Adobe Patches Flash Zero Day Exploited by Black Oasis APT

Adobe today released an out-of-band Flash Player update addressing a zero-day vulnerability being exploited by a little-known Middle Eastern APT group called Black Oasis.

Adobe today released an out-of-band Flash Player update addressing a zero-day vulnerability being exploited by a little-known Middle Eastern APT group.

The group known as Black Oasis was, as recently as this month, using exploits for the flaw to drop FinSpy as a payload. Sold by the controversial German company Gamma International, FinSpy, or FinFisher, is a suite of surveillance and espionage software used to remotely monitor compromised computers. It's sold to governments and law enforcement around the world, including allegations of sales to oppressive regimes including Egypt, Bahrain, Ethiopia, Uganda and elsewhere.

The vulnerability, CVE-2017-11292, was privately disclosed Oct. 10 by researchers at Kaspersky Lab, who saw the payload and exploit used against a customer's network. The attackers spread the exploit via email, embedding the Flash exploit inside an Active X object inside a Word document. Brian Bartholomew, a member of Kaspersky Lab's Global Research and Analysis Team (GReAT), said retrieval of the payload—which is the latest FinSpy version—is done in multiple stages.

Adobe said Flash version 27.0.0.159 on the desktop, Linux and Google Chrome is affected, as well as version 27.0.0.130 for Edge and Internet Explorer 11 on Windows 10 and 8.1. Users should be sure to be running Flash 27.0.0.170 on all platforms, or heed the advice of many security experts to disable Flash all together. Flash has been designated for end-of-life.

Kaspersky Lab published a report today about the zero day on Securelist.com.

Black Oasis is a bit of an enigma among APT groups. The group has been on Kaspersky Lab's radar for nearly a year, Bartholomew said, and has had at least five zero-day vulnerabilities and exploits at its disposal since 2015, all of which have been disclosed and patched. There is only one known victim of the Flash zero day patched today, he said.

"These guys are definitely customers of Gamma. They've been using FinSpy for maybe the last two years," Bartholomew said. "They were also potentially customers of Hacking Team."

Black Oasis appears to have made use of a Hacking Team zero day, CVE-2015-5119, prior to the Italian software company being hacked in the summer of 2015 and having many of its attacks publicly dumped online.

"We know this group was also using that exploit, which we assume was unique to Hacking Team customers," Bartholomew said. "They had access to it prior to the hack. Once the hack happened, I have not seen them using Hacking Team at all but they have been using FinSpy pretty regularly since."

The APT group's targets are government and military organizations in the Middle East, countries in North Africa, as well as some in Russia, Ukraine and elsewhere in Europe.

"FinSpy seems to be their payload of choice," Bartholomew said.

This is the second zero-day vulnerability in possession of Black Oasis to be patched in the last month. In September, FireEye disclosed CVE-2017-8759, which was patched by Microsoft and used to spy on an unnamed Russian individual. The vulnerability was described as a SOAP WSDL parser code injection bug spread via Microsoft Office RTF documents. The code injection was used to download and execute script that included PowerShell commands.

"In the last two months, they've burnt two zero days. It's very evident they have access to a wide swathe of zero days," Bartholomew said.

Zero days can sell for six or seven figures on gray or black markets. They are a source of constant debate between security and privacy experts and governments who buy these attacks for exclusive use as lawful intercept tools in the name of national security or law enforcement purposes.

While Black Oasis may be very well resourced, its operational security may be lacking. For example, the group re-used command and control servers burned by the FireEye disclosure in this recent round of attacks using the Flash zero day.

"They had right around a month to move their infrastructure, but yet they didn't," Bartholomew said.

The emergency update comes less than a week after Patch Tuesday when for the first time in recent memory, Adobe did not publish any security updates for any of its products.

Share this article:

Vulnerabilities

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

Flaws Riddle Zyxel's Network Management Software

Over 16 security flaws, including multiple backdoors and hardcoded SSH server keys, plague the software.

March 11, 2020

Popular ThemeREX WordPress Plugin Opens Websites to RCE

The bug has been under active attack as a zero-day.

March 10, 2020

DISCUSSION

INFOSEC INSIDER

A Practical Guide to Zero-Trust Security

January 14, 2020

7 Tips for Maximizing Your SOC

December 31, 2019

Mean Time to Hardening: The Next-Gen Security Metric

December 30, 2019

Combining AI and Playbooks to Predict Cyberattacks

December 26, 2019

The Case for Cyber-Risk Prospectuses

December 24, 2019

Newsletter

Subscribe to Threatpost Today

Join thousands of people who receive the latest breaking cybersecurity news every day.

Subscribe now

Twitter

A Nigerian cybercriminal hoodwinked hundreds of thousands of victims with a #cybercrime campaign that asked them to... https://t.co/r48fUGi00W

2 hours ago

Follow @threatpost

Subscribe to our newsletter, Threatpost Today. Get the latest breaking news delivered daily to your inbox.

Subscribe now