Infamous Hacker-for-Hire Group DeathStalker Hits the Americas & Europe With New PowerPepper Malware

darkreading.com/vulnerabilities---threats/-infamous-hacker-for-hire-group-deathstalker-hits-the-americas-and-europe-with-new-powerpepper-malware/d/d-id/1339604

December 3, 2020

Vulnerabilities/Threats
4 MIN READ

ARTICLE
Infamous Hacker-for-Hire Group DeathStalker Hits the Americas & Europe With New PowerPepper Malware

December 03, 2020

Woburn, MA – December 3, 2020 – Kaspersky researchers have spotted new malware activity in the wild from DeathStalker, the advanced persistent threat (APT) actor known for offering hacking-for-hire services targeting companies in the financial and legal sectors. The group was found using a new malware implant and delivery tactics involving a backdoor Kaspersky has dubbed PowerPepper.

The backdoor is used to remotely take control of victim devices. It leverages DNS over HTTPS as a communication channel, in order to hide communications with the control server behind legitimate-looking traffic. PowerPepper also uses several evasion techniques, including steganography, a method for disguising data.

DeathStalker is a highly unusual APT actor. Active since at least 2012, the group conducts espionage campaigns against small and medium-sized businesses, particularly law firms and financial services organizations. Unlike other APT groups, it doesn't appear to be politically motivated or seek financial gain from the companies they target. Rather, they act as mercenaries, offering their hacking services for a price.

Kaspersky researchers have recently uncovered new malicious campaigns from DeathStalker. Like other malware strains associated with the group, PowerPepper is typically spread via spearphishing emails with the malicious files delivered via the email body or within a malicious link. The group has exploited international events, carbon emission regulations, and even the pandemic to trick their victims into opening the malicious documents.

The main malicious payload is disguised using steganography, a process that allows attackers to hide data amid legitimate content. In the case of PowerPepper, the malicious code is embedded in what appears to be regular pictures of ferns or peppers (hence the name) and is then extracted by a loader script. Once that happens, PowerPepper begins to execute remote shell commands sent by DeathStalker operators, which are aimed at stealing sensitive business information. The malware can carry out any shell command on the targeted system, including those for standard data reconnaissance, such as gathering the computer's user and file information, browsing network file shares, and downloading additional binaries or copy content to remote locations. The commands are obtained from the control server though DNS over HTTPS communications, an effective way to disguise malicious communications behind legitimate server name queries.

The use of steganography is just one of several obfuscation and evasion techniques employed by the malware. The loader is disguised as a verification tool from identity services provider GlobalSign. It uses custom obfuscation, and parts of the malicious delivery scripts are hidden in Word-embedded objects. Communications with the implant and servers are encrypted and, thanks to the use of trusted, signed scripts, antivirus software won't necessarily recognize the implant as malicious at startup.

PowerPepper has been seen in attacks across Europe primarily, but also in the Americas and Asia. In previously described campaigns, DeathStalker mainly targeted law consultancy firms and organizations that provide financial or cryptocurrency services.

"PowerPepper once again proves that DeathStalker is a creative threat actor: one capable of consistently developing new implants and toolchains in a short period of time," said Pierre Delcher, security expert at Kaspersky. "PowerPepper is already the fourth malware strain affiliated with the actor, and we have discovered a potential fifth strain. Even though they are not particularly sophisticated, DeathStalker's malware has proven to be quite effective, perhaps because their primary targets are small and medium-sized organizations—organizations that tend to have less robust security programs. We expect DeathStalker to remain active, and we will continue to monitor its campaigns."

PowerPepper was part of the most recent GReAT Ideas: *Powered by Croissant. Baguette Edition*. You can watch the recording, as well as other presentations on the latest threat developments by Kaspersky's top-level experts here:

Read more about PowerPepper and its evasion techniques at Securelist.

To protect your organizations from attacks like PowerPepper, Kaspersky experts recommend:

- Provide your SOC team with access to the latest threat intelligence (TI). The Kaspersky Threat Intelligence Portal is a single point of access for the company's TI, providing cyberattack data and insights gathered by Kaspersky over more than 20 years.
- To minimize the risk of infection through phishing emails, companies should educate their employees with basic cybersecurity hygiene training to be wary of emails from unknown senders. If they receive such letters, they shouldn't open attachments or click any links in them before making sure the letter is legitimate.
- To protect medium-sized businesses from such advanced attacks, it's better to use endpoint security solutions with EDR functionality. Kaspersky's Integrated Endpoint Security solution detects an attack and provides a wide range of response actions optimized for IT and security teams of mid-sized companies.