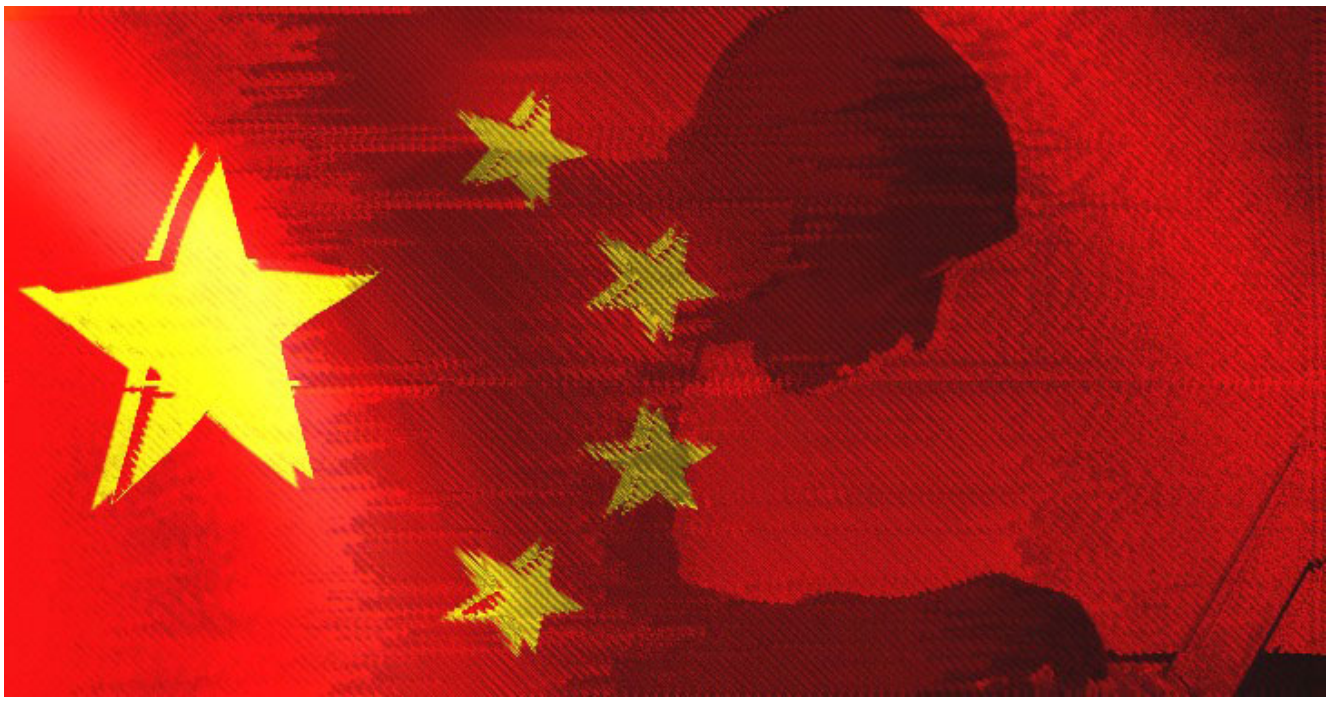
Researchers Link ShadowPad Malware Attacks to Chinese Ministry and PLA

thehackernews.com/2022/02/researchers-link-shadowpad-malware.html

February 15, 2022



Cybersecurity researchers have detailed the inner workings of **ShadowPad**, a sophisticated and modular backdoor that has been adopted by a growing number of Chinese threat groups in recent years, while also linking it to the country's civilian and military intelligence agencies.

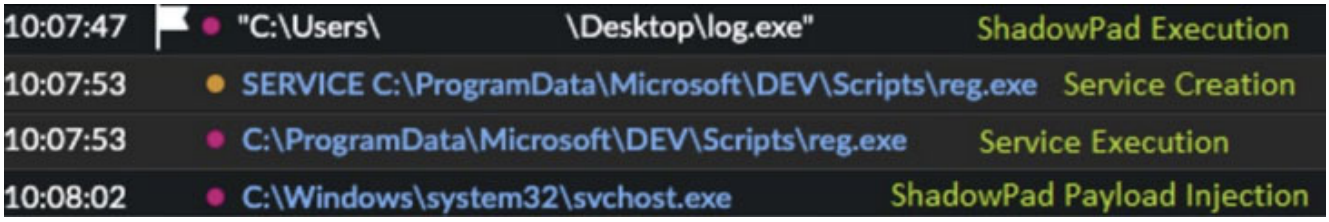
"ShadowPad is decrypted in memory using a custom decryption algorithm," researchers from Secureworks said in a report shared with The Hacker News. "ShadowPad extracts information about the host, executes commands, interacts with the file system and registry, and deploys new modules to extend functionality."

ShadowPad is a remote access trojan capable of maintaining persistent access to compromised computers and executing arbitrary commands and next-stage payloads. It also shares noticeable overlaps with the PlugX malware and has been put to use in high-profile attacks against NetSarang, CCleaner, and ASUS, causing the operators to shift tactics and update their defensive measures.

While initial campaigns that delivered ShadowPad were attributed to a threat cluster tracked as Bronze Atlas (aka APT41, Barium, or Winnti Umbrella) – Chinese nationals working for a networking security company named Chengdu 404 – it has since been used by multiple Chinese threat groups post 2019.

In a detailed overview of the malware in August 2021, cybersecurity company SentinelOne dubbed ShadowPad a "masterpiece of privately sold malware in Chinese espionage." A subsequent analysis by PwC in December 2021 disclosed a bespoke packing mechanism – named ScatterBee – that's used to obfuscate malicious 32-bit and 64-bit payloads for ShadowPad binaries.

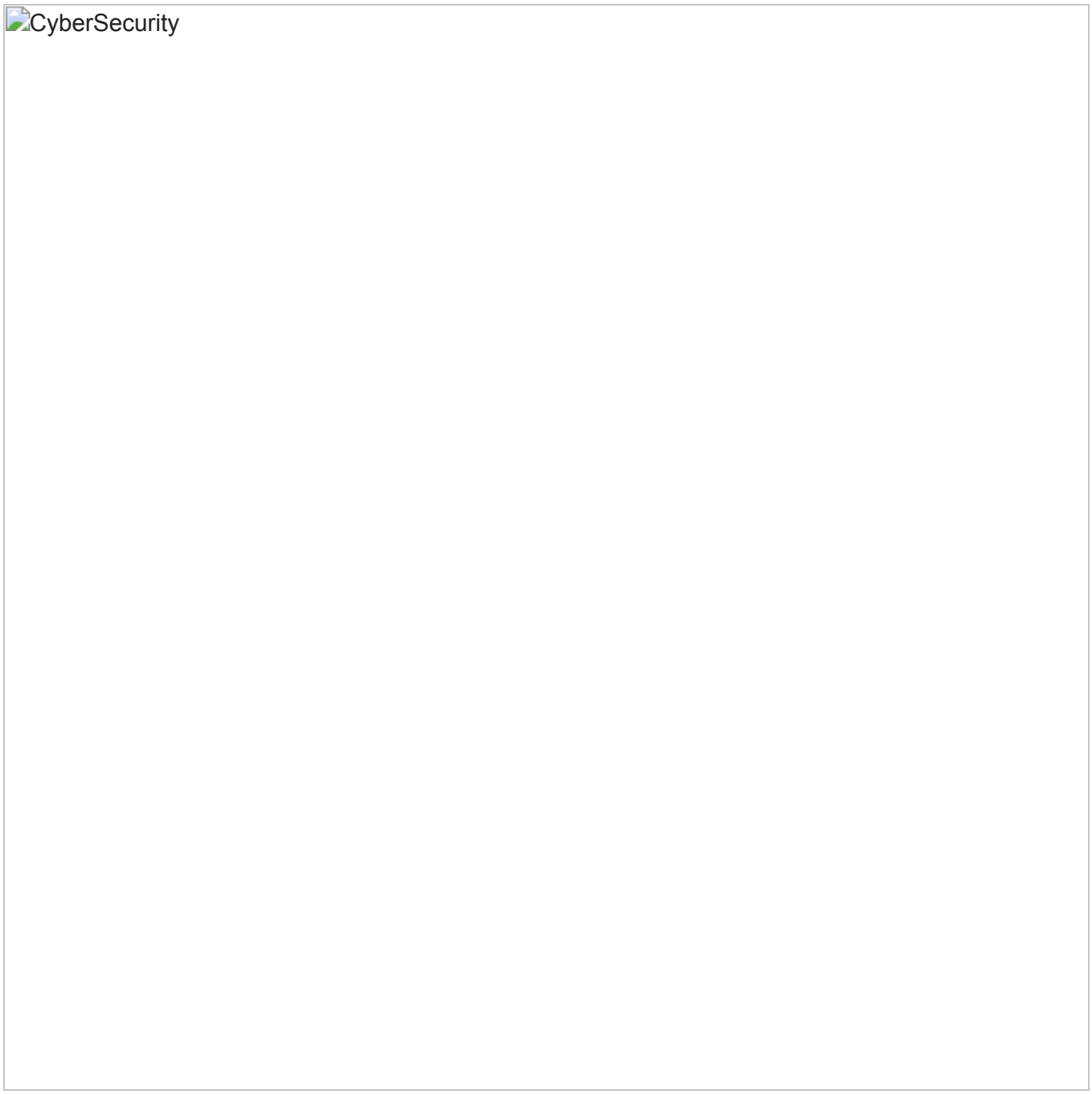
The malware payloads are traditionally deployed to a host either encrypted within a DLL loader or embedded inside a separate file along with a DLL loader, which then decrypts and executes the embedded ShadowPad payload in memory using a custom decryption algorithm tailored to the malware version.



These DLL loaders execute the malware after being sideloaded by a legitimate executable vulnerable to DLL search order hijacking, a technique that allows the execution of malware by hijacking the method used to look for required DLLs to load into a program.

Select infection chains observed by Secureworks also involve a third file that contains the encrypted ShadowPad payload, which work by executing the legitimate binary (e.g., BDReinit.exe or Oleview.exe) to sideload the DLL that, in turn, loads and decrypts the third file.

Alternatively, the threat actor has placed the DLL file in the Windows System32 directory so as to be loaded by the Remote Desktop Configuration (SessionEnv) Service, ultimately leading to the deployment of Cobalt Strike on compromised systems.



In one ShadowPad incident, the intrusions paved the way for launching hands-on-keyboard attacks, which refer to attacks wherein human hackers manually log into an infected system to execute commands themselves rather than using automated scripts.

Additionally, Secureworks attributed distinct ShadowPad activity clusters, including Bronze Geneva (aka Hellsing), Bronze Butler (aka Tick), and Bronze Huntley (aka Tonto Team), to Chinese nation-state groups that operate in alignment with the People's Liberation Army Strategic Support Force (PLASSF).

"Evidence […] suggests that ShadowPad has been deployed by MSS-affiliated threat groups, as well as PLA-affiliated threat groups that operate on behalf of the regional theater commands," the researchers said. "The malware was likely developed by threat actors affiliated with Bronze Atlas and then shared with MSS and PLA threat groups around 2019."

SHARE □ □ □ □ □

SHARE □