APT28 (Fancy Bear) Adversary Profile

APT28, a Russian organization, known for their cyberattacks in American elections which notably included Hillary Clinton's campaign, the Democratic National Committee, and the Democratic Congressional Campaign in 2016. The group uses spear phishing mechanisms to gain access to campaign information further using brute force to spray passwords for additional access. Despite the indictment of twelve Russian individuals from the group for their involvement in the 2016 election, the group is still active as it poses threats to U.S. national security and Microsoft in its exploitation of CVE-2022-38028.

Tactics, Techniques & Procedures

1. Initial access (T1669): Access obtained is initially through connecting to wireless networks alongside use of spear-phishing and further exploitation of system vulnerabilities
2. Execution (T1059.003): utilize windows command shell to release payload
3. Persistence (T1547.001): adding program to registry run key and startup folder
4. Defense evasion (T1211): exploit vulnerabilities (i.e. CVE-2015-4902) to bypass system security
5. Credential access (T1003.003): NTDS file utilized to export Active Directory database

Tools

- XAgentOSX: trojan for malware distribution
- ADVSTORESHELL: spying backdoor for espionage
- reGeorg: open-source shell used as proxy to bypass firewall
- USBStealer: malware used to extract info in air-gapped networks

Victims

- Government agencies
- Political organizations (DNC)
- Journalists and media
- National infrastructure (Europe)

Campaigns

- 2016 U.S. election: Democratic National Committee breach and email leak
- Attacks on German Bundestag (2015)
- Cyberattacks on Ukraine (2015-present)

Recommendations

1. Require VPN usage when connected with unfamiliar networks with additional implementation of strong network segmentation and access points

2. Apply Microsoft AppLocker to limit apps ability to run
3. Leverage endpoint detection and response (EDR) solutions
4. Utilize Microsoft Defender Vulnerability Management
5. Set SIEM rules for Microsoft Sentinel to identify unauthorized logins

Sources

1. U.S. Department of Justice. *(2018).* **Grand Jury Indictment: United States v. Viktor Borisovich Netyksho et al.** https://www.justice.gov/archives/opa/page/file/1098481/dl?inline
2. MITRE ATT&CK. *(n.d.).* **APT28 (Fancy Bear) – G0007 Threat Group Profile.** https://attack.mitre.org/groups/G0007/
3. CISA. *(2023).* **Russian FSB Cyber Actor Identified Exploiting Outlook Vulnerability.** Advisory AA23-108A. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108
4. BBC News. *(2018, July 13).* **Russia Hack: US Indicts 12 Russian Intelligence Officers.** https://www.bbc.com/news/world-us-canada-44825345
5. The Hacker News. *(2024, May).* **Microsoft Outlook Flaw Exploited by Russian Hackers to Breach Government Agencies.** https://thehackernews.com/2024/05/microsoft-outlook-flaw-exploited-by.html