Cyber Security Reports

2023.10

NTT Security Japan Inc.

Consulting Services Department OSINT Monitoring Team

NTT Security Holdings

Content

About this report

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

CHAPTER 1

Chapter 1 Hacktivist Group Announces Ransomware GhostLocker

- In early October 2023, new Ransomware-as-a-Service (RaaS) called GhostLocker was announced. The ransomware was developed by GhostSec, a hacktivist group that focuses on counterterrorism and extremist content on the internet.
- The announcement follows the formation of ‘The Five Families’ in late August, purportedly a collaboration of five distinct threat actor groups which includes GhostSec. The release of GhostLocker ransomware is being promoted by members of ‘The Five Families’.
- It's unclear at this point how GhostSec will tie its activities to Ransomware as a Service (RaaS), but it's possible that this represents one of the future trends in the hacker world.

CHAPTER 2

Cisco IOS XE 0 Day Vulnerability; Over 40,000 Posts of Malware

- On October 16, Cisco Systems published a security advisory on a new zero-day vulnerability found in Cisco IOS XE software. A threat actor who successfully exploits this vulnerability could gain privileged access and take control of the device.
- More than 40,000 IOS XE devices were found on the Internet that appeared to be compromised by the attack.
- System management interfaces typically should not be exposed or open to the Internet. At this time, it is recommended that only the minimum necessary services are exposed to the Internet and that appropriate access controls are implemented.

CHAPTER 3

Armed Conflict and Cyber Attacks in Palestine

- Since the beginning of the armed conflict in Palestine in October 2023, hacktivists supporting the Palestinian/Israeli party have carried out a number of cyber attacks, including DDoS attacks and information disclosure, against rival organizations and their sponsors.
- Other attacks have been aimed at shutting down or destroying critical civilian infrastructure systems, such as power plants and flour production plants.
- Against a backdrop of hacktivist activities in the wild, cyberattacks on critical infrastructure in conflict situations are on the rise.

1. Hacktivist Group Announces Ransomware GhostLocker

1.1. 1.1. Overview [*]1 [*]2

In early October 2023, new Ransomware-as-a-Service called GhostLocker was announced. The ransomware was developed by the hacker group GhostSec, known as hacktivists fighting terrorist groups like ISIS and authoritarian states.Prior to GhostLocker's announcement, GhostSec and four other hacker groups formed The Five Families, potentially marking a new phase in threat actor collaboration.

1.2. Formation of The Five Families

At the end of August 2023, five hacker groups — GhostSec, SiegedSec, ThreatSec, Blackforums, and Stormous — announced that they had established a group called The Five Families. The purpose of the group's activities was not disclosed.

Each group member of The Five Families has varying interests, ranging from political demands, financial gains typically from ransomware attacks, or engaging in internet-based pranks. The name may have been inspired by the Five Families, an Italian mafia group that once dominated New York. [*]3

About GhostSec

GhostSec is a group of hackers whose activities have been confirmed since 2015 as an offshoot from the well known Anonymous collective. GhostSec advocates counter terrorism in cyberspace through disruption of online presence and communication of terrorist organizations and interfering with the spread of terrorist recruitment and propaganda on the Internet. [*]4[*]5 In July 2015, it provided intelligence on terrorist attacks in Tunisia and New York to investigative agencies, and succeeded in preventing terrorism. [*]6 Taking this opportunity, the group decided to cooperate with investigative agencies to fight terrorism legally, and decided to change its name to Ghost Security Group. However, some members opted to continue their illegal activities using the original GhostSec name and parted ways. [*]7

When Russia invaded Ukraine, GhostSec came out in support of Ukraine and launched attacks. [*]8 In May 2022, GhostSec gained access to IT systems supporting Russia's subway system which subsequently caused the immobilization of trains for a long time. In July, GhostSec seized control of the ICS (industrial control system) of Russia's hydroelectric power plant and claimed to have caused an explosion. [*]9 [*]10 It also carried out an attack on Iran's SCADA system in October that year to protest the death of a woman in police custody who did not comply with the country’s strict hijab regulations. [*]11 In April 2023, it claimed to have hacked satellite and water pump systems in protest at the storming an Islamic sacred site, Al-Aqsa Mosque, by Israeli police. [*]12

This has led to GhostSec being known as radical hacktivists who, along with political claims, continues to hack illegal and physical systems.

About SiegedSec, [*]13 [*]14 [*]15 [*]16 [*]17

SiegedSec emerged a few days before the Russian invasion of Ukraine in 2022, led by the hacktivist YourAnonWolf, and expressed support for Ukraine. Apart from the attacks, the group's chat channels also feature a number of casual conversations and jokes, indicating motivations for attacks ranging from hacktivist activities to malicious cybercrime for personal gain. Attacks include website defacement and unauthorized access to sensitive information using basic SQL injection and cross-site scripting (XSS).

Attacks include the successful breach of a NATO-controlled portal in July 2023 and the theft of lots of sensitive information.

On Valentine's Day in February 2023, Atlassian, an Australian software company was breached. A "Will you be my valentine?" message was posted on Telegram declaring the hack whilst also leaking Atlassian floor plans and employee information. On Halloween of the same year, SiegedSec launched a Halloween Hack cyberattack against Bezeq, Israel's largest telecom company, leaking information of approximately 50,000 of its customers. It also shut down an Israel-wide surveillance portal, affecting local infrastructure as well as linked Israeli embassy systems in other countries. At the end, it sent supposedly prank emails to Bezeq customers, leaving the recipients confused.

Figure 1 Valentine's Hacking Post via Telegram [*]18

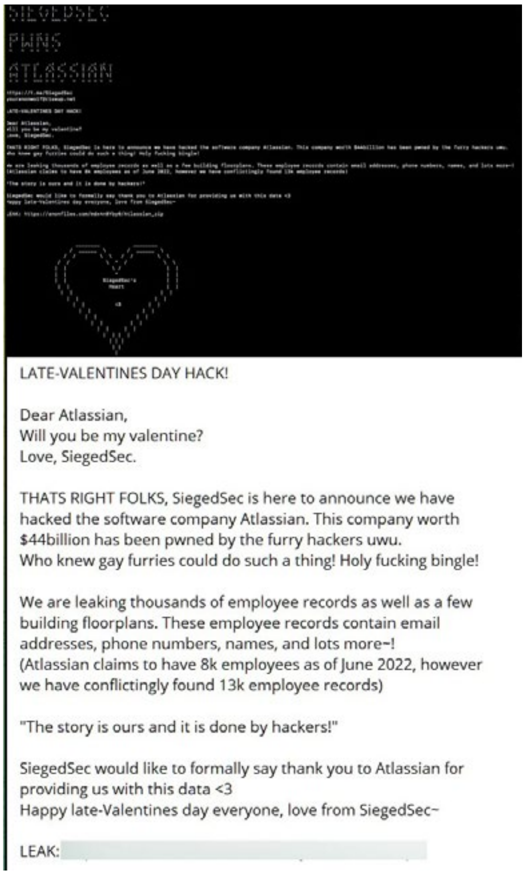

Figure 2 Halloween Hacking Post via Telegram

About ThreatSec

A relatively new hacker group whose activities have been visible since June 2023. Regarding the conflict between Israel and Palestine, the group says that it attacks both parties because it does not like war. Also, it claimes that, in October 2023, it compromised infrastructure of Gaza-based ISP ALFANET. [*]19

About Blackforums

A prominent hacker forum used for activities such as exchange of sensitive data and malware. The group behind Blackforums promotes their services and attracts cyber criminals having established itself as a de-facto point to trade stolen data and offer the sale of malware.

About Stormous

The Stormous Ransomware group have made claims that they have been behind various attacks in 2022 and have attempted to make its name by taking advantage of the conflict between Russia and Ukraine.

1.3. GhostLocker ransomware

In early October, Telegram channel GhostLocker announced the release of the ransomware of the same name, which was later promoted by members of The Five Families. Based on the content of the post, it appears that GhostSec was at the center of development. Stormous also announced that its own operations will include GhostLocker in addition to StormousX, which it previously used.

GhostLocker is offered as Ransomware as a Service (RaaS) at a low price with a monthly subscription. The service also includes the ability to prevent malware from being detected by security software and a panel for managing attack situations, as shown below.

When the GhostLocker malware is executed, the target data is encrypted with a powerful algorithm and the file name is appended with a ".ghost" extension to make it inaccessible. To decrypt it, the victim must pay a ransom, which is increased if the attacker is not contacted within 48 hours, or the data is permanently deleted. The ransom note also suggests that data will be permanently deleted if the victim changes the name of an encrypted file, uses a third-party decryption tool, or engages with law enforcement or a third party. [*]20

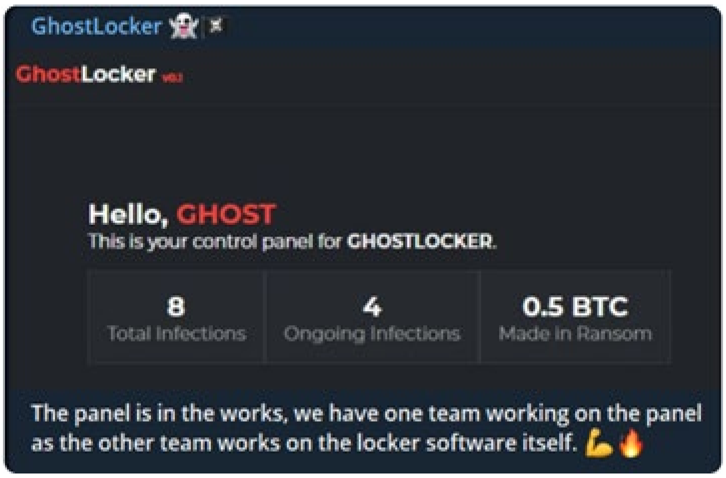

Figure 3 GhostLocker Management Panel [*]21

Figure 4 The Display After GhostLocker Runs (Contains Ransom Notes) [*] 22

1.4. Summary

The Hacktivist group GhostSec attempted to fight counter terrorism and war, but has become increasingly radical, culminating in its work with cybercrime groups and providing RaaS. Against this background, it is thought that the escalation of geopolitical and religious conflicts, such as the invasion of Ukraine and the military conflict between Israel and Hamas, has galvanized hacker activities and movements, and is laying the groundwork for further movements. It remains to be seen how GhostSec will combine its activities with RaaS, and whether it is simply for monetary gain.

Also, unlike DDoS or tampering, which can be done privately, the operation of ransomware services is complex and, as ContiLeaks (In 2022, a person claiming to be a Ukrainian researcher exposed the inner workings of Conti, a Russian-backed ransomware gang) found, requires a large number of people to be organized. It is not clear whether such services can be stably provided, as it is expected to be difficult to operate with a hacker group or a collaboration between such groups.

The activities of this group are radical, and it is possible that this movement represents one of the trends in the hacktivist world in the future.

2. Cisco IOS XE zero-day, more than 40,000 affected hosts

2.1. Overview

On October 16, Cisco Systems ("Cisco") announced a vulnerability in its enterprise networking operating system, Cisco IOS XE. If the operating system's web management user interface is exposed to the Internet, an attacker could exploit the vulnerability and gain full administrative privileges. [*]23 At the time of the announcement, it was already known that the vulnerability was actively being exploited.

On the same day, CISA in the US added the vulnerability to its "Known Exploited Vulnerabilities" and issued a warning. [*]24 Japan's JPCERT/CC also issued a warning on the 18th. [*]25

Figure 5 CISA Alert

2.2. IOS XE and Vulnerabilities

IOS XE

Cisco IOS XE is a member of Cisco's Cisco IOS series of operating systems and is based on Linux. It is widely used in Cisco routers, switches and other networking equipment. [*]26 About 150,000 IOS XE devices have been found on the Internet worldwide, predominantly in the United States. [*]27

CVE-2023-20198 and CVE-2023 -20273 [*]28

The announced vulnerability affects devices with the Web UI (Figure 6) feature enabled in IOS XE. The Web UI is embedded into IOS XE and is enabled through HTTP or HTTPS server commands without requiring licensing. As a result, a significant number of hosts may be affected by the vulnerability.

According to Cisco's investigation, an attacker gains privileged access to the device which is then used to create a local user for further access. The attack exploited two vulnerabilities. First, the attacker exploits CVE-2023-20198 to gain privileged access and create an account. Then, using the local account, exploits another vulnerability, CVE-2023-20273, to inject commands with elevated (root) privileges giving the ability to run commands on the device.

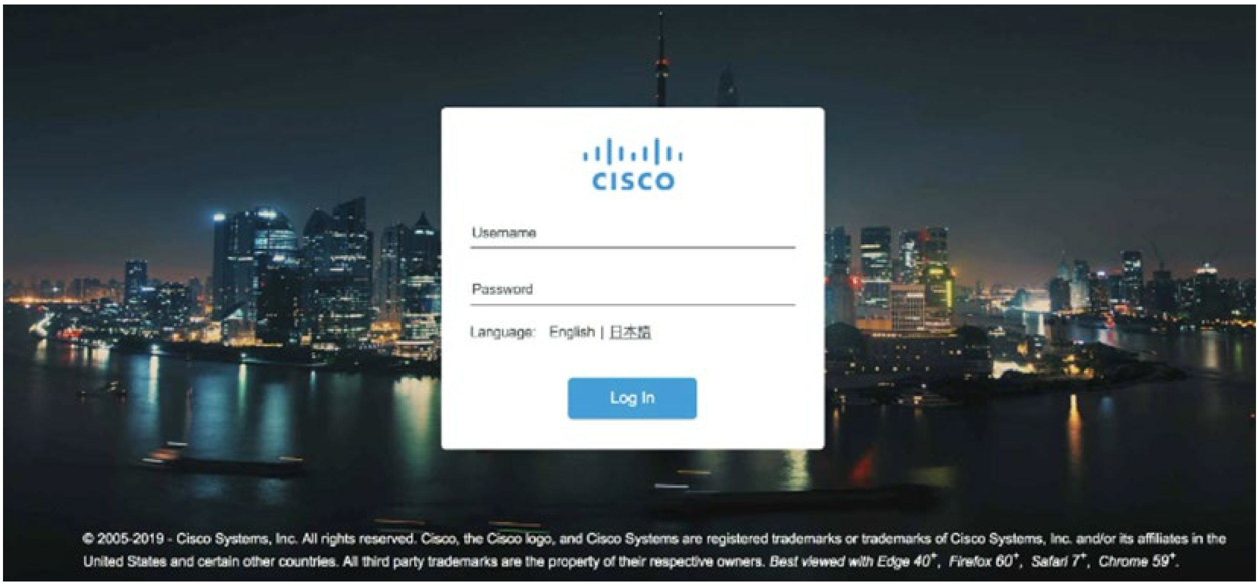

Figure 6 IOS XE Web UI Login Screen

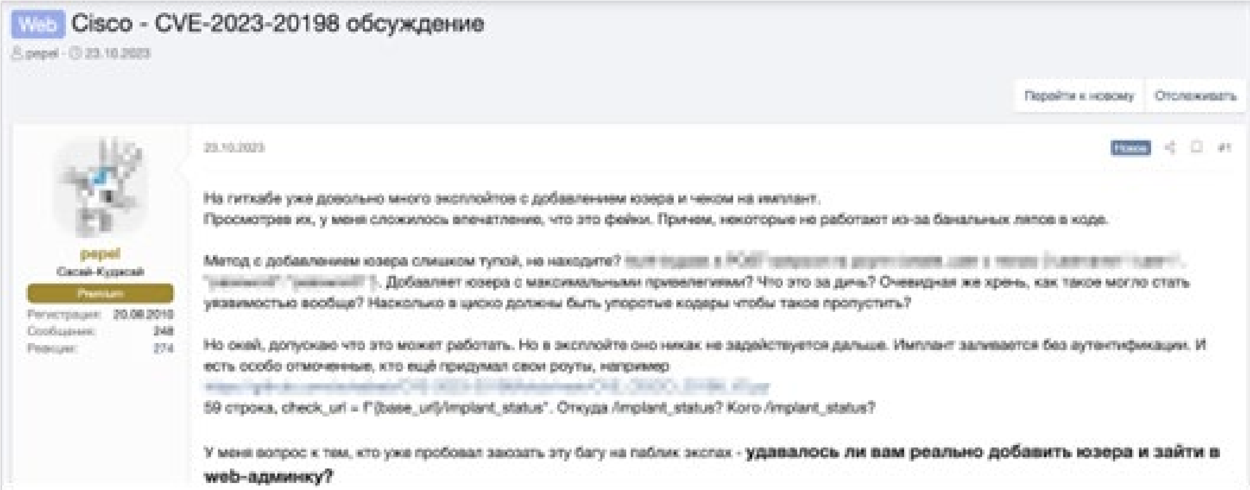

Figure 7 Russian Hacker Forum Thread Entitled "Cisco-CVE -2023-20198 Discussion"

The vulnerability has been a hot topic among hackers and discussed in hacker forums. On October 22, six days after the vulnerability was announced, Cisco began providing versions to fix the vulnerabilities.

Attack and Damage

IOS XE users can run a command on the system to determine if it has been compromised. A specific command (Figure 8) can be run on IOS XE and if the server responds with a 200 status code, along with an 18-byte hexadecimal string, then the device has been compromised. According to research, on October 18th approximately 41,983 hosts were affected. [*]29

NTT Security Holdings

```
curl -k -X POST "https://systemip/webui/logoutconfirm.html?logon_hasl
```

request returns a hexadecimal string, the implant is present

Figure 8 Command to determine compromise (from Cisco)
"If the server responds with a 200 status code along with an 18-byte hexadecimal string then the device has been compromised"

2.3. Risks of exposing the management interface

The web management interface, not limited to IOS XE, should not be exposed to the Internet. In particular, attackers target the management interface of critical systems, such as VPNs and firewalls, in order to penetrate the network.

The methods used to attack the management interface include brute force authentication attempts and injecting code to exploit vulnerabilities. If such attacks succeed, a malicious actor can add users, change settings, and more. Ultimately, an organization's network may be infiltrated potentially leading to information theft and other malicious activity.

In June, CISA issued a "BOD 23-02 (Binding Operational Directive)" to U.S. government agencies in light of the continued damage caused by such attacks, requiring them to take measures such as preventing external access to management interfaces. [*]30

2.4. Summary

The zero-day attack affected more than 40,000 devices. It is once again clear that interfaces for system administration should not be exposed to the Internet. As a result, it is recommended that only the minimum necessary services be exposed to the Internet and that appropriate access controls are implemented.

3. Armed Clashes and Cyber Attacks in Palestine

3.1. Overview

Since the launch of an attack on October 7, 2023, clashes between the Palestinian militant group Hamas and Israel have escalated into war. Immediately after the conflict began, cyber attacks by hacktivists cooperating with the two groups have spread rapidly. [*]31 In addition to a number of DDoS attacks, the attacks have escalated into information leaks, website defacement, and even attacks targeting critical infrastructure.

Cyberattacks on critical infrastructure involving the private sector could violate international humanitarian law. However, the effectiveness of punishment for such violations is slim, and hacktivists continue to carry out attacks undeterred.

3.2. Cyber warfare broke out immediately after the attack

Cyber attacks occurred shortly after the attack by Hamas..[*]32 [*]33 About 12 minutes into the attack, a DDoS attack was detected on a site in Israel that provides civilian warning of rocket attacks. [*]34 Since then, DDoS attacks have spread to media outlets, the software industry, and government sites. DDoS attacks against Palestinian websites as well as Israeli websites have also been detected, with attack-related traffic at one point accounting for 60% of all traffic.[*]35

Hacktivists are the main perpetrators of these cyberattacks. They often claim responsibility for DDoS attacks, post messages through defacing websites, and reveal confidential information. There have also been a number of attacks in which Palestinian and Israeli actors, as well as foreign hacktivists, have assisted both groups. Hacktivists have long been active against the backdrop of the long-simmering Palestinian situation, but this armed conflict has led to a surge in activity.

Pro-Palestinian Hacktivists

There are more than 130 pro-Palestinian hacktivist groups, many of which claim to be Islamic groups in the Middle East and Asia (Indonesia, Malaysia, etc.). [*]36

These groups advocate anti-Israel solidarity with Palestinian Muslims. In addition, they have expanded their attacks not only to Israel itself but also to Western and other countries that take a pro-Israel stance. In particular, Islamic groups in Asia, such as Pakistan and Bangladesh, have been attacking India.

Hacktivists attack Japan

Various groups are targeting Japan. Since Japan opposed a ceasefire proposed by Russia at the UN Security Council on October 16, Japan has been listed as one of the countries supporting Israel.

First, on October 20, several Japanese government websites were listed as targets for DDoS attacks by pro-Palestinian groups. On October 25, a website belonging to a Japanese business was defaced to display pro-Palestinian messages by a Bangladeshi group. [*]37 On November 1, a Pakistani group said it carried out a DDoS attack on Japanese government agencies and other entities.

Pro-Israeli Hacktivists

More than 20 pro-Israel hacktivists have also been identified, although not as many as pro-Palestinian groups, and activities by Indian groups are particularly prominent. [*]38 In addition to DDoS attacks on the Palestinian side, attacks have also been identified, including claims of tampering with Hamas sites and revelations of medical data stolen from Palestinian medical facilities.

3.3. Hacktivists targeting critical infrastructure

Hacktivists have also been identified as plotting to attack critical infrastructure control systems. For example, several pro-Palestinian groups reported that they had successfully infiltrated the systems that control water supplies in Israel (Figure 10, Figure 11). Another group stated it had successfully conducted a cyberattack on an Israeli power plant in mid-October to stop its power supply (Figure 12), and another group stated it had infiltrated the systems of Israel's largest flour production plant in early November (Figure 13). In addition to critical infrastructure attacks, the group also says it has conducted ransomware attacks on Israeli organizations. [*]39

Attacks on critical infrastructure systems can have severe consequences such as long-term supply disruptions of electricity, domestic water and food, ultimately threatening civilian lives.

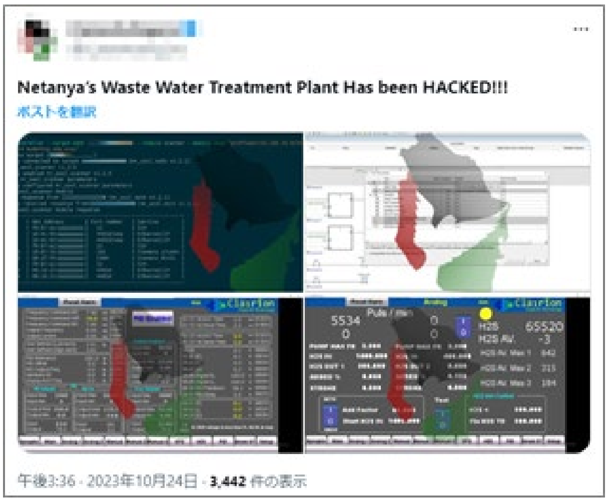

Figure 10 Post suggesting attacks on water facilities

Figure 11 Post Claiming Attacks on Water Facilities

3.4. Cyberattack Rules Proposed by the International Committee of the Red Cross (ICRC)

Shortly before the outbreak of military clashes in Palestine, the International Committee of the Red Cross (ICRC) proposed rules on the conduct of civilian hackers operating in the context of armed conflict. [*]40 It came amid a sense of crisis over the rampant activities of civilian hackers that have flourished since Russia invaded Ukraine.

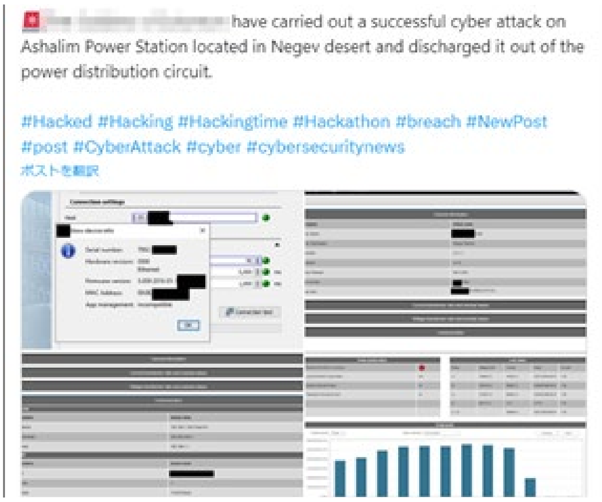

Figure 12 Post Claiming Attacks on Power Plants

Figure 13 Post Claiming Attacks on Flour Production Plants

The rules are aimed at curbing targeting of civilians in violation of international humanitarian law. They call for a ban on cyberattacks on critical civilian infrastructure, hospitals and other facilities, and for compliance even if the enemy does not comply with such rules. The ICRC also calls on states to restrict activities of their own private hackers in order not to deviate from the rules of engagement under international humanitarian law. Under international humanitarian law, hacktivists who carry out cyber attacks that damage critical infrastructure may face international prosecution as criminals or terrorists, unlike military personnel who may conduct lawful acts of war and become 'prisoners of war' if captured.

But soon after the announcement, hacktivists in both Ukraine and Russia reacted negatively to the conduct rules. In response to media interviews, some stated breaking conduct rules was inevitable for a group's cause, while some pro-Ukrainian hacktivists made statements against it by tampering with the site of the Russian Red Cross Society. [*]41 [*]42

3.5. Summary

In the wake of the armed conflict, the activities of hacktivists supporting each side suddenly increased. Although the authenticity of some attacks is unknown, attacks on critical infrastructure have been carried out without hesitation. If the loss of function or damaged facilities affects human life, it may constitute a serious crime or terrorist act. Pro-Palestinian hacktivists have called on hackers around the world to attack US civilian and public infrastructure in addition to Israel, and there are fears that attacks targeting such critical infrastructure could be carried out in countries not directly linked to the armed conflict. [*]43

Hacktivists are said to be declining in developed countries as law enforcement has been cracking down on cybercrime since the late 2010s. Hacktivists, on the other hand, continue to be unchecked in many developing countries, contributing to the boom in Palestinian cyberattacks.

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: Cyberint "GhostLocker: The New Ransomware On The Block"
https://cyberint.com/blog/research/ghostlocker-the-new-ransomware-on-the-block
2. Source: Cyberint GhostSec Raising the Bar
https://cyberint.com/blog/research/ghostsec-raising-the-bar/
3. Source: SOCRadar "The Five Families: Hacker Collaboration Redefining the Game"
https://socradar.io/the-five-families-hacker-collaboration-redefining-the-game/
4. Source: Cyberint, GhostSec Raising the Bar
https://cyberint.com/blog/research/ghostsec-raising-the-bar/
5. Source: ALTIMETRIK "Behind the Mask of GhostSec: Vigilante Hackers on a Cyber Crusade"
https://www.altimetrik.com/behind-the-mask-of-ghostsec-vigilante-hackers-on-a-cyber-crusade/
6. Source: Security Affairs "ANONYMOUS'S TEAM GHOSTSEC THWARTS ISIS TERROR PLOTS"
https://securityaffairs.com/38860/cyber-crime/ghostsec-thwarts-isis-terror-plots.html
7. Source: MIC "Anonymous Divided: Inside the Two Warring Hacktivist Cells Fighting ISIS Online"
https://www.mic.com/articles/129679/anonymous-vs-isis-how-ghostsec-and-ghost-security-group-are-targeting-terrorists#.t7BdOvX5w
8. Source: Cyberint, GhostSec Raising the Bar
https://cyberint.com/blog/research/ghostsec-raising-the-bar/
9. Source: The Tech Outlook "Russian trains still not in function after being hacked by GhostSec"
https://www.thetechoutlook.com/news/technology/russian-trains-still-not-in-function-after-being-hacked-by-ghostsec/
10. Source: OTORIO "Targeting ICS with Country-Specific Tactics: Illuminating GhostSec"
https://www.otorio.com/blog/country-specific-ics-targeting-shining-a-light-on-ghostsec/
11. Source: Industrial Cyber "OTORIO reveals GhostSec hacktivist group now targets Iranian ICS in support of Hijab protests"
https://industrialcyber.co/news/otorio-reveals-ghostsec-hacktivist-group-now-targets-iranian-ics-in-support-of-hijab-protests/
12. Source: ALTIMETRIK "Behind the Mask of GhostSec: Vigilante Hackers on a Cyber Crusade"
https://www.altimetrik.com/behind-the-mask-of-ghostsec-vigilante-hackers-on-a-cyber-crusade/
13. Source: SOCRadar Threat Actor Profile: SiegedSec
https://socradar.io/threat-actor-profile-siegedsec/
14. Source: Cyberint SiegedSec Compromise NATO
https://cyberint.com/blog/research/siegedsec-compromise-nato/
15. Source: Bleeping Computer "Atlassian data leak caused by stolen employee credentials"
https://www.bleepingcomputer.com/news/security/atlassian-data-leak-caused-by-stolen-employee-credentials/
16. Source: The CYBER EXPRESS "SiegedSec Halloween Hack Announcement: Takes Down Bezeq"
https://thecyberexpress.com/bezeq-data-breach-halloween-hack/
17. Source: DarkOwl "Dark Web Cyber Group Spotlight: SiegedSec"
https://www.darkowl.com/blog-content/darkowl-cyber-group-spotlight-siegedsec-and-leaked-data/
18. Source: Bleeping Computer "Atlassian data leak caused by stolen employee credentials"
https://www.bleepingcomputer.com/news/security/atlassian-data-leak-caused-by-stolen-employee-credentials/
19. Source: SecurityWeek "Hackers Join In on Israel-Hamas War With Disruptive Cyberattacks"
https://www.securityweek.com/hackers-join-in-on-israel-hamas-war-with-disruptive-cyberattacks/
20. Source: PCrisk.com "GhostLocker (.ghost) ransomware virus – removal and decryption options"
https://www.pcrisk.com/removal-guides/28068-ghostlocker-ransomware
21. Source: SOCRadar "GhostLocker: A New Generation of Ransomware as a Service (RaaS)"
https://socradar.io/ghostlocker-a-new-generation-of-ransomware-as-a-service-raas/
22. Source: PCrisk.com "GhostLocker (.ghost) ransomware virus – removal and decryption options"
https://www.pcrisk.com/removal-guides/28068-ghostlocker-ransomware
23. Source Cisco Systems "Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature"
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
24. Source CISA "CISA Adds One Known Exploited Vulnerability to Catalog"
https://www.cisa.gov/news-events/alerts/2023/10/16/cisa-adds-one-known-exploited-vulnerability-catalog
25. Source: JPCERT/CC Alert for Cisco IOS XE Web UI Vulnerability (CVE-2023-20198)
https://www.jpcert.or.jp/at/2023/at230025.html
26. Source: Cisco IOS XE, Cisco Systems
https://www.cisco.com/c/ja_jp/products/ios-nx-os-software/ios-xe/index.html
27. Source: Bleeping Computer "Over 40,000 Cisco IOS XE devices infected with backdoor using zero-day"
https://www.bleepingcomputer.com/news/security/over-40-000-cisco-ios-xe-devices-infected-with-backdoor-using-zero-day/
28. Source: Cisco Systems "Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature"
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
29. Source: Censys CVE-2023-20198 – Cisco IOS-XE ZeroDay
https://censys.com/cve-2023-20198-cisco-ios-xe-zeroday/
30. Source: CISA "BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces"
https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02

Sources

31. Source: Reuters "Hacktivists stoke Israel-Gaza conflict online"
https://www.reuters.com/world/middle-east/hacktivists-stoke-israel-gaza-conflict-online-2023-10-11/

32. Source: FalconFeeds "The Evolving Landscape of Cyber Warfare in the Israeli-Palestine Conflict: A Comprehensive Analysis"
https://falconfeeds.io/blog/post/the-evolving-landscape-of-cyber-warfare-in-the-israelpalestine-conflict-a-comprehensive-analysis--356011

33. Source: SOCRadar "Reflections of the Israel-Palestine Conflict on the Cyber World"
https://socradar.io/reflections-of-the-israel-palestine-conflict-on-the-cyber-world/

34. Source: Cloudflare "Internet traffic patterns in Israel and Palestine following the October 2023 attacks"
https://blog.cloudflare.com/internet-traffic-patterns-in-israel-and-palestine-following-the-october-2023-attacks/

35. Source: Cloudflare: Cyber attacks in the Israel-Hamas war
https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/

36. Source: X "@ Cyberknow 20"
https://x.com/Cyberknow20/status/1720217982201409821

37. Source: NHK "Pet Salons in Tokyo ... Cyber attacks in Middle East military conflict"
https://www3.nhk.or.jp/news/html/20231026/k10014237901000.html

38. Source: FalconFeeds "The Evolving Landscape of Cyber Warfare in the Israeli-Palestine Conflict: A Comprehensive Analysis"
https://falconfeeds.io/blog/post/the-evolving-landscape-of-cyber-warfare-in-the-israelpalestine-conflict-a-comprehensive-analysis--356011

39. Source: Security Affairs "Pro-Palestinian hackers group 'Soldiers of Solomon' disrupted the production cycle of the biggest flour production plant in Israel"
https://securityaffairs.com/153778/security/soldiers-of-solomon-hacked-israel-flour-plant.html

40. Source: ICRC Humanitarian Law & Policy Blog "8 rules for “civilian hackers” during war, and 4 obligations for states to restrain them"
https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/

41. Source: BBC News "Rules of engagement issued to hacktivists after chaos"
https://www.bbc.com/news/technology-66998064

42. Source: The Record "‘War has no rules’: Hacktivists scorn Red Cross’ new guidelines"
https://therecord.media/hacktivists-respond-to-red-cross-rules-with-ridicule

43. Source: X "@ FalconFeedsio"
https://twitter.com/FalconFeedsio/status/1711033041827828087


NTT
Security Holdings