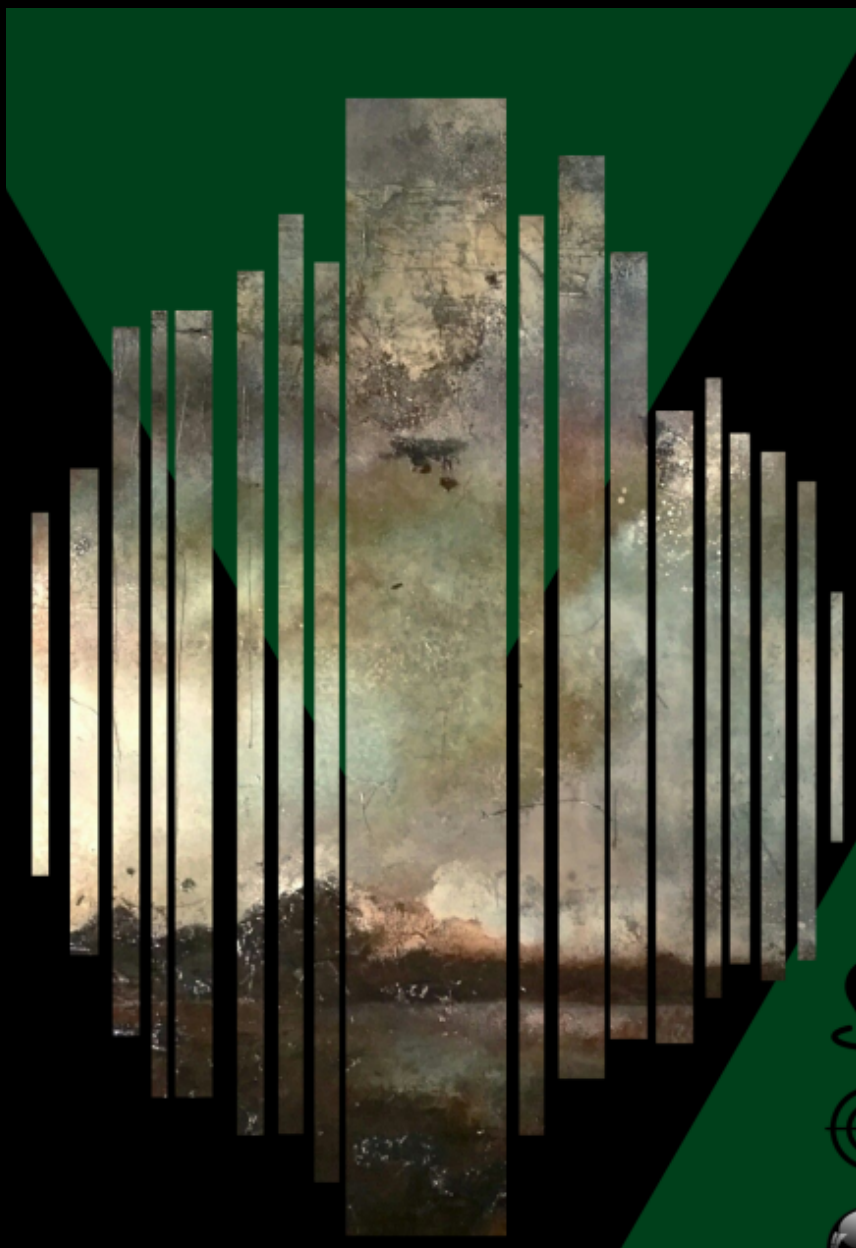
APT-28



AXIAL

APT- 28

FANCY BEAR

RUSSIA

US , WESTERN EUROPE

ZERO DAYS , SPEAR PHISHING

HAWK BASE

HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON APT-28 ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

APT-28 is a threat group based out of Russia and is state sponsored which focuses on information theft and espionage.

II. TARGETS

The targets of this threat group has been focused onto Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations onto multiple countries around the globe.

III. METHODS USED

This threat group has been using multiple methods like Abode Flash 0-days, spear phishing techniques along with multiple tools like Surface, Eviltoss and chopstick, along with tools and techniques like : Cannon, certutil, Computrace, CORESHELL, DealersChoice, Downdelph, Drovorub, Foozer, HIDEDRV, JHUHUGIT, Koadic, Komplex, LoJax, Mimikatz, Nimcy, OLDBAIT, PocoDown, ProcDump, PythocyDbg, Responder, Sedkit, Sedreco, USBStealer, VPNFilter, Winexe, WinIDS, X-Agent, X-Tunnel, Zebrocy, Living off the Land.

IV. CAMPAIGNS

This threat group has been involved in operation Pawn Storm.
This threat group has also been attributed to attacks on the German Parliament.
This threat group has also been involved in operation Russian Doll.
This threat groups have been involved in attacks on Bellingcat, Dutch Safety Board.

ATTRIBUTION

APT 28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT 28 has been active since at least January 2007.

AX1AL

V. IOCS

cfb46234-012a-43c8-a763-f636c056606e
b8b742d5-5dff-4f0f-bda8-0c878c1dd1e1
af36c9b3-d554-46de-9525-c05a0759a399
389c9c03-eaf4-4259-94e5-623334cea26e
c17d001c-df89-40ff-87de-e89bde9f1425
115031bf-f342-4bd0-9f9c-a5d8e1111281
d69b1fb1-f31e-49e2-9ae1-e4d5057d2142

C2

standartnevvs[.]com

novinitie[.]com, n0vinite[.]com

qov[.]hu[.]com

q0v[.]pl, mail[.]q0v[.]pl

poczta.mon[.]q0v[.]pl

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Sofacy%2C%20APT%2028%2C%20Fancy%20Bear%2C%20Sednit

Fireeye Reports