

# JSAC 2022 -Day 1- - JPCERT/CC Eyes

By JPCERT/CC

Published: 2022-03-21 · Archived: 2026-04-05 17:52:34 UTC

- [JSAC](#)

JPCERT/CC held [JSAC2022](#) online on January 27, 2022. The purpose of this conference is to raise the knowledge and technical level of security analysts in Japan, and we aimed to bring them together in one place where they can share technical knowledge related to incident analysis and response. This year was the fifth time the conference was held. 9 presentations and 2 workshops, selected from 18 CFP and CFW submissions, were presented.

Unlike last year, the event had a single track. Day 1 was Conference Day, and Day 2 was Workshop Day. The question-and-answer session was held on Slack, and speakers and the audience lively exchanged their opinions. Most of the presentation slides are available on JPCERT/CC website. This article reports on Day 1, and [Day 2](#) will be covered by our next blog post.

## Opening Talk: Looking Back on the Incidents in 2021

**Speaker: Takayoshi Shiigi (JPCERT/CC)**

[Slides \(English\)](#)

[Video](#)

In the opening talk, Takayoshi discussed some incidents that JPCERT/CC confirmed in 2021 as well as its repositories published in GitHub.

LODEINFO and Gh0stTimes were used in targeted attacks. LODEINFO was updated frequently, even in 2021. Since version 0.4.x, the launch method has been changed to LOLBAS (Living Off The Land Binaries And Scripts). Gh0stTimes is used by an attack group called BlackTech and equipped with a panel called Times. The code and functions are similar to the malware Gh0stRAT, which is also used by BlackTech.

By referring to the information published by JPCERT/CC, the speaker mentioned the restarted Emotet campaign and human-operated ransomware attacks as 2021's features in widespread attacks.

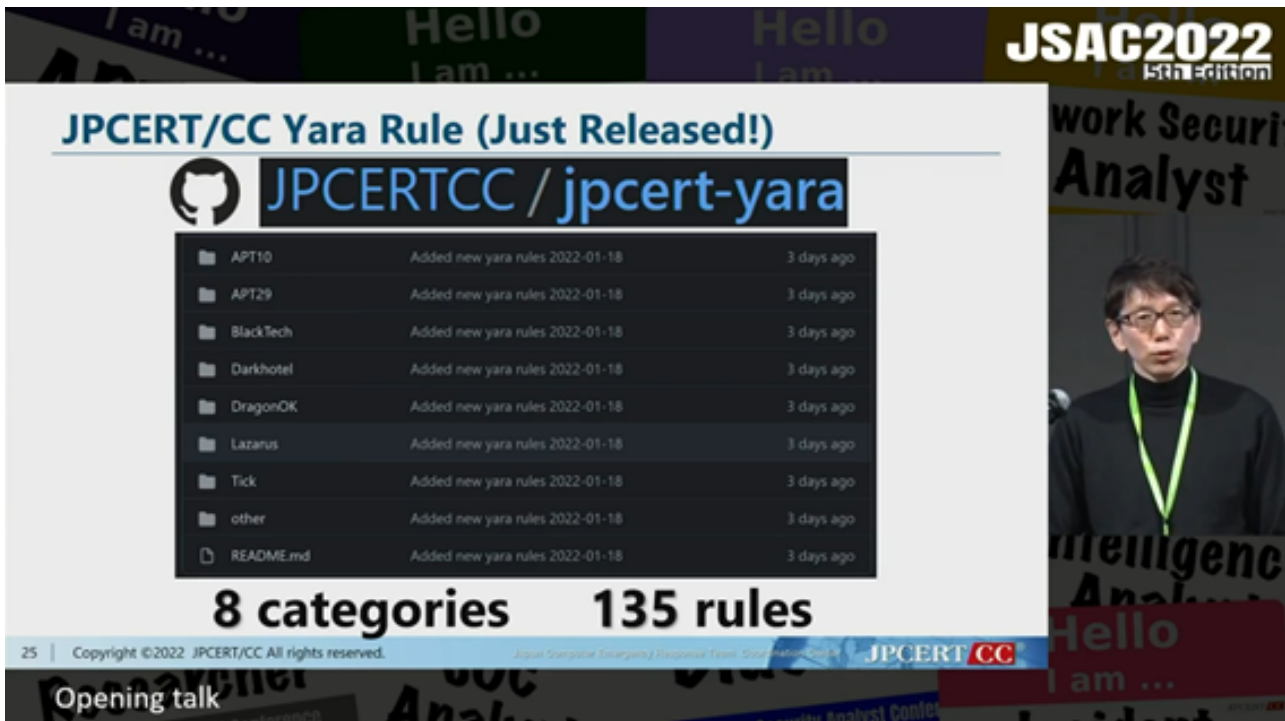
Some of JPCERT/CC's public projects on GitHub were introduced at the end of the talk. YARA rules and the IoC of the redirected domain used for lucky visitor scam are available in the websites below.

**JPCERT/CC YARA rules**

<https://github.com/JPCERTCC/jpcert-yara>

**Lucky Visitor Scam IoCs**

<https://github.com/JPCERTCC/lucky-visitor-scam-ioc>



## Research on Unique Adversaries and its Attack Tools Targeting Widespread CMS in Japan

Speakers: Ryosuke Tsuji, Naoaki Nishibe (LAC Co., Ltd.)

[Slides \(Japanese\)](#)

[Video](#)

Ryosuke and Naoaki described some features of the attack exploiting CVE-2021-20837, the vulnerability in Movable Type (a Contents Management System) published in October 2021, and the functions of the tools used in the attack.

According to the presentation, there was about a week between the release of the PoC for the vulnerability and the launch of the attack. Another aspect of the attack was that Movable Type was used more concentratedly in Japan than in other regions, which resulted in the delay in the actions by foreign security vendors. Japanese local vendors therefore proactively collected and verified information as well as alerted users and provide measures. Next, the analysis of the following tools used in the vulnerability exploit was presented.

- FoxEx-Shell
- FoxWSO

FoxWSO, downloaded by FoxEx-Shell, is a modified WSO (WebShell by Orb) which has features specific to FoxWSO compared to known WSOs. The speakers also added that AnonymousFox, an organisation allegedly selling FoxWSO, may have been involved in the attack as there were several posts from them offering the tool on Telegram.

**タイムラインと振り返り**

| 日付      | できごと   | 振り返り   |
|---------|--|--|
| 10月 20日 | Movable Typeの脆弱性情報(CVE-2021-20837)および修正ソフトウェア公開        | このあたりで対策できていれば万全(ユーザ側)   |
| 22日     | PowerCMSの脆弱性情報および修正ソフトウェア公開                            |  |
| 26日頃    | 攻撃コード(PoC)が一般に公開                                       | 日本のSOCの頑張りとどころ   |
| 27日     | 脆弱性の有無を調査する通信を観測                                       |  |
| 11月 上旬  | セキュリティ製品Aが対応シグネチャリリース                                  | <ul style="list-style-type: none"> <li>・稼働ホストを狙い撃ちされていた可能性のある期間</li> <li>・攻撃件数が少なかったため、攻撃されても都度影響調査の余地があった</li> </ul>    |
| 1日      | 悪質なバックドアの設置(侵害)を試みる通信を観測                               |  |
|         | 脆弱な環境においてインシデント通報(以降、複数環境で継続)                          |  |
| 中旬      | セキュリティ製品Bが対応シグネチャリリース                                  | <ul style="list-style-type: none"> <li>・攻撃件数(攻撃元および宛先)が極端に増加し、取捨がつかなくなる</li> <li>・運良く攻撃者に捕捉されていなかったホストも攻撃を受ける</li> </ul> |
| 17日     | 攻撃観測数が極端に増加  |  |
| 25日     | PowerCMSの脆弱性にCVE-2021-20850が採番                         |  |
| 12月 上旬  | セキュリティ製品Cが対応シグネチャリリース                                  |  |
| 16日     | Movable TypeおよびPowerCMSにおいて修正が不十分であったとして追加の修正ソフトウェアが公開 |  |

日本にシェアが集中するCMSを狙う特異な攻撃者と侵害ツールの調査

## ma2tl: macOS Forensics Timeline Generator Using mac\_apt Analysis Results

Speaker: Minoru Kobayashi (Internet Initiative Japan Inc.)

[Slides \(English\)](#)

[Video](#)

Minoru presented a tool called ma2tl (mac\_apt to timeline), which he has developed. It automates the creation of a forensic timeline based on the results of mac\_apt, an open source software for forensic analysis of macOS devices.

In order to perform forensic analysis of macOS devices, it is necessary to create a timeline that provides clues for the investigation. The background of developing the tool was the fact that there was no tool available with sufficient functionality. The speaker also added that mac\_apt is the suitable tool for creating macOS timeline because it is constantly maintained to keep up with the macOS updates, which frequently change the file names and paths.

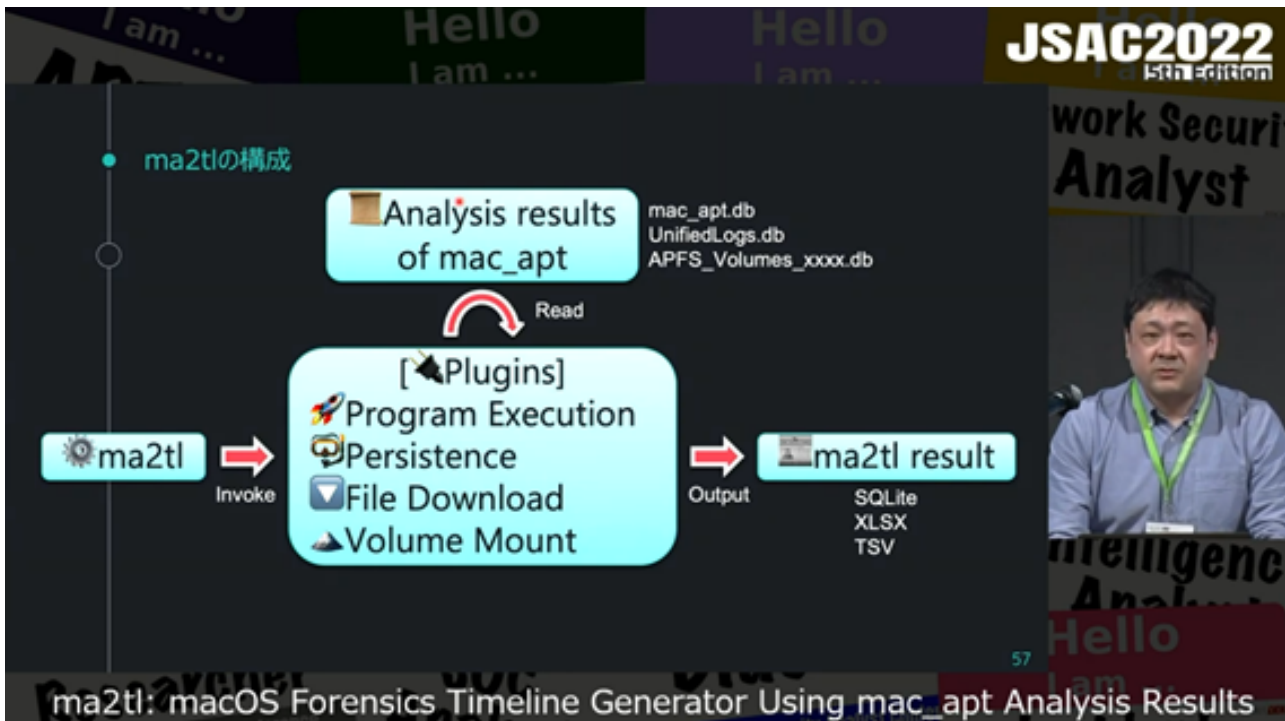
ma2tl helps to create a timeline of the following activities from databases such as mac\_apt.db and UnifiedLogs.db, where the analysis results of mac\_apt are stored.

- Persistence setting status
- Program execution history
- Volume (USB thumb drives or disk images) mount
- File Download

To conclude, the speaker demonstrated ma2tl facilitating forensic analysis of a device infected by the malware.

**ma2tl**

<https://github.com/mnrkbys/ma2tl>



## The Struggle Against Domestic Malicious Proxy Services

Speaker: Yuji Ino (Recruit Holdings Co.,Ltd.)

[Slides \(Japanese\)](#)

Yuji presented on his analysis results of the IP addresses of Japanese Residential IP Proxies (RESIPs), which are exploited in cyber attacks.

He first mentioned that if an attacker abuses RESIPs, which are proxies that provide traffic relay using residential network hosts, they can avoid detection of unauthorized access by setting the access source to Japan when conducting a cyber attack from outside Japan via Japanese RESIPs. Next, he shared and explained the trend of abused Japanese RESIPs, mainly from the following perspectives:

- Percentage of survival period for each IP address
- Active rate (number of days with suspicious activity/survival period) of IP addresses with long-term activity observed
- Ratio of IP addresses per carrier
- Trends in access by unique users to each IP address

Finally, he explained the verification results of fraud detection (spoofed login, unauthorized use of stolen cards, fraud). He compared the data collected in this research and those of fraud cases, and as a result, he found the followings:

- Simple IP address matching causes many false positives.
- False positives can be reduced to some extent by comparing the data with the time of malicious activities.
- It is useful for determining whether an attacker uses Residential IP Proxy.

## An Order of Magnitude Update

## **Speakers: Rintaro Koike, Hajime Takai, Nobuyuki Amakasu (NTT Security Japan)**

[Slides \(Japanese\)](#)

Rintaro and Hajime gave an update on an exploit kit called Magnitude Exploit Kit observed in 2021 and the analysis results of ransomware called Magniber, which is executed by this kit.

The kit has been frequently observed since around October 2021 in Japan. The speakers remarked that the exploitation of new vulnerabilities (e.g., CVE-2021-40444) and the distribution of Magniber through social engineering were the features of 2021.

Next, a case study of the Magniber infection using Magnitude Exploit Kit and social engineering was described.

When the kit was executed, a window asking for update appeared on Microsoft Edge. The malware was transmitted by downloading and installing AppX file (Windows Application Package) with a valid digital signature. The speakers also noted that Magniber has been updated to remove unnecessary features.

In the end, a few methods for investigating and detecting the Magnitude Exploit Kit and Magniber were presented based on their distinctive features.

## **Emotet vs EmoCheck: The Battle Against Emotet Developers**

**Speakers: Tomoaki Tani (NTT Social Information Laboratories), Kota Kino, Ken Sajo (JPCERT/CC Incident Response Group)**

[Slides \(Japanese\)](#)

[Video](#)

Tomoaki and Kota presented on the changes after Emotet restarted its activity and EmoCheck, a tool to detect Emotet processes.

One of the changes after Emotet restarted its activity is that the malware now directly distributes Cobalt Strike beacon. It is necessary to pay attention because this tool can lead to ransomware infection just like before.

Regarding EmoCheck, they said that the main purpose of developing it was to provide users with a tool to easily check for Emotet infection. They also explained the change in detection logic of EmoCheck. The first detection logic reproduced Emotet's process, which selects multiple keywords for drive serials and set file names. Then, the logic was repeatedly updated as Emotet renewed its version and changed its processing logic.

They also explained about the obfuscation process implemented in EmoCheck to prevent Emotet developers from bypassing the detection logic of EmoCheck. They said that the latest version of EmoCheck (version 2.0) uses obfuscation methods same as or equivalent to those Emotet uses as follows.

- String Obfuscation
- Mixed Boolean Arithmetic
- Control Flow Flattening
- Win32API Hashing Obfuscation
- Function Argument Randomization

### **EmoCheck**

<https://github.com/JPCERTCC/EmoCheck>



## Crazy Journey: Evolution of Smoky Camouflage

Speakers: Ryuichi Tanabe, Yuta Sawabe (NTT Security Japan)

[Slides \(Japanese\)](#)

[Video](#)

Ryuichi and Yuta presented on an attack campaign called Malsmoke and the investigation and detection methods for the campaign.

They said that the Japanese users are one of the main targets of Malsmoke. The campaign has features such as using malvertising to infect them with Zloader malware eventually, and its attack methods have been frequently updated with new attack techniques.

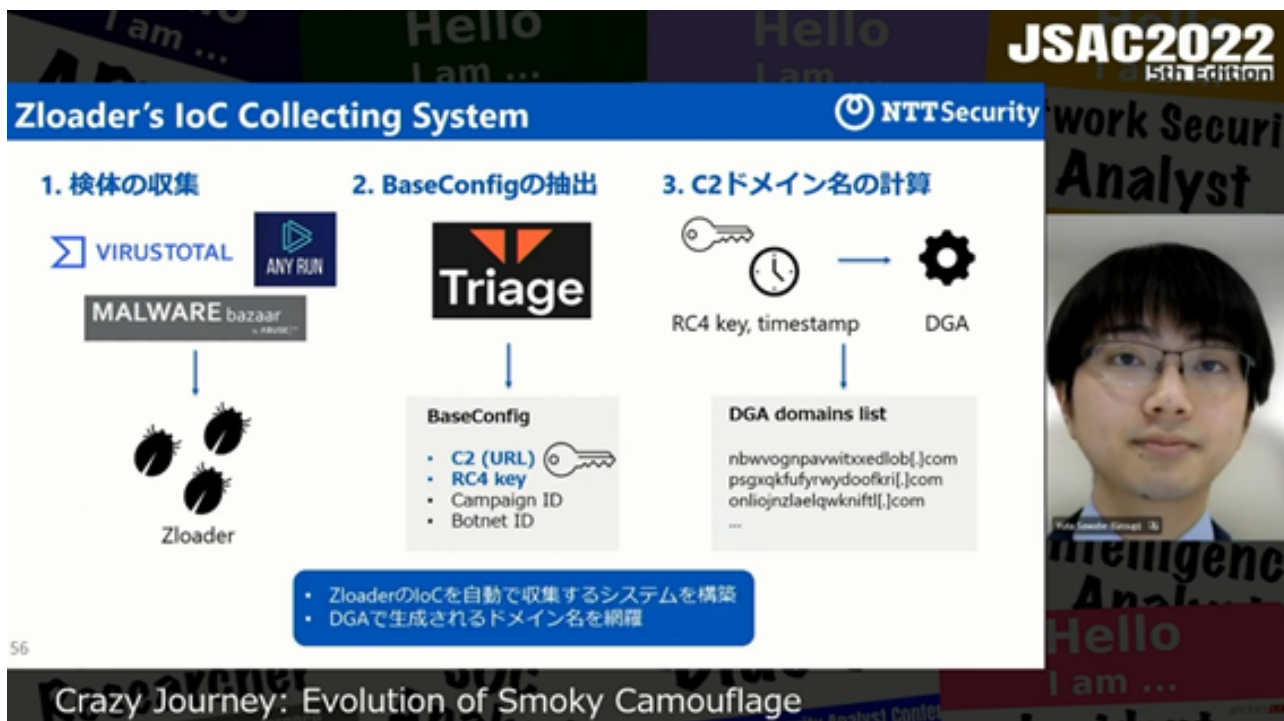
Malvertising used in this campaign is characterized by the landing page that appears after advertisement page displays a fake Java plug-in installation screen in the language of the target's country based on the geographic information of the IP address.

In addition, they said that the following campaigns are probably conducted by the same attack group since they are similar to Malsmoke in that they use malvertising and geographic information of IP address, etc.

- Seamless
- PseudoGate

They also explained the detection method of Malsmoke. They focused on the fact that Zloader's C2 server domains are generated by DGA (Domain Generation Algorithm), which does not change. They first collected Zloader samples from VirusTotal and other sources and then extracted Zloader configuration files with Triage, an online sandbox.

Based on the information, they explained how DGA calculates the C2 server domains.



## LuoYu: espionage in 2021 targeting Japan with new WinDealer

Speakers: Leon Chang (TeamT5), Yusuke Niwa (Itochu), Suguru Ishimaru (Kaspersky)

[Slides \(English\)](#)

[Video](#)

Leon and Yusuke presented on the updated information on LuoYu, a Chinese APT group on which Leon presented at [JSAC2021](#).

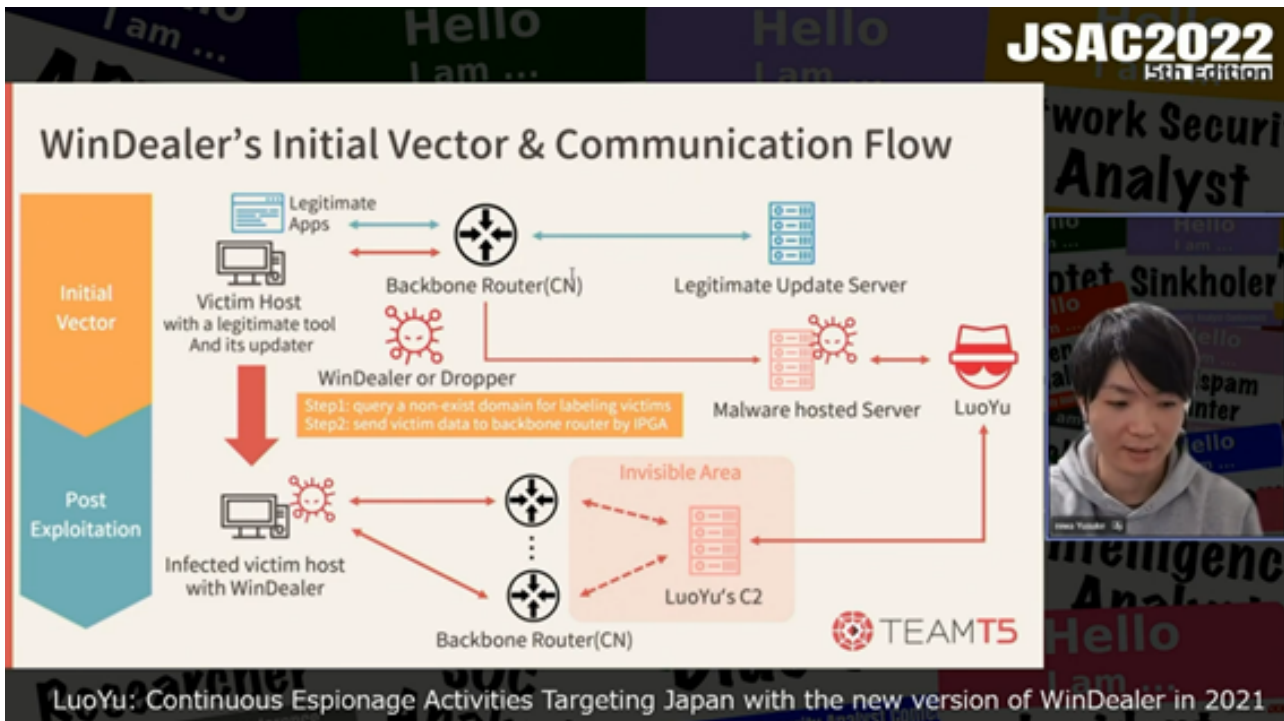
They said LuoYu have newly used the following malware since JSAC2021:

- Malware: XDealer, ShadowPad, PlugX

In addition, the following industries and areas have been newly targeted:

- Industries: Finance, Foreign Affairs, Military, Communications, Logistics
- Areas: Russia, United States, Czech Republic, Australia, Germany

They also explained the features of WinDealer, a type of malware LuoYu uses. WinDealer converts information for identifying each device, such as user name, into a format similar to an IP address before saving it in the registry. When communicating with the C2 server, the malware accesses a domain or URL that does not exist, and a part of the response data (NXDOMAIN) is used for a label that identifies WinDealer-infected devices. The label is used for a custom header when sending data to the C2 server. In addition, WinDealer uses IPGA (IP Generation Algorithm) to generate a random IP address from a specified range for C2 server to avoid tracking. They also introduced an incident case of LuoYu. In this case, a legitimate application such as TIM (a communication tool) downloaded WinDealer, and then the device got infected with it. Finally, they described the results of threat analysis of the campaign using frameworks such as Diamond Model and MITRE ATT&CK.



LuoYu: Continuous Espionage Activities Targeting Japan with the new version of WinDealer in 2021

## Ambiguously Black: The Current State of Earth Hundun's Arsenal

Speaker: Hiroaki Hara (TrendMicro)

[Slides \(English\)](#)

[Video](#)

Hiroaki presented on the attack operations observed in 2021 which were conducted by an attack group called Earth Hundun.

He explained about the attack campaigns which used the following malware. The features, attack methods, and attack infrastructure of each type of malware were covered.

- Campaign 1: LAMICE, BUSYICE (a.k.a Flagpro), etc.
- Campaign 2: SLEFMAKE, SPIDERPIG

He first presented Campaign 1. The attack starts with a phishing email with the malware LAMICE attached. LAMICE drops BUSYICE and other type of malware, which then downloads new backdoors. He found that the way LAMICE generates a file name for the malware it drops is identical to that of Earth Hundun's TTP. In addition, he found connections and overlaps between the attack infrastructure of malware used by Earth Hundun, such as Gh0stTimes, and that of BUSYICE. For these reasons, he associated Campaign 1 with Earth Hundun.

He next presented Campaign 2. This campaign drops SELFMAKE through ProxyLogon, a vulnerability in Microsoft Exchange Server or via malware bundled installer. It eventually executes SPIDERPIG on memory. He found that the format of the Mutex strings created by SPIDERPIG and BUSYICE are similar, and he also observed a case where SPIDERPIG was dropped from LAMICE in November 2021. For these reasons, he concluded that the attack groups of Campaign 1 and 2 are probably the same and therefore that Campaign 2 is Earth Hundun.

Finally, he explained that in the future, it will be important to continuously disclose the process of attribution and

redefine attack groups in order to keep up with attacker groups, which keep changing by sharing attack tools with other groups.

| #             | Campaign #1   | Campaign #2   |
|---------------|---|---|
| Timeline      | Active since at least 2020/09   | Active since at least 2021/03   |
| Victims       | <ul style="list-style-type: none"> <li>Media, Telecommunication, Defense and Academic in Japan</li> <li>Individual users</li> </ul>   | <ul style="list-style-type: none"> <li>Possibly unspecified companies / organizations / regions</li> </ul>                                  |
| Attack Vector | <ul style="list-style-type: none"> <li>Email</li> </ul>   | <ul style="list-style-type: none"> <li>Exploit Public-Facing Application</li> <li>Malware Bundled Installer</li> </ul>                      |
| Tools         | <ul style="list-style-type: none"> <li>Trojan.W97M.LAMICE</li> <li>Backdoor.Win32.BUSYICE</li> <li>Backdoor.Win32.BTSDOOR</li> <li>Backdoor.MSIL.TELESWORD</li> <li>Backdoor.Win32.DELTABEEF</li> </ul> | <ul style="list-style-type: none"> <li>Trojan.Win64.SELFMAKE</li> <li>Backdoor.Win32.SPIDERPIG</li> <li>Backdoor.Win64.SPIDERPIG</li> </ul> |

© 2022 Trend Micro Inc.

TREND MICRO

Ambiguously Black: The Current State of Earth Hundun's Arsenal

### What we can do to the chaotic A41APT campaign

**Speakers: Gen Yanagishita (Macnica Networks Corp), Kiyotaka Tamada, Yu Nakatsuru (SecureWorks), Suguru Ishimaru (Kaspersky)**

[Slides \(English\)](#)

[Video](#)

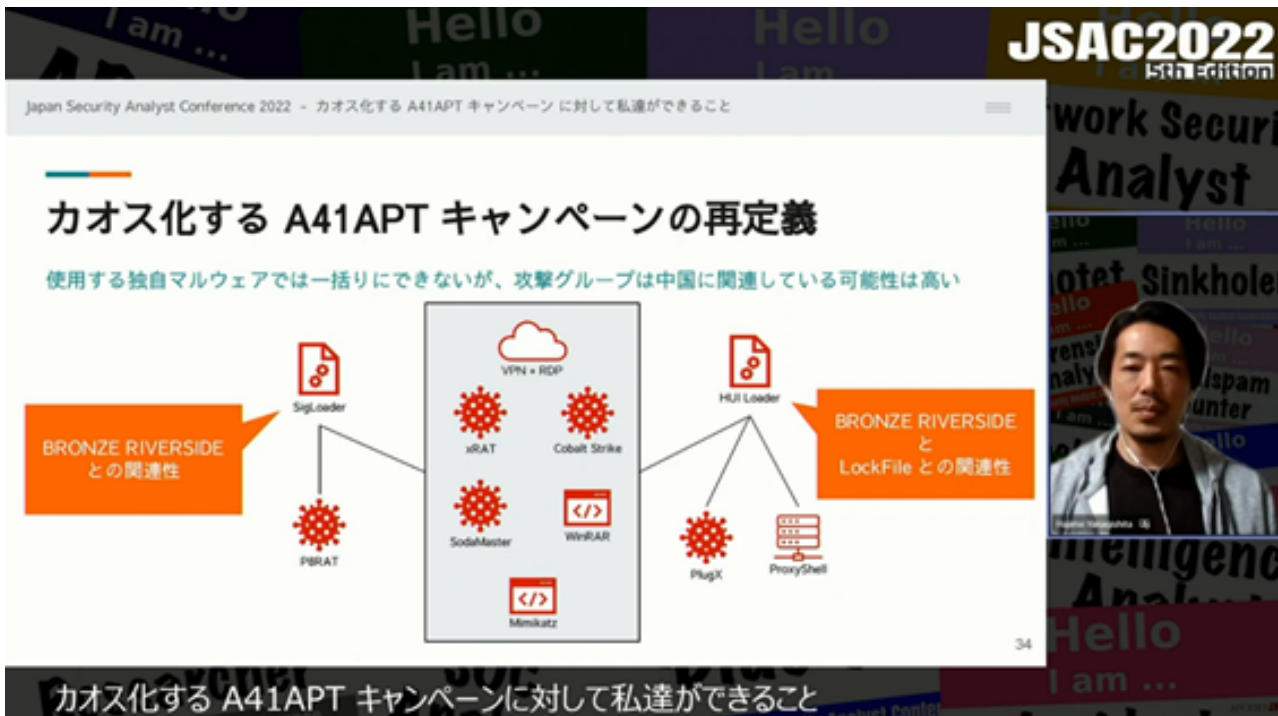
Kiyotaka and Gen presented on the updates of A41APT, which they presented in [JSAC2021](#).

They first explained that the decryption process and commands of SigLoader and SoadMaster, the malware A41APT has long used, were updated. The following new attack methods that they confirmed after JSAC2021 were also introduced:

- Exploit Jackpot Webshell
- Penetration through exploiting ProxyShell (Microsoft Exchange Server vulnerability)
- Exploit HUI Loader

Next, they explained about HUI Loader. It loads SoadMaster by using an attack technique called DLL side-loading on legitimate files. HUI Loader and SoadMaster stores the DLL files they load in a different folder. Regarding the connection between the A41APT campaign and attack groups, they discussed the possibility of multiple attack groups involved, based on the fact that security researchers overseas identified HUI Loader in LockFile ransomware and BRONZE RIVERSIDE (a.k.a. APT10) incidents.

Finally, he said that it is important to understand the status of security measures in one's own and related organizations because since 2020, incidents are more likely to occur in places with weak security measures.



### In closing

In this article, we reported on the 9 presentations on Day 1 of JSAC 2022. In our next blog post, we will cover the workshops on [Day 2](#).

Shohei Iwasaki  
(Translated by Takumi Nakano and Masa Toyama)



[JPCERT/CC](#)

Please use the below contact form for any inquiries about the article.

### Related articles



[JSAC2026 -Workshop/Lightning Talk Session/Panel Discussion-](#)



•

[JSAC2026 -Day 2-](#)



•

[JSAC2026 -Day 1-](#)



•

[ICS Security Conference 2025](#)



•

[JSAC2025 -Workshop & Lightning Talk-](#)

Source: <https://blogs.jp-cert.or.jp/en/2022/03/jsac2022report1.html>