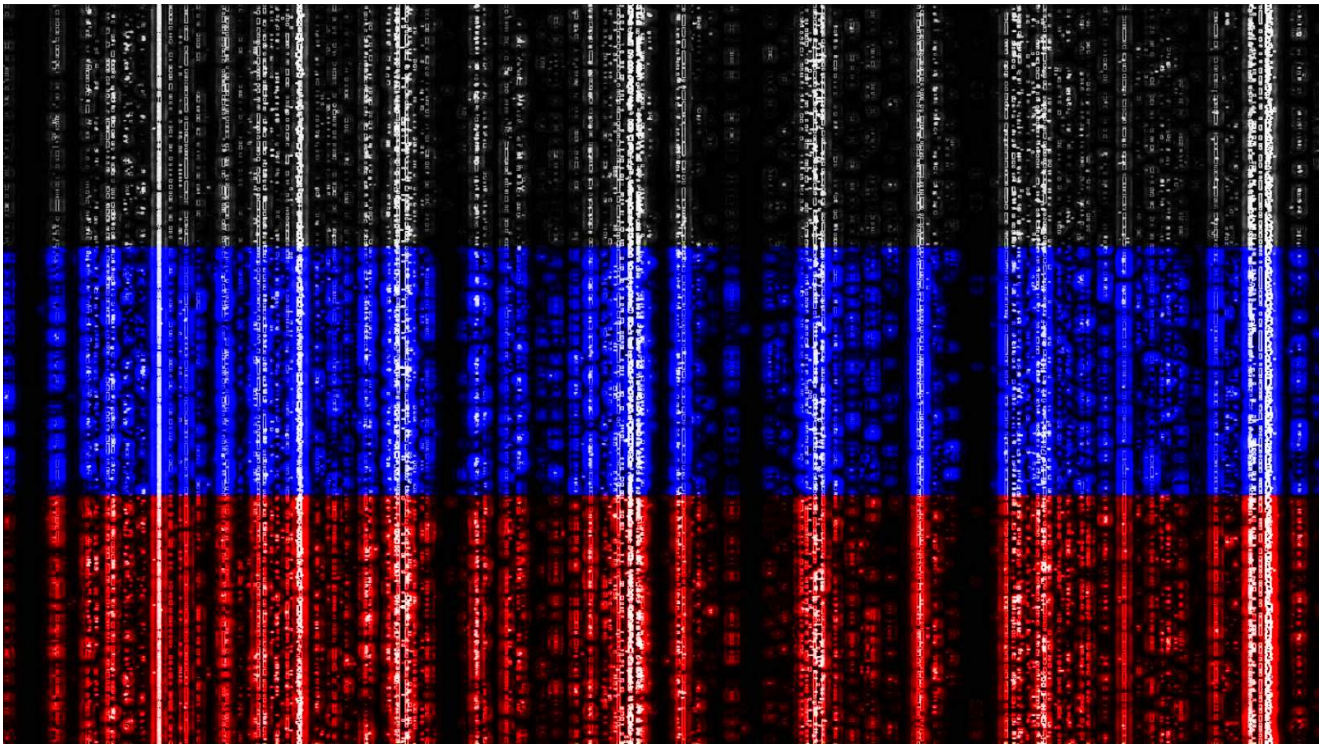
Russian 'Gamaredon' hackers use 8 new malware payloads in attacks

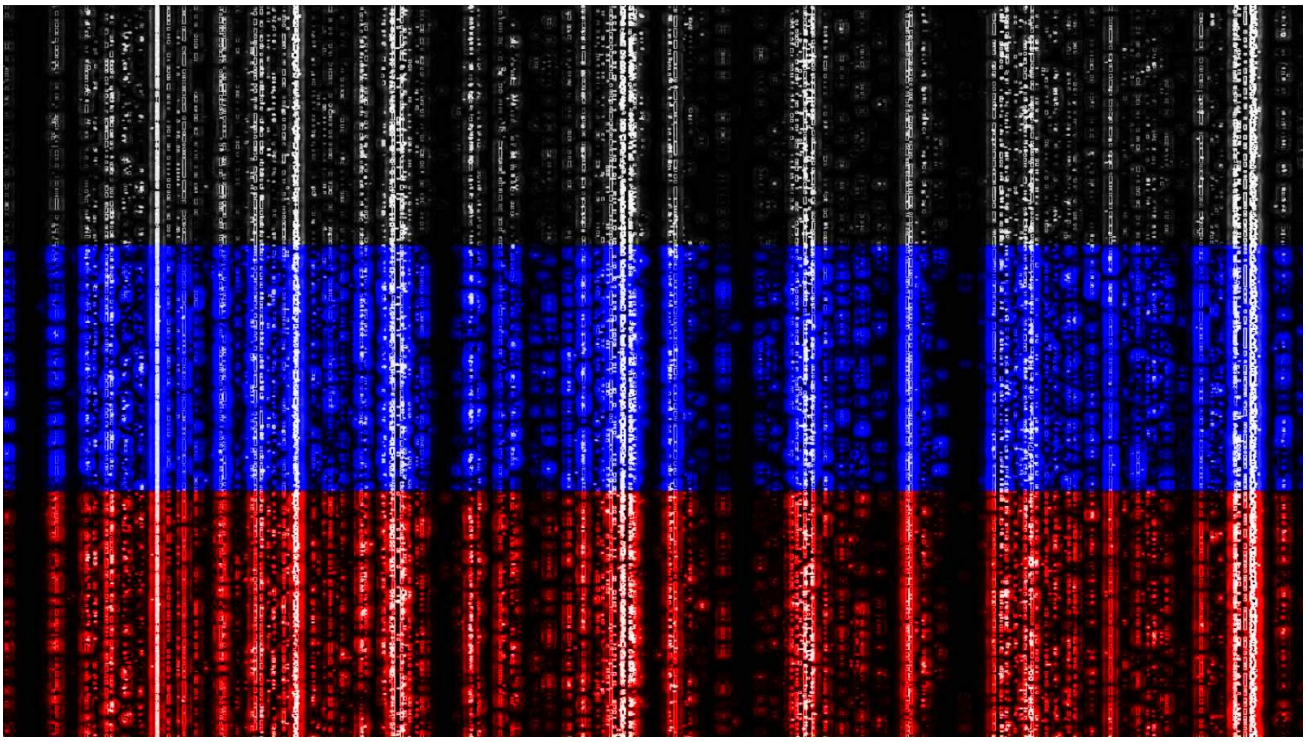
bleepingcomputer.com/news/security/russian-gamaredon-hackers-use-8-new-malware-payloads-in-attacks/

Bill Toulas



By
Bill Toulas

- January 31, 2022
- 11:14 AM
- 1



The Russia-linked hackers known as 'Gamaredon' (aka Armageddon or Shuckworm) were spotted deploying eight custom binaries in cyber-espionage operations against Ukrainian entities.

This hacking group is believed to be operated directly by the Russian FSB (Federal Security Service) and has been responsible for thousands of attacks in Ukraine since 2013.

Researchers at Symantec's Threat Hunter team, a part of Broadcom Software, have analyzed eight malware samples used by Gamaredon against Ukrainian targets in recent attacks, which could provide essential information for defenders to protect against the ongoing wave attacks.

Files used in recent Gamaredon attacks

According to Symantec's report, the monitored attacks began in July with the dissemination of spear-phishing emails that carried macro-laced Word documents.

These files launched a VBS file that dropped "Pteranodon," a well-documented backdoor that Gamaredon has been developing and improving for almost seven years now.

However, while recent attacks are still conducted using phishing emails, these attacks now drop eight different payloads, as described below.

All eight files sampled by Symantec's analysts from recent Gamaredon attacks are 7-zip self-extracting binaries that minimize user-interaction requirements.

- **descend.exe** – Executes to drop a VBS file on "%USERPROFILE%\Downloads\deerbrook.ppt" and "%PUBLIC%\Pictures\deerbrook.ppt", and creates a scheduled task on the compromised system. The VBS contacts the C2 and fetches the payload.
- **deep-sunken.exe** – The downloaded payload which executes to drop four more files on the compromised computer: baby.cmd, baby.dat, basement.exe (wget binary), vb_baby.vbs. A new scheduled task is created and the C2 is contacted again for the next payload.
- **z4z05jn4.egf.exe** – Next-stage payload which is similar to the previous one but features different C2, drops files in different folders, and uses different filenames.
- **defiant.exe** – Executes to drop VBS files onto "%TEMP%\\deep-versed.nls" and "%PUBLIC\Pictures\deep-versed.nls", and then create a scheduled task for their execution.
- **deep-green.exe** – UltraVNC remote administration tool that connects to a repeater.
- **deep-green.exe** – Process Explorer binary for Microsoft Windows.
- **deep-green.exe** – Same as defiant.exe but with different hard-coded C2 and filenames.
- **deep-green.exe** – Drops VBS in "%PUBLIC%\Music\" and creates a scheduled task that searchers for removable drives on the infected system.

Other indicators of compromise include C2 URLs and IPs allocated by the AS9123 TimeWeb Ltd., and they all use a unique URI structure as shown below:

- http + IP + /.php?=, OR
- http + IP + /.php?=,-

Also, the most common directories that host malicious files are:

- csidl_profile\links
- csidl_profile\searches
- CSIDL_PROFILE\appdata\local\temp\
- CSIDL_PROFILE\

The Symantec report also concludes that many of the dropped files have unknown parent process hashes which weren't analyzed, so parts of the Gamaredon operation remain unclear.

File hashes for the new malware payloads discovered by Symantec can be found in their report.

Related Articles:

Ukraine warns of "chemical attack" phishing pushing stealer malware

Russian state hackers hit Ukraine with new malware variants

Sandworm hackers fail to take down Ukrainian energy provider

Ukraine: Russian Armageddon phishing targets EU govt agencies

Russian hackers perform reconnaissance against Austria, Estonia

- Gamaredon
- Hacker
- Malware
- Russia
- Ukraine

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

Comments

ubscal99 - 3 months ago

-
-

Heads up you used the wrong "there" in the last sentence, I believe it should be "their". Great article!

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: