabilities (2018–2022)

Date published	Product vendor	CVE ID	CVSS v3 base score	When exploitable	Impact
Dec. 2022	Citrix	CVE-2022-27518	9.8	Before authentication	Execute arbitrary code
Dec. 2022	Fortinet	CVE-2022-42475	9.8	Before authentication	Execute arbitrary code
Oct. 2022	Fortinet	CVE-2022-40684	9.8	Before authentication	Bypass authentication on admin interface
Dec. 2021	SonicWall	CVE-2021-20038	9.8	Before authentication	Execute arbitrary code
Sep. 2021	SonicWall	CVE-2021-20034	9.1	Before authentication	Delete arbitrary file
Apr. 2021	Pulse Secure	CVE-2021-22893	10.0	Before authentication	Execute arbitrary code
Mar. 2021	F5 Networks	CVE-2021-22986	9.8	Before authentication	Execute arbitrary code
Feb. 2021	SonicWall	CVE-2021-20016	9.8	Before authentication	Steal credentials and session information
Jul. 2021	F5 Networks	CVE-2020-5902	9.8	Before authentication	Execute arbitrary code
Dec. 2019	Citrix	CVE-2019-19781	9.8	Before authentication	Execute arbitrary code
Jul. 2019	Palo Alto Networks	CVE-2019-1579	8.1	Before authentication	Execute arbitrary code
May 2019	Fortinet	CVE-2018-13379	9.8	Before authentication	Download arbitrary files
May 2019	Pulse Secure	CVE-2019-11510	10.0	Before authentication	Download arbitrary files
Apr. 2019	Pulse Secure	CVE-2019-11539	7.2	Before authentication	Execute arbitrary code

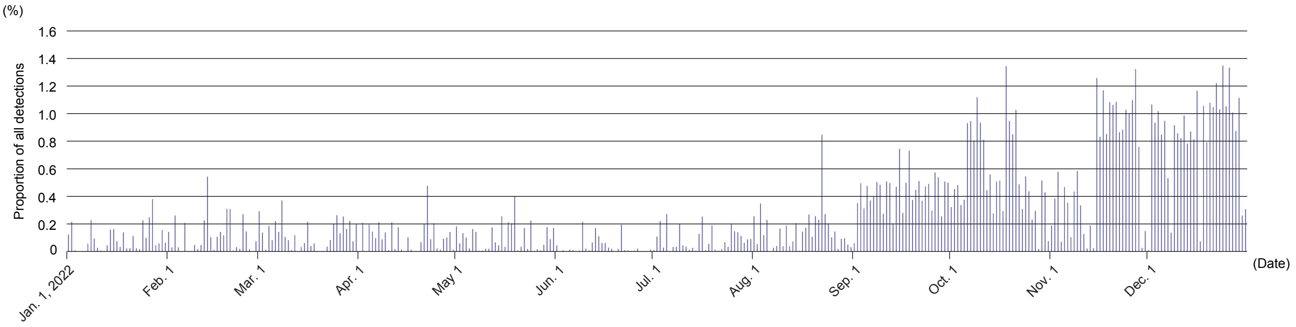


Figure 3: Observations of Attacks Targeting VPN Device Vulnerabilities (January – December 2022)

[*10] JPCERT/CC (https://www.jpcert.or.jp/english/at/2022.html).

As Figure 3 shows, attack activities targeting VPN device vulnerabilities persisted throughout the year, with the number of detections per day rising from September 2022. In Figure 4, we give a breakdown of detection counts (as a proportion of total) in 2022 for each of the CVE IDs in Table 3.

Of the vulnerabilities shown in Figure 4, our SOC analysts paid particular attention to the following.

CVE-2018-13379 (File-Stealing Vulnerability in Fortinet VPN devices)

CVE-2018-13379 was the most commonly detected vulnerability at 91.70% of total. Attackers can exploit this vulnerability to steal credentials needed to connect to VPNs. Despite more than three years having passed since it was published, many attacks were still being carried out, with damage actually being caused in cases. A hospital that had been the subject of a ransomware attack in October 2021 published a report[*11] in June 2022 saying that the attacker had likely exploited CVE-2018-13379 to infiltrate its systems. The medical center hit by a ransomware attack in October per the incident calendar (Tables 1 and 2) may also have been affected, as it was shown[*12] that this vulnerability was present in the OS version used on VPN devices of the medical center's trading partner identified as the likely intrusion vector.

CVE-2022-40684 (Authentication Bypass Vulnerability in Fortinet VPN devices)

CVE-2022-40684 is a relatively new vulnerability published in October 2022. Attackers can exploit this vulnerability to bypass authentication and access the administration interface of the VPN device, which could provide a foothold for infiltrating an organization's internal network by changing settings. Figure 4 shows this accounted for 1.48% of detections in 2022, putting it in the No. 4 spot, but most of these detections occurred over a mere 11 days, December 21–31, 2022. Ongoing vigilance is required as such attacks may continue in 2023 and beyond.

Preventing Your Organization from Becoming a Victim

Steps you can take to prevent your organization from becoming another victim include: updating the OS and firmware of your VPN devices, turning off unnecessary functionality, not externally exposing functionality that does not need to be (e.g., administration interfaces), setting source IP address restrictions to allow VPN connections, and setting up two-factor authentication.

It must be remembered that even if you have not yet discovered an intrusion into your internal network, an attacker may have already established a foothold by stealing credentials or changing settings. In September 2021,

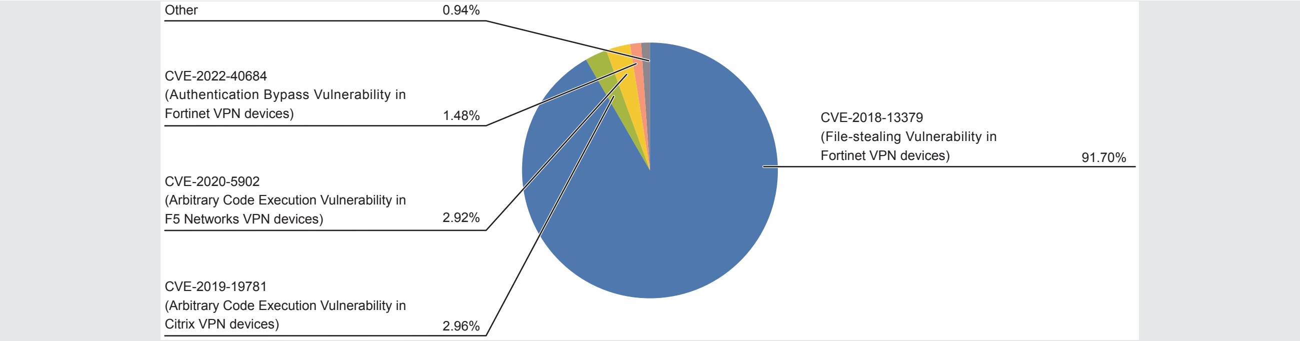


Figure 4: Detections by CVE ID (January–December 2022)

[*11] Tsurugi Municipal Handa Hospital, Tokushima Prefecture, "Tsurugi Municipal Handa Hospital Computer Virus Infection Incident: Expert Committee's Investigation Report" (https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf, in Japanese).

[*12] Ministry of Health, Labor and Welfare, "13th Health/Medical/Nursing Care Information Utilization Investigative Committee, Materials of the Working Group on the Utilization of Medical Information" (https://www.mhlw.go.jp/stf/newpage_29667.html, in Japanese).

Fortinet announced that someone had disclosed credentials for some 87,000 Fortinet VPN devices worldwide[*13]. It said that the information disclosed was collected from VPN devices around the world via attacks exploiting the above-mentioned CVE-2018-13379. It has also been revealed[*12] that the information disclosed included credentials of ransomware victims in the incident calendar (Tables 1 and 2). When updating an OS or firmware, please also check for traces of unauthorized access to the VPN device and changes to device settings, and be sure to change credentials.

1.3.3 Vulnerabilities in 2022

As shown in the incident calendar (Tables 1 and 2), multiple software vulnerabilities were also published in 2022, and attacks exploiting those vulnerabilities occurred. This section covers vulnerabilities published in 2022 that our SOC observed as being exploited. Figure 5 shows a breakdown of the observations. All of the most commonly observed vulnerabilities carried the potential for remote code execution. Remote code execution (RCE) is when an attacker feeds a script containing specially crafted strings into an application (via an HTTP request, for example), causing arbitrary code to be executed on the application server that processes the input. Attackers can exploit RCE vulnerabilities to attempt various activities, including information theft, system hijacking and tampering, and malware distribution. This type of vulnerability is therefore generally considered a serious threat.

■ F5 BIG-IP Remote Code Execution Vulnerability (CVE-2022-1388)

TA BIG-IP iControl vulnerability (CVE-2022-1388) was published on May 4, 2022[*14]. BIG-IP is a family of communications control equipment made by F5 Networks. These products are deployed on corporate networks around the world. iControl is a REST API for operating BIG-IP products.

Attackers can use this vulnerability to pass specially crafted HTTP requests to the targeted BIG-IP system's iControl in order to bypass authentication and thereby gain the ability to execute arbitrary system commands with root privileges. If iControl on a BIG-IP system with this vulnerability is exposed on the Internet, attackers may be able to change device settings, which could lead

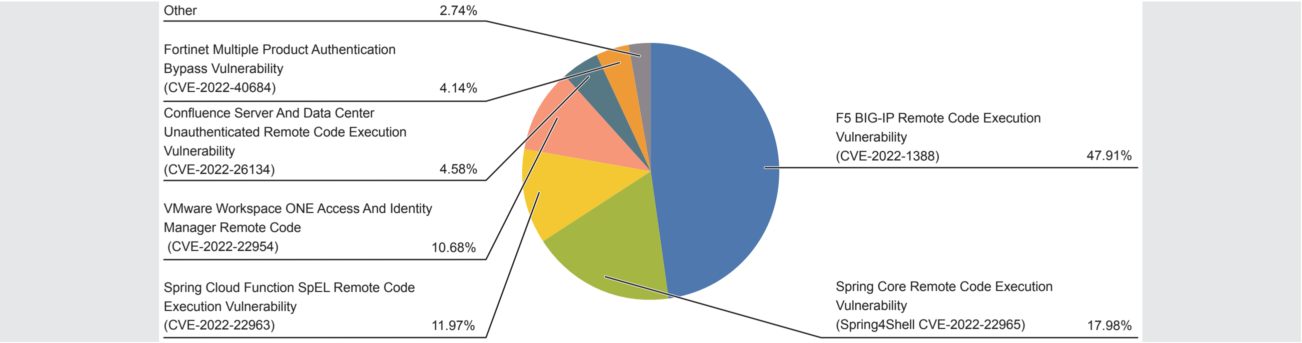


Figure 5: Breakdown of 2022 Vulnerability Exploits Observed

[*13] Fortinet, "Malicious Actor Discloses FortiGate SSL-VPN Credentials" (https://www.fortinet.com/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials).

[*14] F5 Networks, "Final - K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388" (https://support.f5.com/csp/article/K23605346).

to serious damage including internal network intrusion and traffic eavesdropping.

As Figure 5 shows, this was the most commonly observed vulnerability among those published in 2022, accounting for roughly half (47.91%) of the total. Many tools for exploiting this vulnerability have been released on source code repositories such as GitHub[*15], making them available for anyone to download and run. Code for using this vulnerability is also implemented in Metasploit, an open source penetration testing tool. Attackers do abuse Metasploit, and these tools make it easier to mount attacks. The availability of such attack tools and the high popularity of the product likely explain why these attacks are so prevalent. Figure 6 shows the trend in attacks targeting this vulnerability over 2022. The observations are normalized so that the total number of attacks detected during the period sums to 100% on the vertical axis. Observations started on June 1 and peaked two weeks later on June 18. The number of attacks then declined gradually but still remained high until mid-October. The attacks came from a wide range of sources spanning 36 countries across 6 continents. So we can infer that the attacks are being carried out worldwide. Even after this activity died down in November, we continued to intermittently observe a small number of attacks.

■ Spring Core Remote Code Execution Vulnerability (Spring4Shell CVE-2022-22965)

A vulnerability related to the Spring Framework (CVE-2022-22965), commonly known as Spring4Shell, was published on March 31, 2022[*16]. The Spring Framework is a Java-based web application development framework that was open sourced by VMware as one of the Spring Projects[*17].

This vulnerability (CVE-2022-22965) exists in Spring Core (the Spring Framework's core module) and could allow remote code execution in Java applications that use the Spring Framework.

The Spring Framework accounts for a large share of Java-based web application development, but because the conditions under which this vulnerability could be executed were limited, only a small number of users were impacted.

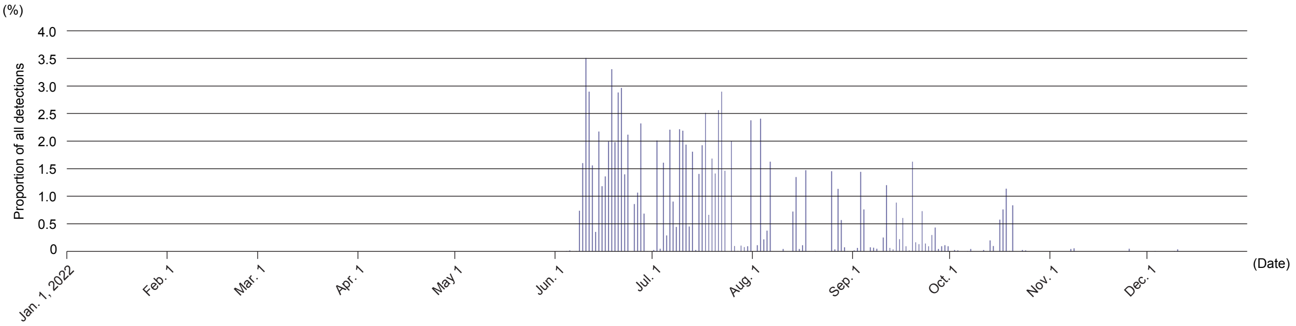


Figure 6: Observations of Attacks Targeting a BIG-IP Vulnerability (CVE-2022-1388) (January–December 2022)

[*15] GitHub (https://github.com/).

[*16] Spring, "Spring Framework RCE, Early Announcement" (https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement).

[*17] Spring (https://spring.io/projects).

When this vulnerability is used to execute remote code, HTTP requests are sent in two steps. The first HTTP request exploits the application logging functionality to write a log file to the web server containing a program (a webshell) for executing arbitrary commands. The second HTTP request then specifies the log file (webshell) created in the previous step as the URL path and sends arbitrary commands. This results in arbitrary code being executed through the webshell created in the first step. Note that Figure 7 only graphs communications used to create the webshell in the first step.

This vulnerability was the second most commonly observed among those published in 2022.

The third most commonly observed vulnerability (CVE-2022-22963) is also related to the Spring Project. It is a separate vulnerability that existed in Spring Cloud[*18]. Spring Cloud is a project concerned with the development of cloud environments, and because it has a limited user base relative to that of the core Spring Framework, the Spring Framework vulnerability (CVE-2022-22965) likely has a greater impact.

■ VMware Workspace ONE Access And Identity Manager Remote Code (CVE-2022-22954)

A vulnerability (CVE-2022-22954) related to VMWare's Workspace ONE Access, formerly known as Identity Manager, was published on April 6, 2022[*19].

Workspace ONE is a cloud-based application platform, and Workspace ONE Access is an application that manages access to workspaces.

This is a remote code execution vulnerability stemming from the way the target application's template engine processes templates. A template engine is a technology that processes input data to generate a document based on a template. Template engines are commonly used by web applications to dynamically generate HTML files. When an HTTP request containing a specially crafted character string is sent to an application server with this vulnerability and the template engine processes the input, it allows arbitrary code to be executed on the server. This sort of attack is called a server-side template injection.

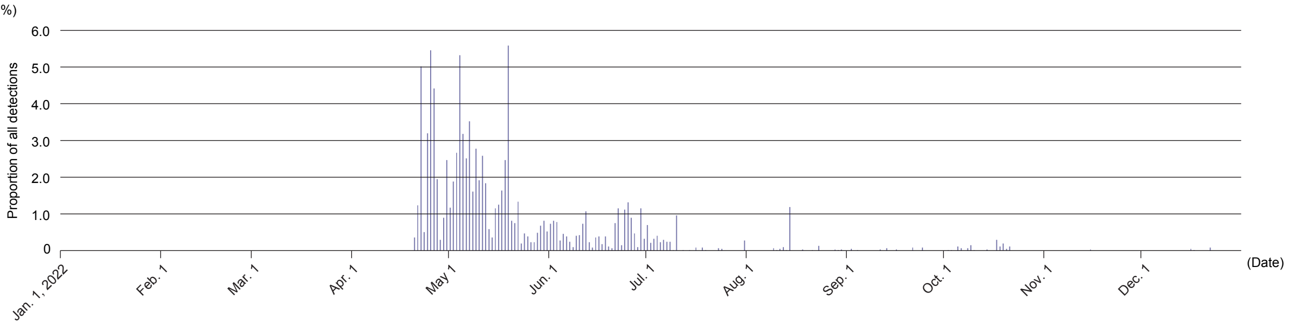


Figure 7: Observations of Attacks Targeting a Spring Framework Vulnerability (CVE-2022-22965) (January–December 2022)

[*18] VMware, "CVE-2022-22963: Remote code execution in Spring Cloud Function by malicious Spring Expression" (https://tanzu.vmware.com/security/cve-2022-22963).

[*19] VMware, "VMSA-2022-0014" (https://www.vmware.com/security/advisories/VMSA-2022-0014.html).

On May 18, the US Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 22-03 instructing US government agencies to take certain actions to combat multiple vulnerabilities in VMware products, including this vulnerability[*20]. This was the only Emergency Directive issued in 2022, which highlights just how much this was seen as high-risk vulnerabilities that could pose a major threat to US government agencies.

This vulnerability was the fourth most commonly observed vulnerability among those published in 2022. As Figure 8 shows, we logged our first observation on June 5, and the attacks continued intermittently thereafter. The number of attacks spiked on August 18 to a level roughly 20 times higher than the second highest number of observations, logged on October 18. Around 99.75% of the August 18 attacks originated from a single source, while the destinations were wide ranging. This surge in attacks was also reported by Mitsui Bussan Secure Directions's SOC[*21], and can be regarded as an example of a single attacker attempting a broad, large-scale attack. In addition, there were large increases in the number of attacks every one to two months, but they originated from a different country each time. As of this writing (January 2023), we continue to observe this vulnerability being exploited.

Confluence Server And Data Center Unauthenticated Remote Code Execution Vulnerability (CVE-2022-26134)

A vulnerability related to Confluence (CVE-2022-26134) was published on June 2, 2022[*22].

Confluence is an enterprise wiki application from Atlassian, and many companies have it installed. This vulnerability is a remote code execution vulnerability in the on-premise versions of Confluence Server and Confluence Data Center. All supported versions contained the vulnerability, so a wide range of users were susceptible. Including out-of-support versions, all versions of Confluence since 1.3.0, the first version released in 2004, were vulnerable. The cloud version of Confluence Cloud is not susceptible to this vulnerability. An updated version was not available when the vulnerability was published; a fix was released the following day, June 3, 2022.

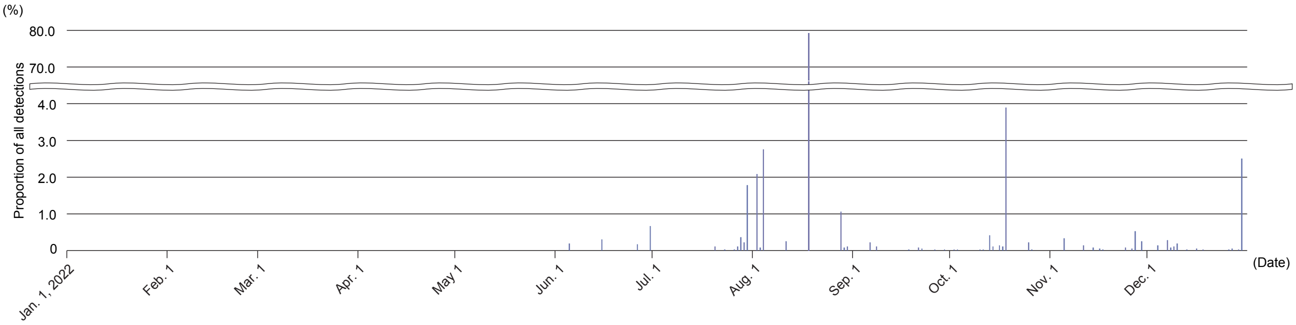


Figure 8: Observations of Attacks Targeting a Workspace ONE Access / Identity Manager Vulnerability (CVE-2022-22954) (January–December 2022)

[*20] US Cybersecurity and Infrastructure Security Agency, "Emergency Directive 22-03: Mitigate VMWare Vulnerabilities" (https://www.cisa.gov/emergency-directive-22-03).

[*21] Mistui Bussan Security Directions, "August 2022: MSBD-SOC Detection Trends and Topics" (https://www.mbsd.jp/research/20220914/20228-mbsd-soc/).

[*22] Atlassian, "Confluence Security Advisory 2022-06-02" (https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html).

The vulnerability is due to the execution of a Java-like expression language called OGNL (Object Graph Navigation Language). The execution of remote code can be triggered by injecting an OGNL expression containing a specially crafted string into an HTTP request and sending it to the targeted server. This is called OGNL injection, and this type of vulnerability is known to have caused major damage on the Apache Struts 2 web application framework in recent years.

This vulnerability was the fifth most commonly observed vulnerability among those published in 2022. As Figure 9 shows, we logged our first observation on June 18, followed by brief increases in attacks at intervals of about a month. On many of the days on which attacks increased, we observed a lot of exploit code attempting to execute the Linux id command. The id command only lists information on the user executing it, so it poses no direct threat when executed. That said, this command is often used by attackers to determine whether a target has a vulnerability, and if attackers find a vulnerability to be present, there is a risk they will carry out a malicious attack at a later time. In addition to exploit code using the id command, exploit code using the Linux wget and curl commands has also been observed. This exploit code downloads a malicious script from an external site and executes it. If this is executed on a server, it could result in malware being installed. As of this writing (January 2023), we continue to observe this vulnerability being exploited.

This section has looked at four vulnerabilities widely observed by our SOC from among those published in 2022. Susceptible product versions can be found via the URLs cited for each vulnerability[*14][*16][*19][*22]. If you are running a susceptible version of one of these applications, we recommend obtaining an updated version.

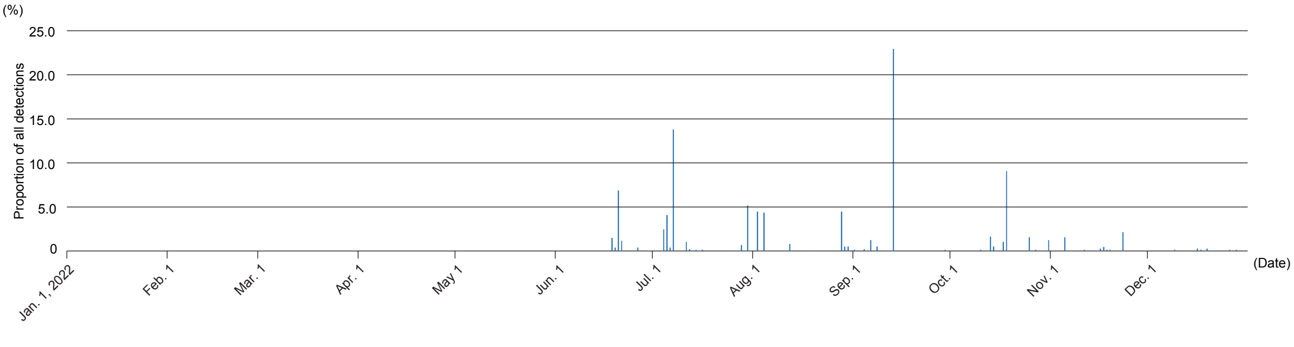


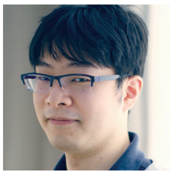
Figure 9: Observations of Attacks Targeting a Confluence Vulnerability (CVE-2022-26134) (January–December 2022)

1.4 Conclusion

This report covered security incidents that drew attention in 2022 and discussed our observations on those that our SOC analysts were focused on during the year. Our observations show that even some older attacks continue to persist. In Section 1.3.1, for example, we discussed how Emotet has seen repeated bouts of proliferation and quiescence while being updated over time, and in Section 1.3.2 we explained that a FortiOS vulnerability (CVE-2018-13379) published in 2019 was the most common one we observed among attacks targeting VPN devices. We need to remain vigilant always, not just when security topics erupt. As Section 1.3.3 discussed, meanwhile, we also observed new attacks exploiting vulnerabilities published in 2022. Constantly gathering information on vulnerabilities and updates for the products and associated services you use is crucial.

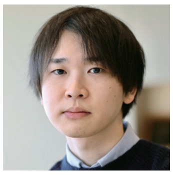
IIJ's SOC will continue to use wizSafe Security Signal and other avenues to publish information on threats observed via our Data Analytics Platform, key security topics, and the like in the hopes that it will prove useful to you in your security responses and operations.

Eisei Honbu
Data Analysis Section, Security Operations Department, Advanced Security Division, IIJ



Shimpei Miyaoka
Data Analysis Section, Security Operations Department, Advanced Security Division, IIJ

Katsuhiro Tomiyama
Data Analysis Section, Security Operations Department, Advanced Security Division, IIJ



Shota Saito
Data Analysis Section, Security Operations Department, Advanced Security Division, IIJ