Threat spotlight: Phobos ransomware lives up to its name

blog.malwarebytes.com/threat-spotlight/2020/01/threat-spotlight-phobos-ransomware-lives-up-to-its-name/

Jovi Umawing January 10, 2020

Ransomware has struck dead on organizations since it became a mainstream tool in cybercriminals' belts years ago. From massive WannaCry outbreaks in 2017 to industry-focused attacks by Ryuk in 2019, ransomware's got its hooks in global businesses and shows no signs of stopping. That includes a malware family known as Phobos ransomware, named after the Greek god of fear.

Phobos is another one of those ransomware families that primarily targets organizations by employing tried-and-tested tactics to infiltrate systems. While this ransomware may have been coined with different aliases, many consider it an off-shoot or variant—if not a rip-off—of the Dharma ransomware family, which is also called CrySis. This is attributed to Phobos' operational and technical likeness to recent Dharma strains.

Phobos ransomware, like Sodinokibi, is sold in the underground in ransomware-as-a-service (RaaS) packages. This means that criminals with little to no technical know-how can create their own ransomware strain with the help of a kit, and organize a campaign against their desired targets.

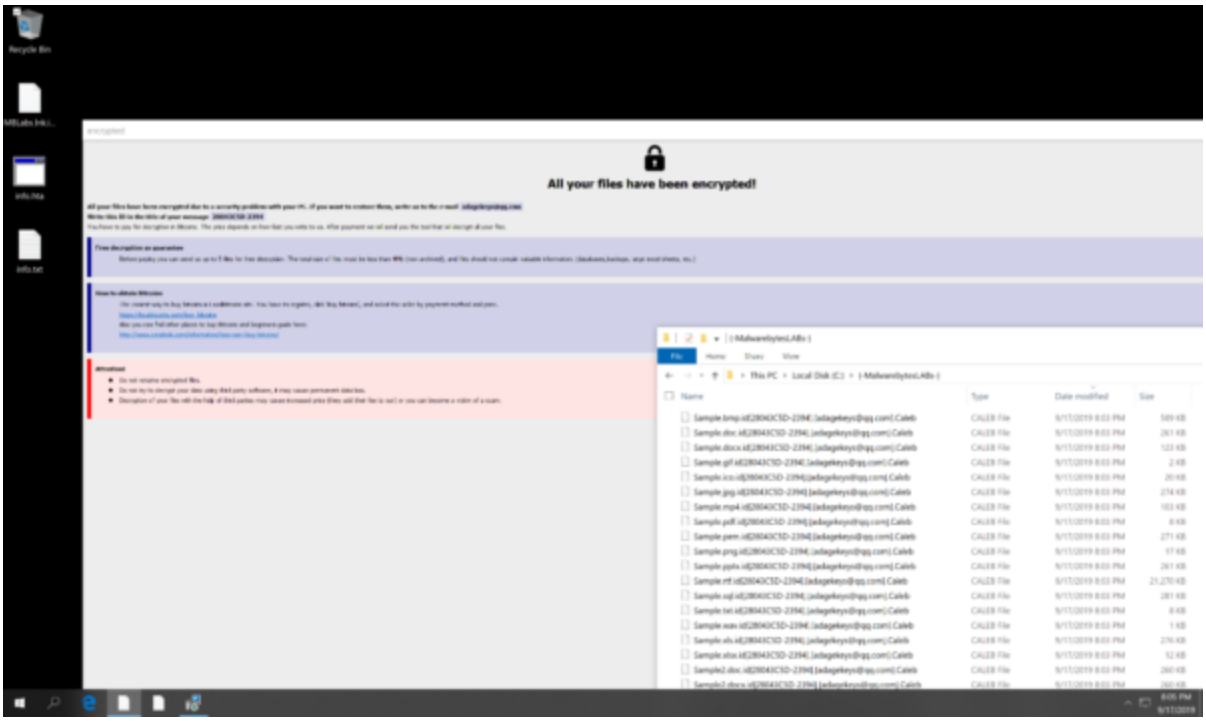
However, Coveware researchers have noted that, compared to their peers, Phobos operators are "less organized and professional," which has eventually led to extended ransom negotiations and more complications retrieving files and systems for Phobos ransomware victims during the decryption process.

Phobos ransomware infection vectors

Phobos can arrive on systems in several ways: via open or insecure remote desktop protocol (RDP) connections on port 3389, brute-forced RDP credentials, the use of stolen and bought RDP credentials, and old-fashion phishing. Phobos operators can also leverage malicious attachments, downloads, patch exploits, and software vulnerabilities to gain access to an organization's endpoints and network.

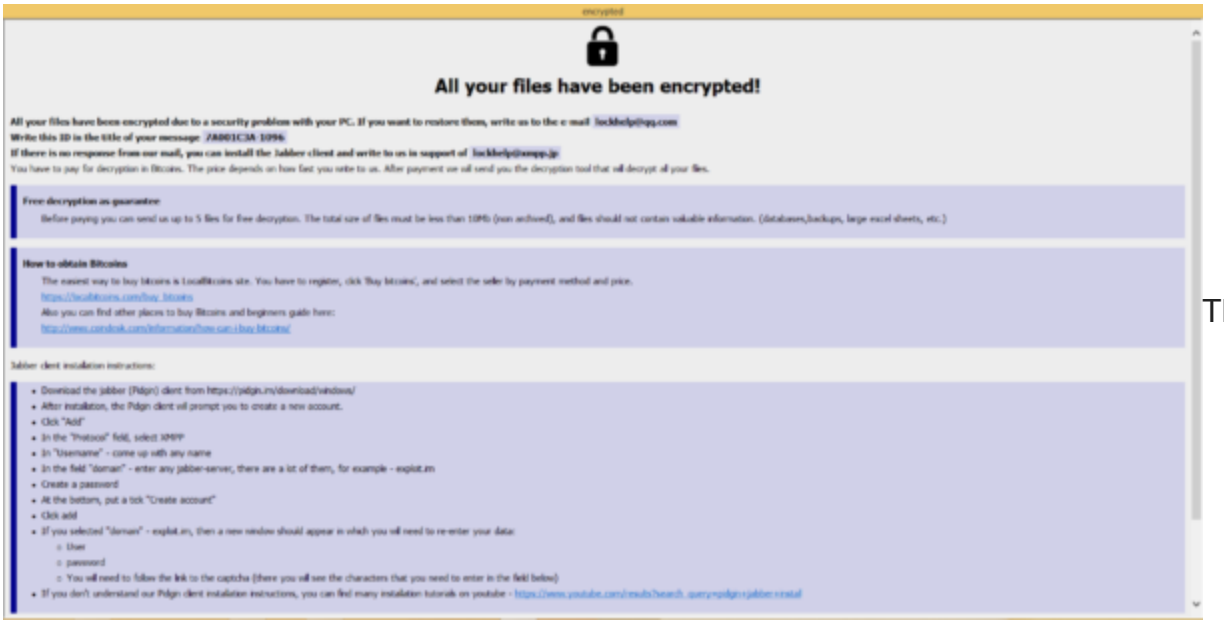
Phobos ransomware primarily targets businesses; however, there have been several reports of consumers finding themselves face-to-face with this adversary, too.

Symptoms of Phobos ransomware infection



Systems affected by variants of the Phobos ransomware display the following symptoms:

Presence of ransom notes. Upon infection, Phobos drops two ransom notes in text (.TXT) and in executable web file (.HTA) format. The latter automatically opens after Phobos finishes encrypting files.



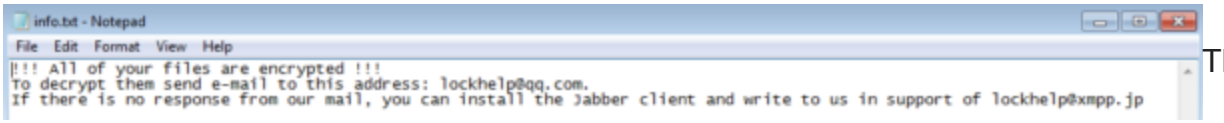
The HTA ransom note, which was noted to be a re-branded version of Dharma's ransom note Here's a snippet of the note:

> All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail [email address 1]
>
> Write this ID in the title of your message [generated ID]
>
> If there is no response from our mail, you can install the Jabber client and write to us in support of [email address 2]
>
> You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

As you can see, Phobos operators are requiring victims to contact them in the event of their ransomware infection.

In some notes from other variants, instructions to reach threat actors via Jabber are not included.

Aside from pertinent channels victims can reach the threat actors, this ransom note also contains information on how they can acquire Bitcoins and how to install the messenger client.



The TXT ransom note, which is notably shorter than its HTA counterpart. This means that non-tech savvy victims would have to resort to doing their own research to understand unfamiliar terms. Note that while this contains the email addresses also found in the HTA file, it doesn't contain the generated ID.

> !!! All of your files are encrypted !!!
>
> To decrypt them send e-mail, to this address: [email address 1]
>
> If there is no response from our mail, you can install the Jabber client and write to us in support of [email address 2]

After triggering the opening of the HTA ransom note, which supposedly signifies the end of Phobos' encryption, we have observed that it is an aggressive ransomware that continues to run in the background and encode new files it is programmed to encrypt. It can do this with or without an Internet connection.

Encrypted files with a long, appended string after the extension name. Phobos encrypts target files using AES-256 with RSA-1024 asymmetric encryption. Both Phobos and Dharma implement the same RSA algorithm; however, Phobos uses it from Windows Crypto API

while Dharma uses it from a third-party static library. Upon encryption, it appends a compound extension name at the end of encrypted files. This implements the format or formula:

```
.ID[ID][email address 1].[added extension]
```

In the formula, **[ID]** is the generated ID number specified in the ransom note. It is a two-part alpha-numeric string: the victim ID and the version ID, separated by a dash. **[email address 1]** is the email address victims are prescribed to use in reaching out to the threat actors. This is also specified in the ransom note. Lastly, **[added extension]** is an extension that Phobos threat actors decide to associate their ransomware with. Below are known extensions Phobos uses:

- 1500dollars
- actin
- Acton
- actor
- Acuff
- Acuna
- acute
- adage
- Adair
- Adame
- banhu
- banjo
- Banks
- Banta
- Barak
- bbc
- blend
- BORISHORSE
- bqux
- Caleb
- Cales
- Caley
- calix
- Calle
- Calum
- Calvo
- CAPITAL
- com
- DDoS
- deal

- deuce
- Dever
- devil
- Devoe
- Devon
- Devos
- dewar
- eight
- eject
- eking
- Elbie
- elbow
- elder
- Frendi
- help
- KARLOS
- karma
- mamba
- phobos
- phoenix
- PLUT
- WALLET
- zax

For example, the new file name of *sample.bmp* after encryption is *sample.bmp.id[23043C5D-2394].[agagekeys@qq.com].Caleb*.

Phobos encrypts files with the following extensions:

```
1cd 3ds 3fr 3g2 3gp 7z accda accdb accdc accde accdt accdw adb adp ai ai3 ai4 ai5
ai6 ai7 ai8 anim arw as asa asc ascx asm asmx asp aspx asr asx avi avs backup bak
bay bd bin bmp bz2 c cdr cer cf cfc cfm cfml cfu chm cin class clx config cpp cr2
crt crw cs css csv cub dae dat db dbf dbx dc3 dcm dcr der dib dic dif divx djvu dng
doc docm docx dot dotm dotx dpx dqy dsn dt dtd dwg dwt dx dxf edml efd elf emf emz
epf eps epsf epsp erf exr f4v fido flm flv frm fxg geo gif grs gz h hdr hpp hta htc
htm html icb ics iff inc indd ini iqy j2c j2k java jp2 jpc jpe jpeg jpf jpg jpx js
jsf json jsp kdc kmz kwm lasso lbi lgf lgp log m1v m4a m4v max md mda mdb mde mdf
mdw mef mft mfw mht mhtml mka mkidx mkv mos mov mp3 mp4 mpeg mpg mpv mrw msg mxl
myd myi nef nrw obj odb odc odm odp ods oft one onepkg onetoc2 opt oqy orf p12 p7b
p7c pam pbm pct pcx pdd pdf pdp pef pem pff pfm pfx pgm php php3 php4 php5 phtml
pict pl pls pm png pnm pot potm potx ppa ppam ppm pps ppsm ppt pptm pptx prn ps psb
psd pst ptx pub pwm pxr py qt r3d raf rar raw rdf rgbe rle rqy rss rtf rw2 rwl safe
sct sdpx shtm shtml slk sln sql sr2 srf srw ssi st stm svg svgz swf tab tar tbb tbi
tbk tdi tga thmx tif tiff tld torrent tpl txt u3d udl uxdc vb vbs vcs vda vdr vdw
vdx vrp vsd vss vst vsw vsx vtm vtml vtx wb2 wav wbm wbmp wim wmf wml wmv wpd wps
x3f xl xla xlam xlk xlm xls xlsb xlsm xlsx xlt xltm xltx xlw xml xps xsd xsf xsl
xslt xsn xtp xtp2 xyze xz zip
```

However, it skips encoding the following OS files and files in the *C:\Windows* folder:

- boot.ini
- bootfont.bin
- ntldr
- ntdetect.com
- io.sys

Phobos fully encodes files with sizes that can be classed as typical. For large files, however, it performs a different algorithm wherein it partially encrypts selected portions of such files. This is an effective method to severely cut down the time it takes to encrypt large files and, at the same time, maximize the damage it could do to such a file if something goes wrong with its decryption.

This ransomware attacks files in all local drives as well as network shares.

Terminated processes. Phobos ransomware is known to terminate the following active processes on affected systems so that no programs can stop it from accessing files to eventually encrypt:

```
msftesql.exe sqlagent.exe sqlbrowser.exe sqlservr.exe sqlwriter.exe
oracle.exe ocssd.exe dbsnmp.exe synctime.exe agntsvc.exe
mydesktopqos.exe isqlplussvc.exe xfssvccon.exe mydesktopservice.exe
ocautoupds.exe agntsvc.exe agntsvc.exe agntsvc.exe encsvc.exe
firefoxconfig.exe tbirdconfig.exe ocomm.exe mysqld.exe mysqld-nt.exe
mysqld-opt.exe dbeng50.exe sqbcoreservice.exe excel.exe infopath.exe
msaccess.exe mspub.exe onenote.exe outlook.exe powerpnt.exe steam.exe
thebat.exe thebat64.exe thunderbird.exe visio.exe winword.exe
wordpad.exe
```

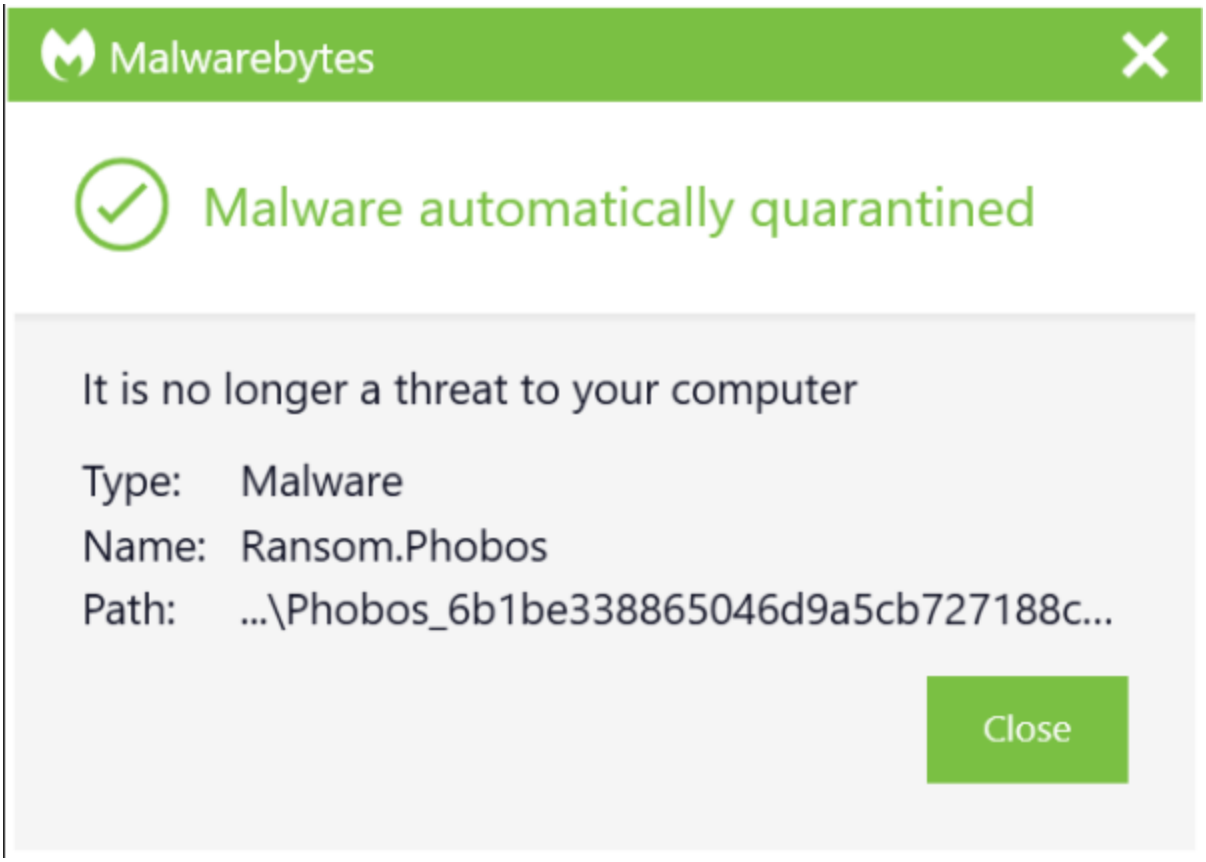
Deleted shadow copies and local backups. Like Sodinokibi and other ransomware families, Phobos deletes shadow copies and backup copies of files to prevent users from restoring encrypted files, thus, forcing them to do the threat actors' bidding.

Systems not booting in recovery mode. Recovery mode is innate in Windows systems. If users encounter a technical flaw leading to the system crashing or getting corrupted, they have the option to restore the OS to its normal state by reloading its last known state before the flaw. Phobos removes this option by preventing users from entering this mode.

Disabled firewall. As we already know, malware that firewalls stop could be allowed into the affected system.

Protect your system from Phobos ransomware

Malwarebytes' signature-less detection, coupled with real-time anti-malware and anti-ransomware technology, identifies and protects consumer and business users from Phobos ransomware in various stages of attack.



We recommend both consumers and IT administrators take the following actions to secure and mitigate against Phobos ransomware attacks:

- Set your RDP server, which is built in in the Windows OS, to deny public IPs access to TCP port 3389, the default port Windows Remote Desktop listens on. If you or your organizations have no need for RDP, better to disable the service altogether. Critical systems or systems with sensitive information should not have RDP enabled.
- Along with RDP port blocking, we also suggest the blocking of TCP port 445, the default port a Server Message Block (SMB) uses to communicate in a Windows-based LAN at the network perimeter. Note that you or your organization may have to do in-depth testing to see how your system and/or programs are impacted by this block. As a rule of thumb, block all unused ports.
- Allow RDP access to IPs that are under you or your organization's control.
- Enable the logging of RDP access attempts and review them regularly to detect instances of potential intrusion.
- Enforce the use of strong passwords and account lockout policies for Active Directory domains and local Windows accounts.
- Enforce multi-factor authentication (MFA) to RDP and local account logons whenever possible.
- Enforce the use of a virtual private networks (VPNs) if your organization allows employees to work remotely.
- Come up with and implement a sound backup strategy.

- Maintain an inventory of running services and applications on your system, and review it regularly. For critical systems, it's best to have an active monitoring and alerting scheme in place.
- Have a disaster recovery scheme in place in case of a successful breach via RDP happens.
- Keep all your software, including OS and anti-malware, up-to-date.

On a final note, if you have all your personal or organization resources properly locked down and secured, and you or your organization adhere to good cyber hygiene practices, there is little to be feared about Phobos or any ransomware in general.

Indicators of Compromise (IOCs)

- e59ffeaf7acb0c326e452fa30bb71a36
- eb5d46bf72a013bfc7c018169eb1739b
- fa4c9359487bbda57e0df32a40f14bcd

Have a threat-free 2020, everyone!