Cyber Security Reports

2023.07

NTT Security Japan Inc.

OSINT Monitoring Team, Consulting Services Department

Information Asset Classification: Public

NTT Security Holdings

Contents

About this report

This report summarizes three topics that are considered to be particularly important among various information security incidents and events that occurred during July 2023 and the changes in the environment surrounding them. The summary of each topic is as follows.

CHAPTER 1
“Ransomware Attack Halts Nagoya Port Operations”

- The port of Nagoya, which handles the largest amount of cargo in Japan, experienced a critical system failure that caused the port to shut down due to a ransomware attack, resulting in a logistical outage that prevented containers from being loaded and unloaded for several days.
- The attack on the port is believed to have been carried out by the LockBit ransomware group, which has caused significant damage worldwide.
- The cyberattack on logistics could also have an impact on the Japanese economy, and it is hoped that Japan will take the lead in preventing crimes committed by such ransomware groups.

CHAPTER 2
“US agencies' Outlook email accounts hacked by Chinese attackers”

- On July 12, Microsoft disclosed that the Outlook email accounts of about 25 organizations worldwide, including at least 2 U.S. government agencies, had been hacked by suspected Chinese hackers.
- In its earlier announcements, Microsoft has not disclosed how the account signing key that was used to launch the attack was stolen and has faced criticism from experts for using language that didn’t acknowledge the vulnerability.
- When high security is required, even for major cloud services, users need to do detailed log monitoring separately rather than leaving it to themselves.

CHAPTER 3
"Increase in APT Attacks Using USB Memories"

- Many cases of APT attacks involving countries such as China and Russia have been confirmed, in which USB thumb drives are used to spread malware inside networks.
- These attacks are thought to target critical systems that are isolated from the network and are also used to deliver malware into the system, spread the infection from the infected system to other systems, and take out sensitive information.
- Any organization that uses a USB thumb drive, whether brought in from outside or for internal use only, must guard against the possibility of a malware infection and take action.

1. Ransomware attack halts Nagoya Port operations

1.1. Overview

On July 4, 2023, a serious system failure occurred in the Nagoya United Terminal System (NUTS) which is used to manage cargo and equipment at the Port of Nagoya, Japan. The Nagoya Harbor Transportation Association, which manages NUTS, disclosed that the cause of the system failure was a ransomware infection, and the Aichi Prefectural Police are investigating the alleged violation of the Unauthorized Access Control Law. [*]1

The Port of Nagoya, the largest in Japan in terms of cargo volume, export value, trade surplus, users, and land area, was unable to move containers in and out of the port for about two and a half days, causing chaos at the site. [*]2

Figure 1 View of Nagoya Port [*]3

1.2. History of the system failure

The NUTS system, which is used at all five container terminals in Nagoya Port, is used to centrally manage the loading and unloading of containers. The new system has been in full operation since January 2023. With this system, Nagoya Port can query the status of the placement of a large number of containers in real time and quickly compute a plan for the loading and unloading of containers by trucks, thereby facilitating efficient operations.
On the morning of July 4, when the failure occurred, an employee of the Nagoya Harbor Transportation Association noticed a system failure and restarted the failed server. This did not restore operations. Instead, a printer started running, and about 100 threatening messages in English were printed, with "LockBit Black Ransomware" at the beginning of the message, notifying that a ransomware infection had taken place. [*]4 Data on all servers was encrypted, and the association disclosed the ransomware infection at noon on July 5 after consulting the police. [*]5

The Nagoya Harbor Transportation Association restored the system using backup data from before the infection, but it took a long time to recover the system. One of the reasons for the difficulty was that ransomware was detected on the backup server and needed to be cleaned, and another system failure occurred further delaying recovery. [*]6
As for the attackers who made the threat, the association said the threat did not include a ransom amount and it did not contact the attackers. As of August 14, the release of the theft information on the disclosure site, which is common in ransomware attacks, has not been confirmed.

A simple timeline from the occurrence of a system failure to recovery is as follows: [*]7

[Time Series]	
· Around 06:30 on July 4	Confirmed that the NUTS system has stopped operating. Container loading and unloading stopped on the same day.
· Around 12:00 on July 5	Nagoya Harbor Transportation Association announces system failure due to ransomware infection (first report)
· Around 07:15 on July 6	Restoration of backup data was completed. Another system failure occurred
· Around 14:15 on July 6	The system failure was resolved. Sequential container loading/unloading operation resumed.
· Around 18:15 on July 6	Resumption of operations at all terminals

1.3. Damage

Due to the suspension of NUTS due to the cyber attack, about 15000 containers could not be transported in and out of Nagoya Port over a period of 2 days, and the area around the port was jammed with waiting container trailers. [*]8 Even after container transportation resumed, the times of operation had to be extended from the usual times to allow for full recovery.
Although Nagoya Port handles many automotive parts, Toyota and its group companies say, "The production has not been affected because of the inventory." [*]9 [*]10
With regard to this issue, the government decided to compile security measures, and on July 31, the Ministry of Land, Infrastructure, Transport and Tourism held its first "Review Committee on Information Security Measures at Container Terminals." [*]11

1.4. About LockBit Ransomware

The attack is believed to be the work of one of the most active hacker groups, the **LockBit Ransomware Group (The following LockBit)**, which is made up of mostly Russian-speaking members. LockBit's top targets include finance, IT and manufacturing, and it has reportedly hit more than 2000 companies and other organizations and more than 15000 individuals worldwide. [*]12 This is the second time LockBit has attacked a port[*]13, the first being Lisbon in Portugal in December 2022.

1.5. VPN device may have been an entry point

The Nagoya Harbor Transportation Association uses FortiGate firewalls to provide VPN services, and it is suspected that the LockBit ransomware was sent through a FortiGate. VPN devices are known to be a major entry point for ransomware, and FortiGate users have also been hit hard by vulnerabilities in the past. The association, which had not applied fixes for the latest critical vulnerabilities, could have had some problems with its security operations. [*]14

1.6. Summary

The incident marked the first time in Japan that one of its critical infrastructure and logistics facilities was stopped by a cyberattack. This time, it was possible to recover the damage within a few days, but if the damage had been prolonged, it could have had a huge impact not only on the lives of ordinary citizens but also on the Japanese economy. Since it is not possible to prevent 100% of cyber attacks, we believe that giving appropriate punishment to those who commit such crimes/acts of terrorism would be effective in preventing the recurrence of such attacks. Unfortunately, it has been difficult to arrest people for ransomware attacks in Japan.

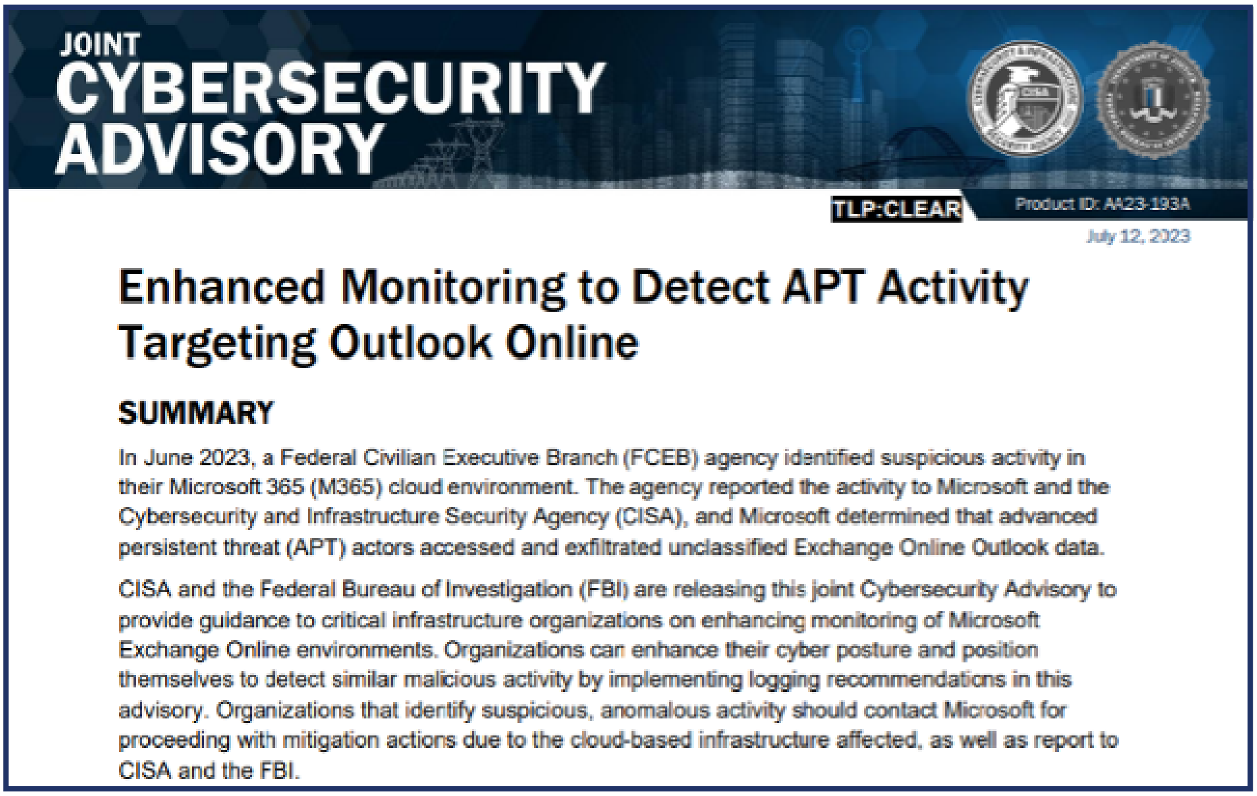
On the other hand, internationally, attacks on critical infrastructure are considered to constitute a violation of sovereignty, and there have been successful efforts to apprehend the perpetrators and close down the exposure sites. In the Colonial Pipeline incident, the US used diplomatic pressure to round up a Russian ransomware group. Since many of these groups are based in Russian-speaking countries, it may be difficult to crack down on the cybercrimes they are involved in at the moment, but we hope that Japan will take the lead in working with the international community to create a new framework that does not allow these criminals to go unchecked as we look to the end of the war in Ukraine.

2. US agencies' Outlook email accounts hacked by Chinese attackers

2.1. Overview

On July 12, Microsoft disclosed that the Outlook email accounts of approximately 25 organizations worldwide, including at least 2 U.S. government agencies, had been hacked by suspected Chinese hackers. [*]15 [*]16

On the same day, CISA (Cybersecurity and Infrastructure Security Agency) and the FBI released documents targeting critical infrastructure organizations. They described ways to increase surveillance and detect the attacks.



JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Product ID: AA23-193A

July 12, 2023

Enhanced Monitoring to Detect APT Activity Targeting Outlook Online

SUMMARY

In June 2023, a Federal Civilian Executive Branch (FCEB) agency identified suspicious activity in their Microsoft 365 (M365) cloud environment. The agency reported the activity to Microsoft and the Cybersecurity and Infrastructure Security Agency (CISA), and Microsoft determined that advanced persistent threat (APT) actors accessed and exfiltrated unclassified Exchange Online Outlook data.

CISA and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory to provide guidance to critical infrastructure organizations on enhancing monitoring of Microsoft Exchange Online environments. Organizations can enhance their cyber posture and position themselves to detect similar malicious activity by implementing logging recommendations in this advisory. Organizations that identify suspicious, anomalous activity should contact Microsoft for proceeding with mitigation actions due to the cloud-based infrastructure affected, as well as report to CISA and the FBI.

Figure 2 CISA and FBI Joint Security Advisory [*]17

According to Microsoft's announcement, there is no evidence of further unauthorized access since the company applied mitigations to the attack. However, the company has not disclosed how the signing key that triggered the attack (see below) was stolen, and it has been criticized by experts as disingenuous in its use of language that does not acknowledge the existence of the vulnerability. [*]18

2.2. How the incident was discovered

On June 16, the U.S. State Department reported to Microsoft an unusual data access identified in the logs of Microsoft's Exchange Online e-mail service, which the Department uses. [*]19 [*]20 The investigation found that someone had compromised e-mail data from about 25 organizations and personal e-mail accounts associated with those organizations for about a month from May 15. Department of Commerce accounts were also compromised, and Commerce Secretary Gina Raimondo was no exception. [*]21

2.3. About the attack and who carried it out

On July 14, Microsoft posted a blog explaining who carried out the attack and how it was carried out. [*]22

[Storm-0558]

The attack came from an attacker that Microsoft is tracking as Storm-0558. Storm-0558 has targeted government agencies in the US and Europe for espionage, data theft, and credential access, including phishing attacks in the past. Storm-0558 is presumed to be a China-based attacker, in part because the April to July activity pattern of Storm-0558 was consistent with typical working hours in China **(Figure 3).**

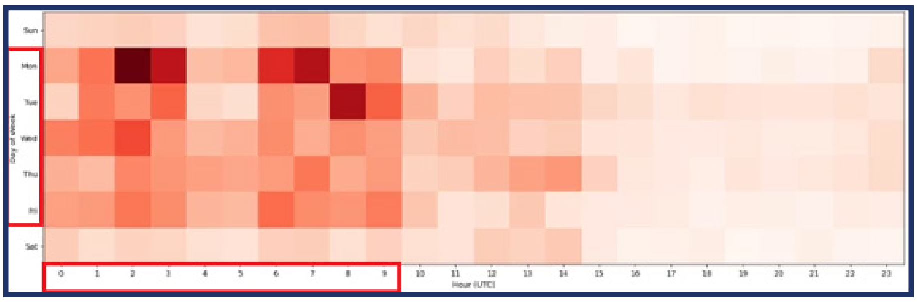


Figure 3 Storm-0558 Activity Days (Vertical Axis) and Times (Horizontal Axis) (from Microsoft)
Mostly active Monday through Friday, 0:00 to 9:00 UTC (8:00 AM to 5:00 PM Chinese Standard Time)

[Attack method]

The attacker first forged a security token for Outlook Web Access (OWA), a webmail version of Outlook, using a Microsoft Account (MSA) signing key obtained by unknown means. The MSA signing key is used in consumer systems and is separate from the compromised key for Azure AD, a cloud service primarily for businesses. By nature, these keys and tokens are only valid within each system. [*]23 However, there was a problem with this token validation, and it was possible to impersonate an Azure AD user with a token forged with an MSA signing key.
In addition, there was a problem in the API of OWA that the new token could be obtained by showing the old token issued in the past, and the data such as mail data and file attachments was stolen through the API by the attacker who obtained the new token illegally by exploiting this problem.

2.4. Questions about Microsoft's announcement

Microsoft's announcement and response to this incident have been questioned by media and security experts.

How to Obtain an MSA Signing Key

The MSA signing key used to forge the security token and the origin of the incident was simply "obtained by [the attacker]," according to the blog. It did not specify how it was obtained, nor did it respond to media requests for clarification. Some media have suggested that Microsoft itself may have been compromised. [*]24

[Predisposition not to acknowledge vulnerabilities]

As mentioned earlier, token verification was vulnerable in that a token created with a consumer key could be used to access Azure AD for businesses. But experts say Microsoft is focusing on damage control in its announcements, using vague terms like "problem" and "defect" instead of using terms like "vulnerability" and "zero-day." [*]25

In addition, when such vulnerabilities are discovered, CVEs are typically used to help users identify and track them, but Microsoft has never acknowledged any vulnerabilities in cloud services and has not issued any CVEs. [*]26

[Microsoft's own detection capabilities and costs to customers]

As noted above, the attack was detected by the US State Department, not by Microsoft itself. Detection also required detailed logs, which can only be obtained with expensive Microsoft contracts. Standard contracts provide limited logs, which would have been insufficient to detect the attack. [*]27 This means that customers would have to spend extra money to be able to detect attacks resulting from Microsoft's flaws.

On July 19, Microsoft opened up detailed logging to standard contract users. [*]28

2.5. Summary

Microsoft's reputably reliable cloud services have been compromised by Chinese attackers, who stole email data. Cybersecurity risks are an important issue in an information infrastructure-based ICT society. Therefore, organizations and companies that have been victimized must promptly and transparently disclose information to prevent the chain of victimization and fulfill their accountability to stakeholders. Since this incident occurred in a cloud service provider that leads the global market and has a significant impact, more appropriate disclosure is required. In addition, when high security is required, even for a major cloud service, users should not be left to their own devices. Customers should obtain detailed logs from their cloud services and ensure that these are monitored and analyzed to detect any breaches.

3. Increase in APT attacks using USB thumb drives

3.1. Overview

In July 2023, Mandiant announced that detection of attacks using malware infected USB drives had increased threefold from the second half of 2022. [*]29 Most of the attacks were by APT groups looking to steal sensitive information, the company said.

The malware used by these cyber attackers is designed to use thumb drives to break into systems and to spread and retrieve information after a breach. This suggests that the use of thumb drives is effective in attacking systems with strong security.

3.2. Examples of attacks detected by Mandiant

As an example of an attack using a USB stick, Mandiant provides [29] examples of attack campaigns by cyber attackers. In the campaign, a device is infected with malware when a user is tricked into running a malware installer on a USB stick. After the malware infection occurred, it accessed other devices in the network to collect sensitive information and set up a backdoor to try to connect outside the network. In addition, the ability to install malware installers on other USB thumb drives inserted into the infected system was confirmed (Figure 4)[29]. The intention of this capability is in order for the malware to be able to self-propagate onwards, using other USB thumb drives.

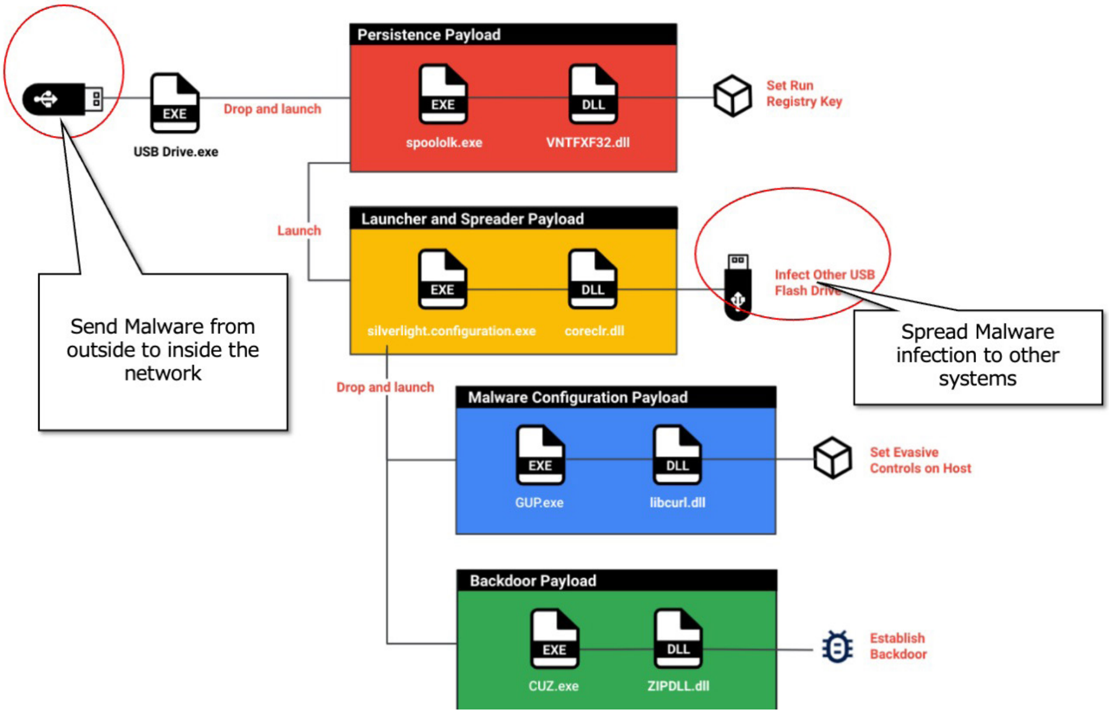


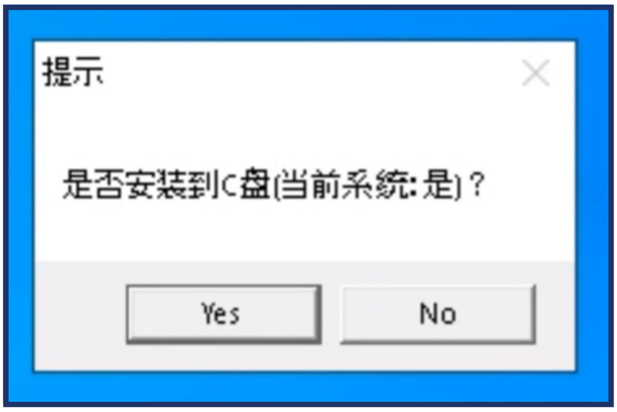
Figure 4 Deployment of malware infection using USB thumb drives (Annotations added to Mandiant's diagram)

3.3. USB thumb drive used for attack vector

In addition to Mandiant, several attack campaigns by APT groups backed by countries such as China and Russia using USB thumb drives were detected from last year to this year. [*]30 [*]31 [*]32 In these attacks, USB thumb drives are used as an attack vector to move malware across systems. The routes can be divided into three categories:

[As a route for sending malware from outside into the system] [*]33

An attacker can infect critical systems through a USB stick. A USB stick that an attacker sends to an employee by mail or that is infected with malware when connected to a device outside the organization is brought into the target organization. [*]34 When an employee connects the USB stick to the device and accidentally executes the installer (Fig. 5)[30], the malware infection spreads in the system.



提示

是否安装到C盘(当前系统:是)？

Fig. 5 Message of a disguised program targeting infection
Do you want to install it on the C drive? (Current system: Yes)

[As the infection spread route from the malware-infected system] [33]

The infected malware resides in the system and monitors the USB memory connection status. When it detects a new USB memory connection, it copies itself to the USB memory. When the infected USB memory is connected to another system, the malware infection spreads to that system. This allows the infection to eventually reach the target system, even if the first infected system is not the target system.

[As an information leak route from a malware-infected system] [*]35

Malware has been found to copy stolen confidential information to a USB thumb drive when a malware-infected system has the USB thumb drive inserted. [*]36 This is thought to be an attempt to transfer confidential information from a system with strong security where it would otherwise be difficult to exfiltrate information to another system with relatively low security through the use of a USB thumb drive.

3.4. Why is a USB thumb drive being targeted as an attack vector?

Critical systems are difficult to penetrate from the outside due to measures such as network isolation, defense-in-depth and targeted mail filtering. In such highly secure systems, USB thumb drives are often used to facilitate data transfers for purposes such as maintenance while avoiding the use of network communication for security reasons. Cyber attackers seem however to be trying the same methods in order to bypass security controls.

In fact, several such methods have been found in attacks targeting governments and the private sector by APT groups such as those related to the Chinese and Russian governments, including attacks related to Japanese organizations (Figure 6)[29.]

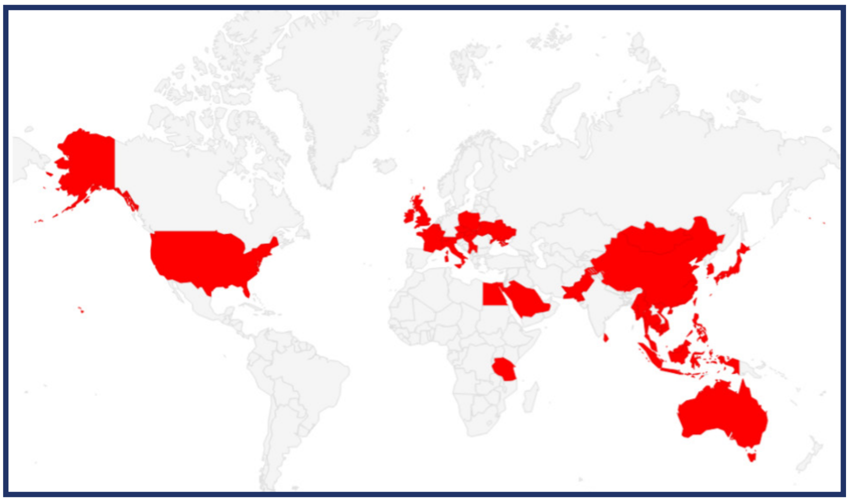


Figure 6 Attacks by Chinese government-affiliated APT groups
Distribution of organizations affected by attacks using USB thumb drives

3.5. Summary

Recent actions by cyber attackers have made it clear that organizations need to be more vigilant in their use of thumb drives. In the past, people have been wary of thumb drives brought in from outside, but in the future, they should be equally wary of thumb drives used only in organizations and operate under the assumption that they may be infected with malware.

Disclaimer

Please note that although the contents of this article are best kept accurate, the contents are not guaranteed and no compensation is given for any damage or loss arising from the use of this article. If you have any questions, such as typographical errors, content errors, or other issues, please contact us at the following address:

Contact: NTT Security Japan Inc.

OSINT Monitoring Team, Consulting Services Department
Email address: WA_Advisorysupport@ntt.com

Sources

1. Source: Yomiuri Shimbun Online ""Ransomware Infected" in English, Printed 100 Sheets from Printer ... Nagoya Port System Failed"
https://www.yomiuri.co.jp/national/20230705-OYT1T50220/

2. Source: Nagoya Port Management Association "Japan's Best Nagoya Port"
https://www.port-of-nagoya.jp/shokai/kohoshiryo/kids/1001074.html

3. Source: Nagoya Port Management Association "The Full Story of Nagoya Port"
https://www.port-of-nagoya.jp/shokai/kohoshiryo/photogallery/photogallery/1001055.html

4. Source: Asahi Shimbun DIGITAL "Printers Exposed English Endlessly to Cyber-Damaged Port of Nagoya"
https://www.asahi.com/articles/ASR7C5H87R7BOIPE003.html

5. Source: NHK Nagoya Broadcasting Station "Cyber attack on Nagoya Port? What was the damage of ransomware?"
https://www.nhk.or.jp/nagoya/lreport/article/001/44/

6. Source: Nikkei XTECH "Delayed recovery from backup due to malware detection, Nagoya Port Unified Terminal System"
https://xtech.nikkei.com/atcl/nxt/news/18/15539/

7. Source: Nagoya Port Transportation Association, "History Report of NUTS System Failure"
https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf

8. Source: Nikkei XTECH "Delayed recovery from backup due to malware detection, Nagoya Port Unified Terminal System"
https://xtech.nikkei.com/atcl/nxt/news/18/15539/

9. Source: NHK "Nagoya Port System Failure" Ransomware "Infection Confirmation Recovery Hurry
https://www3.nhk.or.jp/news/html/20230705/k10014119091000.html

10. Source: Tokai TV "TRAILER DRIVER: "I can't get to work." Nagoya Port System Failure Restored in the Morning of 6th. Resumption of Container Entry/Exit Delayed"
https://www.tokai-tv.com/tokainews/article_20230706_28617

11. Source: the Ministry of Land, Infrastructure, Transport and Tourism, "Review Committee on Information Security Measures at Container Terminals"
https://www.mlit.go.jp/report/press/port02_hh_000189.html

12. Source: Sankei News "Russia-based Hackers Accuse 2000 Japanese Companies of the World's Largest Cybercrime Group, 15000"
https://www.sankei.com/article/20220905-KWCTLULU4VN4PPPYVSGWQKRVFU/

13. Source: TechFinitive LockBit ransomware attackers target Japan's biggest port: but who's next?
https://www.techfinitive.com/lockbit-ransomware-attackers-target-japans-biggest-port/

14. Source: Yomiuri Shimbun Online "Nagoya Port System Stopped, Vulnerable VPN Targeted ... Unprotected without Applying Latest Hotfix"
https://www.yomiuri.co.jp/national/20230727-OYT1T50215/

15. Source: Bleeping Computer "Microsoft: Chinese hackers broken US govt Exchange email accounts"
https://www.bleepingcomputer.com/news/security/microsoft-chinese-hackers-breached-us-govt-exchange-email-accounts/

16. Source: Microsoft "Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email"
https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

17. Source: CISA "Enhanced Monitoring to Detect APT Activity Targeting Outlook Online"
https://www.cisa.gov/sites/default/files/2023-07/aa23-193a_joint_csa_enhanced_monitoring_to_detect_apt_activity_targeting_outlook_online_2.pdf

18. Source: Ars Technica "Microsoft takes pains to obscure role in 0-days that caused email breach"
https://arstechnica.com/security/2023/07/microsoft-takes-pains-to-obscure-role-in-0-days-that-caused-email-breach/

19. Source: Microsoft "Mitigation for China-Based Threat Actor Activity"
https://blogs.microsoft.com/on-the-issues/2023/07/11/mitigation-china-based-threat-actor/

20. Source: Reuters "Chinese hackers broken State, Commerce Depts, Microsoft and US say"
https://www.reuters.com/technology/chinese-hackers-accessed-government-emails-microsoft-says-2023-07-12/

21. Source: The Washington Post "Chinese hackers breach email of Commerce Secretary Raimondo and State Department officials"
https://www.washingtonpost.com/national-security/2023/07/12/microsoft-hack-china/

22. Source: Microsoft "Analysis of Storm-0558 techniques for unauthorized email access"
https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

23. Source: Microsoft "Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email"
https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

24. Source: The Stack "Microsoft clams up over critical Azure key breach, security incident as attackers breach US agencies"
https://www.thestack.technology/microsoft-msa-key-breach-mystery/

25. Source: TechCrunch "Microsoft lost its keys, and the government got hacked"
https://techcrunch.com/2023/07/17/microsoft-lost-keys-government-hacked/

26. Source: Ars Technica "Microsoft takes pains to obscure role in 0-days that caused email breach"
https://arstechnica.com/security/2023/07/microsoft-takes-pains-to-obscure-role-in-0-days-that-caused-email-breach/

27. Source: Reuters "Microsoft under fire after hacks of US State and Commerce departments"
https://www.reuters.com/technology/microsoft-under-fire-after-hacks-us-state-commerce-departments-2023-07-13/

28. Source: CISA "CISA and Microsoft Partnership Expands Access to Logging Capabilities Broadly"
https://www.cisa.gov/news-events/news/cisa-and-microsoft-partnership-expands-access-logging-capabilities-broadly

29. Source: Mandiant "The Spies Who Loved You: Infected USB Drives to Steal Secrets"
https://www.mandiant.com/resources/blog/infected-usb-steal-secrets

30. Source: NTT Security Technical Blog "Attack Using FlowCloud Based on USB Memory"
https://jp.security.ntt/tech_blog/102id0t

31. Source: Check Point Research "Beyond the Horizon: Traveling the World on Camaro Dragon's USB Flash Drives"
https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/

32. Source: Symantec Enterprise Blogs "Shuckworm: The other side of Russia's relentless cyber campaign against Ukraine"
https://symantec-enterprise-blogs.security.com/blogs/japanese/shuckworm-roshianiyoruukurainaniduisuru-zhiaonasaihakiyanhennolice

33. Source: MITRE ATT&CK "Replication Through Removable Media, Technique T1091 – Enterprise"
https://attack.mitre.org/techniques/T1091/

34. Source: Recorded Future "FBI: FIN7 hackers target US companies with BadUSB devices to install ransomware"
https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware

35. Source: MITRE ATT&CK "Exfiltration Over Physical Medium: Exfiltration over USB, Sub-technique T1052.001"
https://attack.mitre.org/techniques/T1052/001/

36. Source: Kaspersky ICS CERT "Common TTPs of attacks against industrial organizations. Implants for gathering data"
https://ics-cert.kaspersky.com/publications/reports/2023/07/31/common-ttps-of-attacks-against-industrial-organizations-implants-for-gathering-data/

NTT Security Holdings