China's APT3 Pilfers Cyberweapons from the NSA

Author:
Tara Seals

September 6, 2019 / 3:18 pm

5 minute read

Skip to:
A Tale of Two Bugs

Share this article:

Large portions of APT3's remote code-execution package were likely reverse-engineered from prior attack artifacts.

The advanced persistent threat (APT) group known as APT3, which researchers across the board link to the Chinese government, has built a full in-house battery of exploits and cybertools collectively dubbed "UPSynergy." An analysis of the toolkit has uncovered a geopolitical cat-and-mouse spy game: It turns out that many parts of the package are likely gleaned from watching attacks by the National Security Agency's Equation Group APT on target networks where APT3 also has a presence.

Prior research from Symantec shows that APT3 was able to acquire a variant of the NSA-developed cyberweapon known as EternalRomance – prior to the Shadow Brokers leak of the spy agency's arsenal in 2017. It has been a bit of a mystery as to how APT3 accomplished that – but research from Check Point offers a hypothesis.

"The threat group known as APT3 recreated its own version of an Equation group exploit using captured network traffic," according to the analysis, published Thursday. "We believe that this artifact was collected during an attack conducted by the Equation Group against a network monitored by APT3, allowing it to enhance its exploit arsenal with a fraction of the resources required to build the original tool...One possible modus operandi – the Chinese collect attack tools used against them, reverse-engineer and reconstruct them to create equally strong digital weapons."

APT3 (a.k.a Buckeye or UPS Team) from there went on to equip the reverse-engineered attack tool, named Bemstour, with an additional zero-day, researchers said. Bemstour is used by APT3 to gain remote code-execution on a victim's machine; the enhancement consists of a new exploit that allows APT3 to cast a wider net in terms of victimology.

"EternalRomance targeted mostly Windows 7 systems (as well as lower version of Windows NT where SMBv1 is located)," Check Point explained. "One of the problems in adapting EternalRomance to higher Windows versions was a patch introduced in Windows 8 which eliminated the possibility to use an information leak vulnerability leveraged by it."

The NSA got around this by chaining EternalRomance to a different tool that exploited Windows 8, called EternalChampion, to create a hybrid exploit named EternalSynergy. APT3 instead found a whole new zero-day information leak exploit to bolt onto its EternalRomance variant, which allowed the group to upgrade their version to be effective against OS higher than Windows 7.

"All of this activity suggests that the group was not exposed to an actual NSA exploitation tool, as they would then not need to create another zero-day exploit," according to the analysis. "We decided to name APT3's bundle of exploits UPSynergy, since, much like in the case of Equation group, it combines two different exploits to expand the support to newer operating systems."

Interestingly, the goal of the weapon is to deploy a payload on the victim's machine which is injected to a running process using an implant, which bears striking resemblance to the Equation group's DoublePulsar tool.

"As far as APT3's implant is concerned, it seems likely that the DoublePulsar code was reused as is," Check Point researchers noted. "The code is not executed directly, but has several layers of obfuscation. Essentially, the Equation Group's DoublePulsar code is wrapped with an APT3 position independent crypter and loader."

In all, the research shows a cyberspy drama played out between the United States and Beijing.

"If network traffic was indeed used by the group as a reference, the traffic was likely collected from a machine controlled by APT3," Check Point researchers pointed out. "This means either a Chinese machine that was targeted by the NSA and monitored by the group, or a machine compromised by the group beforehand on which foreign activity was noticed. We believe the former is more likely, and in that case could be made possible by capturing lateral movement within a victim network targeted by the Equation Group."

Along with spying on each other, the U.S. and China are apparently in the midst of a cyber-arms race to develop new exploits.

"Finding a zero-day info leak, recreating the exploit based on the aforementioned vulnerability, and utilizing a lot of internal undocumented structures of SMB in the implants, implies that there was a similar expertise with and analysis performed on SMB drivers (with an eye to exploiting them) on the Chinese side, roughly at the same time it was widely used

INFOSEC INSIDER

A Practical Guide to Zero-Trust Security
January 15, 2020 2

7 Tips for Maximizing Your SOC
December 31, 2019 5

Mean Time to Hardening: The Next-Gen Security Metric
December 30, 2019 4

Combining AI and Playbooks to Predict Cyberattacks
December 26, 2019 1

The Case for Cyber-Risk Prospectuses
December 24, 2019 1

by the NSA," according to the analysis.

A Tale of Two Bugs

The zero-day that APT3 found (CVE-2019-0703) is "an information disclosure vulnerability [that] exists in the way [...] the Windows SMB Server handles certain requests," according to Microsoft. However, the flaw is actually a logical bug related to querying information from the Windows Named Pipes mechanism, according to Check Point, and not a vulnerability in the SMB protocol nor its implementation.

"While it can be triggered using SMB, there are other ways to leverage it, e.g. using the NtQueryInformationFile Windows API call that is unrelated to SMB," the researchers said. "The bug resides within npfs.sys (Name Pipe File System driver) in a function named NpQueryInternalInfo. The latter is used to query named pipes and return a value called a file reference number....[the number] is a pointer to a kernel structure named CCB (Client Control Block). This is an undocumented struct defined in npfs.sys, which has a partial definition (named NP_CCB) provided by the ReactOS project. Clearly, this is not the intended value to be returned in this case, and the leak of this struct discloses useful information that can be leveraged by attackers."

In APT3's case, the group triggered the vulnerability by establishing an SMB connection to a named pipe on the victim's machine via SMB.

"The method was used to determine the bitness of the attacked operating system and overwrite (using a write primitive) a field in the leaked structure, which eventually provided the group with remote code-execution," according to Check Point.

Meanwhile, the original vulnerability (CVE-2017-0143) targeted by EternalRomance and repurposed by APT3 is rooted in a type confusion bug; as a result of type confusion between SMB messages, the server considers an unrelated SMB message as part of an SMB Transaction of a different type, and activates the wrong type of SMB handler.

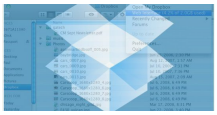
"This handler in turn shifts the Transaction struct's pointer to the incoming data buffer by the amount of data received in the SMB message," said the researchers. "Because the pointer value was shifted by the wrong handler, data of further SMB messages (which are treated by the correct type of handler) can be potentially written outside the boundaries of the incoming data buffer. If there was successful grooming (i.e. the heap was correctly shaped beforehand), this out-of-bound write may allow us to overwrite an adjacent SMB Transaction structure."

In all, the research shows two highly sophisticated nation-state actors jockeying for cyber-dominance with exploit developments and tool espionage.

"It's not always clear how threat actors achieve their exploitation tools, and it's commonly assumed that actors can conduct their own research and development or get it from a third party," Check Point concluded. "In this case we have evidence to show that a third (but less common) scenario took place – one where attack artifacts of a rival (i.e. Equation Group) were used as the basis and inspiration for establishing in-house offensive capabilities by APT3."

Government | Vulnerabilities

SUGGESTED ARTICLES



Dropbox Passes $1M Milestone for Bug-Bounty Payouts

The file-sharing service also disclosed details of past notable bugs for the first time.

February 6, 2020

New Bill Proposes NSA Surveillance Reforms

The newly-introduced bill targets the Patriot Act's Section 215, previously used by the U.S. government to collect telephone data from millions of Americans.

January 24, 2020 2

PoC Exploits Published For Microsoft Crypto Bug

Two proof-of-concept exploits were publicly released for the major Microsoft crypto-spoofing vulnerability.

January 16, 2020 1

DISCUSSION