

Cybereason vs. Prometheus Ransomware

 cybereason.com/blog/cybereason-vs.-prometheus-ransomware



Cybereason vs. Prometheus Ransomware



Cybereason vs. Prometheus Ransomware

Written By
Cybereason Nocturnus

July 15, 2021 | 10 minute read

Prometheus is a relatively new variant of the [Thanos](#) ransomware that is operated independently by the Prometheus group, and was first observed in February of 2021. In just a short period of time, Prometheus caused a lot of damage, and breached over 40 companies.

Key Findings

- **High Severity:** The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
- **Human Operated Attack:** Prior to the deployment of the ransomware, the attackers attempt to infiltrate and move laterally throughout the organization, carrying out a fully-developed attack operation.
- **Shared Builder:** The Prometheus group, as well as other threat actors, used the Thanos builder to build and customize their ransomware.
- **Group of REvil?:** Prometheus ransomware branding themselves as part of the REvil group, probably in an attempt to piggyback on the fame of one of the most infamous - and successful - ransomware groups.
- **Detected and Prevented:** [The Cybereason Defense Platform](#) fully detects and prevents the Prometheus ransomware:

Cybereason Detects and Blocks Prometheus Ransomware

Like other prominent ransomware groups, such as the [DarkSide](#) group, Prometheus follows the RaaS business model and operates as a professional enterprise where it refers to its victims as “customers,” and communicates with them using a customer service ticketing system.

In addition, Prometheus follows the [double extortion trend](#) and hosts a leak site, where it has a “hall of shame” for victims and posts stolen data for sale. The names of the victims are posted on the website even before the victims decide whether to pay or not, either under the status “waiting for the company decision” or “company paid, data is not for sale.”

When it comes to the affected industries and regions, the group seems to attack almost indiscriminately. According to their website, the group claims to have breached over 40 organizations from different industries/sectors. Among their victims observed were companies in the following industries: consulting, oil and gas, financial, media, governments, advertising, manufacturing, retail, food, hotels, manufacturing, insurance, transportation, and medical services. The regions affected are South America, US, UK, Middle-East, UAE, Asia and Europe.

It’s also interesting to note that some victims appear to be on the list more than once, but attacked in different time periods. Since those victims had paid, it’s unclear at this point if it’s by mistake or that the group has attacked the same victim more than once before or even after paying.

A recent Cybereason report titled [Ransomware: The True Cost to Business](#), found that 80% of organizations that paid a ransom were hit by a second attack, and almost half of those were hit by the same threat group.

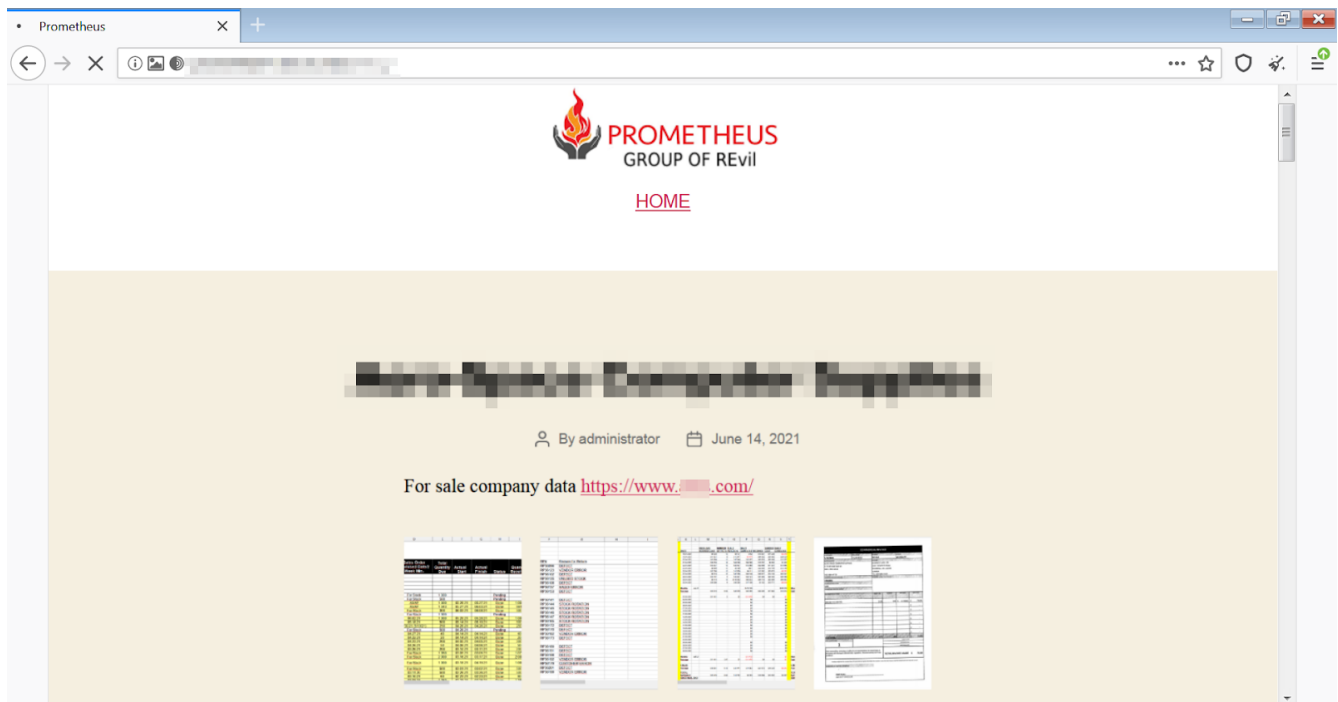
Group of REvil?

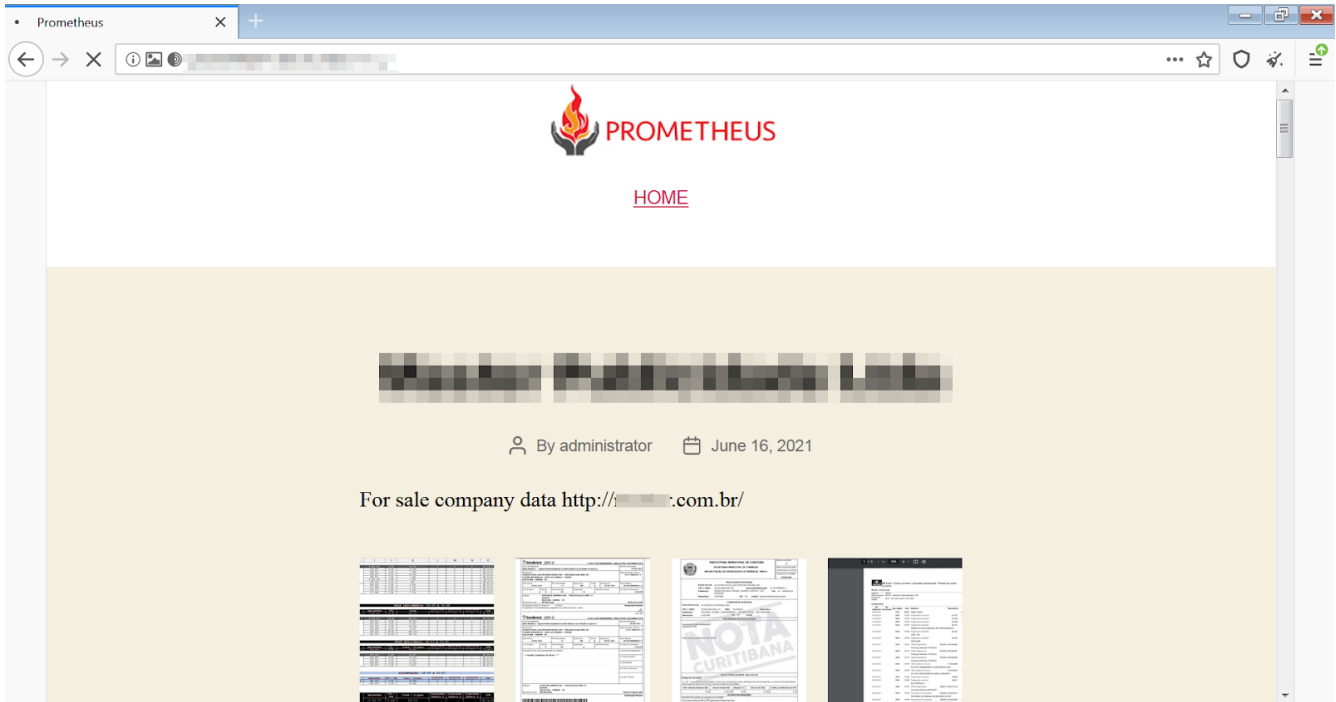
Up until June 14th, the operators of [Prometheus claimed to be part of the notorious REvil ransomware group](#), and even mentioned them in their logo. On June 15th, the group decided to delete the name of REvil from their logo, and remove any potential relation to the group.

It is worth noting that there hasn't been strong or conclusive evidence of a real connection or collaboration between the two groups and the assumption is that the Prometheus group was most likely just using the name and reputation of REvil to increase the likelihood of ransom payments.

Although it is unclear why the group has decided to remove the name of REvil from their logo, it's interesting to look at the timing. The REvil group was just attributed to another major attack infecting potentially thousands of companies by way of an exploit against Kaseya VSA remote management service which propagated ransomware through the IT service provider's Managed Services Provider network, and a recent attack against the global food company JBS which drew attention to them from the US authorities.

In May, it was the DarkSide group that made big headlines after attacking the Colonial Pipeline network, which caused the US authorities to take actions that eventually led to the DarkSide group shutting down their operations (allegedly). Ransomware operators will usually try to evade such unwanted publicity because of their fear of retaliation from law enforcement agencies.

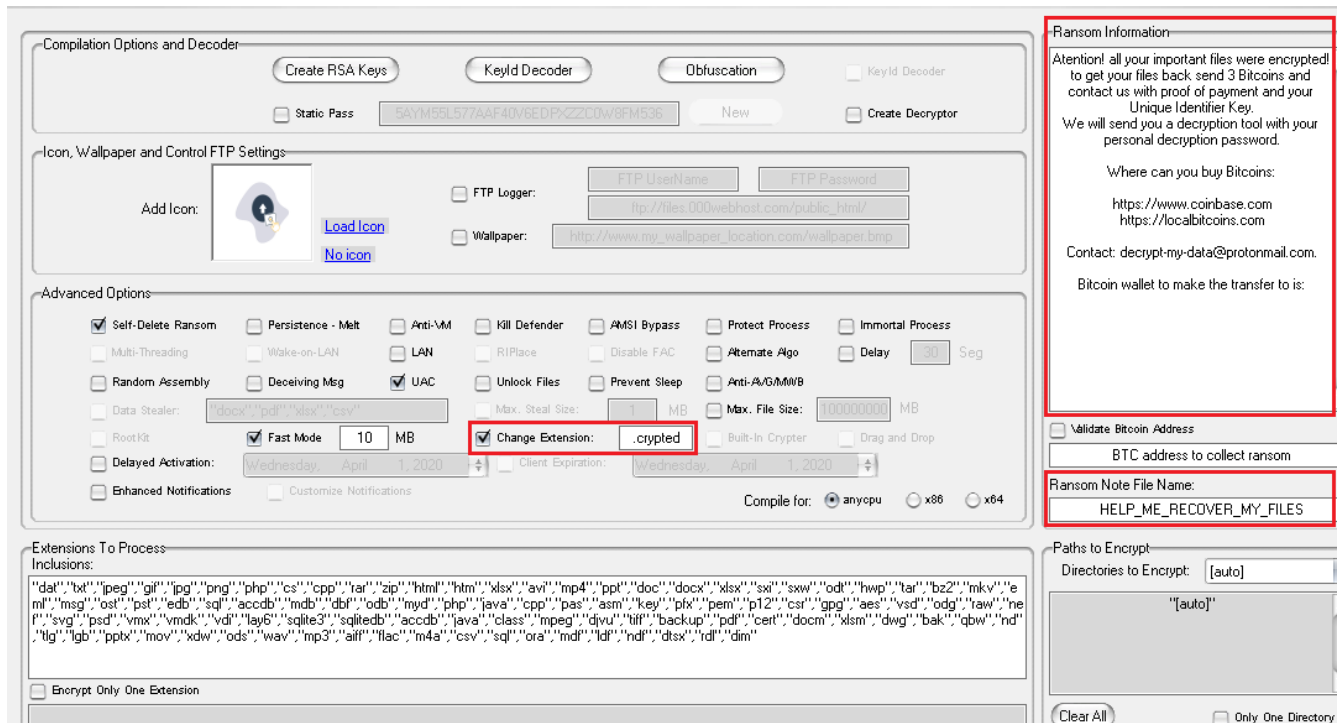




Screenshots from the Prometheus leaks website

From one Builder to Multiple Ransomware

As mentioned in the beginning of this blog post, Prometheus is not an entirely new ransomware. It is a variant of the Thanos ransomware, which has been sold in underground forums since late 2019. The group behind Prometheus, as well as other threat actors, bought Thanos and used the builder that comes with it to customize their ransomware:



The builder used to configure Thanos. Credit: [Recorded Future](#)

Most of the distinguishing changes observed include the extension that is added to the encrypted files and of course the ransom note content. Because of that, there are different variants of the Thanos ransomware out there, with most of them named after the extension that is appended to the encrypted files.

The following table presents some of the variants found in the wild:

Ransomware Name	Ransom note	Extension
Thanos	RESTORE_FILES_INFO.txt	.crypted random string
Hakbit	HOW_TO_RECOVER_YOUR_FILES.txt	.[ID-30BC8771]. [black_private@tuta.io].CRYSTAL .VIPxxx
Abarcy	Abarcy#2996.txt	.abarcy
Hard	RESTORE_FILES_INFO.txt	.hard
Milleni5000	RESTORE_FILES_INFO.txt	.secure
Ravack	HELP_ME_RECOVER_MY_FILES.txt	.ravack
Energy	HOW_TO_DECYPHER_FILES.txt	.energy[potentialenergy@mail.ru]
Alumni	HOW_TO_RECOVER_YOUR_FILES.txt	.alumni
Prometheus	RESTORE_FILES_INFO.txt	.[XXX-XXX-XXXX] format (unique per victim) .PROM[prometheushelp@mail[.]ch] XXXXXXXXXX[prometheusdec@yahoo[.]com] (unique per victim)

Prometheus Ransomware Analysis

The binary generated by the builder is an obfuscated .NET executable that consists of a main function that is responsible to decode base64 strings in memory and pass them to the other functions.

Among the functionality observed by the malware is the ability to enumerate processes and manipulate with them, changing registry keys, setting persistence, downloading additional files, collecting information about the machine and more:



The execution of the ransomware as shown in the Cyberreason Defense Platform

Setting Persistence

Prometheus creates persistence by copying the file into the startup folder of the user. This ensures that the malware will continue to run after logoff-login of the user:

Value	Type
@ "C:\Users\... \AppData\Roaming\Microsoft\Windows\Start Men...	string
{string[0x00000000]}	string[]
{ov @ "C:\Users\... \AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\"	string
{System.Diagnostics.ProcessModule (Prometheus-cleaned.exe)}	System.Diagnostics.Proce...
@ "C:\Users\... \Desktop\Prometheus-cleaned.exe"	string

Adding the ransomware binary to the startup folder

Ensuring Successful File Encryption

Upon execution, Prometheus performs a series of tasks to ensure that it will run smoothly without interference.

These tasks include stopping common security tools and backup related processes, interacting with the registry and scheduled task, deleting files, and interacting with services.

Deleting Raccine:

Raccine is a ransomware prevention tool that tries to stop ransomware from deleting shadow copies in Windows. Prometheus deletes the scheduled task and the registry keys of the software:

```
reg delete "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Raccine Tray" /F
```

```
reg delete HKCU\Software\Raccine /F
```

```
schtasks /DELETE /TN "Raccine Rules Updater" /F
```

Value	Type
"reg"	string
@"delete ""HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"...	string
@"delete ""HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"" /V ""Raccine Tray"" /F"	

Value	Value
{System.Text.SBCSCodePageEncoding}	"taskkill"
"schtasks"	"/F /IM RaccineSettings.exe"
"/DELETE /TN \"Raccine Rules Updater\" /F"	null

Deleting Raccine: deleting the registry key and scheduled task and killing the process

Stopping Processes:

Prometheus stops different processes that may interfere with its execution, and also to free DB related files for encryption:

```

taskkill.exe /IM sqlagent.exe /F
taskkill.exe /IM steam.exe /F
taskkill.exe /IM Ntrtscan.exe /F
taskkill.exe /IM msftesql.exe /F
taskkill.exe /IM tmlisten.exe /F
taskkill.exe /IM dbeng50.exe /F
taskkill.exe /IM mbamtray.exe /F
taskkill.exe /IM firefoxconfig.exe /F
taskkill.exe /IM mydesktopservice.exe /F
taskkill.exe /IM synctime.exe /F
taskkill.exe /IM agntsvc.exe /F
taskkill.exe /IM mysqld-opt.exe /F

taskkill.exe /IM mspub.exe /F
taskkill.exe /IM PccNTMon.exe /F
taskkill.exe /IM sqbcoreservice.exe /F
taskkill.exe /IM visio.exe /F
taskkill.exe /IM encsvc.exe /F
taskkill.exe /IM thebat64.exe /F
taskkill.exe /IM outlook.exe /F
taskkill.exe /IM mydesktoppqos.exe /F
taskkill.exe /IM msaccess.exe /F
taskkill.exe /IM excel.exe /F
taskkill.exe /IM isqlplussvc.exe /F

taskkill.exe /IM ocomm.exe /F
taskkill.exe /IM CNTAoSMgr.exe /F
taskkill.exe /IM onenote.exe /F
taskkill.exe /IM thebat.exe /F
taskkill.exe /F /IM RaccineSettings.exe
taskkill.exe /IM sqlwriter.exe /F
taskkill.exe /IM wordpad.exe /F
taskkill.exe /IM dbsnmp.exe /F
taskkill.exe /IM xfssvcon.exe /F
taskkill.exe /IM powerpnt.exe /F
taskkill.exe /IM mysqld.exe /F

taskkill.exe /IM tbirdconfig.exe /F

```

Locals	
Name	Value
ovnaSovhORzB.EEGkMyyVIDL.DRIXtEGdcAr returned	"firefox.exe"
SmartAssembly.Delegates.GetString.Invoke returned	"Y2FsYy5leGU="
ovnaSovhORzB.EEGkMyyVIDL.DRIXtEGdcAr returned	"calc.exe"
SmartAssembly.Delegates.GetString.Invoke returned	"bXlzcWxkLmV4ZQ=="
ovnaSovhORzB.EEGkMyyVIDL.DRIXtEGdcAr returned	"mysqld.exe"
SmartAssembly.Delegates.GetString.Invoke returned	"ZGxsaHN0LmV4ZQ=="
ovnaSovhORzB.EEGkMyyVIDL.DRIXtEGdcAr returned	"dllhst.exe"
SmartAssembly.Delegates.GetString.Invoke returned	"b3BlcmEzMi5leGU="
ovnaSovhORzB.EEGkMyyVIDL.DRIXtEGdcAr returned	"opera32.exe"
SmartAssembly.Delegates.GetString.Invoke returned	"bWVtb3AuZXhl"
ovnaSovhORzB.EEGkMyyVIDL.DRIXtEGdcAr returned	"memop.exe"
SmartAssembly.Delegates.GetString.Invoke returned	"c3Bvb2xjdj5leGU="
ovnaSovhORzB.EEGkMyyVIDL.DRIXtEGdcAr returned	"spoolcv.exe"
SmartAssembly.Delegates.GetString.Invoke returned	"Y3RmbW9tLmV4ZQ=="
ovnaSovhORzB.EEGkMyyVIDL.DRIXtEGdcAr returned	"ctfmom.exe"
SmartAssembly.Delegates.GetString.Invoke returned	"U2t5cGVBCHAuZXhl"
ovnaSovhORzB.EEGkMyyVIDL.DRIXtEGdcAr returned	"SkypeApp.exe"

Process enumeration

Stopping Services:

Prometheus stops different services that may interfere with it's execution, and also to free DB related files for encryption:

net.exe start Dnscache /y	net.exe stop MSSQLFDLauncher\$PROFXENGAGEMENT /y	net.exe stop VeeamTransportSvc /y
net.exe start FDResPub /y		
net.exe start SSDPSRV /y	net.exe stop MSSQLFDLauncher\$SBSMONITORING /y	net.exe stop VeeamTransportSvc /y
net.exe start upnphost /y		net.exe stop W3Svc /y
net.exe stop BMR Boot Service /y	net.exe stop MSSQLFDLauncher\$SHAREPOINT /y	net.exe stop YooBackup /y
net.exe stop BackupExecAgentAccelerator /y	net.exe stop MSSQLFDLauncher\$SQL_2008 /y	net.exe stop YooIT /y
net.exe stop BackupExecAgentBrowser /y	net.exe stop MSSQLFDLauncher\$SYSTEM_BGC /y	net.exe stop avpsus /y
net.exe stop BackupExecDiveciMediaService /y	net.exe stop MSSQLSERVER /y	net.exe stop bedbg /y
net.exe stop BackupExecJobEngine /y	net.exe stop MSSQLServerOLAPService /y	net.exe stop ccEvtMgr /y
net.exe stop BackupExecVSSProvider /y	net.exe stop McAfeeDLPAgentService /y	net.exe stop ccSetMgr /y
net.exe stop CAARCUpdateSvc /y	net.exe stop McAfeeFrameworkMcAfeeFramework /y	net.exe stop ekrn /y
net.exe stop DefWatch /y	net.exe stop MsDtsServer100 /y	net.exe stop kavfssl /y
net.exe stop EPSecurityService /y	net.exe stop MySQL80 /y	net.exe stop klnagent /y
net.exe stop EPUUpdateService /y	net.exe stop NetBackup BMR MTFTP Service /y	net.exe stop macmnsvc /y
net.exe stop ESHASRV /y	net.exe stop PDVFSService /y	net.exe stop mfemms /y
net.exe stop EhttpSrv /y	net.exe stop PDVFSService /y	net.exe stop mfewc /y
net.exe stop EsgShKernel /y	net.exe stop POP3Svc /y	net.exe stop mozyprobackup /y
net.exe stop FA_Scheduler /y	net.exe stop QBCFMonitorService /y	net.exe stop ntrtscan /y
net.exe stop Intuit.QuickBooks.FCS /y	net.exe stop QBFCService /y	net.exe stop sophos /y
net.exe stop KAVFS /y	net.exe stop QBIDPService /y	net.exe stop stc_raw_agent /y
net.exe stop KAVFSGT /y	net.exe stop RTVscan /y	net.exe stop veeam /y
net.exe stop MBEndpointAgent /y	net.exe stop ReportServer /y	net.exe stop zhudongfangyu /y
net.exe stop MMS /y	net.exe stop ReportServer\$SQL_2008 /y	net.exe stop "Acronis VSS Provider" /y
net.exe stop MExchangeIS /y	net.exe stop SDRSVC /y	net.exe stop "Enterprise Client Service" /y
	net.exe stop SMTPSvc /y	net.exe stop "SQL Backups" /y
	net.exe stop SQLAgent\$VEEAMSQL2008R2 /y	net.exe stop "Sophos AutoUpdate Service" /y

net.exe stop MSExchangeMGMT /y	net.exe stop SQLWriter /y	net.exe stop "Sophos Clean Service" /y
net.exe stop MSSQL\$SQLEXPRESS /y	net.exe stop SamSs /y	net.exe stop "Sophos Device Control Service" /y
net.exe stop MSSQL\$SQL_2008 /y	net.exe stop SavRoam /y	net.exe stop "Symantec System Recovery" /y
net.exe stop MSSQL\$SYSTEM_BGC /y		net.exe stop VeeamBackupSvc /y
net.exe stop MSSQL\$TPS /y		net.exe stop VeeamBrokerSvc /y
net.exe stop MSSQL\$TPSAMA /y		net.exe stop VeeamCloudSvc /y
net.exe stop MSSQL\$VEEAMSQL2008R2 /y		net.exe stop VeeamDeploySvc /y
net.exe stop MSSQL\$VEEAMSQL2008R2 /y		net.exe stop VeeamDeploymentService /y
net.exe stop MSSQL\$VEEAMSQL2012 /y		net.exe stop VeeamMountSvc /y
		net.exe stop VeeamNFSSvc /y
		net.exe stop SstpSvc /y
		net.exe stop VSNAPVSS /y

Deleting Shadow Copies

Like other ransomware, Prometheus deletes the shadow copies to prevent restoring backups of the machine after encrypting files. To do so, it runs the following PowerShell command:

```
"powershell.exe" & Get-WmiObject Win32_Shadowcopy | ForEach-Object { $_.Delete(); }
```

Configuring Services

<i>sc.exe config SSDPSRV start= auto</i>	Enables discovery of UPnP devices on your home network
<i>sc.exe config Dnscache start= auto</i>	Caches DNS names and registers the full computer name for your computer
<i>sc.exe config upnphost start= auto</i>	Allows UPnP devices to be hosted on your computer
<i>sc.exe config FDResPub start= auto</i>	Publishes your computer and resources attached to your computer so they can be discovered over the network

<code>sc.exe config SQLTELEMETRY\$ECWDB2 start=disabled</code>	SQL service, disabled to prevent backup and unlocking files
<code>sc.exe config SQLTELEMETRY start=disabled</code>	SQL service, disabled to prevent backup and unlocking files
<code>sc.exe config SQLWriter start=disabled</code>	SQL service, disabled to prevent backup and unlocking files
<code>sc.exe config SstpSvc start=disabled</code>	Prevent users from being able to use SSTP (Secure Socket Tunneling Protocol) to access remote servers

Spreading Across The Network

Once successfully executed, Prometheus will try to spread in the network using different methods. First, it will “prepare the ground” by performing some reconnaissance commands that include running “Net view” and “arp -a”, followed by a ping sweep to check the connections and potential machines to infect.

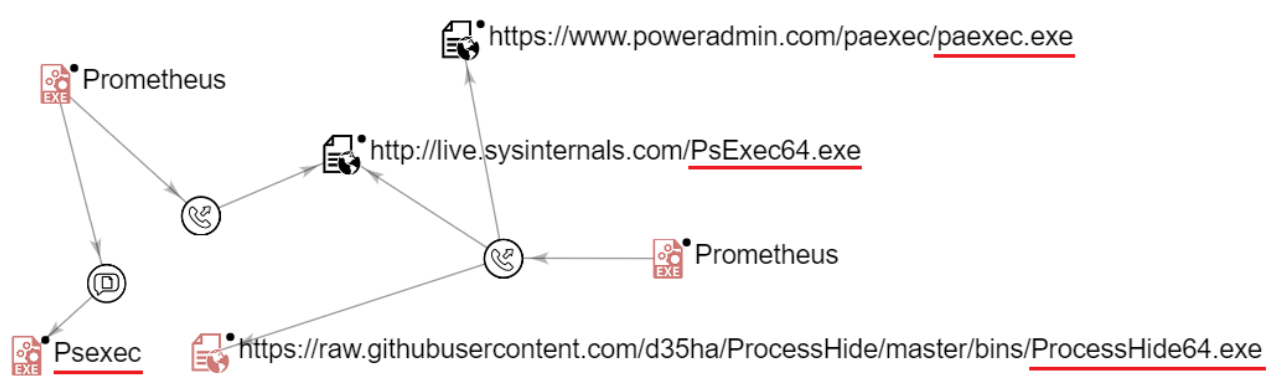
Then it continues with changing local firewall rules, downloading [Psexec/Paexec](#) and in some cases [ProcessHider](#) as well, and enabling SMB1 protocol - most likely to exploit a vulnerability for spreading using SMB, much like as [EternalBlue](#):

```
netsh advfirewall firewall set rule group="Network Discovery" new enable=Yes
```

```
netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes
```

```
powershell.exe & Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

After that, the malware begins the spreading process. Initially it will try an easy way using the “Net use” command to try to copy itself into shared folders. Then it will run PsExec/PaExec remotely to execute the binary. On other occasions it will try to exploit a SMB vulnerability to spread:



A VirusTotal graph showing the connection between Prometheus binaries and Psexec, Paexec and ProcessHider

Encrypting The Files

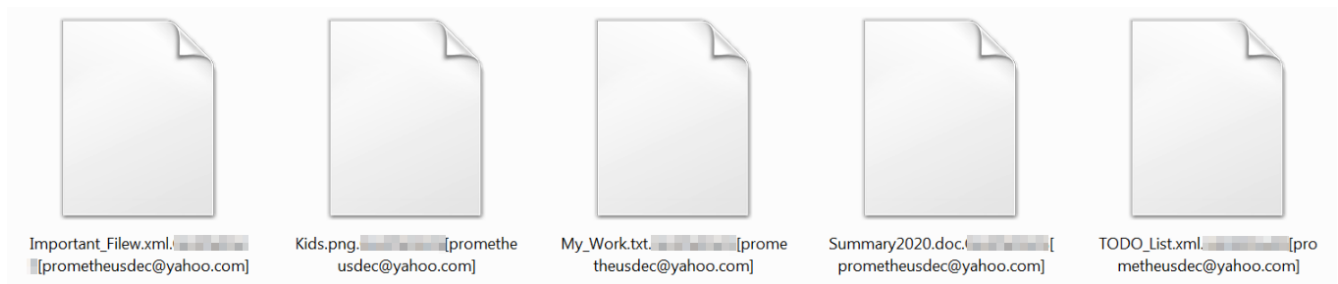
After ensuring successful execution of the malware and deleting backup files, Prometheus begins its encryption routine. First, it will search for files matching extensions that were passed in build time. Those extensions vary from Microsoft Office files, images, scripts, archives, music, videos, and different database files:

	Value	Type
return...	"\db\","dbf","accdb","\dbx","\mdb","\mdf","epf","\ndf","\ldf",...	string
	"\db\","dbf","accdb","\dbx","\mdb","\mdf","epf","\ndf","\ldf","\1cd","\sdf","\nsf","\fp7","\cat","\log"	

Searching for DB files

The builder also supports a “fast mode” of encryption where only a portion of each file is encrypted. When this mode is enabled during build time, the ransomware encrypts a preconfigured amount of data from each file and overwrites the file with the encrypted content. This technique saves Prometheus time and shortens the entire encryption time, which can take just seconds up to a few minutes, depending on the number of files on the targeted machine.


Prometheus appends a custom extension that is unique for every executable and in some variants even contains the name of the victim:



Custom extension appended to the encrypted files

Finally, Prometheus drops a ransom note in .hta and text format, and presents the .hta file to the end user:

C:\Users\ Desktop\RESTORE_FILES_INFO.hta



YOUR COMPANY NETWORK HAS BEEN HACKED

All your important files have been encrypted!

Your files are safe! Only modified.(AES)
No software available on internet can help you.
We are the only ones able to decrypt your files.

[We also gathered highly confidential/personal data.](#)
[These data are currently stored on a private server.](#)
[Files are also encrypted and stored securely.](#)


As a result of working with us, you will receive:

- Fully automatic decryptor, all your data will be recovered within a few hours after itd€™s installation.
 - Server with your data will be immediately destroyed after your payment.
 - Save time and continue working.

You will can send us 2-3 non-important files and we will decrypt it for free to prove we are able to give your files back.

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 O](#)
[So you can expect your data to be publicly available in the near future..](#)
 - [The price will increase over time.](#)



YOUR COMPANY NETWORK HAS BEEN HACKED
 All your important files have been encrypted!
 Your files are safe! Only modified. (AES)
 Codemeter

.hta file ransom note

RESTORE_FILES_INFO - Notepad

File Edit Format View Help

!!! 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 purch
 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 INTERNE

We recommend you upload 3 encrypted files in <https://privatlab.com/file> and paste link to y
 * 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>
 c) Register account
 d) Click Compose and write to us, our username: Prometheus, in message write Your key iden

2) Using a email
 Write to 3 emails address at once, in message write Your key identifier (it is at the end o
prometheusdec@yahoo.com

.txt file ransom note

Cybereason Detection and Prevention

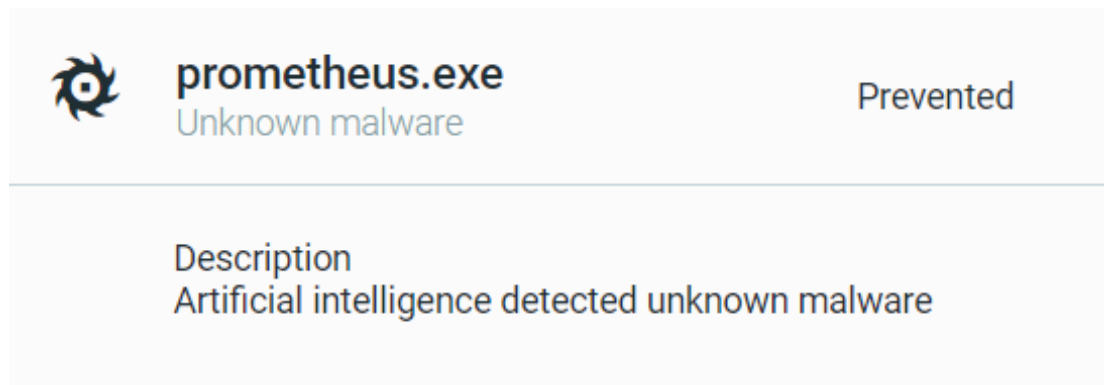
Ransomware attacks are on the rise. A recently released report by Cybereason, titled *Ransomware: The True Cost to Business*, detailed how malicious actors are fine-tuning their ransomware campaign tactics and how both the frequency and severity of successful ransomware attacks have tremendous impact on victim organizations and their ability to conduct business.

The Cybereason Defense Platform is able to prevent the execution of the Prometheus Ransomware using multi-layer protection that detects and blocks ransomware with threat intelligence, machine learning, and next-gen antivirus (NGAV) capabilities. Additionally, when the Anti-Ransomware feature is enabled, behavioral detection techniques in the platform are able to detect and prevent any attempt to encrypt files and automatically generates a Malop™ for it with the complete attack narrative:

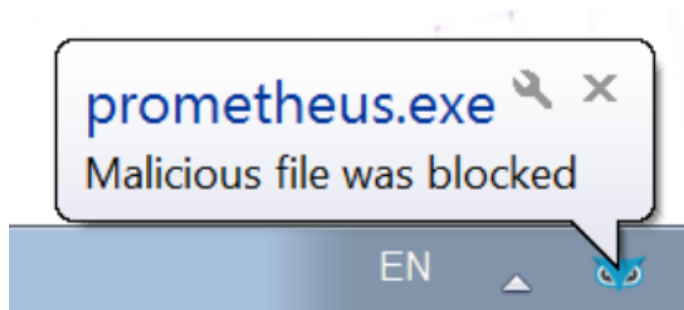


Malop for Prometheus ransomware as shown in the Cybereason Defense Platform

Using the Anti-Malware feature with the right configurations (listed in the recommendations below), the Cybereason Defense Platform will also detect and prevent the execution of the ransomware and ensure that it cannot encrypt targeted files. The prevention is based on machine learning, which blocks both known and unknown malware variants:



Prevention alert of the Prometheus ransomware as shown in the Cybereason Defense Platform



Cybereason user notification for preventing the execution of Prometheus

Security Recommendations

- **Enable the Anti-Ransomware Feature on Cybereason NGAV:** Set Cybereason Anti-Ransomware protection mode to *Prevent* - [more information for customers can be found here](#)

- **Enable Anti-Malware Feature on Cybereason NGAV:** Set Cybereason Anti-Malware mode to *Prevent* and set the detection mode to *Moderate* and above - [more information for customers can be found here](#)
- **Keep Systems Fully Patched:** Make sure your systems are patched in order to mitigate vulnerabilities
- **Regularly Backup Files to a Remote Server:** Restoring your files from a backup is the fastest way to regain access to your data
- **Use Security Solutions:** Protect your environment using organizational firewalls, proxies, web filtering, and mail filtering

Cybereason is dedicated to teaming with defenders to end cyber attacks from endpoints to the enterprise to everywhere - including modern ransomware. [Learn more about ransomware defense here](#) or [schedule a demo today](#) to learn how your organization can benefit from an [operation-centric approach](#) to security.

LIOR ROCHBERGER, SENIOR THREAT RESEARCHER AND THREAT HUNTER, CYBEREASON



As part of the Nocturnus team at Cybereason, Lior has created procedures to lead

threat hunting, reverse engineering and malware analysis teams. Lior has also been a contributing researcher to multiple threat and malware blogs including Bitbucket, Valak, Ramnit, and Racoon stealer. Prior to Cybereason, Lior led SOC operations within the Israeli Air Force.



About the Author

Cybereason Nocturnus



The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system

vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

[All Posts by Cybereason Nocturnus](#)