Zooming into Darknet Threats Targeting Japanese Organizations

ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela

November 18, 2020

In light of rising cyberattacks and ahead of the 2021 Tokyo Games, Japan is investing in cybersecurity efforts, with one of them being the establishment of a government entity dubbed the Digital Agency. The decision follows recent fraud involving Japanese bank accounts linked to cashless payments services, which could be achieved by brute-forcing, using compromised credentials to banking accounts or via other attack vectors. Attacks on the banking infrastructure is just a part of threats targeting Japanese organizations, recently explored by KELA. They include:

- **Leaked data and compromised accounts**. KELA detected that data belonging to Japanese corporations, as well as government and educational entities, is actively circulating in the darknet and being demanded by threat actors. This data can be used to gain initial network accesses, i.e. entry points to targeted networks.
- **Initial network accesses.** KELA observed several Japanese compromised companies, ranging from corporations to universities, including one Japan ministry target during June-October 2020. These accesses can be leveraged to eventually deploy ransomware.
- **Ransomware incidents.** KELA detected at least 11 Japanese victims of ransomware attacks in June-October 2020. The affected companies are from manufacturing, construction and government-related industries, with top victims having around $143 billion, $33 billion and $2 billion yearly revenue.
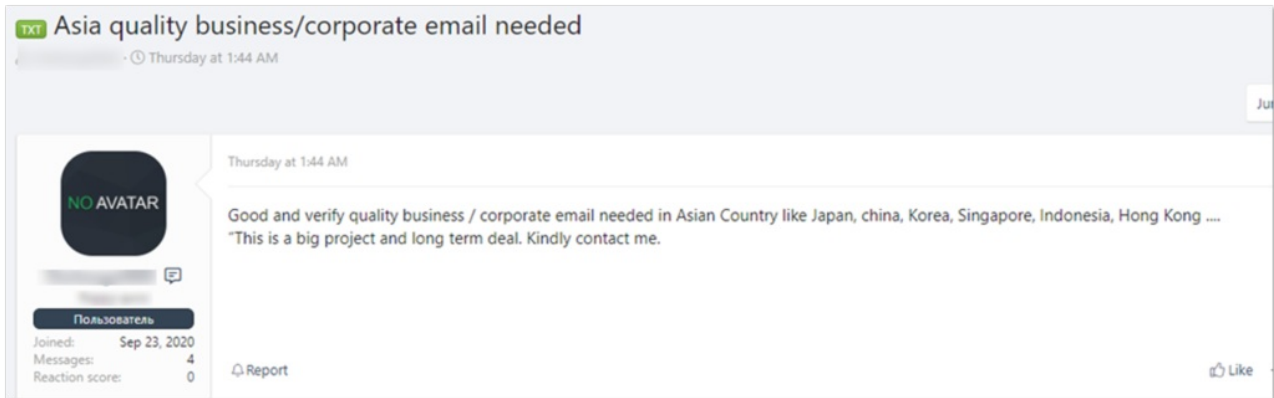
Leaked Data and Compromised Accounts: Demand for Japanese Companies

Among the most prominent threats on the darknet, KELA observed leaks and sales of Japanese entities' data. **While many offers are related to regular users, some actors are specifically looking for corporate data of Japanese organizations.**


A threat actor requesting for corporate emails in Asian countries, including Japan
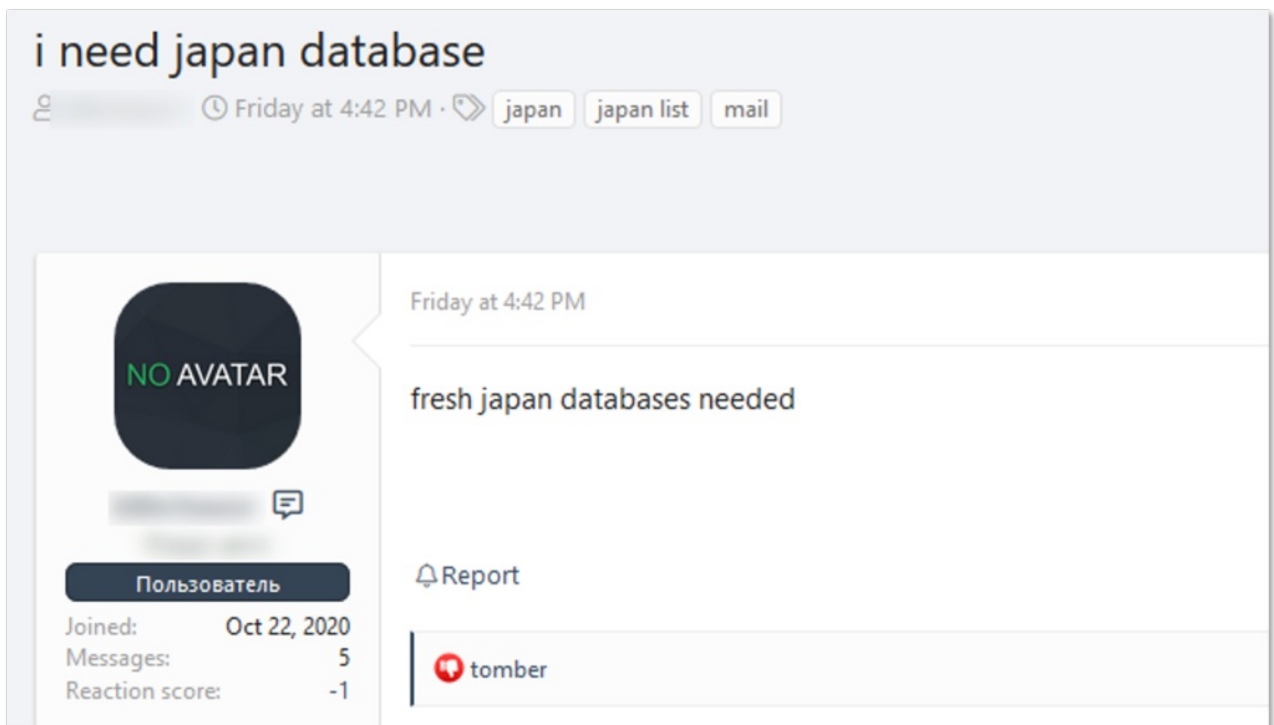
A threat actor requesting for fresh Japan databases. During several days, he received three answers from potential sellers asking for contacts to probably make a deal

Exposed data may include personal information of companies' customers and employees, sensitive internal documents, and credentials to the company's resources. For example, the KelvinSecurityTeam hacking group has been trading a database of a major Japan corporation since July 2020. It has been recently promoted again as a part of their offers.

The threat actor claimed that the database contains records of 150,000 customers, possibly Japanese ones. As KELA observed from samples of the database, the records include names, addresses, birth dates, emails, and phone numbers, as well as some data related to their work history. KelvinSecurityTeam is a hacking collective with some members from Venezuela, Peru, and Colombia, which is known for selling hacking tools, carding services, and private data dumps on forums.
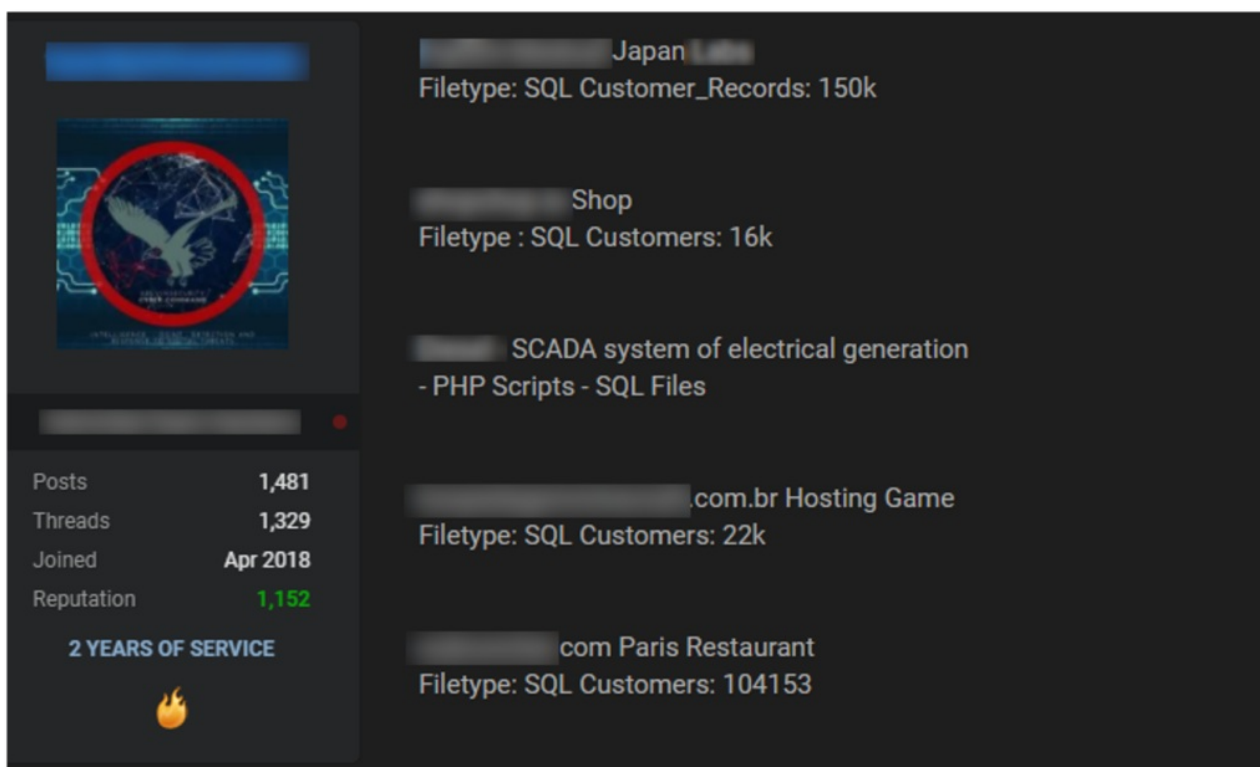

While personal information and internal documents require malicious actors to perform multiple steps to attack the company further (for example, via specially-crafted phishing campaigns), exposed credentials provide an easier way to compromise the company via accessing its internal systems and software in use.

Exposed credentials can be divided into two types:

- **Leaked credentials.** Corporate email logins, with or without passwords, which are usually being leaked or sold by threat actors on underground forums. **Overall, KELA discovered more than 100 million exposed Japanese emails in our sources.**

- **Compromised accounts.** Logins and passwords to accounts that grant access to tools and software used in a compromised environment, such as RDP, VPN solutions, and more, which are usually being sold through underground autoshops.
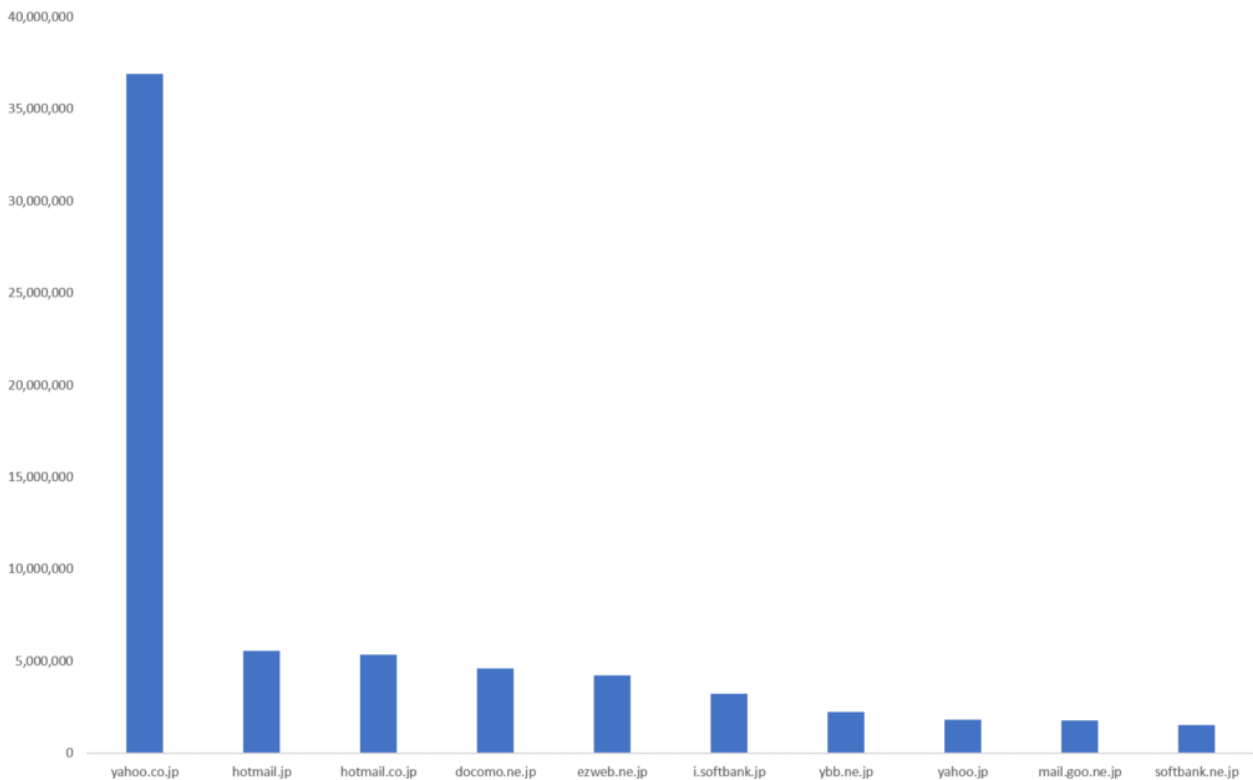
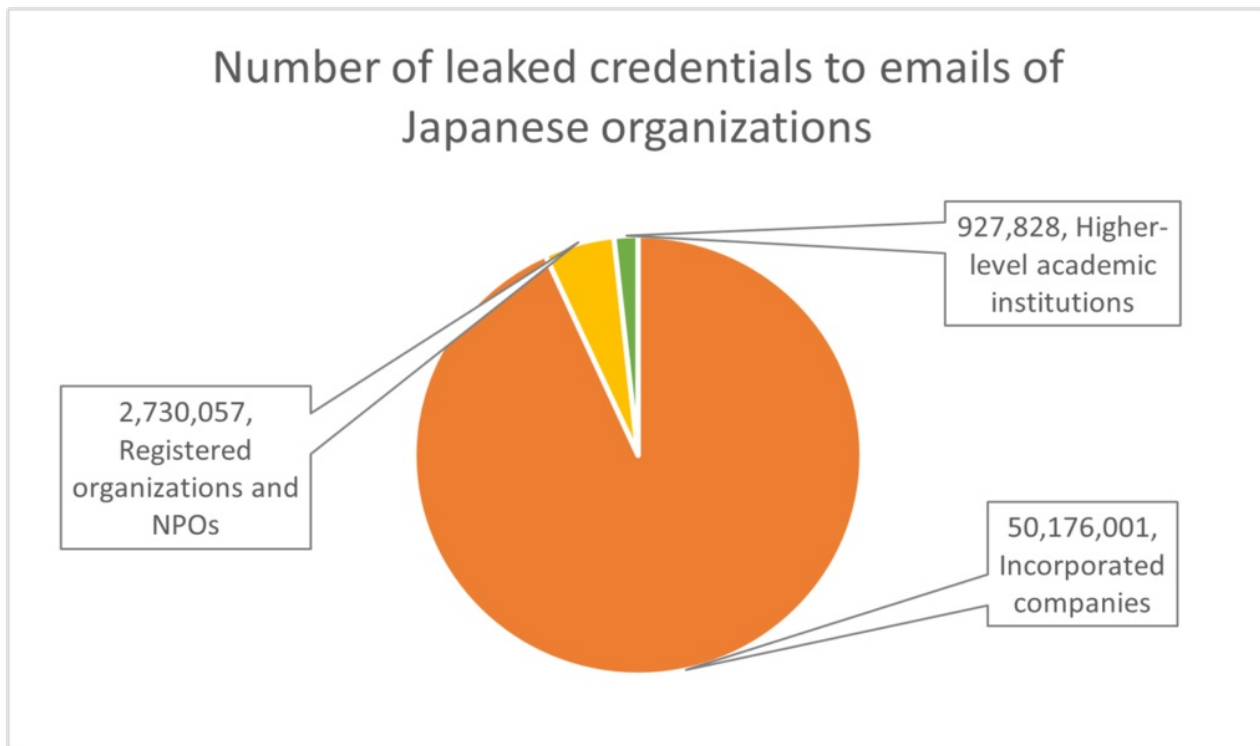*Top 10 email domains featured in leaked credentials gathered by KELA's tools from cybercrime communities*

Part of compromised accounts offered in autoshops (shown within KELA's DARKBEAST)

This data can enable attackers to access the company's resources and provide further malicious activity, ranging from social engineering to malware attacks. **Ultimately, every leaked data can theoretically become an entry point for large-scale attacks.**

Based on information gathered from multiple darknet sources that KELA tracks, we defined that many Japanese corporations, as well as government and educational entities, are suffering significantly from these types of threats:

Number of compromised accounts related to Japanese organizations

- 1955, Registered organizations and NPOs
- 2756, Higher-level academic institutions
- 78,962, Incorporated companies
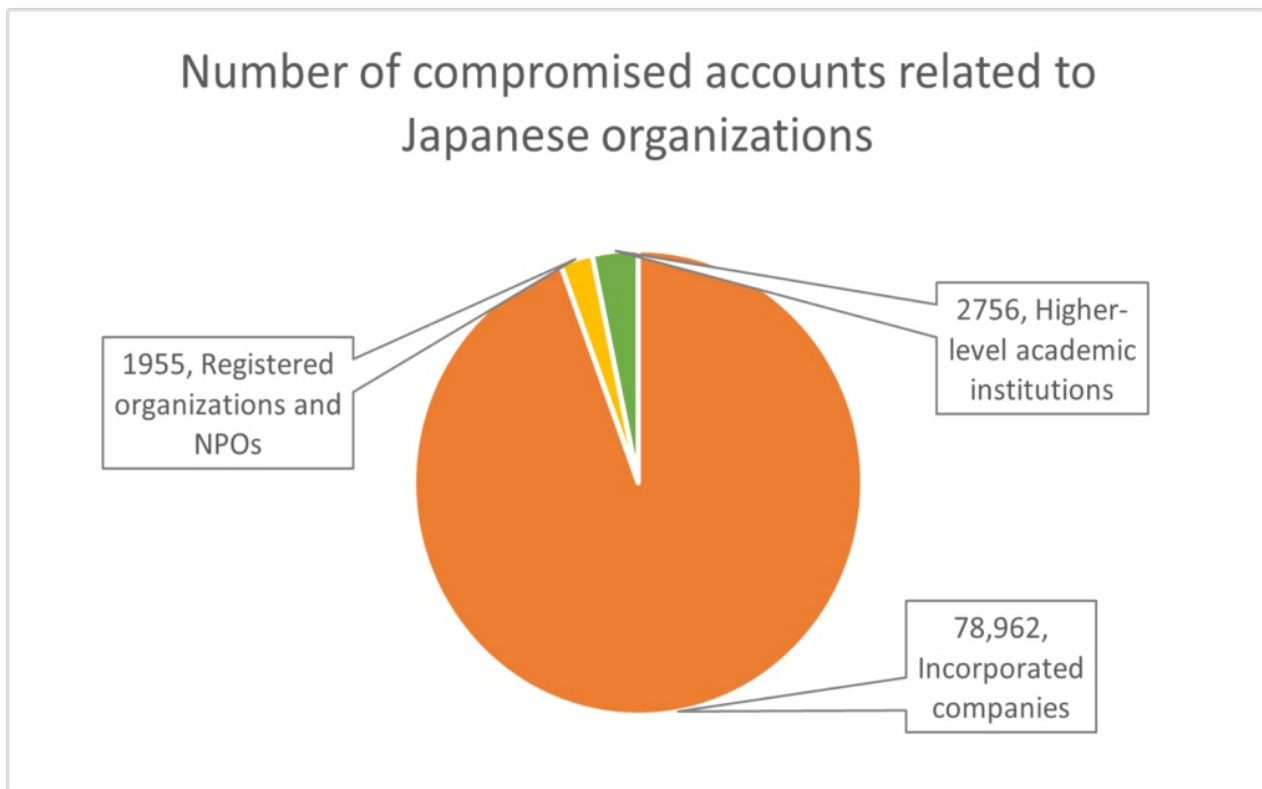
Network Accesses: Entry Points to Japanese Networks for Ransomware Attackers

Initial network accesses, offered on underground forums, can serve as entry points for ransomware operators and other malicious actors looking for a foothold from where they can move laterally and deploy ransomware or steal intellectual property. Over the last three months, KELA observed several accesses to Japanese organizations being sold in the darknet. While overall numbers are lower than other countries like the US, considering the scale of initial network accesses' sales, **each of these accesses can be turned into millions of ransom demanded by buyers who would manage to leverage them to infect the victims with ransomware.**

The most dangerous offer appears to be related to a remote code execution vulnerability in the Japanese Ministry of Justice network. According to a threat actor who posted the offer for 210,000 JPY, exploiting this vulnerability could grant NT Authority/System privileges, meaning a high level of permissions.

Another access on sale during the last months allegedly belonged to a "Japan ship inspection network" and had domain admin level privileges, which enables attackers to perform malicious actions on behalf of the targeted network's administrator. It was offered for 157,000 JPY. Interestingly, one week later, the Sodinokibi (REvil) ransomware gang attacked a victim which appears to be the same company based on the description on the victim's website — "certification body of ship equipment." However, it's not known if the two incidents were related. **Ransomware operators usually wait for negotiations deadlines to expire before exposing a victim on their blogs, so it's hardly possible they would manage both to attack the victim and lose patience for one week.**

London executing broker (brokerage services, foreign currency exchange) - **domain admin** - 5000$

Switzerland real estate network (publicly traded on Swiss exchange) - **domain admin** - 3000$

Japan ship inspection network (sponsor by government) - **domain admin** - 1500$

Mexico credit union network - **domain user** - 500$

Israel supply chain network - **domain user** - 500$

＋ Цитата

I do not need help selling access. I do not teach hacking. I do not work for free. I do not work with new users. Do not waste my time.

Access to the Japanese "ship inspection network" offered for sale

Sodinokibi's victim

Among other offers, KELA observed access to a Japanese medical university being offered for 105,000 JPY. **The example highlights that despite the pandemic and the disapproval of some members of the underground community, many actors continue to target the healthcare industry, as well as the education sector.**

Продам доступ к мед университету в Японии. 2к+ хостов

Автор: ____ 27 июня в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

Опубликовано: 27 июня (изменено)

Продам доступ к медицинскому универу в Японии, в ядре более 1000 машин, хостов в АД более 2к+. ОС на японском языке (!)

Локальный админ, цена 999$

PM или Jabber (обязательно делайте верификацию джаббера через ПМ) !!!

Изменено 27 июня пользователем TrueFighter

Платная регистрация
❶ 17
121 публикация
Регистрация
03.11.2019 (ID: 96 836)
Деятельность
другое / other

✚ Цитата

Ransomware Incidents: (At Least) Seven Gangs Targeting Japanese Organizations

During June-October 2020, at least 11 Japanese victims suffered ransomware attacks (based on the media reports and data on ransomware gangs' "naming-and-shaming" portals used to threaten victims, monitored by KELA technology), with the most well-known victims being <u>Honda</u> and <u>Canon</u>.

Ransomware Gangs Targeting Japanese Entities
June-October 2020

7 ransomware gangs

- DopplePaymer
- Maze
- Ekans (Snake)
- Egregor
- Lockbit
- Sodinokibi (Revil)
- Conti

11 ransomware victims from:

- Manufacturing
- Construction
- Government-related

With yearly revenue ranging from
10.6 billion JPY to **15.1** trillion JPY

The most active ransomware gang targeting Japanese entities appears to be the DoppelPaymer gang. The DoppelPaymer ransomware emerged in 2019 and <u>is believed to have links</u> with former members of the TA505 hacking group. This group has recently attacked four large Japanese companies from the construction, automotive and manufacturing industries, including a corporation with $1 Billion in revenue, as well as a German subsidiary of a leading manufacturer of specialty paper in Japan.

Interestingly, one of the victims of DoppelPaymer was later claimed to be attacked by Conti, a new ransomware operation that started in August 2020 and believed to be associated with the Ryuk ransomware.

DoppelPaymer's leak blog featuring a Japanese manufacturing company with $153 million revenue

Other ransomware gangs spotted attacking Japanese entities are well-known Maze, Sodinokibi and Ekans (Snake), and two ransomware operations that have recently adopted a tactic of public shaming – Egregor and LockBit.
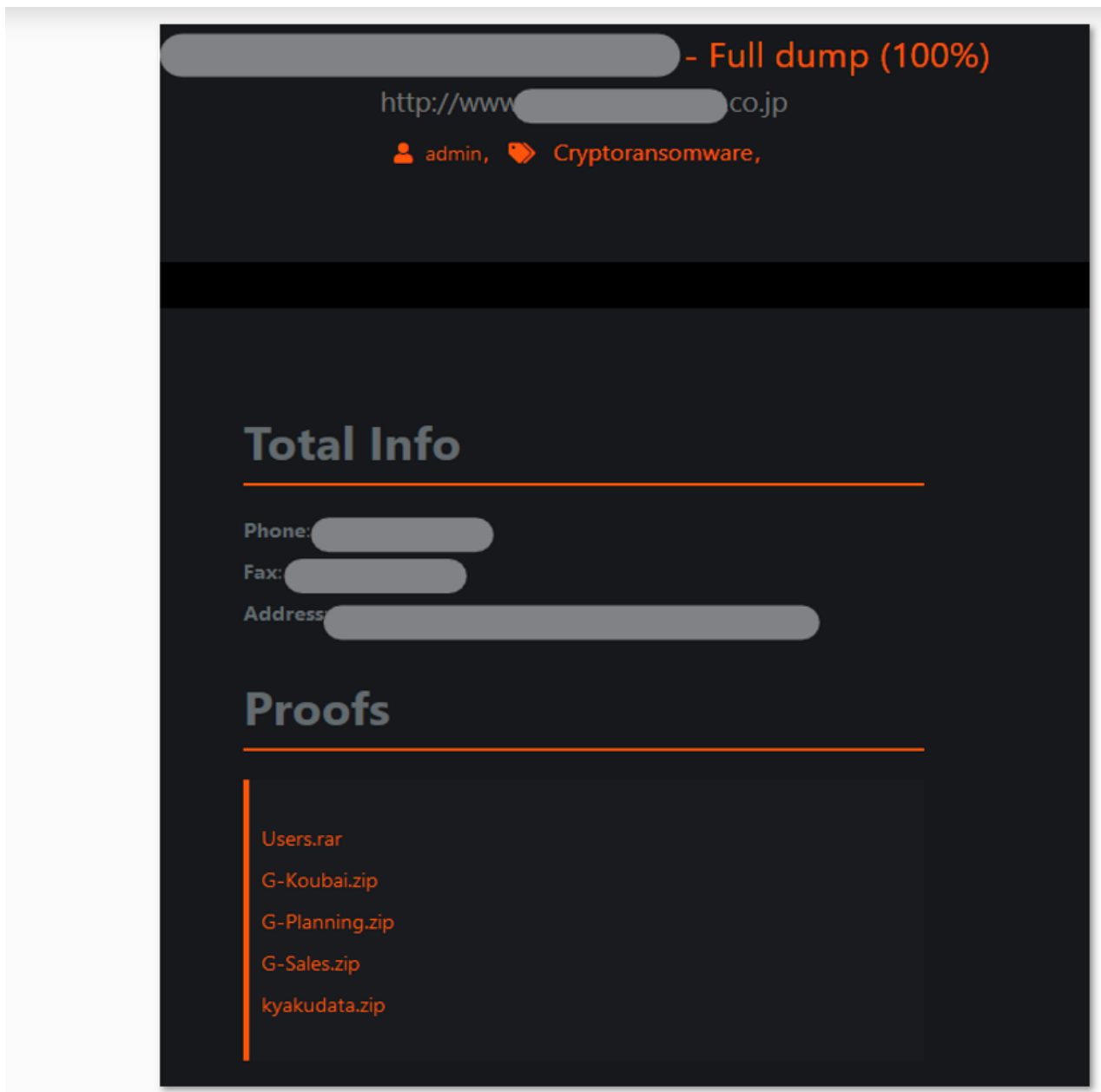
Maze's leak site featuring a full dump of stolen documents belonging to a Japanese manufacturing company

---

Not much is known about initial infection vectors used to compromise networks of Japanese victims. However, it's clear that the attack surface is expanding due to COVID-19-related issues and increasing trend for remote working, meaning that more and more employees are using vulnerable software and exposed credentials to access corporate networks remotely.
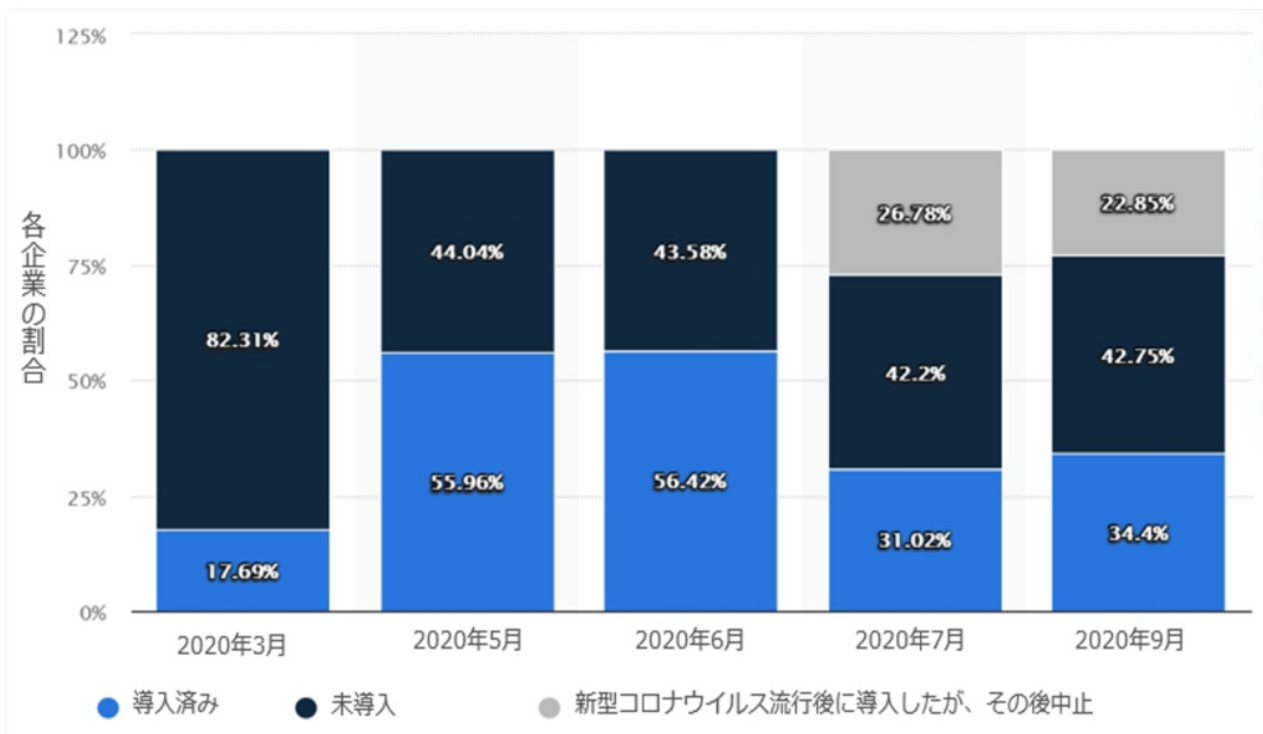
Business enterprises in Japan that implemented home office for employees after the outbreak of COVID-19 (source: Statista)

For example, **one Japanese victim, a manufacturing company, was probably attacked by LockBit using exploit code for a Pulse Secure vulnerability (CVE-2019-11510).** The clue stems from the fact that the company's IP address was included in a leak posted on a cybercrime community containing details and credentials of over 900 enterprise Pulse Secure servers exploited by threat actors.
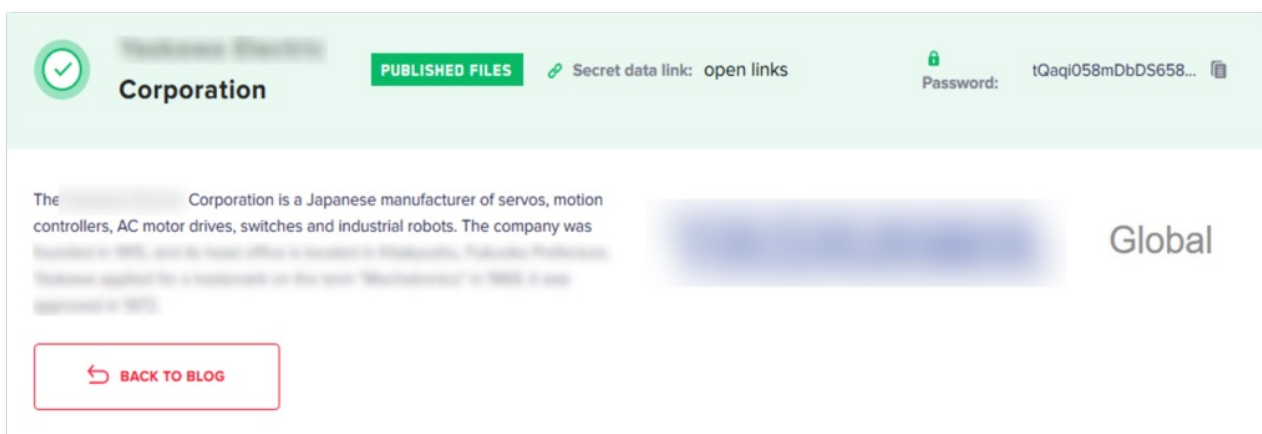
The victim was first shared by LockBit in their thread on a Russian-speaking underground forum with a domain that had a Chinese TLD, which could indicate it is a Chinese branch that was attacked. When LockBit started their blog a few days later, the victim appeared there without domains mentioned.

Aug 22, 2020

https://www._____:om.cn/
_____Corporation - японский производитель сервоприводов, контроллеров движения, приводов переменного тока, переключателей и промышленных роботов
Даю 7 дней на то чтоб отписать и оплатить!
Либо данные будут опубликованы!

Attachments

Screenshot_1.png
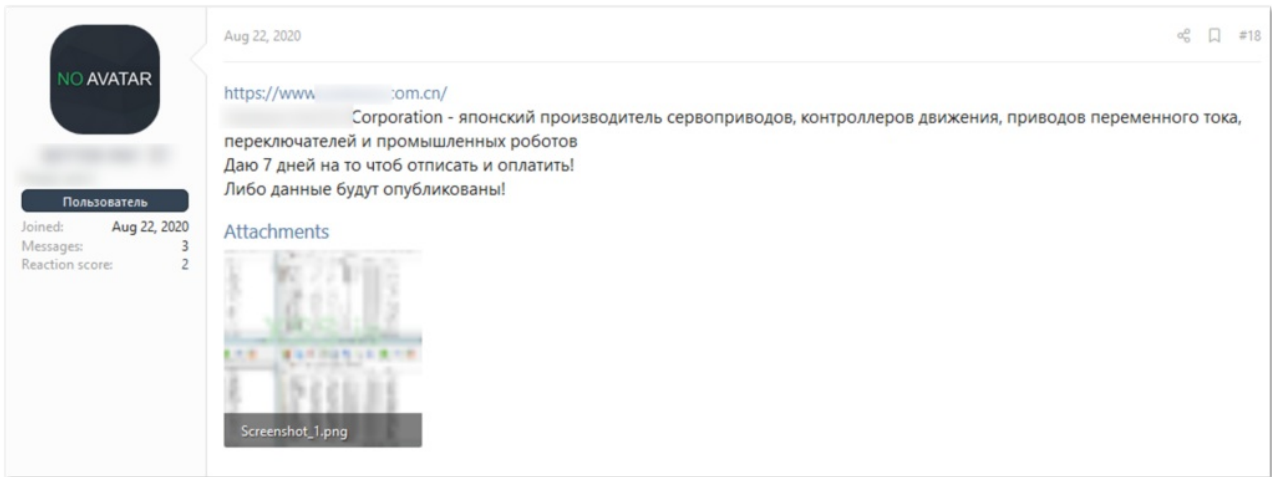
A post in LockBit's thread, where the ransomware gang is recruiting affiliates, on a Russian-speaking underground forum


The Pulse Secure leak, for which additional directories were shared several days later, possibly affects about 117 Japanese entities, based on KELA's analysis of the IP addresses. Darknet chatter on the matter shows that this information has been circulated between malicious actors before the leak that happened in August 2020. Therefore, credentials to affected Japanese organizations' Pulse Secure servers could be used by different actors in their malicious campaigns, including ransomware attacks.

Japan entities in the Pulse Secure leak

10%

90%

■ Japan entities ■ Entities from the rest of the world
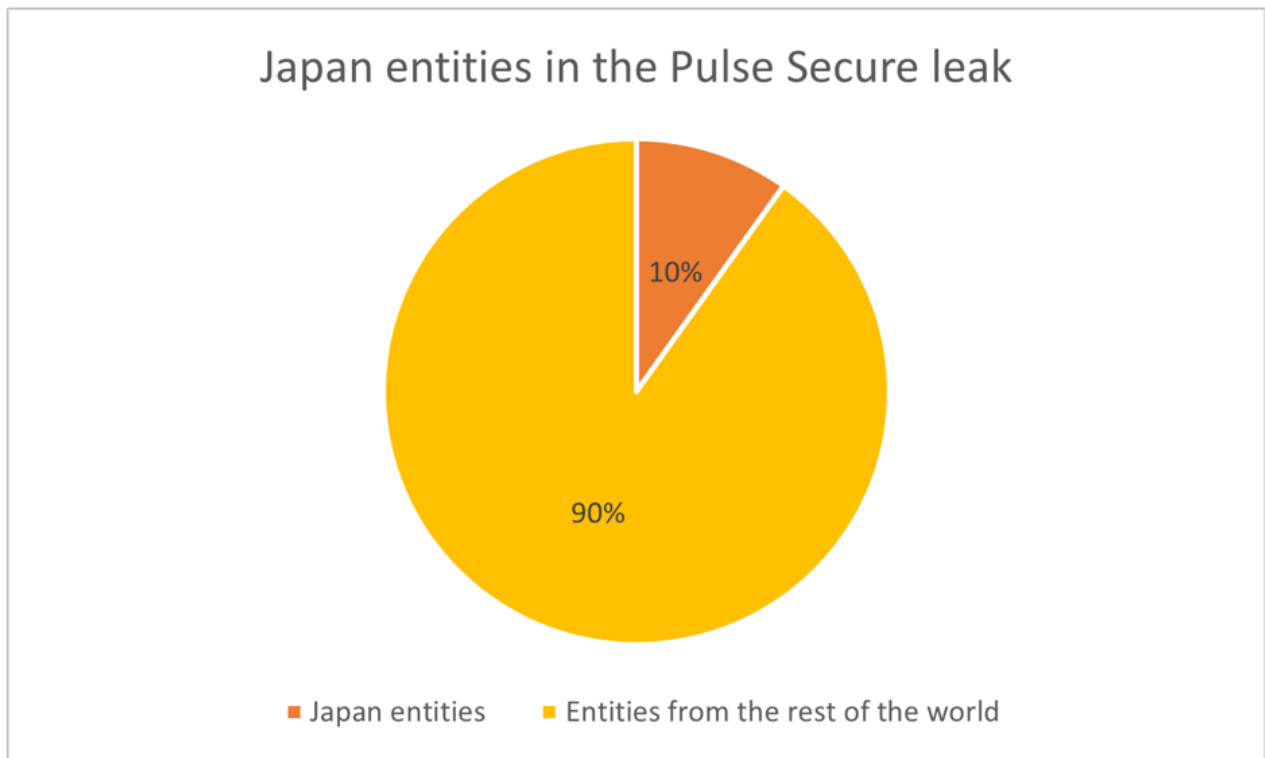
IP	Country	City	ISP	Domain from list
101.	Japan	Minato	Softbank BB Corp.	co.jp
101.	Japan	Suita	K-Opticom Corporation	om
101.	Japan	Osaka	K-Opticom Corporation	jp
113.	Japan	Osaka	UCOM Corp.	.jp
113.	Japan	Minato	UCOM Corp.	com
114.	Japan	Chiyoda	NTT Communications Corporation	com
114.	Japan	Niigata	NTT Communications Corporation	jp
114.	Japan	Tokyo	NTT Communications Corporation	jp
115.	Japan	Edogawa	ARTERIA Networks Corporation	jp
118.	Japan	Uenohara	Softbank BB Corp.	p
118.	Japan	Kyoto	Softbank BB Corp.	com
118.	Japan	Tokyo	Softbank BB Corp.	co.jp
118.	Japan	Shinagawa	So-net Entertainment Corporation	co.ltd
120.	Japan	Chiyoda	ARTERIA Networks Corporation	om
121.	Japan	Osaka	K-Opticom Corporation	com

Part of Japanese entities contained in the Pulse Secure leak (KELA's document based on the leaked directory)

Conclusions and Mitigation Efforts

As can be concluded from this research, more and more threat actors, Advanced APT group and nation state actors are considering Japanese organizations as valuable targets and are actively attacking them via opportunistic and targeted attacks.

Given the latest "work from home" trend and the increased attack surface, KELA has observed many commercial and governmental Japanese entities being recently attacked by known actors – from ransomware gangs to nation-state actors and other financially motivated groups. They're using multiple attack vectors aimed to compromise Japanese entities, gain a foothold into their network and steal sensitive information and funds.

KELA strongly believes that real-time monitoring of darknet communities for both supply and demand can hold significant intelligence value for Japanese defenders. It enables Japanese entities to be more proactive to threats, learn about new tactics used by malicious actors, and take measures to protect against them.

In our next blog post, we will cover the Japanese financial ecosystem and the opportunities threat actors see in targeting both the consumer and the organizations' sides.