SANDWORM

AXIAL

SANDWORM TEAM

RUSSIA

UKRAINIAN ELECTRICAL COMPANIES & NOTPETYA ATTACKS

BLACK ENERGY

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON SANDWORM : ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

This threat actor targets industrial control systems, using a tool called Black Energy, associated with electricity and power generation for espionage, denial of service, and data destruction purposes. Some believe that the threat actor is linked to the 2015 compromise of the Ukrainian electrical grid and a distributed denial of service prior to the Russian invasion of Georgia. Believed to be responsible for the 2008 DDoS attacks in Georgia and the 2015 Ukraine power grid outage

II.TARGETS

Ukrainian , Georgia , France

III. ATTRIBUTION

The Sandworm Team, also known as Unit 74455, is a Russian cybermilitary unit of the GRU.

IV. TOOLS USED

Killdisk , Industroyer , NotPetya

V. METHODS USED

- Their computer attacks used some of the world's most destructive malware to date, including: KillDisk and Industroyer, which each caused blackouts in Ukraine; NotPetya, which caused nearly $1 billion in losses to the three victims identified in the indictment alone; and Olympic Destroyer, which disrupted thousands of computers used to support the 2018 PyeongChang Winter Olympics.

-SandWorm heavily leveraged PowerShell commands and scripts to discover system information, execute code, and download malware. In one instance, the group executed a malicious PowerShell script that contained versions of a credential harvesting tool. The tool operated only in memory and was not easily detectable by antivirus software.

- Many of the spearphishing emails sent by SandWorm contained malware-laced documents that required user execution to deploy.

AX1AL

VI. CAMPAIGNS

- Around December 2015 and December 2016, SandWorm attempted to destabilize Ukraine by launching cyberattacks against companies that support the country's electric infrastructure, disrupting the supply of electricity to more than 225,000 Ukrainian customers.

-SandWorm launched spearphishing campaigns targeting local government entities, political parties, and campaigns in France, including those connected with French President Emmanuel Macron's presidential campaign.

-Around June 2017, SandWorm launched its "NotPetya" malware campaign, causing hundreds of victim organizations worldwide to lose one billion dollars collectively.

- SandWorm retaliated against the 2018 Winter Olympics by launching cyberattacks against critical infrastructure after a Russian government-sponsored doping effort led to Russian athletes being unable to participate under the Russian flag.

- Around April 2018, SandWorm undermined efforts to hold Russia accountable for its use of a weapons-grade nerve agent on foreign soil by launching spearphishing campaigns against international and government organizations investigating the poisoning of a former GRU officer and his daughter.

- SandWorm defaced approximately 15,000 websites in Georgia by launching a cyberattack around October 2019.

VII. REFERENCES

1. https://www.securitymagazine.com/articles/93793-digital-shadows-maps-out-mitre-attck-to-sandworm-apts-campaign
2. https://www.helpnetsecurity.com/2020/10/20/sandworm-hackers/
3. https://threatpost.com/sandworm-apt-team-found-using-windows-zero-day-vulnerability/108815/
4. https://threatpost.com/doj-charges-6-sandworm-apt-members-in-notpetya-cyberattacks/160304/
5. https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html
6. https://www.csoonline.com/article/3455172/russias-sandworm-hacking-group-heralds-new-era-of-cyber-warfare.html