APT Group Exploiting Hacking Team Flash Zero Day

Security company Volexity said that the Wekby APT group, allegedly responsible for hitting Community Health Systems last year, is using the Hacking Team Flash Player zero-day exploit.

The Wekby APT group, implicated in a number of targeted attacks against health care organizations such as Community Health Systems and major pharmaceutical companies, is reportedly making use of the Adobe Flash Player zero-day found in the Hacking Team data dump.

According to Virginia-based security company Volexity, spear phishing messages purporting to be from Adobe have been found spreading a modified version of the Hacking Team exploit that affects Flash Player versions up to 18.0.0.194. Labels found in the code, in fact, refer to Hacking Team, the company said.

Internal emails, sales invoices and other documents leaked since the breach was made public implicate Hacking Team in selling exploits and intrusion software to oppressive governments and sanctioned countries.

The spear phishing message found by Volexity urges the victim to download and install an updated version of Flash and includes a link to http://get[.]adobe[.]com that instead redirects the recipient to a site hosted by PEG TECH Inc. The site loads a malicious .swf file exploiting the Flash vulnerability patched yesterday by Adobe.

The malware executes and connects to a known Webky command and control address hosted in Singapore, Volexity said.

"Any connection involving this IP address or these hostnames should be consider hostile and a likely indicator of compromise," the company said in its report.

In the past, the Webky APT group, also known as APT 18, has hosted other malware families from the Singapore IP address, including Poison Ivy and the Gh0st remote access Trojan in this case.

Volexity said that current, patched versions of Flash will display a pop-up dialog with the word "faile!" prominently displayed.

"It looks like the attackers may have left a debug message from their testing," Volexity said. "Not very subtle at all.

"The attackers are having a field day with this exploit and will not slow down any time soon," the company said. "Patching is the most prudent course of action to deal with this exploit that is very much in the wild."

Adobe yesterday patched the zero day in Flash Player, CVE-2015-5119, one of 36 vulnerabilities patched in the update. The Hacking Team bug was the only one being publicly exploited. The update patched a mix of vulnerability classes, including memory address randomization issues, heap buffer overflows, memory corruption bugs, security bypass vulnerabilities, same-origin bypasses, and use-after-free flaws.

The Flash zero day, it was revealed yesterday as well, was quickly integrated into the major exploit kits, including Angler, Nuclear and Neutrino, as well as the Metasploit Framework.

Security company Bromium, published its analysis of the zero day, determining it was a byte array use-after-free memory issue that allows an attacker to gain control of a Windows machine running the vulnerable Flash Player. Researcher Nick Cano wrote that Hacking Team built its proof-of-concept code based on a 2014 vulnerability known as the ActionScript-Spray attack (CVE-2014-0322) which took advantage of a UAF bug in Internet Explorer to gain access to the heap of a process.

Meanwhile, yesterday, Department of Homeland Security's CERT at the Software Engineering Institute at Carnegie Mellon University released an advisory warning users about a still unpatched Windows kernel vulnerability that was also part of the Hacking Team data dump.

The flaw lives specifically in the Adobe Type Manager kernel module in Windows; the module provides support for OpenType fonts.

"A memory-corruption flaw in Adobe Type Manager allows for manipulation of Windows kernel memory, which can result in a wide range of impacts," said the CERT advisory. In this case, a successful exploit such as Hacking Team's could allow an attacker to bypass browser and operating system sandbox protection to obtain System privileges on a Windows computer.

"We have confirmed that the exploit code successfully obtains SYSTEM privileges on Windows XP through Windows 8.1 systems, both 32-bit and 64-bit," CERT said.

Share this article:

Hacks Malware Vulnerabilities Web Security

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

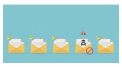
The Case for Cyber-Risk Prospectuses
December 24, 2019 1

SUGGESTED ARTICLES

Coronavirus-Themed APT Attack Spreads Malware

The APT group was spotted sending spear-phishing emails that purport to detail information about coronavirus – but they actually infect victims with a custom RAT.

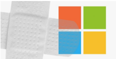
March 13, 2020



Spear-Phishing Attack Lures Victims With 'HIV Results'

Attackers are purporting to send victims HIV test results – but in reality are convincing them to download the Koadic RAT.

March 10, 2020



Microsoft Exchange Server Flaw Exploited in APT Attacks

A vulnerability is Microsoft Exchange servers is being actively exploited by multiple APT groups, researchers warn.

March 9, 2020

DISCUSSION