Serpent Backdoor Slithers into Orgs Using Chocolatey Installer

Author: Elizabeth Montalbano March 22, 2022 10:21 am 3:30 minute read Write a comment

Share this article:

An unusual attack using an open-source package installer called Chocolatey, steganography and Scheduled Tasks is stealthily delivering spyware to companies.

Researchers have discovered a cyberattack that uses unusual evasion tactics to backdoor French organizations with a novel malware dubbed Serpent, they said.

A team from Proofpoint observed what they call an "advanced, targeted threat" that uses email-based lures and malicious files typical of many malware campaigns to deliver its ultimate payload to targets in the French construction, real-estate and government industries.

However, between initial contact and payload, the attack uses methods to avoid detection that haven't been seen before, researchers revealed in a blog post Monday.

These include the use of a legitimate software package installer called Chocolatey as an initial payload, equally legitimate Python tools that wouldn't be flagged in network traffic, and a novel detection-bypass technique using a Scheduled Task, they said.

“The ultimate objectives of the threat actor are presently unknown,” Proofpoint researchers Bryan Campbell, Zachary Abzug, Andrew Northern and Selena Larson acknowledged in the post. “Successful compromise would enable a threat actor to conduct a variety of activities, including stealing information, obtaining control of an infected host or installing additional payloads.”

Serpent: A Slippery Attack Chain

The attack chain begins as many email-based attacks do——with an email that appears to be coming from a legitimate source that includes a Microsoft Word document containing malicious macros. Various parts of the macro include ASCII art that depicts a snake, giving the backdoor its name, researchers said.

The macro-laden document purports to have important information related to the “règlement général sur la protection des données (RGPD),” aka the European Union’s General Data Protection Regulations (GDPR), a law which mandates how companies must report data leaks to the government.

If macros are enabled, the document executes the document’s macro, which reaches out to an image URL—e.g., https://www.fhccu[.]com/images/ship3[.]jpg—that contains a base64 encoded PowerShell script hidden using steganography.

The PowerShell script first downloads, installs and updates the installer package and repository script for Chocolatey, a software management automation tool for Windows that wraps installers, executables, .ZIP files and scripts into compiled packages, researchers said.

“Leveraging Chocolatey as an initial payload may allow the threat actor to bypass threat-detection mechanisms because it is a legitimate software package and would not immediately be identified as malicious,” researchers noted.

The script then uses Chocolatey to install Python, including the pip Python package installer. This component then installs various dependencies including PySocks, a Python-based reverse proxy client that enables users to send traffic through SOCKS and HTTP proxy servers, researchers said.

Next, the PowerShell script fetches another image file—e.g. https://www.fhccu[.]com/images/7[.]jpg,—which contains a base64 encoded Python script that also is obscured using steganography, they said. The PowerShell script saves the Python script as “MicrosoftSecurityUpdate.py” and then creates and executes a .bat file that in turn executes the Python script.

The attack chain ends with a command to a shortened URL which redirects to the Microsoft Office help website, researchers said. The steganographic images used to hide the scripts are hosted on what appears to be a Jamaican credit-union website, they added.

Serpent Backdoor

Once successfully installed on a targeted system, the Serpent backdoor periodically pings the “order” server, or the first onion[.]pet URL), and expects responses of the form <random integer>—<hostname>—<command>.

If <hostname> matches the hostname of the infected computer, the infected host runs the command provided by the order server (<command>), researchers said. This could be any Windows command as designated by the attacker, the output of which is then recorded.

Next, Serpent uses PySocks to connect to the command-line Pastebin tool called Termbin, pastes the output to a bin, and receives the bin’s unique URL.

As its final act, the backdoor sends a request to the “answer” server (a second onion[.]pet URL), including the hostname and bin URL in the header. This allows the attacker to monitor the bin outputs via the “answer” URL and see what the infected host’s response was, researchers observed. Once this entire process is complete, Serpent cycles through it indefinitely, they added.

Task-Scheduler Evasion Tactic

In addition to using steganographic images and the Chocolatey package installer to hide its nefarious activities, the attack also uses what Proofpoint researchers said is a never-before-seen application of signed binary proxy execution using a Scheduled Tasks executable, as “an attempt to bypass detection by defensive measures.”

A command that leverages schtasks.exe to create a one-time task to call a portable executable is contained within a Swiper image called ship.jpg after the end of file marker, researchers said.

“In this case the executable is called calc.exe,” researchers wrote in the post. The trigger for this task is contingent on the creation of a Windows event with EventID of 777, after which the command then creates a dummy event to trigger the task ,and deletes the task from the task scheduler as if it never occurred, they said.

“This peculiar application of tasking logic results in the portable executable being executed as a child process of taskhostsw.exe, which is a signed Windows binary,” researchers said.

Moving to the cloud? Discover emerging cloud-security threats along with solid advice for how to defend your assets with our FREE downloadable eBook, “Cloud Security: The Forecast for 2022.” We explore organizations’ top risks and challenges, best practices for defense, and advice for security success in such a dynamic computing environment, including handy checklists.