Cyber Security Reports

2023.09

NTT Security Japan Co., Ltd.

Consulting Services Department OSINT Monitoring Team

NTT Security Holdings

Contents

About this report

This report summarizes three interesting cyber security related topics that occurred during September 2023. The summary of each topic is as follows.

CHAPTER 1
“AKIRA Attacks on Cisco ASA and Ransomware Attack Manual.”

- On September 6, Cisco announced a vulnerability, CVE-2023-20269, in Cisco ASA and FTD software. The vulnerability was being exploited by the Akira ransomware group at the time of the announcement.
- The group may have followed a manual on breaking into corporate networks written by a Ukrainian ransomware operator.
- Analysis of the manual showed that many of the attack steps were known and defensible, while others exploited zero-day vulnerabilities. In addition to implementing basic security measures, such as keeping systems up to date, it is also important to actively collect information about threat actors.

CHAPTER 2
“Pentagon unveils 2023 cyber strategy”

- In September, the Pentagon released a condensed version of the cyber strategy it submitted to Congress in May.
- In the past, the US military focused on defense and deterrence against cyber attacks, but major incidents in the private sector in 2020 and 2021, as well as Hunt Forward in the Ukraine War, significantly changed the Pentagon's mindset.
- The new strategy places an emphasis on helping US allies and partners build cyber capabilities and working together to improve response capabilities in cyberspace.

CHAPTER 3
"Bankruptcy notices and tampering of Japanese official corporate websites"

- At the beginning of September, falsified notices of bankruptcy and other problems were posted on official corporate websites.
- In addition to the falsification of official corporate websites, there were also cases in which emails of similar notices were sent due to unauthorized access to email systems.
- This website defacement that could affect corporate management, and it reminded us that security measures for systems that disclose corporate information, such as official websites, are essential to protect corporate management.

1. The AKIRA Attack on Cisco ASA and Ransomware Attack Manual

1.1. Overview

On September 6, US network giant Cisco Systems announced that the remote access VPN feature of its Cisco Adaptive Security Appliance (ASA)" software and Cisco Firepower Threat Defense (FTD) software, had a vulnerability, CVE-2023-20269. [*]1

Figure 1 Cisco ASA Series

If multi-factor authentication is not used on the Cisco ASA or FTD, an attacker who exploits the vulnerability could use a brute force attack to break authentication and establish an SSL VPN session. It has been exploited by the AKIRA ransomware group since spring, but remained a zero-day until a fix was made available on October 11.

1.2. Akira Ransomware Group

The Akira Ransomware Group (Akira) has been active since March this year. In addition to Cisco ASA, companies using VMware ESXi, have also been affected. [*]2. Attacks have been seen on companies in various sectors, including healthcare, manufacturing, and oil and gas. Yamaha Canada Music (Yamaha Canada Music Ltd.) was hit in July. [*]3

Figure 2 Akira Exposure Site

1.3. Ransomware Attack Manual

Akira brute-forces Cisco ASA login. Experts point out that this method is described in a manual on breaking into corporate networks available on the dark web. [*]4. The author of the manual is a Ukrainian ransomware hacker who worked for ransomware groups such as REvil. [*]5. An early version of the manual, which was distributed free in 2021, and version 2.0, which was later released in December 2022 and distributed for a fee, are both distributed among ransomware groups and other attackers. [*]6

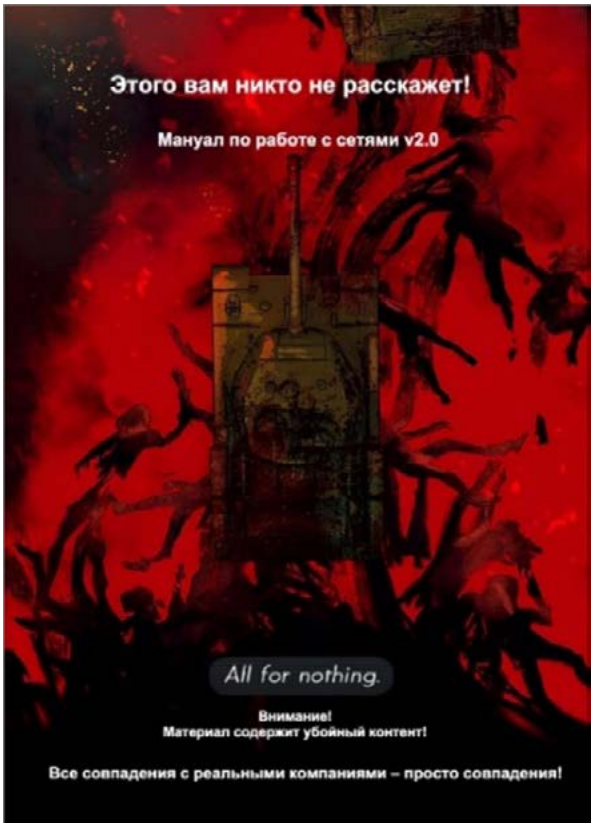

Figure 3 The cover of the manual (from version 2.0)

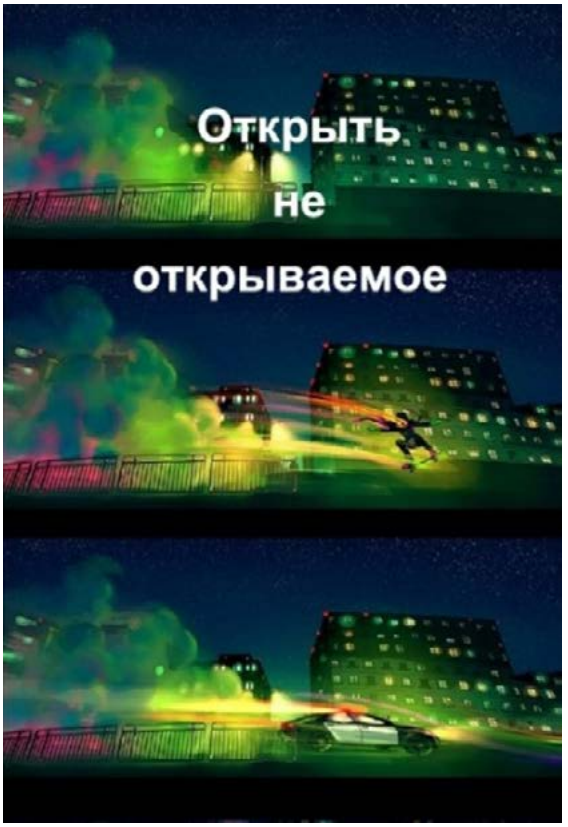

Figure 4 The cover of the network intrusion chapter Opening Things That Don't Open (from version 2.0)

Both manuals leaked on the Internet were obtained and analyzed. With an initial version of 63 pages and version 2.0 of 24 pages, the purpose of each manual was to teach criminals how to conduct ransomware attacks. As noted in the foreword "There are no pointless explanations of how a certain exploit works and mountains of incomprehensible code, we will apply it immediately in practice". The chapters follow an actual attack sequence, starting with setting up the environment necessary for the attack through to gaining access to a corporate network and elevating privileges. In particular, in the case of Cisco's VPN, the procedure for executing the brute force attack apparently carried out by Akira is specifically explained in version 2.0 (Figure 5).

You can also see the description of the VMware ESXi attack mentioned (Figure 6).

Figure 5 From the Manual (1) translation at the top of the page "Next, create a list. Brute force Cisco SSL VPN ..."

Figure 6 From the manual (2) Abstract at the bottom of the page "... resulting in information on computers that enable password theft from ESXi"

When asked in an interview whether ransomware attacks are possible if someone with little knowledge of how to code has the manual, the author said that it is possible if both versions of the manual are available. [*]7

1.4. Summary

From the analysis of the manual, it was found that many of the procedures described are well known and defenses available with the latest security measures and correct configuration. On the other hand, it was also found that attackers were exploiting vulnerabilities that vendors were unaware of until December.

In addition to implementing basic security measures such as keeping systems up to date, it is also important to proactively gather information about threat actors to prevent attacks.

2. Pentagon unveils 2023 cyber strategy

2.1. Overview

On September 12, 2023, the US Department of Defense (United States Department of Defense [DoD]) released a summary of its cyber strategy (2023 DoD Cyber Strategy Summary [DoD Cyber Strategy]). [*]8. This is the first revision to the cyber strategy in nearly five years, after it was submitted to Congress in May this year and the classified section was removed. [*]9.

The DoD Cyber Strategy explains how to deter the various threats facing the United States in cyberspace and how to promote domestic defense. [*]10.

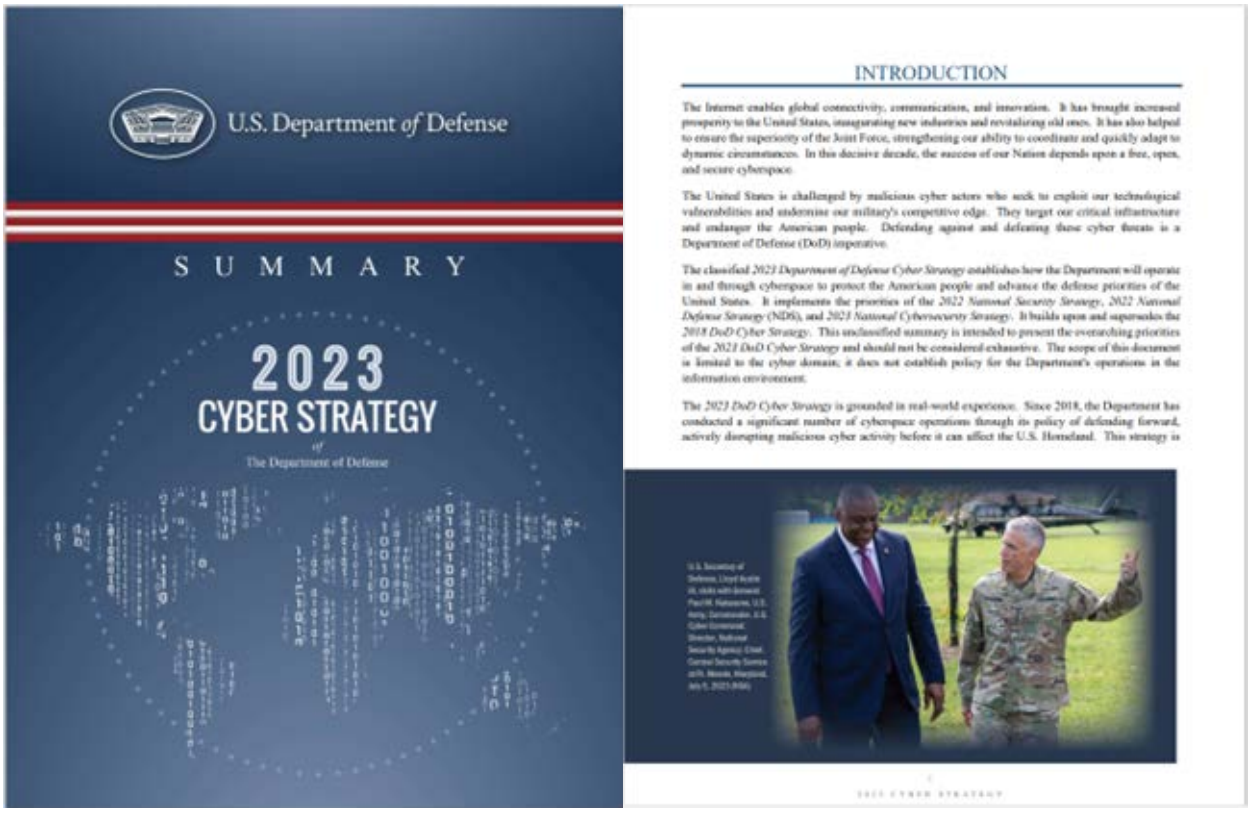

Figure 7 2023 DoD Cyber Strategy Summary Cover and INTRODUCTION [*]11

2.2. Changing DoD Cyber Strategy

The DoD Cyber Strategy has been revised in 2011, 2015 and 2018.
The first DoD Cyber Strategy, released in July 2011 under the Obama administration, emphasized that the strategy was designed to strengthen the defense system and did not intend to "militarize" cyberspace. [*]12.
Since then, the policy has changed due to an increase in cyber incidents that have a significant impact on the United States. The strategy, published in 2015, looked less optimistic and singled out Russia, China, Iran, North Korea and non-state actors as adversaries requiring the utmost vigilance. But even then, it said it would avoid relying on the military to deal with cyber threats

and maintain a deterrent approach. [*]13.
The strategy, published in 2018 after Russia's cyber-intelligence operations in the 2016 US presidential election, said it would "resolutely protect our interests" and "step up our defense" from a deterrence-focused regime. In other words, it adds a new concept called "Defend Forward," in which the US actively engages with the source of malicious cyber activity to disrupt the enemy and thwart attacks. [*]14[*]15
"Persistent Engagement" is also intended as a change to a proactive stance. This is aimed at proactively engaging with, addressing and responding to incidents that occur in cyberspace in order to continuously increase the ability to respond in an emergency and prevent destructive damage that could jeopardize national security. [*]16
By adopting such concepts as Defend Forward and Persistent Engagement, the US military aimed to break out of its defense and deterrence-focused regime.

2.3. About DoD Cyber Strategy in 2023

The outline of the Cyber Strategy, lists China, Russia, North Korea, Iran, violent extremist groups, and foreign criminal organizations as persistent threats to the United States and states that it aims to improve the US military's ability to respond. [*]17 [*]18. Among the countries/organizations mentioned, it seems that the threat from China is particularly in-depth. It also adds a section on increasing cooperation with allies and partners. [*]19

U.S. cyber damage and policy change " " [*]20 [*]21[*]22[*]23[*]24
Even after drafting its cyber strategy in 2018, the Pentagon focused much of its resources on protecting U.S. military networks from cyberattacks. However, a series of large-scale cyberattacks occurred outside of U.S. military networks.
In December 2020, the Russian Foreign Intelligence Service (SVR) conducted a mass hacking of SolarWinds products. The company's customers included a number of Fortune 500 companies and US government agencies. This is believed to have led to the theft of sensitive government information, including from the US military.

In May 2021, a Russia-based DarkSide ransomware attack on Colonial Pipeline on the East Coast shut down about half of the East Coast's gas supply. This caused major disruption to American civilian life. At the same time, JBS, the world's largest meat processing company, was shut down in Brazil following an attack by the ransomware group REvil, which could affect meat supplies in the United States.

These incidents, which caused enormous damage to American organizations and society, shocked the United States government, and the President issued an "Executive Order 1402835 on Improving National Cybersecurity" in May 2021, shortly after the incidents. This led the Pentagon to recognize that cybersecurity is national security concern. In response to this trend, the 2023 Cyber Strategy emphasizes the improvement of cyber capabilities through cooperation not only with U.S. military networks but also with U.S. government agencies and private companies responsible for critical infrastructure.

Hunt Forward' ' [*]25 [*]26 [*]27
The DoD Cyber Strategy promotes "Hunt Forward" as part of "Persistent Engagement" since 2018. This means that the US Cyber Command, at the request of its allies and partners, will dispatch defense personnel to inspect the system to uncover vulnerabilities, detect malware, and advise on countermeasures.

The Hunt Forward team was also deployed during Russia's invasion of Ukraine in 2022, helping to protect Ukraine from Russian cyberattacks, as well as bringing back valuable information about Russia's strategy and tactics in cyberwarfare.

Strengthening cooperation with allies and partners in the cyber domain ' [*]28 [*]29
Due to the number of serious security incidents mentioned above, as well as Hunt Forward's track record, the Department of Defense realized the need to communicate with allies and partners and provide defense support, leading to the development of the 2023 Cyber Strategy to protect cyberspace together.

Mieke Eoyang, Deputy Assistant Secretary of Defense for Cyber Policy, said:
"Unlike in the past, this DoD cyber strategy promises to increase our collective resilience to cyber attacks by building cyber capabilities with allies and partners. Allies and partners have a strategic advantage that competitors cannot match."

Figure 8 Deputy Assistant Secretary of Defense Mieke Eoyang at a press conference at the Pentagon, Washington, D.C., September 12 [*]30

2.4. Summary

The U.S. cyber strategy has been revised 3 times since 2011, but the way the military interacts with cyberspace threats has changed significantly in line with the situation at the time of publication.

The new security strategy provides a direction to check and contain the activities of hostile forces that had previously gone unchecked in the private sector and allies. The development of this strategy is expected to increase the cyber capabilities of the US military and allies.

3. Bankruptcy notices and tampering continues on Japanese corporate websites

3.1. Overview

At the beginning of September, a series of false announcements of bankruptcy were posted on the front page of official corporate websites. They are believed to have been defaced through unauthorized access. [*]31

3.2. Disclosure of false information through unauthorized access

Site tampering

From August 31 to September 4, notices such as "Bankruptcy proceedings were commenced on X 2023." were found to have been posted on several company official websites, likely in an attempt to affect business performance. These notices were unfounded and false. Threat actors are believed to have compromised web servers and altered the content without the victim's knowledge. [*]32

There were at least seven website defacement incidents across the country during the same period. [*]33. Although there is no similarity in industry or region, it is considered to be a series of linked incidents due to the similarity of the content in all cases.

Spoofed mail

It was not only web servers that were illegally accessed. The email systems of several victims were also apparently compromised. Fraudulent e-mails announcing bankruptcy were sent to email subscribers associated to “Shonan Village Center”. In the case of Nishijima Livestock, a victim of the incident, an email was sent to customers stating “the public health center has notified us of a food poisoning outbreak, and we are forced into bankruptcy due to defaulting on debts. 33.

It is believed that the same method was used in similar cases before this incident in which the vulnerable email system "acmailer" was illegally accessed and false email sent. In fact, before and after the incident, the Kyoto Prefectural Police and hosting companies alerted server administrators about the exploitation of the acmailer vulnerability. [*]34 [*]35

Damage Response

The victim companies have been notifying their customers and partners of the fraudulent announcements. Each company has filed a complaint with the police, and an investigation is underway on the of fraudulent activity. Companies that had e-mail systems compromised have also reported the possibility of personal information stored in the system being stolen. [*]36

Figure 9 Example of the announcement of tampering damage (Kagoshima Gyoza no Osho) [*]

3.3. Official corporate websites and measures against unauthorized access

In this case, due to the lack of context of the attack, it is considered that adversaries were able to gain unauthorized access due to vulnerabilities in public facing servers. Companies with official websites should take measures to prevent unauthorized access to their web servers and email systems, for example by ensuring to keep up with the latest patches available for these systems.

Effective countermeasure to be able to continue sharing information other than official websites when an incident occurs. For example, an official SNS account should be prepared and the existence of the account should be made known to the public in advance.

3.4. Summary

Traditionally, threat actors company's defacement of web sites make political claims and boast results of their success, and rarely affects the management of the company. Although this incident is considered to be defacement, it can have a detrimental affect on the company and considered malicious. If the business partners and customers believe it to be true, it could have interfered with business operations and led to a drop in stock prices and confidence of the company.

It was a reminder that the security of systems that disclose corporate information to the internet is also important in protecting corporate management.

Disclaimer

Please note that although the contents of this article are believed to be 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: Cisco Systems "Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote Access VPN Unauthorized Access Vulnerability"
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC

2. Source: Bleeping Computer "Linux version of Akira ransomware targets VMware ESXi servers"
https://www.bleepingcomputer.com/news/security/linux-version-of-akira-ransomware-targets-vmware-esxi-servers/

3. Source: Malwarebytes "Ransomware groups claim responsibility for double-attack on Yamaha"
https://www.malwarebytes.com/blog/news/2023/07/ransomware-groups-claim-responsibility-for-double-attack-on-yamaha

4. Source: Rapid7 "Under Siege: Rapid7-Observed Exploitation of Cisco ASA SSL VPNs"
https://www.rapid7.com/blog/post/2023/08/29/under-siege-rapid7-observed-exploitation-of-cisco-asa-ssl-vpns/

5. Source: The Record "The hacker ******** in his own words: Portrait of an access broker as a young man"
https://therecord.media/bassterlord-interview-hacker-initial-access-broker

6. Source: Analyst1 "Ransomware Diaries: Volume 2 – A Ransomware Hacker Origin Story"

7. Source: The Record "The hacker ******** in his own words: Portrait of an access broker as a young man"
https://therecord.media/bassterlord-interview-hacker-initial-access-broker

8. Source: U.S. Department of Defense 2023 DOD Cyber Strategy Summary
https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

9. Source: Mainichi Newspaper, The New U.S. Department of Defense Strategy Warns of China's Rise of Digital Authoritarianism
https://mainichi.jp/articles/20230913/k00/00m/030/043000c

10. Source: Cyber Daily "US DOD releases 2023 cyber strategy to combat emerging threats"
https://www.cybersecurityconnect.com.au/defence/9585-us-dod-releases-2023-cyber-strategy-to-combat-emerging-threats

11. Source: U.S. Department of Defense 2023 DOD Cyber Strategy Summary
https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

12. Source: Nihon Keizai Shimbun "Pentagon announces strategy to boost cyberspace defense"
https://www.nikkei.com/article/DGXDZO32274060V10C11A7EB2000/

13. Source: OXFORD ACADEMIC "The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation" https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988

14. Source: OXFORD ACADEMIC "The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation" https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988

15. Source: U.S. Department of Defense "CYBER STRATEGY SUMMARY FINAL"
https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

16. Source: U.S. Department of Defense "CYBER STRATEGY SUMMARY FINAL"
https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

17. Source: Cyber Daily "US DOD releases 2023 cyber strategy to combat emerging threats"
https://www.cybersecurityconnect.com.au/defence/9585-us-dod-releases-2023-cyber-strategy-to-combat-emerging-threats

18. Source: U.S. Department of Defense 2023 DOD Cyber Strategy Summary
https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

19. Source: U.S. Department of Defense "DOD's Cyber Strategy Emphasis Building Partner Capacity"
https://www.defense.gov/News/News-Stories/Article/Article/3523540/dods-cyber-strategy-emphasizes-building-partner-capacity/

20. Source: GIZMODE, What We Know So Far About the SolarWinds Hack
https://www.gizmodo.jp/2020/12/what-we-know-so-far-about-the-solarwinds-hacking-scandal.html

21. Source: REUTERS "'Flattered' Russian spy chief denies SolarWinds attack - BBC"
https://www.reuters.com/technology/russian-spy-chief-denies-svr-was-behind-solarwinds-cyber-attack-bbc-2021-05-18/

22. Source: T BBC NEWS JAPAN "FBI, Cyber attacks on meat processing giant are linked to Russian hackers"
https://www.bbc.com/japanese/57339918

23. Source: Tokio Cyber Port "Colonial Pipeline Affair, U.S. Cybersecurity Is on the Verge of Cataclysm "
https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/column-detail93

24. Source: THE WHITE HOUSE “Executive Order on Improving the Nation’s Cybersecurity”
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

25. Source: U.S. CYBER COMMAND "U.S. Cyber Command 2022 Year in Review"
https://www.cybercom.mil/Media/News/Article/3256645/us-cyber-command-2022-year-in-review/

26. Source: Nihon Keizai Shimbun "US military’s cyber strategy works with mainland allies"
https://www.nikkei.com/article/DGXZQOGN131AW0T10C23A9000000/

27. Source: Wedge ONLINE " Japan Can’t Protect Its Own Country by Refusing U.S. Military Training Due to Legal Restrictions"
https://wedge.ismedia.jp/articles/-/29268?page=3

28. Source: Mainichi Newspaper "The U.S. Department of Defense's New Strategy on China's Rise of Digital Authoritarianism"
https://mainichi.jp/articles/20230913/k00/00m/030/043000c

29. Source: U.S. Department of Defense " DoD's New Cyber Strategy Includes Developing Tech To ‘Confound’ Malicious Actors "
https://www.defense.gov/News/News-Stories/Article/Article/2523840/dods-cyber-strategy-emphasizes-building-partner-capacity/

30. Source: DEFENSE DAILY "DoD ’ s New Cyber Strategy Includes Developing Tech To ‘Confound’ Malicious Actors"
https://www.defensedaily.com/dods-new-cyber-strategy-includes-developing-tech-to-confound-malicious-actors/cyber/

31. Source: ITmedia NEWS "Disinformation falsification of "bankrupt" on official website continues to be damaged by training facilities, consultants, etc."
https://www.itmedia.co.jp/news/articles/2309/04/news118.html

32. Source: Netorabo ""Bankruptcy proceedings have begun." A series of "Gyoza no Ohsho" operators across the country have also been affected by tampering with corporate websites."
https://nlab.itmedia.co.jp/nl/articles/2309/04/news117.html

33. Source: FNN Prime Online, "Bankruptcy Procedure Begins," "Tampering Damage of Corporate Website Continues"
https://www.fnn.jp/articles/-/521910

34. Source: X "Kyoto Police Cyber Center"
https://x.com/KPP_cyber/status/1677210845170810880

35. Source: Sakura Internet "Be aware of the acmailer vulnerability" | Sakura Support Information
https://help.sakura.ad.jp/notification/n-2621/

36. Source: Nishijima Livestock Co., Ltd. "Notice of Website Restoration"
https://n-meat.co.jp/archives/36088

37. Source: Kagoshima Gyoza No Ohsho "Notice to Customers"
https://kagoshima-ohsho.jp/news/4916.html


NTT
Security Holdings