

Advanced Persistent Threat (APT) 28

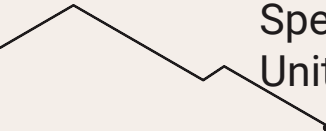
•
Fancy Bear





About APT28

APT group Fancy Bear has been operating since at least 2008. It focuses mainly on cyber espionage. The group tends to leak stolen data for Russia's political interests.



According to an indictment by the United States Special Counsel (2018) Fancy Bear is, in fact, GRU Unit 26165.

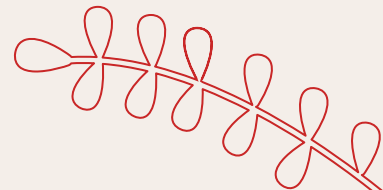




01 Motivations

Motivations for attacks by APT28

01010101
01010101



Motivations



● Russian Political Interest

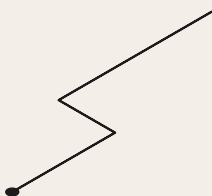
APT28 has been linked to Russia. Many of its attacks have been in retaliation of any move made against Russian interest. Including attacking the Olympics in 2018 after Russia was banned.

● Money

Like many cyber attacks, money is a factor. APT28 has attacked private companies with RansomWare attacks, demanding Bitcoin as payment.

● Military information

Fancy Bear has attacked the DNC, White House, and NATO. Always looking for data to exfiltrate away, APT28 has a history of attacking defense ministries.



Tactics, Techniques and Procedures(TTPs)

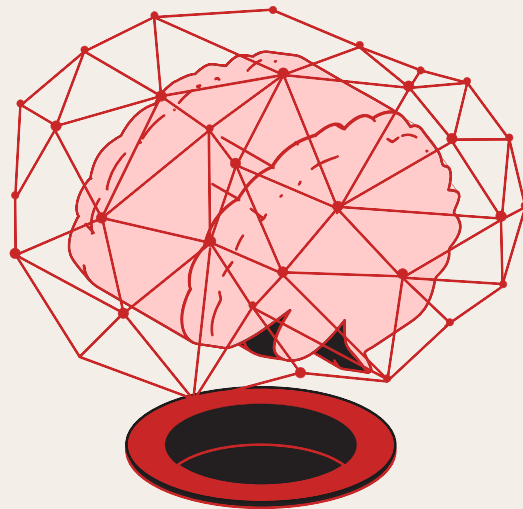


Tactics, Techniques and Procedures (TTPs)

- Phishing and credential harvesting using spoofed websites closely resembling legitimate organizations
- Phishing emails contain shortened links to avoid spam filters and are typically sent on Mondays and Fridays
- Code is regularly updated and obfuscated to avoid detection
- Primary implant is a RAT known as Xagent, which Keylogs and exfiltrates data
- X-TUNNEL is a network tunneling tool used to traverse the network and pivot. This is used to create a secure tunnel to their external command and control server.
- Zero - days. Microsoft has identified Fancy Bear using numerous Zero- days which would indicate a large team of programmers.

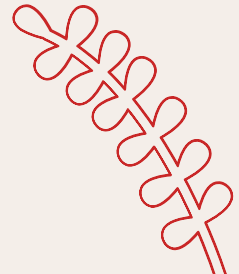
Famous Attacks

A few of Fancy Bear's most famous attacks



International Olympic Committee (2018)


On January 10, 2018, Fancy Bear leaked stolen International Olympic Committee and U.S. Olympic Committee emails dated from late 2016 to early 2017. They were leaked in what seemed to be retaliation for banning Russian from the 2018 Winter Olympics. Note that Russia was banned as a sanction against their systematic doping program. The mode of attack is not known, but is suspected to be phishing.



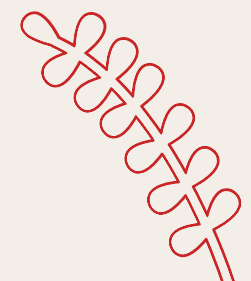
Democratic National Committee (2016)



In the first quarter of 2016 Fancy Bear carried out a spear phishing campaign. On March 10, phishing emails that were mainly directed at old email addresses of 2008 Democratic campaign staffers began to arrive. The next day, after receiving an updated email list, phishing attacks were carried out to high level party officials. Podesta's Gmail account was breached and 50k emails stolen.



On June 14, CrowdStrike released a report publicizing the DNC hack and identifying Fancy Bear as the culprits.



Bibliographical references

- Editorial Team. (2019, February 12). Fancy Bear Hackers (APT28): Targets & Methods | CrowdStrike. CrowdStrike.Com. <https://www.crowdstrike.com/blog/who-is-fancy-bear/>
- Wikipedia contributors. (2022, April 19). Fancy Bear. Wikipedia. https://en.wikipedia.org/wiki/Fancy_Bear#Characteristics_and_techniques
- Indicators of compromise for malware used by APT28. (n.d.). National Cyber Security Centre. <https://www.ncsc.gov.uk/news/indicators-of-compromise-for-malware-used-by-apt28>

Continued on next slide



Bibliographical references

- The story of the four bears: Brief analysis of APT groups linked to the Russian government. (n.d.). Cyber Security Help. <https://www.cybersecurity-help.cz/blog/2507.html>
- Team, T. R. (2021, November 2). Russian Cyber Operations on Steroids. ThreatConnect | Risk-Threat-Response. <https://threatconnect.com/blog/fancy-bear-anti-doping-agency-phishing/>
- Newman, L. H. (2020, October 16). Fancy Bear Imposters Are on a Hacking Extortion Spree. Wired. <https://www.wired.com/story/ddos-extortion-hacking-fancy-bear-lazarus-group/>

Continuation



Thanks!

Do you have any questions?

Techtony2013@gmail.com

917•518•0103

<https://www.linkedin.com/in/techtony/>



CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon** and infographics & images by **Freepik**

