Japan and Its Global Business Footprint

The Cyber Threat Landscape Report

Paul Prudhomme, Principal Security Analyst

RAPID7

CONTENTS

INTRODUCTION AND SCOPE

Japan has the world's third-largest economy, after the United States and China. It is the country of origin for many global businesses, through which Japan has a major footprint in the economies of other countries. Despite Japan's great economic significance, there is relatively little English-language coverage of cyber threats to Japanese companies and key Japanese industries, such as automotive, manufacturing, financial services, and technology, media, and telecommunications.

Rapid7 aims to help close this gap in English-language coverage of the Japanese cyber threat landscape by covering threats to Japanese organizations, based on our own data and third-party sources. Rapid7 would nonetheless like to acknowledge the work of researchers at the JPCERT, whose English-language publications shed valuable light on the Japanese threat landscape.

This paper enumerates threats to Japanese organizations by relevant industry and highlights two key cross-industry phenomena: ransomware and state-sponsored threats. Certain industries are more salient targets than others, given their greater economic significance. For example, the Japanese automotive industry is a large part of the Japanese economy and its overseas footprint. It is thus not surprising that Japanese automotive companies have been the victims of many of the documented attacks on Japanese organizations. Financial services organizations are key targets in any economy, and Japan is no different, especially in light of its wealth. Japanese cryptocurrency exchanges and other Japanese sources of cryptocurrency nonetheless stand out as key targets, in addition to the traditional financial sector. Japanese companies in the technology, media, and telecommunications sector are also significant targets for a variety of reasons relevant to consumers, businesses, and governments.

The geographic scope of this threat landscape extends beyond the borders of Japan to include the overseas operations, subsidiaries, affiliates, and other holdings of Japanese businesses. Many Japanese brands have such extensive presence overseas that we did not limit the scope of this research to incidents within Japanese territory. Compromises of Japanese-owned businesses overseas can facilitate attacks on their Japanese parent companies, such as via lateral movement across an internal network, compromised credentials, or other means. Disruptions of overseas industrial operations that produce components for their parent Japanese manufacturing companies can also have supply chain implications for the latter, if the former experience disruptive ransomware or Industrial Control System (ICS) malware attacks.

A review of incidents affecting Japanese companies indicates that many began with compromises of overseas subsidiaries or affiliates, enabling attackers to move laterally into the infrastructure of the Japanese parent company. The most marked example of this phenomenon is the pair of attacks that a major Japanese shipping company experienced in March and June 2021, respectively. In both cases, the attackers reportedly gained access to the shipping company's systems in Japan through the compromise of an overseas subsidiary.

We believe that there are two possible explanations for the recurring use of compromised overseas subsidiaries as an access vector for compromising Japanese companies. Overseas subsidiaries may have less optimal security oversight due to a variety of factors. The acquisition of new overseas holdings may bring previously existing security issues into the fold of a new parent company. Even those overseas holdings that originated under the auspices of the parent company may develop separate hierarchies that coordinate less with the parent company. Large global businesses also face many impediments to optimal communication and coordination, such as a variety of different business, technology, legal, and regulatory environments, time zone differences, and language barriers.

The second explanation also involves language barriers. All other things being equal, criminal actors tend to prefer targets whose language they speak, as a shared language makes it easier to conduct social engineering attacks on them and exploit compromised data. The Japanese language has a large number of speakers, but the vast majority of them are inside Japan. Overseas subsidiaries of Japanese companies that operate in English or other more widely spoken languages may be more linguistically accessible (and thus more desirable) targets for foreign criminals lacking Japanese language skills.

RANSOMWARE

Ransomware is a major criminal threat to organizations around the world, and Japan is no different. Indeed, enough Japanese organizations have become victims of ransomware attacks that this phenomenon deserves special consideration in its own right, separate from other types of criminal threats.

The salience of manufacturing, including automotive manufacturing, within the Japanese economy gives it high exposure to ransomware risks. Indeed, most of the incidents affecting Japanese manufacturing organizations outside the automotive industry that were reviewed for coverage in this report were ransomware incidents. Criminals that compromise manufacturing organizations often end up using ransomware against them, or selling their unauthorized access to these networks to ransomware operators. The types of data that manufacturing organizations typically possess is often harder for criminals to monetize via fraud or sale to other criminals. It may thus be more cost-effective for them to encrypt data for ransom and/or threaten to disclose it for another layer of ransom. Manufacturing organizations may also be desirable targets for ransomware operators due to a perception that they are more vulnerable to extortion via the disruption of manufacturing operations and lower tolerance for downtime.

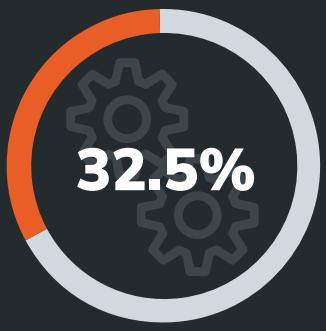
For example, Honda experienced a ransomware attack in June 2020 that disrupted its customer service, financial services, and some manufacturing operations as the company responded to the incident. The perpetrators specifically targeted Honda; a sample of the Snake/EKANS ransomware submitted from a Japanese IP address around that time actively searched for internal Honda network domains to trigger the file encryption process. The targeting of a vehicle manufacturer suggests that the perpetrators may have hoped that the disruption of manufacturing operations would pressure the victim to pay the ransom. Snake is unusual among ransomware families in that it targets some ICS processes for termination. It is unknown if the perpetrators used that ICS process termination capability in this attack on Honda, and if any use of such ICS capabilities contributed to the disruption of Honda manufacturing operations.

The Snake incident was not Honda's first experience with ransomware and its potential to disrupt manufacturing operations. The global WannaCry ransomware outbreak of 2017 infected Honda, as well as the Japanese vehicle manufacturer Nissan and the French vehicle manufacturer Renault. Those WannaCry infections of the three automotive companies disrupted some of their respective manufacturing operations.

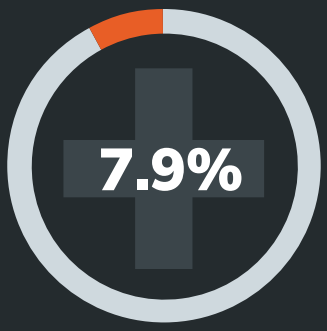
Ransomware attacks can disrupt vehicle manufacturing operations indirectly via disruptions of their suppliers. For example, in September-October 2019, Subaru of Indiana Automotive temporarily shut down its manufacturing operations in connection with "a supplier issue" and a ransomware incident. In December 2021, a Japanese automotive components manufacturer which is part of the Toyota Group experienced a ransomware attack by Rook ransomware operators. They claimed to have compromised 1.1 TB of data. The company reported that the attack had little impact on its domestic Japanese assets but did manage to infect a manufacturing facility in Mexico, possibly compromising the personally identifiable information (PII) of its workers.

According to Japan's National Police Agency (NPA), 32.5% of the reported Japanese victims of ransomware attacks in the first half of 2022 were in the manufacturing sector. This percentage of manufacturing victims of ransomware was far higher than that of healthcare victims, whose industry is normally considered a top target for ransomware but represented only 7.9% of the Japanese victims in this sample. In the vast majority of cases in which the attack vector was apparent, the ransomware operators gained access to their targets via either VPNs or the Remote Desktop Protocol (RDP).

Ransomware: Japanese Manufacturers Favored Over Healthcare



of ransomware attacks reported in the first half of 2022 were in the manufacturing sector.



of ransomware attacks reported in the healthcare industry during that same period.

Source: National Police Agency (NPA), Japan

Rapid7 researchers observed that, as of late 2022 and early 2023, LockBit 3.0 ransomware operators were targeting Japanese organizations in general and manufacturers in particular. Ransomware attacks on Japanese manufacturers that disrupt their operations can have implications for manufacturing supply chains worldwide, as many foreign manufacturers depend on supplies of Japanese components. For example, in October 2022, LockBit 3.0 operators claimed to have compromised the Japanese manufacturer Oomiya. Oomiya supports the supply chains of organizations in multiple industries, including automotive, manufacturing, telecommunications, semiconductors, and healthcare. The attackers threatened to disclose compromised Oomiya data if the company did not pay the ransom.

This late 2022-early 2023 campaign was not the first time that operators of LockBit variants targeted Japanese manufacturing organizations. As early as September 2020, Rapid7 researchers observed that operators of the original version of LockBit had disclosed data that they claimed to have obtained from a compromise of a Japanese manufacturer. that produces industrial robots, servos, motion controllers, AC motor drives, and switches.

Since 2020, Rapid7 has observed several additional examples of ransomware data disclosures and threats thereof against Japanese manufacturing organizations. A layer of data disclosure extortion has become a common feature of ransomware attacks, including attacks on manufacturers. The types of data that some manufacturers possess may be harder for criminals to monetize in ways other than using the threat of its disclosure to extort ransom, or an extra layer of ransom, from victims. Indeed, some attacks involve no file encryption at all but merely threaten to disclose compromised data.

Panasonic India experienced a data disclosure extortion incident in October 2020, resulting in the release of more than 4 GB of sensitive data. The Russian-speaking attacker demanded a ransom of $500,000 USD to refrain from disclosing the data and offered to sell other criminals the compromised data and unauthorized network access for $40,000 USD if the victim refused to pay the ransom. The disclosed data included bank account numbers, accounting records, credentials, and information about vendors, customers, and employees. A separate ransomware incident later affected the company's Canadian operations in February 2022. Conti ransomware operators leaked data that they claimed to have obtained from the breach, including HR and accounting records.

Similarly, Nissan Canada Finance (NCF), which finances the purchase or lease of cars from Nissan, INFINITI and Mitsubishi dealers, received a ransom demand in December 2017. The extortionist provided a sample of NCF customer data and threatened to disclose it if NCF did not pay the ransom. NCF's investigation yielded no evidence of a breach and indicated instead that an insider abused legitimate access to the customer data of fewer than 300,000 NCF customers for the purpose of the extortion attempt.

More typical, however, are those attacks that involve both file encryption and data disclosure extortion. In April 2021, Astro Locker ransomware operators disclosed data that they claimed to have obtained from a compromise of a Japanese manufacturer of optical products for the technology and healthcare industries. The 300 GB of compromised data included financial records, production details, email correspondence, patient data, network credentials, and safety reports (Figure 1).

U.S.-based subsidiaries or branches of Japanese parent companies that produce materials or components for subsequent stages of the manufacturing process have become targets. For example, in December 2020, Rapid7 researchers observed that DopplePaymer ransomware operators disclosed data that they claimed to have obtained from a compromise of Mitsubishi Polysilicon, a U.S.-based part of Japan-based Mitsubishi Materials Corporation. Mitsubishi Polysilicon produces silicon for semiconductor manufacturing. The sample of compromised data included Human Resources records, invoices, and lists of machines on the company's network.

Similarly and also in December 2020, Rapid7 researchers reported that Netwalker ransomware operators disclosed data that they claimed to have obtained from a compromise of NTN Bearing Corporation of America, a U.S.-based subsidiary of the Japan-based NTN Corporation. The U.S.-based subsidiary produces ball bearings, constant-velocity joints, and other industrial and automotive components. The compromised data included financial records, sales documents, and employees' PII.

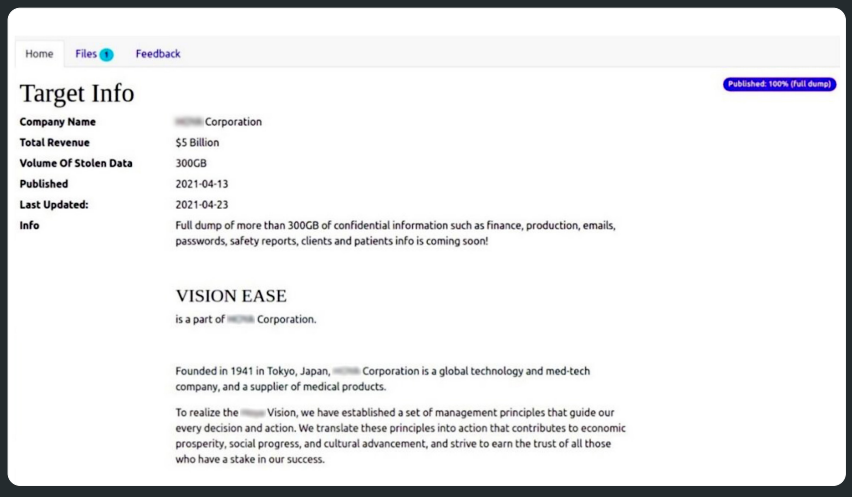


FIGURE 1

STATE-SPONSORED THREATS

Japan is a significant target for state-sponsored threats. Historic and more recent tensions with Japan's Chinese, North Korean, and Russian neighbors, three of the four state sponsors of cyber attacks that security researchers cover most frequently, make Japan a potential target for political, diplomatic, military, and other national security reasons. Additionally, Japan's advanced, affluent economy also makes it a target for state-sponsored actors seeking economic or financial gain via the compromise of Intellectual Property (IP) or the theft of funds — including cryptocurrency, which has become a significant target in Japan.

Japan accordingly revised its National Security Strategy (NSS) in December 2022 to improve both its conventional military defensive posture, as well as its cyber defense posture. The Russian invasion of Ukraine was a key factor in this revision, but other threats include the growth of Chinese military power and North Korea's ballistic missile program. The revised NSS also called for a more active defense against cyber attacks that hostile foreign governments are increasingly likely to integrate into a "hybrid warfare" strategy against Japan, along with conventional military force.

Chinese Cyber Espionage

IP theft is a common goal of Chinese cyber espionage groups. Japan is a significant target for such IP theft both as a regional economic competitor of China and also as the potential source of a large amount of valuable IP in key industries, such as manufacturing, automotive, and technology. For example, a subset of Chinese APT10 activity known as "Earth Tengshe" or "Bronze Riverside" targeted mostly Japanese manufacturing, engineering, electronics, automotive, energy, and technology companies and their overseas subsidiaries in the "A41APT" campaign, as of late 2021. This campaign targeted overseas subsidiaries and suppliers of Japanese companies in what security researchers believe was an attempt to gain access to the parent companies in Japan. Researchers believed that the attackers may have hoped to exploit reduced oversight at overseas subsidiaries and vendors to bypass tighter security in Japan.

An adjacent subset of APT10 activity, known as "Bronze Starlight," took IP theft to another level in mid-2021 by disguising IP theft attacks as ransomware and data disclosure extortion attacks. The presumed goal of this strategy is to prevent victimized businesses from discovering the IP theft goals of these attacks. We believe that understanding the true purpose of these attacks would enable those targeted businesses to adjust their business strategies to mitigate the competitive consequences of the exposure of their IP to competitors. File encryption also has the added advantage of concealing forensic evidence of any earlier cyber espionage, and the incident response to the ransomware might distract security teams from previous exfiltration of files with IP content. Japanese targets of this Bronze Starlight activity included designers and manufacturers of electronic components.

Chinese subsidiaries of or vendors for Japanese companies present Chinese actors with opportunities to target the Japanese parent companies or clients. For example, Japanese press reports attributed the 2019 compromise of a Japanese electronics manufacturer to the Chinese cyber espionage group Tick, also known as "Bronze Butler." The breach exposed information on both private and public sector clients, including Japanese defense and critical infrastructure organizations. The breach reportedly began within a Chinese affiliate of the business. The compromise of a server at this Chinese affiliate enabled the attackers to move laterally into the rest of the company. The attackers exploited a zero-day directory traversal and arbitrary file upload vulnerability in malware detection software (CVE-2019-18187).

Another Chinese cyber espionage group, LuoYu, specifically targeted Chinese subsidiaries of Japanese technology companies in 2021 with its WinDealer modular backdoor. As of mid-2022, LuoYo had begun leveraging automatic update services to deliver WinDealer to targets in "Man-on-the-Side" (MotS)" or "Quantum Insert" attacks. MotS attacks preempt client-server communications by timing their own malicious responses to beat the legitimate traffic to its destination before the latter arrives.

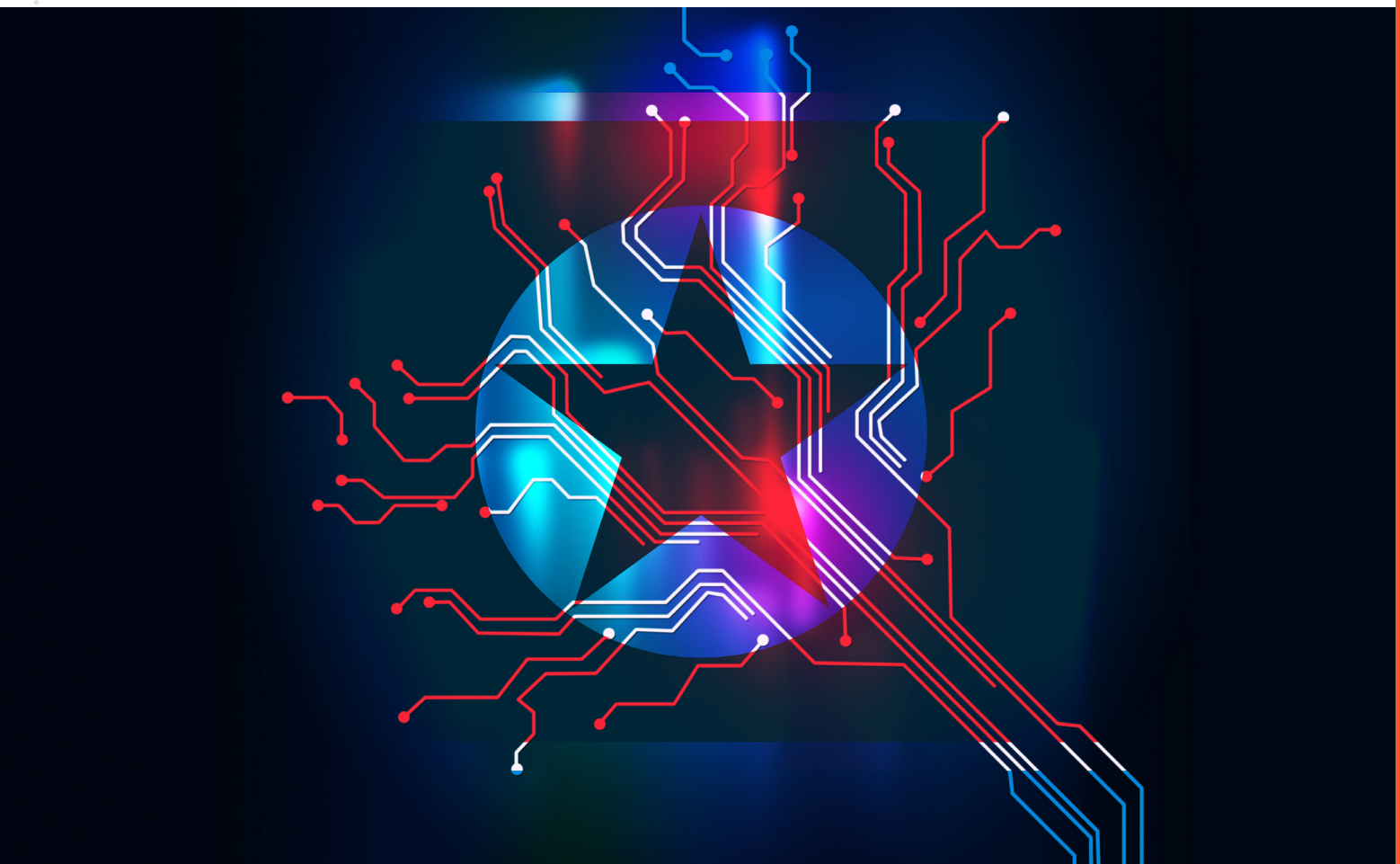
The risk of exposing Japanese data to China via Chinese subsidiaries of Japanese companies, even without an actual attack, generated headlines in March 2021. It emerged that engineers at a Chinese affiliate of the Japanese chat app Line had access to the personal data of Line's approximately 86 million Japanese users, including names, phone numbers, street and email addresses, and identification numbers, via servers in Japan. Japan's government accordingly ordered officials to stop using Line.

Japan and its government are significant targets for Chinese cyber espionage for political, diplomatic, and military reasons. Chinese BlackTech actors were reportedly responsible for the May 2021 breach of a cloud-based information sharing software-as-a-service (SaaS) platform, which exposed data for many Japanese government agencies. The company's investigation revealed that attackers used compromised credentials to blend in with legitimate traffic and disguise the malicious nature of their activities. The perpetrators of the breach sought information on Japan's nuclear power plants and the Tokyo Olympics. BlackTech has historically used its Flagpro malware in attacks on Japanese defense, telecommunications, and media organizations. As recently as September 2022, BlackTech exploited CVE-2022-1388, a vulnerability in F5 BIG-IP devices, in attacks on Japanese organizations.

In June-July 2022, the Chinese threat group MirrorFace conducted its "Operation LiberalFace" spearphishing campaign against Japanese political targets, particularly members of a Japanese political party. It is believed that MirrorFace may be part of, or have some connection to, the more well-documented APT10. MirrorFace has historically pursued other Japanese targets of a political, military, diplomatic, or academic nature. The timing of this campaign corresponded to the eve of a Japanese House of Councillors election in July 2022. The messages impersonated a Japanese political party and specifically referenced the upcoming election. The malicious email messages in this campaign delivered MirrorFace's proprietary LODEINFO malware, which compromised targets' credentials, email communications, and files. Of note, MirrorFace specifically searched for files with the extension ".jtd," which is for files from the Japanese word processor Ichitaro, made by JustSystems Corporation. LODEINFO also used a malicious file impersonating a legitimate JustSystems executable as part of its infection chain.

North Korea and Its Criminal Operations

In October 2022, a statement from Japan's National Police Agency and Financial Services agency warned of North Korean Lazarus Group attacks on Japanese cryptocurrency exchanges. It alluded to the occurrence of recent incidents but did not provide further identifying details and mentioned phishing and social engineering as attack vectors. Recently, cryptocurrency has been a preferred target for North Korean criminal operations because it enables them to collect revenue outside of traditional financial institutions.



The Lazarus Group may have been targeting Japanese cryptocurrency holdings as far back as 2018, if not earlier. A United Nations (UN) report attributed the 2018 compromise of Japanese cryptocurrency exchange Coincheck to the Lazarus Group. This compromise yielded approximately $533 million USD. The exact means of compromise remained unclear, but Coincheck had been storing the stolen cryptocurrency in "hot wallets," which are more vulnerable to compromise because of their accessibility from the Internet, compared to more secure offline "cold wallets."

Cryptocurrency exchanges are not the only potential sources of cryptocurrency. A late 2021 campaign attributed to the Bluenoroff subset of the Lazarus Group impersonated a Japanese venture capital firm specializing in financial services, technology, and financial technology (FinTech) in attacks that aimed to steal cryptocurrency from victims. It included a malicious domain spoofing the name of the Japanese venture capital firm and lure documents pertaining to investment opportunities.

The traditional Japanese financial sector — specifically Japanese banks and venture capital firms — was the target of a fall 2022 campaign also attributed to BlueNoroff. The group registered fake domains for this campaign, most of which spoofed the names of Japanese financial organizations. The campaign used unconventional file formats, such as .iso and .vhd, to avoid triggering alerts warning users of files downloaded from the Internet. The use of Japanese file names in malicious files from this campaign, such as one alluding to a bonus chart, underscored its focus on the Japanese financial sector.

Ransomware is another source of criminal revenue for the Lazarus Group. A Japanese housing company was the first victim of Maui ransomware, attributed to the separate Andariel subset of the Lazarus group, in April 2021. A comparison of the compilation date of the Maui payload with the timing of the incident at the Japanese company indicated the latter must have been the first victim. Andariel compromised the network of the Japanese company in December 2020, using the reverse proxy tool 3proxy to maintain persistent access. After a "dwell time" of 3-4 months, Andariel deployed its DTrack reconnaissance tool shortly before deploying Maui.

The Lazarus Group also conducts more conventional cyber espionage, including IP theft, in addition to its distinctive criminal operations. It was reportedly responsible for a series of early-mid 2022 attacks on energy organizations in Japan and North America that aimed to steal their IP. This campaign exploited vulnerabilities in VMWare Horizon Servers to gain initial access to these energy organizations and install the Lazarus Group's proprietary YamaBot malware, which JPCERT documented and is compatible with both Windows and Linux operating systems.

Japan is also a significant target for North Korean espionage for political, diplomatic, and military reasons. In mid-2021, Japanese incident responders observed a series of phishing and malware email attacks on Japanese defense and media professionals specializing in North Korea. The social engineering content of these malicious email messages pertained to North Korea. The tools used in these attacks were consistent with those attributed to the North Korean cyber espionage group Kimsuky.

The Russia and Ukraine War

In September 2022, the pro-Russian hacktivist group Killnet claimed responsibility for DDoS attacks on the websites of Japanese government organizations and private sector companies. Killnet targets countries (such as Japan) that have taken actions against Russia (such as sanctions) in response to the Russian invasion of Ukraine. It is important to note that Killnet has denied that it is state-sponsored and accused Japan of "militarism."

The timing of a February 2022 ransomware attack on a components supplier for Toyota fueled suspicions of Russian responsibility for the incident. The ransomware attack, which caused Toyota to suspend manufacturing operations in Japan briefly, came shortly after the Russian invasion of Ukraine. The Russian Ambassador to Japan had previously warned Japan against participation in international sanctions against Russia for its invasion of Ukraine. In any event, the disruption in production also affected Toyota subsidiaries Hino and Daihatsu. Toyota's practice of "just-in-time manufacturing," a characteristic of some Japanese manufacturing business culture, left it more vulnerable to a supply chain disruption. This practice calls for moving materials or components from suppliers immediately into production, rather than maintaining a stockpile in reserve.

Vietnam and Foreign Competitors

The Vietnamese APT32, also known as OceanLotus, has demonstrated a special interest in the targeting of foreign competitors of Vietnam's budding automotive industry. An anonymous official at one of the largest Japanese automotive manufacturers reportedly confirmed in 2019 that APT32 had targeted that company and its overseas operations. Security researchers observed that APT32 had created domains to spoof that automotive manufacturer's legitimate infrastructure as an attack vector. The targeting of the Japanese automotive manufacturer's operations may have aimed to provide a means of access to the infrastructure of the parent Japanese company.

Untethered Threat Group: Earth Yako

One cyber espionage group specifically targeting Japan remains difficult to attribute to any one foreign country, although some researchers have identified potential Chinese, Korean, and Russian suspects. "Earth Yako" has been targeting Japanese organizations — including public sector, energy, and academic organizations — since at least October 2021 and is most well-known for its "Operation RestyLink" campaign. Earth Yako used social engineering content pertaining to Japanese foreign relations in East Asia to deliver .zip archives containing malicious .lnk and .iso files. The attackers even used Japanese IP addresses, presumably in an effort to appear Japanese to their Japanese targets. Subsequent infection stages featured the Cobalt Strike penetration testing framework and the open source C2 framework Covenant. The use of such off-the-shelf tools impedes attribution. Earth Yako remained active as of January 2023.

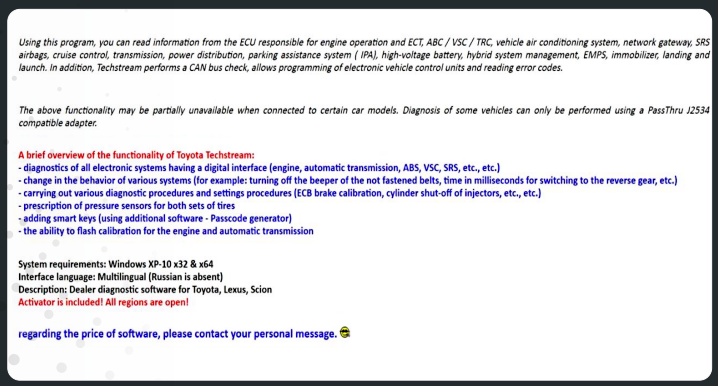
TARGET INDUSTRIES

Automotive

The automotive industry stands out as a key target within the Japanese threat landscape. Japan's automotive industry is large, many of its companies have extensive overseas presence, and its brands have a large footprint among consumers worldwide. The automotive industry has exposure to a wide variety of threats, including: product security threats to the technology in their vehicles; incidents that disrupt manufacturing operations, such as ransomware attacks; the compromise of customer data; third-party breaches at vendors or other partners compromising their own data or systems; and security misconfigurations that leave organizations more vulnerable to attacks.

Product Security Threats

Product security is a significant consideration for automotive manufacturers, as vehicles themselves and the technology within them are targets of interest for some attackers. Tools and techniques for attacks on cars, including Japanese brands, are available in underground criminal forums. For example, in June 2019, Rapid7 researchers observed that criminal forum username "Oleg-Maslov" offered to sell access to an unauthorized copy of Toyota Techstream, a dealership diagnostic tool. Threat actors could abuse this legitimate software to conduct reconnaissance on targeted vehicles and collect information with which to plan an attack (Figure 2).



Using this program, you can read information from the ECU responsible for engine operation and ECT, ABC / VSC / TRC, vehicle air conditioning system, network gateway, SRS airbags, cruise control, transmission, power distribution, parking assistance system (IPA), high-voltage battery, hybrid system management, EMPS, immobilizer, landing and launch. In addition, Techstream performs a CAN bus check, allows programming of electronic vehicle control units and reading error codes.

The above functionality may be partially unavailable when connected to certain car models. Diagnosis of some vehicles can only be performed using a PassThru J2534 compatible adapter.

A brief overview of the functionality of Toyota Techstream:
- diagnostics of all electronic systems having a digital interface (engine, automatic transmission, ABS, VSC, SRS, etc., etc.)
- change in the behavior of various systems (for example: turning off the beeper of the not fastened belts, time in milliseconds for switching to the reverse gear, etc.)
- carrying out various diagnostic procedures and settings procedures (ECB brake calibration, cylinder shut-off of injectors, etc., etc.)
- prescription of pressure sensors for both sets of tires
- adding smart keys (using additional software - Passcode generator)
- the ability to flash calibration for the engine and automatic transmission

System requirements: Windows XP-10 x32 & x64
Interface language: Multilingual (Russian is absent)
Description: Dealer diagnostic software for Toyota, Lexus, Scion
Activator is included! All regions are open!

regarding the price of software, please contact your personal message.

FIGURE 2

Good day, dear guests and participants of the Duplicates forum. Your attention is provoked with equipment for testing the security systems of car security from different manufacturers. We will select the right equipment for your budget. The theme will be gradually updated and equipment will be added. Ask all questions in private messages, we will be happy to answer them. Transactions are carried out through the guarantor of this forum. Delivery is almost any country

The cost of the device is 320 000.00 RUB (three hundred twenty thousand rubles)

PRICE: 5000 USD

Smart Key Emergency Start System Toyota / Lexus / Subaru 2020 + Multibrand

Keyless fishing rod repeater - a radio transmitting and receiving device located at intermediate points of radio communication lines, amplifying the received signals and transmitting them further. Thus increasing the range of the signal. Codegrabber - a repeater fishing rod has many names; universal "Fishing Rod", "Long Arm", "Wave", "Multi-brand" works with cars in which the standard Keyless G Keyless Entry comfort access system is installed, the system allows you to open doors and start the car engine.

This device allows you to open and start a car equipped with Keyless Go, Keyless Entry systems at a distance of 300 meters.
In its functional has 2 modes of operation:

1. **Operating mode with cars equipped with the Keyless Go Toyota system the entire lineup (2009-2020) Lexus the whole lineup (2006-2020) Subaru the whole lineup (2008-2020)**
2. **The operating mode with cars equipped with the Keyless Go or Keyless Entry system of other brands inclusive until 2017 - 2018.**
3. **This device makes it possible to open and start a car equipped with Keyless Go, Keyless Entry systems at a distance of up to 300 meters. In its functional has 2 modes of operatior**

The operating mode with cars equipped with the Keyless Go Toyota system the entire lineup (2009-2019) Lexus the whole lineup (2006-2019) Subaru the whole lineup (2008-2019) T

FIGURE 3

More alarmingly, Rapid7 researchers observed that, in October 2019, the "AgentGrabber" car theft tool appeared for sale in Russian-speaking criminal forums. The $5,000 USD tool enables the abuse of Keyless Entry and Keyless Go systems to gain unauthorized access to and control of vehicles from several manufacturers, including Honda, Toyota, Subaru, Mazda, and Nissan (Figure 3).

Compromised Customer Data

Customer data is one of several types of data sets that threat actors may seek to obtain in attacks on automotive companies for identity theft, fraud, and other malicious purposes. In March 2019, Toyota Japan announced a breach of Japanese dealerships and sales subsidiaries that may have exposed the PII of 3.1 million customers. Toyota Japan emphasized that the potentially exposed data did not include payment card information but may have included names, dates of birth, and employment details. Details such as dates of birth and employment history are useful to identity thieves seeking to establish fraudulent lines of credit. Toyota Vietnam and Toyota Thailand announced around the same time that they had experienced security incidents, but they did not provide any further details.

Customer service operations, including those that carmakers outsource to vendors, are another potential source of consumer data, beyond the manufacturers themselves. In July 2020, the South American criminal group KelvinSecTeam breached a call center providing customer service to 500,000 owners of vehicles from a variety of car manufacturers, including Honda. The group sold access to the data in underground criminal communities. The PII included names, email addresses, street addresses, and car registration details. In 2010, a breach at a third-party vendor that sent out welcome emails to newly registered Honda customers exposed the data of millions of Honda customers. The breach included names, email addresses, and VINs for 2.2 million Honda customers and just the email addresses of 2.7 million Honda Acura owners.

JULY 2020

500,000

owners of vehicles from a variety of car manufacturers data may have been exposed.

DECEMBER 2010

2.2 million

Honda customers' data breached including names, email addresses, and VINs.

MARCH 2019

3.1 million

Toyota customers' PII may have been exposed.

DECEMBER 2010

2.7 million

Honda Acura customers' email addresses were exposed.

Misconfigurations

Security misconfigurations can exacerbate an already challenging threat landscape for any organization, including automotive companies. For example, in November 2022, Toyota learned that a vulnerability in its Global Supplier Preparation Information Management System (GSPIMS) would have enabled an attacker to compromise accounts on that web portal simply by identifying the email addresses associated with them. An attacker could infer what those email addresses were simply by knowing Toyota's email naming convention and conducting open-source reconnaissance to learn the names of Toyota employees whose supply chain job functions likely required access to GSPIMS. The portal used JSON Web Tokens (JWTs) to authenticate users but only required their email addresses and not any passwords. This vulnerability affected all 14,000 users of the website, including a system administrator account.

Rapid7 research yielded more examples of misconfigurations affecting Japanese automotive brands. For example, in January 2021, a username/password combination of "admin/admin" on an Internet-exposed Bitbucket Git server exposed approximately 20 GB of source code from Nissan North America, which attackers released on Telegram. The source code included that of: Nissan North America's mobile app; its Dealer Business Systems/Dealer Portal; its vehicle diagnostics tool: sales and marketing and client acquisition and retention tools; and vehicle connected services (Figure 4).

JANUARY 2021

20 GB

of source code from Nissan North America, which attackers released on Telegram.

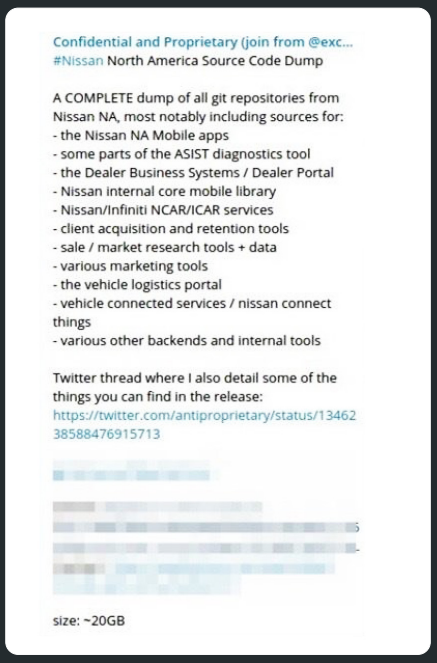


FIGURE 4

Similarly, it emerged in September 2022 that the inadvertent exposure of source code for Toyota's "T-Connect" vehicle management application had left more than 296,000 users exposed to potential attackers for almost five years. A vendor supporting the development of the T-Connect website had uploaded source code to GitHub and left it publicly available. The source code included a key granting access to a server that stored user information, including email addresses and vehicle management numbers.

Security misconfigurations in ElasticSearch databases occurred twice at Honda within one year. In December 2019, a security researcher discovered the inadvertent exposure of PII for 26,000 North American customers of Honda via an ElasticSearch database. The database was accessible via the open internet without authentication. The exposed PII included names, street addresses, phone numbers, email addresses, VINs, vehicle details, and vehicle service records. Another security researcher previously discovered another exposed ElasticSearch database at Honda in July 2019. This database exposed 40 GB of internal Honda network details for approximately 300,000 Honda employees worldwide, including the company's CEO, CFO, and CSO, with no authentication. These details, which could have facilitated network intrusions, included hostnames, MAC and internal IP addresses, OS versions, and the status of patching and endpoint security software. One pointedly named table, "uncontrolledmachine," listed those machines that had no endpoint security software.

The misconfiguration of third-party cloud services poses another risk, as another example of exposed Honda customer data demonstrates. In May 2018, Honda India exposed the data of 50,000 users of the company's Honda Connect mobile vehicle management and customer service app on two public AWS S3 buckets.

DECEMBER 2019

26,000

North American Honda customers inadvertent exposure of PII via an ElasticSearch database.

SEPTEMBER 2022

296,000

Toyota "T-Connect" customers exposed to potential attackers for 5 years.

JULY 2019

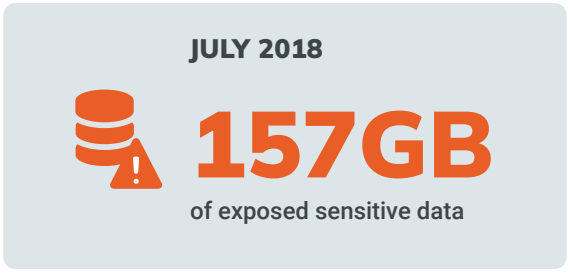
40GB

of internal Honda network details exposed for

300,000

Honda employees worldwide, including the company's CEO, CFO, and CSO, with no authentication.

Security misconfigurations at automotive companies' partners can accidentally expose trade secrets as well. Reliance on vendors can expose customers to third-party risks in connection with their vendors' security. For example, in 2018, it emerged that a server misconfiguration at Level One Robotics, a Canadian provider of industrial automation services, exposed sensitive documents from several automotive companies, including Toyota. The 157 GB of exposed data included: assembly line schematics; factory floor plans; robotic blueprints and configurations; request forms for VPN access and ID badges; employees' PII; and banking details for the company. The rsync file transfer protocol, which enables backups of large amounts of data, had no restrictions on that server, enabling any rsync client connecting to the rsync port to download data.



Third-Party Risks

Breaches can occur at vendors serving multiple automotive companies, such as the Canadian incident described above. For example, Rapid7 researchers observed that, in May 2021, criminal forum username "kurdishhacker" offered to sell web shell access to the server of an organization supporting multiple car manufacturers, including the Japanese brands Suzuki and Toyota. The compromised server supported more than 20 websites. The actor claimed that he could reinstall the web shell if the server's administrator deleted it because he had an unspecified exploit for the server (Figure 5).

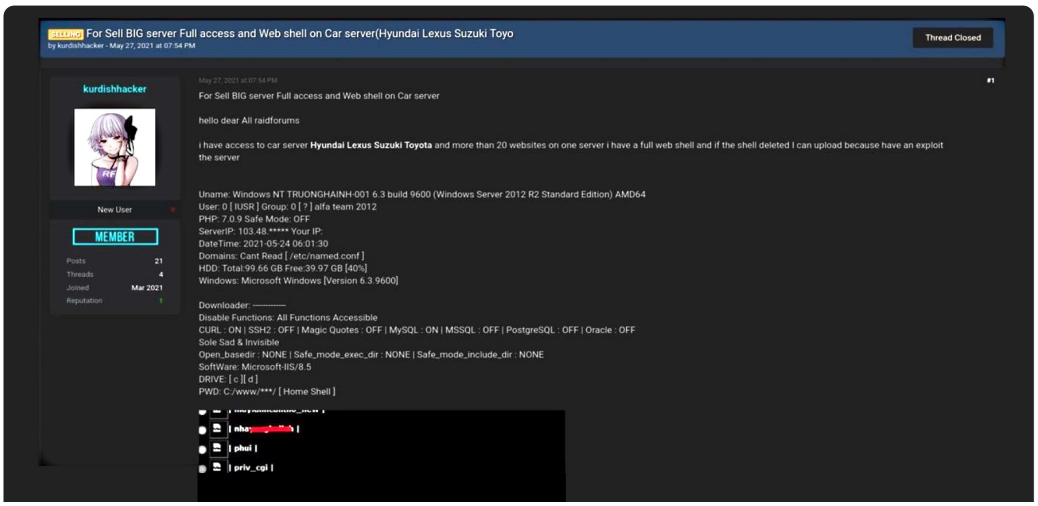
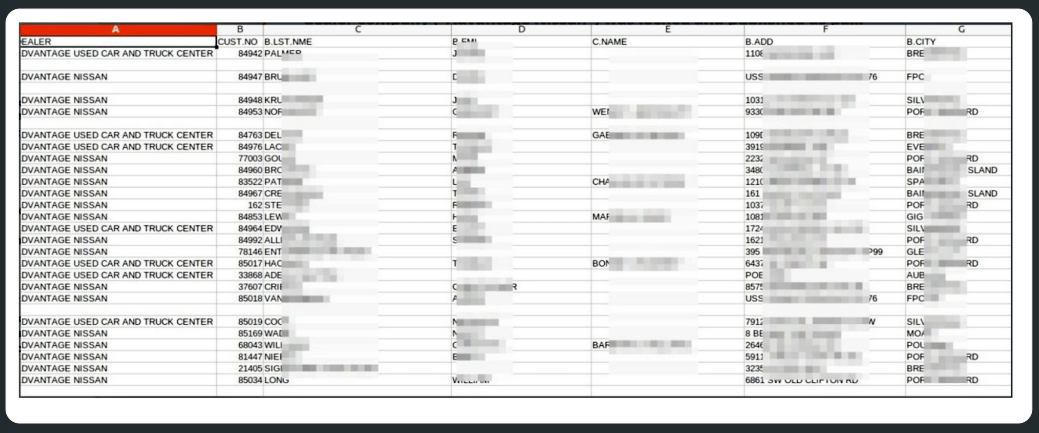


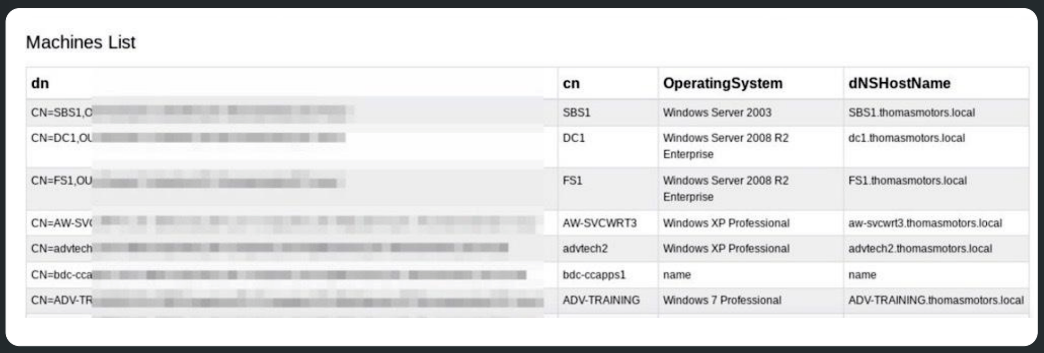
FIGURE 5

Third-party breaches at branded automotive dealerships can have implications for manufacturers, even if dealerships are separate businesses. The exposure of dealership data in ransomware data disclosures could have implications for associated manufacturers if it reveals sales and marketing or other business details that undermine their competitive position, or if it provides competitive intelligence to manufacturers or dealers of competing brands. Consumers may also lose confidence in the brand associated with a compromised dealership, even if it is a separate business and the manufacturer whose brand name it bears had no control over the dealership's security. Breaches at dealerships could also facilitate attacks on manufacturers if the dealers share access to any infrastructure, such as manufacturers' portals for dealerships. For example, in October 2020, Rapid7 researchers observed that ransomware operators disclosed customer data, a list of machines, and other sensitive data that they reportedly obtained from a breach of a U.S. Nissan dealership (Figures 6 and 7).



A	B	C	D	E	F	G
EALER	CUST.NO	B.LST.NME	B.EMI	C.NAME	B.ADD	B.CITY
DVANTAGE USED CAR AND TRUCK CENTER	84942	PAL	J		110	BRE
DVANTAGE NISSAN	84947	BRU	D		USS 76	FPC
DVANTAGE NISSAN	84948	KRU	J		103	SILV
DVANTAGE NISSAN	84953	NOF	C	WEI	933	POF RD
DVANTAGE USED CAR AND TRUCK CENTER	84763	DEL	F	GAE	109	BRE
DVANTAGE USED CAR AND TRUCK CENTER	84976	LAC	T		391	EVE
DVANTAGE NISSAN	77003	GOL	M		223	POF RD
DVANTAGE NISSAN	84960	BRC	A		348	BAI SLAND
DVANTAGE NISSAN	83522	PAT	L	CHA	121	SPA
DVANTAGE NISSAN	84967	CRE	T		161	BAI SLAND
DVANTAGE NISSAN	162	STE	F		103	POF RD
DVANTAGE NISSAN	84853	LEV	H	MAI	108	GIG
DVANTAGE USED CAR AND TRUCK CENTER	84964	EDV	E		172	SILV
DVANTAGE NISSAN	84992	ALL	S		162	POF RD
DVANTAGE NISSAN	78146	ENT			395 99	GLE
DVANTAGE USED CAR AND TRUCK CENTER	85017	HAC	T	BON	643	POF RD
DVANTAGE USED CAR AND TRUCK CENTER	33868	ADE			POE	AUB
DVANTAGE NISSAN	37607	CRI	C R		857	BRE
DVANTAGE NISSAN	85018	VAN	A		USS 76	FPC
DVANTAGE USED CAR AND TRUCK CENTER	85019	COC	N		791 W	SILV
DVANTAGE NISSAN	85169	WAL	N		8 BE	MOU
DVANTAGE NISSAN	68043	WIL	C	BAF	264	POL
DVANTAGE NISSAN	81447	NEI	E		591	POF RD
DVANTAGE NISSAN	21405	SIG			323	BRE
DVANTAGE NISSAN	85034	LONG	WILL		6861 SW OLD CLIFTON RD	POF RD

FIGURE 6



Machines List

dn	cn	OperatingSystem	dNSHostName
CN=SBS1,O	SBS1	Windows Server 2003	SBS1.thomasmotors.local
CN=DC1,OU	DC1	Windows Server 2008 R2 Enterprise	dc1.thomasmotors.local
CN=FS1,OU	FS1	Windows Server 2008 R2 Enterprise	FS1.thomasmotors.local
CN=AW-SV	AW-SVCWRT3	Windows XP Professional	aw-svcwrt3.thomasmotors.local
CN=advtech	advtech2	Windows XP Professional	advtech2.thomasmotors.local
CN=bdc-cca	bdc-ccapps1	name	name
CN=ADV-TR	ADV-TRAINING	Windows 7 Professional	ADV-TRAINING.thomasmotors.local

FIGURE 7

Business Email Compromise

Automotive businesses can also become targets for business email compromise (BEC) attacks, which affect organizations in all industries. BEC attacks trick businesses into sending large sums of money to attackers by posing as senior executives or external partners via compromised email accounts or by impersonating genuine people. BEC attackers typically compromise enterprise email accounts in spear-phishing attacks or with keystroke loggers. They typically use this access to lure employees into sending money to them, or as a source of information on business processes with which to manipulate targets by other means. A European subsidiary supplier of seats and interiors for Toyota vehicles became the victim of an unusually large $37 million BEC attack in August 2019. The attacker socially engineered a company employee into paying a fraudulently altered vendor invoice.

AUGUST 2019

$37 million

losses in business email compromise (BEC) attack

Automotive manufacturing brands may be the most salient targets in the Japanese automotive industry, but they are not the only ones. For example, in November 2020, criminal forum username "pizza50" offered to sell the reportedly compromised user database of a Japanese exporter of previously owned vehicles for $250 USD. The database of 27,547 users included usernames, cleartext passwords, email addresses, phone numbers, dates of birth and other details. The actor claimed to have compromised this database in a SQL injection (SQLi) attack (Figure 8).

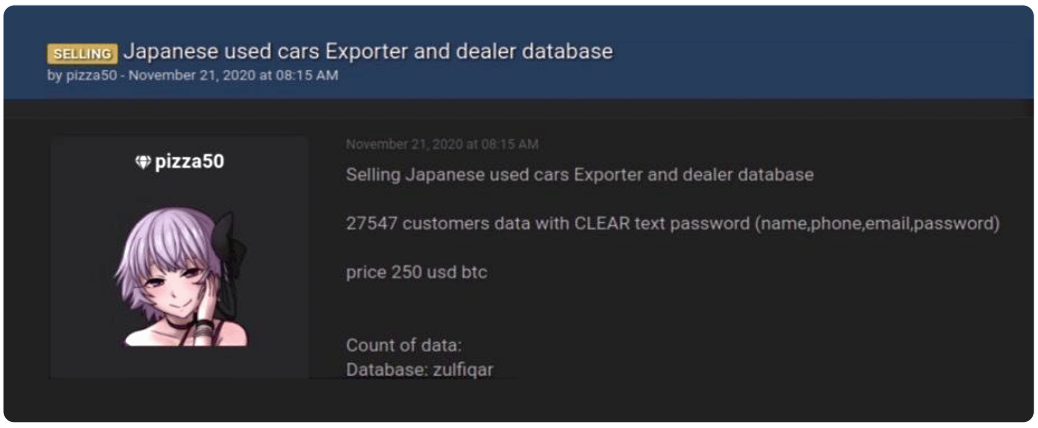


FIGURE 8

Financial Services

Financial institutions are significant targets around the world, particularly for criminals, and Japan is not an exception. Japan's significant wealth makes its financial sector a desirable and potentially lucrative target for criminals worldwide.

Cryptocurrency Exchanges

Beyond the traditional financial sector, Japanese cryptocurrency exchanges have become targets of cyber attacks. The theft of approximately $460 million USD worth of cryptocurrency from the Tokyo-based exchange Mt. Gox was a seminal incident in this field, coming to light in 2014 and paving the way for more large-scale theft from cryptocurrency exchanges.

More recently, the Japanese cryptocurrency exchange Liquid suffered a theft of the equivalent of approximately $97 million USD in cryptocurrency in August 2021. As in the case of the Coincheck incident, Liquid had been storing the stolen cryptocurrency in less secure "hot wallets" and moved funds into more secure "cold wallets" after the incident. As in the case of so many other compromises of Japanese companies, Liquid determined that these thefts had begun with the compromise of the multiparty computation (MPC) wallet of Quoine, its Singapore subsidiary. In a (presumably) separate November 2020 incident, Liquid suffered a DNS hijacking attack via its hosting provider that enabled the attacker(s) to compromise customers' names, street addresses, email addresses, hashed passwords, and possibly more PII data points.

Compromised Customer Data

Phishing is a common tactic for criminals seeking to compromise the credentials of financial institutions' customers around the world, including Japan. A sample of 2021 phishing attacks in Japan indicated that the financial sector was the most common spoofing target of phishing pages, representing 31% of all attacks. Many of these phishing domains used the brand name of a financial target in the sub-domain of a domain with an English-language character string referring to financial services, such as "card." Others, however, used Japanese-language Internationalized Domain Names (IDNs), presumably for users unfamiliar with English.

Much threat intelligence coverage of criminal operations against the global financial sector comes from either Russian-speaking or English-speaking underground criminal communities, but Japan's financial sector is a target for Chinese-speaking criminals as well. For example, Rapid7 researchers observed that Chinese-speaking criminal forum username "sherrybaby889" offered to sell an October 2020 database of 48,201 Japanese bank customers. The database included data points such as name, phone numbers, email addresses, street addresses, dates of birth, and credentials (Figure 9).

Criminals typically target the customers of financial institutions via their online banking credentials or payment card information obtained via compromises of retail and hospitality businesses or other merchants. Third-party payment processors are another potential source of bulk payment card data, as indicated by the payment card breach affecting more than 100,000 customers of Japanese cosmetics e-commerce retailer Acro. The attackers exploited a vulnerability in the third-party payment processor's software and collected customer payment card details from two of Acro's retail cosmetics e-commerce websites between May 2020 and August 2021.

FIGURE 9

The Japanese customer credentials of online payment services other than cards can also become targets for criminals. For example, it emerged in November 2022 that an Android malware family was targeting the devices of Japanese-speaking users in order to compromise their online payment platform credentials. The Japanese-language social engineering attacks via SMS aimed to lure victims into installing the malware for false security reasons. The malware prompted users to enter their payment service credentials into fake Japanese-language prompts emulating the targeted services. The malware also initiated reverse proxy connections from compromised devices, enabling attackers to initiate fraudulent transactions from victims' own IP address, so as to appear more legitimate and reduce the risk of triggering fraud detection systems.

Criminals can also directly target banks themselves in order to obtain information on their customers. In this case, Rapid7 researchers discovered that criminal forum username "WICK1" offered to sell customer data purportedly obtained from the compromise of a Japanese bank.

Compromised Employee Data

Criminal attacks on financial institutions typically aim to enable fraud against customer accounts but can also affect employees as well. In this case, Rapid7 researchers observed that criminal forum username "B14CK-J0K3R" offered to sell the PII of 684,200 Japanese and Australian bank employees in November 2020. The PII database included data points such as credential pairs, street addresses, phone numbers, email addresses, dates of birth, mothers' maiden names, national ID numbers, and credit card details (Figure 10).

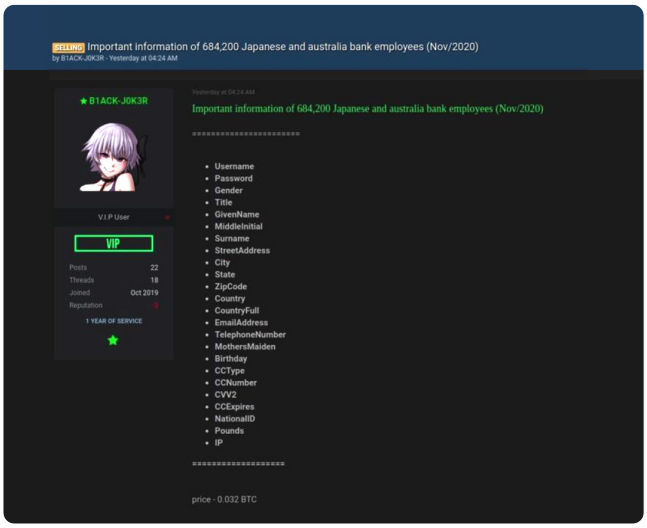


FIGURE 10

Technology, Media and Telecommunications

Technology companies may become valuable targets for threat actors seeking information on or access to their customers, rather than the companies themselves. Information technology (IT) vendors are a preferred target for ransomware operators in particular, who can use compromises of managed service providers (MSPs) and other IT vendors to maximize their ability to infect large numbers of companies with little effort.

An IT vendor breach that came to light in December 2022 created just such an opportunity for a large-scale supply chain attack with ransomware. The breach has affected at least 10 Japanese companies as of early 2023, including a cyber insurance provider. This insurance provider is a high-value target for ransomware operators in particular because it possesses data points that could facilitate ransomware attacks on its customers.

The May 2020 breach of a Tokyo-headquartered Fortune 500 company is both an example of technology/telecommunications company breaches exposing information on government customers and yet another example of the role of the overseas operations of Japanese companies as points of entry into Japanese networks. The compromise of the hosting and cloud services infrastructure of a subsidiary, which exposed information on 62 customers, reportedly began with the compromise of machines supporting the company's operations in Singapore. Japanese media reports indicated that the compromise may have exposed sensitive information on, or communications infrastructure for, Japanese military customers.

The Japanese government is not the only stakeholder that suffers in attacks on Japanese technology, media, and telecommunications companies. In May 2022, a ransomware attack affected the Singapore-based Asian operations of a Japanese media company with a significant footprint in global markets. This incident was not the first time that this media giant's foreign operations were the focus of an attack on the company. In September 2019, a New York-based employee unwittingly enabled a BEC theft by sending approximately $29 million USD to a fraudster posing as a company executive.

Gaming is another field in which Japanese companies are market leaders. Threat actors have thus targeted them as well, in types of incidents more likely to affect individual consumers. For example, in July 2022, it emerged that the BlackCat/AlphV ransomware group had compromised a Japanese video game company that has published famous titles such as Pac-Man and Elden Ring. BlackCat is believed to be a rebranding of the DarkSide ransomware group that attacked the U.S. Colonial Pipeline in May 2021. In this instance, the attackers gained unauthorized access to systems at the company's Asian operations outside Japan. The video game company claimed that the incident may have compromised data on the company's Asian customers outside Japan.

Conclusion and Recommendations

Japan has a huge attack surface as the world's third-largest economy and the home of many global businesses and brands. Manufacturing organizations, automotive or otherwise, are significant targets within the Japanese threat landscape, given their importance to the Japanese economy and Japan's key role as a global market leader in such industries. Financial institutions are usually top targets for criminals in any country, and Japan's extensive wealth makes them an even more desirable target in that regard. Japanese technology, media and telecommunications companies are significant targets insofar as their compromise can have damaging effects on public and private sector customers and consumers. The governments of neighboring countries also target Japan's public and private sectors for various economic, financial, and political reasons.

The following recommendations can help Japanese companies and their subsidiaries defend against attacks:

- Educate employees to be wary of emails or instant messages with spelling, grammatical, social, or other errors that could indicate that the true author was not actually a native Japanese speaker. Foreign attackers using social engineering techniques against Japanese-speaking targets may inadvertently reveal themselves with such errors in their Japanese writing.
- Japanese businesses with extensive foreign operations, subsidiaries, or other holdings should take steps to reduce the risk that any compromises in their overseas infrastructure could enable lateral movement into the networks of the parent companies. Possible means of accomplishing this goal may include:
  - Integrating security assessments of foreign companies into the mergers and acquisitions (M&A) process, in order to identify and remedy any risks or existing breaches that the acquiring company may inherit.
  - Closer oversight and coordination of the security practices of overseas subsidiaries, to ensure the implementation of best security practices.
  - Creating network segmentation to prevent attackers from using unauthorized access to a compromised overseas subsidiary to move laterally into the networks of the parent Japanese company.

- Establish a third-party risk program to vet vendors and other partners for risks that could affect your own organization by exposing its data or infrastructure.
  - Integrate security considerations into the vendor selection process.
  - Establish requirements for the reporting of security incidents at vendors and other partners. Write them into contracts, if possible.
- Identify those data assets that are most valuable to attackers and provide them with additional layers of protection, such as network segmentation and file encryption. When determining which assets are more valuable, consider the following possible use cases for compromised data:
  - Fraud, identity theft, and other financially motivated misuse of customers' or employees' compromised PII;
  - Data disclosure extortion, typically in conjunction with a file-encrypting ransomware attack, but potentially on its own as well;
  - Theft of IP that could give competing businesses or countries economic, political, or military advantages against the targeted business.
- Do not pay ransoms to ransomware operators. Ransom payments encourage more attacks, both in general and specifically against organizations that pay them. Ransoms give ransomware operators more funds with which to finance their operations. Ransom payments mark the organizations that pay them as vulnerable to extortion and thus more desirable targets for future attacks. If you nonetheless decide to pay ransom anyway, it should be only as a last resort, after exhausting all other options.
  - The best defense against the file-encryption layer of a ransomware attack is a system of frequent, segmented, and redundant backups, enabling victims to restore their files without paying ransoms.
  - Network segmentation and your own file encryption can also reduce the impact of the data disclosure extortion layer of many contemporary ransomware attacks.
- Manufacturing organizations should prepare for the risk of ransomware or ICS malware attacks at vendors or suppliers of components or raw materials disrupting their own manufacturing operations by cutting off supply chains. If your organization practices "just-in-time" manufacturing, ensure that it can immediately access a backup supply chain so that manufacturing operations can continue with minimal disruption.

PRACTITIONER-FIRST SECURITY SOLUTIONS ARE HERE

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/