

The background of the entire page is a photograph of a traditional Japanese street scene. In the foreground, a person wearing a dark kimono with a floral pattern is holding a large, open, light-colored paper umbrella. The street is paved with cobblestones and lined with traditional wooden buildings. In the background, a multi-tiered pagoda with a dark roof and a spire is visible against a light sky. The overall image has a blue and green color overlay.

Cyberint

Impactful Intelligence

JAPAN THREAT LANDSCAPE REPORT

June 2024

TABLE OF CONTENTS

Executive Summary	4
Phishing and Social Engineering	5
A Global Rise of Smishing	5
Generative AI	7
Data breaches	8
Fujitsu Incident	8
LINE Breach	8
An Increasing Targeting by Chinese-Speaking Threat Actors	9
Ransomware	14
Regional statistics and Impact	14
Lockbit	17
Tactics, Techniques, and Procedures (TTPs)	18
Latest Japan Incident	18
IOCs	19
ALPHV	20
Tactics, Techniques, and Procedures (TTPs)	20
Latest Japanese Incident	21
Notable IOCs	21
Hunters International	22
Tactics, Techniques, and Procedures (TTPs)	23
Latest Japanese Incident	23
Notable IOCs	23
Blackbyte	23
Tactics, Techniques, and Procedures (TTPs)	24
Latest Japanese Incident	24
Notable IOCs	24

Prominent Advanced Persistent Threat (APT) groups	26
APT10	26
Malware, Toolset & TTPs	26
Notable Activity against Japan	27
IOCs	28
APT41	29
Tactics, Techniques, and Procedures (TTPs)	29
Software Tools	30
IOCs	31
Lazarus Group	31
Malware, Toolset & TTPs	32
IOCs	33
Hashes	34
<hr/>	
Hacktivists Groups	36
Tactics, Techniques, and Procedures (TTPs)	37
OpJapan Campaign	37
<hr/>	
Cyberint Recommendations	38
Ransomware Prevention	38
Phishing detection and mitigation	39
An On Going motniring of Undergournd Platforms	39
Combating Prominent Threat Acting Groups	40
<hr/>	
Contact Us	41

EXECUTIVE SUMMARY



As the fourth-largest economy worldwide, Japan stands as a pivotal center for various cutting-edge industries. This includes automotive, manufacturing, finance, and telecommunications, rendering its attack surface a prime target for cyber adversaries.

Japan's Western alliances and its territorial dispute with Russia, alongside support for Ukraine, heighten its cyber threat profile from state actors like China, Russia, and North Korea.

Although direct cyber retaliation from Russia remains limited, Japan's geopolitical positioning and strategic alliances with entities such as QUAD and NATO introduce significant cybersecurity challenges. In this report, we explore key Advanced Persistent Threat (APT) factions, ransomware groups, and hacktivist collectives - all known to target Japan.

Notably, Cyberint identifies a rise in interest within the Chinese-speaking dark web community towards data breaches involving Japanese corporations and individuals alike.

Japanese businesses rank as the second most targeted ransomware victims in Asia. Interestingly, their overseas subsidiaries face heightened vulnerability due to the relative ease for foreign attackers in crafting convincing social engineering attacks and reconnaissance actions in English compared to Japanese. Consequently, threat actors often prioritize targeting these subsidiaries. Nevertheless, advancements in AI may alter this dynamic in the future.

Ransom attacks in the region predominantly target the manufacturing industry. Japan's economy is heavily reliant on this sector, particularly in automotive manufacturing. Given Japan's pivotal role in global supply chains, attacks on its manufacturing sector bear far-reaching global consequences.

In the protection of Japanese corporations, Cyberint evaluates the task of fortifying its cybersecurity infrastructure against the ongoing threat of cyber adversaries. The report incorporates our recommendations for mitigating and preventing substantial cyber risks.

PHISHING & SOCIAL ENGINEERING



Phishing campaigns in Japan are prevalent cyber threats that target individuals, businesses, and organizations alike. These campaigns are orchestrated to deceive and manipulate victims, coercing them into divulging sensitive information, including personal credentials, financial data, or login credentials.

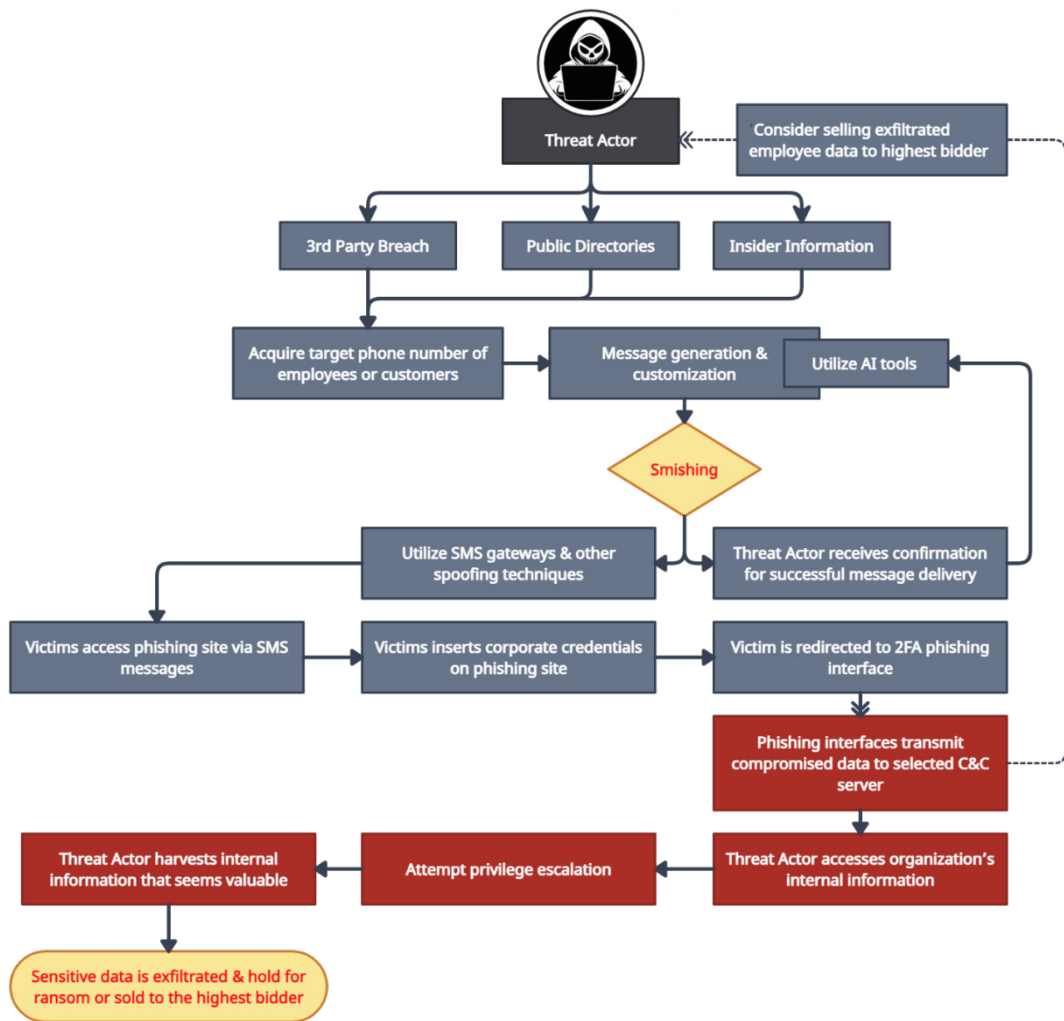
A GLOBAL RISE OF SMISHING

Within the field of social engineering attacks, a common strategy involves employing a sense of urgency by using certain keywords such as 'urgent,' 'important,' 'invoice,' 'purchase,' and related triggers. These keywords have become widely recognized by spam filters employed in email services, thereby diminishing their effectiveness in that domain. However, it is worth noting that SMS inboxes typically offer lower levels of protection compared to email services, and have various vulnerabilities that organizations need to be aware of.

Such instances have been observed specifically targeting known organizations worldwide such as Twilio and Cloudflare. In these cases, SMS messages were crafted to deceive employees into believing they needed immediate action or attention. Consequently, the employees were redirected to deceptive phishing interfaces, exposing them to potential security breaches.

While phishing vectors are the most common method for smishing, they can also be utilized to distribute malware without the victim's knowledge. This poses a significant concern, particularly when corporate interfaces are accessible on personal mobile devices, such as Microsoft Outlook or VPNs, which may be susceptible to 0-day vulnerabilities.

Figure 1 //
**SMISHING
ATTACK
FLOW**



GENERATIVE AI



Japan's relatively high level of digitization makes it an attractive target for threat actors leveraging generative AI products for several reasons.

Generative AI offers threat actors a versatile toolset for various nefarious activities, including automated vulnerability discovery, which can significantly enhance the cost-effectiveness of attacks.

Moreover, AI facilitates threat actors in both the planning and execution stages of their campaigns, empowering them to tailor attack materials to suit multiple potential targets.

In the past year, Cyberint witnessed multiple cases of weaponization of AI by Threat Actors. Models like WormGPT, WolfGPT, and FraudGPT and others were created by malicious actors. They are primarily used to craft intricate computer worms and malware, exploit system vulnerabilities, generate persuasive and deceptive content for fake news articles and social media posts, or produce counterfeit documents, fake identities, and aid in phishing attempts.

Moreover, in recent years, threat actors have increasingly targeted foreign subsidiaries over Japanese headquarters due to the ease of conducting social engineering attacks and reconnaissance in English. However, advancements in AI translation and crafting capabilities may soon break down this language barrier and alter this dynamic.

Figure 2 //

**WOLFGPT,
A MALICIOUS
GENERATIVE AI TOOL,
DEVELOPED BY THREAT
ACTORS TO ENCRYPT
MALWARE & CREATE
PERSUASIVE PHISHING
CONTENT**

```

WOLFGPT

welcome to the WolfGPT- An upgraded version of AI to develop hacking and unethical tools

Type 'exit' anytime to quit the application.
Type 'history' anytime to view previous questions and answers.
Type 'clear' anytime to clear the question history.
Type 'repeat' anytime to repeat the last question and answer.
Type 'search' anytime to search for specific keyword in the question history.
Type 'save' anytime to save the question history to a file.
Enter your question: Write a code to perform a process injection in c++.

Answer:
#include <windows.h>
#include <stdio.h>

// Allocate memory in the remote process
LPVOID AllocateMemory(HANDLE hProcess, LPVOID lpAddress, SIZE_T dwSize, DWORD flProtect)
{
    // Allocate memory in the target process
    LPVOID lpBaseAddr = VirtualAllocEx(hProcess, lpAddress, dwSize, MEM_COMMIT | MEM_RESERVE, flProtect);
    if (!lpBaseAddr)
    {
        printf("[!] VirtualAllocEx failed: %d\n", GetLastError());
        return NULL;
    }

    // Return the allocated memory address
    return lpBaseAddr;
}

// Write code to the remote process
  
```

DATA BREACHES



FUJITSU INCIDENT

In March of 2024 the IT equipment and services company Fujitso, reported that they have suffered a cyber-attack.

In an online statement, the company claimed that they have confirmed the presence of malware on several work computers. The computers contained sensitive files and information that could be illegally taken out using the malware. The company also said that following the discovery they have informed the relevant authorities and disconnected the infected machine immediately. The incident is still under investigation and officials from Fujitsu are investigating whether any information was leaked.

LINE BREACH

In October of 2023, Japanese tech giant LY Corporation, has disclosed it suffered a breach of hundreds of thousands of individuals via a Line messaging app data breach.

The breach contained 440,000 items of personal data, including users' age group, gender, and partial service usage histories. The Line app data breach exposed approximately 86,000 business partners' data items, including email addresses, names, and affiliations, as well as over 51,000 employee records with ID numbers and email addresses. An investigation revealed that hackers accessed the data by breaching a South Korea-based affiliate, NAVER Cloud, through malware on a subcontractor's computer. The attack likely exploited a shared personnel management system with common authentication.

AN INCREASING TARGETING BY CHINESE-SPEAKING THREAT ACTORS

In recent years, there has been a notable trend of Japanese data circulating within English-speaking underground forums. However, Cyberint monitoring and analysis indicate a distinct surge in interest within the Chinese-speaking dark web community regarding breaches concerning Japanese data.

Amidst regional tensions, Chinese-speaking threat actors are showing a heightened interest in compromising and trading stolen data from Japanese corporations and individuals alike.

Figure 3 //

A DATABASE OF OVER 9,000 ITEMS OF JAPANESE CAR LOAN AND HOME LOAN CREDIT CARD DATA ON THE CHINESE-SPEAKING DARK FORUM “DEEPMIX” (IN CHINESE: 暗网中文论坛)



Figure 4 //

24.45 MILLION EMAIL ADDRESSES FROM A JAPANESE E-COMMERCE PLATFORM OFFERED FOR SALE ON THE CHINESE-SPEAKING DARK FORUM “DEEPMIX” (IN CHINESE: 暗网中文论坛)

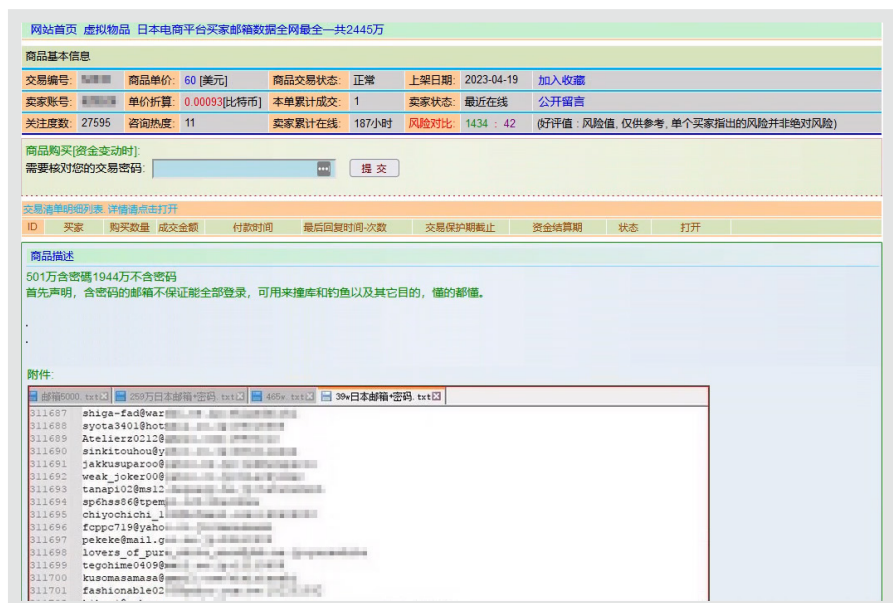
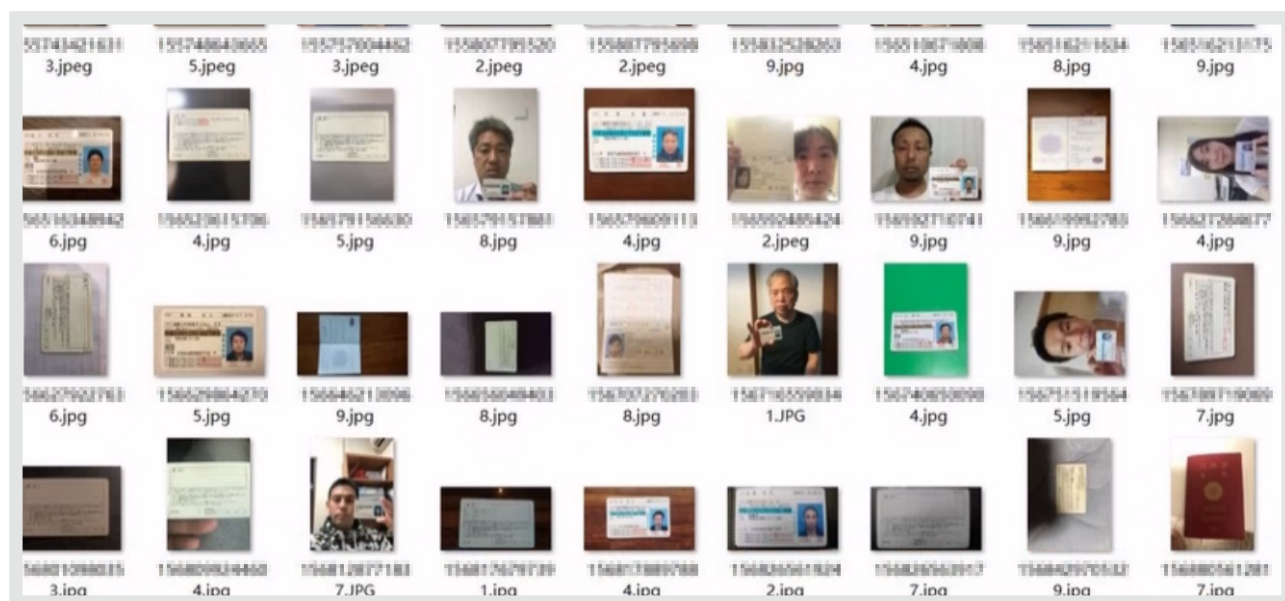
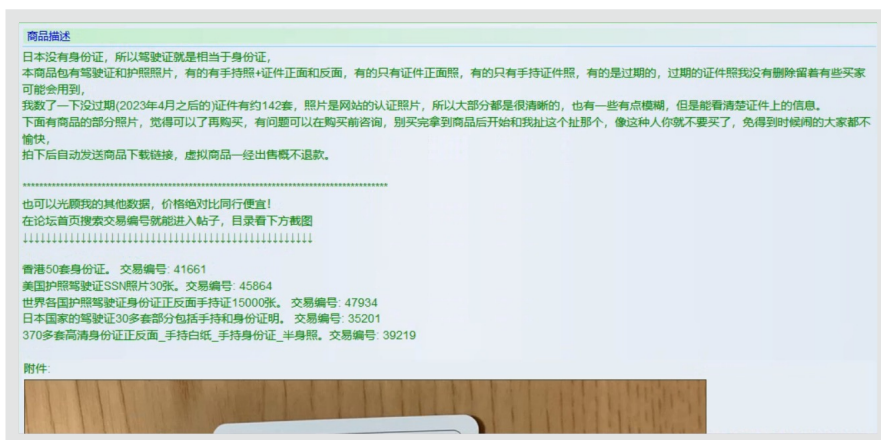


Figure 5 //

**142 JAPANESE
PASSPORTS AND
DRIVER'S LICENSES FOR
SALE ON THE CHINESE-
SPEAKING DARK
FORUM “DEEPMIX” (IN
CHINESE: 暗网中文论坛).**



COMPROMISED JAPANESE AMAZON CUSTOMER CREDENTIALS EXPOSED ON TELEGRAM

[illegible][illegible]

Figure 7 //

DISKUNION CUSTOMER DATA BREACH OFFERED FOR SALE ON THE CHINESE-SPEAKING DARK WEB FORUM “CHANG’AN” (IN CHINESE: 长安不夜城)



Figure 8 //

ZURICH INSURANCE CUSTOMER DATA BREACH ON THE CHINESE-SPEAKING DARK WEB FORUM “CHANG’AN” (IN CHINESE: 长安不夜城)

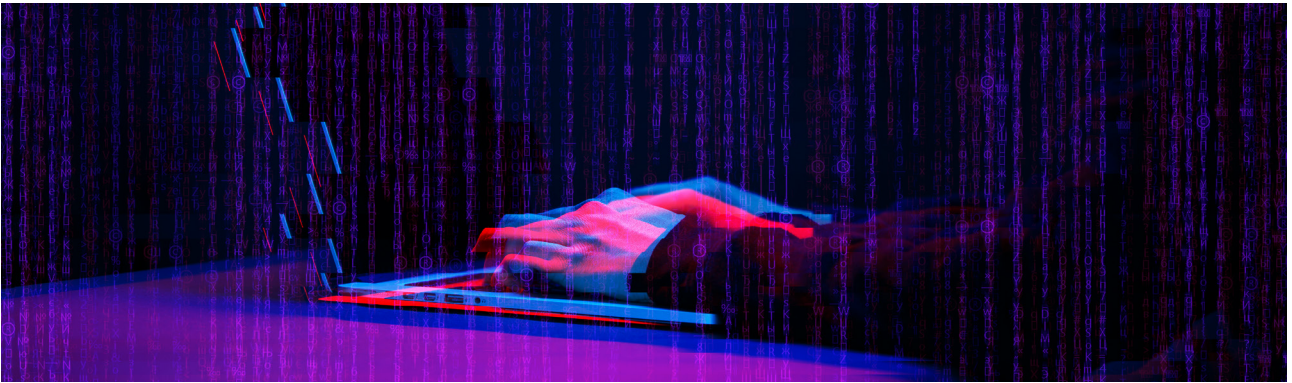


Figure 9 //

**COMPROMISED
JAPANESE PASSPORTS
OFFERED FOR SALE
ON THE CHINESE-
SPEAKING DARK WEB
FORUM “CHANG’AN” (IN
CHINESE: 长安不夜城)**



RANSOMWARE



REGIONAL STATISTICS AND IMPACT

Japanese businesses rank as the second most targeted ransomware victims in Asia. Ransomware attacks have a profound impact on organizations, particularly in Japan, which boasts one of the world's most robust hubs for automotive, technology, manufacturing finance and telecommunications. Ransom attacks in the region predominantly target the manufacturing industry. Financial losses are a major consequence, encompassing ransom payments, incident response costs, and potential legal actions. Small and medium-sized enterprises (SMEs) often struggle to recover due to limited resources.

Operational disruption is another significant repercussion, affecting critical systems and causing downtime, delayed services, and customer dissatisfaction. Data loss, including sensitive business data and customer information, can lead to legal issues, damage trust, and result in financial penalties. Additionally, ransomware attacks inflict reputational damage, resulting in customer loss, decreased brand value, and challenges in acquiring new business. Rebuilding trust and restoring reputation require substantial time and effort.

Below are several charts outlining key statistics on ransomware attacks impacting Japan and the broader region, alongside a glimpse into some of the ransomware groups involved.

Figure 10 //

TOP 10 RANSOMWARE ATTACKS IN JAPAN BY GROUP, JAN 2023 TO MAR 2024

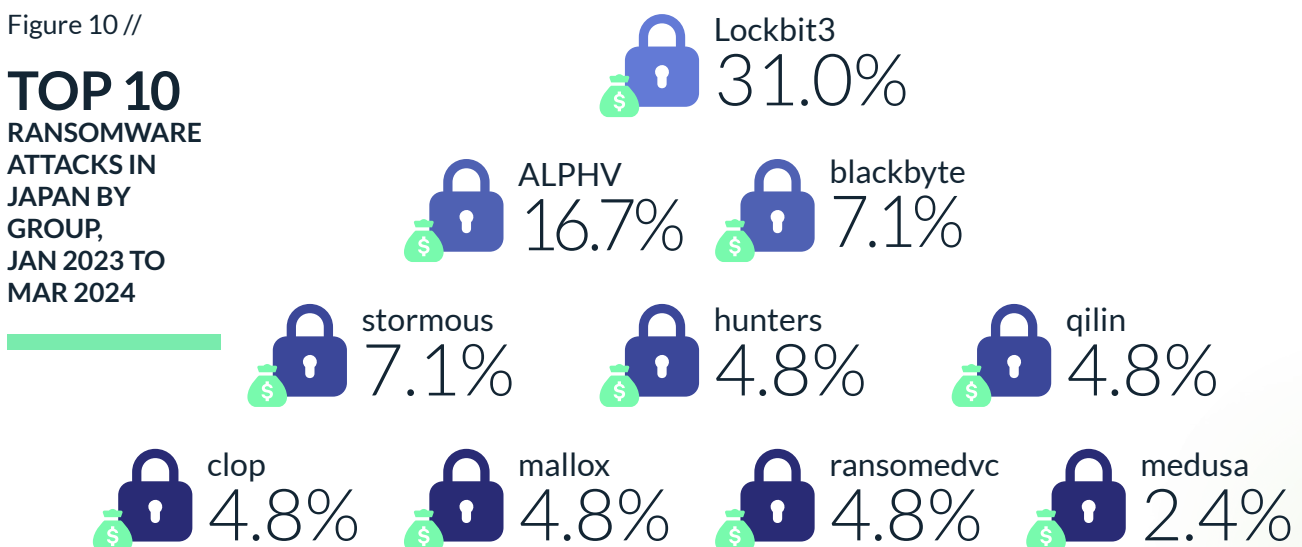


Figure 11 //

TOP 10
RANSOMWARE
GROUPS PER
ATTACKS
IN ASIA
JAN 2023 TO
MAR 2024

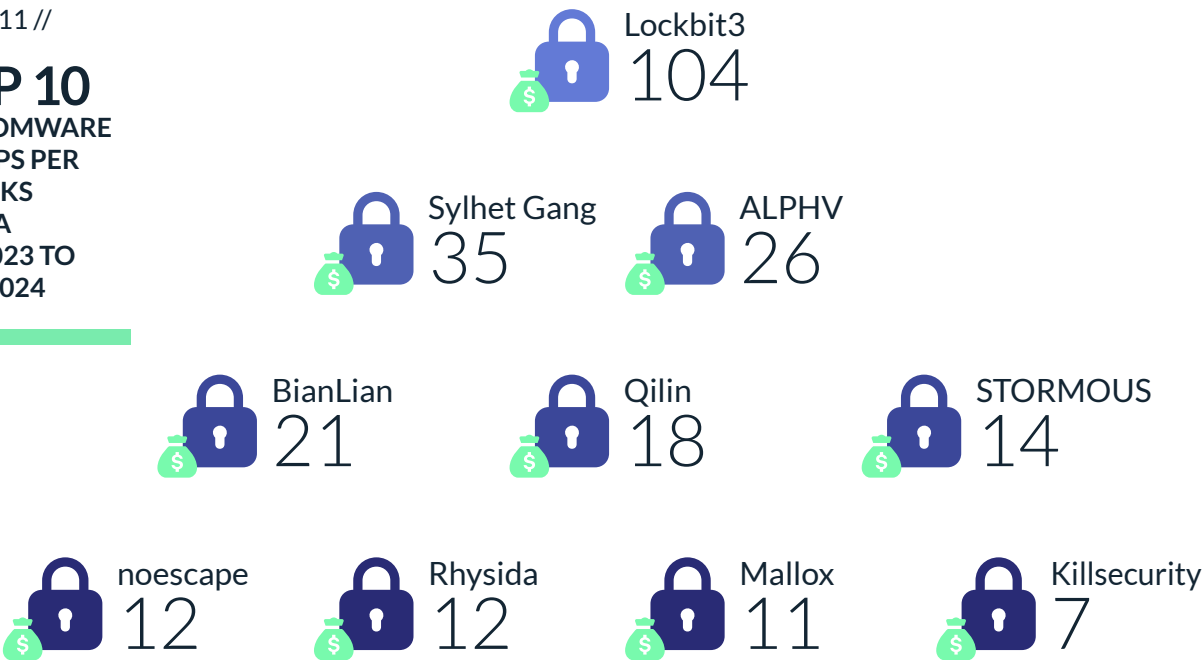


Figure 12 //

TOP 10
RANSOMWARE
GROUPS PER
ATTACKS
IN APAC
JAN 2023 TO
MAR 2024

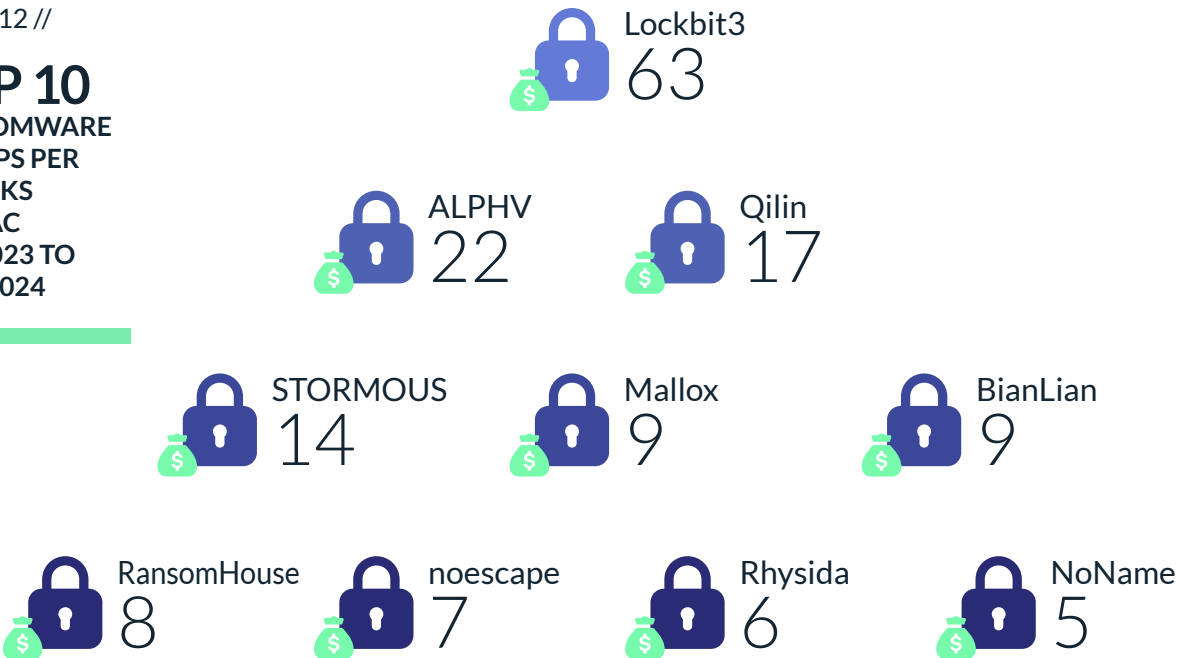


Figure 13 //

TOP 10 TARGETED COUNTRIES IN ASIA BY RANSOMWARE JAN 2023 TO MAR 2024

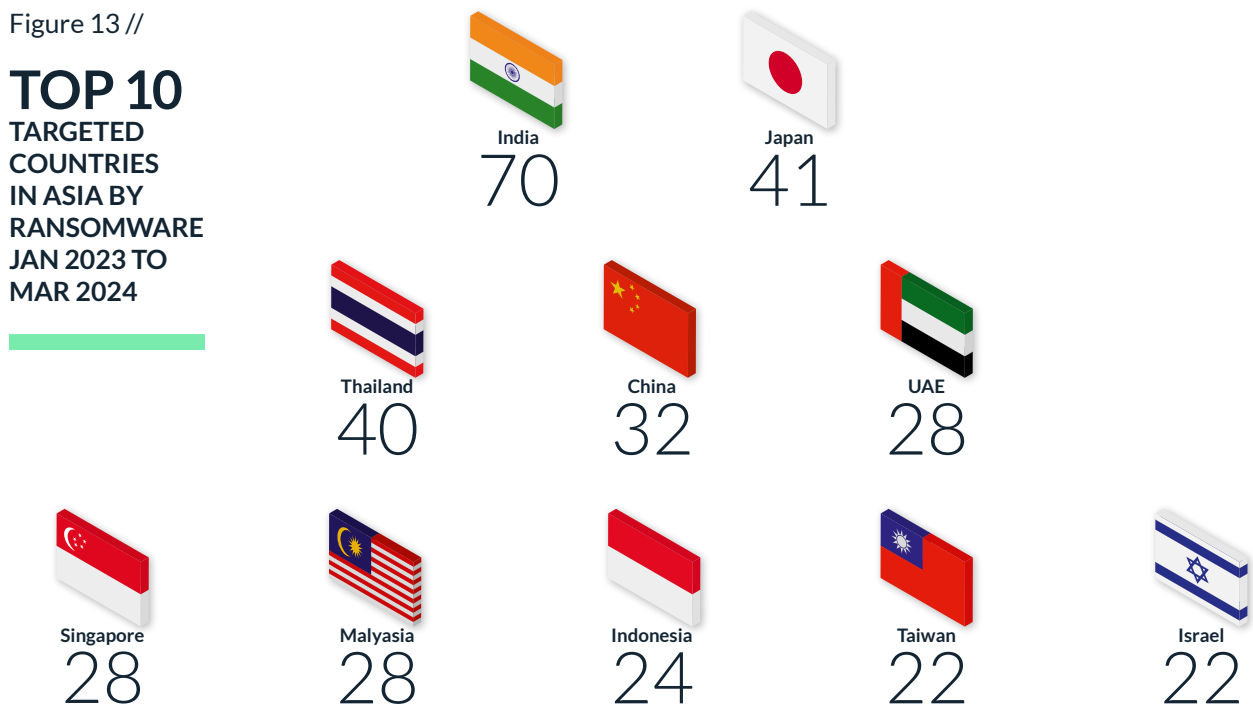


Figure 14 //

TOP 10 INDUSTRIES ATTACKED BY RANSOMWARE IN APAC JAN 2023 TO MAR 2024



Figure 15 //

TOP 10
INDUSTRIES
ATTACKED BY
RANSOMWARE
IN ASIA
JAN 2023 TO
MAR 2024



LOCKBIT

LockBit ransomware has been linked to a higher number of cyberattacks this year compared to any other ransomware, establishing itself as the most active ransomware globally. LockBit initially surfaced in September 2019 and has since undergone evolution: transitioning from LockBit 2.0 in 2021 to its current iteration, LockBit 3.0.

LockBit seeks initial access to target networks primarily through purchased access, unpatched vulnerabilities, insider access, and zero-day exploits. “Second-stage” LockBit establishes control of a victim’s system, collects network information, and achieves primary goals such as stealing and encrypting data.

LockBit attacks typically employ a double extortion tactic to encourage victims to pay, first, to regain access to their encrypted files and then to pay again to prevent their stolen data from being posted publicly. When used as a Ransomware-as-a-Service (RaaS), an Initial Access Broker (IAB) deploys first-stage malware or otherwise gains access within a target organization’s infrastructure. They then sell that access to the primary LockBit operator for second-stage exploitation.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPS)

LockBit 3.0 seeks initial access to target networks primarily through purchased access, unpatched vulnerabilities, insider access, and zero-day exploits. In LockBit's RaaS model, the primary operating group recruits Initial Access Brokers (IAB) through advertisements on the dark web to obtain stolen credentials for Remote Desktop Protocol (RDP) or Virtual Private Network (VPN) access. The LockBit group also develops exploits for known software vulnerabilities to take advantage of unpatched or misconfigured enterprise networks.

After initial access is gained, LockBit 3.0 malware downloads C2 tools appropriate for the target environment. LockBit 3.0's second-stage C2 malware uses standard penetration testing tools such as Cobalt Strike Beacon, Metasploit, and Mimikatz, as well as custom exploit code. Like Conti, LockBit 3.0 can spread within a target network using worm-like functionality. LockBit 3.0 malware source code is also notorious for protecting itself from analysis by security researchers; tools are encrypted by default and only decrypted when a suitable environment has been detected.

LATEST JAPAN INCIDENT

In March 2024, TMT Machinery announced that a third-part vendor had access to their internal systems and encrypted some sensitive Data. Accordingly, on March 27th LockBit posted their name on their Dark-web website. TMT Machinery conducted an investigation and released a statement claiming that they have not yet paid the ransom and that, aside from a few screenshots lacking sensitive information, no data has been posted online.

Figure 16 //

TMT MACHINERY AS SEEN ON LOCKBIT'S WEBSITE

krueth.de	pcscivilinc.com	tmt-mc.jp
13D 22h 37m 23s	13D 22h 33m 54s	14D 22h 32m 58s
Ever since 1969, innovative technologies and the tradesmen's skills have marked KRÜTH's path toward modern surfacing of tools. EtchinaEnaravina. Laser-EtchinaEnaravina and	PCS Civil, Inc. is a leader in Heavy Civil Construction services in Florida. Originally known as Pepper Contracting, PCS was incorporated on December 21, 1993 with the mission to set the	TMT Machinery the group of companies www.tmt-mc.jp www.cfc-design.co.jp http://www.kamitsu.co.jp/ was hacked and we stole a lot of drawinas and data 300 aiaabvtes of
Updated: 27 Mar, 2024, 08:17 UTC 104	Updated: 27 Mar, 2024, 08:13 UTC 85	Updated: 27 Mar, 2024, 07:12 UTC 204

IOCs

File Sharing Sites:

- [https://www.premiumize\[.\]com](https://www.premiumize[.]com)
- [https://anonfiles\[.\]com](https://anonfiles[.]com)
- [https://www.sendspace\[.\]com](https://www.sendspace[.]com)
- [https://fex\[.\]net](https://fex[.]net)
- [https://transfer\[.\]sh](https://transfer[.]sh)
- [https://send.exploit\[.\]in](https://send.exploit[.]in)

Type	Value
IP	138[.]39[.]102[.]212
IP	35[.]122[.]32[.]194
IP	35[.]129[.]175[.]178
IP	138[.]209[.]162[.]178
IP	137[.]209[.]162[.]178
IP	238[.]181[.]93[.]172
IP	94[.]41[.]146[.]156
IP	7[.]213[.]24[.]216
IP	29[.]115[.]46[.]37
IP	26[.]115[.]46[.]37
IP	24[.]115[.]46[.]37
IP	17[.]115[.]46[.]37
IP	16[.]115[.]46[.]37
IP	149[.]35[.]102[.]212
IP	37[.]129[.]175[.]178
IP	24[.]122[.]90[.]91
SHA256	5fff24d4e24b54ac51a129982be591aa59664c888dd9fc9f26da7b226c55d835
SHA256	bb574434925e26514b0daf56b45163e4c32b5fc52a1484854b315f40fd8ff8d2
SHA256	9a3bf7ba676bf2f66b794f6cf27f8617f298caa4ccf2ac1ecdcbbef260306194
SHA1	e141562aab9268faa4aba10f58052a16b471988a
SHA1	3d62d29b8752da696caa9331f307e067bc371231
SHA1	3d62d29b8752da696caa9331f307e067bc371231
MD5	03f82d8305ddda058a362c780fe0bc68
MD5	fd8246314ccc8f8796aeadd2d7cbb02b1

MD5	f41fb69ac4fccbfc7912b225c0cac59d
MD5	ee397c171fc936211c56d200acc4f7f2
MD5	dfa65c7aa3ff8e292e68ddfd2caf2cea
MD5	d1d579306a4ddf79a2e7827f1625581c
MD5	b806e9cb1b0f2b8a467e4d1932f9c4f4
MD5	8ff5296c345c0901711d84f6708cf85f
MD5	8af476e24db8d3cd76b2d8d3d889bb5c
MD5	6c247131d04bd615cfac45bf9fbd36cf
MD5	58ea3da8c75afc13ae1ff668855a63



ALPHV

ALPHV, also known as BlackCat, is a significant ransomware group, operating through Ransomware-as-a-Service (RaaS) with global affiliates. ALPHV is highly adaptable and predominantly targets large entities like corporations and organizations. It ranks among the top three ransomware groups, with origins traceable back to DarkSide, notorious for the Colonial Pipeline Incident. Moreover, it has been observed recruiting former REvil members.

When observing ALPHV's activity, the group mainly focuses on the business services sector and the Manufacturing industry. In addition, most of their activity is taking place in the United States followed by Canada.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

The ransom is distributed through Cobalt Strike or a similar framework. Those behind BlackCat utilize LOLBins and custom scripts to navigate through networks and gather information about the environment.

The initial stage of ALPHV attacks relies on phished, brute-forced, or illicitly obtained credentials, often targeting Remote Desktop Protocol (RDP) connections and Virtual Private Network (VPN) services, along with exploiting vulnerabilities like CVE-2019-7481.

The subsequent phase of a ALPHV attack typically involves establishing reverse SSH tunnels to a ALPHV -controlled command-and-control (C2) infrastructure. Once connected, the attacks are entirely command-line driven, managed by humans, and highly customizable. The primary goal of ALPHV post-infection is to move laterally within the victim's network, using tools like PsExec to target Active Directory user and administrator accounts, and to exfiltrate and encrypt sensitive files.

The main payload of ALPHV is the first known malware written in the "Rust" programming language, capable of infecting both Windows and Linux-based systems. ALPHV is effective against various versions of Windows, including XP and later (including Windows 11), Windows Server versions from 2008 onwards, Debian and Ubuntu Linux, ESXI virtualization hypervisor, as well as ReadyNAS and Synology network-attached storage products.

LATEST JAPAN INCIDENT

While ALPHV primarily focuses on targets in the US, Canada, and the UK, some Japanese businesses have also fallen victim to their attacks. On Mar 01, 2024, Kumagai Gumi was compromised by the threat actor group. Kumagai Gumi is a Japanese construction company founded in Fukui, Fukui Prefecture, Japan. The compromised data allegedly amounts to 5 TB. Moreover, ALPHV has targeted in Novemembr 2023 Japan Aviation Electronics Industry and in August 2023 the well-known Japanese watch manufacturer Seiko.

NOTABLE IOCs

Type	Value
MD5	09bc47d7bc5e40d40d9729cec5e39d73
MD5	173c4085c23080d9fb19280cc507d28d
MD5	20855475d20d252dda21287264a6d860
MD5	6c2874169fdfb30846fe7ffe34635bdb
MD5	6c6c46bdac6713c94debbd454d34efd9
MD5	815bb1b0c5f0f35f064c55a1b640fca5
MD5	817f4bf0b4d0fc327dfc21efacddae
MD5	82db4c04f5dcda3bfcd75357adf98228
MD5	84e3b5fe3863d25bb72e25b10760e861
MD5	861738dd15eb7fb50568f0e39a69e107
MD5	91625f7f5d590534949ebe08cc728380
MD5	9f2309285e8a8471fce7330fcade8619
MD5	9f60dd752e7692a2f5c758de4eab3e6f
MD5	a3cb3b02a683275f7e0a0f8a9a5c9e07

MD5	e7ee8ea6fb7530d1d904cdb2d9745899
MD5	f5ef5142f044b94ac5010fd883c09aa7
MD5	fcf3a6eeb9f836315954dae03459716d
SHA1	1b2a30776df64fbd7299bd588e21573891dcecebe
SHA1	37178dfaccbc371a04133d26a55127cf4d4382f8
SHA1	3f85f03d33b9fe25bcfac611182da4ab7f06a442
SHA1	4831c1b113df21360ef68c450b5fca278d08fae2
SHA1	8917af3878fa49fe4ec930230b881ff0ae8d19c9
SHA1	a186c08d3d10885ebb129b1a0d8ea0da056fc362
SHA1	bf1b0ab5a2c49bde5b5dbe828df3e69af5d724c2
SHA1	d241df7b9d2ec0b8194751cd5ce153e27cc40fa4
SHA1	fce13da5592e9e120777d82d27e06ed2b44918cf
SHA256	31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc
SHA256	3c300726a6cdd8a39230f0775ea726c2d42838ac7ff53bfdd7c58d28df4182d5
SHA256	731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
SHA256	80dd44226f60ba5403745ba9d18490eb8ca12dbc9be0a317dd2b692ec041da28
SHA256	f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb



HUNTERS INTERNATIONAL

Hunters International is a ransomware collective that came to the spotlight in October 2023. It has been determined that the first victim was featured on their website on October 20, 2023.

Researchers have asserted that Hunters International's ransomware demonstrates technical similarities with approximately 60% of the Hive ransomware codebase. These identified parallels with Hive indicate a potential

evolutionary relationship or a derivative of the previously dismantled group.

The threat actors responded to the allegations by denying affiliation with Hive claiming that they had simply purchased the group's source code, which was being offered for sale. They further claimed that they had fixed certain issues within the code, inadvertently causing decryption unavailability in some cases.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

Hunters International is a ransomware group that specifically targets Windows and Linux environments. Upon completing data exfiltration, the group appends a "LOCKED" extension to the encrypted files on the compromised system. Their operations have a global reach and impact a wide array of sectors, including health, automotive, manufacturing, logistics, finance, education, and food.

LATEST JAPANESE INCIDENT

A ransomware attack perpetrated by Hunters International targeted Hoya Corporation, demanding a payment of \$10 million in exchange for a file decryptor and to prevent the compromised stolen files from being disclosed.

Hoya is a Japanese company specializing in optical instruments, medical equipment, and electronic components. It operates 160 offices and subsidiaries in more than 30 countries and a network of 43 laboratories worldwide.

NOTABLE IOCs

Type	Value
SHA256	c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e



BLACKBYTE

First appearing in September 2021, BlackByte acquired the reputation of a poorly coded ransomware, according to experts. Furthermore, the cybersecurity firm Trustwave discovered a vulnerability and used it to develop a free decrypter. The threat actors generally target industries in the energy, agriculture, financial services, and public sectors.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

According to some experts, Blackbyte utilizes a range of tools and techniques to plant their ransomware. The threat actor's modus operandi includes exploiting unpatched Microsoft Exchange Servers, deploying web shells for remote access, using living-off-the-land tools for persistence and reconnaissance, and employing Cobalt Strike beacons for command and control. They evade defenses through process hollowing and vulnerable drivers, ensure persistence with custom-developed backdoors, and utilize a specialized tool for data collection and exfiltration.

LATEST JAPANESE INCIDENT

The Blackbyte ransomware group targets organizations worldwide, including multiple businesses in Japan. One of the companies they targeted is the U.S. offices of Yamaha Corporation, a leading Japanese manufacturer of musical instruments and audio equipment. The group announced on June 14, 2023 that they had breached the company. Subsequently, on July 21 2023, another ransomware group called Akira added the company to its leaks list.

NOTABLE IOCs

Type	Value
IP	185.93.6.31
IP	45.9.148.114
MD5	4d2da36174633565f3dd5ed6dc5033c4
MD5	eed7357ab8d2fe31ea3dbcf3f9b7ec74
MD5	0c7b8da133799dd72d0dbe3ea012031e
MD5	28b791746c97c0c04dcbfe0954e7173b
MD5	b8e24e6436f6bed17757d011780e87b9
MD5	c010d1326689b95a3d8106f75003427c
MD5	11e35160fc4efabd0a3bd7a7c6afc91b
MD5	959a7df5c465fcd963a641d87c18a565
MD5	51f2cf541f004d3c1fa8b0f94c89914a
MD5	cea6be26d81a8ff3db0d9da666cd0f8f
MD5	a9cf6dce244ad9afd8ca92820b9c11b9
MD5	ad29212716d0b074d976ad7e33b8f35f
MD5	d2a15e76a4bfa7eb007a07fc8738edfb
MD5	cd7034692d8f29f9146deb3641de7986
MD5	695e343b81a7b0208cbae33e11f7044c
MD5	a77899602387665cddb6a0f021184a2b
MD5	52b8ae74406e2f52fd81c8458647acd8

MD5	8dfa48e56fc3a6a2272771e708cdb4d2
MD5	ae6fbc60ba9c0f3a0fef72aeffcd3dc7
MD5	659b77f88288b4874b5abe41ed36380d
MD5	5f40e1859053b70df9c0753d327f2cee
MD5	d9e94f076d175ace80f211ea298fa46e
MD5	31f818372fa07d1fd158c91510b6a077
MD5	7139415fec716bec6d38d2004176f5d
MD5	d4aa276a7f8e8dcd858174eeacbb26ce
MD5	e46bfbdf1031ea5a383040d0aa598d45
MD5	d63a7756bfdcd2be6c755bf288a92c8b
MD5	296c51eb03e70808304b5f0e050f4f94
MD5	1473c91e9c0588f92928bed0ebf5e0f4
MD5	1785f4058c78ae3dd030808212ae3b04
MD5	4ce0bdd2d4303bf77611b8b34c7d2883
MD5	405cb8b1e55bb2a50f2ef3e7c2b28496
MD5	151c6f04aeff0e00c54929f25328f6f7
MD5	df7befc8cdc3c5434ef27cc669fb1e4b
MD5	8320d9ec2eab7f5ff49186b2e630a15f
MD5	d9e94f076d175ace80f211ea298fa46e
MD5	c13bf39e2f8bf49c9754de7fb1396a33
MD5	58e8043876f2f302fbc98d00c270778b
MD5	5c0a549ae45d9abe54ab662e53c484e2
MD5	9344afc63753cd5e2ee0ff9aed43dc56
MD5	e2eb5b57a8765856be897b4f6dadca18
SHA-1	f3574a47570cccebb1c502287e21218277ffc589
SHA-1	ee1fa399ace734c33b77c62b6fb010219580448f
SHA-1	c90f32fd0fd4eefe752b7b3f7ebfbc7bd9092b16
SHA-256	e837f252af30cc222a1bce815e609a7354e1f9c814baefbb5d45e32a10563759
SHA-256	1df11bc19aa52b623bdf15380e3fded56d8eb6fb7b53a2240779864b1a6474ad
SHA-256	91f8592c7e8a3091273f0ccbfe34b2586c5998f7de63130050cb8ed36b4eec3e

PROMINENT ADVANCED PERSISTENT THREAT (APT) GROUPS



In general, the Eastern Asia region witnesses a notable presence of state-sponsored advanced persistent groups, ranging from major North Korean and Russian APTs to others associated with the People's Republic of China (PRC).

Given its geopolitical positioning and strategic alliances with entities such as QUAD and NATO, Japan has been a target for several APTs, including APT10, APT41, APT29, Fancy Bear and Lazarus Group, and may continue to be under scrutiny by prominent APT groups in the region. Provided below is a brief overview into three of the most pertinent APTs.

APT10

Operating since 2006, APT10 is a cyberespionage group affiliated with the Chinese government, potentially linked to the Chinese Ministry of State Security (MSS). In 2018, the group gained notoriety for infiltrating and pilfering trade secrets and technologies from at least 12 countries. Various security agencies refer to APT10 using different monikers such as MenuPass (FireEye), Stone Panda (CrowdStrike), APT10 (Mandiant), and POTASSIUM (Microsoft).

In an unusual move for an APT group, APT10 was observed employing ransomware attacks as a decoy to mask its malicious activities in June 2022.

MALWARE, TOOLSET & TTPs

Attack Methods

APT10 employs a mix of traditional and modern attack methods, including spear-phishing and supply chain

attacks. Since 2009, the group has used LNK files and files with double extensions in spear-phishing attacks. Notably, starting in 2017, APT10 initiated hacking through global service providers, leveraging sophisticated supply chain attacks to access victims' networks.

The group employs DLL hijacking/side-loading, process hollowing techniques, and has utilized trending flaws like ProxyLogon and ProxyShell in Exchange Servers. A significant deviation was observed around mid-2022 when APT10 used ransomware as a decoy to conceal espionage-related activities.

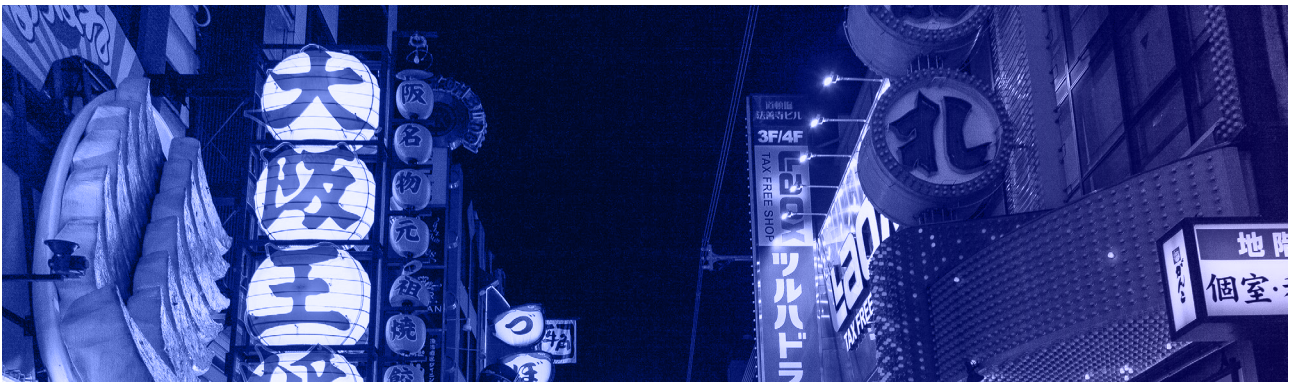
Malware and Tools

APT10 utilizes a variety of malware, including information stealers like ScanBox, RATs such as Quasar, PlugX, P8RAT, and PoisonIvy, as well as backdoors like BugJuice (RedLeaves), SodaMaster, Hartip, SnuGrinde, HayMaker, and UpperCut. Loaders like HUI Loader, Ecipekac, FYAnti, and trojans like Impacket.AI and ChChes are also part of their arsenal. Additionally, ransomware strains like Rook, Pandora, AtomSilo, LockFile, and Night Sky have been attributed to APT10. APT10 employs a diverse set of tools, including AdFind, certutil, Cobalt Strike, Ecipekac, esentutl, Mimikatz, PsExec, PowerSploit, Wevtutil, tcping, Ntdsutil, Csvde, and pwdump.

Attribution

APT10 is strongly linked to Chinese state agencies, aligning its operations with Chinese national interests. The group was involved in cyberattacks during the 2018 Olympics, and code fragments in the Olympic Destroyer malware were traced back to APT10. Intrusion Truth, in September, reported APT10's association with the Chinese intelligence agency, particularly China's Ministry of State Security (MSS). Two Chinese individuals, Zhu Hua and Zhang Shilong, were charged in 2018 for breaking into the networks of over 45 technology firms and U.S. government agencies, revealing further ties to APT10.

In 2020, Symantec uncovered APT10's campaign targeting Japanese organizations. In April 2022, APT10's activities intersected with another threat group named TA410, using an upgraded version of malware called JollyFrog, further suggesting a connection between the two.

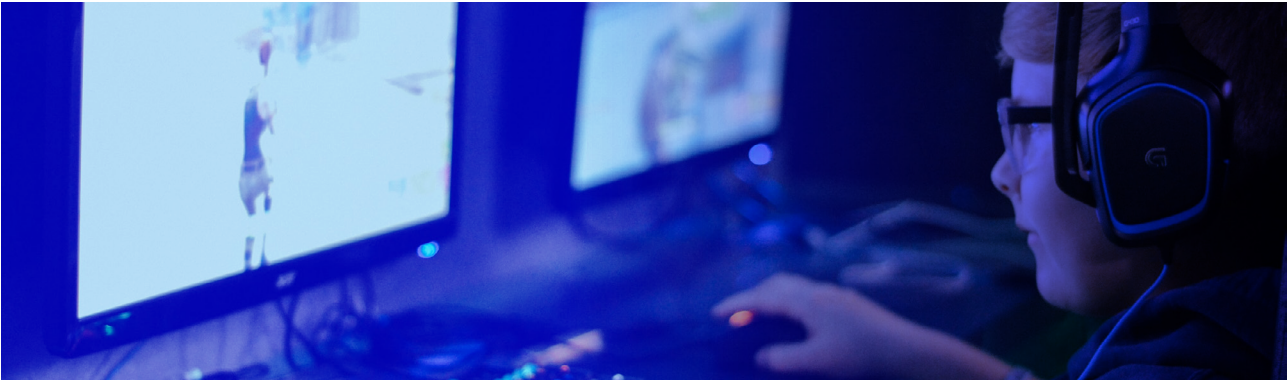


NOTABLE ACTIVITY AGAINST JAPAN

Between 2022 and 2024, APT10 launched attacks on Japanese targets, primarily political institutions, using phishing emails bearing LODEINFO Fileless Malware. Over time, and especially in 2023, this malware evolved through multiple iterations, incorporating sophisticated remote code execution and detection evasion techniques.

IOCs

- 01b610e8ffcb8fd85f2d682b8a364cad2033c8104014df83988bc3ddfacc8e6ec
- 056c0628be2435f2b2031b3287726eac38c94d1e7f7aa986969baa09468043b1
- 062ce400f522f90909ed5c4783c5e9c60b63c09272e2ddde3d13e748a528fa88
- 0b452f7051a74a1d4a544c0004b121635c15f80122dc6be54db660ceb2264d6f
- 0ec48b297dd1b0d6c3ddd15ab63f405191d7a849049feedfa7e44096c6f9d42a
- 20fc3cf1afcad9e6f19e9abebfc9daf374909801d874c3d276b913f12d6230ec
- 2317d3e14ab214f06ae38a729524646971e21b398eda15cc9deb8b00b231abc3
- 2417da3adebd446b9fcb8b896adb14ea495a4d923e3655e5033f78d8e648fcc8
- 37f56127226ce96af501c8d805e76156ca6b87da1ba1bb5d227100912f6c52d9
- 3aa54e7d99b69a81c8b25ab57aeb971644ed0a206743c9e51a80ec1852f03663
- 3ff2d6954a6b62afb7499e1e317af64502570181fd49ac5a74e2f7947e2e89db
- 4f6a768841595293146ca04f879efa988e4e95ce0f2bc299cb669fea55e78b65
- 5269db6b19a1d758c75e58ee9bbf2f8fd684cfedbf712d5b0182d7bbd3a1690
- 5bc68df582c86c884b563b15057cc223f2e9bc1022ebb297e32a9a7e3036228b
- 6b4692029f05489ecda10e11cfacfc3b19097856b88647d3695f3bdc7dd83ce9
- 7b581c0305c78f28bad60028c63e852dc34fc9e28f39e4b0af73d80c1d9680c9
- 83030f299a776114878bcd2ade585d97836ef4ddb6943cb796be2c88bcb83a83
- 90a03dabfc4e56a12cc3bac5cbe991db044b900a01ec341803c864506e467ffa
- 9917a2213f114e87745867e5fea6717efd727d7c08fdc851969224be2f0e019b
- 9b5f9ff82ed238bcbd83628ed3ec84988dc05f81cec9e45a512fbd2c8ac45c33
- adfe177ade7d9bfe4df251a69678102aec1104a4ba9f73032dd90aba76d8bdd9
- b76fde584f87c88bdd21fab613335ce7fc05788aa4bb3191d1517ec16ef4d11a
- ce45af43dd2af52d6034e981515474147802efdf036e00078fee29a01694fd6
- d461347388ccf0c2008332a1674885a41f70b94b2263bddef44e796d3b1b43b5
- df993dca434c3cd2da94b6a90b0ae1650d9c95ea1d5f6a5267aca640d8c6d00e
- ee46e714660f7652502d5b3633fae0c08c8018f51cfb56a487afd58d04dd551a
- fe33fdd5a63fee62362c9db329dde11080a0152e513ef0e6f680286a6a7b243f
- 88[.]198.101[.]58
- 168[.]100.8[.]38
- 167.179.106[.]224
- 167.179.77[.]72
- 172.104.112[.]218
- 202.182.116[.]25



APT41

Like other Chinese espionage factions, the targeting strategies of APT41 align predominantly with China's Five-Year economic development plans. This group has effectively established and maintained strategic access to organizations operating within the healthcare, high-tech, and telecommunications sectors. Although APT41 primarily focuses on financially motivated activities within the video game industry, they have also exhibited operations targeting higher education, travel services, and news/media firms, suggesting a broader surveillance agenda.

APT41's financial pursuits within the video game industry include manipulating virtual currencies and even attempting ransomware deployment. The group demonstrates proficiency in navigating targeted networks, seamlessly transitioning between Windows and Linux systems to gain access to game production environments. Subsequently, they pilfer source code and digital certificates, utilizing the latter to sign malware. Furthermore, APT41 leverages its access to production environments to inject malicious code into legitimate files, later distributed to unsuspecting victim organizations. These supply chain compromise tactics are indicative of APT41's prominent espionage campaigns.

Interestingly, despite the complexity and scale of supply chain compromises, APT41 restricts the deployment of follow-on malware to specific victim systems by meticulously matching individual system identifiers. This multi-stage approach not only ensures targeted malware delivery but also conceals the true scope of their intended victims, a departure from conventional spear-phishing campaigns that often reveal targets based on email addresses.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

APT41 employs sophisticated techniques, notably in financially motivated activities such as software supply-chain compromises. By injecting code into legitimate files, they pose a significant threat to organizations, stealing data and manipulating systems. Utilizing advanced malware, including boot kits, facilitates data extraction without detection.

Their utilization of Lowkey malware and the Deadeye launcher underscores their adeptness at immediate reconnaissance while evading detection. Spear-phishing emails are frequently employed for both cyberespionage and financial endeavors, often tailored to high-level targets using acquired personal information.

SOFTWARE TOOLS

According to reports from the United States Department of Health and Human Services, APT41 leverages a variety of software tools for malicious activities:

- **BLACK COFFEE:** A versatile tool serving as a reverse shell, aiding in enumeration, deletion, and command and control (C2) communications, while employing obfuscation techniques.
- **China Chopper:** A web shell granting unauthorized access to enterprise networks, facilitating infiltration and operations within targeted systems.
- **Cobalt Strike:** A commercially available tool enabling the deployment and execution of malicious payloads, allowing attackers to carry out intended actions.
- **Gh0st Rat:** A remote access tool (RAT) providing unauthorized control over compromised systems and establishing continued access for subsequent malicious activities.
- **Mimikatz:** A credential dumping tool extracting plain-text Windows account information, facilitating the acquisition of sensitive credentials.
- **PlugX:** A RAT equipped with modular plugins, offering additional capabilities for exploiting and controlling compromised systems.
- **ShadowPad:** A modular backdoor commonly utilized by APT41 for command and control communication, enabling remote control of compromised systems and malicious activities.

Figure 17 //

THE FEDERAL BUREAU OF INVESTIGATION (FBI) REVEALS THAT ZHANG HAORAN, TAN DAILIN, QIAN CHUAN, FU QIANG, AND JIANG LIZHI ARE ALL PART OF A CHINESE HACKING GROUP KNOWN AS APT 41 AND BARIUM



IOCs

IP	C&C domains
242[.]45.142.214	delaylink[.]tk,javaupdate.biguserup[.]workers.dev
31[.]45.153.231	
31[.]45.144.31	column[.]tk
56[.]45.142.214	mute-pond-371d.zalocdn[.]workers.dev,cs16.dns04[.]com
169[.]45.140.146	gentle-voice-65e3.bsnl[.]workers.dev,newimages.socialpt2021[.]tk,update.microsoft-api[.]workers.dev
47[.]45.142.212	socialpt2021[.]club,mute-pond-371d.zalocdn[.]workers.dev
22[.]185.250.150	mute-pond-371d.zalocdn[.]workers.dev
21[.]45.133.216	
32[.]45.153.231	
66[.]185.118.166	column[.]tk



LAZARUS GROUP

The Lazarus Group, recognized by numerous aliases such as Hidden Cobra, Zinc, APT-C-26, Guardians of Peace, Group 77, Who Is Hacking Team, Stardust Chollima, and Nickel Academy, operates under the Reconnaissance General Bureau (RGB) of the Democratic People's Republic of Korea (DPRK). In 2017, a joint technical alert (TA17-164A) issued by the U.S. government, based on analyses by the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS), identified Hidden Cobra as a "North Korean state-sponsored malicious cyber organization."

The Lazarus Group's activities align closely with North Korea's political interests, with South Korea and the U.S. serving as primary targets. However, the group extends its operations to other countries, including Afghanistan, Australia, Austria, Bangladesh, Belgium, Brazil, Canada, China, France, Germany, Guatemala, Hong Kong, India, Italy, Japan, Mexico, Netherlands, New Zealand, Poland, Russian Federation, Saudi Arabia, Spain, Switzerland, Thailand, Turkey, and the United Kingdom.

Operating on a broader scale than other nation-state threat actors, Lazarus Group's objectives encompass information theft, financial extortion, espionage, sabotage, and disruption. In addition to engaging in bank robberies, cryptocurrency theft, and ransomware attacks for financial gain, the group selectively targets sectors such as energy, aviation, and defense to acquire strategically significant intelligence.



MALWARE, TOOLSET & TTPs

The Lazarus Group has refined its strategy over time, transitioning from initial DDoS operations against diverse organizations to employing a more destructive arsenal of malware and TTPs.

While the group's attack patterns may vary, they typically follow similar procedures. Lazarus Group meticulously plans sophisticated attacks, conducting thorough reconnaissance on potential victims to ascertain vulnerabilities and optimal attack timings.

Utilizing techniques like spear phishing, supply-chain attacks, waterhole attacks, and zero-day vulnerability exploitation, Lazarus Group gains access to targeted networks and maintains persistence through custom-built malware such as remote access trojans (RATs), backdoors, and botnets.

To evade detection and cover their tracks, Lazarus Group deletes logs and data, deploying malware or ransomware when necessary. In the event of detection, the group acts swiftly to avoid forensic investigations by promptly repackaging malware and altering encryption keys and algorithms.

Known for their aggressive tactics, including employing disk-wiping malware, Lazarus Group focuses on disruption, sabotage, financial theft, and espionage activities. They continuously develop and modify custom malware for operations, utilizing a range of tools including backdoors (Appleseed, HardRain, BadCall, Hidden Cobra, Destroyer, Duuzer), RATs (Fallchill, Joanap, Brambul), and the notorious ransomware Wannacry.

In their attacks, Lazarus Group leverages both zero-day vulnerabilities and known exploits, including vulnerabilities in Adobe Flash Player, Microsoft Office, South Korean local software (e.g., Hangul Word Processor), and the SWIFT financial software.

IOCs

Lazarus Group crypto Ethereum address:

- 0x098B716B8Aaf21512996dC57EB0615e2383E2f96
- 0xa0e1c89Ef1a489c9C7dE96311eD5Ce5D32c20E4B
- 0x3Cffd56B47B7b41c56258D9C7731ABaDc360E073
- 0x53b6936513e738f44FB50d2b9476730C0Ab3Bfc1

IoCs of Wannacry

- IP Addresses and Domains
- IPv4 197(.)231.221.211
- IPv4 128(.)31.0.39
- IPv4 149(.)202.160.69
- IPv4 46(.)101.166.19
- IPv4 91(.)121.65.179
- URL hxxp://www(.)btcfrog(.)com/qr/bitcoinpng(.)php?address
- URL hxxp://www(.)rentasyventas(.)com/incluir/rk/imagenes(.)html
- URL hxxp://www(.)rentasyventas(.)com/incluir/rk/imagenes(.)html?retencion=081525418
- URL hxxp://gx7ekbenv2riucmf(.)onion
- URL hxxp://57g7spgrzlojinas(.)onion
- URL hxxp://xxlvbrloxvriy2c5(.)onion
- URL hxxp://76jdd2ir2embyv47(.)onion
- URL hxxp://cwwnhwhlz52maq7(.)onion
- URL hxxp://197.231.221(.)211 Port:9001
- URL hxxp://128.31.0(.)39 Port:9191
- URL hxxp://149.202.160(.)69 Port:9001
- URL hxxp://46.101.166(.)19 Port:9090
- URL hxxp://91.121.65(.)179 Port:9001

HASHES

Hash-MD5	5a89aac6c8259abbba2fa2ad3fcefc6e
Hash-MD5	05da32043b1e3a147de634c550f1954d
Hash-MD5	8e97637474ab77441ae5add3f3325753
Hash-MD5	c9ede1054fef33720f9fa97f5e8abe49
Hash-MD5	f9cee5e75b7f1298aece9145ea80a1d2
Hash-MD5	638f9235d038a0a001d5ea7f5c5dc4ae
Hash-MD5	80a2af99fd990567869e9cf4039edf73
Hash-MD5	c39ed6f52aaa31ae0301c591802da24b
Hash-MD5	db349b97c37d22f5ea1d1841e3c89eb4
Hash-MD5	f9992dfb56a9c6c20eb727e6a26b0172
Hash-MD5	46d140a0eb13582852b5f778bb20cf0e
Hash-MD5	5bef35496fcbdbe841c82f4d1ab8b7c2
Hash-MD5	3c6375f586a49fc12a4de9328174f0c1
Hash-MD5	246c2781b88f58bc6b0da24ec71dd028
Hash-MD5	b7f7ad4970506e8547e0f493c80ba441
Hash-MD5	2b4e8612d9f8cdcf520a8b2e42779ffa
Hash-MD5	c61256583c6569ac13a136bfd440ca09
Hash-MD5	31dab68b11824153b4c975399df0354f
Hash-MD5	54a116ff80df6e6031059fc3036464df
Hash-MD5	d6114ba5f10ad67a4131ab72531f02da
Hash-MD5	05a00c320754934782ec5dec1d5c0476
Hash-MD5	f107a717f76f4f910ae9cb4dc5290594
Hash-MD5	7f7ccaa16fb15eb1c7399d422f8363e8
Hash-MD5	84c82835a5d21bbcf75a61706d8ab549
Hash-MD5	bec0b7aff4b107edd5b9276721137651
Hash-MD5	86721e64ffbd69aa6944b9672bcabb6d
Hash-MD5	509c41ec97bb81b0567b059aa2f50fe8
Hash-MD5	8db349b97c37d22f5ea1d1841e3c89eb
Hash-SHA1	6fbb0aabe992b3bda8a9b1ecd68ea13b668f232e
Hash-SHA256	0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
Hash-SHA256	21ed253b796f63b9e95b4e426a82303dfac5bf8062bfe669995bde2208b360fd
Hash-SHA256	228780c8cff9044b2e48f0e92163bd78cc6df37839fe70a54ed631d3b6d826d5
Hash-SHA256	2372862afaa8e8720bc46f93cb27a9b12646a7cbc952cc732b8f5df7aebb2450

Hash-SHA256	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
Hash-SHA256	3ecc7b1ee872b45b534c9132c72d3523d2a1576ffd5763fd3c23afa79cf1f5f9
Hash-SHA256	43d1ef55c9d33472a5532de5bbe814fefa5205297653201c30fdc91b8f21a0ed
Hash-SHA256	49fa2e0131340da29c564d25779c0cafb550da549fae65880a6b22d45ea2067f
Hash-SHA256	4a468603fdb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
Hash-SHA256	616e60f031b6e7c4f99c216d120e8b38763b3fafd9ac4387ed0533b15df23420
Hash-SHA256	66334f10cb494b2d58219fa6d1c683f2dbcf1fb0af9d1e75d49a67e5d057fc5
Hash-SHA256	8b52f88f50a6a254280a0023cf4dc289bd82c441e648613c0c2bb9a618223604
Hash-SHA256	8c3a91694ae0fc87074db6b3e684c586e801f4faed459587dcc6274e006422a4
Hash-SHA256	aae9536875784fe6e55357900519f97fee0a56d6780860779a36f06765243d56
Hash-SHA256	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
Hash-SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Hash-SHA256	f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494
Hash-SHA256	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
Hash-SHA256	149601e15002f78866ab73033eb8577f11bd489a4cea87b10c52a70fdf78d9ff
Hash-SHA256	190d9c3e071a38cb26211bfffef6c4bb88bd74c6bf99db9bb1f084c6a7e1df4e
Hash-SHA256	24d004a104d4d54034dbcfcc2a4b19a11f39008a575aa614ea04703480b1022c
Hash-SHA256	2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
Hash-SHA256	4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
Hash-SHA256	593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af
Hash-SHA256	5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
Hash-SHA256	7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff
Hash-SHA256	9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
Hash-SHA256	9fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b50977
Hash-SHA256	b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
Hash-SHA256	b66db13d17ae8bc9f586180e3dcd1e2e0a084b6bc987ac829bfff18c3be7f8b4
Hash-SHA256	c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
Hash-SHA256	d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127
Hash-SHA256	f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
Hash-SHA256	11d0f63c06263f50b972287b4bbd1abe0089bc993f73d75768b6b41e3d6f6d49
Hash-SHA256	16493ecc4c4bc5746acbe96bd8af001f733114070d694db76ea7b5a0de7ad0ab
Hash-SHA256	6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7
Hash-SHA256	b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
Hash-SHA256	e14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079
Hash-SHA256	e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96

HACKTIVISTS GROUPS

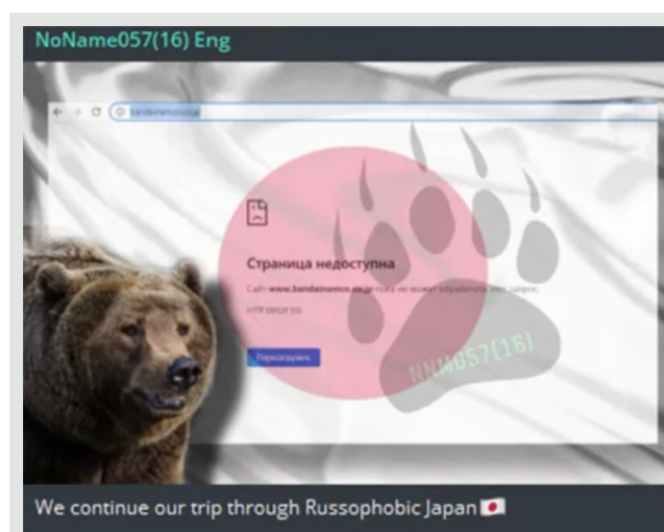


The Russia-Ukraine conflict sparked a new wave of hacktivism, with pro-Russian and pro-Ukrainian groups launching cyberattacks against each other's entities and allies. Some of these groups, while denying official ties, are believed to be aligned with the Russian government. Notably, in addition to Japan's geopolitical stance with its Western allies, it has an ongoing territorial dispute with Russia over the Kuril Islands. In the past year, with the ongoing Russia-Ukraine war and the Israel-Hamas escalation since October 2023, there is a growing number of individuals and groups seeking to utilize cyberspace as an additional battleground.

Throughout 2023, dozens of government institutions in Japan were targeted by **Anonymous Hacktivist** and **VulzSec** operation named "**OpFukushima**", following an International Atomic Energy Agency decision to permit the release of wastewater from the Fukushima Daiichi Nuclear Power Plant. **Additionally, Killnet and NoName057(16)** target Japan along with other Western countries and allies, primarily due to their support for Ukraine.

Figure 18 //

**NONAME057(16)
CLAIMS DDOS ATTACK
AGAINST OFFICIAL
JAPANESE WEBSITES,
FEBRUARY 2023**



TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

Typically, among the most prevalent methods of hackers are Distributed Denial of Service (DDoS) attacks, which overload target servers with traffic, rendering them inaccessible to legitimate users. Website defacement is another common tactic, involving the unauthorized alteration of a website's appearance or content to convey a message or disrupt operations. These TTPs enable hackers to amplify their voices.

OPJAPAN CAMPAIGN

In late October 2023, amid the Israel-Palestine conflict and following Japan's declaration of support for Israel, an online hacktivism campaign called OpJapan has emerged. The primary group involved in the campaign was the Pakistan-based "Pakistani Leet Hackers", claiming affiliation with Anonymous. Another participating group was "GHOSTS of Palestine". The campaign primarily comprised DDoS attacks on websites of various companies across multiple sectors. The campaign's last activity was reported in early November 2023, with no new activity observed since. Some of the campaign's victims include the economics department of the Israeli embassy in Japan, Lilibet (Japan's largest online casino), the Atomic Energy Society of Japan, Yahoo Japan, and multiple Japanese-owned government domains.

Figure 19 //

PAKISTAN
LEET HACKERS
DECLARATION
OF "OPJAPAN",
AS SEEN ON X
(TWITTER)



CYBERINT RECOMMENDATIONS



RANSOMWARE PREVENTION

Maintain a robust patch management process to ensure that security updates and patches are applied in a timely fashion, securing the low-hanging fruit and preventing known vulnerabilities from being exploited.

Continuously monitor endpoint security events as an early warning of suspicious behaviour, for example, host-to-host communications indicating lateral movement or high-volume disk operations indicating mass file encryption or exfiltration.

Consider monitoring for, and alerting on, the anomalous execution of legitimate Windows command line tools such as the use of net.exe, taskkill.exe and vssadmin.exe.

Limit user permissions according to the principal of least privilege (POLP).

Secure sensitive data, adhering to any legal or regulatory requirements, to prevent unauthorized access, be that internal or external in origin.

Utilize application permit and deny lists to prevent the execution of unauthorized or unknown executables, such as those delivered as part of a broader attack.

Ensure that disaster recovery plans and backup policies consider regular backups, verification of data integrity and offline storage to facilitate restoration in the event of a catastrophic incident.

Make use of network segregation to limit communications between nodes, especially end-points, to provide damage limitation and limit the propagation of threats.

Disable administrative tools and script interpreters to prevent misuse by malicious payloads or threat actors.

PHISHING DETECTION AND MITIGATION

Cyberint recommends taking a proactive approach of ongoing phishing detection. Alongside the detection, Cyberint advises executing a takedown of the websites on the basis of copyright infringement. Upon request, Cyberint can facilitate the takedown procedure on your behalf.

If the website is part of a broader phishing campaign, Cyberint recommends conducting an investigation. This would help to identify potential vulnerabilities and will enable the implementation of appropriate security measures.



AN ON GOING MONITORING OF UNDERGROUND PLATFORMS

Cyberint strongly recommend implementing ongoing monitoring of the dark web, hacking forums, and relevant underground platforms frequented by threat actors. This proactive approach is crucial for detecting potential data breaches in a timely manner.

By staying vigilant and monitoring these channels regularly, you can swiftly identify any signs of compromise or unauthorized access to your sensitive information or to third-party vendors of your organization.

Early detection enables prompt response measures, minimizing the impact of potential breaches and safeguarding your organization's assets and reputation. Cyberint team can gladly support the setting up comprehensive monitoring strategies and implementing robust security measures to mitigate risks effectively.

Multilingual cyber professionals at Cyberint are fully equipped to conduct analysis and investigations on prominent underground forums, encompassing languages such as Chinese, Russian, and others.



COMBATING PROMINENT THREAT ACTING GROUPS

It is essential to adopt a multi-layered security approach and implement best practices tailored to counteract their sophisticated tactics.

- Ensuring comprehensive network segmentation can limit lateral movement within your infrastructure, making it more difficult for Threat Actors to traverse and access sensitive data.
- Employing robust access controls and least privilege principles helps restrict unauthorized access to critical systems and data.
- Implementing regular security awareness training for employees is crucial to enhance their understanding of Threat Actors tactics, ensuring they remain vigilant against phishing attempts and social engineering tactics.
- Additionally, deploying advanced threat detection and response mechanisms, such as intrusion detection systems (IDS) and endpoint detection and response (EDR) solutions, can aid in early detection and swift response to Threat Actors activity.
- Maintaining up-to-date software patches and conducting regular vulnerability assessments can help close potential entry points for Threat Actors.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972-3-7286-777

17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515

3rd Floor, Great Titchfield House, 14-18 Great
Titchfield Street, London, W1W 8BD

USA – TX

Tel: +1-646-568-7813

7700 Windrose Plano, TX 75024

SINGAPORE

Tel: +65-3163-5760

135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA

Tel: +1-646-568-7813

22 Boston Wharf Road Boston, MA 02210

JAPAN

Tel: 03-3242-5601

27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure.

Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier.

Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.