Cyberspies linked to Memento ransomware use new PowerShell malware

bleepingcomputer.com/news/security/cyberspies-linked-to-memento-ransomware-use-new-powershell-malware/

Sergiu Gatlan

By
Sergiu Gatlan

- February 1, 2022
- 02:00 PM
- 0

An Iranian state-backed hacking group tracked as APT35 (aka Phosphorus or Charming Kitten) is now deploying a new backdoor called PowerLess and developed using PowerShell.

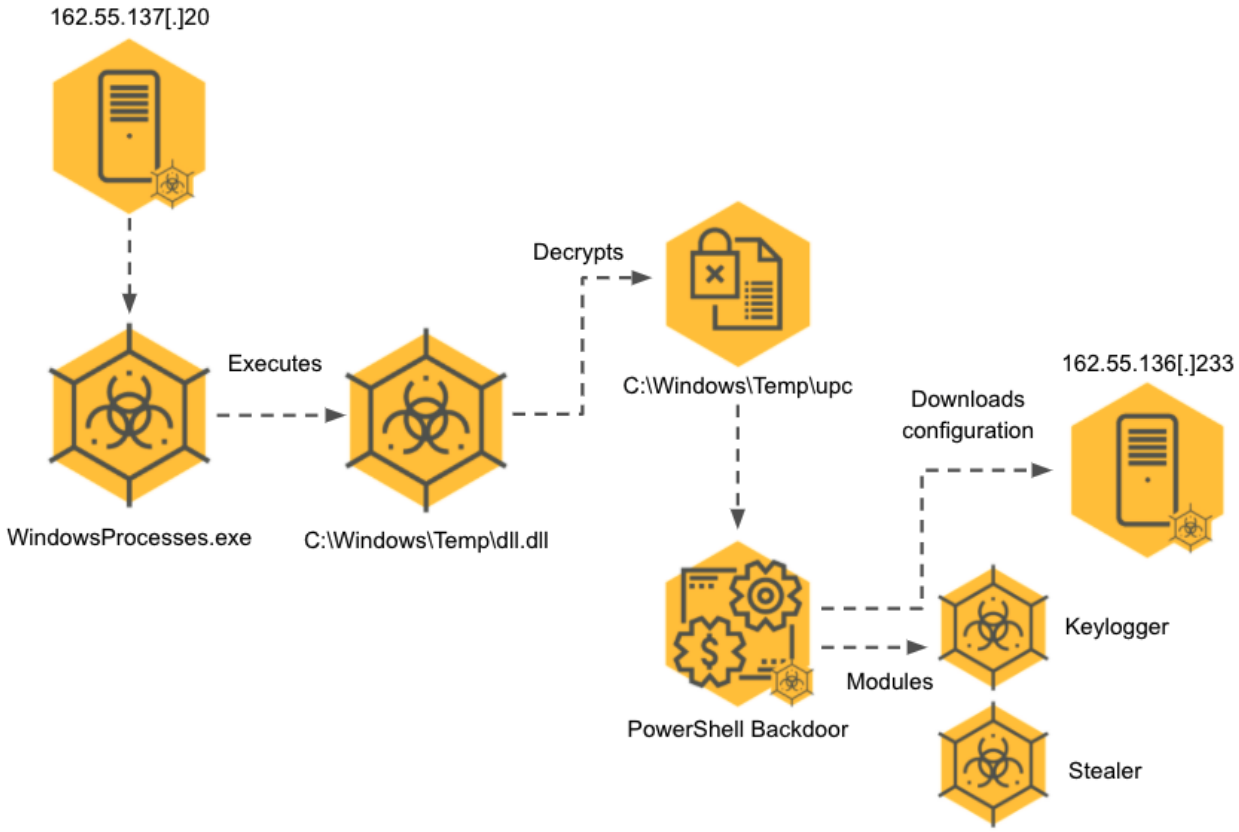
The threat group also used the previously unknown malware to deploy additional modules, including info stealers and keyloggers, according to a report published today by the Cybereason Nocturnus Team.

The PowerLess backdoor features encrypted command-and-control communication channels, and it allows executing commands and killing running processes on compromised systems.

It also evades detection by running in the context of a .NET application which allows it to hide from security solutions by not launching a new PowerShell instance.

"The toolset analyzed includes extremely modular, multi-staged malware that decrypts and deploys additional payloads in several stages for the sake of both stealth and efficacy. At the time of writing this report, some of the IOCs remained active delivering new payloads," the Cybereason researchers said.

In January, APT35 operators were also deploying another previously undocumented PowerShell backdoor dubbed CharmPower in attacks leveraging Log4Shell exploits.



Attack flow (Cybereason)

The Memento ransomware link

While looking into attacks where the newly discovered PowerLess backdoor was used, the researchers also found potential connections to Memento ransomware.

This ransomware has been active since April 2021, being deployed in attacks against VMware vCenter servers using exploits designed to abuse a critical pre-auth remote code execution flaw patched months before, in February 2021.

Sophos has seen Memento operators switching from encrypting systems with a Python-based ransomware strain to moving files into password-protected WinRAR archives due to anti-ransomware protection active on compromised devices.

The links include common TTP patterns, automatically generated strings, and a domain (google.onedriver-srv[.]ml).

This domain is linked to an IP address mentioned in a joint advisory issued by US and UK cybersecurity agencies in November regarding Iranian hacking groups targeting Microsoft Exchange and Fortinet servers.

Also in November, the Microsoft Threat Intelligence Center (MSTIC) said it has been tracking six different Iranian threat groups who have been deploying ransomware and exfiltrating data in attacks that started as far back as September 2020.

Ransomware attacks by Iranian APTs (Microsoft)

"The activity of Phosphorus with regard to ProxyShell took place in about the same time frame as Memento," the Cybereason Nocturnus Team said.

"Iranian threat actors were also reported to be turning to ransomware during that period, which strengthens the hypothesis that Memento is operated by an Iranian threat actor."

Related Articles:

Eternity malware kit offers stealer, miner, worm, ransomware tools

Beware: Onyx ransomware destroys files instead of encrypting them

Hackers exploit critical VMware RCE flaw to install backdoors

OldGremlin ransomware gang targets Russia with new malware

FIN7 hackers evolve toolset, work with multiple ransomware gangs