OSINT: UPSynergy: Chinese-American Spy vs. Spy Story

General information

UUID	5d810f7f-a56c-49fb-9108-72b80a000082
2019-09-17	**Date**
Owner org	No value specified.
Threat level	High (1)
Analysis	Completed (2)
Info	OSINT: UPSynergy: Chinese-American Spy vs. Spy Story
Event date	2019-09-17 17:04:18
Published	**Yes** (2019-09-17 17:04:26)
Creator Org	Profero
# Attributes	5
Tags	**misp-galaxy:mitre-enterprise-attack-intrusion-set="APT3 - G0022"** **misp-galaxy:threat-actor="UPS"** **misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210"** **misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068"** **osint:source-type="blog-post"**

Attributes

Attribute #1

UUID	5d810ff5-4514-45ca-8baa-7c310a000082
Category	External analysis
Type	comment
Value	The group’s exploitation tool named Bemstour makes use of a variant of a single Equation group exploit. Our research shows that the particular equivalent to this exploit is EternalRomance. APT3 developed their own implementation, possibly based on their analysis and understanding of EternalRomance’s leveraged vulnerability. The group attempted to develop the exploit in a way that allowed it to target more Windows versions, similar to what was done in a parallel Equation group exploit named EternalSynergy. This required looking for an additional 0-day that provided them with a kernel information leak. 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 0-day exploit. We decided to name APT3’s bundle of exploits UPSynergy, since, much like in the case of Equation group, it combines 2 different exploits to expand the support to newer operating systems. The underlying SMB packets used throughout the tool execution were crafted manually by the developers, rather than generated using a third party library. As a lot of these packets were assigned with hardcoded and seemingly arbitrary data, as well as the existence of other unique hardcoded SMB artifacts, we can assume that the developers were trying to recreate the exploit based on previously recorded traffic. If network traffic was indeed used by the group as a reference, the traffic was likely collected from a machine controlled by APT3. 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. Finding a 0-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 by the NSA. This, to some extent, suggests a narrative where China and the US are engaged in a cyber arms race to develop new exploits.

Attribute #2

UUID	5d811004-1f68-42fb-a2e3-7c310a000082
Category	External analysis
Type	link
Value	https://research.checkpoint.com/upsynergy/

Attribute #3

UUID	5d8110df-6840-498e-9a88-7c330a000082
Category	Payload delivery
Type	md5
Value	f595228976cc89ffac02d831e774cfa6

Attribute #4

UUID	5d8110ec-af38-463b-b305-7c330a000082
Category	Payload delivery
Type	sha1
Value	80143e32f887b2583b777daec5982fb5c2886fb3

Attribute #5

UUID	5d8110f5-7894-44be-b81e-72b40a000082
Category	Payload delivery
Type	sha256
Value	0b28433a2b7993da65e95a45c2adf7bc37edbd2a8db717b85666d6c88140698a

Objects

No object