Cyber Security Reports

2023.05

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 May 2023 and changes in the surrounding environment. The summary of each topic is as follows.

CHAPTER 1
“Ubiquiti Internal Fraudster Sentenced to Prison”

- In May 2023, a former Ubiquiti employee was sentenced to 6 years in prison and ordered to pay about $1.6 million in compensation, among other things. The individual was arrested at the end of 2020 while at Ubiquiti after stealing sensitive data from the company and posing as an outside hacker to blackmail the company.

- In the UK, a company employee was reportedly convicted of using an external cyberattack to impersonate the attacker and demand a ransom from the company. There are also posts on Telegram that appear to be fraudulent activities looking for outside collaborators.

- In the future, there may be an increase in incidents that straddle the boundary between internal improprieties and external cyber-attacks, and we believe that there is a need for closer coordination between organizations to address these issues.

CHAPTER 2
'SIM Swap Scams and Countermeasures as Damage Begins to Spread in Japan'

- On May 11, the National Police Agency arrested a woman in Tochigi Prefecture for illegally transferring money by misusing her phone number through online banking in a scheme called SIM Swap, which involves reissuing a SIM card for someone else's smartphone and then hijacking the phone number.

- The attacker hijacks the victim's phone number by impersonating the victim and then having the SIM card reissued. Once the takeover is complete, the attacker will be able to break through SMS authentication using the phone number, and then use banking and cryptoasset apps to send money from the victim's account to the attacker's.

- To protect against SIM swapping, if you're using SMS authentication for a critical service, we recommend switching to multi-factor authentication using FIDO, an authentication app, or a physical key.

CHAPTER 3
"NPA calls for simple website tampering checks"

- In May, the Japanese National Police Agency demonstrated a technique that applied Internet searches as a method to detect website tampering.

- Using this technique, the doctored pages appear in search results for easy verification.

- The Google Dorks method described above, which is based on Internet searches, can efficiently search a large area and help companies find security problems.

1. Ubiquiti insider gets prison sentence

1.1. Overview

In May 2023, Nickolas Sharp, a former Ubiquiti employee, was sentenced to 6 years in prison and ordered to pay substantial compensation. Sharp had been arrested while employed at Ubiquiti in late 2020 after posing as a hacker and threatening the company. [*]1 [*]2

1.2. Background of the Internal Fraud Incident [*]3

Ubiquiti is a New York City-based company that provides wireless networking products and more. Sharp, who lives in Oregon, had been with Ubiquiti since August 2018, where his responsibilities included software development and cloud infrastructure security.
Ubiquiti uses AWS and Github in its development environment, and as a senior developer, Sharp had access to credentials for both environments.

Summary of the attack

Sharp abused his access to steal a large amount of sensitive information stored in AWS and GitHub by Ubiquiti in mid to late December 2020. In addition to hiding traces of the attack, he also made it appear that 5 other Ubiquiti employees were involved in the breach.
By January 2021, Sharp had disguised himself as an outside attacker and sent emails to Ubiquiti senior employees demanding a total ransom of 50 bitcoins, worth about $1.9 million. In the emails, Sharp offered to return the stolen data without disclosing it in exchange for money.
Ubiquiti did not respond, however, and a few minutes before the payment was due, Sharp sent a message to the company on the Keybase social network saying, "No BTC. No talk (negotiation). It's done here." The message contained a link to a folder accessible to any Keybase user, to which Sharp had uploaded some of the data stolen from Ubiquiti.

Arrest

In December 2021, 1 year after the attack, Sharp was arrested on charges including wire fraud and perjury by the FBI. [*]4 On May 10, 2023, Sharp was sentenced to 6 years in prison and ordered to pay about $1.6 million in damages. [*]5

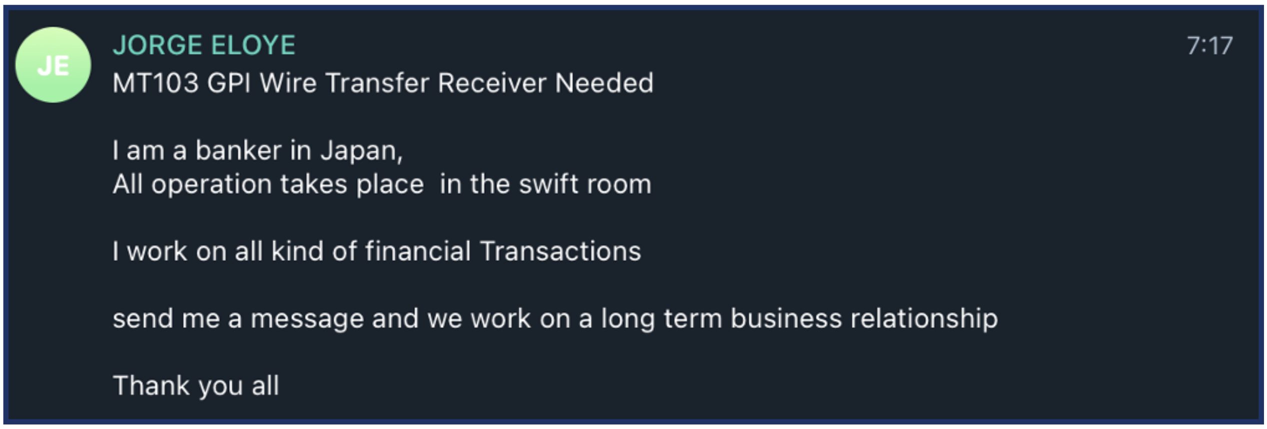
1.3. The chasm between internal fraud and cyberattacks

Sharp’s case is not the only instance of employees disguising their identity and demanding money from their organizations.

In February 2018, a company in the UK, Oxford Biomedica, was hit by a cyberattack that involved ransom demands. Ashley Liles, an employee of the company, was investigating the incident as an IT security analyst and came up with the idea of taking the ransom himself instead of the attacker. He then repeatedly compromised the private emails of the company's executives, tampering with the threatening emails sent by actual attackers, and changing the originally specified destination for the ransom to his own cryptocurrency wallet. He also impersonated the attackers with fake email addresses and pressed the company to pay the ransom, but the company never complied. Liles was arrested shortly after this.

More than 5 years later, in May 2023, he finally pleaded guilty. [*]6 [*]7

While the aforementioned Sharp and Liles cases are confirmed cases of internal fraudsters posing as outside hackers, our own team recently discovered a post on Telegram, which was unverified, by someone claiming to be a Japanese banker, seeking outside collaborators (Fig. 1). This post potentially indicates that this type of incident may be more frequent that previously suspected.



JORGE ELOYE

7:17

MT103 GPI Wire Transfer Receiver Needed

I am a banker in Japan,
All operation takes place in the swift room

I work on all kind of financial Transactions

send me a message and we work on a long term business relationship

Thank you all

Fig. 1 Posts posted by someone claiming to be a Japanese banker seeking recipients for wire transfers
*Network system for international financial transactions between banks

1.4. Summary

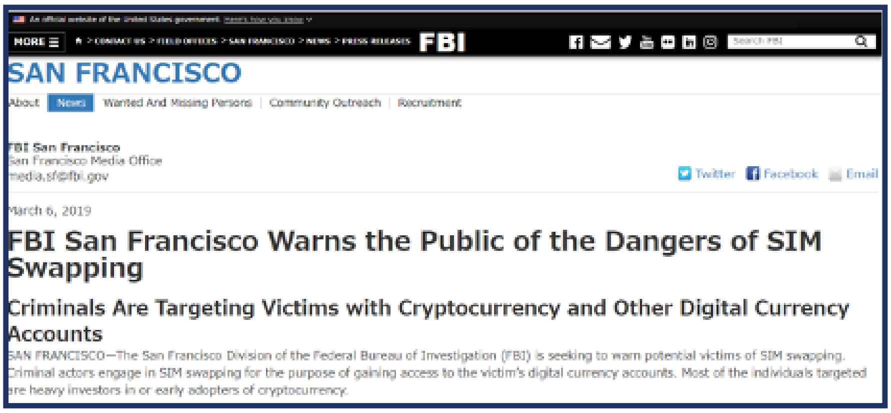
Many companies view internal fraud and external cyberattacks as separate categories of events, with different departments in charge. However, as described above, there are already various cases in which internal fraudsters incorporate cyberattacks or external collaborators into their crimes, and it is possible that this number will increase in the future. In order to respond to these cases, it is necessary to strengthen cooperation between departments within organizations and prepare for cross-category incidents.

2. SIM Swap Scams Starting to Spread in Japan and Countermeasures

2.1. SIM swap scam starting to spread in Japan

On May 11, the Japanese National Police Agency arrested a woman in Tochigi Prefecture on suspicion of hijacking a phone number by reissuing a SIM card in someone else's smartphone and using the phone number to illegally transfer money via online banking. [*]8 Since a man in Kanagawa Prefecture was arrested in January, in a scam known as SIM swapping a number of victims have been confirmed in Japan. [*]9

Incidents of this kind have been reported in the United States for about 5 years, with the first arrest in July 2018. The damage has continued to spread, especially in Europe and the United States. [*]10 [*]11 The FBI's San Francisco office has issued repeated warnings to users and mobile carriers since March 2019 **(Figure 2)**, and Europol since March 2020. [*]12 [*]13 While such tactics had already been confirmed overseas, Japan had not previously issued a public alert.


An official website of the United States government. Here's how you know
MORE ☰
CONTACT US > FIELD OFFICES > SAN FRANCISCO > NEWS > PRESS RELEASES
FBI
Search FBI
SAN FRANCISCO
About
News
Wanted And Missing Persons
Community Outreach
Recruitment
Twitter
Facebook
Email

FBI San Francisco
San Francisco Media Office
media.sf@fbi.gov

March 6, 2019

FBI San Francisco Warns the Public of the Dangers of SIM Swapping

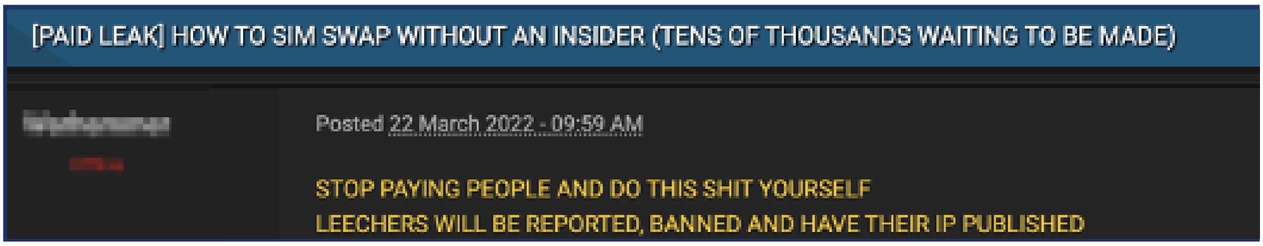
Criminals Are Targeting Victims with Cryptocurrency and Other Digital Currency Accounts

SAN FRANCISCO—The San Francisco Division of the Federal Bureau of Investigation (FBI) is seeking to warn potential victims of SIM swapping. Criminal actors engage in SIM swapping for the purpose of gaining access to the victim's digital currency accounts. Most of the individuals targeted are heavy investors in or early adopters of cryptocurrency.

Figure 2 FBI alert on SIM swaps

2.2. What is a SIM swap?

A SIM (Subscriber Identity Module) card is a small IC chip that links a subscriber to a phone number and handles communication over 4G or 5G phone lines. [*]14 By inserting it into a smartphone, you can originate phone calls, SMS, and Internet communications. Typically, it's this SIM card that manages phone numbers , not the phone itself, so you can, for example, use the same phone with a different phone number by replacing it with a SIM card from a different company. But if a malicious person takes advantage of this mechanism, they can take over the victim's phone number by pretending to be the victim and requesting the carrier to reissue the SIM card. [*]15 This is an attack technique called SIM swap, and specific information can easily be found on hacker forums and other sites.



[PAID LEAK] HOW TO SIM SWAP WITHOUT AN INSIDER (TENS OF THOUSANDS WAITING TO BE MADE)

[redacted]

[redacted]

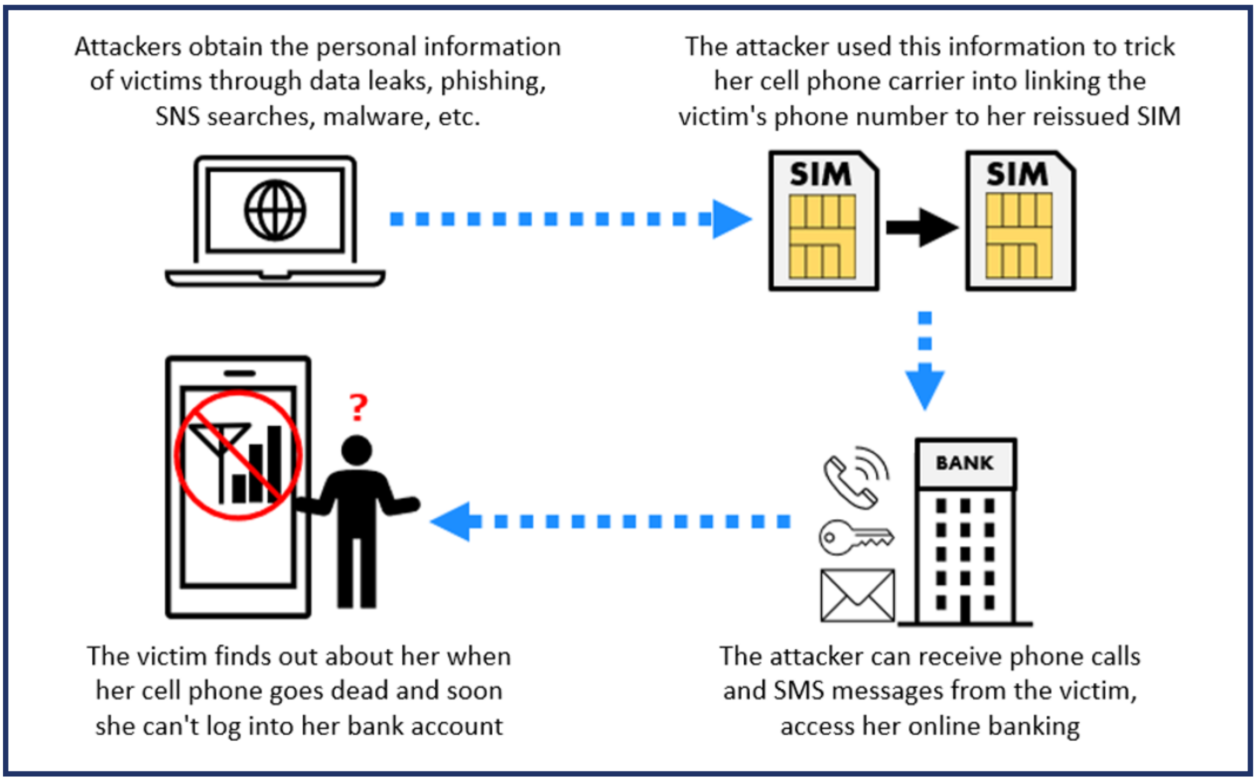
Posted 22 March 2022 - 09:59 AM

STOP PAYING PEOPLE AND DO THIS SHIT YOURSELF
LEECHERS WILL BE REPORTED, BANNED AND HAVE THEIR IP PUBLISHED

Figure 3 Hacker forum post on how to run SIM swap (modified part of image) "How to do SIM swap without insiders"

For example, an attacker first steals a target's personal information through phishing or other means, then forges an identity card. [*]16 Then, they contact the mobile carrier's support desk to impersonate the victim and request that the carrier issue a new SIM card with the same phone number either by reporting the loss of their SIM card, or going through the process of MNP switching to another carrier. This will activate the new SIM card held by the attacker and invalidate the SIM card in the victim's phone, so that phone calls, SMS, etc. will be received by the attacker's smartphone, not the victim's.

Once the takeover is complete, it will be possible to breach things like SMS authentication using phone numbers, and it will be possible to use banking and crypto apps to send money from the victim's account to the attacker's.



Attackers obtain the personal information of victims through data leaks, phishing, SNS searches, malware, etc.

The attacker used this information to trick her cell phone carrier into linking the victim's phone number to her reissued SIM

The attacker can receive phone calls and SMS messages from the victim, access her online banking

The victim finds out about her when her cell phone goes dead and soon she can't log into her bank account

Figure 4 Schematic diagram of SIM swaps (translated into Japanese and simplified with reference to Europol's reminder)

2.3. How to protect against SIM swaps

While SIM swapping attacks can involve enlisting the staff of a cellular carrier or stealing SIM cards directly, it often requires the attacker to impersonate the victim. As a way to minimize spoofing attacks and their damage, the FBI, Europol, security companies and others recommend the following measures: [*]17 [*]18

Defending against spoofing

To prevent spoofing, it is important to keep personal information private to avoid being targeted by attackers. For example, to avoid inadvertently attracting the interest of attackers by preventing information such as the possession of assets (especially crypto assets) from being transmitted via social media. As much as possible, personal information should not be registered on services on the Internet such as social media and shopping sites. Also avoid opening suspicious links and files that arrive via email or SMS as these might be phishing attacks.

Minimizing damage if attacked

SMS authentication, which involves entering numbers and keywords received via SMS, is risky because it can be breached if a SIM swap attack occurs. Instead of using SMS for authentication, users can minimize damage from SIM swapping by implementing FIDO (A method that uses biometrics and public key authentication and does not send or store passwords on the server side) or multi-factor authentication using an authentication app or physical key.

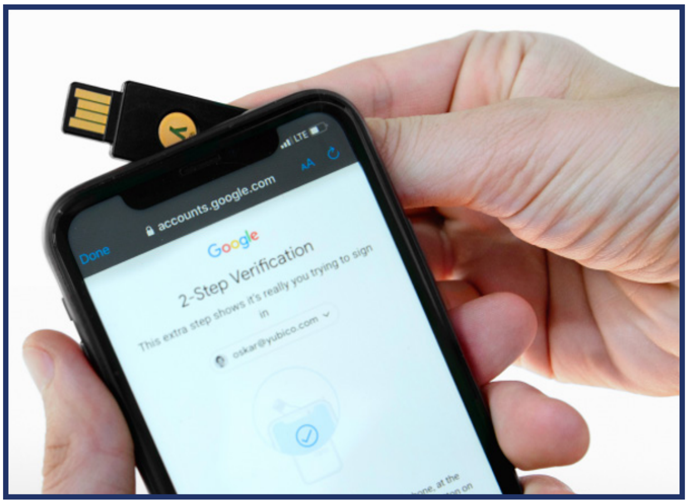


Figure 5 Example of authentication using a physical security key [*]19

2.4. Summary

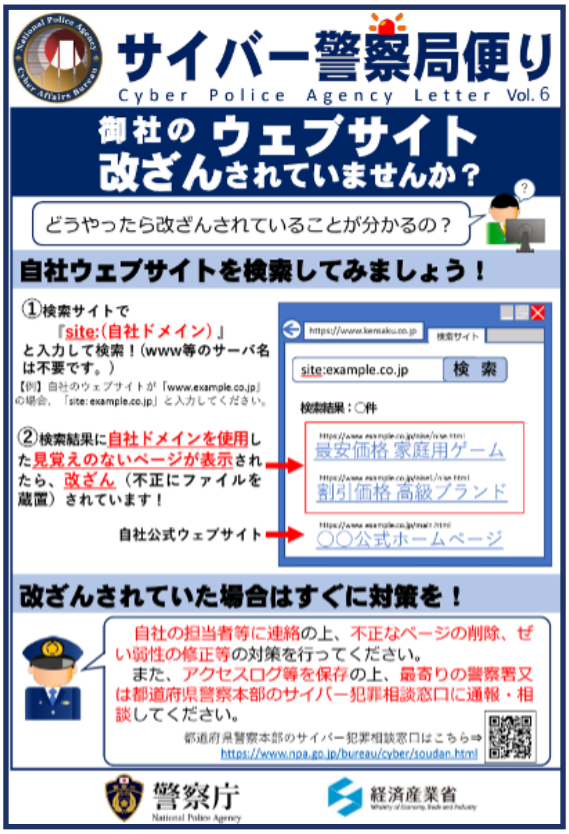
Cases of losses caused by SIM swaps have been confirmed in Japan. Overreliance on SMS authentication can lead to significant losses, including loss of assets, in the event of an attack. To reduce the risks associated with SIM swapping, it is important to avoid SMS authentication by using multi-factor authentication with FIDO, authentication apps or physical keys for critical services.

3. NPA calls for simple website tampering checks

3.1. NPA calls

The issue of threat actors compromising websites and using them to host content related to fake e-commerce sites is a problem which has been ongoing for a number of years and is a global phenomenon. In 2020, hacked Wordpress sites were being used to host scam online stores.[*]20. This raises not only the challenge of securing potentially vulnerable sites, but also the question of how site owners can more easily detect when they have been compromised. To this end, on May 8, the Japanese NPA demonstrated a method for companies that have set up websites to check if any unfamiliar pages were created on their websites, using Internet search engines such as Google (Fig. 6). [*]21

While there is no end to cases of website tampering leading to the installation of fake sites that companies do not recognize, it is not uncommon for such sites to be used by criminals for long periods of time because it is difficult to detect if a company's web pages have been damaged.



サイバー警察局便り

Cyber Police Agency Letter Vol. 6

御社のウェブサイト改ざんされていませんか？

どうやったら改ざんされていることが分かるの？

自社ウェブサイトを検索してみましょう！

①検索サイトで「site:(自社ドメイン)」と入力して検索！(www等のサーバ名は不要です。)

【例】自社のウェブサイトが「www.example.co.jp」の場合、「site: example.co.jp」と入力してください。

②検索結果に自社ドメインを使用した見覚えのないページが表示されたら、改ざん（不正にファイルを蔵置）されています！

自社公式ウェブサイト

site:example.co.jp

検索結果：〇件

改ざんされていた場合はすぐに対策を！

自社の担当者等に連絡の上、不正なページの削除、ぜい弱性の修正等の対策を行ってください。

また、アクセスログ等を保存の上、最寄りの警察署又は都道府県警察本部のサイバー犯罪相談窓口に通報・相談してください。

都道府県警察本部のサイバー犯罪相談窓口はこちら⇒ https://www.npa.go.jp/bureau/cyber/soudan.html

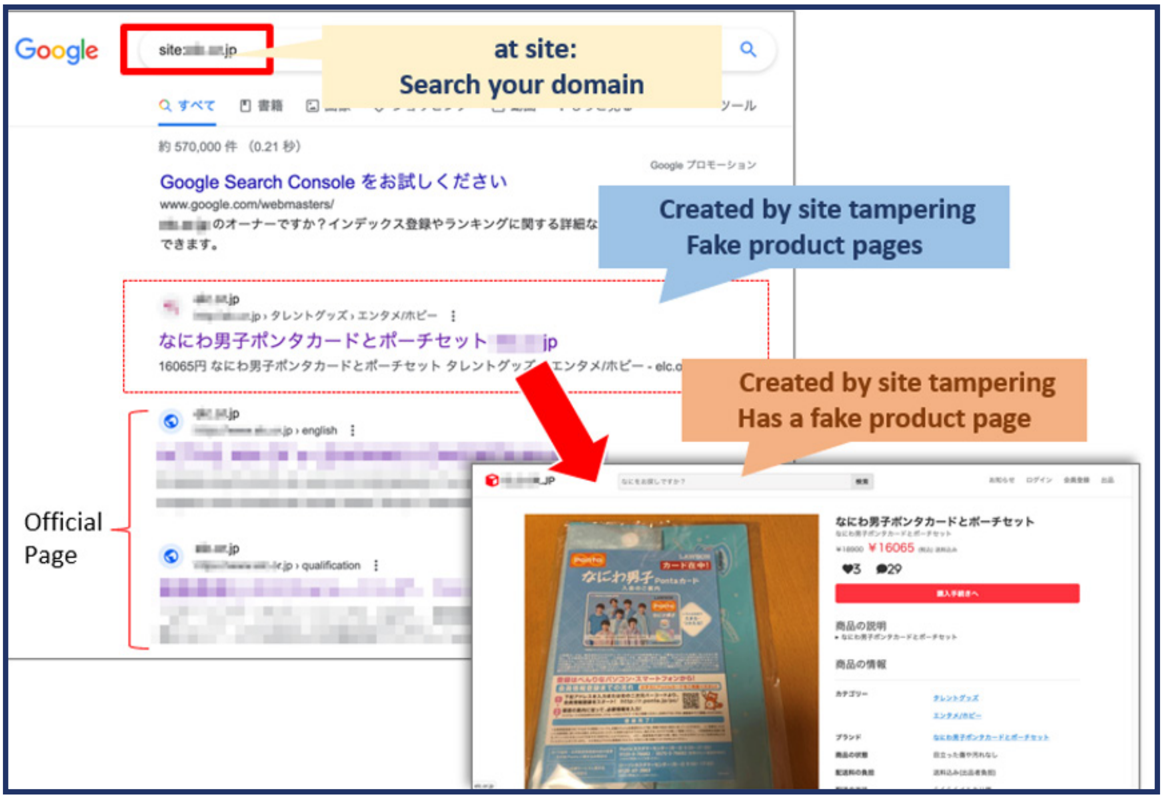
Fig. 6 " Cyber Police Bureau Bulletin" of the National Police Agency

3.2. Self-inspection of website tampering damage

Simple investigation method

The method demonstrated by the National Police Agency is simple: **Just enter the domain name of your company's website after "site:" in a search site such as Google Search, such as "site:"** [20] (Fig. 7).

When you get the search results, check to see if there are any links to pages you don't remember creating. If a page appears that has nothing to do with your business, as in the example below, chances are your website has been tampered with.



site:[redacted].jp

約 570,000 件 （0.21 秒）

Google Search Console をお試しください
www.google.com/webmasters/
[redacted]のオーナーですか？インデックス登録やランキングに関する詳細な
できます。

[redacted].jp
[redacted].jp › タレントグッズ › エンタメ/ホビー
なにわ男子ポンタカードとポーチセット [redacted] jp
16065円 なにわ男子ポンタカードとポーチセット タレントグッズ エンタメ/ホビー - elc.c

[redacted].jp
[redacted].jp › english

[redacted].jp
[redacted].jp › qualification

なにわ男子ポンタカードとポーチセット
¥16065
♥3 💬29
購入手続きへ
商品の説明
商品の情報
カテゴリー タレントグッズ エンタメ/ホビー
ブランド なにわ男子ポンタカードとポーチセット

Figure 7 Example of actual falsification found by search

Internet search and website falsification

Internet search results often show links to fake product pages like the one above. Many of these are pages set up by attackers by tampering with corporate sites, etc., with the aim of leading visitors to fake shopping sites (Fig. 8). Fake shopping sites use scams such as imitating legitimate shopping sites to trick users into paying for inferior goods or even making payment for goods which are never delivered. [*]22

Attackers indiscriminately attack sites on the Internet to improve the success rate of website tampering. This "shotgun" approach means that any site which has vulnerabilities is potentially at risk. [*]23. Even when a website is tampered with, the official pages created by the company are still displayed, making it difficult to notice anomalies. In fact, threat actors go to great length to obfuscate and hide their tampering in the hope that the website owner will not detect the tampering.

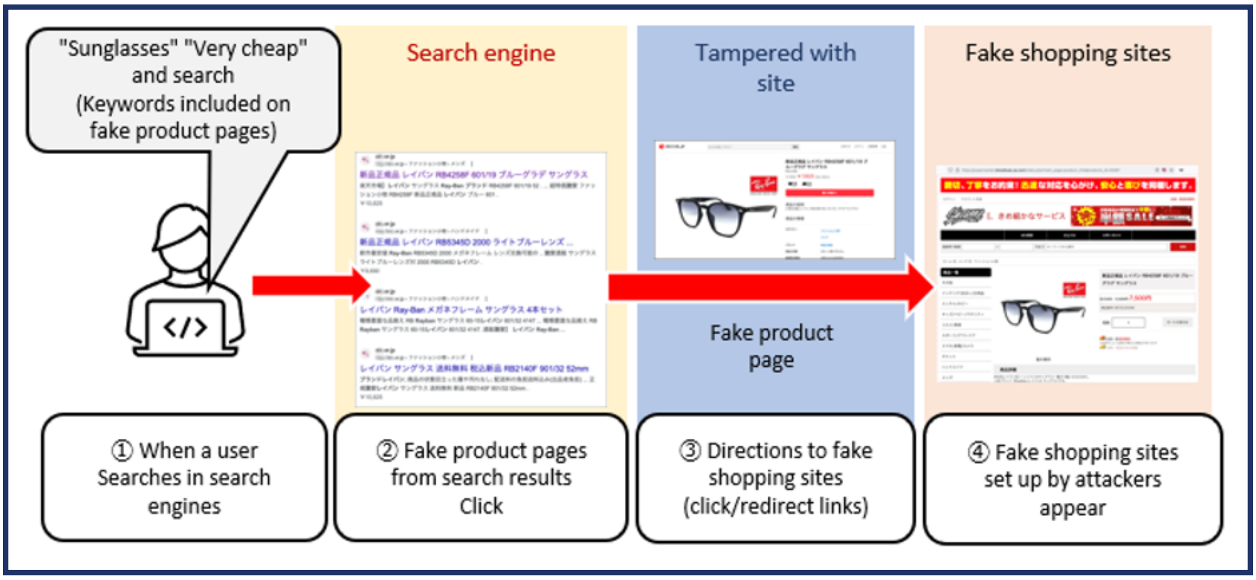

"Sunglasses" "Very cheap" and search (Keywords included on fake product pages)
Search engine
Tampered with site
Fake shopping sites
Fake product page
① When a user Searches in search engines
② Fake product pages from search results Click
③ Directions to fake shopping sites (click/redirect links)
④ Fake shopping sites set up by attackers appear

Figure 8 Using a tampered website to lead to a fake shopping site

Aim of the attackers

While general sites, such as corporate sites, receive high ratings from search engines and are more likely to appear at the top of search results, fake shopping sites are less likely to appear at the top. Attackers, therefore, are thought to be aiming to parasitize corporate sites so that they appear at the top of search results (Figure 9).

The method demonstrated by the National Police Agency takes advantage of the aim of the aforementioned attackers.

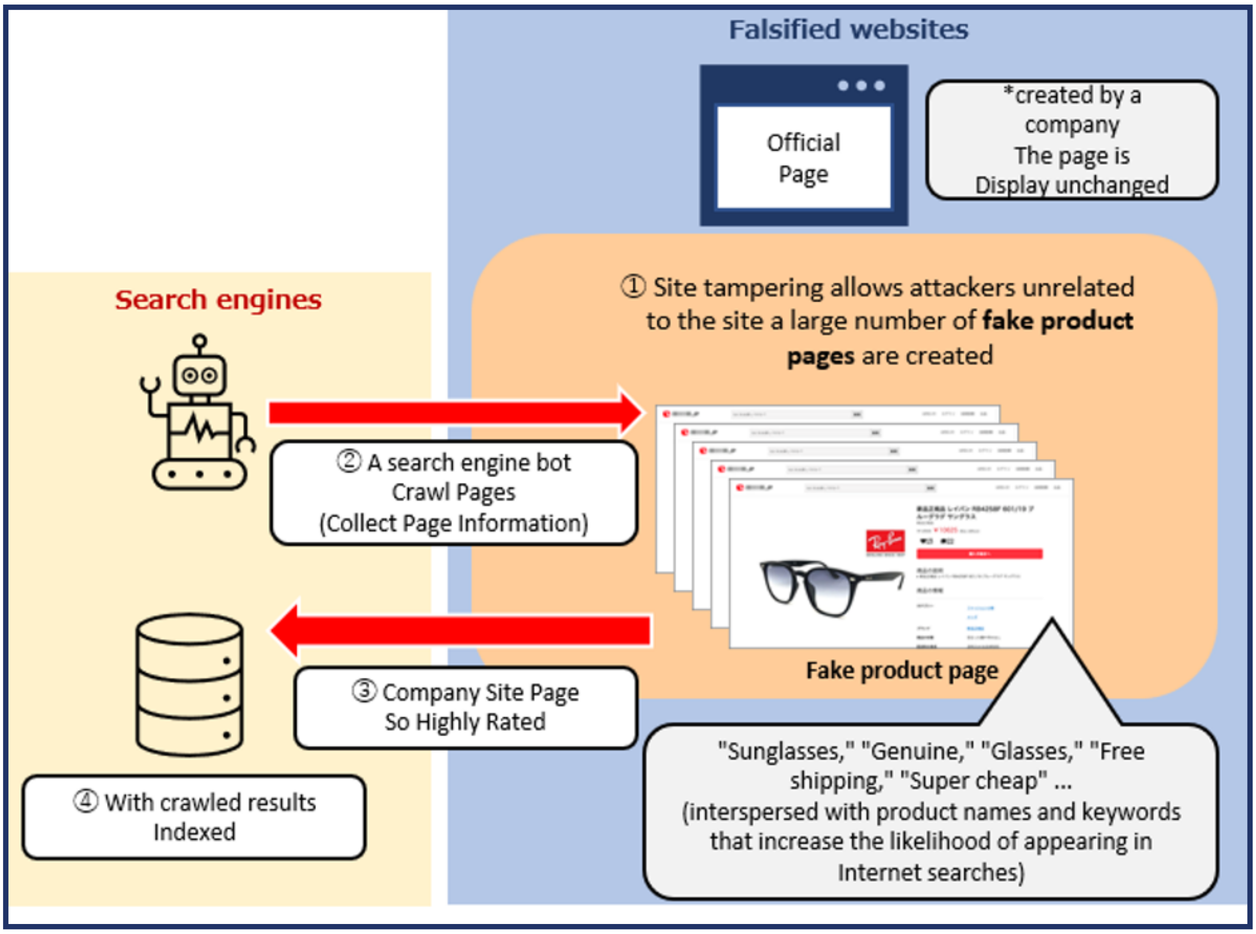
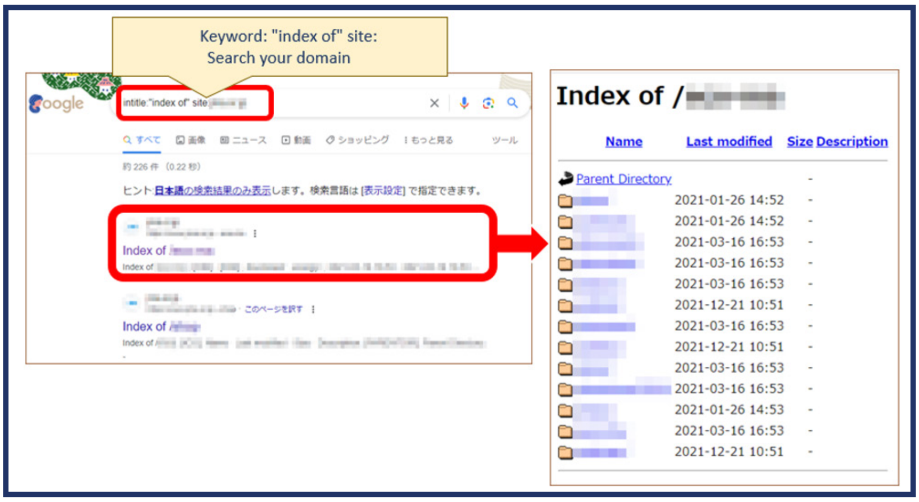

Falsified websites
Official Page
*created by a company The page is Display unchanged
Search engines
① Site tampering allows attackers unrelated to the site a large number of **fake product pages** are created
② A search engine bot Crawl Pages (Collect Page Information)
③ Company Site Page So Highly Rated
④ With crawled results Indexed
Fake product page
"Sunglasses," "Genuine," "Glasses," "Free shipping," "Super cheap" ... (interspersed with product names and keywords that increase the likelihood of appearing in Internet searches)

Figure 9 How fake product pages are registered in search engines due to website tampering

3.3. Leveraging Google Dorks techniques

The method being proposed by the NPA makes use of advanced Google search techniques known as “Google Dorks”. By investigating your own site with Google Dorks, you can not only find damage from attacks such as website tampering, but also find administrative deficiencies.

For example, a Google search on your own company’s website **intitle: "index of" site <your website URL>** will find any instances of exposed page directories (or index pages) (Figure 10). Unintentionally exposing such a page index could give attackers a hint of an attack or give them access to files that should not be visible to the outside world, such as sensitive information. Therefore, it is advisable to modify the directory settings to private once they are discovered.



Keyword: "index of" site:
Search your domain

intitle:"index of" site:[redacted]

約 226 件 （0.22 秒）

ヒント: 日本語の検索結果のみ表示します。検索言語は [表示設定] で指定できます。

[redacted]

Index of [redacted]

Index of [redacted]

[redacted]

Index of [redacted]

Index of [redacted]

Index of /[redacted]

Name	Last modified	Size	Description
Parent Directory		-	
[redacted]	2021-01-26 14:52	-	
[redacted]	2021-01-26 14:52	-	
[redacted]	2021-03-16 16:53	-	
[redacted]	2021-03-16 16:53	-	
[redacted]	2021-03-16 16:53	-	
[redacted]	2021-12-21 10:51	-	
[redacted]	2021-03-16 16:53	-	
[redacted]	2021-12-21 10:51	-	
[redacted]	2021-03-16 16:53	-	
[redacted]	2021-03-16 16:53	-	
[redacted]	2021-01-26 14:53	-	
[redacted]	2021-03-16 16:53	-	
[redacted]	2021-12-21 10:51	-	

Figure 10 Directory Screen Discovered by Google Search

There are a number of other Google Dorks that are also useful for security.
Here are some examples (Table 1):

Search Keywords (＊＊＊＊.jp is the company's website)	Research purpose	Remarks
inurl:backup site:○△□.jp	Check if the URL containing the string "backup" exposes backup data	Backup data may contain sensitive information
ext:log site:○△□.jp	Check if log data with extension ".log" is exposed	Log may contain ID/password

Table 1 Examples of Google Dorks Search Keywords

3.4. Summary

Google Dorks is a convenient way to efficiently survey a large area that would take a long time to sift through web pages one by one and discover security problems and administrative errors. Why not look for ways to take advantage of it for your company?

Disclaimer

While we do our best to be accurate in the content of this article, we do not guarantee its accuracy and will not compensate you for any damages or losses arising from your use of this article. If you have any questions or concerns regarding typographical errors, errors in content, or other matters pointed out in the article, please contact us at the address below.

Contact: NTT Security Japan Inc.

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

Sources

1. Source: SecurityWeek "Former Ubiquiti Employee Who Posed as Hacker Sentenced to Prison"
https://www.securityweek.com/former-ubiquiti-employee-who-posed-as-hacker-sentenced-to-prison/

2. Source: U.S. Department of Justice "Former Employee Of Technology Company Sentenced To Six Years In Prison For Stealing Confidential Data And Extorting Company For Ransom"
https://www.justice.gov/usao-sdny/pr/former-employee-technology-company-sentenced-six-years-prison-stealing-confidential

3. Source: Condé Nast "UNITED STATES DISTRICT COURT, SOUTHERN DISTRICT OF NEW YORK "GOVERNMENT'S SENTENCING MEMORANDUM REGARDING DEFENDANT NICKOLAS SHARP""
https://cdn.arstechnica.net/wp-content/uploads/2023/05/US-v-Sharp-Sentencing-5-11-2023.pdf

4. Source: U.S. Department of Justice "Former Employee Of Technology Company Charged With Stealing Confidential Data And Extorting Company For Ransom While Posing As Anonymous Attacker"
https://www.justice.gov/usao-sdny/pr/former-employee-technology-company-charged-stealing-confidential-data-and-extorting

5. Source: U.S. Department of Justice "Former Employee Of Technology Company Sentenced To Six Years In Prison For Stealing Confidential Data And Extorting Company For Ransom"
https://www.justice.gov/usao-sdny/pr/former-employee-technology-company-sentenced-six-years-prison-stealing-confidential

6. Source: South East Regional Organised Crime Unit "Man prevailed of blackmail and other offences"
https://serocu.police.uk/man-convicted-of-blackmail-and-other-offences/

7. Source: Bleeping Computer "IT employee personnel ransomware gang to export employee"
https://www.bleepingcomputer.com/news/security/it-employee-impersonates-ransomware-gang-to-extort-employer/

8. Source: Sankei Newspaper, Japan's Metropolitan Police Department Arresting a Woman on Charges of Sim Swap Fraud or Withdrawing Money Under the guise of Someone Else
https://www.sankei.com/article/20230511-75NGJHDMMBJGZL2QFQMFUC3QLE/

9. Source: Yomiuri Shimbun "Fraudulent acquisition of someone else's SIM card, forged driver's license ... smartphone hijacking, money transfers"
https://www.yomiuri.co.jp/national/20230127-OYT1T50032/

10. Source: Bleeping Computer, Third SIM Swapper Arrested in the US
https://www.bleepingcomputer.com/news/security/third-sim-swapper-arrested-in-the-us/

11. Source: VICE "'TELL YOUR DAD TO GIVE US BITCOIN: 'How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers"
https://www.vice.com/en/article/a3q7mz/hacker-allegedly-stole-millions-bitcoin-sim-swapping

12. Source: FBI "FBI San Francisco Warns the Public of the Dangers of SIM Swapping"
https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/fbi-san-francisco-warns-the-public-of-the-dangers-of-sim-swapping

13. Source: Europol on Twitter
https://twitter.com/europol/status/1238378996179574787

14. Source: SIM(Subscriber identity module) card on NTT West
https://www.ntt-west.co.jp/business/glossary/words-00067.html

15. Source: SIM SWAPPING - A mobile phone scam on EUROPOL
https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/sim-swapping-%E2%80%93-mobile-phone-scam

16. Source: Norton Blog "What is SIM swapping? SIM swap fraud explained and how to help protect yourself"
https://us.norton.com/blog/mobile/sim-swap-fraud

17. Source: FBI "Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public"
https://www.ic3.gov/Media/Y2022/PSA220208

18. Source: EUROPOL, SIM SWAPPING - A MOBILE PHONE SCAM
https://www.europol.europa.eu/cms/sites/default/files/documents/sim_swapping.pdf

19. Source: Yubico, Yubico Authenticator
https://www.yubico.com/products/yubico-authenticator/

20. SourceL ZDNet: “Malware creates scam online stores on top of hacked WordPress sites” https://www.zdnet.com/article/malware-creates-online-stores-on-top-of-hacked-wordpress-sites/

21. Source: National Police Agency "Cyber Police Bureau Bulletin Vol. 6 "Has your company website been tampered with?" (reminder)"
https://www.npa.go.jp/bureau/cyber/pdf/Vol.6cpal.pdf

22. Source: Japan Cyber Crime Center (JC3), Beware of Fake Shopping Sites
https://www.jc3.or.jp/threats/topics/article-462.html

23. Source: National Police Agency, Countermeasures against Website Tampering
https://www.npa.go.jp/bureau/cyber/countermeasures/hacked-website.html

NTT Security Holdings