Cyber Security Reports

2023.03

NTT Security Japan Inc.

OSINT Monitoring Team, Consulting Services Department

NTT Security Holdings

Content

About this report

In this report, we have selected and summarized 3 topics that are considered to be especially notable among the various information security incidents and events that occurred during March 2023. The following summaries provide brief overviews of these three topics:

CHAPTER 1
"Blackbaud pays $3 million for botched disclosure of cyberattack"

- On March 9, the United States' Securities and Exchange Commission (SEC) announced that Blackbaud, a cloud software company, had agreed to pay $3 million to settle disclosures that led investors to misjudge the 2020 ran somware attack that stole more than 1 million files.
- In its initial statement, Blackbaud denied that the attackers had unauthorized access to bank account information and other information, When in fact access did occur. It also failed to disclose information in a timely manner. The SEC considered these to be important issues.
- This incident also highlights the fact that it is an important responsibility for investors to ensure that policies and procedures are reviewed and prepared by members of a company's board of directors or their technology and security departments to inform them timeously of any incidents that may occur.

CHAPTER 2
"The APT Activities of Kimsuky, a North Korean Hacker"

- In March, targeted emails believed to be from Kimsuky, a North Korean APT group, were detected. Aiming to steal information related to the situation on the Korean Peninsula, Kimsuky carried out malware attacks against South Korean government agencies, think tanks and experts, as well as against Japan, the United States, Russia and European countries.
- In response to the flurry of activity, German and South Korean intelligence agencies called attention to Kimsuky's attacks which involved clever schemes to use browser extensions and Google account syncing on Android devices. North Korea's cyber-attacks occur against the backdrop of its ongoing missile development. Kimsuky's activities are likely to continue. This kind of activity represents an evolving threat of infiltration which requires vigilance from security teams.

CHAPTER 3
"Owner of BreachForums, the world's largest hacker forum, arrested"

- On March 15, the FBI arrested New York resident Conor Brian Fitzpatrick, owner of BreachForums, the world's largest hacker forum.
- Fitzpatrick, who identified himself as "pompompurin," was a well-known cybercriminal on the dark net. He used Tor and VPN connections to hide his real whereabouts, but the FBI was able to determine that he was pompom-purin by analyzing data which included the database of RaidForums, which was shut down last year.
- The FBI also obtained the BreachForums database as part of this investigation. Analysis of the database is ex pected to help identify other cybercriminals who were active on the forum.

1. Blackbaud pays $3 million for botched disclosure of cyberattack

1.1. Overview

On March 9, 2023, the US Securities and Exchange Commission (Hereafter, SEC) announced that Blackbaud had agreed to pay a $3 million civil penalty to SEC to settle charges related to misleading disclosures of a 2020 ransomware attack that resulted in investors being misled. [*]1

Figure 1 Press Release by SEC

1.2. About Blackbaud

Blackbaud is a cloud software company headquartered in Charleston, South Carolina. [*]2 It provides CRM (customer relationship management software) to a variety of nonprofit organizations, including charities, schools, higher education institutions, medical institutions, and religious/cultural organizations. Through its services, it raises and invests more than $100 billion annually Over $100 billion has been fundraised on its platform and is used in more than 100 countries. [*]3 It is publicly traded on the NASDAQ, with revenues of $1.1 billion in 2022. [*]4

Figure 2 Blackbaud HQ

1.3. Ransomware attack

Unauthorized access revealed

Starting in February 2020, someone had been illegally accessing Blackbaud's systems. The company's technical staff discovered this on May 14 of that year. By the 20th, the cybersecurity team, with the help of law enforcement and others, blocked the attackers' entry route, preventing employees from losing access to the system and attackers from fully encrypting files. Unfortunately some copies of the data had already been deleted (and stolen) from the company's self-hosted environment. The attackers continued to attempt to regain access to the system, but by June 3 they stopped their attempts. [*]5 [*]6

The attackers left multiple messages on the company's systems saying they had stolen data about customers and were demanding a ransom in bitcoin, and on June 18 they notified the company which files they had stolen. [*]7 [*]8

The company's cybersecurity officials consulted third-party vendors and contacted the attackers. In the end, Blackbaud paid a ransom in exchange for the attackers' promise to destroy the data they had on hand. [7.] No group or person has been publicly identified as responsible for the attack.

Disclosure of the incident [7]

On July 16, Blackbaud disclosed the breach for the first time and also notified affected customer organizations. The company said the attackers did not access credit card information, bank account details or Social Security numbers. However, this determination was not based on the contents of the leaked files, but rather on an analysis of file names.

In the days following the disclosure of the incident, Blackbaud received more than 1,000 communications from client organizations. Many organizations raised concerns, including that sensitive data about donors, such as those listed above, were stored in unencrypted data areas.

About payment of ransom

At the time of disclosure of the incident, a Blackbaud spokesperson said that the company had been working with third-party experts to communicate with cybercriminals and paid ransoms when there was reliable confirmation that data copies had been destroyed. As a precaution, it had hired an outside party to monitor the Internet, including the dark web, but had found no evidence that the breach had been made public. [*]9 The company's press release also stated that, given the nature of the incident and the findings of the investigation, there was no reason to believe any data was misused or released. [*]10

However, there was no objective way to verify whether a criminal really has destroyed data, and Blackbaud's decision to take the other person's word for it and pay the ransom drew criticism. In 2020, as now, the FBI did not recommend or support victims to pay ransoms. This is because there are no assurances that attackers will not retain or exploit stolen data, or that organizations will regain access to it (if systems are encrypted). Rather there is also a possibility that payment of ransoms will embolden attackers to target more organizations in the future, or that other criminals will become interested in and involved in ransomware attacks. [*]11 [*]12

Victims [7] **[*13] [*]14 [*]15**

More than 1 million files were compromised in the attack, which included a variety of customer data, including individuals' names, addresses, donation histories, and information about their spouses and assets.

More than 13,000 organizations, or about 1/4 of the company's customers, were affected by the data breach. These included the British Labour Party and the international human rights group Human Rights Watch. The number of individuals further affected is believed to be more than 10 million in healthcare alone. Others, such as the Boy Scouts of America alumni network of 50 million, raised concerns about the widespread impact of the breach.

1.4. Updating Important Information

Revision of Disclosure Information

On September 29, the company filed a material affairs report, Form 8-K, on the incident with SEC, **saying that in the cases of some of the impacted customers, cybercriminals may have accessed unencrypted data including Bank account information, Social Security numbers, user names and passwords.** [*]16 The new facts were also notified to the customers involved, but it had already been two and a half months since the incident was made public.

Blackbaud Company Struggling to Respond

About 570 customers in the United States, United Kingdom and Canada demanded reimbursement for costs related to the incident, according to Blackbaud's 2020 annual report. [*]17 There were also 30 consumer class action lawsuits filed in the United States and Canada alleging damages from Blackbaud's alleged actions/inactions related to the incident. Blackbaud took a $10.4 million charge this year (for payments, including legal fees, to primarily third-party service providers and consultants, and increased cybersecurity measures) to address the incident. The estimated recovery from insurance was $9.4 million.

Securities Act Violations and Settlement with SEC [17] **[*]18 [*]19**

In the United States, SEC investigates and prosecutes companies for information leaks caused by cyberattacks.

In a press release dated March 9, 2023, SEC said it found Blackbaud had violated (several provisions contained in) two securities laws:

The first is the Securities Act of 1933, which deals with the disclosure obligations of stock companies. This makes it illegal to obtain money or property by making a false statement or omission of a material fact in the offering/sale of securities, etc., and to engage in a transaction, practice or business process that is believed to be fraudulent or to function as a fraud against the purchaser. The second is the Securities Exchange Act of 1934, which requires reporting to SEC. It requires bond issuers to file quarterly reports with the Commission pursuant to the Commission's rules, to include any material information in order to ensure that the statements required in such reports are accurate, and to maintain disclosure controls and procedures to process the information required to be disclosed in reports filed under this Act within the time

period specified by the Commission's rules. Blackbaud, without acknowledging or denying the Commission's findings, agreed to cease the violations and pay a $3 million civil penalty to settle the case.

1.5. Problems with Blackbaud's response

The SEC stated that "Public companies have an obligation to provide their investors with accurate and timely material information; Blackbaud failed to do so" [1]. The commission took particular issue with two points:

1. Inadequate internal reporting system and delayed disclosure of updates [7] [*]20

Days after Blackbaud cited several important types of personal information and said they had not been accessed when the incident was disclosed on July 16, its technical and customer relations staff learned that the attackers had access to donors' bank account information (stored in unencrypted form) and Social Security numbers. Nevertheless, **none of the officials reported this fact to the top management responsible for the company's disclosures. There were also no policies or procedures for reporting.** Thus, while the incident was mentioned in the quarterly report, Form 10-Q, dated August 4, there was no mention of unauthorized access to the above critical data. It is possible that the senior management did not learn the facts until weeks after the report was submitted.

In addition to these management flaws, the fact that it took about two and a half months from the initial disclosure of the incident until its update in late September drew scrutiny from SEC.

2. Assuming Facts [7] [20]

The aforementioned August quarterly report noted: “A compromise of our data security that results in customer or donor personal or payment card data being obtained by unauthorized persons could adversely affect our reputation with our customers and others, as well as our operations, results of operations, financial condition and liquidity and could result in litigation against us or the imposition of penalties.”

Commenting on the statement, the SEC said that Blackbaud's technical and customer relations personnel were aware of unauthorized access to bank account information and other information, but the company failed to include this important information in its quarterly reports, **making a misleading statement that was based on assumptions about the risk of leaking confidential donor information.** This problem, too, was caused by a lack of policies and procedures in place to properly communicate information internally, so it is likely that the most senior management was unaware of this. (It was not intended to purposefully omit important information or mislead investors).

1.6. New cybersecurity rules

In 2011 and 2018, SEC issued Interpretive Guidance, which provided the Commission's views on how existing rules should be interpreted for disclosure of cybersecurity risks and incidents. [*]21 Since then, however, according to the Commission, while organizations have made improvements in both handling of material security incidents and disclosure of security risk management and governance, disclosure practices have been inconsistent. [*]22

In an effort to revise the above guidance, in March 2022, the Commission released draft cybersecurity regulations, in which it listed a variety of new requirements. For example, it required organizations to disclose (1) critical incidents (Timing of disclosure is within four days of the organization's judgment that an incident occurred), (2) corporate cybersecurity policies, procedures, and governance, and (3) cybersecurity expertise of directors. [*]23 Given that the cybersecurity rules are expected to be finalized in April 2023, it is expected that the SEC will continue to actively investigate and prosecute cases.

1.7. Summary

The 2018 interpretive guidance from SEC requires companies to "Establish and maintain appropriate and effective disclosure controls and procedures to enable accurate and timely disclosure of important events, including cybersecurity related events" and also tells companies to consider whether they need to reconsider/update past disclosures (even during the investigation of a security incident) [23.] [*]24 Blackbaud's failure to follow this guidance led to a failure to adequately inform investors of material information, which also caused confusion among many client organizations and individuals.

SEC's new cybersecurity rules, which require disclosure within four days of critical incidents being confirmed, are expected to take effect soon. The EU's General Data Protection Regulation (GDPR) also requires data breaches to be reported to regulators within 72 hours of becoming aware of them.

It is also an important responsibility for investors to ensure that policies and procedures are reviewed and prepared among corporate boards and members of technology and security to ensure smooth disclosure of information about incidents that may occur suddenly, including ransomware attacks.

2. North Korean hacker Kimsuky's APT activities

2.1. Overview

In March 2023, a targeted email was detected targeting experts on North Korea in South Korea and thought to be from Kimsuky, an APT group affiliated with North Korea. Kimsuky has long been active in sending targeted emails carrying malware infections to South Korea for cyber-espionage purposes, including information theft and account hijacking.
In the same month, German and South Korean intelligence agencies issued a joint alert (Fig. 3) on Kimsuky's activities. [*]25

Fig. 3 Joint reminder by the German Federal Bureau of Investigation (BfV) and the South Korean National Intelligence Service (NIS) [*]26

2.2. About Kimsuky

The main external intelligence agency tasked with gathering intelligence and conducting covert operations in North Korea is the Reconnaissance General Bureau (RGB). Kimsuky is an APT group (Figure 4) that is thought to be affiliated with the RGB and has been operating since around 2012. [*]27

Kimsuky conducts cyber espionage activities targeting government agencies, think tanks and experts for the purpose of gathering information on foreign and security issues, nuclear policies and economic sanctions. The activities have been confirmed to have targeted South Korea, as well as Japan, the United States, Russia and European countries.
Attacks use techniques such as social engineering, spear-phishing and waterhole attacks to infect targets with malware and then steal information. Attack campaigns targeting South Korean media and think tanks have been identified since early 2022, and South Korea's National Police Agency said that between April and October 2022, Kimsuky sent targeted emails to hundreds of foreign and security experts, stealing lists of personal information and email addresses. [*]28 [*]29

A panel of experts from the UN Security Council's North Korea Sanctions Committee, which reported on Kimsuky's activities to date in its annual report released on April 5, 2023, places Kimsuky as one of the leading APT groups in North Korea, along with the Lazarus Group (APT 38) and others known for attacks targeting crypto assets. [*]30 [*]31

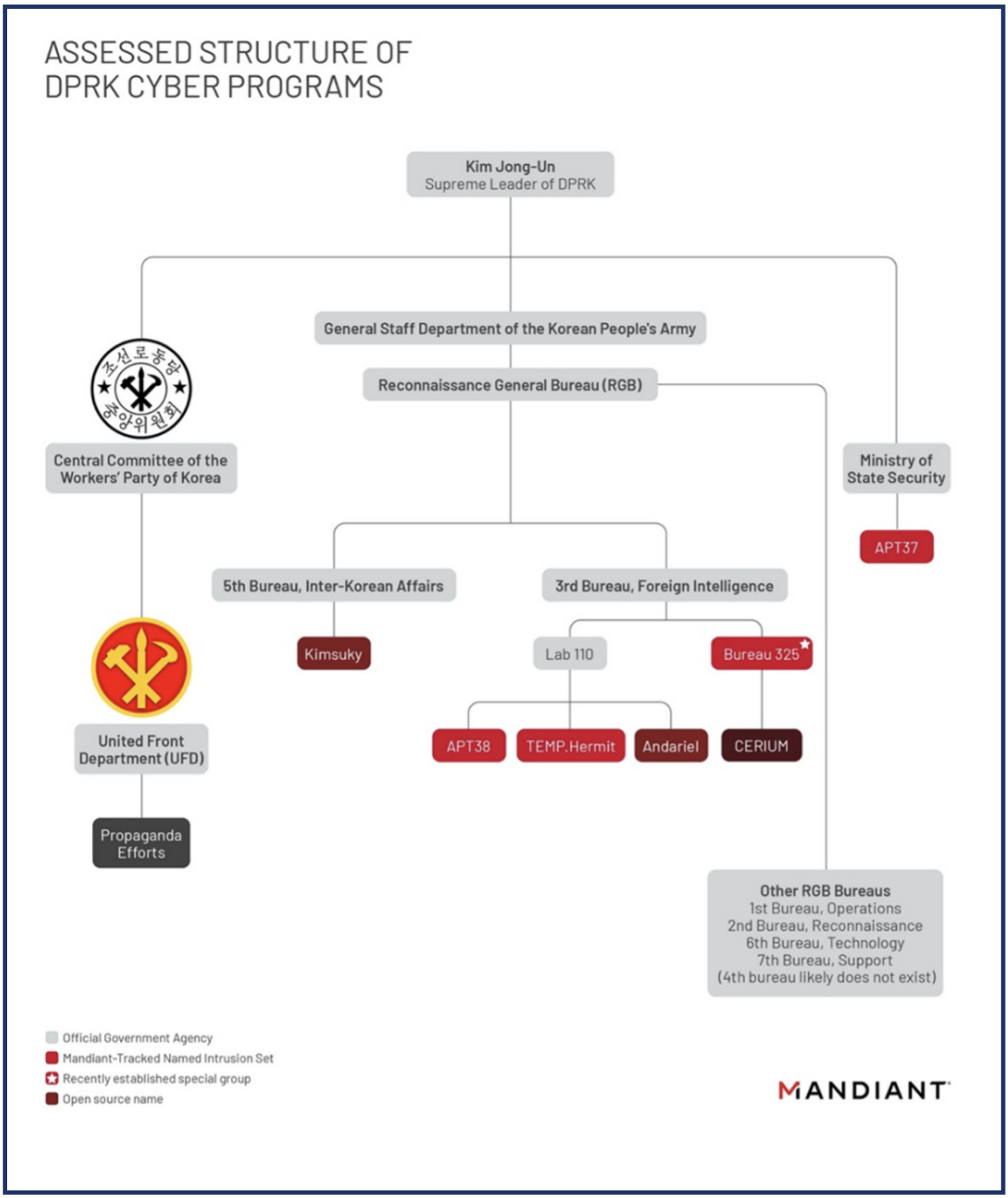


Figure 4 Kimsuky in the North Korean Cyber Attack Organization Chart [*]32
(* Kimsuky's location is circled in red in the figure created by Mandiant.)

2.3. Kimsuky's recent targeted email attack

On March 7, 2023, experts on North Korea in South Korea received a targeted email. The sender's name was spoofed to a current news reporter at KBS, South Korea's public television station. The subject line read, "KBS. I want an interview with KBS." The text requested an interview with an expert with knowledge of the relationship between North Korea's rapidly rising missile threat and external affairs, and requested a response (Fig. 5).

When the recipient responded to the request, they would receive an email with a ZIP file attached (Fig. 6). Analysis by South Korean security firm AhnLab found that the ZIP file contained a CHM file (a Windows help file) disguised as a questionnaire, and that opening the CHM file would run a script to infect it with information-stealing malware. [*]33

Figure 5 Targeted emails disguised as KBS coverage [*] 34

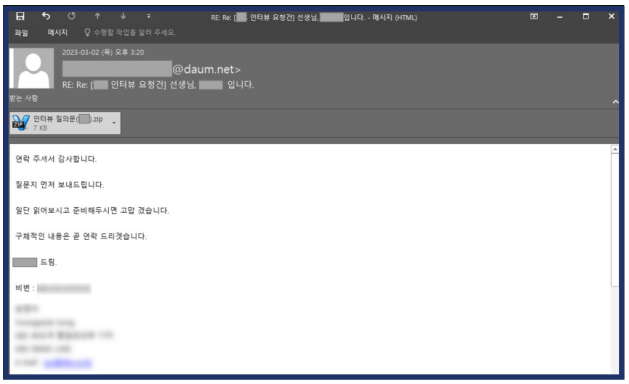


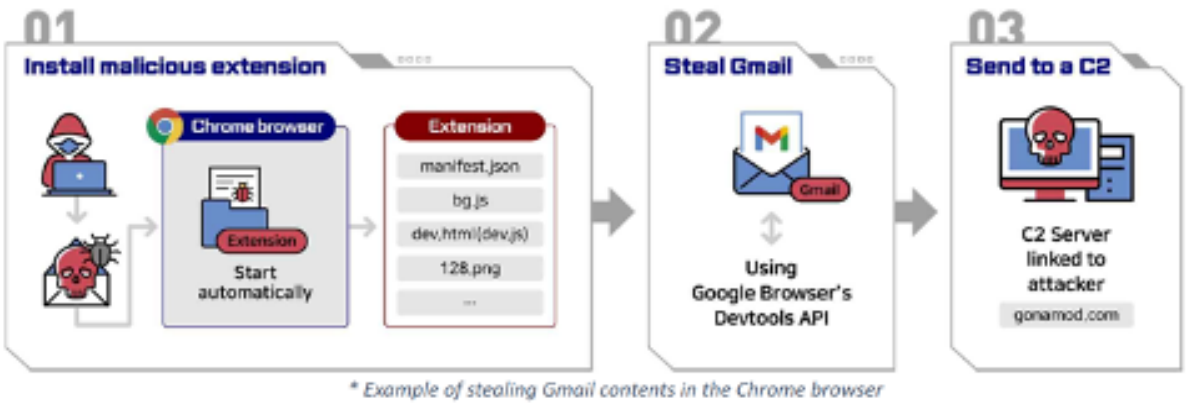
Figure 6 File attachment emails received in reply [*]35

Based on the similarity to previously identified targeted attacks, the attack was assessed to have been carried out by Kimsuky. Other emails disguised as coming from South Korea's National Pension Service and the Cyber Safety Bureau of the National Police Agency were observed around the same time. They are also believed to be targeted attacks initiated by North Korea's APT group.

2.4. Intelligence agency issues alert on Kimsuky

On March 20, the German Federal Bureau of Investigation (BfV) and South Korea's National Intelligence Service (NIS), both intelligence agencies, issued a joint alert on Kimsuky's active cyber espionage activities. [*]36 The joint alert appears to be prompted by Kimsuky's use of targeted email to target South Korean and German entities over the past several years. It goes on to warn that an analysis of recently observed attack campaign techniques indicates that the attacks have escalated to targeting "global think tanks in diplomacy and security with North Korea."

The alert outlines another form of information-stealing, using targeted emails as an entry point, that differs from the March attack described earlier. There are two types of attacks, one in which malicious browser extensions are installed (Fig. 7), and the other in which malicious apps are automatically delivered to Android devices (Fig. 8). It is believed that these attacks circumvent security settings such as two-factor authentication and create a backdoor, with the aim of continuing to steal information without the target noticing.

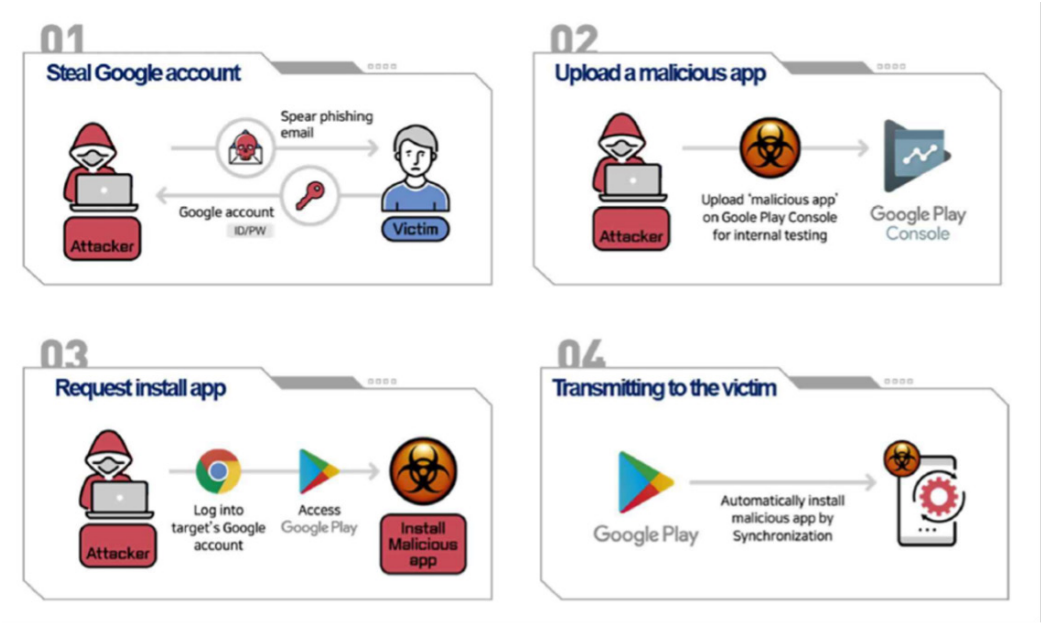


1 Targeted emails induce users to install malicious browser extensions linked to emails

2 Installed browser extensions steal Gmail account contents

3 Browser extension sends stolen information to attacker's server

Figure 7 Browser extension for information theft, installed through targeted mail attack (from reminder)



1 Steal target's Google account through targeted mail

2 Upload malicious apps to developer's Google Play account

3 Unauthorized access to stolen target's Google account. Register the account on the developer's Google Play

4 Malicious apps from Google Play are automatically delivered to Android devices tied to the target's Google account

Figure 8 Malicious app installation on Android devices through targeted mail attack (from reminder)

2.5. Summary

In its most recent annual report, the UNSC Sanctions Committee on North Korea recommended that Ri Chang-ho, director general of the Reconnaissance General Bureau, which oversees the Kimsuky and other groups (Fig. 9), be added to the sanctions list, suggesting that the international community is alarmed by the activities of the North Korean APT group. [*]37 [*]38 Also, on April 7, 2023, in a joint statement expressing strong condemnation of North Korea's repeated ballistic missile launches and moves to develop nuclear weapons, senior officials from Japan, the United States, and South Korea expressed deep concern over money theft, money laundering, and intelligence gathering through malicious cyber activities in support of North Korea's national interests. [*]39 [*]40 Now that North Korea is escalating its threats, Kimsuky's cyber espionage activities are expected to continue to flourish, and we need to be vigilant against various evolving means of infiltration, as noted in the alert.

Figure 9: Li Changho Director General, Reconnaissance General Bureau

3. Owner of BreachForums, the world's largest hacker forum, arrested

3.1. Overview

On March 15, the FBI arrested Conor Brian Fitzpatrick of New York, owner of BreachForums, the world's largest hacker forum. [*]41 He identified himself on the darknet as a Japanese character called pompompurin.
Around March 20, as a result of a takedown, the BreachForums website became unavailable and displayed an error to anyone visiting the site.

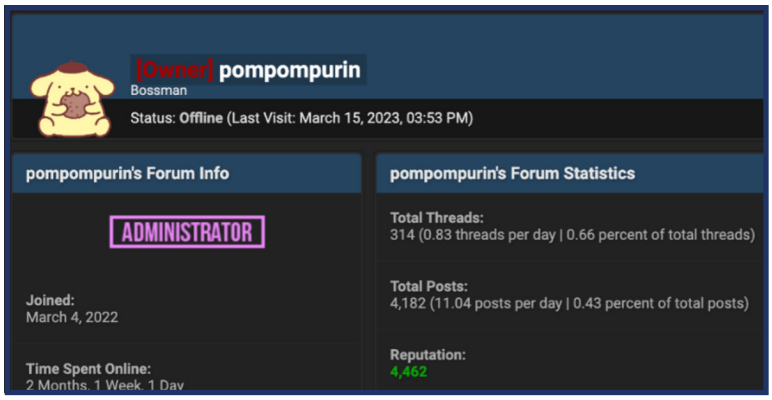


Figure 10 Fitzpatrick's profile screen

Figure 11 BreachForums error screen

3.2. What is BreachForums?

BreachForums was founded in April 2022 by a man who identified himself as pompompurin. It was a hacker forum where the sale and purchase of leaked information stolen through cyberattacks and the exchange of information about attack methods were conducted. It opened shortly after another hacker forum, RaidForums, which was the largest in the world at the time, was shut down by a joint Western investigation. As a result, it started by recruiting RaidForums' users and then proceeded to attract more hackers. By June of that year, it handled more than 10.9 billion records of compromised data. Pompompurin posted that it had "surpassed the number of records on RaidForums," making BreachForums the largest hacker forum in the world.

Figure 12 Post claims to have overtaken RaidForums

3.3. 'Pompompurin' and the circumstances of his arrest

Who is pompompurin?

Fitzpatrick, who went by the name "pompompurin" on the dark net, was active on the RaidForums and Russian hacker boards before BreachForums launched. Before that, he was a well-known cybercriminal who attacked a variety of companies and organizations, including hacking FBI mail servers to send fake email alerts from legitimate FBI email addresses notifiying recipients that their systems were being attacked and their data was being stolen, and stealing and selling customer data from Robinhood, a popular investment app in the United States. [*]42 [*]43

Background of his arrest

When Fitzpatrick acted as pompompurin, he usually used Tor or a VPN connection to keep his source IP address secret so that his real whereabouts remained unknown. [*]44 But when the VPN connection failed, the FBI detected that he was logging into BreachForums' system from his own provider's IP address. This was one of the decisive factors in his arrest.

Separately, the FBI also owns a closed RaidForums database, whose analysis also provided evidence leading to the arrest. For example, in chatting with the owner of RaidForums about the leaked database of an app used by pompompurin, the FBI found that he told them that his email address "**conorfitzpatrick02** @ gmail [.] com" was not included in the leaked database. [*]45 In addition, they were able to obtain records from Google showing that Fitzpatrick was actually using that address. Building on this evidence, the FBI determined and confirmed that Fitzpatrick was the pompompurin.

3.4. Moves to close BreachForums

In addition to Fitzpatrick, BreachForums had several other administrators. One of them, who goes by the name "Baphomet", posted messages on Telegram and his own site telling people what was going on in an attempt to keep the community alive. After Fitzpatrick's arrest, Baphomet initially considered shutting down BreachForums and moving it into a new environment. However, the discovery of a login history that did not belong to him or his associates, led to the suspicion that the FBI might be using Fitzpatrick's PC and information such as his ID/password to access the platform and copy data and source code. As a result, Baphomet and the remaining administrators decided to close BreachForums because they were concerned that even the source code may have been acquired by authorities. They set up a group on Telegram where users can join and talk to each other about what the future holds, but so far there's been no concrete action on opening a new forum.

Although several new hacker forums have sprung up since the shutdown, Baphomet insists he has nothing to do with them. To date, none appear to be attracting users as quickly as BreachForums did after the closure of RaidForums. [*]46

3.5. Summary

After the closure of RaidForums, the owner of BreachForums, which effectively took over as the world's largest hacker forum, was arrested and the forum was shut down. The remaining administrators, including Baphomet, also appear to be exercising caution, having failed to launch a new forum at this time. The closure of BreachForums seems to have dealt a significant blow to its administrators and users.

The FBI also obtained the BreachForums database as part of this investigation. Its analysis is expected to help identify other cybercriminals who were active on the forum.

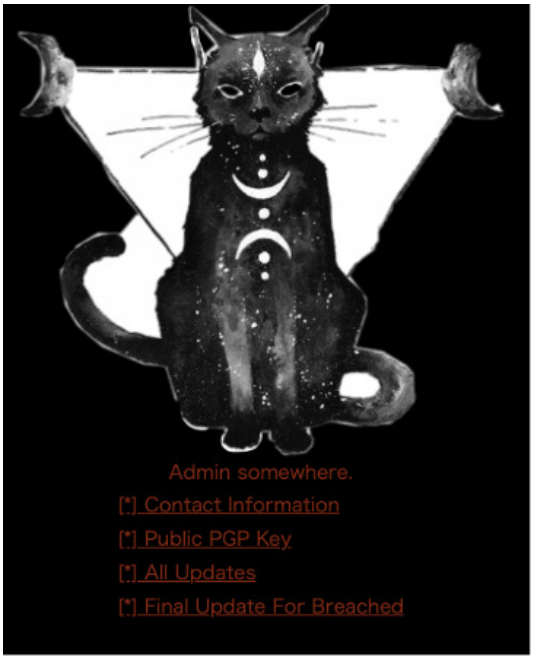


Figure 13 The Baphomet Website

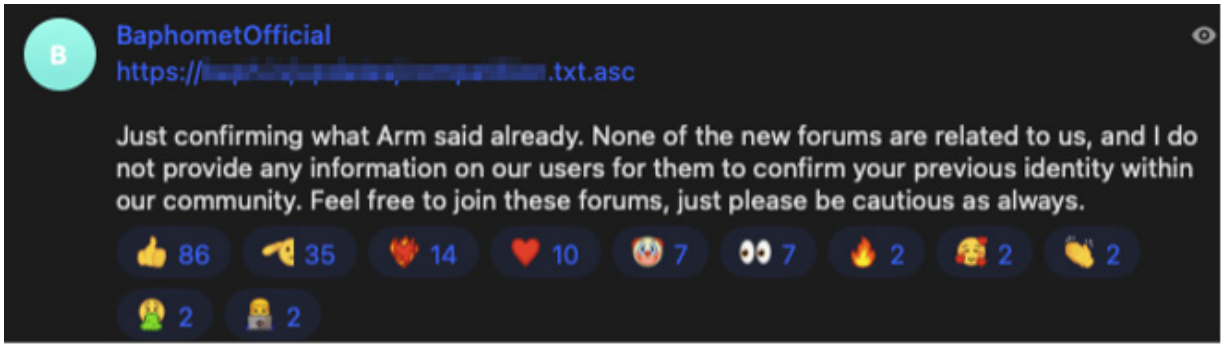


Figure 14 Baphomet's Telegram Post That Emerging Forums Have Nothing To Do With them

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: U.S. Securities and Exchange Commission "SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors"
https://www.sec.gov/news/press-release/2023-48

2. Source: The Post and Courier "SC tech firm's cyberattack sent shockwaves across the globe and frustrated customers"
https://www.postandcourier.com/business/sc-tech-firms-cyberattack-sent-shockwaves-across-the-globe-and-frustrated-customers/article_dd46954a-eb88-11ea-8eb5-4ffd4b680168.html

3. Source: About Blackbaud
https://www.blackbaud.com/company

4. Source: Blackbaud "Blackbaud Announces 2022 Fourth Quarter and Full Year Results"
https://www.blackbaud.com/newsroom/article/2023/02/13/blackbaud-announces-2022-fourth-quarter-and-full-year-results

5. Source: The NonProfit Times "The Hack Of Blackbaud: Damage Is Still Being Assessed"
https://thenonprofittimes.com/npt_articles/the-hack-of-blackbaud-damage-is-still-being-assessed/

6. Source: HealthITSecurity "Blackbaud Ransomware Hack Affects 657 K Maine Health System Donors"
https://healthitsecurity.com/news/blackbaud-ransomware-hack-affects-657k-maine-health-system-donors

7. Source: U.S. Securities and Exchange Commission "ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTION 8 A OF THE SECURITIES ACT OF 1933 AND SECTION 21 C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER"
https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf

8. Source: VeroNews.com Thieves steal Vero Beach Museum of Art's donor info
https://veronews.com/2020/08/13/thieves-steal-vero-beach-museum-of-arts-donor-info/

9. Source: The NonProfit Times "Breaking: Blackbaud Hacked, Ransom Paid"
https://thenonprofittimes.com/npt_articles/breaking-blackbaud-hacked-ransom-paid/

10. Source: BankInfoSecurity "Blackbaud's Bizarre Ransomware Attack Notification"
https://www.bankinfosecurity.com/blogs/blackbauds-insane-ransomware-attack-notification-p-2929

11. Source: Top Class Actions "How Did the Blackbaud Ransomware Attack Occur?"
https://topclassactions.com/lawsuit-settlements/privacy/ransomware/how-did-the-blackbaud-ransomware-attack-occur/

12. Source: Federal Bureau of Investigation (Ransomware)
https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

13. Source: TechCrunch "SEC charges Blackbaud for failing to disclose 'full impact' of ransomware attack"
https://techcrunch.com/2023/03/10/sec-blackbaud-charged-ransomware/

14. Source: The HIPAA Journal "Blackbaud SEC Filing Provides Further Information on Data Breach and Mitigation Costs"
https://www.hipaajournal.com/blackbaud-sec-filing-provides-further-information-on-data-breach-and-mitigation-costs/

15. Source: The Dallas Morning News "Bush Presidential Center, Boy Scouts, Texas Tech, UT Austin hit in Blackbaud ransomware attack"
https://www.dallasnews.com/business/technology/2020/08/03/bush-presidential-center-boy-scouts-of-america-texas-tech-foundation-among-hundreds-hit-in-blackbaud-ransomware-attack/

16. Source: Blackbaud, Form 8-K
https://investor.blackbaud.com/static-files/58a4ae64-afc5-45f7-81df-69dfc93888fc

17. Source: Blackbaud, Form 10 -K (2020 Annual Report)
https://investor.blackbaud.com/static-files/61e8a7e6-73d1-4e28-8c81-fd3013107288

18. Source: SOMPO CYBER SECURITY, What is the U.S. Securities and Exchange Commission?
https://www.sompocybersecurity.com/column/glossary/sec-us

19. Source: U.S. Government Publishing Office (SECURITIES ACT OF 1933)
https://www.govinfo.gov/content/pkg/COMPS-1884/pdf/COMPS-1884.pdf

20. Source: Blackbaud, Form 10 - Q
https://investor.blackbaud.com/static-files/370a20eb-ef91-42cd-a212-e9b743b26ed1

21. Source: Deloitte "SEC Proposals New Requirements for Cybersecurity Disclosures"
https://dart.deloitte.com/USDART/home/publications/deloitte/heads-up/2022/sec-proposal-cybersecurity-disclosures

22. Source: U.S. Securities and Exchange Commission "FACT SHEET Public Company Cybersecurity; Proposed Rules"
https://www.sec.gov/files/33-11038-fact-sheet.pdf

23. Source: Cleary Cybersecurity and Privacy Watch "SEC Charges Public Company For Alleged Misleading Disclosures Surrounding Ransomware Attack"
https://www.ddaily.co.kr/news/article/?no=255980

24. Source: U.S. Securities and Exchange Commission "Commission Statement and Guidance on Public Company Cybersecurity Disclosures"
https://www.sec.gov/rules/interp/2018/33-10459.pdf

25. Source: Recorded Future "North Korean APT group 'Kimsuky' targeting experts with new spearphishing campaign"
https://therecord.media/north-korea-apt-kimsuky-attacks

26. Source: German Federal Office for the Defence of the Constitution "Bundesamt für Verfassungsschutz-Counter-intelligence - Joint Cyber Security Advisory"
https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/EN/2023/2023-03-20-joint-cyber-security-advisory.html

27. Source: MITRE ATT & CK "Kimsuky, STOLEN PENCIL, Thallium, Black Banshee, Velvet Chollima, Group G0094"
https://attack.mitre.org/groups/G0094/

28. Source: Kaspersky "Kimsuky's GoldDragon cluster and its C2 operations | Securelist"
https://securelist.com/kimsukys-golddragon-cluster-and-its-c2-operations/107258/

29. Source: Hankyoreh Newspaper "A North Korean hacker group poses as a South Korean 'reporter and congressman's office'"
http://japan.hani.co.kr/arti/politics/45493.html

30. Source: United Nations Security Council Sanctions Committee on North Korea "Final report of the Panel of Experts submitted purchasers to resolution 2627 (2022)"
https://undocs.org/S/2023/171

31. Source: The Yomiuri Shimbun "North Korea Cyber Attack Steals Cryptographic Assets $1 billion ... 2022"
https://www.yomiuri.co.jp/world/20230406-OYT1T50082/

32. Source: Mandiant "Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations"
https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government

33. Source: AhnLab CHM malware disguised as a survey on North Korea - ASEC blog
https://asec.ahnlab.com/jp/49306/

34. Source: RFA "KBS"
https://www.rfa.org/korean/in_focus/nk_nuclear_talks/hacking-03082023084805.html

35. Source: AhnLab "CHM malware disguised as a survey on North Korea (Kimsuky) - ASEC blog"
https://asec.ahnlab.com/jp/49306/

36. Source: German Federal Office for the Defence of the Constitution "Bundesamt für Verfassungsschutz-Counter-intelligence - Joint Cyber Security Advisory"
https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/EN/2023/2023-03-20-joint-cyber-security-advisory.html

37. Source: Unification Ministry of the Republic of Korea, North Korea information portal,
https://nkinfo.unikorea.go.kr/nkp/theme/viewPeople.do?menuId=PEOPLE&nkpmno=2307

38. Source: United Nations Security Council Sanctions Committee on North Korea "Final report of the Panel of Experts submitted purchasers to resolution 2627 (2022)"
https://undocs.org/S/2023/171

39. Source: the Ministry of Foreign Affairs, Trilateral Consultations on North Korea (Results)
https://www.mofa.go.jp/mofaj/press/release/press1_001412.html

40. Source: Reuters "US, S. Korea, Japan concerned over N. Korea's' malicious' cyber activities"
https://www.reuters.com/world/asia-pacific/us-south-korea-japan-express-concern-over-nkoreas-malicious-cyber-activities-2023-04-07/

41. Source: Bleeping Computer "Alleged BreachForums owner Pompompurin arrested on cybercrime charges"
https://www.bleepingcomputer.com/news/security/alleged-breachforums-owner-pompompurin-arrested-on-cybercrime-charges/

42. Source: Bleeping Computer "FBI system hacked to email 'urgent' warning about fake cyberattacks"
https://www.bleepingcomputer.com/news/security/fbi-system-hacked-to-email-urgent-warning-about-fake-cyberattacks/

43. Source: Bleeping Computer "Robinhood discloses data breach impacting 7 million customers"
https://www.bleepingcomputer.com/news/security/robinhood-discloses-data-breach-impacting-7-million-customers/

44. Source: Bleeping Computer "FBI confirms access to Breached cybercrime forum database"
https://www.bleepingcomputer.com/news/security/fbi-confirms-access-to-breached-cybercrime-forum-database/

45. Source: TechCrunch "How the FBI caught the BreachForums admin"
https://techcrunch.com/2023/03/24/how-the-fbi-caught-the-breachforums-admin/

46. Source: Bleeping Computer "Breached shutdown sparks migration to ARES data leak forums"
https://www.bleepingcomputer.com/news/security/breached-shutdown-sparks-migration-to-ares-data-leak-forums/


NTT
Security Holdings