# Cyber Security Reports

2023.08

**NTT Security Japan Co., Ltd.**

**Consulting Services Department OSINT Monitoring Team**

Information Asset Classification: Public

NTT | Security Holdings

# Contents

# About this report

This report summarizes three interesting cyber security related incidents and related events that occurred during August 2023. The summary of each topic is as follows.

## CHAPTER 1

## “The Japanese National Police Agency arrested an overseas individual for the first time in an international joint investigation in relation to phishing.”

- On August 8, the National Police Agency announced that it had arrested Der Kalisna, a resident of Indonesia, in cooperation with local police on charges of illegally collecting and using credit card information through phishing (a form of social engineering attack).
- Der collected credit card information through phishing. He then worked with an accomplice in Japan to purchase and resell electrical goods and transfer the funds to him
- This is the first case in which Japan's Special Cyber Investigation Unit conducted an international joint investigation that led to the arrest of a suspect

## CHAPTER 2

## “North Korea hacks top Russian missile company”

- A group of hackers linked to the North Korean government has been found to have hacked a missile company with close ties to the Russian military in an attempt to steal information.
- Several North Korean hacker groups installed backdoors in Windows to hack into sensitive internal infrastructure, including email servers.

## CHAPTER 3

## "SMS Traffic Pumping Scam"

- SMS Traffic Pumping is activity conducted by cybercriminals resulting in fraudulent SMS charges for an organization.
- Cybercriminals typically manipulate mobile network providers to inflate charges for SMS messages that are sent to high-cost destinations.
- Organizations should take measures to detect and prevent SMS traffic pumping such as monitoring unexpected traffic spikes and introducing transmission restrictions.

# 1. National Police Agency arrests overseas phishers for first time in international joint investigation

## 1.1. Suspect arrested in an international joint investigation

On August 8, the National Police Agency announced the arrest of Der Kalisna, a resident of Indonesia, in cooperation with local police for allegedly collecting and illegally using credit card information through phishing attacks. [*][1] This is the first case in which the National Police Agency Cyber Task Force cooperated with law enforcement agencies in another country to arrest a suspect in an incident that occurred in Japan

**Figure 1 Cyber Special Investigation Team Symbols**

## 1.2. Incident and Investigation

**[Outline of Incident]**

Der, who was arrested, used a notorious Phishing as a Service (PhaaS) platform called "16 Shop" to create a fake website. Using “16 Shop” Der was able to collect personal information and credit card information [*][2] [*][3]When Der used the credit card information to purchase electrical goods, he had an Indonesian individual living in Japan resell the goods, and send him the money. He is believed to have used this method to avoid identification in order to cash out stolen credit card information.

**[History of the arrest of the suspect]**

Der emerged during the investigation due to the arrest of his accomplice (mentioned above) by the Osaka Prefectural Police in August 2022. The suspicion was that Der had stolen the credit card information of another individual through use of the phishing service in October 2019 and purchased a personal computer online.

In April this year, the Osaka Prefectural Police and Cyber Special Investigation Unit established a joint investigation. In July, the Indonesian police visited Japan and conducted an investigation in cooperation with Japanese police. The results confirmed suspicions leading to Der's arrest in Indonesia on July 9. The total amount of damage caused by Der's crimes in Japan was approximately 1.6 billion rupiah (about 15.2 million yen). [*][4]

**Figure 2 Jakarta Cybercrime Bureau holding press conference on arrest of suspect through cooperationwith Japan [*][5]**

## 1.3. 16Shop and PhaaS

Der used 16Shop, a Phishing-as-a-Service (PhaaS) platform that provides a set of tools and environments necessary to conduct phishing attacks. The use of PhaaS for attacks is known to be on the rise in recent years. PhaaS allows cybercriminals to easily launch attacks without having to provide their own tools and servers. Common features of PhaaS include tools to create phishing sites that resemble well-known shopping sites, the ability to deliver fraudulent emails, and dashboards to view victim information. [*][6]

16Shop has been in operation since around 2018, and in addition to the general PhaaS features listed above, it also includes features that make it difficult to detect [*][7] The service was sold to cybercriminals and had at least 70,000 victims. [*][8] [*][9]An investigation led by Interpol in 2021 led to the closure of 16Shop and arrests of their operators. It is believed that this information led to the above-mentioned international investigation by the National Police Agency.[*][10

## 1.4. Summary

Der's arrest marks the first time the Special Investigation Unit has uncovered an international cybercrime in a joint investigation with foreign law enforcement agencies. As many cybercrimes are committed across national borders, international cooperation among law enforcement agencies is essential, and we look forward to further efforts in the future.

# 2. North Korea hacks top Russian missile company

## 2.1. Overview

On August 7, 2023, a group of North Korean hackers were found to have illegally accessed the networks of a major Russian missile company for more than 5 months, Reuters reported. This incident demonstrates North Korea will also target one of its few allies in an attempt to acquire new technology [*][11].

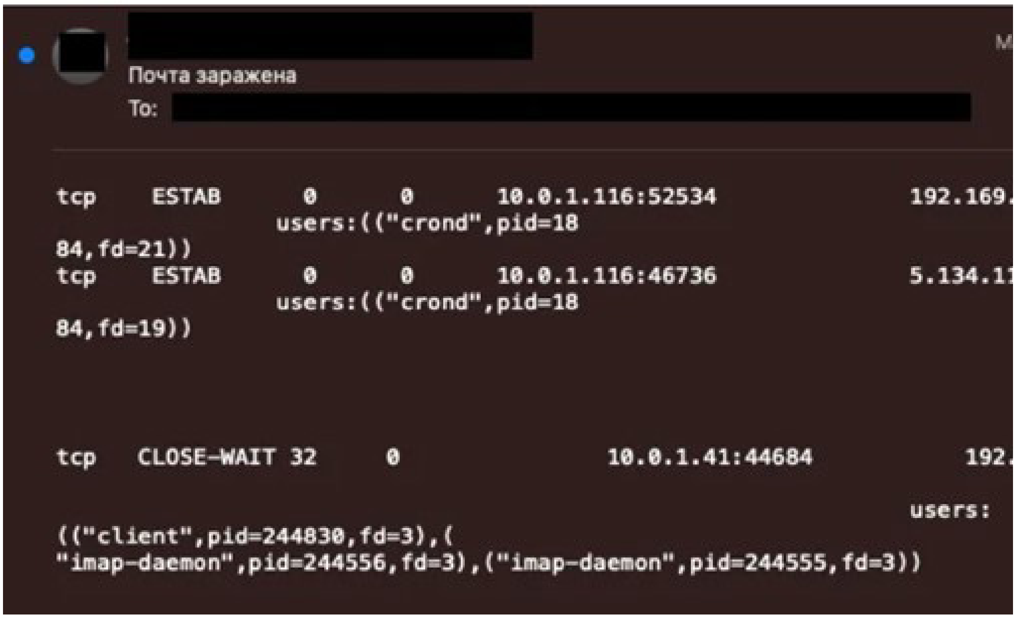
## 2.2. About hacking

**[Illegal intrusion by North Korean hacker group]**

US cybersecurity firm SentinelOne provided the following information.
Between at least December 1, 2021 and May 2022, the North Korea-linked hacker groups Lazarus and ScarCruft secretly installed a remote backdoor tool on systems of the Russian missile engineering organization NPO Masinostroyenya and repeatedly accessed data. It is not clear exactly what kind of information they accessed 11. [*][12]

**[SentinelOne investigation results] 11, [*][13]**

First, Lazarus installed a Windows backdoor called OpenCarrot onto NPO systems. Another hacker group, ScarCruft, appeared to have compromised sensitive internal infrastructure, including email



[redacted] [redacted]

M

Почта заражена

To: [redacted]

```
tcp     ESTAB      0       0       10.0.1.116:52534              192.169.
                   users:(("crond",pid=18
84,fd=21))
tcp     ESTAB      0       0       10.0.1.116:46736              5.134.11
                   users:(("crond",pid=18
84,fd=19))


tcp    CLOSE-WAIT 32     0               10.0.1.41:44684             192.

                                                                  users:
(("client",pid=244830,fd=3),(
"imap-daemon",pid=244556,fd=3),("imap-daemon",pid=244555,fd=3))
```

**Figure 3 Example of an email leaked from NPO regarding the investigation of the breach (Contains the IP associated with the attacker that NPO Mash detected as suspicious network communication) [*][14]**

servers. The links between the groups are unclear, but both are believed to be aligned with the North Korean state's strategy, suggesting that the North Korean state was trying to increase the odds of a successful breach by assigning multiple attack groups to a single target.
SentinelOne's confirmation comes after it investigated an email archive of NPO while investigating and tracking North Korean threat actors. The email collection was leaked by NPO when it discovered and began its own investigation into the incident. By matching the hacking information discussed in the emails with other cyber attack trails, it was possible to find a connection with the activities of the above groups

## 2.3. About the damaged organization

NPO is a company engaged in missile and military spacecraft development and possesses highly confidential and sensitive intellectual property of the Russian military. Its hypersonic cruise missile, the Zircon, has been highly praised by President Vladimir Putin.
North Korea, on the other hand, manufactures an intercontinental ballistic missile (ICBM) capable of striking the U.S. mainland, and it is thought that NPO have strong interests in related technologies and fields.
Missile experts say that even if North Korea obtains information about Zircon, it won't be able to produce zircon anytime soon. But they also point out that North Korea may have tried to obtain information about its other technologies, such as manufacturing processes related to missile fuel. After the NPO breach, North Korea disclosed several developments in ballistic missile development, but the link to the breach is unclear. 11.

## 2.4. Russian Defense Minister Visits North Korea

On July 26, 2023, Russian Defense Minister Sergei Shoigu visited North Korea to attend an event commemorating the 70 year armistice of the Korean War. North Korean radio reported that Shoigu praised the Korean People's Army as "the strongest." Shoigu also took the stage next to North Korean leader Kim Jong Un at a military parade the next day, which was highly unusual. [*][15]
Russia, which is facing a shortage of weapons amid the prolonged war with Ukraine, may have turned to friendly countries for help. [*][16]
On July 31, it was confirmed that a Russian VIP-only aircraft was staying in Pyongyang, and it is speculated that they discussed arms trafficking at that time. [*][17] It was a week later that Reuters reported on the possibility that North Korea had hacked NPO, while Russia was closely approaching North Korea.
As of September 13, North Korean leader Kim Jong Un visited Russia for talks and is expected to discuss military cooperation, including providing ammunition, with Russian President Vladimir Putin. [*][18]

**Figure 4: Russian Defense Minister Sergei Shoigu and Russian Defense Minister Sergei Shoigu inspect weapons in North Korea**
North Korean leader Kim Jong Un guiding them 11

## 2.5. Summary

North Korea has a high level of cyber attack capability, despite the fact that most of its citizens do not have access to the Internet, and in this case, North Korea has shown that it will use its cyber attack capability to target even friendly countries..
North Korea's interest for missile development technology in cyberspace has greatly affected the security environment of neighboring countries.

# 3. SMS traffic pumping scam

## 3.1. Overview

SMS is widely used by organizations for marketing, notifications and OTPs (one time passwords) However, it has recently come into focus that cybercriminals are taking advantage of SMS systems to inflate traffic and receive a share of the revenue. . [*][19]

## 3.2. SMS traffic pumping technique

**[SMS traffic pumping scam mechanism] 19 [*][20]**

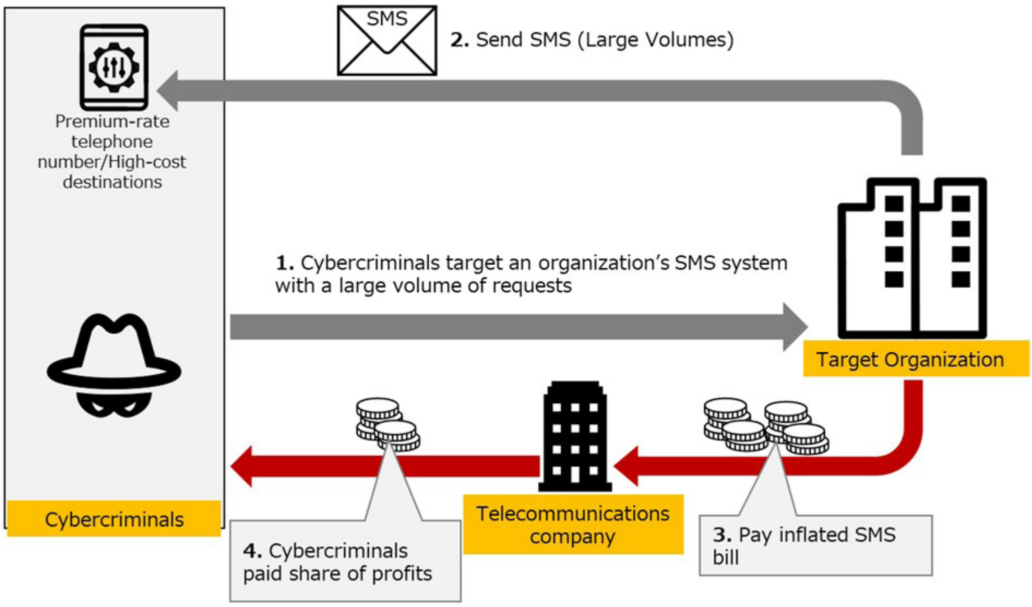

SMS
2. Send SMS (Large Volumes)
Premium-rate telephone number/High-cost destinations
1. Cybercriminals target an organization's SMS system with a large volume of requests
Target Organization
Cybercriminals
Telecommunications company
3. Pay inflated SMS bill
4. Cybercriminals paid share of profits

**Figure 5 SMS traffic pumping simplified**

In the United States and many other countries, "Premium-rate telephone numbers" are available that charge higher rates for select services.

The cybercriminals may obtain a Premium-rate telephone number from a carrier. It then targets companies that use SMS to send notifications from apps to users. The scam group sends a flurry of requests to target companies to send SMS to their Premium-rate telephone number. The target company that sends SMS in response to the request pays the telco a hefty phone bill. (Figure 3 SMS traffic pumping simplified

In SMS traffic pumping scams, a portion of the phone bill paid to the telecom company is paid to the criminal group.It is believed that there are two types of scams: either the criminal group misuses the payment system to make money, or the telecom company that aims to increase the telecom fee pays kickbacks to the criminal group through collusion with the criminal group.

**[Example of damage]**

A typical example of this fraud is a scheme to exploit SMS authentication provided by Web services. One example is the service change of Twitter (now X).

Since March 2023, Twitter has restricted SMS authentication, which was previously available to all users, to paid users only. In introducing the restriction, Twitter president Elon Musk claimed that the SMS traffic pumping scam caused Twitter to send a lot of SMS, in countries other than North America costing the company $60 million a year. [*][21]

## 3.3. Countermeasures

Companies sending SMS should take measures against the potential for significant financial losses from SMS traffic pumping fraud.

First, the following restrictions should be introduced to prevent fraudulent SMS transmissions 19 and 20.

- Prohibit SMS transmissions to countries outside the service
- Set rate limits and delays for transmissions to prevent frequent SMS transmissions
- Suppress sending requests by bots with CAPTCHA

Also, monitor the sending status of SMS, find the sending destination suspected of fraud, and restrict sending.

In addition, among the services that send SMS upon request, SMS authentication has many other security problems, such as low resistance to man-in-the-middle attacks. As a fundamental countermeasure, consider adopting multi-factor authentication such as FIDO and OTP tokens that do not rely on SMS.

Awareness of the existence of the "Premium-rate telephone number" and the threat posed by SMS traffic pumping fraud will be necessary for future use of SMS transmission.

## 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: Sankei News "Indonesian National Police Arrest Suspect of Phishing for First Time in International Joint Investigation"
https://www.sankei.com/article/20230808-EP5Q3NPC6NIEDPOD5D6JQFQLQI/

2. Source: Asahi Shimbun DIGITAL "First International Cyber Investigation Arrests Indonesian Using Global Fraud Tool"
https://www.asahi.com/articles/ASR884RWLR87UTIL040.html

3. Source: WNEWS247 "Japan-Indonesia phishing probe leads back to a teenage ‘genius’"
https://wnews247.com/2023/08/09/japan-indonesia-phishing-probe-leads-back-to-a-teenage-genius/

4. Source: DIVISI HUMAS POLRI "Bareskrim Ungkap Peretasan Kartu Kredit di Jepang, Kerugian Capai 1,6 Milyar"
https://humas.polri.go.id/2023/08/08/bareskrim-ungkap-peretasan-kartu-kredit-di-jepang-kerugian-capai-16-milyar/

5. Source: DIVISI HUMAS POLRI "Bareskrim Ungkap Peretasan Kartu Kredit di Jepang, Kerugian Capai 1,6 Milyar"
https://humas.polri.go.id/2023/08/08/bareskrim-ungkap-peretasan-kartu-kredit-di-jepang-kerugian-capai-16-milyar/

6. Source: Bleeping Computer "Interpol takes down 16shop phishing-as-a-service platform"
https://www.bleepingcomputer.com/news/security/interpol-takes-down-16shop-phishing-as-a-service-platform/

7. Source: McAfee Blog: 16Shop Phishing Kit Targets Amazon Users
https://ascii.jp/elem/000/001/898/1898098/

8. Source: INTERPOL "Notorious phishing platform shut down, arrests in international police operation"
https://www.interpol.int/en/News-and-Events/News/2023/Notorious-phishing-platform-shut-down-arrests-in-international-police-operation

9. Source: Asahi Shimbun DIGITAL "16 SHOP" Sold to Over 70,000 People in 43 Countries "ICPO Announces International Investigation
https://www.asahi.com/articles/ASR8953J9R89UTIL01B.html

10. Source: Cyber Defense Institute "Behind the Scenes of 16Shop Arrest"
https://io.cyberdefense.jp/entry/16Shop/

11. Source: REUTERS "North Korean hackers broken top Russian missile maker"
https://www.reuters.com/technology/north-korean-hackers-breached-top-russian-missile-maker-2023-08-07/

12. Source: Jiji News "North Korean Hackers Invade Russian Companies? - Technology theft by unauthorized access, Reuters report"
https://sp.m.jiji.com/article/show/3015587?free=1

13. Source: SentinelLabs "Comrades in Arms? | North Korea Compromises Sanctioned Russian Missile Engineering Company"
https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/

14. Source: SentinelLabs "Comrades in Arms? | North Korea Compromises Sanctioned Russian Missile Engineering Company"
https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/

15. Source: REUTERS "North Korea's Kim shows off banned missiles to Russian minister"
https://www.reuters.com/world/north-koreas-kim-jong-un-meets-russian-defence-minister-2023-07-27/

16. Source: NHK Saturday Watch 9 "Unusual! Defense Minister's Visit to North Korea Aims to Hold Africa, Russia to Boost Diplomacy"
https://www.nhk.jp/p/ts/7K78K8ZNJV/blog/bl/pZWdy5qgmE/bp/p2n9q1mPE6/

17. Source: Bloomberg, "North Korea Becomes Worried About Russian Military VIPs - Weapons Trade
https://www.bloomberg.co.jp/news/articles/2023-08-07/RZ0DX2T1UM0W01

18. Source: Asahi Shimbun DIGITAL "What kind of space base are Kim Jong Un and Putin expected to meet?"
https://www.asahi.com/articles/ASR9D72LVR9DUHBI038.html

19. Source: Twilio SMS Traffic Pumping Fraud
https://support.twilio.com/hc/en-us/articles/8360406023067-SMS-Traffic-Pumping-Fraud

20. Source: kasada "SMS Fraud Takes A Toll: The Evolving Threat of SMS Pumping and Toll Fraud"
https://www.kasada.io/sms-fraud-evolving-sms-pumping-toll-fraud/

21. Source: Commsrisk "Elon Musk Says Twitter Lost $60mn a Year Because 390 Telcos Used Bot Accounts to Pump A2P SMS"
https://commsrisk.com/elon-musk-says-twitter-lost-60mn-a-year-because-390-telcos-used-bot-accounts-to-pump-a2p-sms/

NTT Security Holdings