TLP:AMBER

JPCERT/CC Monthly Report January 2021

February 1, 2021

JPCERT Coordination Center

Contents

1. Topics for this month

2. Open Source News in Japan

3. Incident Handling Statistics

4. Open Source News in East Asia

TLP: AMBER

1. Topics for this month

<TOPIC 1> Emotet observation, EmoCheck v2 and takedown

Confirming on December 21, 2020 that emails leading to Emotet infection were distributed,　JPCERT/CC released CyberNewsFlash to call attention the next day. In January 2021, the emails were still observed, and some of them contained Japanese subject line and texts related to COVID-19. On January 27, 2021, JPCERT/CC released EmoCheck v2.0 an Emotet infrastructure detection tool. On the same day, takedown of Emotet was reported.

<TOPIC 2> (3) Blog posts on tools and malware used by Lazarus

On January 19, 2021, JPCERT/CC published a blog entitled “Commonly Known Tools Used by Lazarus” to introduce some of the tools used by Lazarus attack group, a.k.a. Hidden Cobra　when they collect information and spread the infection. On January 26, JPCERT/CC also published “Operation Dream Job by Lazarus” to share its analysis on Torisma and LCPDot, the two types of malware used by the group.

Open Source News in Japan

JPCERT Coordination Center
Early Warning Group
ew-info@jpcert.or.jp

2. Open Source News in Japan - Summary

	Malware
1	Emotet observation, EmoCheck v2 and takedown
2	Blog posts on tools and malware used by Lazarus

	Phishing
3	Fake emails disguised as MIC's information on COVID-19

	Business
4	Salesforce warned about inappropriate setting for guest users
5	NISC published alert regarding the teleworking

2. Open Source News in Japan

(1) Emotet observation, EmoCheck v2 and takedown

[Summary]

Confirming on December 21, 2020 that emails leading to Emotet infection were distributed, JPCERT/CC released CyberNewsFlash to call attention the next day. In January 2021, the emails were still observed, and some of them contained Japanese subject line and texts related to COVID-19. On January 27, 2021, JPCERT/CC released EmoCheck v2.0 an Emotet infrastructure detection tool. On the same day, takedown of Emotet was reported.

[References] (English)

https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

[Sources] (Japanese)

https://www.jpcert.or.jp/newsflash/2020122201.html
https://twitter.com/IPA_anshin/status/1352513186625331200
https://twitter.com/jpcert_ac/status/1354257487390679042

2. Open Source News in Japan

(2) Salesforce warned about inappropriate setting for guest users

[Summary]

On December 25, 2020, Salesforce.com Co., Ltd. announced that its customers who used some of its products had reported possible information leakage cases. These cases allegedly had been caused by inappropriate setting for guest users. On February 1, the company released information and called for more cautions again as more companies publicly spoke about their possible information leakage.

[References] (English)

[Sources] (Japanese)

https://www.salesforce.com/jp/company/news-press/press-releases/2020/12/201225/

2. Open Source News in Japan

(3) Blog posts on tools and malware used by Lazarus

[Summary]

On January 19, 2021, JPCERT/CC published a blog entitled “Commonly Known Tools Used by Lazarus” to introduce some of the tools used by Lazarus attack group, a.k.a. Hidden Cobra when they collect information and spread the infection. On January 26, JPCERT/CC also published “Operation Dream Job by Lazarus” to share its analysis on Torisma and LCPDot, the two types of malware used by the group.

[References] (English)

https://blogs.jpcert.or.jp/en/2021/01/Lazarus_tools.html
https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html

[Sources] (Japanese)

2. Open Source News in Japan

(4) Fake emails disguised as MIC’s information on COVID-19

[Summary]

On January 8, 2021, JC3 released a security alert that fake emails regarding special cash benefits as COVID-19 countermeasures had been distributed. The emails were disguised as if they were sent from the Ministry of Internal Affairs and Communications, and such emails have been observed since the day when the state of emergency was declared in 1 metropolitan area and 3 prefectures in Japan. Multiple organizations including JC3 published information and called for caution. Similar emails were also observed previously in October 2020.

[References] (English)

[Sources] (Japanese)

https://www.jc3.or.jp/topics/kyuhukin_phishing.html

2. Open Source News in Japan

(5) NISC published alert regarding the teleworking

[Summary]

On January 8, 2021, NISC Japan published “Alert regarding the implementation of teleworking under the State of Emergency (January 7, 2021),” following the state of emergency for Tokyo and three prefectures (Chiba, Saitama, and Kanagawa) in response to the spread of COVID-19. This state of emergency aims to reduce the number of employees who commute to their office by 70%, promoting teleworking. The alert published by NISC is intended to strongly raise awareness of security measures during teleworking, as the risk of teleworking-related cyber attacks and support fraud would increase.

[References] (English)

[Sources] (Japanese)

https://www.nisc.go.jp/press/pdf/20210108_caution_press.pdf

Incident Handling Statistics

JPCERT Coordination Center
Incident Response Group
info@jpcert.or.jp

TLP: AMBER

3. Incident Handling Statistics

- This section introduces statistics on incidents that were reported to/handled by JPCERT/CC during 1-31 January. Please note that the numbers are provisional. The finalized data will be provided on JPCERT/CC Incident Handling Quarterly Report.

http://www.jpcert.or.jp/english/doc/reports.html

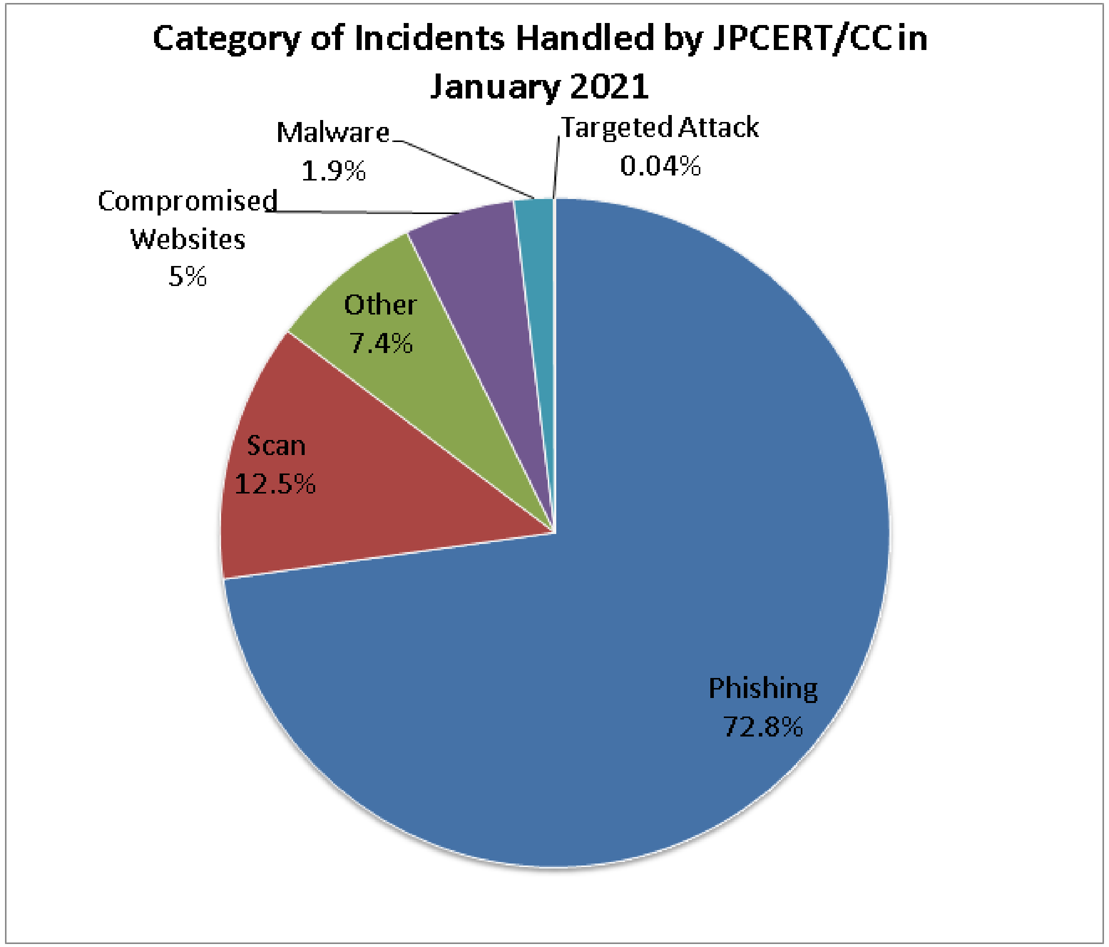
- The following table shows the number of incident reports sent to JPCERT/CC during the month and the comparison with the previous month.

	Dec, 2020	Jan, 2021	Comparison
From Domestic	3601	3102	-13.9%
From Overseas	1263	1135	-10.1%
Total	4864	4237	-12.9%

3. Incident Handling Statistics

- Incidents reported to JPCERT/CC during the month are categorized as follows:

	Jan, 2021
Phishing	1775
Compromised websites	130
Malware	47
Scan	305
DoS	0
ICS	0
Targeted Attack	1
Other	181
Total	2439



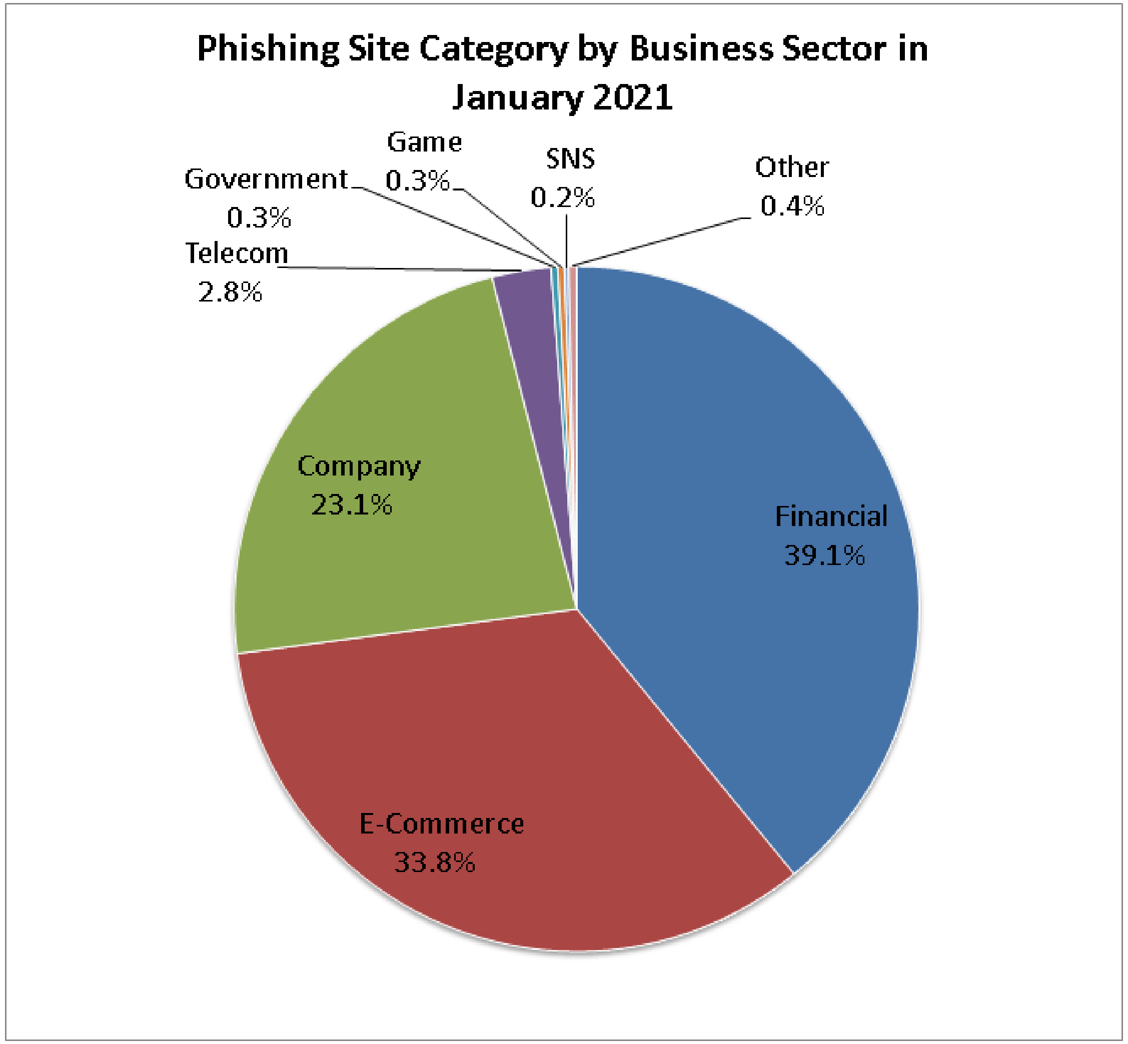
Category of Incidents Handled by JPCERT/CC in January 2021

TLP: AMBER

3. Incident Handling Statistics

- Phishing sites handled by JPCERT/CC during the month are as follows:

Sector	Domestic	Overseas	Total
E-Commerce	3	533	536
Company	323	43	366
Financial	573	46	619
Telecom	43	1	44
SNS	0	3	3
Game	5	0	5
Academic	1	0	1
Government	1	4	5
Portal	0	0	0
Other	2	4	6
Sector Total	951	634	1585
Unknown	* Websites reported as phishing but already inactive		190
Phishing Total	* Sector Total + Unknown		1775



Open Source News in East Asia

JPCERT Coordination Center
Early Warning Group
ew-info@jpcert.or.jp

4. Open Source News in East Asia

China

APT Group Activity Summary Report for 2020

https[:]//ti.qianxin[.]com/uploads/2021/01/21/3df9fce0e9abf71265f88d45188f8fec.pdf

On January 21, 2021, Qianxin published a report summarizing the activities of APT groups in 2020. This report summarizes not only APT attacks targeting China but also overseas attack trends.

Attack activity of mining malware TOPMiner

https[:]//mp.weixin.qq[.]com/s/9U1V0dkL0AUIPYZWmNSjpA

On January 4, 2021, Tencent's security team released information on the attack activity in which mining malware was used. The company named this activity TOPMiner after Top, the malware used. According to the company's estimate, TOPMiner attackers control about 15,000 servers for their cryptocurrency mining. TOPMiner compromises system through SSH brute force attack and downloads malicious shell scripts, and then the shell script launches mining malware to perform mining. During the analysis, several other types of malware were observed including backdoor malware with remote command execution function and Trojan horse malware kaiji with DDoS attack function.

Public opinion for the draft on Internet Information Service Management Law

https://www.reuters.com/article/technologyNews/idUSKBN29D0GC

On January 8, 2021, the CAC released a revised draft of the "Internet Information Service Management Law," which was drafted with MIIT and MPS. The draft is open for public consultation until Feb 7 and aims to promote the healthy and orderly development of Internet information services.

Korea

Phishing site disguised as messenger program and distribute malicious code

https[:]//asec.ahnlab[.]com/ko/19439/

On December 31, 2020, AhnLab released information about a fake messenger program that could lead to Quasar RAT infections. According to the company, phishing sites disguised as KakaoTalk have been confirmed, and it has a download link of a malicious installation file, which ultimately leads to Quasar RAT infection. The company also found sites which were intended to disseminate malicious code using disguised download page of commercial groupware.

CLOP Ransomware Analysis Report

https[:]//asec.ahnlab[.]com/en/19542/

On January 5, 2021, AhnLab released an analysis report of CLOP ransomware. The ransomware attacked South Korean distribution giant E-Land Group in November 2020. This report summarizes CLOP ransomware's infection routes, attack targets, attack processes, and changes made so far. CLOP ransomware targets companies that operate Active Directory (AD), steals administrator privileges on AD servers, and attacks many systems within the companies. Not only infection with ransomware but also information leak may occur. The targets of the attack are wide-ranged across various industries, including public institutions, education, broadcasting, finance, manufacturing, IT, distribution, and telecommunications carriers. Manufacturing is the most affected (53%), and it is followed by finance (15%), information services (11%) and wholesale and retail (9%).

Spear phishing attack disguised as COVID-19 related application

https[:]//blog.alyac[.]co.kr/3536

On January 19, 2021, ESTsecurity released information about an attack that distributed fraudulent files disguised as an application for recipient of COVID-19-related donation. Emails with a malicious file attached were sent to a specific private sector association in the country during the year-end adjustment season. The email comes with a zip file containing documents titled "donation certificate (PDF file)," "receipt issuance application (xlsb file)," and the like. When the xlsb file is opened and its "Enable Content" button is clicked, a malicious script is executed, and it connects to the FTP server specified by the attacker. As a result, additional malicious commands may be executed. According to ESTsecurity, the malicious files used in this attack are similar to those used in another attack by APT group Thallium (also known as Kimsuky).

JPCERT Coordination Center

- Web: https://www.jpcert.or.jp/english/

Global Coordination Division

- Email: global-cc@jpcert.or.jp

Incident Reports

- Email: info@jpcert.or.jp
- Web: https://www.jpcert.or.jp/english/ir/form.html