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. Four years have now passed since we launched wizSafe, and at our SOC, we have been constantly reworking our systems with a view to incident response capabilities and to optimize our operations. The SOC had so far focused on creating frameworks for detecting threats using the Data Analytics Platform[*1], and we have now shifted direction toward actually using the information obtained through the Data Analytics Platform. This has enabled us to step up threat detection and the use of the information we report.

Since 2017, the SOC has reported via the wizSafe Security Signal[*2] site on threats observed via the Data Analytics Platform, which collates logs from IIJ services, and on a variety of security topics. Most events and conferences in 2020 were held remotely, and the SOC also shared its knowledge and insight by presenting remotely at IIJ Technical NIGHT and the Japan Security Analyst Conference (JSAC) 2021[*3]. IIJ Technical NIGHT is a seminar aimed at engineers, and three members of the SOC, each with different areas of expertise, presented on their activities to a large number of attendees[*4,5]. At JSAC 2021, we presented on our efforts in 2020 to proactively collect threat information on attack campaigns targeting cryptocurrency operators[*6].

In this report, we summarize our SOC's observations in the hopes they will provide useful insights to our readers. Section 1.2 looks at security topics that rose to prominence in Japan in 2020 along with security service statistics for the year. Section 1.3 discusses topics our SOC analysts focused on.

1.2 2020 Security Summary

Here, we look at prominent security incidents in 2020 along with information on attacks observed by the SOC.

1.2.1 Incident Calendar

Tables 1 and 2 summarize the major security incidents that our SOC focused on in 2020.

[*1] Internet Infrastructure Review (IIR) Vol. 38 (https://www.iij.ad.jp/en/dev/iir/038.html).

[*2] wizSafe Security Signal (https://wizsafe.iij.ad.jp/, in Japanese).

[*3] Japan Security Analyst Conference 2021 (https://jsac.jpcert.or.jp/en/index.html).

[*4] Presentation materials: IIJ Technical NIGHT Vol. 9 (https://eng-blog.iij.ad.jp/archives/6453, in Japanese).

[*5] COVID-19 IT study session, 2 realizations from the switch from physical to online (https://eng-blog.iij.ad.jp/archives/7141).

[*6] JPCERT/CC, "Hunting threat information on attack campaigns targeting cryptocurrency operators" (https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_302_kodera_jp.pdf).

Table 1: Incident calendar (January–June)

Month	Summary/URL(s)
January	**It was announced that a breach of personal/confidential information may have occurred because of unauthorized system access that exploited vulnerabilities in an electronics manufacturer's antivirus system for which security patches had not yet been released.** (Mitsubishi Electric) "Possible breach of personal information and corporate secrets due to unauthorized system access" https://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf (in Japanese) "Possible breach of personal information and corporate secrets due to unauthorized system access (2nd report)" https://www.mitsubishielectric.co.jp/news/2020/0210-b.pdf (in Japanese) "Possible breach of personal information and corporate secrets due to unauthorized system access (3rd report)" https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf (in Japanese)
January	**A major electronics manufacturer announced that due to unauthorized access to some servers used by its defence business division, files shared between its internal departments had been accessed.** (NEC) "Unauthorized access of NEC's internal servers" https://jpn.nec.com/press/202001/20200131_01.html (in Japanese)
March	**Microsoft announced that the SMBv3 protocol contains a vulnerability that could allow an unauthenticated attacker to execute arbitrary code on an SMB server or client.** (Microsoft) "Microsoft Guidance for Disabling SMBv3 Compression" https://portal.msrc.microsoft.com/en-JP/security-guidance/advisory/adv200005 "Windows SMBv3 Client/Server Remote Code Execution Vulnerability" https://portal.msrc.microsoft.com/en-JP/security-guidance/advisory/CVE-2020-0796
March	**Trend Micro announced that several of its products had critical vulnerabilities and that it had observed attempts against at least one of these vulnerabilities in the wild.** (Trend Micro) "Security Bulletin: Multiple Critical Vulnerabilities in Trend Micro Apex One and OfficeScan" https://success.trendmicro.com/solution/000245571
April	**An education platform company announced there had been unauthorized access to a service it operates, and that around 1.22 million records, including service IDs and encrypted passwords, may have been viewed.** (Classi) "Investigation report on temporary service outage and password change request" https://corp.classi.jp/news/1926/ (in Japanese)
April	**A video game company announced that around 160,000 accounts may have been compromised due to an unauthorized third party logging into accounts on the network service the company provides.** (Nintendo) "Unauthorized logins using Nintendo Network IDs and advisory on the safe use of your Nintendo account" https://www.nintendo.co.jp/support/information/2020/0424.html (in Japanese)
April	**A vulnerability was revealed in Microsoft Teams that could allow an account to be taken over by an attacker who causes a user to view a GIF file or link on a subdomain controlled by the attacker.** (CyberArk) "Beware of the GIF: Account Takeover Vulnerability in Microsoft Teams" https://www.cyberark.com/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams/
May	**A telecommunications carrier announced that an intrusion into an overseas-based server running its services facilitated unauthorized access to one of its servers in Japan, possibly resulting in the breach of service-related construction information pertaining to 621 corporate clients.** (NTT Communications) "NTT Com confirms possible information leak due to unauthorized access" https://www.ntt.com/en/about-us/press-releases/news/article/2020/0702.html
June	**A foreign security company announced a set of 19 vulnerabilities, collectively called Ripple20, found in products with the TCP/IP stack developed by Treck for embedded devices. Ripple20 includes vulnerabilities that allow the execution of remote code.** (JSOF) "Overview- Ripple20" https://www.jsof-tech.com/ripple20

Table 2: Incident calendar (July–December)

Month	Summary/URL(s)
July	**Our SOC confirmed that the distribution of emails designed to spread the malware Emotet had resumed after not having been observed since February. The attacks methods had become more sophisticated and included, for example, the use of emails and other information stolen from infected devices in subsequent attacks as well as password-protected ZIP files. These attacks were observed up until October.**
August	**It was reported that attackers had exploited a vulnerability in a VPN product for which an update had been released in 2019, resulting in usernames, passwords, and other information used on some 900 servers being published on a hacking forum and thus made available to third parties. It was subsequently reported in the Japanese media that the leaked information included information on several Japanese companies.** (Nikkei xTECH) "Unpatched Pulse Secure VPN exposes IP addresses of 46 Japanese companies" https://xtech.nikkei.com/atcl/nxt/news/18/08605/ (in Japanese)
September	**A provider of e-money services announced that money had been illegally withdrawn owing to unauthorized use of its e-money service by a third party at a partnering financial institution. A string of similar announcements subsequently emerged from other e-money service providers and their partnering financial institutions.** (NTT Docomo) "Unauthorized use of Docomo accounts using information on accounts at some banks" https://www.nttdocomo.co.jp/info/notice/page/200908_02_m.html (in Japanese)
September	**JPCERT/CC announced that several organizations in Japan had confirmed they had received extortionary demands for cryptocurrency under threat of DDoS attacks or that they had been impacted by DDoS attacks.** (JPCERT/CC) "Extortion attempts (DDOs threats) demanding transfer of cryptocurrency under threat of DDoS attack" https://www.jpcert.or.jp/newsflash/2020090701.html (in Japanese)
September	**A foreign security company released a report on a privilege escalation vulnerability (CVE-2020-1472) in Netlogon used in Active Directory. This vulnerability was dubbed Zerologon. It is relatively easy to exploit, and tools available to attackers also implement the ability to exploit this vulnerability. When exploited, the domain admin account password can be changed and domain admin privileges can be obtained.** (Secura) "Zerologon: Instantly Become Domain Admin by Subverting Netlogon Cryptography (CVE-2020-1472)" https://www.secura.com/blog/zero-logon
October	**The Ministry of Internal Affairs and Communications and the Council of Anti-Phishing Japan released alerts to say that emails and phishing websites purporting to offer the government's Special Cash Payments had been seen.** (Ministry of Internal Affairs and Communications) "Alert on emails purporting to offer Special Cash Payments" https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000438.html (in Japanese) (Council of Anti-Phishing Japan) "Phishing posing as notifications regarding Special Cash Payments (Oct 15, 2020)" https://www.antiphishing.jp/news/alert/kyufukin_20201015.html (in Japanese) "Update: Phishing posing as notifications regarding Special Cash Payments (Oct 19, 2020)" https://www.antiphishing.jp/news/alert/kyufukin_20201019.html (in Japanese)
November	**A video game developer announced it had been the victim of a customized ransomware attack following unauthorized access to its network by a group of attackers calling itself Ragnar Locker. As of January 2021, up to 390,000 information records had been compromised, it said, including personal information of customers, employees, and other related individuals (investigation ongoing as of this writing).** (Capcom) "Notice Regarding Network Issues due to Unauthorized Access" https://www.capcom.co.jp/ir/english/news/html/e201104.html "Update Regarding Data Security Incident Due to Unauthorized Access" https://www.capcom.co.jp/ir/english/news/html/e201116.html "3rd Update Regarding Data Security Incident Due to Unauthorized Access" https://www.capcom.co.jp/ir/english/news/html/e210112.html
November	**Our SOC observed IcedID malware infections, and these observations persisted until early December.**
November	**An operator of an event/communications management service announced that the service it operates had been the victim of unauthorized access, resulting in the theft of up to 6.77 million customer information records, including personal information. Subsequently, many organizations that had been using the service issued alerts on this incident.** (Peatix) "Apology and notification of unauthorized access of our Peatix (https://peatix.com/) service" https://announcement.peatix.com/ 20201117_ja.pdf (in Japanese) "Report of third-party investigation into unauthorized access of our Peatix (https://peatix.com/) service and our response going forward" https://announcement.peatix.com/20201216_ja.pdf (in Japanese)
December	**A power generation systems company announced it had been the victim of unauthorized access by a third party via a managed service provider (MSP), resulting in servers and PCs being infected. It also noted that the root cause was a vulnerability in software provided by the MSP but that the vulnerability was undisclosed and a patch or other countermeasures had not been made available.** (Mitsubishi Power) "Unauthorized access of our network by a third party via a managed service provider" https://power.mhi.com/jp/news/20201211.html (in Japanese)

1.2.2 Observational Data from IIJ Managed Security Services

This section looks at the SOC's observations using the Data Analytics Platform in 2020.

■ DDoS Attacks

Here, we look at DDoS attacks detected by the IIJ DDoS Protection Service.

The methods used in DDoS attacks in 2020 were largely unchanged from previous years. So existing countermeasures are likely still effective as well. Table 3 summarizes attacks detected in each month of 2020.

The largest-scale attacks in each month were all Amplification attacks using UDP as the transport protocol. Commonly used application protocols included DNS, NTP, and LDAP, and a series of attacks using multiple protocols was also observed. And aside from UDP Amplification attacks, SYN flood attacks were also observed among the longest-duration attacks in each month.

■ Attacks Detected by IPS/IDS Devices

Here, we look at attacks detected by IIJ Managed IPS/IDS Service devices.

We observed attacks that infect IoT (Internet of Things) devices with malware throughout 2020. Attackers have been specifically targeting IoT devices in recent years in a trend that is ongoing. IoT devices are increasing rapidly in number, yet some devices continue to operate with known vulnerabilities exposed because of a lack of proper patch management. Attackers exploit such vulnerabilities to infect devices with malware, allowing them to control the devices remotely. IoT devices seized by an attacker are at risk of being exploited to launch other attacks, such as DDoS attacks. Many types of malware that infects IoT devices (IoT malware) have been identified, and the range of vulnerabilities exploited to infect devices is broad. The most commonly detected attacks in 2020 were those exploiting vulnerabilities in Netis/Netcore routers. Many of these attacks were intended to infect the routers with a variant of Gafgyt, a type of IoT malware.

Table 3: Summary of Observational Data on DDoS in 2020

Month	No. of incidents (daily avg.)	Approx. max. no. of packets per sec.(x10,000)	Maximum traffic		Maximum attack duration	
			Bandwidth (Gbps)	Method	Duration (h:mm)	Method
1	14.45	~25	2.19	SNMP Amplification	0:16	NTP Amplification
2	13.07	~1114	29.02	SSDP Amplification	1:50	SYN Flood
3	16.41	~999	90.86	DNS & NTP Amplification	0:51	Amplification of DNS, NTP, LDAP, etc.
4	24.63	~184	19.17	DNS Amplification	0:19	Amplification of DNS, NTP, LDAP, etc.
5	15.06	~296	32.11	NTP & LDAP Amplification	0:22	NTP Amplification
6	23.33	~824	21.42	SSDP Amplification	1:19	SSDP Amplification
7	11.84	~93	3.34	NTP Amplification	0:29	NTP Amplification
8	11.29	~743	58.90	DNS & Apple Remote Management Service Amplification	2:43	DNS & Apple Remote Service Amplification
9	12.73	~114	11.21	DNS & LDAP Amplification	0:23	LDAP Amplification
10	18.45	~78	7.54	DNS & LDAP Amplification	0:15	DNS Amplification
11	17.00	~434	43.23	DNS Amplification	3:11	DNS Amplification
12	17.39	~532	56.56	DNS Amplification	0:32	SYN Flood

Observations showed a lot of infections for IoT malware called XTC in April and Mozi in September. The XTC infections observed in April exploited multiple vulnerabilities (CVE-2020-9054, CVE- 2020-5722, CVE-2020-8515)[*7].

■ Malware Detected with Accessing the Web

We now take a look at malware detected when accessing the web using the IIJ Secure Web Gateway Service.

We observed malicious JavaScript throughout the year in 2020. In many cases, legitimate websites had been modified, with malicious JavaScript being injected. Observations confirmed that visiting such websites results in cookies, device information, and the like being sent to external sites, and the browser being redirected to other sites including fake prize sites and advertisements.

We also detected a lot of traffic related to Emotet. We take a detailed look at Emotet in Section 1.3.2.

■ Malware Detected When Receiving Emails

Here, we look at malware detected when emails were received on the IIJ Secure MX Service. In 2020, we observed cases of attackers using emails cleverly crafted to be relevant to current events in a bid to dupe users into malware infections.

First, we look at samples of emails that use attention-grabbing words in the subject line etc. From around March, for example, we detected an increase in malware-laden English-language emails purporting to provide information on COVID-19. Similarly, we observed an increase in Japanese-language emails using terms like “work at home”, “cold & flu”, and “bonus”.

Next, we look at examples in which attackers may have deliberately timed malware emails. Figure 1 shows the hour-by-hour count of emails in which a signature indicating a suspicious Microsoft Office document was detected in September 2020. The vertical axis is normalized by setting the total number of such signatures detected over the sample period to 100%. It is evident from the graph that the emails tend to be sent during standard working hours for companies in Japan. Several factors may be behind this, one being that attackers may have deliberately selected what time to send their emails out.

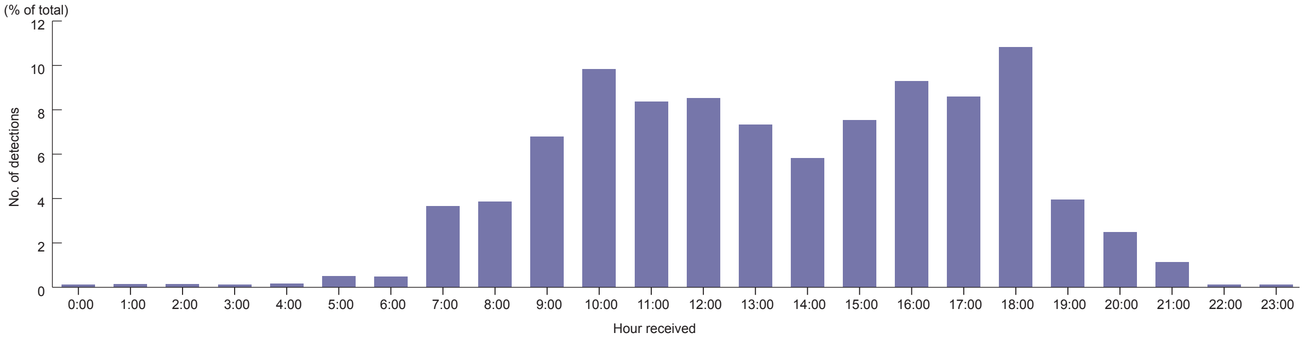


Figure 1: No. of Emails Containing Suspicious Microsoft Office Documents Received each Hour (Sep. 2020)

[*7] Observations of infections with Mirai variant (https://wizsafe.iij.ad.jp/2020/05/967/, in Japanese).

1.3 Security Topics

This section looks at key topics our analysts focused on from among attacks detected by the SOC in 2020.

1.3.1 SSL-VPN Product Vulnerabilities

Virtual private networks (VPNs) are used to connect to internal systems from outside of an organization via the Internet and the like. COVID-19 sparked rapid changes in the way we work in 2020, prompting more and more companies to roll out VPNs to facilitate working from home, so it seems that a lot of VPNs are now being used in this way. Since they provide a means of accessing internal systems from outside of an organization, VPNs necessitate even greater diligence in addressing vulnerabilities. Indeed, 2020 saw cases of VPN product vulnerabilities being exploited and leading to data breaches. VPNs can use SSL/TLS to encrypt communications, and several vulnerabilities in products that use this method were revealed in 2019[*8,9]. In 2020, we observed attacks targeting these products with the 2019 vulnerabilities not properly fixed[*10,11].

Our SOC observed traffic involved in attacks targeting SSL-VPN vulnerabilities in Fortinet's FortiOS (CVE-2018-13379) and in Citrix Systems' Citrix Application Delivery Controller and Citrix Gateway (CVE-2019-19781).

■ Observations of Attacks Targeting a Vulnerability in Fortinet's FortiOS (CVE-2018-13379)

Figure 2 graphs the proportion of traffic targeting CVE-2018-13379 as detected on the IIJ Managed IPS/IDS Service. The vertical axis is normalized by setting the total number of such signatures detected over the sample period to 100%.

Exploiting this SSL-VPN vulnerability in Fortinet's FortiOS may allow an attacker to remotely read an arbitrary file on the product without authentication. We observed high levels of this traffic on November 4 and December 11 in particular, respectively accounting for 10.27% and 10.83% of the total. Traffic targeting this vulnerability tended to rise toward the end of the year, with the December detection count making up 37.93% of the total. In November, a list of hosts affected by the vulnerability was published on the Internet[*12]. Although this may have been a factor in the rise in detections in December, we did not find any clear evidence of a relationship here.

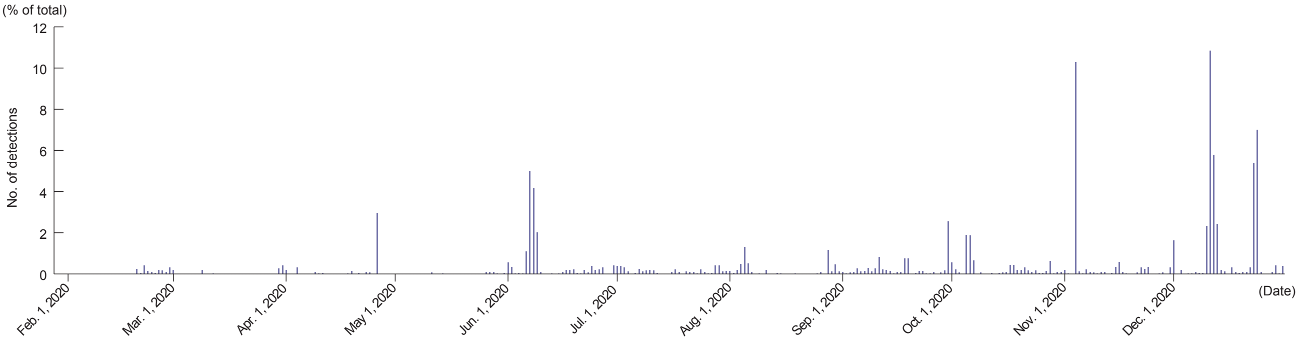


Figure 2: CVE-2018-13379 Detections (Feb.–Dec. 2020)

[*8] JPCERT/CC, "Alert Regarding Vulnerabilities in Multiple SSL VPN Products" (https://www.jpcert.or.jp/at/2019/at190033.html, in Japanese).

[*9] JPCERT/CC, "Alert Regarding Vulnerability (CVE-2019-19781) in Citrix Products" (https://www.jpcert.or.jp/at/2020/at200003.html, in Japanese).

[*10] Bad Packets, "Over 14,500 Pulse Secure VPN Endpoints Vulnerable to CVE-2019-11510" (https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/).

[*11] Bad Packets, "Over 25,000 Citrix (NetScaler) Endpoints Vulnerable to CVE-2019-19781 (https://badpackets.net/over-25000-citrix-netscaler-endpoints-vulneraeble-to-cve-2019-19781/).

[*12] JPCERT/CC, "About the disclosure of information regarding hosts affected by vulnerability (CVE-2018-13379) in Fortinet's FortiOS SSL VPN feature" (https://www.jpcert.or.jp/newsflash/2020112701.html, in Japanese).

Observations of Attacks Targeting a Vulnerability in Citrix Application Delivery Controller and Citrix Gateway (CVE-2019-19781)

Figure 3 graphs the proportion of traffic targeting CVE-2019-19781 as detected on the IIJ Managed IPS/IDS Service. The vertical axis is normalized by setting the total number of such signatures detected over the sample period to 100%.

Exploiting this vulnerability in Citrix Systems' Citrix Application Delivery Controller and Citrix Gateway may allow an attacker to remotely execute arbitrary code without authentication. We observed high levels of this traffic on February 18 and March 13 in particular, respectively accounting for 13.23% and 10.36% of the total. The number of detections tended to decline from March onward, but we observed traffic targeting this vulnerability intermittently right up until December. Given the rise in detections at points in November and December, this activity will also bear close watching ahead.

Countermeasures

The vulnerabilities CVE-2018-13379 and CVE-2019-19781 were disclosed in 2019, but we observed attacks on them throughout 2020. If you are using an affected version of these products, you need to address this by updating to a fixed version of the software. We also recommend staying abreast of information on vulnerabilities in products used within your organization and not just VPN products.

1.3.2 Observations on Emotet and IcedID

This section looks at the Emotet and IcedID malware, which featured prominently in 2020. First, we describe the characteristics of Emotet and summarize observations related to Emotet detections on the IIJ Security MX Service and IIJ Secure Web Gateway Service. We then look at IcedID's characteristics and summarize observations related to its detection on the IIJ Security MX Service and IIJ Secure Web Gateway Service.

Emotet Observations

Attacks that spread malware via emails occur every day. Most prominent among these are attacks that spread Emotet, and they were rampant in 2020. Emotot originally started out as a type of malware called a banking Trojan, designed to steal financial information and the like, but it has morphed as new functionality has been added to it. Specifically, it has gained the ability to spread itself, botnet functionality, and loader functionality that lets it distribute other malware. The self-spreading functionality steals data from infected computers such as email addresses, account information, and email text and attachments, and sends this to a C&C server. Also, based on the information it steals, Emotet sends forged emails to the original email senders, inducing them to open attachments. These characteristics make Emotet a powerful type of malware. Known methods by which Emotet spreads are emails with doc file attachments, and URLs in email text and document files that cause

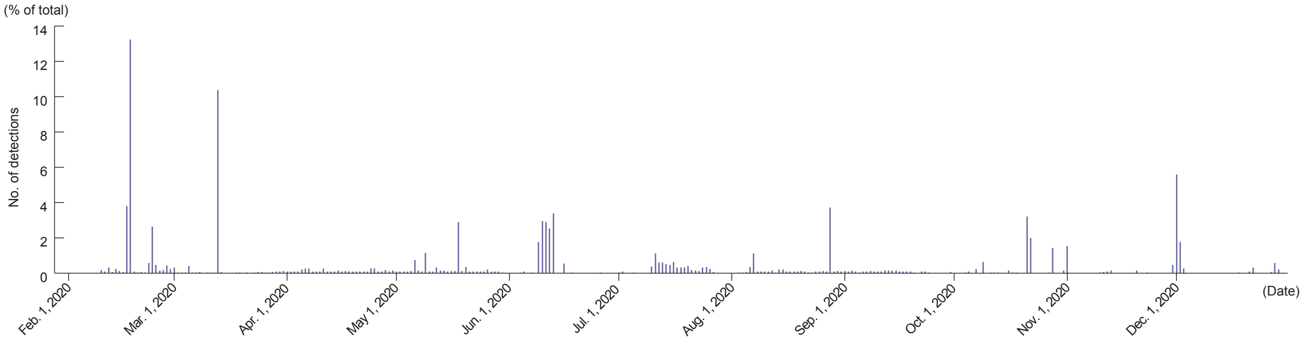


Figure 3: CVE-2019-19781 Detections (Feb.–Dec. 2020)

doc files to be downloaded. This is now joined by a new method observed in September whereby Emotet sends a doc file in a password-protected ZIP archive[*13]. Because the contents of files compressed into password-protected ZIP archives cannot be scanned, the files cannot be inspected by antivirus tools, sandboxing tools, and so forth. So password-protected ZIP files have a greater chance of reaching the user than doc files that are simply attached in the conventional way.

JPCERT/CC observations confirmed an increase in email activity related to Emotet around July[*14]. And Cisco reported[*15] that this activity continued beyond that. The activity died down from end-October, but activity related to the distribution of Emotet resumed in late December[*16].

Our SOC observed Emotet-related attacks from July through September. We saw a sharp rise in attacks spreading Emotet in September in particular.

Figure 4 shows the Emotet-related detection rates for attacks detected on the IIJ Secure MX Service between July and October. The vertical axis is normalized by setting the total number of Emotet-related detections over the sample period to 100%.

Emotet observations were increasing from late July. They then increased rapidly around September 15 and peaked on September 18.

Emotet traffic was also detected on the IIJ Secure Web Gateway Service. The service detected two types of Web access related to Emotet.

1. Downloads of files in Microsoft Word 97-2003 (doc) format that contain macros designed to cause Emotet infections
2. Emotet communications with command and control (C&C) servers post infection

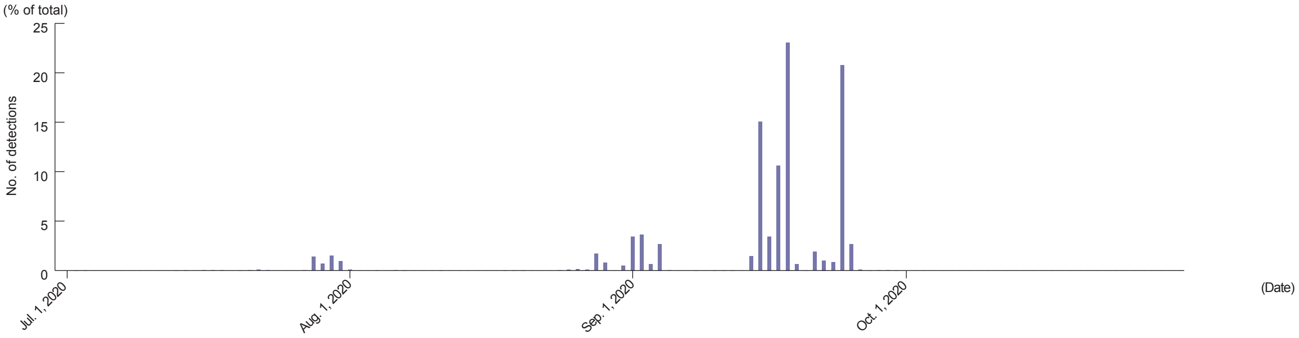


Figure 4: Detection of Emotet when Receiving Emails (Jul.–Oct. 2020)

[*13] Information-technology Promotion Agency, Security Center, "Sharp increase in inquiries / Example of attack using password-protected ZIP file (added Sep. 2, 2020)" in "Emails designed to cause infections with the virus called Emotet" (https://www.ipa.go.jp/security/announce/20191202.html#L13, in Japanese).

[*14] JPCERT/CC, "Resumption of distribution of emails leading to infections with the Emotet malware (update)", https://www.jpcert.or.jp/newsflash/2020072001.html, in Japanese).

[*15] Cisco Japan Blog, "Activity resumes: Analysis of 2020 Emotet activity" (https://gblogs.cisco.com/jp/2020/11/talos-emotet-2020/, in Japanese).

[*16] JPCERT/CC, "Stay wary of emails likely to cause Emotet and other malware infections" (https://www.jpcert.or.jp/newsflash/2020122201.html, in Japanese).

Figure 5 graphs Emotet-related traffic detected on the IIJ Secure Web Gateway Service between July and October. The vertical axis is normalized by setting the total number of Emotet-related detections over the sample period to 100%.

In our 2019 IIR periodic observation report[*17], we only had detections of HEUR:Trojan.MSOffice.SAgent, but in 2020, we also detected Trojan-Banker.Win32.Emotet. In the case of HEUR:Trojan.MSOffice.SAgent, we detected doc files that download Emotet. In the case of Trojan-Banker.Win32.Emotet, we confirmed that all files detected were Emotet. HEUR:Trojan.MSOffice.SAgent detections first appeared on July 21 and peaked on July 28. Trojan-Banker.Win32.Emotet was first detected on September 2 and peaked on September 3.

IcedID Observations

In November, when Emotet declined after showing up repeatedly since July, we observed attacks spreading malware called IcedID. Like Emotet, IcedID was originally a type of banking Trojan, but in addition to this functionality, it has now gained the ability to serve as a loader for other malware. Once it infects a computer, IcedID steals financial institution credentials and other information, and sends the data to a C&C server. Emotet and IcedID share commonalities in that they both use emails to spread malware, and they use doc files as an infection vector. And since it was first observed, IcedID has been spreading by attaching password-protected ZIP archives to emails, similar to the method Emotet has been using since September[*18]. So there are commonalities between the two, but unlike Emotet, IcedID does not build botnets.

Figure 6 graphs proportional counts for communications with C&C servers observed on the IIJ Secure Web Gateway Service between October and December. The vertical axis is normalized by setting the total number of communications with C&C servers over the sample period to 100%. The first observation came on November 3, with November 20 being the peak. As the graph shows, these communications continued up to December 2. We also determined that there were changes between the November 3 and November 20 observations in terms of the operations performed between when the doc file used in the attack was opened and when the infection occurred[*19], and these dates correspond to the day on which we first observed communications with C&C servers and the point in time in our observational window at which these communications were at their peak.

Countermeasures

Both Emotet and IcedID infect computers when a doc file is opened and a VBA macro executed. So one way of reducing the damage caused by infections is to disable the execution of macros when files are opened. See our wizSafe Security Signal article[*20] for details of how to disable macros to prevent malware infections. It is also crucial that users do not

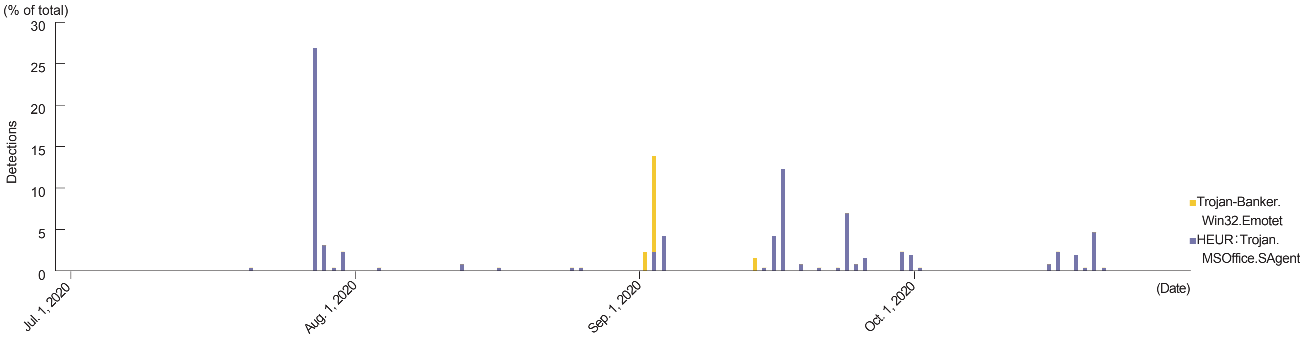


Figure 5: Detections of Emotet-related Traffic when Accessing the Web (Jul.–Oct. 2020)

[*17] Internet Infrastructure Review (IIR) Vol. 46 (https://www.iij.ad.jp/en/dev/iir/046.html).

[*18] JPCERT/CC Analysis Center (https://twitter.com/jpcert_ac/status/1324561915738091522/, in Japanese).

[*19] Analysis of the IcedID campaign directed at Japan (https://mal-eats.net/2020/11/12/analysis_of_the-_icedid_campaign_for_japan/, in Japanese).

[*20] Disabling VBA macros as a countermeasure against malware infections (https://wizsafe.iij.ad.jp/2020/09/1044/, in Japanese).

inadvertently open attached files that cannot be confirmed as safe.

1.4 Conclusion

This report presented a 2020 incident calendar, annual data for IIJ security services, and observational information that our SOC analysts were focused on in 2020. We expect to continue to see attacks targeting the SSL-VPN vulnerabilities we discussed in Section 1.3.1 and attacks using Emotet and IcedID, which we covered in Section 1.3.2, even as the targets, methods, and names involved change over time. We also observe a range of other security threats, beyond the examples discussed here, every day. And to go beyond the discussion in Sections 1.2 and 1.3, properly understanding and dealing with such threats is crucial. IIJ's SOC will continue to publish a range of information such as updates on threats observed on the Data Analytics Platform and key security topics, and we hope this information will prove useful in your security countermeasures and operations.

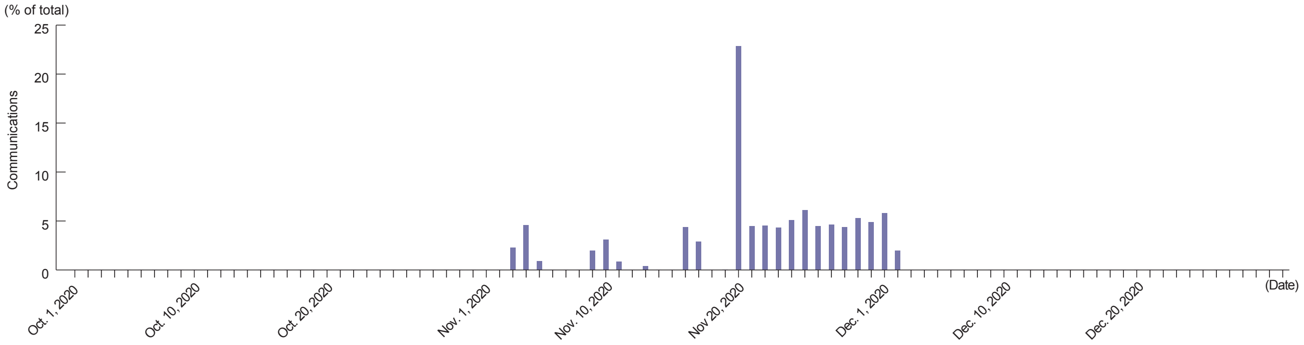
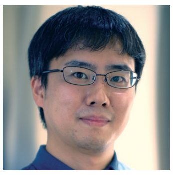
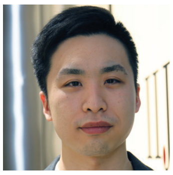


Figure 6: Communications with C&C Servers by IcedID (Oct.–Dec. 2020)

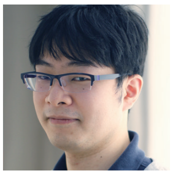


Hiroyuki Kamogawa
Security Operations Center, Security Business Department, Advanced Security Division, IIJ

Satoshi Kobayashi
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