Easy Way In? 5 Ransomware Victims Had Their Pulse Secure VPN Credentials Leaked

ke-la.com/easy-way-in-5-ransomware-victims-had-their-pulse-secure-vpn-credentials-leaked/

December 3, 2020

Rising ransomware attacks around the world, together with the recent lists of exposed Pulse Secure VPN credentials set the backdrop for KELA's latest research. While not all ransomware attacks used CVE-2019-11510 (a vulnerability of unpatched Pulse Secure VPN servers) or the previously shared credentials to the compromised corporate networks, it does add another layer to the analysis of possible initial infection vectors used in ransomware incidents. Moreover, the recent exposure of credentials to nearly 50,000 vulnerable Fortinet VPNs raises further concern of possible infection vectors that can be used for ransomware attacks.

Our key findings include:

- **Five victims of ransomware attacks whose credentials to their Pulse Secure VPN servers were exposed** as part of two Pulse Secure VPN lists (i.e., directories with folders and files) that were shared by malicious actors in August 2020.
- **Data of three of the victims were leaked to ransomware gangs' blogs in an attempt to force them to pay a ransom**. Based on KELA's conversation with threat actors related to the attack, at least one victim (unnamed) paid the ransom.
- A threat actor involved in the attack confirmed that they **gained initial access to at least one compromised network via the CVE-2019-11510**.
- Proactive monitoring of darknet threats, such as the Pulse Secure VPN lists, helps enterprise defenders secure their networks and prevent further, more sophisticated attacks, such as ransomware attacks.

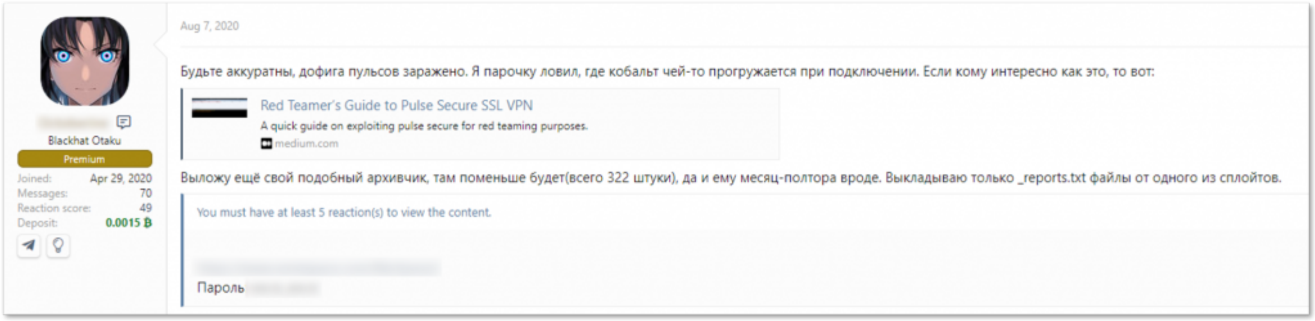
Exploiting the CVE-2019-11510

A vulnerability in Pulse Secure VPN servers, tracked as CVE-2019-11510, is one of the most popular flaws exploited by ransomware gangs to deploy encrypting malware. Travelex, for example, is among the victims compromised through this flaw.

The ransomware operators or their affiliates often use vulnerabilities to gain access to the targeted network, escalate privileges, move laterally, and eventually infect the system with ransomware. In some cases, the operators don't exploit the vulnerabilities by themselves — instead, they buy so-called network access from initial access brokers who had already exploited the flaws, gained privileges, and now sell access via RDP, VPN, or other means.

A recent incident involving the disclosure of Pulse Secure credentials created an opportunity to analyze the CVE-2019-11510 exploitation's internal procedures. As we reported in August 2020, a list of plaintext usernames and passwords, along with IP addresses of more than 900 Pulse Secure VPN enterprise servers, was posted on a Russian-speaking underground forum (we'll call it the first Pulse Secure list).

Darknet chatter indicates the information circulated among malicious actors even before sharing the list. But it doesn't mean threat actors were sharing this list; It's more likely that the actors compiled lists based on open-source research and an automated script weaponizing CVE-2019-11510. For example, a few days after the original list was shared, another threat actor shared an archive of credentials to vulnerable Pulse Secure VPNs (the second Pulse Secure list).



[redacted]
Blackhat Otaku
Premium
Joined: Apr 29, 2020
Messages: 70
Reaction score: 49
Deposit: 0.0015 Ƀ

Aug 7, 2020

Будьте аккуратны, дофига пульсов заражено. Я парочку ловил, где кобальт чей-то прогружается при подключении. Если кому интересно как это, то вот:

> Red Teamer's Guide to Pulse Secure SSL VPN
> A quick guide on exploiting pulse secure for red teaming purposes.
> medium.com

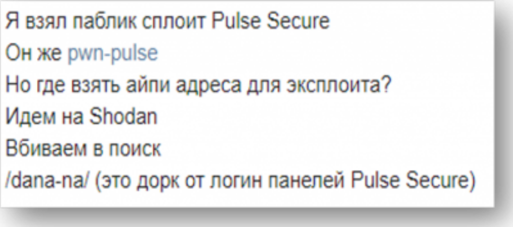
Выложу ещё свой подобный архивчик, там поменьше будет(всего 322 штуки), да и ему месяц-полтора вроде. Выкладываю только _reports.txt файлы от одного из сплойтов.

> You must have at least 5 reaction(s) to view the content.
>
> [redacted]
> Пароль [redacted]

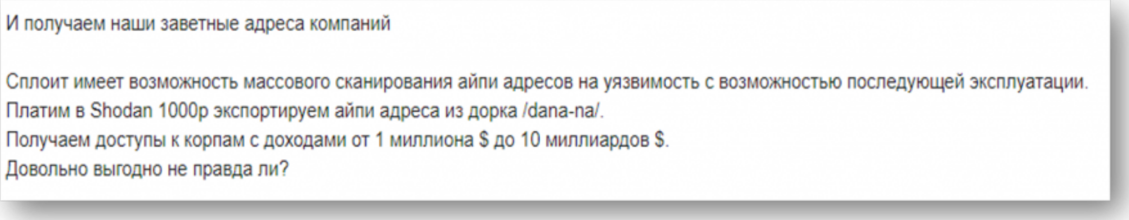
A threat actor shares a "similar archive" collected over 45 days

---

This second list featured more than 300 IP addresses; however, only 131 items were unique compared to the first leak. This finding proves that multiple threat actors targeted the same companies through vulnerable Pulse Secure VPN servers, tracing victims through open-source tools, specifically Shodan. Out of five victims discussed in this post, two still have their IPs present in Shodan results when using the same dork as threat actors looking for a Pulse Secure VPN server.



Я взял паблик сплоит Pulse Secure
Он же pwn-pulse
Но где взять айпи адреса для эксплоита?
Идем на Shodan
Вбиваем в поиск
/dana-na/ (это дорк от логин панелей Pulse Secure)



И получаем наши заветные адреса компаний

Сплоит имеет возможность массового сканирования айпи адресов на уязвимость с возможностью последующей эксплуатации.
Платим в Shodan 1000р экспортируем айпи адреса из дорка /dana-na/.
Получаем доступы к корпам с доходами от 1 миллиона $ до 10 миллиардов $.
Довольно выгодно не правда ли?

An initial access broker, who's primary TTPs include exploiting CVE-2019-11510, describes searching for other vulnerable targets – create a tailored search query on Shodan, export the retrieved addresses and use a public exploit against the vulnerability.

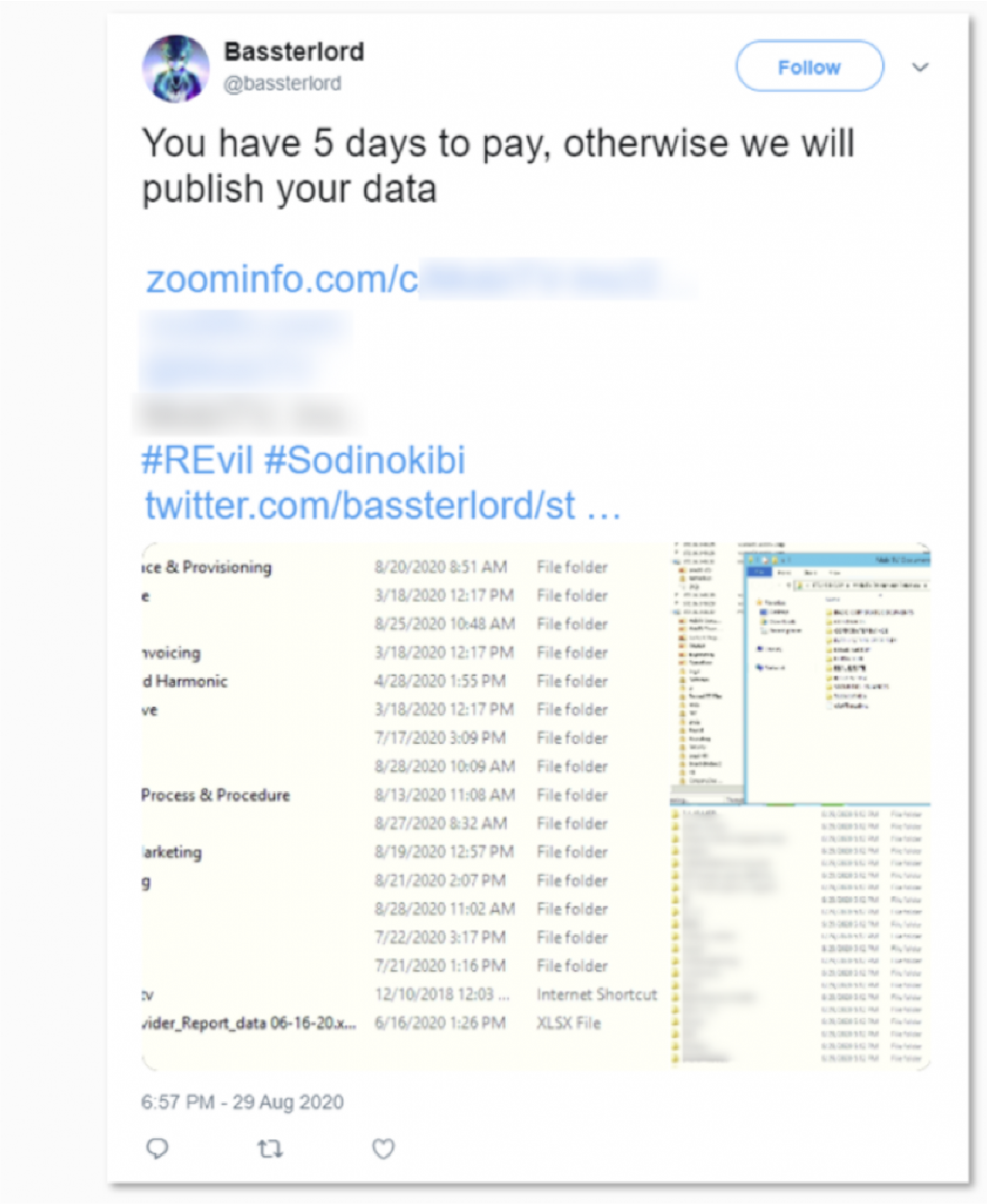
These findings confirm that multiple threat actors might target vulnerable companies for different purposes, including ransomware deployment.

The Victims

KELA discovered five recent ransomware victims in the Pulse Secure lists, indicating that these victims' initial infection vector could be credentials obtained either from the lists or independently through the same vulnerability. Victims were attacked by different ransomware gangs: Egregor, LockBit, Sodinokibi, Maze, and an unknown group. The incidents illustrate how an unpatched Pulse Secure flaw can result in successful, lucrative ransomware attacks.

American Video Delivery Solutions Provider

On August 30, an initial access broker and a known collaborator of the Sodinokibi ransomware gang listed a new victim on their Twitter account: an American video delivery solutions provider.



Bassterlord
@bassterlord

You have 5 days to pay, otherwise we will publish your data

zoominfo.com/c[redacted]

[redacted]

#REvil #Sodinokibi
twitter.com/bassterlord/st …

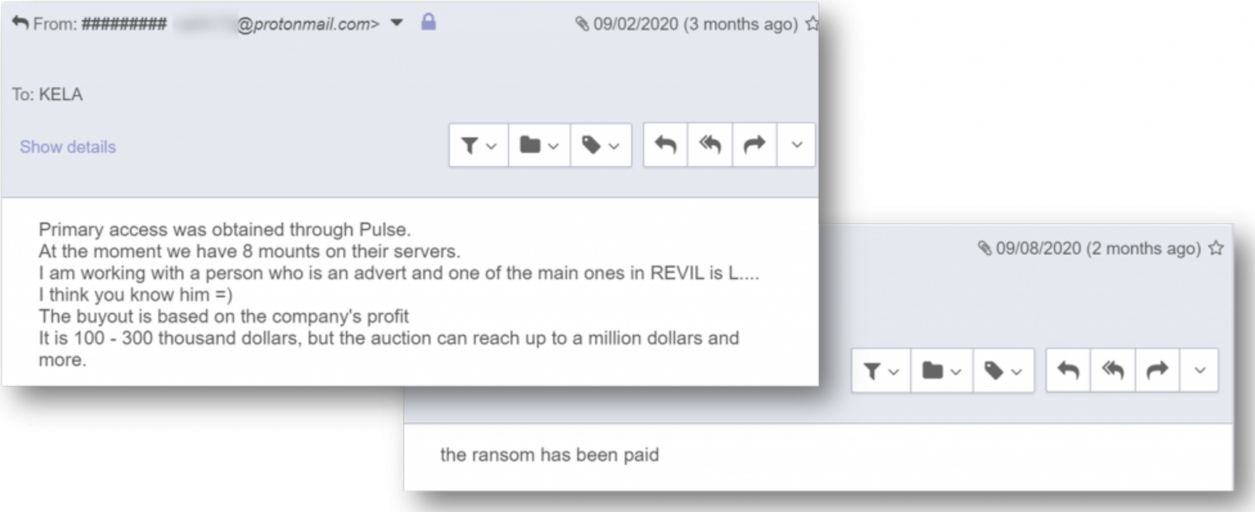
ıce & Provisioning	8/20/2020 8:51 AM	File folder
e	3/18/2020 12:17 PM	File folder
	8/25/2020 10:48 AM	File folder
ıvoicing	3/18/2020 12:17 PM	File folder
d Harmonic	4/28/2020 1:55 PM	File folder
ve	3/18/2020 12:17 PM	File folder
	7/17/2020 3:09 PM	File folder
	8/28/2020 10:09 AM	File folder
Process & Procedure	8/13/2020 11:08 AM	File folder
	8/27/2020 8:32 AM	File folder
ıarketing	8/19/2020 12:57 PM	File folder
g	8/21/2020 2:07 PM	File folder
	8/28/2020 11:02 AM	File folder
	7/22/2020 3:17 PM	File folder
	7/21/2020 1:16 PM	File folder
ıv	12/10/2018 12:03 ...	Internet Shortcut
ɿider_Report_data 06-16-20.x...	6/16/2020 1:26 PM	XLSX File

6:57 PM - 29 Aug 2020

A few days later, the broker contacted KELA offering proof of a successful ransomware attack. He said he plans to post the stolen data on a well-known Russian-speaking underground forum.

An IP belonging to the company appeared in the first Pulse Secure list. Answering KELA's questions, the broker confirmed he used CVE-2019-11510 to obtain access to the compromised network. He claimed to work with Lalartu, a well-known affiliate of Sodinokibi, suggesting that he sold the initial access to this affiliate.

Unfortunately, in this scenario, as stated by the broker, the ransomware operators eventually received the ransom, amounting to $100K- $300K. The broker probably took a share and didn't sell it for the fixed price since he made significant efforts to intimidate the victim and force them to pay. In a recent interview, Sodinokibi acknowledged their affiliates receive 70-80% of the ransom, meaning a potential gain of $70K-$240K in this attack.



From: ######### [redacted]@protonmail.com>

09/02/2020 (3 months ago)

To: KELA

Primary access was obtained through Pulse.
At the moment we have 8 mounts on their servers.
I am working with a person who is an advert and one of the main ones in REVIL is L....
I think you know him =)
The buyout is based on the company's profit
It is 100 - 300 thousand dollars, but the auction can reach up to a million dollars and more.

09/08/2020 (2 months ago)

the ransom has been paid

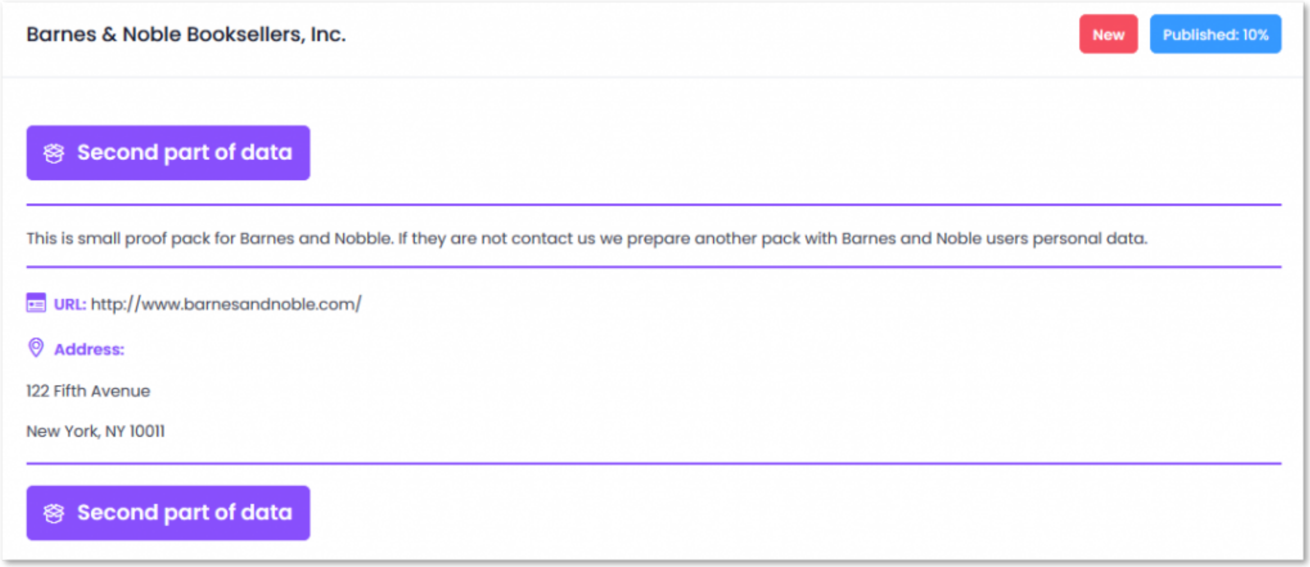
The broker shares details of the attack with KELA, probably attempting to pressure the victim

---

Barnes & Noble

Five IP addresses of Barnes & Noble were present in both Pulse Secure lists, implying the company was vulnerable to CVE-2019-11510. In October 2020, the company disclosed it was a victim of a ransomware attack. The Egregor ransomware gang, which emerged in September 2020 as a possible successor to Sekhmet, claimed responsibility for the attack on its blog.

While the initial infection vector in this attack remains unknown, Barnes & Noble's Pulse Secure VPN credentials were already exposed in the darknet three months ago. Attackers obtained the credentials using the CVE-2019-11510 vulnerability, which means that at some point, the company had unpatched Pulse Secure VPN servers. This initial hypothesis was later revoked when an actor involved in the attack shared that he did not exploit vulnerable Pulse Secure credentials in order to access Barnes & Noble's network.


Barnes & Noble Booksellers, Inc.

This is small proof pack for Barnes and Nobble. If they are not contact us we prepare another pack with Barnes and Noble users personal data.

URL: http://www.barnesandnoble.com/

Address:

122 Fifth Avenue
New York, NY 10011

SK Hynix

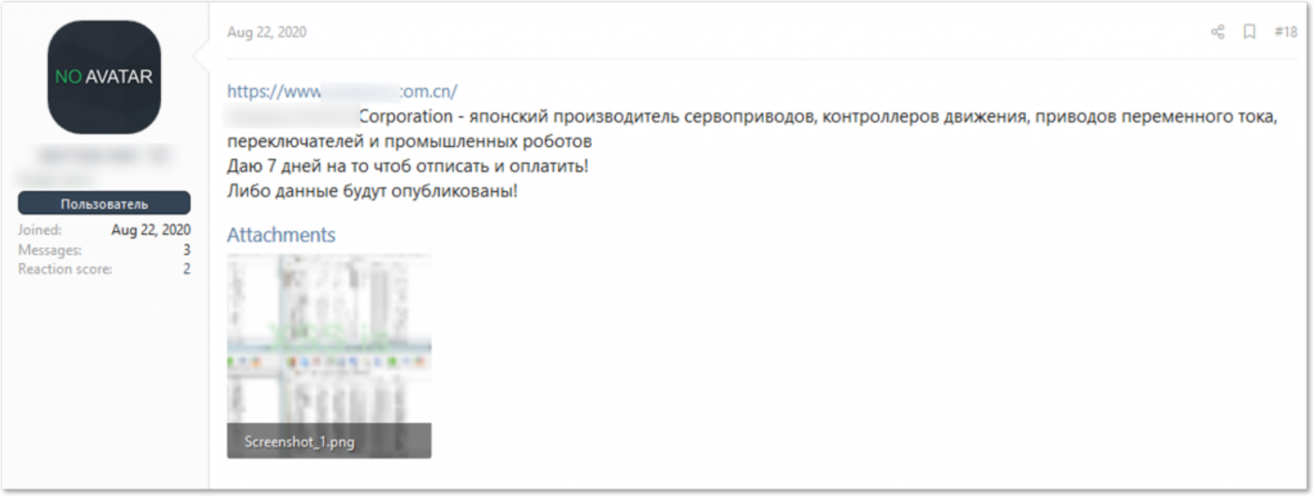
Maze attacked the South Korean memory and semiconductor manufacturer SK Hynix, one of the world's top hardware companies reporting $22 billion in revenue, in August 2020. The attackers stole documents, including emails relating to price negotiations with clients like Apple and IBM. The company had one IP in the Pulse Secure list – in Italy, where the company's European R&D Centre is situated. While no details of the attack are known, exploitation of CVE-2019-11510 is among Maze's TTPs.

A Vietnamese IT Corporation

Based on confidential information obtained by KELA, a Vietnamese IT corporation suffered a ransomware incident in August 2020. Two of the company's IP addresses were exposed in the Pulse Secure lists, one of them present in both lists – suggesting several threat actors might target it. Based on TTPs used in the attack, Maze could be responsible, although the ransomware gang has not mentioned the company online, and there were no media reports of the incident.

Japanese Manufacturing Company

LockBit ransomware operators launched an attack against this Japanese manufacturing company. The gang first exposed the victim in a thread on a Russian-speaking underground forum, listing a .cn domain, indicating the target was a Chinese branch. A few days later, LockBit listed the victim on their blog without mentioning any domain names.



[redacted]

Пользователь

Joined: Aug 22, 2020
Messages: 3
Reaction score: 2

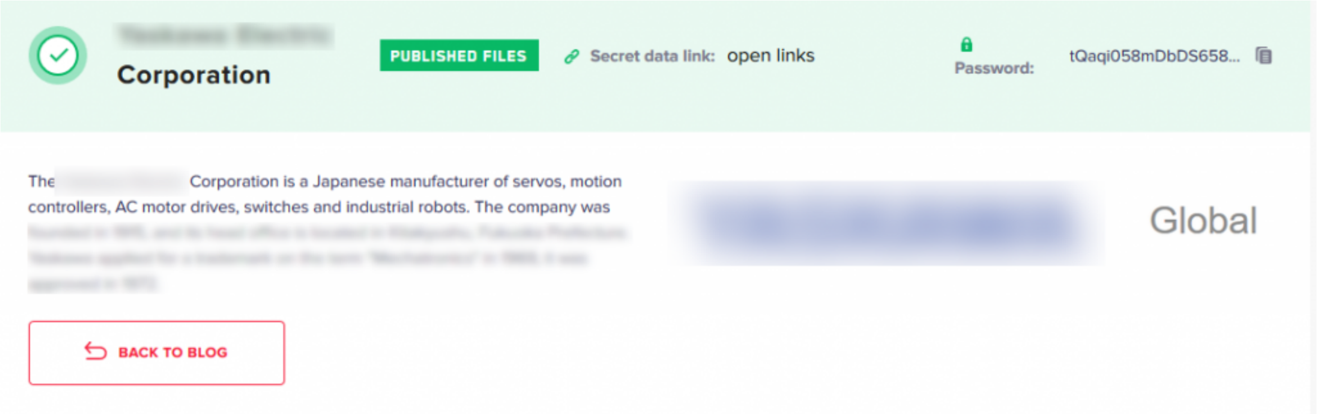
Aug 22, 2020 #18

https://www[redacted]om.cn/
[redacted]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

The victim announced in the LockBit's thread



[redacted] Corporation

PUBLISHED FILES

Secret data link: open links

Password: tQaqi058mDbDS658...

The [redacted] Corporation is a Japanese manufacturer of servos, motion controllers, AC motor drives, switches and industrial robots. The company was [redacted]

Global

The victim shared on the LockBit's website

While malicious actors often leverage Pulse Secure flaws to launch ransomware attacks, we usually discover the initial infection vector after the incident occurred and the investigation has been concluded.

However, as our post indicates, it is possible to prevent some intrusions by regularly monitoring darknet forums and repositories in order to detect potential threats to organizations. Organizations globally are continually threatened by the exposure and ongoing circulation of their sensitive credentials that are posted on the web. Taking into consideration the nature of the underground ecosystem, the credentials exposed in recent instances (such as the exposures of the Pulse Secure VPNs and Fortinet VPNs) will likely continue to be leveraged for more crucial cyber-attacks, creating a greater need for enterprise defenders to monitor weakness in their networks and exposure of their data in the Dark Net.