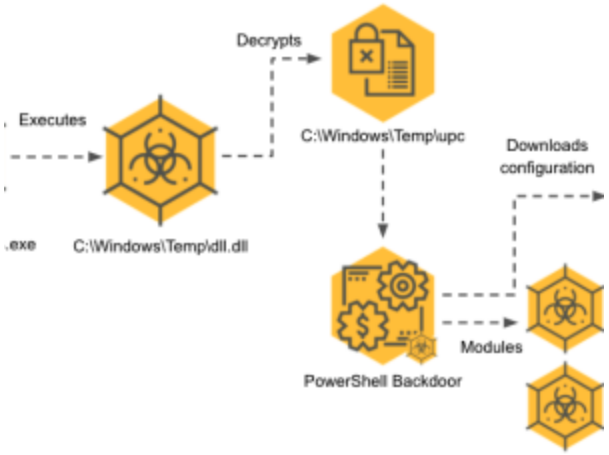
Experts warn of a spike in APT35 activity and a possible link to Memento ransomware op

securityaffairs.co/wordpress/127526/apt/apt35-spike-memento-op.html

February 2, 2022



February 2, 2022 By Pierluigi Paganini

The Cybereason Nocturnus Team reported a spike in the activity of the Iran-linked APT group APT35 (aka Phosphorus or Charming Kitten).

The Cybereason Nocturnus Team observed a spike in the activity of the Iran-linked APT group APT35 (aka 'Charming Kitten', 'Phosphorus', Newscaster, and Ajax Security Team)

The Phosphorus group made the headlines in 2014 when experts at iSight issued a report describing the most elaborate net-based spying campaign organized by Iranian hackers using social media.

Microsoft has been tracking the threat actors at least since 2013, but experts believe that the cyberespionage group has been active since at least 2011.

The APT group previously targeted medical research organizations in the US and Israel in late 2020, and for targeting academics from the US, France, and the Middle East region in 2019.

They have also previously targeted human rights activists, the media sector, and interfered with the US presidential elections.

The APT35 group is now deploying a new PowerShell backdoor called PowerLess Backdoor using a stealthy technique to avoid detection. The group is running the PowerShell Backdoor in a .NET context rather than spawning the PowerShell process.

Below is the capabilities supported by the PowerLess backdoor:

- Encrypted channel with the C2
- Executing arbitrary commands
- Killing processes
- Stealing browser data
- Keylogging

Experts noticed a lot of typos and grammatical mistakes in the code of the backdoor, a circumstance that suggests that the native language of the backdoor's authors is likely not English.

"It is worth mentioning that the backdoor is being run within a .NET context, so therefore it does not spawn "powershell.exe"." reads the analysis published by the researchers. "This behavior can be interpreted as an attempt to evade certain PowerShell detections, although PowerShell logs are being saved on the machine" "Oddly enough, there is a part of the code in the PowerLess Backdoor, that do spawn a powershell.exe process, when the request to kill a process is received from the C2"

The toolset analyzed by Cybereason includes modular, multi-staged malware used to deploy additional payloads. The attackers also used previously undetected malware, including info stealers and keyloggers.

In Mid-January, the Iran-linked APT35 group has been observed leveraging the Log4Shell flaw to drop a new PowerShell backdoor tracked as CharmPower.

Cybereason also found evidence that links the APT group to the Memento Ransomware operations that first appeared in the threat landscape in 2021.

The gang was observed exploiting the CVE-2021-21972 vulnerability in VMware vCenter Server for the initial access to target networks.

In October, Sophos researchers have spotted the Memento ransomware that adopts a curious approach to block access to victims' files. The ransomware copies files into password-protected WinRAR archives, it uses a renamed freeware version of the legitimate file utility WinRAR. The Memento ransomware then encrypts the password and deletes the original files from the victim's system.

Experts found multiple similarities between TTPs used by Phosphorus and the Memento ransomware operation and attack infrastructure.

“Another IP that appears in US CERT’s list is 91.214.124[.]143. Searching it in VirusTotal reveals other malicious files communicating with it, as well as unique URL directory patterns that reveal a potential connection to Memento Ransomware.” concludes the report. “The activity of Phosphorus with regard to ProxyShell took place in about the same time frame as Memento. 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.”

Pierluigi Paganini

(SecurityAffairs – hacking, APT35)

You might also like

Experts believe that Russian Gamaredon APT could fuel a new round of DDoS attacks

May 28, 2022 By Pierluigi Paganini

There you can buy or download for free private and compromising data of your competitors. We public schemes, drawings, technologies, political and military secrets, accounting reports and clients databases. All this things were gathered from the largest worldwide companies, conglomerates and concerns with every activity. We gather data using vunlerability in their IT infrastructure. in their IT infrastructure.

Industrial spy team processes huge massives every day to devide you results. You can fid it in their portal:

http://[redacted]

(Tor browser required)

We can save your time gaining your own goals or goals of your company.With our information you could refuse partnership with unscrupulous partner, reveal dirty secrets of your competitors and enemies and earn millions dollars using insider information.

"He who owns the information, owns the world"

Nathan Mayer Rothschild

The strange link between Industrial Spy and the Cuba ransomware operation

May 28, 2022 By Pierluigi Paganini

Back to top

- Home
- Cyber Crime
- Cyber warfare
- APT
- Data Breach

- Deep Web
- Digital ID
- Hacking
- Hacktivism
- Intelligence
- Internet of Things
- Laws and regulations
- Malware
- Mobile
- Reports
- Security
- Social Networks
- Terrorism
- ICS-SCADA
- EXTENDED COOKIE POLICY
- Contact me