FIREEYE

Solutions   Services   Customers   Partners   Resources   Company

Home > FireEye Blogs > Threat Research > Demonstrating Hustle, Chinese APT Groups Quickly U...

Threat Research

Demonstrating Hustle, Chinese APT Groups Quickly Use Zero-Day Vulnerability (CVE-2015-5119) Following Hacking Team Leak

July 13, 2015 | by FireEye Threat Intelligence | Threat Intelligence

ADVANCED PERSISTENT THREAT DETECTION   THREAT INTELLIGENCE   ADVANCED PERSISTENT THREAT

The FireEye as a Service team detected independent phishing campaigns conducted by two Chinese advanced persistent threat (APT) groups that we track, APT3 and APT18. Each threat group quickly took advantage of a zero-day vulnerability (CVE-2015-5119), which was leaked in the disclosure of Hacking Team's internal data. Adobe released a patch for the vulnerability on July 8, 2015. Before that patch was released, the groups launched phishing campaigns against multiple companies in the aerospace and defense, construction and engineering, education, energy, health and biotechnology, high tech, non-profit, telecommunications, and transportation industries.

As of publication, we have no reason to believe APT3 and APT18 are working together. Their opportunism demonstrates each group's flexibility, organization, and awareness of developments in the information security community.

APT3's Campaign

APT3 actors targeted at least 10 organizations in the following industries:

- Aerospace and Defense
- Construction and Engineering
- Energy
- High Tech
- Non-Profit
- Telecommunications
- Transportation

An example of an APT3 phishing email is below in Figure 1:

FROM: "<first.last>" <first.last>@perrydale.com

SUBJECT: <Target> Analysis report- 2015

URLs:

hxxp://report.perrydale[.]com/ema/RR201507[.]pdf

hxxp://vic.perrydale[.]com/logo2.jpg

hxxp://rpt.perrydale[.]com/en/rep201507101[.]pdf

Figure 1: An example of APT3 phishing email using CVE-2015-5119

As of July 8, all three domains observed in the URLs resolved to 194.44.130.179. Similar to APT3's activity in Operation Clandestine Wolf, the URLs redirect to JavaScript profilers and a malicious Adobe Flash file. The Flash file downloads an obfuscated GIF, which contains a SHOTPUT payload compiled the day APT3 sent the phishing emails. SHOTPUT is a DLL backdoor that that communicates over HTTP and may be capable of uploading or downloading files, managing processes, executing system commands, and collecting system information. SHOTPUT may also be detected as Backdoor.APT.CookieCutter. The SHOTPUT backdoor communicates to the following command and control (CnC) addresses, which are hardcoded into the malware:

- psa.perrydale[.]com
- link.angellroofing[.]com
- 107.20.255.57
- 23.99.20.198

This is the third time since mid-2014 that we have observed APT3 using a zero-day, which attests to its ability to capitalize on new exploits.

APT18's Campaign

APT18 actors targeted at least 13 organizations in the following industries:

- Aerospace and Defense
- Construction and Engineering
- Education
- Health and Biotechnology
- High Tech
- Telecommunications
- Transportation

An example of an APT18 phishing email is shown in Figure 2:

FROM: <various> @duwrt.com

SUBJECT: Important:Flash Update

Body:

Dear,

If you already have Flash installed on your computer, you'll be asked to download and install update. Once the new update is installed, Flash should function normally. Update Outlook Many Flash problems can be solved by updating your client software to the latest version. Please verify that you have all the latest updates available for your version of Adobe flash software. Here's how:

1.Download update hxxp://get[.]adobe[.]com/ (masked URL: hxxp://137.175.4[.]132/index.htm)

2.Click Check for Updates.

3.Restart your computer after you have verified that all updates are installed. You must have administrative privileges on your computer to install any Flash. Please contact your desktop support staff if you need assistance.

Figure 2: An example of APT18 phishing email using CVE-2015-5119

Once the victim clicks the URL, the system downloads a malicious Adobe Flash (.swf) file with the properties shown in Figure 3.
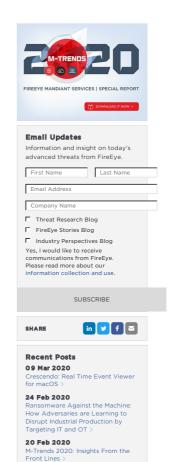
Filename: movie.swf

MD5: 079a440bee0f86d8a59ebc5c4b523a07

Filesize: 214976

Figure 3: APT18 Malicious SWF Properties

Upon exploitation, a GH0ST RAT variant is delivered to the victims' system, which calls out to a previously known APT18 CnC address 223.25.233.248. GHOST RAT is a backdoor derived from public source code. It may also be detected as Backdoor.APT.Gh0stRat. The compiled source code provides attackers with many ways to control a victim's system, including the ability to create, manipulate, delete, launch, or transfer files; perform screen or audio capture; enable a webcam; list or kill processes; open a command shell; and wipe event logs. However, since the source code is public, threat groups may tailor the code by removing or adding functionality.

Email Updates

Information and insight on today's advanced threats from FireEye.

First Name   Last Name

Email Address

Company Name

☐ Threat Research Blog
☐ FireEye Stories Blog
☐ Industry Perspectives Blog

Yes, I would like to receive communications from FireEye. Please read more about our information collection and use.

SUBSCRIBE

SHARE

Recent Posts

09 Mar 2020
Crescendo: Real Time Event Viewer for macOS >

24 Feb 2020
Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT >

20 Feb 2020
M-Trends 2020: Insights From the Front Lines >

RSS FEED: STAY CONNECTED

Comparing the Campaigns

APT3 and APT18 took a slightly different approach in employing the exploit, which demonstrates they likely work independently. As usual, APT3 used compromised infrastructure, while APT18 relied on procured infrastructure. APT3 used customized phishing emails that sometimes contained the names of the targeted organizations, whereas APT18's emails were nonspecific and likely crafted to be used on multiple targets.

Quick Turnaround Time Demonstrates Adaptability and Opportunism

The groups demonstrated their adaptability and skill by quickly employing Hacking Team's leaked zero-day before the vulnerability was patched. Both groups likely monitor information from security research to learn what exploits are available and how network defenders are reacting to them. We have previously observed APT3 monitoring and quickly changing tactics based on public research. After we exposed details about Operation Clandestine Wolf, APT3 changed its phishing emails, modified filenames, and updated its backdoor.

In the past, APT3 and APT18 have frequently developed or adapted zero-day exploits for operations, which were likely planned in advance. Using data from the Hacking Team leak demonstrates how they can shift resources—selecting targets, preparing infrastructure, crafting messages, and updating tools—to take advantage of unexpected opportunities like newly exposed exploits.

Recommendations

FireEye maintains endpoint and network detection for CVE-2015-5119, the backdoors used in these campaigns, and other tools used by these groups. Additionally, we highly recommend:

- Applying Adobe's patch for Flash immediately,
- Querying for additional activity by source addresses or email indicators,
- Blocking CnC addresses via outbound communications, and
- Scope the environment to prepare for incident response.

Note: IOCs for this campaign can be found here.