APT28 group is rushing to exploit recent CVE-2017-11292 Flash 0-Day before users apply the patches

October 22, 2017 By Pierluigi Paganini

The APT28 group is trying to exploit the CVE-2017-11292 Flash zero-day before users receive patches or update their systems.

Security experts at Proofpoint collected evidence of several malware campaigns, powered by the Russian APT28 group, that rely on a Flash zero-day vulnerability that Adobe patched earlier this week.

According to the experts who observed attacks on organizations across Europe and in the US, the APT28 group is trying to exploit the CVE-2017-11292 zero-day before users receive patches or update their systems.

The state-sponsored hackers focused their attacks on state departments and private-sector businesses in the aerospace industry.

"On Tuesday, October 18, Proofpoint researchers detected a malicious Microsoft Word attachment exploiting a recently patched Adobe Flash vulnerability, CVE-2017-11292. We attributed this attack to APT28 (also known as Sofacy), a Russian state-sponsored group." states the report published by Proofpoint.

"Targeting data for this campaign is limited but some emails were sent to foreign government entities equivalent to the State Department and private-sector businesses in the aerospace industry. The known geographical targeting appears broad, including Europe and the United States. The emails were sent from free email services."

The patch was released on Monday, October 16, at that time Kaspersky detected attacks leveraging the CVE-2017-11292 allegedly conducted by the BlackOasis APT group.

Researchers believe that APT28 was also in possession of the exploit (whether purchased, discovered on their own, or reverse engineered from the BlackOasis attack), and is trying to use it in targeted attacks.

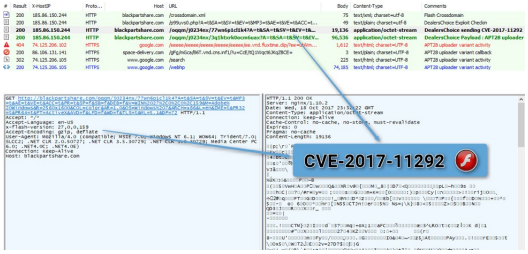
The APT28 rushed to assemble the exploit and the distribution campaign, reusing code from past attacks, the APT28 hackers did the same in May after Microsoft patched three zero-days flaws exploited by the Russian APT group.

Back to the present, researchers believe the APT28 found a way to exploit the CVE-2017-11292, it is unclear if they purchased the zero-day or reverse engineered it from the BlackOasis attack.

The researchers noticed that the recent attacks exploiting the CVE-2017-11292 flaw employed the same old DealersChoice malware, a Flash exploit framework also used by the APT28 group against Montenegro.

When the target user opens these the weaponized files, DealersChoice contacts the remote server to download the CVE-2017-11292 exploit code and execute it.

"The document "World War 3.docx" contacts DealersChoice.B, APT28's attack framework that allows loading exploit code on-demand from a command and control (C&C) server. DealersChoice has previously been used to exploit a variety of Flash vulnerabilities, including CVE-2015-7645, CVE-2016-1019, CVE-2016-4117, and CVE-2016-7855 via embedded objects in crafted Microsoft Word documents." continues the report.



The Proofpoint researcher Kafeine, confirmed his company currently trying to take down C&C servers associated with the DealersChoice attack framework used in the CVE-2017-11292 attacks.

"APT28 appears to be moving rapidly to exploit this newly documented vulnerability before the available patch is widely deployed. Because Flash is still present on a high percentage of systems and this vulnerability affects all major operating systems, it is critical that organizations and end users apply the Adobe patch immediately. " concluded Proofpoint.

Further technical details are available in the report published by Proofpoint, including the IOCs.

Pierluigi Paganini

(Security Affairs – APT28, cyber espionage)

Share this...

Adobe Flash CVE-2017-11292 cyber espionage malware Russia state-sponsored hacking

Yoroi Blog

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS ARTICLE
A leaked document raises a doubt about NSA knew the #Krack attack since 2010

NEXT ARTICLE
Security Affairs newsletter Round 133 – News of the week

YOU MIGHT ALSO LIKE

Trump signed a bill to help small telecoms replace Huawei equipment

March 14, 2020 By Pierluigi Paganini

Cookiethief, the Android malware that hijacks Facebook accounts

March 13, 2020 By Pierluigi Paganini