Chinese Experts Uncover Details of Equation Group's Bvp47 Covert Hacking Tool

ךFeb 23, 2022ךRavie Lakshmanan ⋮ 6-8 minutes

Researchers from China's Pangu Lab have disclosed details of a "top-tier" backdoor put to use by the **Equation Group**, an advanced persistent threat (APT) with alleged ties to the cyber-warfare intelligence-gathering unit of the U.S. National Security Agency (NSA).

Dubbed "Bvp47" owing to numerous references to the string "Bvp" and the numerical value "0x47" used in the encryption algorithm, the backdoor was extracted from Linux systems "during an in-depth forensic investigation of a host in a key domestic department" in 2013.

The defense research group codenamed the attacks involving the deployment of Bvp47 "Operation Telescreen," with the implant featuring an "advanced covert channel behavior based on TCP SYN packets, code obfuscation, system hiding, and self-destruction design."

Bvp47 is said to have been used on more than 287 targets in the academia, economic development, military, science, and telecom sectors located in 45 countries, mainly in China, Korea, Japan, Germany, Spain, India, and Mexico, all the while going largely undetected for over a decade.

The elusive backdoor is also equipped with a remote control function that's protected using an encryption algorithm, activating which requires the attacker's private key – something the researchers said they found in the leaks published by the Shadow Brokers hacker group in 2016.

Pangu Lab is a research project of Pangu Team, which has a history of jailbreaking Apple iPhones dating all the way back to 2014. At the Tianfu Cup hacking contest last year, the white hat hacking team demonstrated several security flaws that allowed for remotely jailbreaking a fully patched iPhone 13 Pro running iOS 15.

The Shadow Brokers leaks#

Equation Group, designated as the "crown creator of cyber espionage" by Russian security firm Kaspersky, is the name assigned to a sophisticated adversary that's been active since at least 2001 and has used previously undisclosed zero-day exploits to "infect victims, retrieve data and hide activity in an outstandingly professional way," some of which were later incorporated into Stuxnet.

The attacks have targeted a variety of sectors in no less than 42 countries, counting governments, telecom, aerospace, energy, nuclear research, oil and gas, military, nanotechnology, Islamic activists and scholars, media, transportation, financial institutions, and companies developing encryption technologies.

The group is believed to be linked to the NSA's Tailored Access Operations (TAO) unit, while intrusion activities pertaining to a second collective known as Longhorn (aka The Lamberts) have been attributed to the U.S. Central Intelligence Agency (CIA).

Equation Group's malware toolset became public knowledge in 2016 when a group calling itself the Shadow Brokers leaked the entire tranche of exploits used by the elite hacking team, with Kaspersky uncovering code-level similarities between the stolen files and that of samples identified as used by the threat actor.

Bvp47 as a covert backdoor#

The incident analyzed by Pangu Lab comprises two internally compromised servers, an email and an enterprise server named V1 and V2 respectively, and an external domain (identified as A), sporting a novel two-way communication mechanism to exfiltrate sensitive data from the systems.

"There is abnormal communication between external host A and the V1 server," the researchers said. "Specifically, A first sends a SYN packet with a 264-byte payload to port 80 of the V1 server, and then the V1 server immediately initiates an external connection to the high-end port of the A machine and maintains a large amount of exchange data."

Simultaneously, V1 connects to V2 via the SMB service to perform a number of operations, including logging in to the latter with an administrator account, trying to open terminal services, enumerating directories, and executing

PowerShell scripts through scheduled tasks.

V2, for its part, also connects to V1 to retrieve a PowerShell script and an encrypted second-stage payload, the encrypted execution results of which are sent back to V1, which, according to the researchers, "acts as a data transfer between the A machine and the V2 server."

The Bvp47 backdoor installed on the servers consists of two parts, a loader which is responsible for decoding and loading the actual payload into memory. "Bvp47 generally lives in the Linux operating system in the demilitarized zone that communicates with the Internet," the researchers said. "It mainly assumes the core control bridge communication role in the overall attack."

Links to the Equation Group#

Pangu Lab's attribution to Equation Group stems from overlaps with exploits contained in a GPG-encrypted archive file published by the Shadow Brokers – "eqgrp-auction-file.tar.xz.gpg" – as part of a failed auction of the cyber weapons in August 2016.

"In the process of analyzing the 'eqgrp-auction-file.tar.xz.gpg' file, it was found that Bvp47 and the attacking tools in the compressed package were technically deterministic, mainly including 'dewdrops,' 'suctionchar_agents,' 'tipoffs,' 'StoicSurgeon,' 'incision' and other directories," the researchers explained.

"The 'tipoffs' directory contains the RSA asymmetric algorithm private key used in the Bvp47 covert channel [for] command execution and other operations. On this basis, it can be confirmed that Bvp47 is from [the] Equation group."

The findings mark the second time hitherto undocumented malware developed by the Equation Group has come to light in as many months. In late December 2021, Check Point Research disclosed details of a diagnostic utility called "DoubleFeature" that's used in conjunction with the DanderSpritz malware framework.

"Judging from the attack tools related to the organization, including Bvp47, Equation group is indeed a first-class hacking group," the researchers concluded.

"The tool is well-designed, powerful, and widely adapted. Its network attack capability equipped by zero-day vulnerabilities was unstoppable, and its data acquisition under covert control was with little effort. The Equation Group is in a dominant position in national-level cyberspace confrontation."

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.