Cyber Security Reports

2023.06

NTT Security Japan Inc.

Consulting Services Department OSINT Monitoring Team

NTT | Security Holdings

Content

About this report

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

CHAPTER 1

“CISA issues binding operational directives for exposed management interfaces"

- CISA, which oversees the U.S. government's security efforts, issued a "binding operating directive" (BOD23 – 02) that directs all government agencies not to expose their management interfaces to the Internet in the wake of frequent network intrusions.

- The directive requires that management interfaces be restricted to access only from internal networks so that they cannot be accessed from the Internet.

- The directive is limited to U.S. government agencies, but we recommend that private companies follow suit.

CHAPTER 2

Ransomware hits Shalom, a software-as-a-service for Labor and Social Security Attorney offices

- MKSystem, the provider of “Shalom”, a software-as-a-service (SaaS) platform that supports social insurance services procedures, was hit by a ransomware attack, which disrupted work at Labor and Social Security Attorney offices, etc., that use the software.

- If a system that handles personal information is damaged by a cyberattack and may leak information, it must report the incident to Personal Information Protection Commission, Japan. In this case, not only MKSystem but also Labor and Social Security Attorney offices (as contractors) that use Shalom and their client companies are required to report the incident.

- In order to respond to the reporting requirement promptly even if personal information is leaked from SaaS, companies are required to identify and cooperate with the contractors of customer and employee personal information.

CHAPTER 3

Hacker forum BreachForums revived after owner's arrest

- On June 13, BreachForums, the world's largest hacker forum, returned to action after a three-month hiatus. As before the shutdown, there has been a lot of discussion about posting various leaks and hacking.

- Soon after the shutdown, rival forums were hit with DDoS attacks and hacks, but there has been no significant impact, and the number of users has been growing steadily.

- BreachForums is likely to continue to be a leading community among hackers, and we need to be vigilant about what is posted and what hackers are doing.

1. CISA issues binding operational directives for exposed management interfaces

1.1. Overview

On June 13, 2023, the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued a binding operating directive, BOD23 – 02. [*]1

The directive, which applies to devices belonging to the US Federal Civilian Executive Branch (Hereinafter referred to as "U.S. Government Agencies"), enforces measures to mitigate the risk of cyberattacks when a "management interface" for configuring and managing a network is exposed to the Internet.

Possible cases that need to be handled includes, for example, that the login screen of the Web management portal, which should be used only by users of the organization, is accessible to anyone from the Internet.

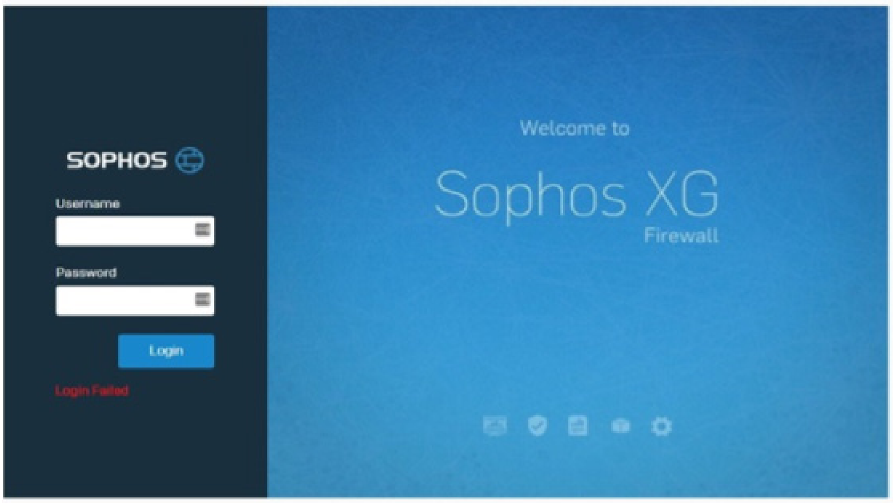


Figure 1 Login screen of the Web management portal (sample) [*]2

1.2. Background

US government agencies hold vast amounts of sensitive data and represent one of the most targeted sectors for cyberattacks. This requires stringent security measures. [*]3 However, many US government agencies provide direct access to device management interfaces inside their networks from the public Internet for maintenance and other purposes. When management interfaces are exposed on the Internet, they can be easily discovered from anywhere in the world, which has led to hackers exploiting them as an entry point into organizational networks in recent years. [*]4 In light of this, CISA has issued binding operational directives which seek to mitigate intrusions into U.S. government networks. [*]5

1.3. Countermeasures

Devices with management interfaces covered by this Directive include network devices such as routers, firewalls, proxies, and load balancers, as well as servers.

CISA requires U.S. government agencies to limit management interfaces to access only from internal networks so that they cannot be accessed from the Internet. Alternatively, an ideal solution is to incorporate a zero-trust architecture that controls access on internal networks to the minimum through user management and policy enforcement. It requires that interfaces that are not configured be removed within 14 days of the date they are discovered on the Internet (or notified by a CISA scan). It also requires the implementation of countermeasures/controls to ensure that the management interface, including any newly added devices, is protected as described above.

The following is an example of a prohibited and acceptable configuration proposed by CISA for a Remote/On-Site Administrator to use a management interface in an organization's network. [*]6

Prohibited Configuration

FIG. 2 is prohibited because access from the outside (External Entities [upper left of the figure]) to the inside of the network is not controlled and the management interface can be connected from the Internet.

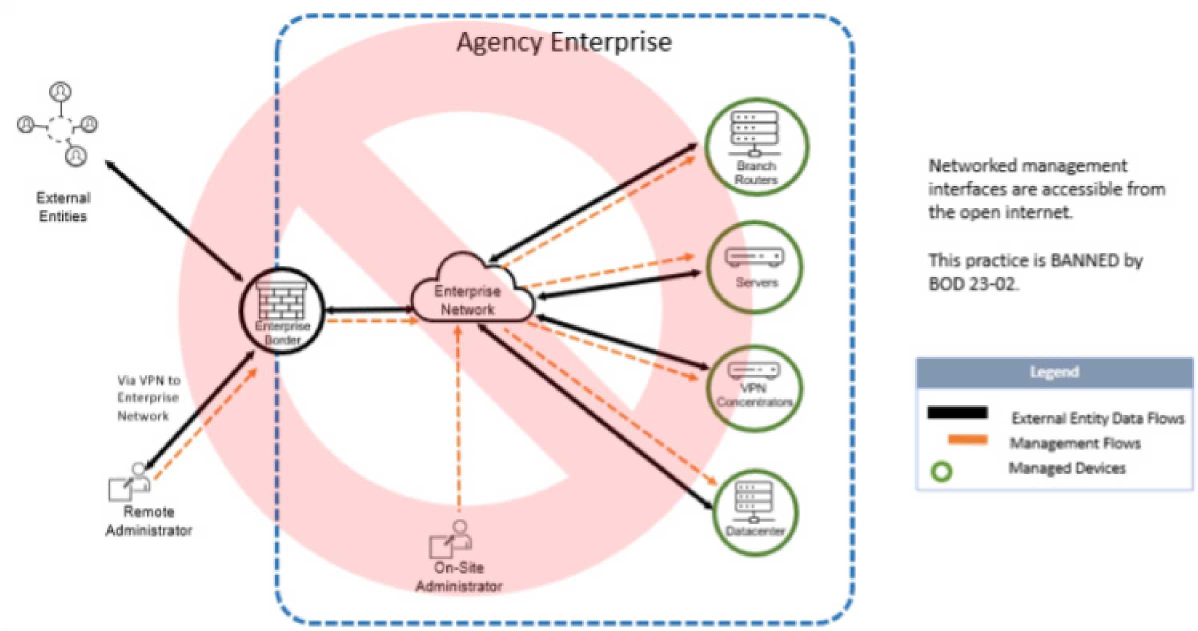
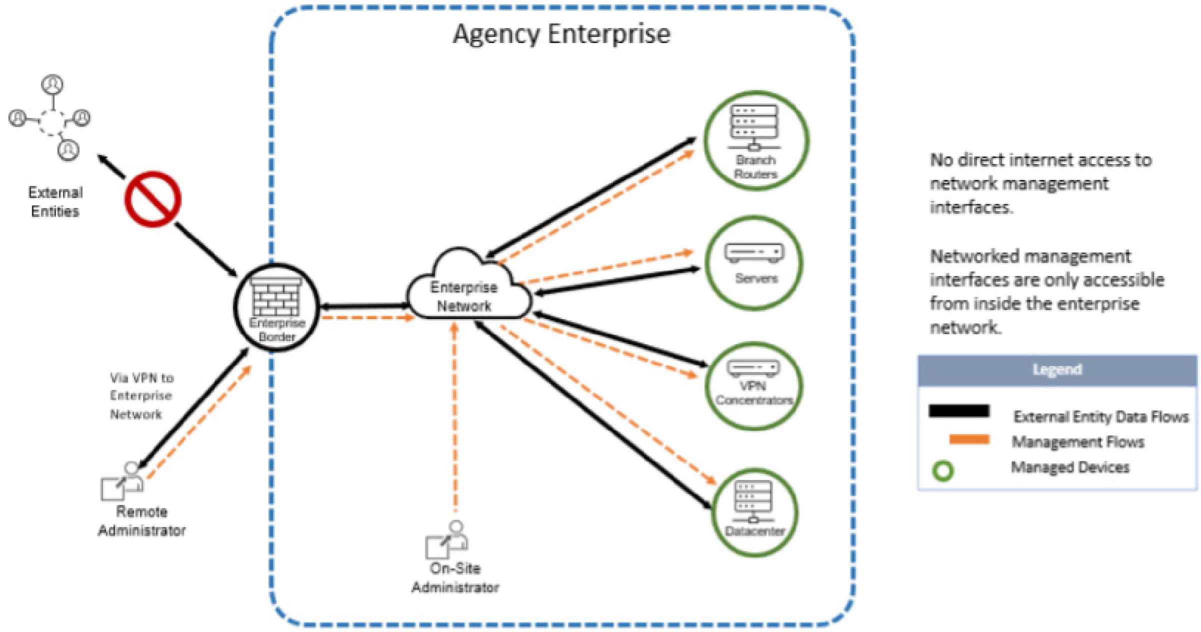


FIG. 2 Management interface accessible from the Internet

Allowed configurations

In the subsequent configurations, the internal network is separated from the Internet, making it difficult to attack from the outside.

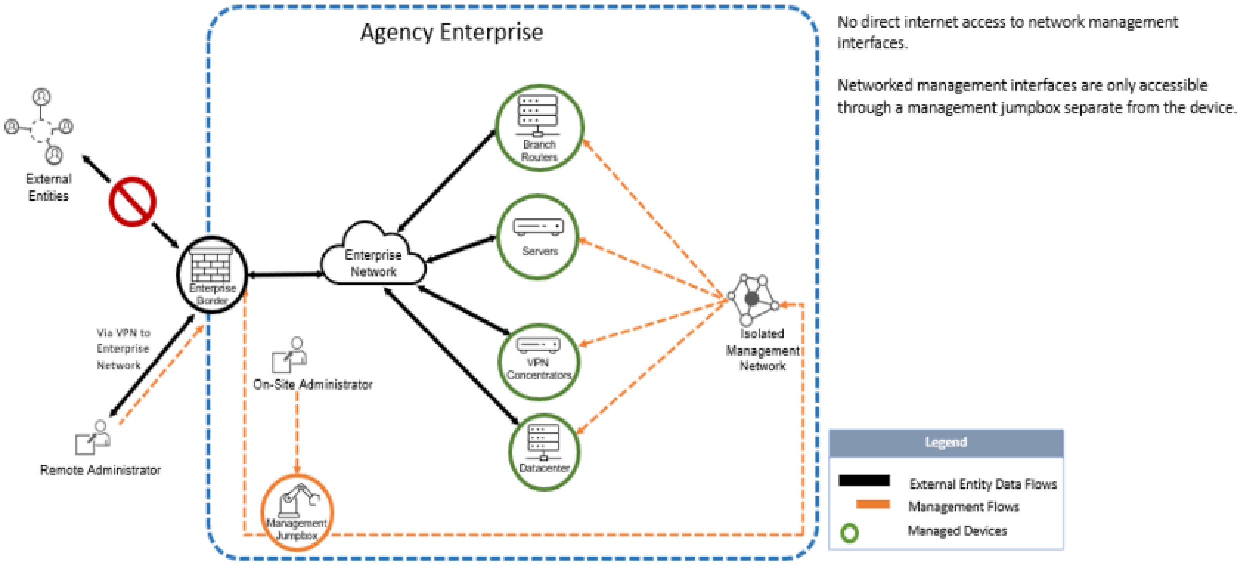


No direct internet access to network management interfaces.

Networked management interfaces are only accessible from inside the enterprise network.

Figure 3 Accessible only from within the organization

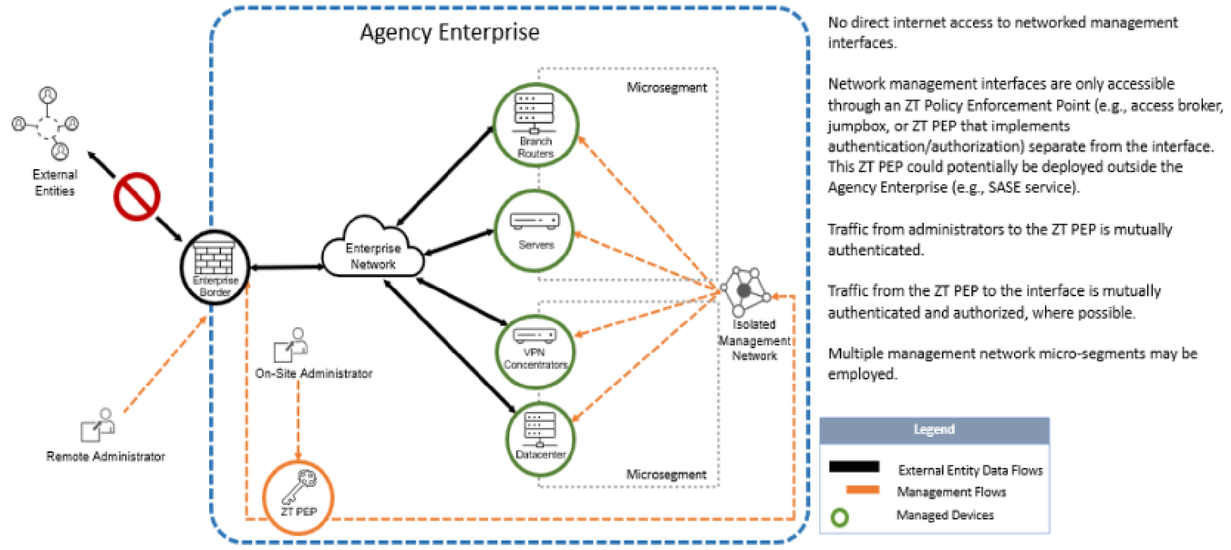
(Only authorized administrators can access management interface [via network internal/VPN].)



No direct internet access to network management interfaces.

Networked management interfaces are only accessible through a management jumpbox separate from the device.

Figure 4 Accessible only through the Jump Server



No direct internet access to networked management interfaces.

Network management interfaces are only accessible through an ZT Policy Enforcement Point (e.g., access broker, jumpbox, or ZT PEP that implements authentication/authorization) separate from the interface. This ZT PEP could potentially be deployed outside the Agency Enterprise (e.g., SASE service).

Traffic from administrators to the ZT PEP is mutually authenticated.

Traffic from the ZT PEP to the interface is mutually authenticated and authorized, where possible.

Multiple management network micro-segments may be employed.

Figure 5 Only accessible from microsegment of management network via ZT PEP
Access is limited to the administrator and his/her terminal authenticated with ZT PEP (zero-trust policy enforcement points)

1.4. Summary

This CISA operational directive follows the principle of least privilege, which states that the management interface is used only by system administrators and is not exposed to the Internet where anyone can access it. Similar advisories and reminders have been issued by various public agencies before, but it is worth noting that this CISA action as a binding directive is an indication that the risk of a publicly exposed management interface is unacceptable to the US government.

The directive is limited to U.S. government agencies, but since the risk of attack exists in both the public and private sectors, we recommend that private companies follow suit.

2. Ransomware hits Shalom, a software-as-a-service for Labor and Social Security Attorney offices

2.1. Overview

On June 5, a ransomware attack hit MKSystem, which provides software-as-a-service (SaaS) platforms such as “Shalom” for Labor and Social Security Attorney offices, and corporate human resources and labor departments in Japan. As a result, it affected many of those offices that were unable to use the services. [*]7

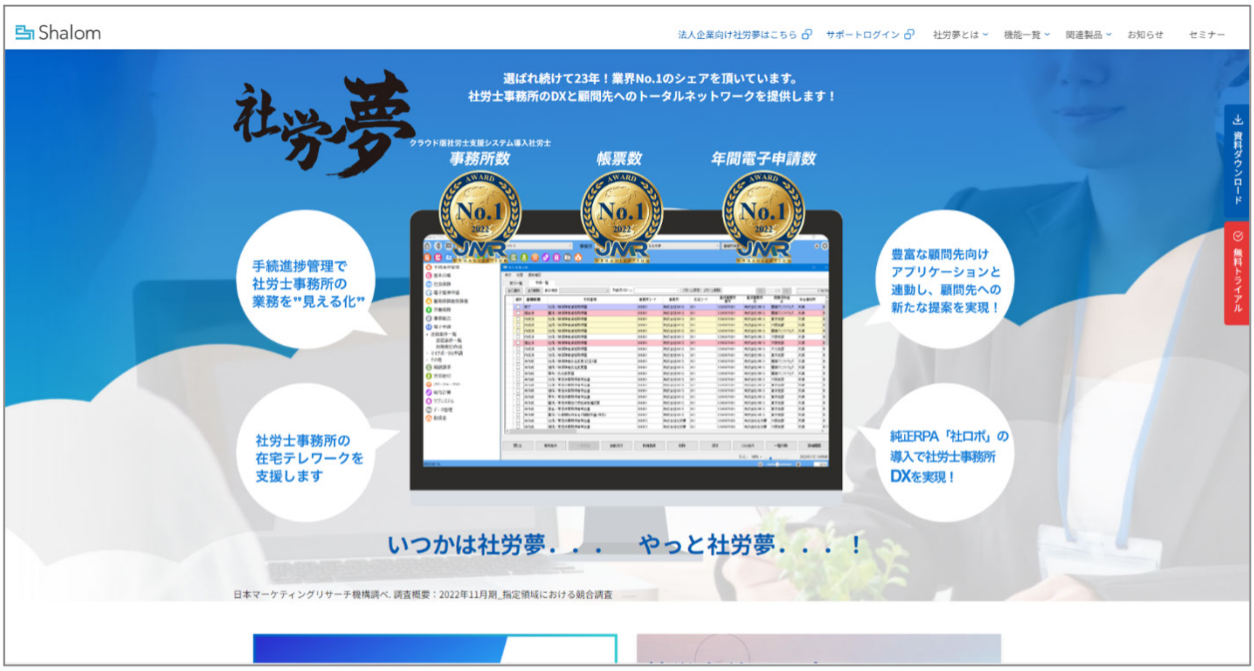

Shalom
法人企業向け社労夢はこちら
サポートログイン
社労夢とは
機能一覧
関連製品
お知らせ
セミナー
選ばれ続けて23年！業界No.1のシェアを頂いています。
社労士事務所のDXと顧問先へのトータルネットワークを提供します！
社労夢
クラウド版社労士支援システム導入社労士
事務所数
帳票数
年間電子申請数
AWARD No.1 2022 JMR
手続進捗管理で社労士事務所の業務を"見える化"
社労士事務所の在宅テレワークを支援します
豊富な顧問先向けアプリケーションと連動し、顧問先への新たな提案を実現！
純正RPA「社ロボ」の導入で社労士事務所DXを実現！
いつかは社労夢．．．　やっと社労夢．．．！
日本マーケティングリサーチ機構調べ. 調査概要：2022年11月期_指定領域における競合調査
資料ダウンロード
無料トライアル

Figure 6 MKSystem SaaS "Shalom" website

2.2. MKSystem "Shalom" service stopped

MKSystem provides software-as-a-service (SaaS) such as "Shalom," a Web system that supports procedures for social insurance, etc., and "Net de Chingin (Wage) Web version," a payroll system, for Labor and Social Security Attorney offices, etc. MKSystem claims that Shalom has "No. 1 market share" and is used by 50.4% of Labor and Social Security Attorney offices in Japan (Figure 6). [*]8 These offices, using Shalom, manage about 570,000 business places and about 8.26 million employees. [*]9

Damage from ransomware infection

In the early morning hours of June 5, all servers providing services became inoperable due to ransomware encryption, and services such as Shalom became unavailable. MKSystem said the attack affected most of its roughly 3,400 users (organizations). [*]10

Potential breach of personal information

MKSystem announced that there was no evidence of exfiltration of personal information or any other data transmission to the outside world. In addition, MKSystem explained that social security and tax numbers (“My Number”), which are stored by Shalom and other systems, are in an environment separate from the service environment and are encrypted. These records were not impacted by the breach. [*]11

Restoration and Impact on the Labor and Social Security Attorney offices

Since the backup data of the system was not damaged, MKSystem resumed the delivery of services one by one by restoring the backups and by bringing forward the release date of the new system that was under development. [*]12 [*]13

On the other hand, significant disruption was caused by the fact that Shalom could not be used in June, a busy month of the year, due to various administrative procedures such as the change of resident tax and bonus payment processing. Many of the processes that are automated by the system had to be performed manually, and the workload of employees at Labor and Social Security Attorney offices increased as a result. Since the system under development, which was provided ahead of schedule, was unstable due to high system loads, some staff met their deadlines by waking up in the middle of the night and working at night when system load was reduced. [*]14

2.3. SaaS Users and Reporting Obligations

In Japan, Organizations that handle personal information that has been damaged by a cyberattack and where there is a risk of information being exposed are required to promptly report such damage to the Personal Information Protection Commission, in accordance with the Act on the Protection of Personal Information. They are required to provide a preliminary report within three to five days of the date of discovery of the breach with a final report being required within 30 days. (Leaks which are the result of criminal activity such as cyberattacks must be reported within 60 days from the date of discovery.) [*]15

Reporting is mandatory not only for system providers but also for businesses using such a system to deliver services. The Personal Information Protection Commission states in its guidelines that the subject of the reporting requirement is "A personal information handling business operator handling personal data in which a leak, etc. has occurred or is likely to have occurred." [*]16 In this case, not only MKSystem but also **Labor and Social Security Attorney offices (contractor that use MKSystem’s products) and their clients are required to report.**

At first, MKSystem is said to have lobbied the Personal Information Protection Commission to exempt its clients (Labor and Social Security Attorney offices) from reporting. However, the Personal Information Protection Commission maintained its view that there is no exemption mechanism for this reporting requirement. As a result, MKSystem was forced to issue an apology to its clients for erroneously having suggested the possibility of an exemption from disclosure obligations. [*]17

A contractor and its clients are allowed to report jointly. In this case, the Japan Federation of Labor and Social Security Attorney's Associations provided a joint report format, and the Labor and Social Security Attorney offices used the format to report jointly with their clients. [*]18 [*]19

2.4. Summary

Over the past few years, ransomware attacks have become increasingly damaging to SaaS. [*]20 In this context, it is increasingly necessary to assume that personal information stored in SaaS could be compromised. [*]21

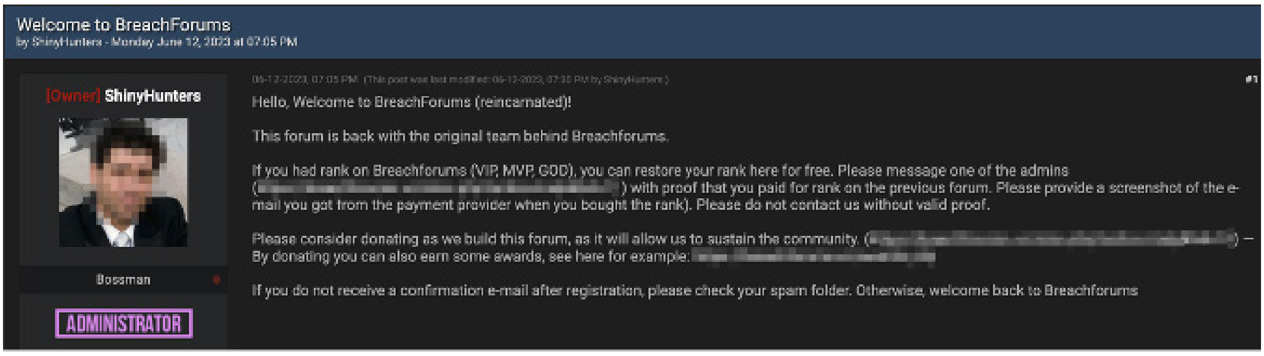
In this case, it was reaffirmed that companies that use such a service and those that entrust personal information to such companies are required to report the incident under the Act on the Protection of Personal Information. It is important for each company, as a contractor, to identify the parties, such as the Labor and Social Security Attorney offices, to which personal information is entrusted, to organize the incident response flow, and to prepare for cooperation in reporting, etc. when a leakage incident occurs. In addition, when handling personal information of a resident of a foreign country, it is necessary to pay attention to and confirm the possibility of violating foreign laws and regulations such as the GDPR(EU). [*]22 While this specific example deals with a breach which occurred in Japan, and focuses on Japanese laws and regulations, the risk is one that is universal. Most countries also have similar requirements for disclosure and reporting, which will however vary from country to country. It is important for businesses to understand the particular reporting requirements of the countries in which they operate.

3. Hacker forum BreachForums revived after owner's arrest

3.1. BreachForums revived

BreachForums, the world's largest hacker forum that shut down in March after the site's owner was arrested, returned to action on June 13 with a new owner. [*]23

The resurgence has been a hot topic among hackers, with more than 10,000 registered as of July 13. As before the shutdown, various leaks have been posted and hacking discussions are raging.



Welcome to BreachForums
by ShinyHunters - Monday June 12, 2023 at 07:05 PM

[Owner] ShinyHunters

Bossman

ADMINISTRATOR

06-12-2023, 07:05 PM (This post was last modified: 06-12-2023, 07:30 PM by ShinyHunters.) #1

Hello, Welcome to BreachForums (reincarnated)!

This forum is back with the original team behind Breachforums.

If you had rank on Breachforums (VIP, MVP, GOD), you can restore your rank here for free. Please message one of the admins ([redacted]) with proof that you paid for rank on the previous forum. Please provide a screenshot of the e-mail you got from the payment provider when you bought the rank). Please do not contact us without valid proof.

Please consider donating as we build this forum, as it will allow us to sustain the community. ([redacted]) – By donating you can also earn some awards, see here for example: [redacted]

If you do not receive a confirmation e-mail after registration, please check your spam folder. Otherwise, welcome back to Breachforums

Figure 7 BreachForums Welcome Message from New Owner ShinyHunters (Image partially altered)
"Welcome to BreachForums! This forum is back with the original team."

3.2. From Closure to Resurrection

Movement before and after Closure

BreachForums began operating in April 2022 after the closure of RaidForums, the largest hacker forum in the world at the time. Since then, it has attracted more hackers and handled 15 billion records of leaked information, surpassing RaidForums.

But in March, the FBI arrested a hacker named Conor Brian Fitzpatrick (aka pompompurin), the owner of BreachForums. At the time, the forum system was being operated by co-administrators, who shut down BreachForums out of concern that investigators might be using administrator rights seized from Fitzpatrick to gain access.

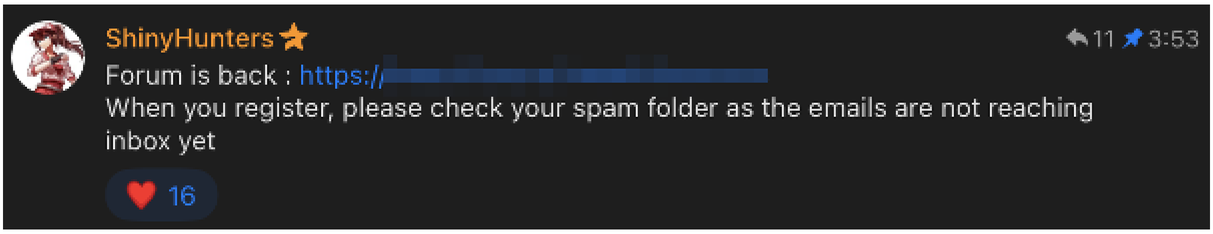
One of these administrators, who called himself "Baphomet," led the decision to shut down the forum and review future policies. Baphomet set up a chat group on Telegram to allow BreachForums users to communicate while the forum was closed. More than 4,000 people took part in the chat, which included discussions about how the new forum should work, cursing about emerging forums that aimed at taking BreachForums’ place, and other mundane chatter.

Baphomet had already been contacted by administrators of several competing forums when he decided to shut down the forum, and said he hoped to work with some of them in the future to build a new community with BreachForums functionality.

New Owner: ShinyHunters
Nearly three months after BreachForums was shut down, new owner ShinyHunters posted a new BreachForums URL in the Telegram chat group, which had previously been created by Baphomet, with a declaration that the forum was back.

ShinyHunters is a notorious hacking group responsible for hacking Microsoft's GitHub account and stealing nearly 7.7 million pieces of user data from its Nitro PDF software. [*]24 [*]25

The new BreachForums is a collaborative effort between ShinyHunters and the previous administrators, including Baphomet.



ShinyHunters
Forum is back : https:/[redacted]
When you register, please check your spam folder as the emails are not reaching inbox yet

Figure 8 ShinyHunters Posts Announcing the Reopening of BreachForums

3.3. Reaction of other hacker forums to the shutdown

Three months ago, BreachForums was the largest hacker forum in the world. This led to the creation of a number of similar forums and a scramble for users, including existing ones, in an attempt to lock in users who had become "homeless" after the forum shut down.

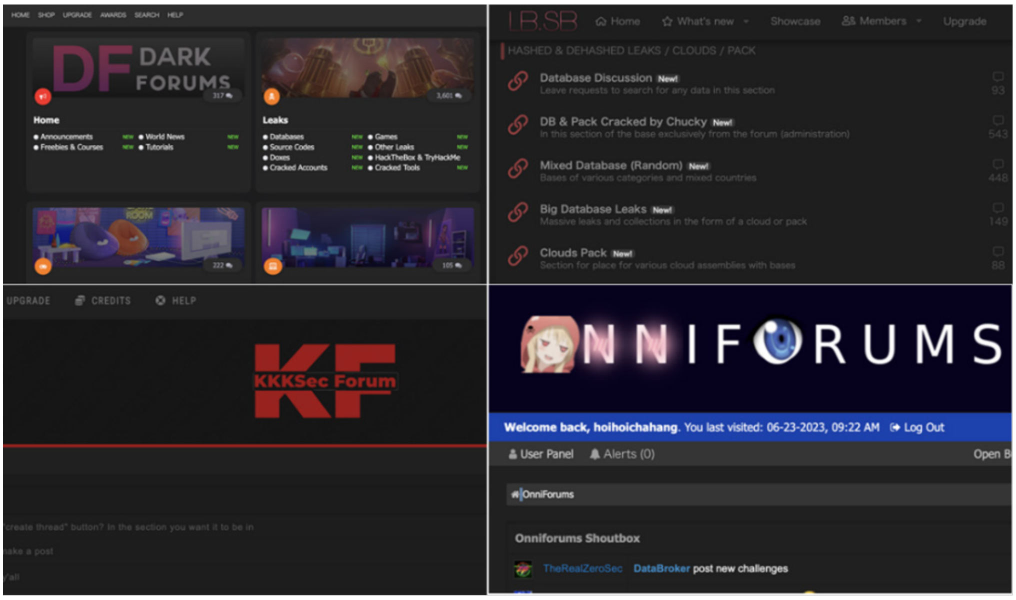


Figure 9 Examples of forums that became active after BreachForums shut down

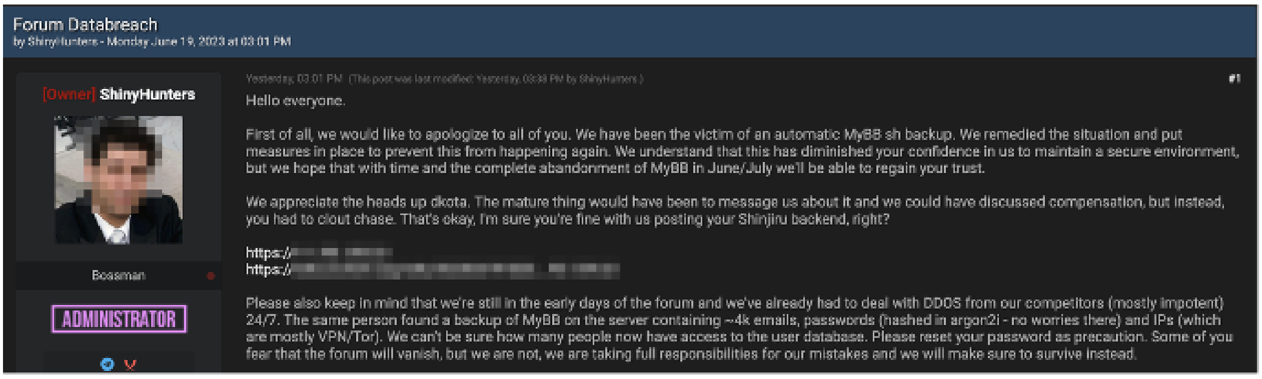
These forums tried to attract the attention of hackers by advertising on social networks such as Telegram and Twitter, and by posting messages on their forums that were created by reusing data previously leaked from large corporations and government organizations, but none of them were as successful in attracting users as the previous BreachForums.

Attack on the new BreachForums

After BreachForums was revived, some competitors gave up trying to steal users from the forum, and shut down their own forums, while others launched attacks in an attempt to disrupt BreachForums activities.

BreachForums, for example, was destabilized by a DDoS attack less than an hour after its revival. One of the forum's administrators claimed that administrators of the rival Exposed forum used a DDoS attack service to carry out the attack. [*]26

The administrator of another forum OnniForums going by the name dkota, used a zero-day vulnerability to attack BreachForums systems and steal data. He then posted data on his forum, including the email addresses and source IP addresses of about 4,000 BreachForums users. [*]27 ShinyHunters acknowledged the hack and posted an apology to users.



Forum Databreach
by ShinyHunters - Monday June 19, 2023 at 03:01 PM

[Owner] ShinyHunters

Bossman

ADMINISTRATOR

Yesterday, 03:01 PM (This post was last modified: Yesterday, 03:38 PM by ShinyHunters.) #1

Hello everyone.

First of all, we would like to apologize to all of you. We have been the victim of an automatic MyBB sh backup. We remedied the situation and put measures in place to prevent this from happening again. We understand that this has diminished your confidence in us to maintain a secure environment, but we hope that with time and the complete abandonment of MyBB in June/July we'll be able to regain your trust.

We appreciate the heads up dkota. The mature thing would have been to message us about it and we could have discussed compensation, but instead, you had to clout chase. That's okay, I'm sure you're fine with us posting your Shinjiru backend, right?

https://[redacted]
https://[redacted]

Please also keep in mind that we're still in the early days of the forum and we've already had to deal with DDOS from our competitors (mostly impotent) 24/7. The same person found a backup of MyBB on the server containing ~4k emails, passwords (hashed in argon2i - no worries there) and IPs (which are mostly VPN/Tor). We can't be sure how many people now have access to the user database. Please reset your password as precaution. Some of you fear that the forum will vanish, but we are not, we are taking full responsibilities for our mistakes and we will make sure to survive instead.

Figure 10 ShinyHunters Posts Apologizing for the Hack

Since the use of VPNs and anonymous email services has become common among hackers, the data leaked by the attack did not lead to any damage such as identity disclosure, and the forum has steadily increased its user base since then.

3.4. Summary

The return of BreachForums seems to have been welcomed by many hackers and their would-be allies. Since the days of the forum's predecessor, RaidForums, hackers of various nationalities and skills have participated, not only posting leaked information for profit or to gain fame as a hacker, but also as a place to chat and teach hacking skills, forming the largest hacker community in the English-speaking world. Participants have been involved in a number of cyberattacks, and as a result, BreachForums has amassed a large database of leaks. It is likely that the forum will continue to take a leading role in the hacker community, and we need to be vigilant about what is posted and what happens to participating hackers.

Disclaimer

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

Contact: NTT Security Japan Inc.

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

Sources

1. Source: CISA Binding Operational Directive 23 – 02
https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02
2. Source: Sophos Community Web Interface Login Failed 17.03
https://community.sophos.com/sophos-xg-firewall/f/discussions/100119/web-interface-login-failed-17-03
3. Source: InvGate "The 5 Industries Most Vulnerable to Cyber Attacks in 2023"
https://blog.invgate.com/industries-most-vulnerable-to-cyber-attacks
4. Source: The Record "CISA orders US civil agencies to remove tools from public-facing internet"
https://therecord.media/cisa-binding-operational-directive-remove-tools-from-public-internet
5. Source: CISA "CISA Directs Federal Agencies to Secure Internet-Exposed Management Interfaces"
https://www.cisa.gov/news-events/news/cisa-directs-federal-agencies-secure-internet-exposed-management-interfaces
6. Source: CISA "Binding Operational Directive 23-02 Implementation Guidance"
https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02-implementation-guidance
7. Source: ITmedia NEWS "Two Weeks After Ransomware Attack on Workers' System Lacks Full Recovery"
https://www.itmedia.co.jp/news/articles/2306/22/news163.html
8. Source: MK System Co., Ltd. "Industrial Dream | Cloud Industrial Business System with No. 1 Market Share"
https://www.mks.jp/shalom/
9. Source: MK System Co., Ltd. "MK System at a Glance"
https://www.mks.jp/company/ir-information/ataglance/
10. Source: Nikkei DIGITAL "MK System [3910]: Notification of Response to Ransomware Infections by Third Parties (2nd Report) June 21, 2023 (Timely Disclosure)"
https://www.nikkei.com/nkd/disclosure/tdnr/20230620507046/
11. Source: MK System Co., Ltd. "About the article published in Tokyo Shimbun"
https://www.mks.jp/company/topics/20230616
12. Source: Security NEXT "HR Labor System Failure, Payroll System Delivered - MK System"
https://www.security-next.com/146843
13. Source: MK System Co., Ltd. "Report on Resumption of Some Services"
https://www.mks.jp/company/topics/20220703a
14. Source: Nikkei Cross Tech (xTECH) "Workplace Trouble Counseling Room: Ransomware Attacks Are Hating, and Customers Are Struggling to Get Paychecks in Time"
https://xtech.nikkei.com/atcl/nxt/column/18/00084/00270/
15. Source: Personal Information Protection Commission, "Leakage Response and Useful Materials"
https://www.ppc.go.jp/personalinfo/legal/leakAction/
16. Source: Personal Information Protection Commission, "Guidelines on the Act on the Protection of Personal Information (General Rules) -3 -5 Reporting of Personal Data Leakage, etc. (Re. Article 26 of the Act)"
https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a3-5
17. Source: Asahi Shimbun Tsuginojidai "Ransomware could leak personal data"
https://smbiz.asahi.com/article/14930843
18. Source: "Tokyo Society Insurance Labor Consultants Association (Official)" on Twitter
https://twitter.com/tokyosr_/status/1669609709719130113
19. Source: Sakura Management Office, Social Insurance Labor Consultants Corporation "Notice to companies that have previously entered into advisory and spot contracts with our company and to the employees or former employees listed on the left"
https://www.sr-sakuram.jp/news/20230703/259/
20. Source: Odaseva "New Research: Ransomware Attacks Targeting SaaS Data"
https://www.odaseva.com/blog/new-research-ransomware-attacks-targeting-saas-data/
21. Source: Nikkei Cross Tech (xTECH) "Software as a Service (SaaS) Attacks Reveal Bad Hypotheses"
https://xtech.nikkei.com/atcl/nxt/column/18/00138/061901311/
22. Source: the Ministry of Economy, Trade and Industry Kyushu Bureau of Industry "Lecture at the 2021 Regional SECUNITY Cybersecurity Seminar "National Laws and Regulations on Cybersecurity: Commentary on Frequent Issues in Overseas Business" by Shunsuke Teramoto, Partner, TMI General Law Firm"
https://www.kyushu.meti.go.jp/seisaku/jyoho/pamph/pdf/cs21_2_3.pdf
23. Source: Cybernews "BreachForums is back – for real this time"
https://cybernews.com/security/breachforums-back-online/
24. Source: HACKREAD "Hackers claim to breach Microsoft's GitHub account; steel 500GB of data"
https://www.hackread.com/hackers-breach-microsoft-github-account-steal-500gb-data/
25. Source: Bleeping Computer "Hacker leaks full database of 77 million Nitro PDF user records"
https://www.bleepingcomputer.com/news/security/hacker-leaks-full-database-of-77-million-nitro-pdf-user-records/
26. Source :DataBreaches.net "The “reincarnation” of BreachForums: A cyberdrama in three acts"
https://www.databreaches.net/the-reincarnation-of-breachforums-a-cyberdrama-in-three-acts/
27. Source :DataBreaches.net "Confused about the drama with the new BreachForums? Reading this will either help you or make your head spin."
https://www.databreaches.net/confused-about-the-drama-with-the-new-breachforums-reading-this-will-either-help-you-or-make-your-head-spin/

NTT Security Holdings