APT28 racing to exploit CVE-2017-11292 Flash vulnerability before patches are deployed

CREATED 877 DAYS AGO by mpeter05 | Public | TLP: ● Green

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. 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.

REFERENCES: sources.txt
https://www.proofpoint.com/us/threat-insight/post/apt28-racing-exploit-cve-2017-11292-flash-vulnerability-patches-are-deployed

TAG: APT28, Flash

Indicators of Compromise (9) Related Pulses (4) Comments (0) History (0)

Fancy Bear Infrastructure

MODIFIED 571 DAYS AGO by AlienVault | Public | TLP: ○ White

FileHash-SHA256: 1 | **Domain:** 46

sofacy, fancy bear

104,181
SUBSCRIBERS

Fancy Bear continue to operate through phishing emails and much more

CREATED 814 DAYS AGO by bartblaze | Public | TLP: ○ White

CVE: 2 | **FileHash-SHA1:** 37 | **IPv4:** 11 | **URL:** 1 | **Domain:** 19

The Sednit group — also known as Strontium, APT28, Fancy Bear or Sofacy — is a group of attackers operating since 2004, if not earlier, and whose main objective is to steal confidential information from specific targets. This article is a follow-up to ESET's presentation at BlueHat in Nove…

sednit, xagent, sedkit, dealerschoice, seduploader, word, october, microsoft, april, august, eset, excel, september, december, november, windows, adobe flash, delphi, flash, macros, internet, full, adobe, proofpoint, version, android, microsoft word, xtunnel, europe, sofacy, …

608
SUBSCRIBERS

APT28 racing to exploit CVE-2017-11292 Flash vulnerability before patches are deployed | Proofpoint

48