Chinese TA459 APT exploits CVE-2017-0199 flaw to target Financial firms

May 3, 2017 By Pierluigi Paganini

Malware researchers at security firm ProofPoint reported the Chinese TA459 APT has exploited the CVE-2017-0199 vulnerability to target Financial firms.

The notorious cyber espionage group tracked as TA459 APT has targeted analysts working at major financial firms using the recently patched CVE-2017-0199 Microsoft Office vulnerability.

Experts at Proofpoint published a detailed analysis of the espionage campaign conducted by the TA459 APT group against military and aerospace organizations in Russia and Belarus.

"Proofpoint is tracking this attacker, believed to operate out of China, as TA459. The actor typically targets Central Asian countries, Russia, Belarus, Mongolia, and others." reads the analysis published by Proofpoint. "TA549 possesses a diverse malware arsenal including PlugX, NetTraveler, and ZeroT"

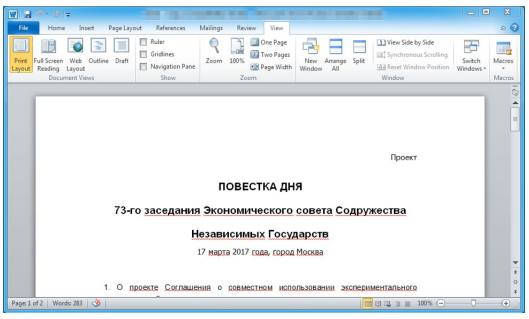
The TA459 APT group has been active since at least 2013, the hackers leveraged several malware in their campaign, including NetTraveler , PlugX, Saker, Netbot, DarkStRat, and ZeroT. The hackers most focused their efforts on spying on organizations in Russia and neighboring countries.

The attacks conducted by the TA459 APT group were apparently aimed at analysts covering the telecommunications industry, Proofpoint researchers speculate this latest campaign is likely a continuation of the campaign they uncovered in the summer of 2015.

"Proofpoint researchers recently observed a campaign targeting telecom and military in Russia. Beginning in July 2015 (and possibly earlier), the attack continued into August" wrote Proofpoint.

The TA459 APT leveraged spear-phishing emails using weaponized Word document that trigger the CVE-2017-0199 flaw. The hackers started exploiting the Office flaw just a few days after Microsoft released a fix.

When victims open the decoy document, an HTML application (HTA) file disguised as an RTF document is downloaded. The attack exploits PowerShell to download and executes a script that fetches and runs the ZeroT downloader.



Proofpoint noticed some improvements in the last ZeroT version such as the use of a legitimate McAfee utility for sideloading instead of a Norman Safeground utility.

"The attack group has made incremental changes to ZeroT since our last analysis. While they still use RAR SFX format for the initial payloads, ZeroT now uses a the legitimate McAfee utility named mcut.exe instead of the Norman Safeground AS for sideloading as they have in the past. The encrypted ZeroT payload, named Mctl.mui, is decoded in memory revealing a similarly tampered PE header and only slightly modified code when compared to ZeroT payloads we analyzed previously." continues the analysis.

Proofpoint reported that the TA459 APT group used both PlugX and a Trojan tracked as PCrat/Gh0st in the last wave of attacks.

The experts invite multinational organizations to stay vigilant about state-sponsored actors that use sophisticated malware in their cyber espionage campaigns.

"Ongoing activity from attack groups like TA459 who consistently target individuals specializing in particular areas of research and expertise further complicate an already difficult security situation for organizations dealing with more traditional malware threats, phishing campaigns, and socially engineered threats every day." concluded Proofpoint.

[adrotate banner="9"]

Pierluigi Paganini

(Security Affairs – TA459 APT group, cyber espionage)

[adrotate banner="13"]

Share this...

APT CVE-2017-0199 cyber espionage Hacking malware TA459 APT

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
Number of WordPress Attacks powered by compromised routers is rapidly dropping

NEXT ARTICLE
Travel Tech Giant Sabre suffered a Data Breach, traveler data potentially at risk

YOU MIGHT ALSO LIKE

Trend Micro addresses two issues exploited by hackers in the wild

March 18, 2020 By Pierluigi Paganini

TrueFire Guitar tutoring website was hacked, financial data might have been exposed

March 18, 2020 By Pierluigi Paganini

Yoroi Blog