APT 28 – FANCY BEAR

ARHUM ZAHID

ADVERSARIES/VICTIMS

- Adversaries: APT 28 is linked to the Russian Military intelligence, as a result they have goals that are often related to political positions as well as gaining influence.
- Victims: History shows that they have targeted many government bodies, NATO allies, defensive operations, media, and often times we can see that these attacks are centralized towards the U.S. and or Europe.

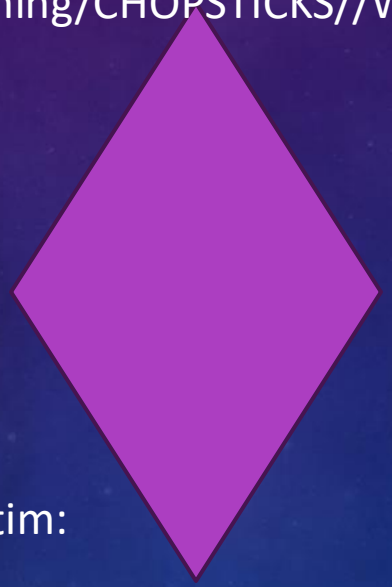
CAPABILITIES/INFRASTRUTURE

- Infrastructure: Levarage different methodologies but often we can see attacks like watering hole attacks, and spear fishing. By using different set of domains that can play and act as services that many people often use they are able to fulfill their malware and attacks onto the services/networks they need.
- Capability: Malware tools like X-Tunnel, X-Agent with a mix of spear fishing and water hole attacks and zero day exploits help with their capabilities.

DIAMOND MODEL OF INTRUSION ANALYSIS

Adversary: Location: Russia
Names: Fancy Bear
Attacks: Spear Fishing/CHOPSTICKS//Waterhole

Capabilities:
- X-Agent
-X-Tunnel
Spear Fishing
C2 Servers



Infrastructure:
hxxp://yovtube[dot]co
hxxp://defenceiq[dot]us
- Servers set up host payloads with fake news to gather info through compromised servers

Victim:
US
NATO
European Nations
EX: DNC Hack in 2016 and German Bundstag Hack

APT 28 KILL CHAIN

Reconnaissance	• Gather information on target using open source intelligence. • Identify gaps and vulnerabilities available to exploit
Weaponization	• Develop malware to deploy • Create files or websites to exploit the known vulnerabilities
Delivery	• Send spear fishing emails or leverage other attacks such as watering hole • Attach different malwares in the email and or other attacks
Exploitation	• Use malware to exploit the workstation • Leverage zero-day exploits to attack any unauthorized sources and or websites
Installation	• Install all the malware that needs to be installed i.e backdoors or remote access tools • Maintain access
Command and Control	• Establish a maintained connection • Use encryption to maintain malicious traffic
Action and Objective	• Steal sensitive data and or disrupt any current workflows • Maintain access to logs and or systems to ensure proper information is being retrieved.

CITATIONS

- 1. **CrowdStrike**. (2020). *Global Threat Report 2020*.
- [CrowdStrike Threat Reports](https://www.crowdstrike.com/resources/reports/)
- 2. **FireEye**. (2019). *APT28 Activity Report: Targeting European and U.S. Institutions*.
- [FireEye Threat Intelligence Reports](https://www.fireeye.com/current-threats/threat-intelligence-reports.html)
- 3. **Palo Alto Networks Unit 42**. (2021). *APT28 Technical Analysis: APT Attack Strategies and Tools*.
- [Unit 42 Threat Intelligence](https://unit42.paloaltonetworks.com/)
- 4. **MITRE ATT&CK**. (n.d.). *APT28 - Tactics, Techniques, and Procedures (TTPs)*.
- [MITRE ATT&CK - APT28](https://attack.mitre.org/groups/G0007/)