

Prometheus Ransomware Gang: A Group of REvil?

unit42.paloaltonetworks.com/prometheus-ransomware/

Doel Santos

June 9, 2021

By [Doel Santos](#)

June 9, 2021 at 3:00 AM

Category: [Ransomware](#), [Unit 42](#)

Tags: [Prometheus](#), [REvil](#), [Thanos](#)



This post is also available in: [日本語 \(Japanese\)](#).

Executive Summary

Unit 42 has spent the past four months following the activities of Prometheus, a new player in the ransomware world that uses similar malware and tactics to ransomware veteran [Thanos](#).

Prometheus leverages double-extortion tactics and hosts a leak site, where it names new victims and posts stolen data available for purchase. It claims to have breached 30 organizations in government, financial services, manufacturing, logistics, consulting,

agriculture, healthcare services, insurance agencies, energy and law firms in the United States, United Kingdom and a dozen more countries in Asia, Europe, the Middle East and South America.

Like many ransomware gangs, Prometheus runs like a professional enterprise. It refers to its victims as “customers,” communicates with them using a customer service ticketing system that warns them when payment deadlines are approaching and even uses a clock to count down the hours, minutes and seconds to a payment deadline.

“We are closing the ticket and have started an auction on your data,” the group threatens when victims fail to pay up. But there’s an out: Victims can click to open a new “ticket” if they’re willing to pay up to stop the auction and recover their data.

Only four victims have paid to date, according to the group’s leak site. It claims that a Peruvian agricultural company, a Brazilian healthcare services provider and transportation and logistics organizations in Austria and Singapore paid ransoms. However, we’re unable to confirm the ransom amounts.

One interesting note is that Prometheus claims to be part of the notorious ransomware gang REvil. Unit 42 has seen no indication that these two ransomware gangs are related in any way. The claim may be an attempt to exploit REvil’s name to persuade victims to pay up, or it could be a false flag to take attention away from Thanos.

We’ve compiled this report to shed light into the threat posed by the emergence of new ransomware gangs like Prometheus, which are able to quickly scale up new operations by embracing the ransomware-as-a-service (RaaS) model, in which they procure ransomware code, infrastructure and access to compromised networks from outside providers. The RaaS model has lowered the barrier to entry for ransomware gangs.

Full visualization of the Prometheus techniques observed and the courses of action relevant for response can be viewed in the [Unit 42 ATOM Viewer](#).

If you think you may have been impacted, please email unit42-investigations@paloaltonetworks.com or call (855) 875-4631 to get in touch with the Unit 42 Incident Response team.

Prometheus Ransomware Overview

Prometheus ransomware was first observed in February 2021 and is a new variant of a known strain called Thanos. Thanos ransomware has been advertised for sale on underground forums since at least the first half of 2020, where it has a builder that allows actors to customize a sample with a wide variety of available settings. This suggests that different threat actors may have leveraged this builder to create their own variants and brands.

In this case, we turn our attention to one of those threat actors, Prometheus. While this ransomware gang claims to be part of REvil, we haven't seen any other solid connection between the two groups. REvil operates on an affiliate-driven RaaS program, but we believe the Prometheus ransomware gang may be acting on their own and attempting to leverage the infamous REvil name and reputation to improve the chance that victims will pay the demanded ransom. This would not be the first time adversaries have used the names of well-known threat groups to strengthen their credibility.

At the time of writing, we don't have information on how Prometheus ransomware is being delivered, but threat actors are known for buying access to certain networks, brute-forcing credentials or spear phishing for initial access.

When Prometheus ransomware is executed, it tries to kill several backups and security software-related processes, such as Raccine, a ransomware prevention tool that tries to stop ransomware from deleting shadow copies in Windows. Here is a sample of its approach:

```
"taskkill" /F /IM RaccineSettings.exe
"reg" delete
"HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Raccine
Tray" /F
```

Prometheus ransomware appends an extension using the following format `.[XXX-XXX-XXXX]` (Figure 1). We found that the extensions are hardcoded into the sample. We believe that the Prometheus ransomware operators generate a unique payload per victim, which is used for their negotiation site to recover files. We obfuscated the extensions because they could be used to identify the victims on the leak site. Prometheus also adds an hexadecimal string of `GotAllDone` at the end of all encrypted files.

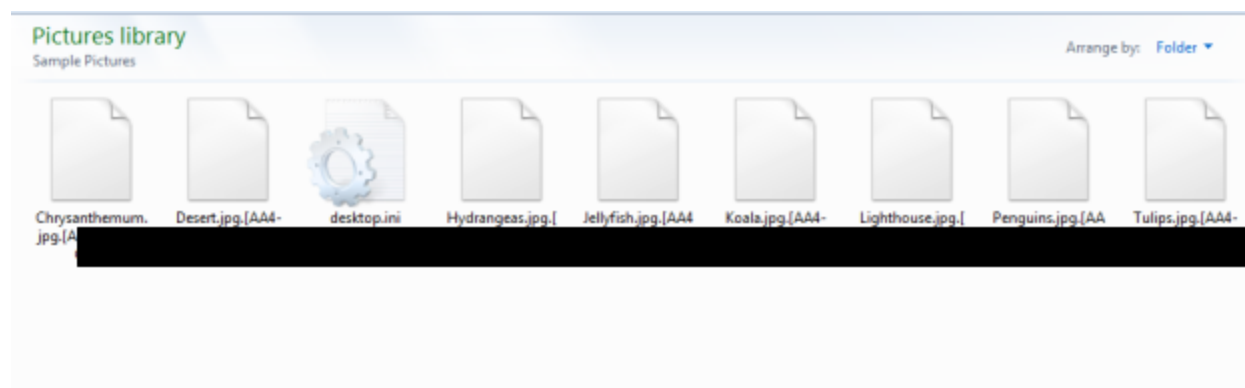


Figure 1. Encrypted files after execution.

After the backup and security processes are terminated and encryption is complete, Prometheus ransomware drops two ransom notes: a `RESTORE_FILES_INFO.TXT` file and a `RESTORE_FILES_INFO.TXT.hta` file (Figure 2), both containing the same information.



Figure 2. RESTORE_FILES_INFO.hta.

The ransom note also includes instructions for contacting Prometheus ransomware operators to recover files, as well as informing the victim that, if the demands are not met, the threat actors will release the data to the public or sell it to a third party.

Since the extensions are used as a victim identifier, by following the instructions on the ransom note, we were able to take a look at the negotiation part of their site using the extensions ID to gain access. Interestingly, this group uses a ticketing system for tracking victims. The tickets include a tracking ID, created date, resolution status and priority. A victim can even open a ticket with the threat actors to request data recovery – though this will cost you extra, according to the site (Figure 3).

Immediately after payment we will send you decryption tool and decryption key.
You just have to run decryption tool and files will be decrypted automatically!
Waiting for your answer.

[If you don't answer is within 48 hours, then we put your data on a private auction for sale](#)

[You can see status of your data in our blog](#)

[Refresh this page](#)

Reply by **Prometheus - group of REvil** » about 7 hours ago



You have not contacted us within 3 days.
We are closing the ticket and started an auction on your data.
If you still want to recover data, open a request.

Ticket Details [Refresh this page](#)

Tracking ID: YHA-GH6-JI7Y

Ticket status: Resolved

[\[Open ticket\]](#)

This message verified by Prometheus Team.



Figure 3. Prometheus reply to a victim ticket.

The Prometheus ransomware gang tailors their ransom demand depending on the victim organization. From the available instances observed, we have seen payments requested as low as \$6,000 and as high as \$100,000 in Monero (XMR). This price is doubled if the victims don't contact the threat actors within the established timeframe, which on average is a week. At the time of writing, four victims paid the ransom including a Peru-based agricultural company, a healthcare services provider in Brazil, and two transportation and logistics organizations – one located in Austria and the other in Singapore.

YOUR COMPANY NETWORK HAS BEEN HACKED

Company: [REDACTED] 4 days ago

our XMR wallet:
48D26uLnC1q7ZnKV152Kbsdtbc25Rq5SDGx5XcpcP4q7VpKFNf1N3LdPg57rEARcwi6GAGb86eN9gEoY1muPPMfDqZ7vrxk
* After payment please send a screen-shot or ID of the transaction!

You have: 3 days, 19:06:19

* If you do not pay on time, the price will be doubled
* Time end on **Jun 06, 06:30:10**

Current price: 100000 \$
After time ends: 200000 \$

Hello dear customer,

Your data was encrypted with strong crypto algorithm and can be decrypted fast and safely. Don't worry, we can help you to restore your servers to initial state.

If you want to be sure that we can decrypt your data please send us up to 2-3 small files for free test decryption (zip files, archive should be no more 2 MB). Files must not contain valuable information.

If you decide not to work with us:
- All data on your computers will remain encrypted forever.
- **YOUR DATA ON OUR SERVER AND WE WILL RELEASE YOUR DATA TO PUBLIC OR RE-SELLER!**
(Information about companies and status in our blog)
- So you can expect your data to be publicly available in the near future.
- The price will increase over time.

If doesn't matter to us what you choose pay us or we will sell your data. We only seek money and our goal is not to damage your reputation or prevent your business from running.

We accept payments in Monero (XMR) cryptocurrency.
Buy XMR (no need for verification): <https://localmonero.co/>
Buy XMR with bank: <https://www.kraken.com/>
Buy XMR locally with cash or online: <https://www.kraken.com/>
All change: <https://www.bestchange.com/>
[You can buy bitcoins and exchange for monero.](#)

Immediately after payment we will send you decryption tool and decryption key.
You just have to run decryption tool and files will be decrypted automatically!
Waiting for your answer.

Ticket Details [Refresh this page](#)

Tracking ID: [REDACTED]

Ticket status: **Resolved**
[\[Open ticket\]](#)

Created on: 2021-05-22 06:30:10

Last repiler: Prometheus - group of REvil

Replies: 1

Priority: ■ Medium

Figure 4. Prometheus victim ticket.

Like many current ransomware gangs, this group also created a leak site (a different section of the same website that hosts the “ticketing system”) where they name and shame their victims (Figure 5).



Figure 5. Prometheus leak site.

The Prometheus ransomware operators include a status per victim. We found that some of the information posted on the leak site has already been sold to an unknown third party. There are also posts showing that victims within impacted industries paid the ransom and their data was removed from the site (Figure 6).

Leak Status

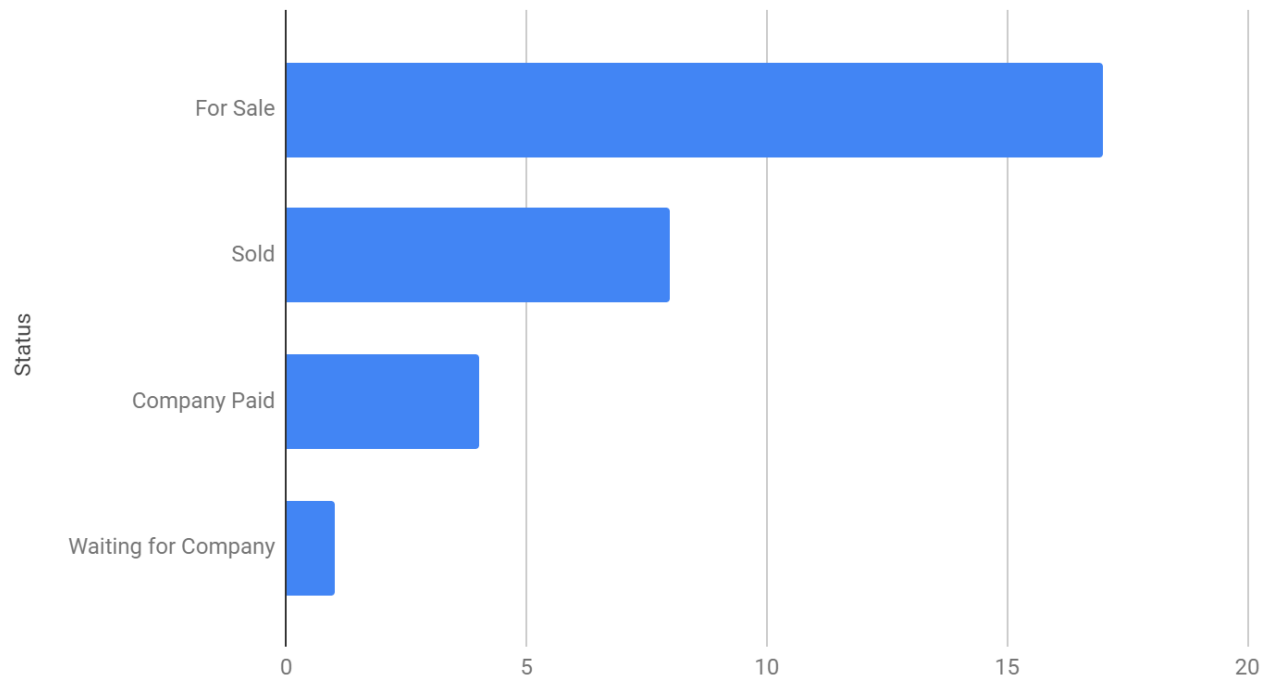


Figure 6. Leak site victim status for Prometheus ransomware out of 30 victims.

Prometheus Victimology

At the time of this writing, the Prometheus leak site hosts 30 victims, impacting multiple industries globally. By taking a look at their victims listed, we generated this graph, showing the locations of organizations impacted by this ransomware.

Impacted Countries

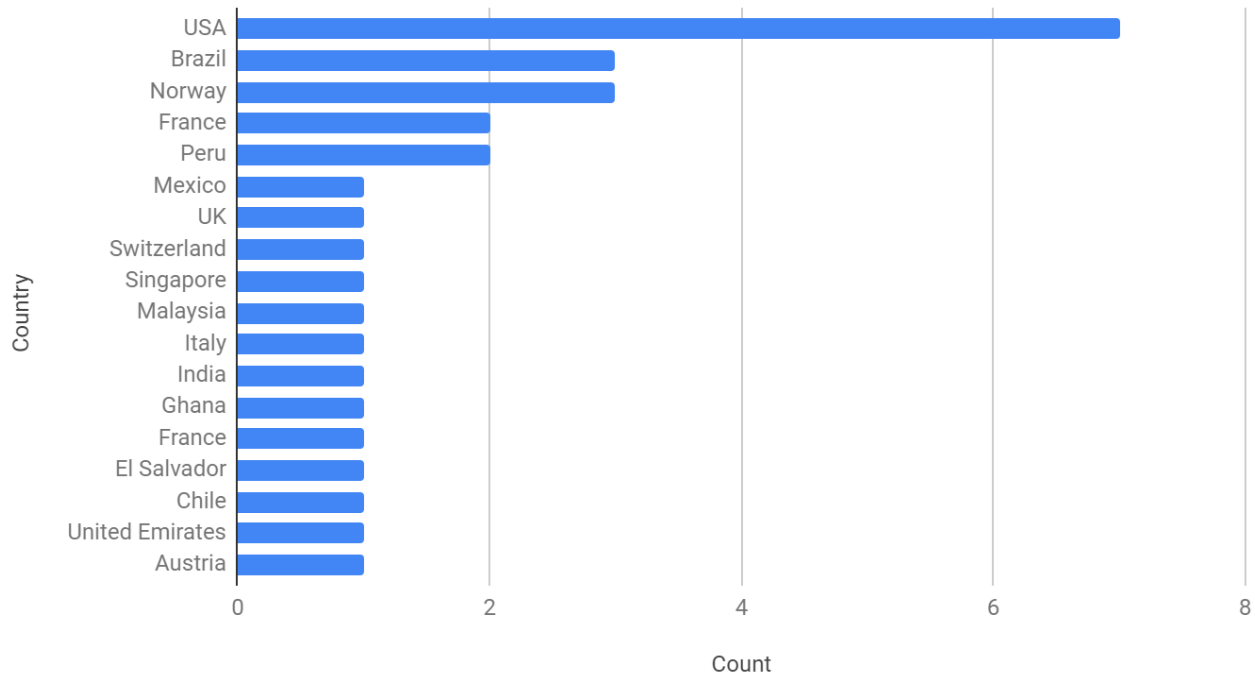


Figure 7. Countries impacted by Prometheus ransomware out of 30 victims. Manufacturing was the most impacted industry among the victim organizations we observed, closely followed by the transportation and logistics industry.

Impacted Industries

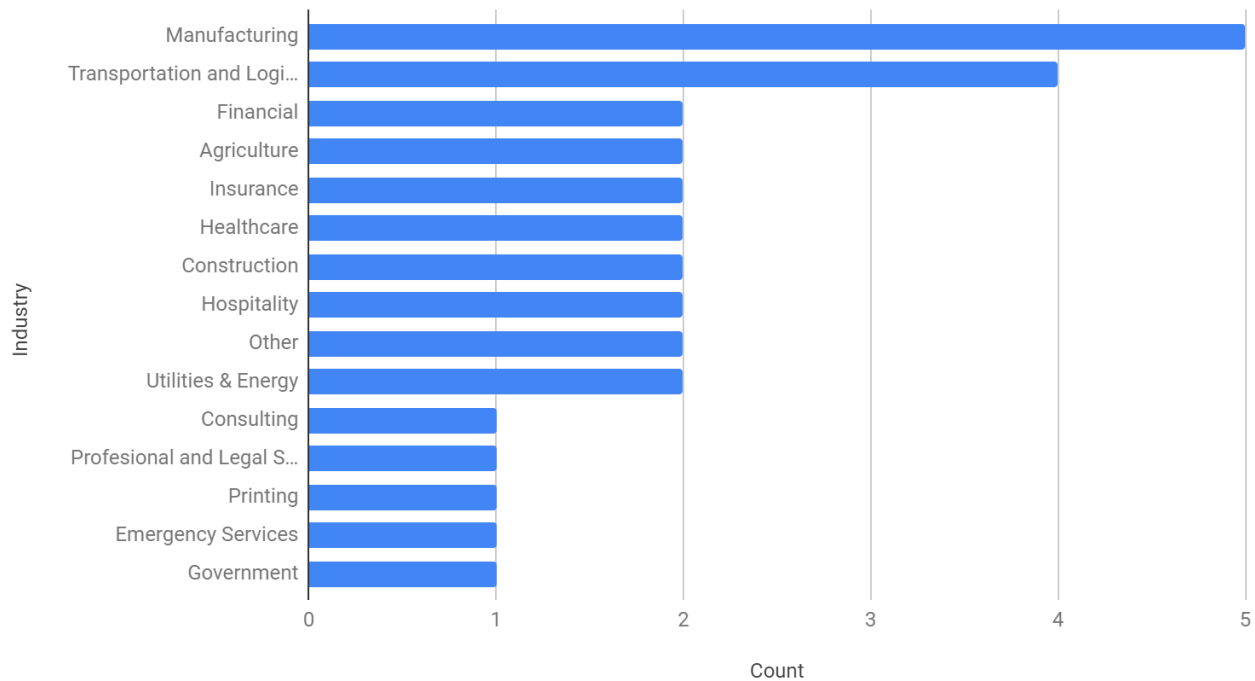
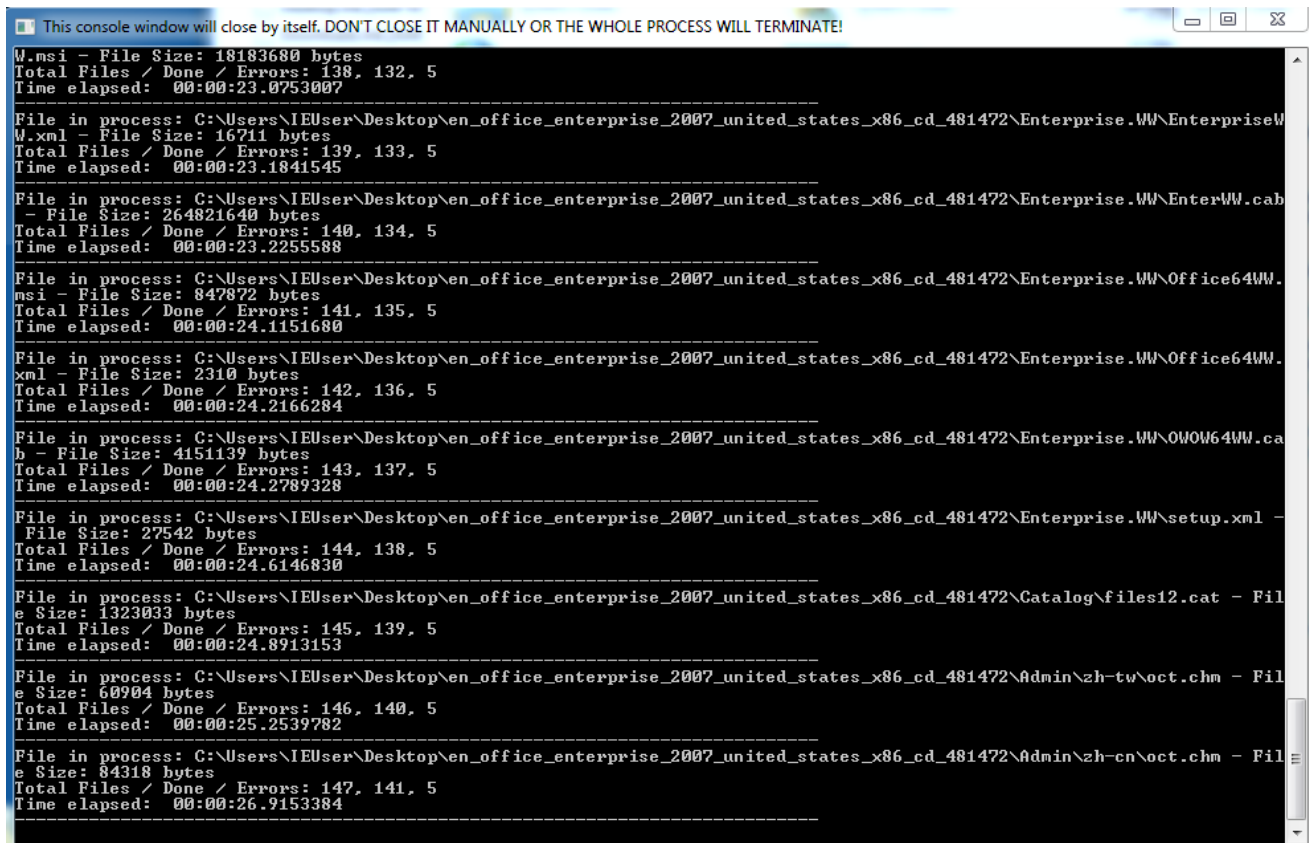


Figure 8. Industries impacted by Prometheus ransomware out of 30 victims.

Older Prometheus Variants

The first encountered Prometheus sample, first observed in February 2021 (SHA256: 9bf0633f41d2962ba5e2895ece2ef9fa7b546ada311ca30f330f0d261a7fb184), behaves similarly to the more recent variant we are currently tracking. However, it appends the following extension to the encrypted files: .PROM[prometheushelp@mail[.]ch].

Some of the observed samples, when executed, opened a Windows Command Shell showing the encryption progress (Figure 9). The most recent Prometheus samples do not display this information.



```
This console window will close by itself. DON'T CLOSE IT MANUALLY OR THE WHOLE PROCESS WILL TERMINATE!
W.msi - File Size: 18183680 bytes
Total Files / Done / Errors: 138, 132, 5
Time elapsed: 00:00:23.0753007

-----
File in process: C:\Users\IEUser\Desktop\en_office_enterprise_2007_united_states_x86_cd_481472\Enterprise.WW\EnterpriseW
W.xml - File Size: 16711 bytes
Total Files / Done / Errors: 139, 133, 5
Time elapsed: 00:00:23.1841545

-----
File in process: C:\Users\IEUser\Desktop\en_office_enterprise_2007_united_states_x86_cd_481472\Enterprise.WW\EnterWW.cab
- File Size: 264821640 bytes
Total Files / Done / Errors: 140, 134, 5
Time elapsed: 00:00:23.2255588

-----
File in process: C:\Users\IEUser\Desktop\en_office_enterprise_2007_united_states_x86_cd_481472\Enterprise.WW\Office64W.
msi - File Size: 847872 bytes
Total Files / Done / Errors: 141, 135, 5
Time elapsed: 00:00:24.1151680

-----
File in process: C:\Users\IEUser\Desktop\en_office_enterprise_2007_united_states_x86_cd_481472\Enterprise.WW\Office64W.
xml - File Size: 2310 bytes
Total Files / Done / Errors: 142, 136, 5
Time elapsed: 00:00:24.2166284

-----
File in process: C:\Users\IEUser\Desktop\en_office_enterprise_2007_united_states_x86_cd_481472\Enterprise.WW\OWOW64W.ca
b - File Size: 4151139 bytes
Total Files / Done / Errors: 143, 137, 5
Time elapsed: 00:00:24.2789328

-----
File in process: C:\Users\IEUser\Desktop\en_office_enterprise_2007_united_states_x86_cd_481472\Enterprise.WW\setup.xml -
File Size: 27542 bytes
Total Files / Done / Errors: 144, 138, 5
Time elapsed: 00:00:24.6146830

-----
File in process: C:\Users\IEUser\Desktop\en_office_enterprise_2007_united_states_x86_cd_481472\Catalog\files12.cat - Fil
e Size: 1323033 bytes
Total Files / Done / Errors: 145, 139, 5
Time elapsed: 00:00:24.8913153

-----
File in process: C:\Users\IEUser\Desktop\en_office_enterprise_2007_united_states_x86_cd_481472\Admin\zh-tw\oct.chm - Fil
e Size: 60904 bytes
Total Files / Done / Errors: 146, 140, 5
Time elapsed: 00:00:25.2539782

-----
File in process: C:\Users\IEUser\Desktop\en_office_enterprise_2007_united_states_x86_cd_481472\Admin\zh-cn\oct.chm - Fil
e Size: 84318 bytes
Total Files / Done / Errors: 147, 141, 5
Time elapsed: 00:00:26.9153384
```

Figure 9. Encryption progress window.

Another variant (SHA256:

11aebdff8c064c160c2b21f3a844bacaecd581d9dc2e4224d31903d2a56e2dd3) appended the .XXXXXXXXXX[prometheusdec@yahoo[.]com] extension format to encrypted files where the X is the victim ID. Like the current variant, it generates two ransom note files. The ransom note includes two ways to contact the group that are different from those offered by the current variant (Figure 10). Based on the content and instructions provided by this variant, we believe Prometheus didn't have a leak site established at the time they distributed it.

!!! ALL YOUR FILES ARE ENCRYPTED !!!

All your files, documents, photos, databases and other important files are encrypted.

You are not able to decrypt it by yourself! The only method of recovering files is to purchase a unique private key. Only we can give you this key and only we can recover your files.

!!!!!!! We backed up all your documents and databases. IF YOU NOT START DIALOGUE WITH US, WE WILL POST ALL YOUR DOCUMENTS AND DATABASES ON INTERNET. !!!!!!!

We recommend you upload 3 encrypted files in <https://privatlab.com/file> and paste link to you message. We will demonstrate that we can recover your files.

** Please note that files must not contain any valuable information.*

Do you really want to restore your files?

1) Using a TOR browser!

a) Download and install TOR browser from this site: <https://torproject.org/>

b) Open website: <http://sonarmsniko2lvfu.onion/?a=reg>


Registration Form

There is no way to recover the password, make sure you don't forget it.

Username
Valid characters: a-Z, 0-9, _ and -


Password


Same Password




Enter the captcha.

c) Register account

d) Click Compose  [Compose · Inbox · Sent · Settings](#) and write to us, our username: Prometheus, in message write Your key identifier (it is at the end of file) and file extension (forexample .TEST[prometheushelp@mail.ch]) and link to 3 encrypted files in <https://privatlab.com/file>

To:  Write our username

Subject:

Message:  Write you Key Identifier here

There is a limit of 8000 characters

2) Using a email!

Write to 3 emails address at once, in message write Your key identifier (it is at the end of file) and file extension (forexample .TEST[prometheushelp@mail.ch]) and link to 3 encrypted files in <https://privatlab.com/file> :

prometheusdec@yahoo.com
prometheusdec@hotmail.com
prometheusdec@gmail.com

We recommend using 1 method via TOR browser to contact us.

Email letters may not reach us. Therefore, if you do not receive a response within 12 hours, please use method 1.

Figure 10. RESTORE_FILES_INFO.hta (as sent by an older Prometheus variant).

Instead of directing the victim to the leak site as the current variant does, the older variant of Prometheus instructs the victim to go to a Tor site called Sonar, a web-based messaging service, and create an account. After the account is created, the ransom note instructs the

victim to send a message to the username Prometheus, containing the file extension identifier and a link to three encrypted files to provide proof of decryption. The second method of contact is through email and includes three email addresses for contact, requesting the same information as the first method.

This helps us understand how the Prometheus ransomware group originally operated and shows the evolution of their approach to securing payment before deciding to start their own leak site.

Conclusion

Prometheus is a new and emerging ransomware gang that uses a personalized variant of Thanos ransomware. The operators behind this ransomware are actively targeting multiple industries globally. Like many other ransomware groups, Prometheus hosts a leak site to create additional pressure and shame victims into paying the ransom. While Prometheus claims to be part of the REvil ransomware gang, during our research, we didn't find a solid connection between the two ransomware groups at the time of writing this report.

Indicators associated with this Threat Assessment are available on [GitHub](#), have been published to the [Unit 42 TAXII](#) feed and are viewable via the ATOM Viewer.

Palo Alto Networks customers are protected from this threat by:

- [WildFire](#): All known samples are identified as malware.
- [Cortex XDR](#) with:
 - Indicators for Prometheus/Thanos.
 - Anti-Ransomware Module to detect Prometheus/Thanos encryption behaviors.
 - Local Analysis detection to detect Prometheus/Thanos binaries.
- [AutoFocus](#): Tracking related activity using the [Thanos](#) tag.

More information on ransomware can be found in the [2021 Unit 42 Ransomware Threat Report](#).

Indicators of Compromise

```
11aebdff8c064c160c2b21f3a844bacaecd581d9dc2e4224d31903d2a56e2dd3
52f7f9e8369a3e89899d40e89766c9642b137b25bfd58a2b564dac67a40445f3
8c723af5c826adea162ef3f2e37a1cca7b43d549c9a5fab7c9ff17f65eb5d8e7
9d85a74f073c4403e3a91017b6757e0368139e672498a2f84f5efaad0d1b573b
A0e20c580e8a82f4103af90d290f762bd847fadd4eba1f5cd90e465bb9f810b7
20d9efe472c01a0a23c9764db679b27a4b6a4d72e697e3508e44f218b8b952f5
e1c46a96effc5df063cea2fae83306ae1f0e2f898b0d2ada86c48052be5fe8d3
f90d4b7491d9f365748dbc3d2379ab20520421ab57790e9a934bb5cf2ecb2404
```

A090bb0e9118d7460c448304ccf47333ea64b90576230b8b4b5dee96f702ecf6
9bf0633f41d2962ba5e2895ece2ef9fa7b546ada311ca30f330f0d261a7fb184
779db1c725f71e54d4f31452763784abe783afa6a78cc222e17796b0045f33fc

Courses of Action

This section documents relevant tactics, techniques and procedures (TTPs) used with Prometheus and maps them directly to Palo Alto Networks product(s) and service(s). It also further instructs customers on how to ensure their devices are configured correctly.

Product / Service

Course of Action

Persistence, Privilege Escalation

The below courses of action mitigate the following techniques:

Registry Run Keys / Startup Folder
[[T1547.001](#)]

Cortex XDR

Enable Anti-Exploit Protection

Enable Anti-Malware Protection

Defense Evasion

The below courses of action mitigate the following techniques:

Disable or Modify Tools [[T1562.001](#)],
Modify Registry [[T1112](#)]

Cortex XDR

Look for the following BIOC alerts to detect activity: Process attempts to kill a known security/AV tool

Enable Anti-Malware Protection

Discovery

The below courses of action mitigate the following techniques:

Process Discovery [[T1057](#)]

Cortex XDR	XDR monitors for behavioral events via BIOC's along a causality chain to identify discovery behaviors*
Impact	
The below courses of action mitigate the following techniques: Data Encrypted for Impact [T1486], Inhibit System Recovery [T1490]	
Cortex XSOAR	Deploy XSOAR Playbook - Ransomware Manual for incident response.
Deploy XSOAR Playbook - Palo Alto Networks Endpoint Malware Investigation	
Cortex XDR	Enable Anti-Malware Protection Look for the following BIOC's alerts to detect activity*: Cortex XDR Agent - Behavioral Threat Detected

Table 1. Courses of Action for Prometheus ransomware. These analytic detectors will trigger automatically for Cortex XDR Pro customers.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).