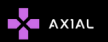


TA459



TA459



CHINA



RUSSIA, BELARUS,
MONGOLIA



SPEAR
PHISHING



A SURVEY ON TEMP.VELES : ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AXIAL

I. INTRODUCTION

TA459 is a threat group believed to operate out of China. The actor typically targets Central Asian countries, Russia, Belarus, Mongolia, and others. 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 attacks conducted by the TA459 APT group were apparently aimed at analysts covering the telecommunications industry. It used both PlugX and a Trojan tracked as PCrat/Gh0st.

II. TARGETS

Sectors:

Telecommunication , Finanacial

Analysts

Countries:

Russia , Belarus , Mongolia & others

III. ATTRIBUTION

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

IV. METHODS USED

- 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.

-ZeroT now uses a the legitimate McAfee utility named mcut.exe instead of the Norman Safeground AS for sideloading.

V. TOOLS USED

Gh0st RAT, NetTraveler, PlugX and ZeroT.



VI. IOCS

1. SHA256
3124fcb79da0bdf9d0d1995e37b06f7929d83c1c4b60e38c104743
be71170efe
2. SHA256
b5c208e4fb8ba255883f771d384ca85566c7be8adcf5c87114a62ef
b53b73fda
3. SHA256
bc2246813d7267608e1a80a04dac32da9115a15b1550b0c4842b9
d6e2e7de374
4. a64ea888d412fd406392985358a489955b0f7b27da70ff604e827d
f86d2ca2aa
5. bf4b88e42a406aa83def0942207c8358efb880b18928e41d60a2d
c59a59973ba

C&C

1. www[.]kz-info[.]net
2. hxxp://www.cis.minsk[.]by/news.php?id=7557
3. hxxp://122.9.52[.]215/news/power.rtf
4. hxxp://122.9.52[.]215/news/power.ps1
5. hxxp://www.firesyst[.]net/info/net/sports/drag/cgi.exe
6. www.firesyst[.]net
7. www.icekkk[.]net

VII. REFERENCES

1. <https://securityaffairs.co/wordpress/58692/apt/ta459-apt-targets-financial-firms.html>
2. <https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts>
3. <https://www.proofpoint.com/us/threat-insight/post/PlugX-in-Russia>
4. <https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests>
5. <https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zeroth-plugx>