Cyber Security Reports

2023.02

NTT Security Japan Inc.

OSINT Monitoring Team, Consulting Services Department

NTT Security Holdings

Content

About this report

This report selects and summarizes 3 topics that are considered to be especially important from among various information security incidents and events that occurred during February 2023 and the changes in the surrounding environment. The summary of each topic is as follows.

CHAPTER 1
Russian hacktivists target companies with DDoS attacks

- Hacktivist "NoName," which carries out DDoS attacks against countries imposing sanctions against Russia, launched DDoS attacks against Japanese government agencies and companies in February 2022.
- Organizations in a number of countries including Japan, Estonia, Latvia and Sweden have been targeted.
- NoName advertised the results of the attacks as revenge for sanctions enacted against Russia. In one instance, the website of the Petroleum Association of Japan was temporarily taken offline.
- Industries related to sanctions against Russia and companies involved in critical infrastructure that have previously been targeted need to be aware of developments in their governments' sanctions against Russia and be on guard in case of further attacks. It is important to introduce DDoS countermeasures such as CDNs to eliminate weak points.

CHAPTER 2
Cybercrime using Google's advertising platform is on the rise

- On February 9, security company Sucuri announced that it had observed a campaign that attacked sites using WordPress and used such things as fake short URLs to lure website visitors to fraudulent ad sites.
- There was also an increase in attacks exploiting ads in Google search results, revealing how the Google ad platform was being used in various ways by cybercriminals.
- Instead of trusting them unconditionally just because they are Google search results, users need to follow and use basic precautions such as checking the URL of the destination, not accessing pages flagged by security software, etc., and not entering or downloading information on sites where they feel suspicious.

CHAPTER 3
Chinese hacker group Xiaoqiying carries out cyberattacks on South Korean organizations

- In early 2023, the suspected Chinese-speaking hacker group Xiaoqiying declared that it would target more than 2,000 South Korean organizations with cyberattacks. In fact, several organizations suffered damage such as site tampering and connection failures.
- In China, many hackers carried out cyberattacks against foreign countries, including Japan, in the past, motivated by patriotism, but such hackers' activities have stagnated in recent years under strict surveillance by the Chinese government.
- We can imagine that revelations of massive Chinese data leaks on international anonymous hacker forums and the way in which hacker groups have taken advantage of global developments have worked as a stimulus for Chinese hackers, and inspired them to act again. The use of Telegram, foreign anonymous message boards and the like has led to situations where anonymous Chinese-speaking hackers can gather.

1. Russian hacktivists target companies with DDoS attacks

1.1. Overview

Since the beginning of February 2023, the pro-Russian hacktivist group “NoName” has frequently launched DDoS attacks against government agencies and companies in a number of countries including Japan, Estonia, Latvia and Sweden. The attacks have focused on government agencies and companies, causing websites of the Petroleum Association of Japan, JR East, and other companies to become difficult to access (Figure 1). The group has been active since around March 2022, immediately after the invasion of Ukraine, and has repeatedly launched DDoS attacks targeting countries that have imposed economic sanctions on Russia. [*]1

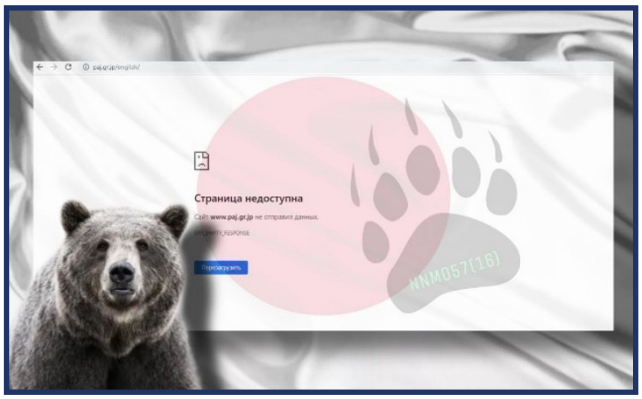

Figure 1 NoName
Screen announcing successful attack on the Petroleum Association of Japan

1.2. NoName Activities

DDoS Attacks on Countries [*]2

The invasion of Ukraine in February 2022 was preceded and followed by increased cyberattacks on countries by pro-Russian hacktivists. KILLNET and Anonymous RUSSIA, which made headlines for their DDoS attacks on the Japanese government in September, are prime examples, and NoName is a similar group.

In addition to Ukraine, DDoS attacks have been carried out against government agencies, financial institutions, and critical infrastructure companies, targeting a wide range of countries allied with Ukraine, including the United States, the Baltic States, Finland, Sweden, Norway, Denmark, Germany, and Italy. While the targets are generally changed on a weekly basis, the attacks have also been timed to coincide with international developments, such as the focused attacks on the host countries of EU summits.

The group has been active since around March 2022, just after the start of the war. In June 2022, a shipment to the Russian enclave territory of Kaliningrad was blocked by Lithuania, whose territory the railway line to Kaliningrad traverses, because of sanctions. Soon after, NoName made headlines when it launched a DDoS attack targeting Lithuanian transport infrastructure companies. In January, it targeted candidate websites with DDoS attacks in an attempt to disrupt the presidential election in the Czech Republic. [*]3

Results announced via Telegram

NoName has set up a public group on Telegram. Since creating the group on March 11, 2022, it has gained followers and now has more than 32,000 participants. The group makes arguments, mostly in Russian, that ridicule countries that sanction Russia. It is customary for NoName

DDoS attacks to post a collage of bears.

Within the Telegram group, there are about 1,400 grassroots collaborators who carry out attacks using a DDoS tool provided by NoName called “DDoS Projects”. NoName releases rankings and awards prizes based on the number of attacks they’ve carried out. [*]4

NoName has actually launched more attacks than the ones it claims to have successfully launched on Telegram, and it has repeatedly attacked sites it previously successfully attacked. Security firm Avast put the attack success rate at around 40%. [*]5

Figure 2: Showing a tweet that makes a mock of NoName, the group ridicules the poster as a Twitter samurai who wants to make useless arguments.

(Exhibitionism)

NoName cares about and observes the reaction of the victim. When a victim organization announces a website malfunction, NoName shares the proof on Telegram and revels in the success of the attack. They also apparently search Twitter and other social networks for their group’s name, and when they find posts condemning the NoName attack, they post them on Telegram with mocking and derisive comments on screenshots. (Fig. 2)

Be wary of reacting with the full name of NoName on social media, as this could escalate the attack by pleasing or upsetting them.

1.3. NoName Targets Japan

On February 13, 2023, NoName declared on Telegram that it had launched an attack on Japan. As justification, it claimed that the attack was in retaliation for sanctions against Russia, including an oil embargo announced by the Japanese government on February 6, as well as for strengthening defense against Russia and providing economic assistance to Ukraine. [*]6 (Fig. 3)

The attacks lasted about a week and NoName claimed successful attacks on the websites of the Ministry of Economy, Trade and Industry, the Petroleum Association of Japan, construction equipment manufacturers, railway operators, electronics manufacturers, financial groups and gaming companies. The following week, NoName switched its targets to Estonia, Latvia and Sweden, and stopped publishing results of its attacks on organizations in Japan.

The week after that, on February 28, the Japanese government announced additional sanctions against Russian Federation officials, including an asset freeze, and on March 1, NoName again launched a DDoS attack targeting a Japanese organization that it had previously successfully attacked.

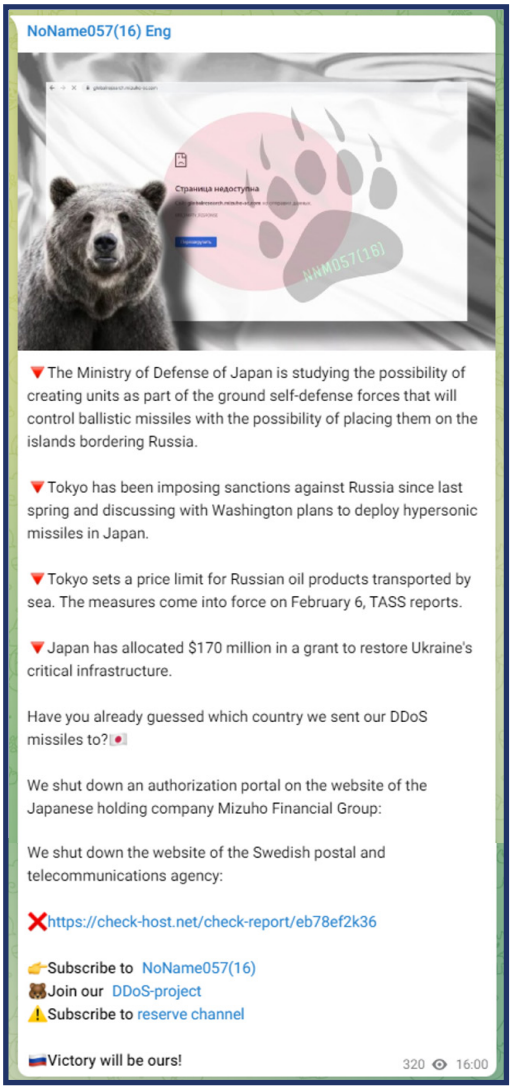

Figure 3 Telegram Post Declares Launch of Attack on Japan

Figure 4 Petroleum Association of Japan Damage Announcement: February 17

Figure 5 Petroleum Association of Japan Damage Announcement: March 1

Damage Case (1): Petroleum Association of Japan

Based on NoName's claims, the Petroleum Association of Japan appears to have been selected for attack in connection with the oil embargo. NoName announced on February 17 and March 1, around the time of the DDoS attack, that its site was becoming harder to access (Figure 4, Figure 5), apparently as a result of the attack. [*]7

Victims (2): JR East

The East Japan Railway Company (JR East) was initially able to resist DDoS attacks because of its use of a CDN (Content Distribution Network), but the attack on February 16 forced the suspension of the travel website and other information sites. [*]8 The fact that the subdomain of the targeted site contains the word "origin2-" (Figure 6) suggests that the origin server behind the CDN was sought out and attacked.

Fig. 6 JR East site apparently targeted by DDoS attack and no longer displayed

1.4. Summary

Since NoName has a pattern of DDoS attacks against countries in response to their governments' sanctions against Russia, industries related to the content of the sanctions and companies involved in critical infrastructure that could be targeted based on past attack records should be on alert for potential future attacks. It is advisable for potential targets to introduce DDoS countermeasures such as introducing the use of CDNs to protect important websites.

It is also important to protect other potential weaknesses in the attack surface, such as by limiting and protecting access to origin servers, and immediately strengthening websites once

2. Cybercrime using Google's advertising platform is on the rise

2.1. Overview

On February 9, the security company Sucuri announced that it had observed a campaign that attacked sites using WordPress and used such things as fake short URLs to lure website visitors to fraudulent advertising sites. [*]9 The attacks enabled attackers to generate ad revenue via Google Adsense by fraudulently generating ad views and clicks. The campaign began in September 2022 and has so far infected more than 10,000 sites.

There has also been an increase in attacks exploiting ads in Google's search results, revealing how the company's ad platform is being used in various ways by cybercriminals.

2.2. Attacks observed by Google Adsense and Sucuri

What is Google Adsense?

When website owners want to earn advertising revenue, they generally do not directly contract with the advertiser's company, but contract with an intermediary to distribute ads, count views, etc., and place ads on their sites and receive compensation. [*]10 "Google AdSense" is an advertising platform where Google acts as such an intermediary. [*]11 [*]12

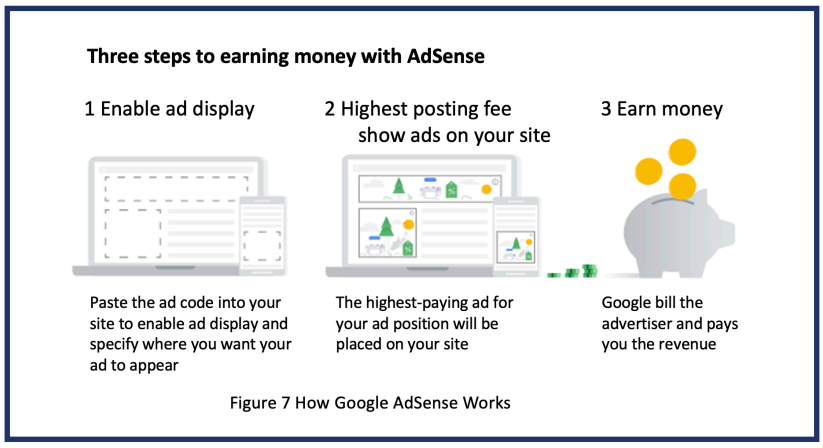

Figure 7 How Google AdSense Works 12

Google Adsense automatically selects and displays relevant ads based on content on a website and information about visitors. Users are prohibited from modifying scripts to place ads, placing violent, sexual or illegal content on pages that contain ads, enticing users to click on an ad, or misleadingly placing an ad. Any violation of these Google policies could result in the forfeiture of revenue.

Reported attack

Beginning in September 2022, malware campaigns targeting sites using WordPress were observed. [*]13 Attackers gained unauthorized access to the WordPress site in some way, such as by exploiting a plug-in vulnerability, to infect the site with malware. The malware embeds scripts in WordPress-generated Web pages. Visitors to the Web pages are repeatedly redirected through several sites to a fake Q & A site.

The embedded script was obfuscated to prevent redirects from being easily analyzed. Domains mimicking well-known redirect services such as “bit.ly” were used as redirects. Hosting the sites via them involved clever cover-ups such as using the services of Russia’s DDoS-Guard as a CDN to obscure the console’s servers (origin servers) from the outside world.

The bogus Q & A sites they were directed to included Google AdSense ads, suggesting that they were aiming to generate revenue by displaying more ads.

Figure 8
Examples of a fake URLs resembling bit.ly

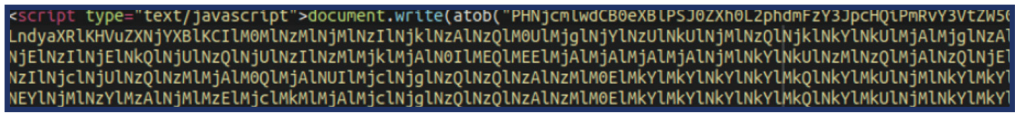

Figure 9 Obfuscated script inserted into an attacked web page

2.3. Other attacks exploiting Google ads

While Sucuri’s report was on an attempt to generate ad revenue from Google, Google ads are being used to commit crimes in other ways.

In October and December 2022, fake JR East Ekinet sites started showing up higher in search results than legitimate JR sites. [*]14 [*]15 The attack abused the manner in which Google places ads above search results. The fake sites had fields for IDs and passwords, which suggests they were fake sites designed to trick users into giving up their credentials.
There has also been a sharp increase since January in “malvertising” attacks, which target users who search for high-profile software and place ads for fake sites above legitimate sites, similar to Ekinet, tricking visitors into downloading malware. [*]16

In the past, threat actors often used to impersonate distribution sites for business-grade software like Microsoft Teams or Adobe Acrobat. This has however changed with the widespread impersonation of high-profile software download sites, not limited to business-grade software, making it difficult to predict which software downloads might be dangerous.

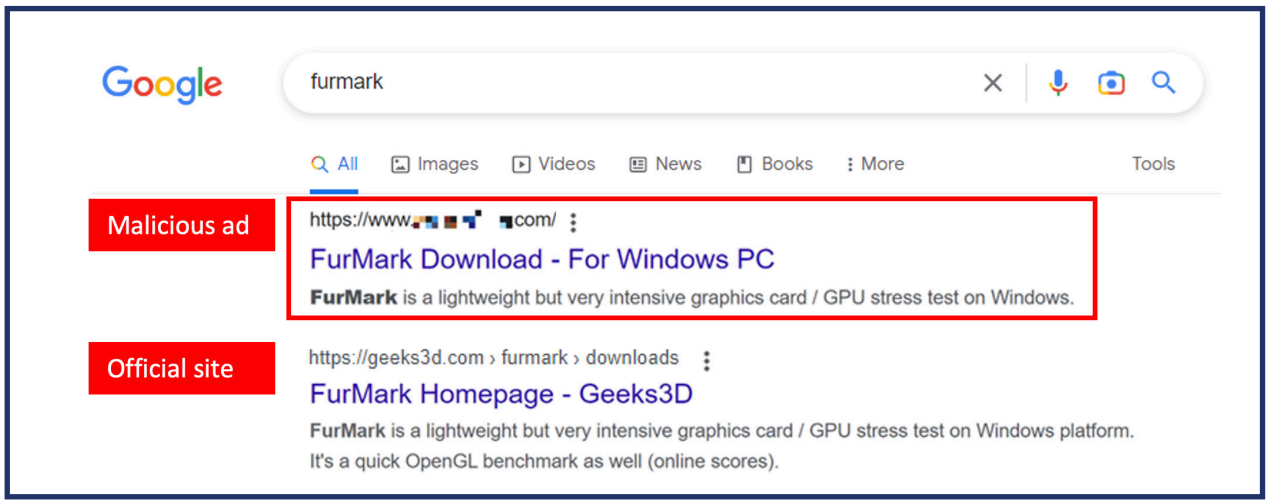

Figure 10 Example of a fake software distribution site ad in Google search results 16

The above Google ad campaign to infect malware has also been reported by security firm Guardio, and the FBI has also warned about attacks using search engine ads. [*]17 [*]18

2.4. Summary

We're starting to see a lot of cybercrime exploiting Google ads in a variety of ways. In particular, information theft and malvertising attacks that use ads in search results are dangerous things that can directly affect end users as well, underscoring the fact that Google's countermeasures haven't kept up. As an anti-phishing measure, it's recommended not to send links via SMS or email, but that assumes that the results from Google and other search engines are trustworthy – an assumption which can no longer be trusted.

Instead of trusting them unconditionally just because they are Google search results, you need to use them with the following basic precautions: check the URL to which you're transiting before you click on it, don't visit a page with a security software or browser warning, don't enter your password or personal information on a suspicious site, and avoid downloading software unless you are absolutely sure that it is genuine. [*]19 [*]20

3. Chinese hacker group Xiaoqiying carries out cyberattacks on South Korean organizations

3.1. Overview

Since the beginning of 2023, a hacker group known as Xiaoqiying (meaning “dawn cavalry” in Chinese), mostly Chinese-speaking, has carried out cyberattacks against academic and research institutions in South Korea, including website tampering and the theft of personal information. There have, in the past, been many hacker groups motivated by patriotism in China, but their activities have stagnated in recent years.

Figure 11 Tampered Korean Lesson Study Group for Social Studies Homepage Screenshot (“Declaring Korean Internet intrusion”)

3.2. Cyber attacks on South Korean organizations

(Attack notice) [*]21 [*]22

On January 7, Xiaoqiying announced on its website that it was preparing an operation against South Korea to cause a long-term data breach. On the 21st, the first day of the Lunar New Year holidays, it threatened to attack more than 2,000 South Korean government agencies and more than 30 media companies, and also said it would steal and release internal documents. In response, the Korea Internet & Security Agency (KISA), a quasi-government agency, advised companies to strengthen surveillance of their sites, block suspicious IP addresses, and report any problems to KISA.

(Attacks occurred) [*]23 [*]24 [*]25 [*]26

From the beginning of the attack, the websites of 12 academic institutions in South Korea were hacked in quick succession. The sites continued to show as unreachable or display doctored pages, and it was on February 1 that these sites were fully restored with KISA support. Based on the IP address information from the attack, the Cyber Terrorism Investigation Unit of the National Police Agency in South Korea requested international cooperation from the Interpol, the US FBI, and the Chinese Public Security Division.

Sending a message

In addition to carrying out these attacks, Xiaoqiying primarily used the messaging service Telegram to send messages. These included threats to attack KISA, and claims that it had stolen a database of 41 organizations – and not only data relating to the original 12. It appears the latter assertion may be based on data stolen from the South Korean education sector. Sarcastic claims were also made on Telegram that the Korean government was trying to cover up the magnitude of the attack. [*]27

Methods of attack [*]28 [*]29

The 12 sites compromised in January lacked security measures, including the absence of firewalls and lax system management. According to analysis by a South Korean security firm, Xiaoqiying mainly used SQL injection, which exploits vulnerabilities in Web applications to manipulate databases, as well as Web shell attacks, which can execute arbitrary commands once installed on a server.

February attacks

In February, attacks by Xiaoqiying continued, including the theft of 40,000 records containing personal and confidential information from a South Korean foundation. [*]30 The group had also listed hacking five South Korean sites as a requirement for new members to join. One who responded with details of five hacked sites, including a convenience store chain and a university, was recruited into the group. [*]31

3.3. What is Xiaoqiying?

Xiaoqiying has been ramping up its activities since the hacking of China's coal mine monitoring platform in Sichuan on December 28, 2022 23. [*]32 The group is believed to be the successor to a previously active group, Teng Snake.

Teng Snake was a group that had been active since the end of 2021. Its activites included disclosure of information stolen through hacking. In April 2022, it released several files claiming to be from Japanese mailing lists. The following month, it claimed to have hacked into the South Korean Ministry of Health's Active Directory server and sold access to the server. [*]33 Also, the data released by Xiaoqiying in early January 2023 included information that Teng Snake had disclosed with a claim that they had stolen them from a South Korean government platform. [*]34

Why Target South Korea? 23 [*]35

"I do not work for the Chinese government. Our team is a free group. Our team will use Korea as a training ground for members, each member will participate in the invasion of South Korea" the group commented on Telegram in late January. The group said it attacked South Korea in retaliation for South Korea's temporary visa restrictions on Chinese citizens (to prevent the spread of the coronavirus) and because it was annoyed by some popular South Korean streamers.

"In a bad mood, post a Korean database for fun" Xiaoqiying said afterward. However, in their message to recruit new members, they also addressed Koreans in a friendly manner (Fig. 12).

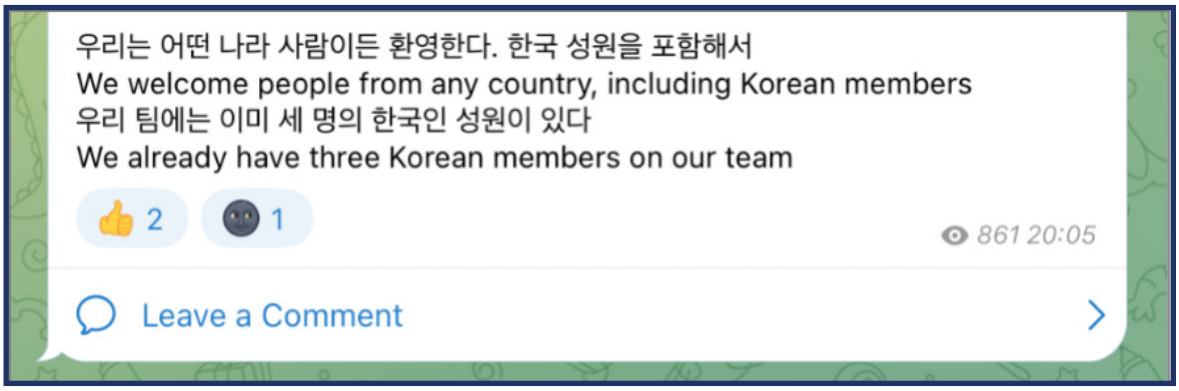

Fig. 12 Message to recruit new members (excerpt)

Xiaoqiying – further developments

On February 1, Xiaoqiying said on Telegram that it would launch a new offensive against South Korea and Japan on the 28th of the following month. [*]36 It is unclear whether this was intended to mean 'March 28' or actually meant 'February 28'. No attacks occurred on the earlier of the two dates.

On February 19, they announced on their website that they had completed the nearly month-long operation in South Korea. On Telegram, they also said that South Korea was no longer a target, and "Korea is not challenging, we will go to another network domain."
The group stopped using Telegram by the end of February as it moved its operations to another messaging service, Signal.

3.4. Attacks by Chinese hackers

China's hacking efforts [*]37 [*]38 [*]39 [*]40

China's first hacker group is said to have emerged around 1994. Since then, many groups (unlike the current APT group, which operates under the auspices of the state) have used cyberattacks as a way to spread their patriotic cause.

The hackers are thought to have started their patriotic activities in the wake of perceived "anti-China" incidents, particularly the 1998 Jakarta riots in which over 1,200 ethnic Chinese Indonesians were slaughtered, and the NATO bombing of the Chinese embassy in Belgrade the following year, which NATO claimed happened in error as a result of the CIA identifying the wrong coordinates for a Yugoslav military target in the same street. Some of these groups later evolved into prominent groups such as the Green Army, the Honker Union of China, and the China Eagle Union. These groups gained notoriety by stealing credentials, tampering with sites, and conducting DDoS attacks against foreign entities they deemed hostile to China.

Attacks on Japanese Organizations
[*]41 [*]42 [*]43 [*]44

Japanese organizations have also been targeted from time to time by Chinese hacker groups. For example, in 2011, tampering and DDoS attacks were carried out against Japanese government agencies and other sites on September 18, the day of the Liutiaohu Incident that triggered the Manchurian Incident. From 2010 to 2014, an increase in SQL injection attacks against Japan from IP addresses originating in China was observed around September 18.

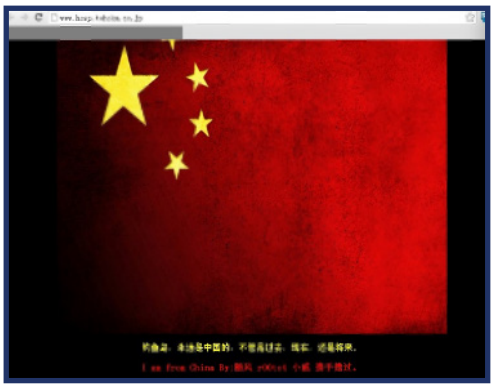

Figure 13 Tohoku University Hospital seen in September 2012

In 2012, when the Senkaku Islands were nationalized on September 11, about 300 Japanese organizations were listed as targets for attack on the Honker Union of China's bulletin board and other media. 11 of those sites were actually inaccessible, and 8 sites, including a court, were tampered with using images of Chinese flags and other materials. Chinese chat sites posted about the attacks, with 4,000 participants.

Slowing down hacker groups

It has been said that the Chinese government allows hackers to operate as long as they do not pose a danger to the state. Against this backdrop, almost every year, cyberattacks have been launched against Japanese organizations in connection with historical and political issues and anniversaries, but after the mid-2010s, similar attacks have rarely been observed.

After the inauguration of the Xi Jinping administration in 2013, censorship and surveillance on the Internet became stricter, which probably made it harder for a culture of anonymity amongst hackers to develop [*]45 [*]46 39.

The Hackers' Awakening: 46 [*]47 [*]48 [*]49 [*]50

In July 2022, someone calling himself ChinaDan put up for sale a database containing personal information on 1 billion Chinese nationals that he said had been leaked by the Shanghai National Police on an international hacker forum (also powered by Xiaoqiying). It was believed to be the largest government-backed database ever created in the world, and made headlines. The following month, a person identified as XJP listed data on 48.5 million users of a health code app that was required to be used in Shanghai as part of measures to prevent the spread of the coronavirus, along with a profile picture of Winnie the Pooh, on the same hacker forum. "XJP" also stands for Xi Jinping, and "Winnie the Pooh" is the nickname Chinese netizens have scornfully given to Xi.

It's easy to imagine how these incidents have served as a stimulus to hackers whose activities have been made more difficult by the Chinese government's censorship and surveillance regime. In fact, after the Shanghai National Police leak, the above-mentioned hacker forums became inundated with Chinese-language posts, and the existence of anonymous overseas hacking forums seems to have become widely known among Chinese hackers and would-be hackers. There have also been a number of cyberattacks around the world in the wake of Russia's

invasion of Ukraine. For example, KILLNET, a pro-Russian hacker group, claimed to have attacked Lockheed Martin and e-Gov, a Japanese e-government contact. Meanwhile, Anonymous, known as a network of cyber-attackers based on claims about human rights, politics and other issues, has taken an anti-Russian stance, hacking multiple video services, including Russian state television, and broadcasting the damage in Ukraine. It is possible that Chinese hackers, who have become aware that they can operate like overseas groups after witnessing the intense activity of hacker groups taking advantage of the global situation, have begun to take action.

3.5. Summary

China's censorship and surveillance system has not changed, but there have been situations in which anonymous Chinese speaking hackers have been able to gather by using Telegram, anonymous overseas bulletin boards and other means. Even today, many Chinese hackers remain pro-government. In those bulletin boards and Telegram, however, censorship and surveillance by the Chinese government is difficult. As a result it is conceivable that dissident activity could spread.

Contact: NTT Security Japan Inc.

OSINT Monitoring Team, Consulting Services Department

Email address: WA_Advisorysupport@ntt.com

Sources

1. Source: The Cyber Express “NoName Hits Japanese Organizations After Country Imposes Latest Sanctions on Russia”
https://thecyberexpress.com/pro-russian-hacker-noname-japanese-companies/

2. Source: Avast “Avast confirms DDoS attack by pro-Russian hacker group NoName 057 (16) against Ukraine, donor countries”
https://press.avast.com/ja-jp/pro-russian-hacker-group-targeting-sites-in-ukraine-and-supporting-countries-with-ddos-attacks

3. Source: Check Point Software “Russia Affiliated NoName 057 (16) Hacktivist Group Puts 2023 Czech Presidential Election on the Spot”
https://blog.checkpoint.com/2023/01/19/russia-affiliated-noname05716-hacktivist-group-puts-2023-czech-presidential-election-on-the-spot/

4. Source: Check Point Software “Russia Affiliated NoName 057 (16) Hacktivist Group Puts 2023 Czech Presidential Election on the Spot”
https://blog.checkpoint.com/2023/01/19/russia-affiliated-noname05716-hacktivist-group-puts-2023-czech-presidential-election-on-the-spot/

5. Source: Avast “Avast confirms DDoS attack by pro-Russian hacker group NoName 057 (16) against Ukraine, donor countries”
https://press.avast.com/ja-jp/pro-russian-hacker-group-targeting-sites-in-ukraine-and-supporting-countries-with-ddos-attacks

6. Source: the Ministry of Economy, Trade and Industry Sanctions Related to Russia and Other Countries
https://www.meti.go.jp/policy/external_economy/trade_control/01_seido/04_seisai/crimea.html

7. Source: the Petroleum Association of Japan on Twitter
https://twitter.com/paj_sekiren/status/1626379596508860419 https://twitter.com/paj_sekiren/status/1630841911748730880

8. Source: JR East (Official) on Twitter
https://twitter.com/JREast_official/status/1626037432197218306

9. Source: Sucuri “Bogus URL Shorteners Redirect Thousands of Hacked Sites in AdSense Fraud Campaign”
https://blog.sucuri.net/2023/02/bogus-url-shorteners-redirect-thousands-of-hacked-sites-in-adsense-fraud-campaign.html

10. Source: Xserver “[Monetize your blog!] Introduces mechanisms to earn advertising revenue and three standard services”
https://www.xserver.ne.jp/blog/how-to-monetize-and-popular-ad-services/

11. Source: Google AdSense
https://adsense.google.com/intl/ja_jp/start/

12. Source: Google How AdSense Works
https://support.google.com/adsense/answer/6242051

13. Source: Sucuri “Massive ois [.] is Black Hat Redirect Malware Campaign”
https://blog.sucuri.net/2022/11/massive-ois-is-black-hat-redirect-malware-campaign.html

14. Source: Sankei Shimbun, Google search for ‘Ekinetto’ - > JR East asks fake site to remove it
https://www.sankei.com/article/20221019-JW6B4XO2PBOQLLBNJSWKAHCXIU/

15. Source: ITmedia NEWS “Google search for “ekinet” leads to fake website currently hidden JR East’s response”
https://www.itmedia.co.jp/news/articles/2212/14/news169.html

16. Source: NTT Security Technical Blog “More SteelClover attacks distributing malware via Google ads”
https://insight-jp.nttsecurity.com/post/102i7af/steelclovergoogle

17. Source: TechGenix “MasquerAds – The Latest Malware Campaign That Leverages Google Ads”
https://techgenix.com/masquerads-leveraging-google-ads/

18. Source: FBI “Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users”
https://www.ic3.gov/Media/Y2022/PSA221221

19. Source: the Ministry of Internal Affairs and Communications “Accident/Damage Case > Case 17: You should have downloaded it from a famous site, but ”
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/case/17.html

20. Source: the Ministry of Internal Affairs and Communications,
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/01.html

21. Source: Digital Today - Digital Today ”중국 해커조직 국내 12개 기관 사이트 해킹…피해 확산”
https://prtimes.jp/main/html/rd/p/000000350.000001340.html

22. Source: Digital Today - “ KISA “중국 해커조직 국내 2000개 홈페이지 해킹 예고 “
https://www.digitaltoday.co.kr/news/articleView.html?idxno=468881

23. Source 디지털데일리 『[단독] “한국 인터넷 침입을 선포하다”… 中 해커에 뚫린 대한민국 보안”:
https://www.ddaily.co.kr/news/article/?no=255980

24. Source: The Korea Times “Korean websites fully restored after Chinese cyberattacks”
https://koreatimes.co.kr/www/nation/2023/02/251_344663.html

25. Source: 헤럴드경제 "경찰, '국내학술단체 해킹'에 인터폴 등 공조 공식 요청…中 협조는 미지수"
http://news.heraldcorp.com/view.php?ud=20230130000167

26. Source: 산업일보 "中 해커조직에 12개 기관 해킹… "공격 IP 확인"
https://www.kidd.co.kr/news/231090

27. Source: MBN "뉴스"[단독] 중국 해킹 조직 "피해단체, 12개 아닌 41개…한국 정부가 덮고 있나""
https://m.mbn.co.kr/news/4899057

28. Source: Byline Network "홈페이지 얼굴 바꾼 '샤오치잉'발 디페이스 해킹…대처 방안은?"
https://byline.network/2023/01/0130_01/

29. Source: 매일경제"설 연휴에 中 해커조직 공격 … "한국사회 혼란 노린듯"
https://www.mk.co.kr/today-paper/view/2023/5369469/

30. Source: Chosun Ilbo IT Chosun "中해킹조직 '샤오치잉' 韓공격 중단 선언…보안업계 "안심은 금물"
https://it.chosun.com/site/data/html_dir/2023/02/21/2023022102058.html

31. Source: 서울경제 "[단독] 편의점 CU 홈피도 뚫렸다…中 해커조직 놀이터 된 韓"
https://www.sedaily.com/NewsView/29LREYG01K

32. Source: 중앙일보 "한국 스타가 날 화나게 했다"…12개 기관 홈피 뚫은 中 해커"
https://www.joongang.co.kr/article/25135792#home

33. Source: Medium "HOTSAUCE | S2W TALON ", Teng Snake (a.k.a. Code Core)""
https://medium.com/s2wblog/%E5%8F%98%E8%84%B8-teng-snake-a-k-a-code-core-8c35268b4d1a

34. Source: 디지털데일리 "中 해커 "한국 정부가 피해 은폐" 주장, 대대적인 공격 예고했지만"
https://www.ddaily.co.kr/news/article/?no=256158

35. Source: 디지털데일리 "中 해커 "한국 정부가 피해 은폐" 주장, 대대적인 공격 예고했지만"
https://www.ddaily.co.kr/news/article/?no=256158

36. Source: 데일리시큐 "[긴급] 한국 정부·공공기관 해킹 선전포고했던 중국 '샤오치잉' 조직…새로운 공격 예고"
https://www.dailysecu.com/news/articleView.html?idxno=143239

37. Source: Infosecurity "State of Denial: The Chinese Cyber Threat"
https://www.infosecurity-magazine.com/magazine-features/state-of-denial-the-chinese-cyber-threat/

38. Source: The 930 Case of the Chinese Massacre in Indonesia, Nikkei Business Electronic Edition
https://business.nikkei.com/atcl/seminar/19/00059/082900168/

39. Source: Recorded Future "Thieves and Geeks: Russian and Chinese Hacking Communities"
https://business.nikkei.com/atcl/seminar/19/00059/082900168/https://www.recordedfuture.com/russian-chinese-hacking-communities

40. Source: ReliaQuest "Honker Union: Has the grandfather of Chinese Hacktivism returned?"
https://www.reliaquest.com/blog/honker-union-has-the-grandfather-of-chinese-hacktivism-returned/

41. Source: European Union Agency for Cybersecurity "Mariko Miya, Cyber Defense Institute, Inc. "Findings and Lessons Learned From Massive Cyber Attack Emergence Mechanisms in Japan""
https://www.enisa.europa.eu/events/2nd-enisa-conference/presentations/mariko-miya-cyber-defence-institute-japan-major.pdf

42. Source: Nihon Keizai Shimbun "Cyber damage after the nationalization of the Senkaku Islands, 19 sites NPA summary"
https://www.nikkei.com/article/DGXNASDG1904B_Z10C12A9CC1000/

43. Source: Nihon the National Personnel Authority (NPA) Keizai Shimbun
https://www.nikkei.com/article/DGXNASFK1901A_Z10C11A9000000/

44. Source: IBM Security Intelligence Blog, Attack Trends Around September 18, When the Ryujo Lake Incident Happened
https://www.ibm.com/blogs/security/jp-ja/liutiaogou-918-2016/

45. Source: "Briefing Memo, July 2020, Keiji Ono, Trends in Cyber Mercenaries," published by the National Institute of Defense Studies.
http://www.nids.mod.go.jp/publication/briefing/pdf/2020/202007.pdf

46. Source: Mercator Institute for China Studies (MERICS) "Chinese public databases leaks reveal growing dissatisfaction with authorities"
https://merics.org/en/opinion/chinese-public-databases-leaks-reveal-growing-dissatisfaction-authorities

47. Source: BBC News Japan "Why Chinese authorities censor Winnie the Pooh again? in a proposal to extend the president's term"
https://www.bbc.com/japanese/features-and-analysis-43208840

48. Source: HACKREAD "Killnet Claim They've Stolen Employee Data from Lockheed Martin"
https://www.hackread.com/killnet-hackers-hit-lockheed-martin-employee-data/

49. Source: Security NEXT "4 Departments and Agencies Fail at 23 Sites, Could Be Caused by DDoS Attack - Private Sites Fail"
https://www.security-next.com/139562

50. Source: YourAnonTV on Twitter
https://twitter.com/YourAnonTV/status/1500557635686486023


NTT
Security Holdings