Introduction to
Threat Intelligence

JARED GRAY
Carson Chubbs

WHAT IS THREAT INTELLIGENCE?

Threat intelligence is data that is **collected, processed, and analyzed** to understand a threat actor's **motives, targets, and attack behaviors**.

https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

WHY DOES IT MATTER?

In the world of cybersecurity, advanced persistent threats (APTs) and defenders are constantly trying to outmaneuver each other.

Data on a threat actor's next move is crucial to proactively tailoring your defenses and preempt future attacks.

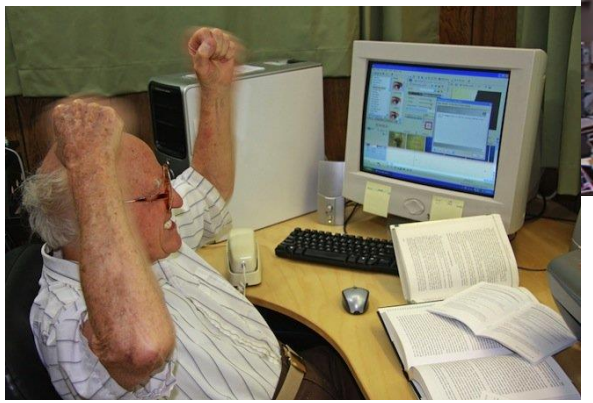
Threat intelligence is important for the following reasons:

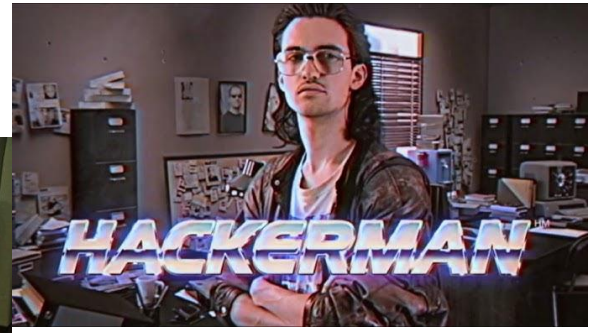
- **sheds light on the unknown,** enabling security teams to make better decisions
- empowers cyber security stakeholders by **revealing adversarial motives** and **their tactics, techniques, and procedures** (TTPs)
- helps security professionals **better understand the threat actor's decision-making process**
- **empowers business stakeholders**, such as executive boards, CISOs, CIOs and CTOs; to invest wisely, mitigate risk, become more efficient and make faster decisions

https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

Type of Threat Actors

- Hacktivists
- Cyber Criminals/Syndicates
- Insiders
- Script Kiddies
- Advanced Persistent Threats (APT)





https://www.proofpoint.com/uk/threat-reference/threat-actor

Threat vectors

Email

Social Media

Direct Access

Wireless Networks

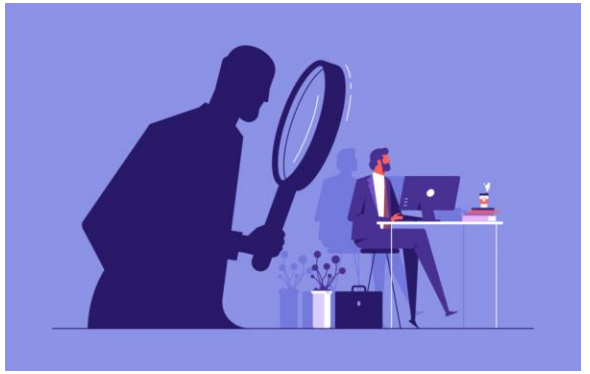
Removeable Media

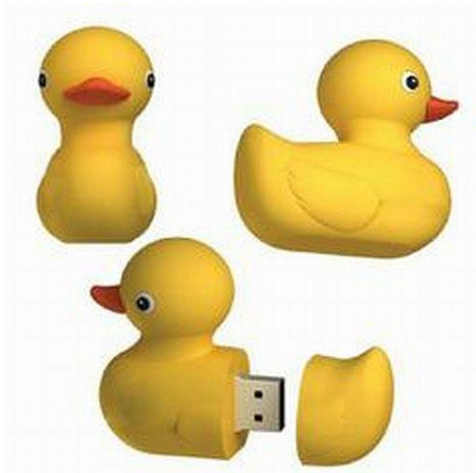
Cloud

3rd Parties

Social Engineering

Insider Threats



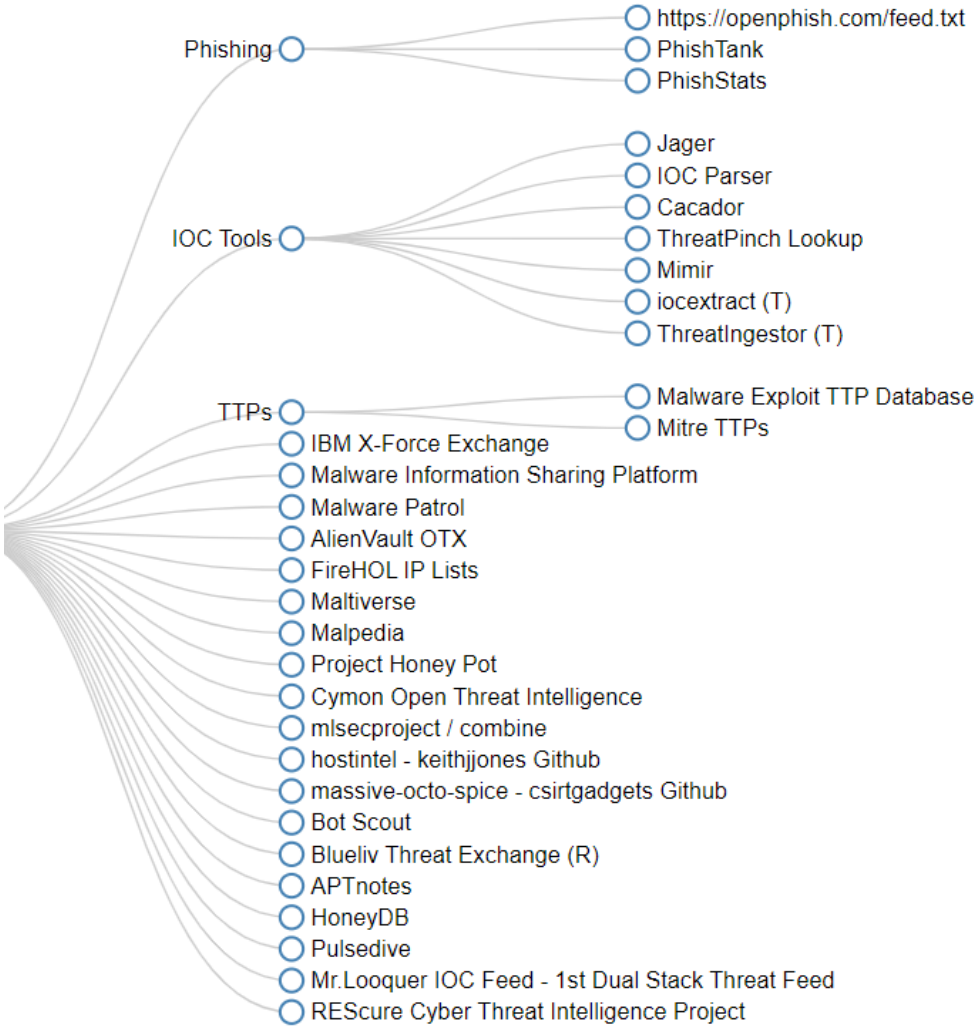


Osint

- Open-Source Intelligence: Gathering and processing already available online to gain insight
  - Carson's favorite CTF category
- Used on both ends
  - Attackers use it to make attacks more efficient
  - Defenders use it to monitor trends

Osint Framework

- Tools available for:
  - Identifying phishses
  - Determining IoC's
  - Researching malware



https://osintframework.com/

THREAT INTELLIGENCE LIFECYCLE

- The intelligence lifecycle is a process to transform raw data into finished intelligence

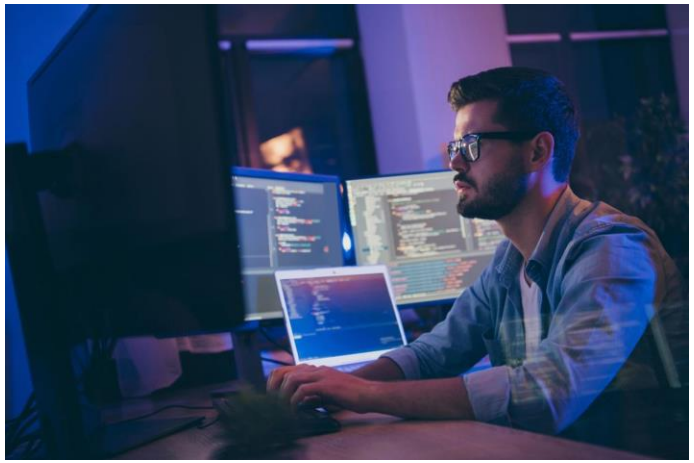
THREAT INTELLIGENCE LIFECYCLE

- The intelligence lifecycle is a process to transform raw data into finished intelligence
- The intelligence cycle provides a framework to enable teams to optimize their resources and effectively respond to the modern threat landscape.

https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

Threat Intelligence as a career

- Researchers
  - Found on vendor side (Cyber companies)
  - Also common in Government
  - Keep track of APTs, know motivations, targets, techniques
- Analysts
  - Found on customer side
  - Receive information and sort it according to sector and threat type
- Skills needed:
  - DFIR
  - Malware Analysis
  - Reverse Engineering
  - Penetration Testing



EMPHASIS MEETINGS

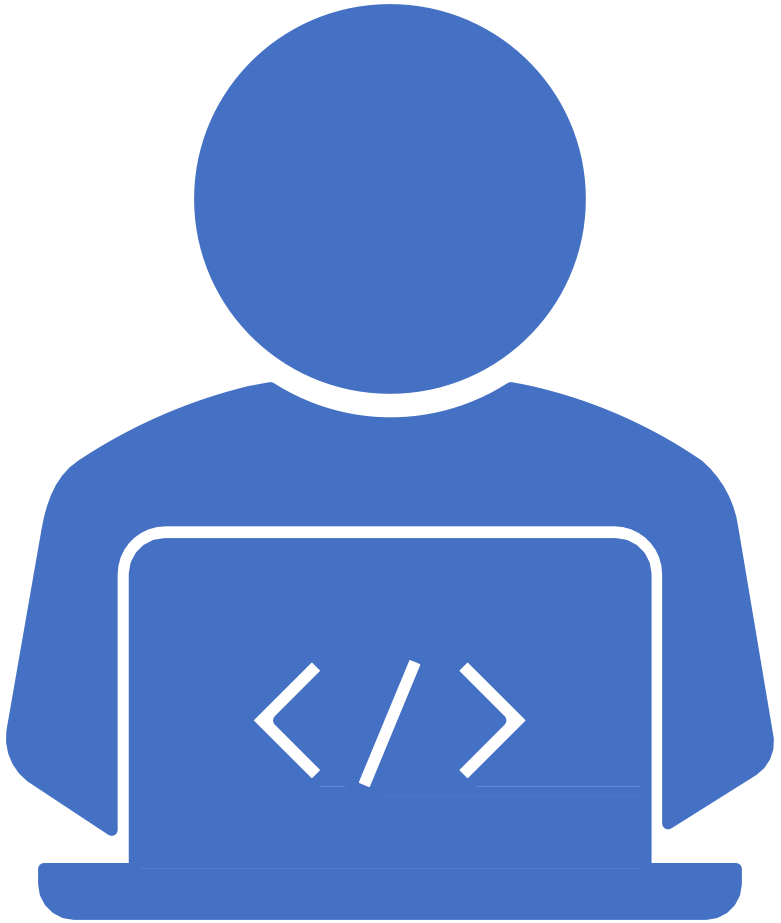
- OSINT
- Advanced Intelligence Gathering: Beyond OSINT
- Mitre Attack Framework
- Dark Web Monitoring
- Cyber Kill Chain

Activity Time

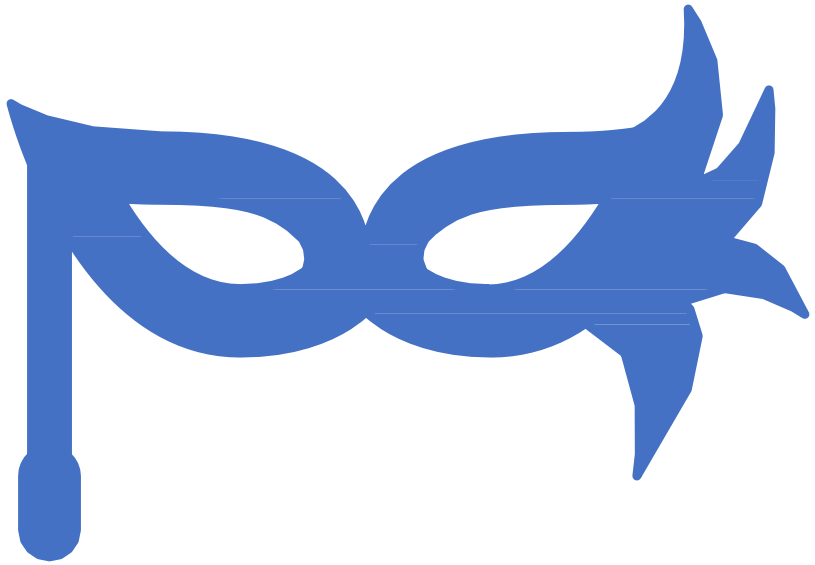
Who are these Hacker groups?

For a 100 points

- **This notorious hacker group is known for conducting cyber-activism and protests against various organizations and governments. Who are they?**



Anonymous



Anonymous is often associated with wearing a specific mask. What is the name of that mask?

For 200 points

The Guy Fawkes Mask

- The illustrator found inspiration for the mask from Guy Fawkes, who tried to blow up the Houses of Parliament in the 1605 Gunpowder Plot. Anonymous donned the mask in 2018 as they protested against the Church of Scientology, leading to other hacking groups using masks to hide their identity.

For 300 points

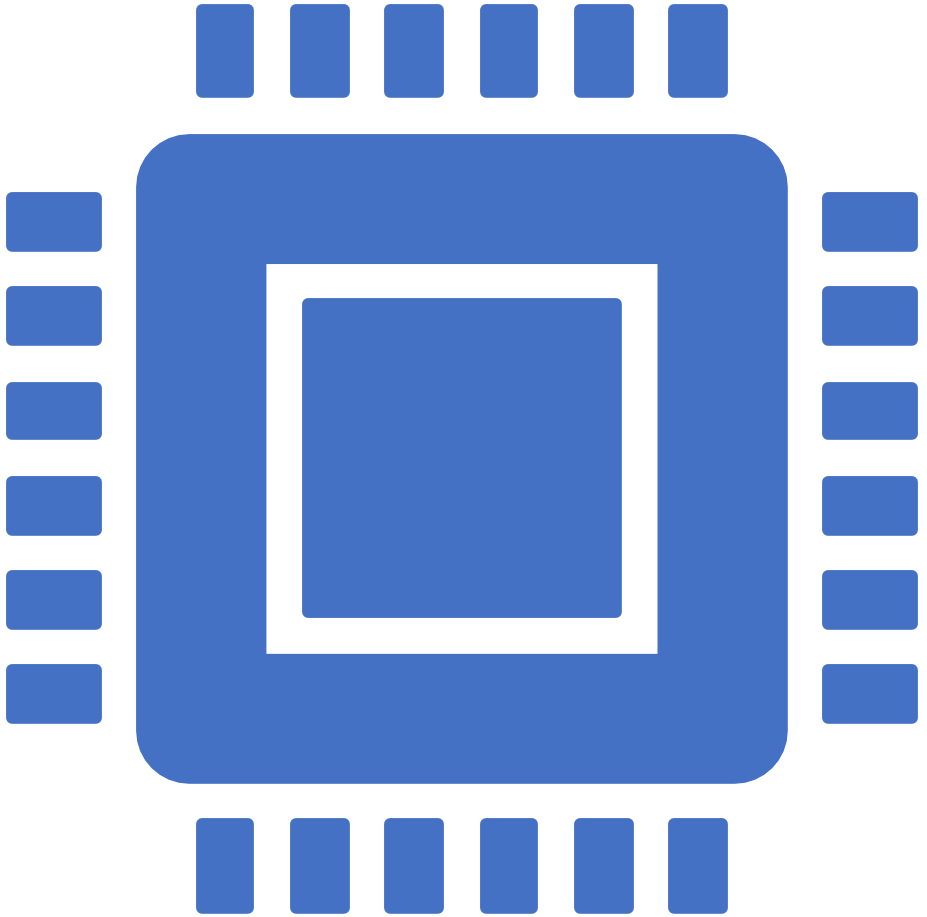
- In what year did Anonymous gain widespread attention for their actions against the Church of Scientology?

In 2008

- The project was publicly launched in the form of a video posted to YouTube, "Message to Scientology", on January 21, 2008. The video states that Anonymous views Scientology's actions as Internet censorship, and asserts the group's intent to "expel the church from the Internet".

For 400 points

- Anonymous has been involved in various high-profile cyber-attacks. Name one electronics organizations that they targeted.



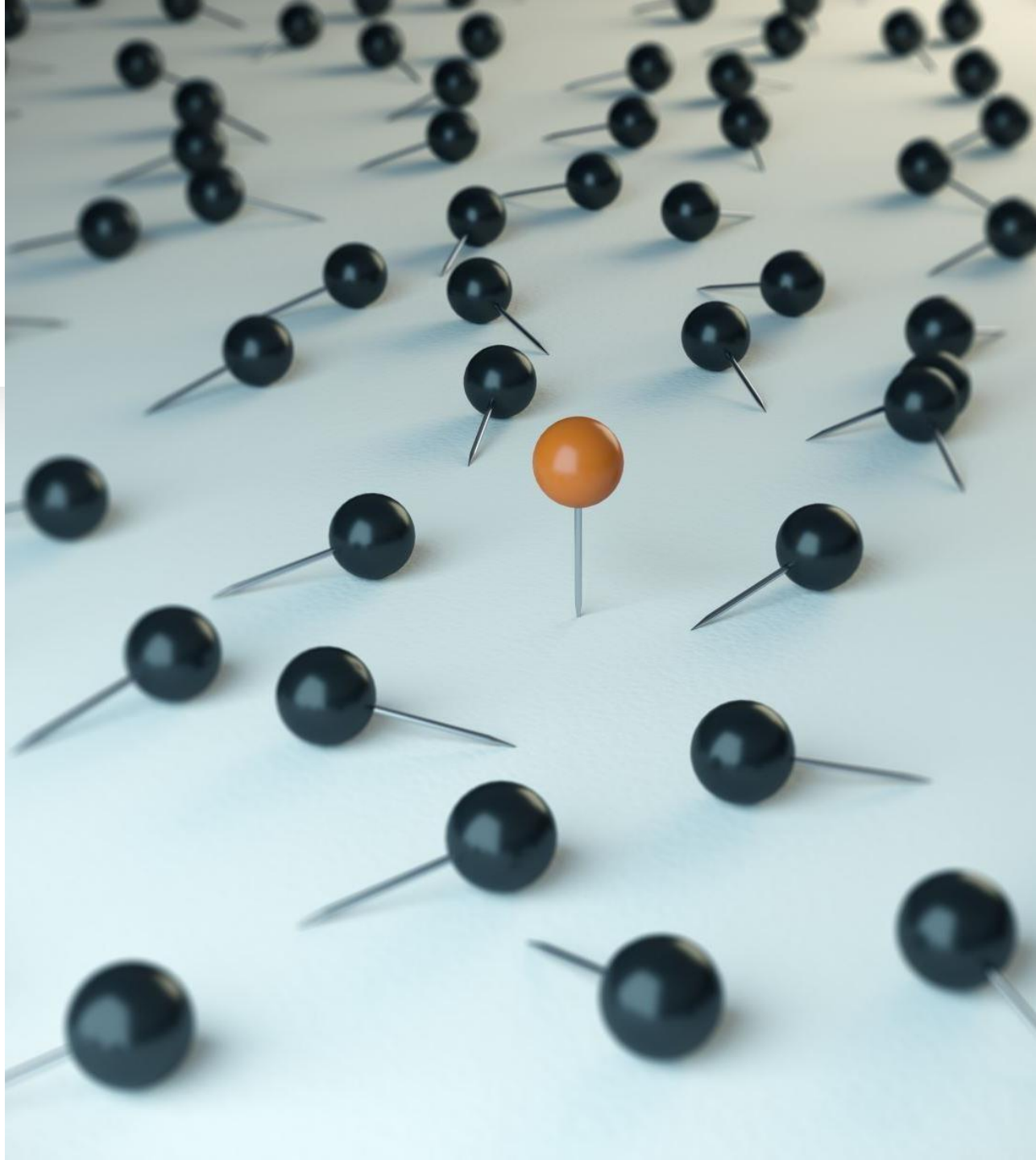
Sony - 2011

For 500 points

When was the last appearance of Anonymous?

In 2022

- They declared war against Russia and are responsible for hacking several Russian state TVs, Twitter account, even the yacht belonging to Vladimir putting was reportedly hacked.



For 100 points

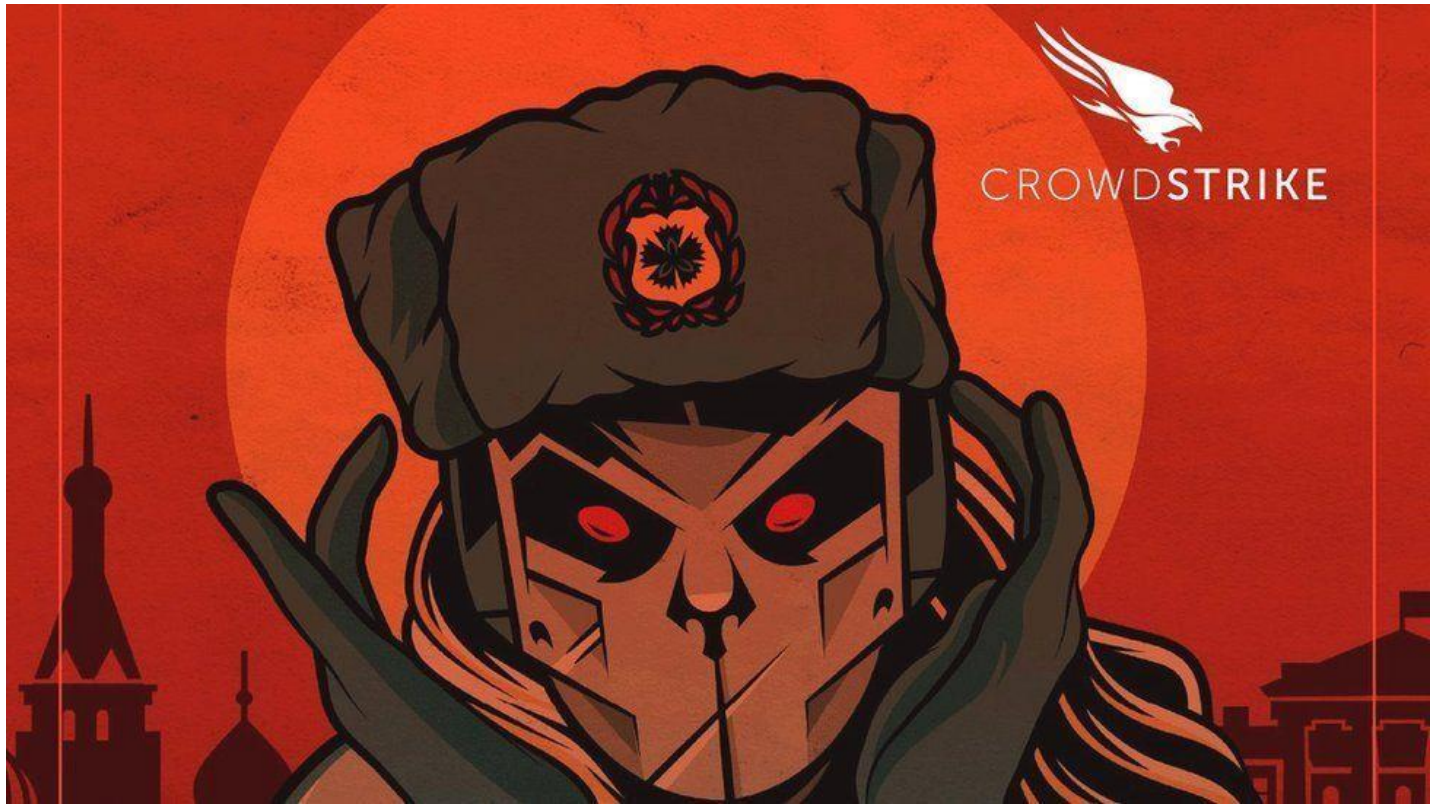
- Which is a cyber-espionage group believed to be associated with Russia?

APT29- Cozy Bear

Which threat actor group is Apt29 often associated with?

For 200 points

APT 28- Fancy Bear



For 300 points

- Apt29 is known for utilizing various malware variants. Name one of the well-known malware tools associated with them.

For 400 points

- In 2016, Apt29 was accused of being involved in cyber-attacks targeting what major U.S. political organization?

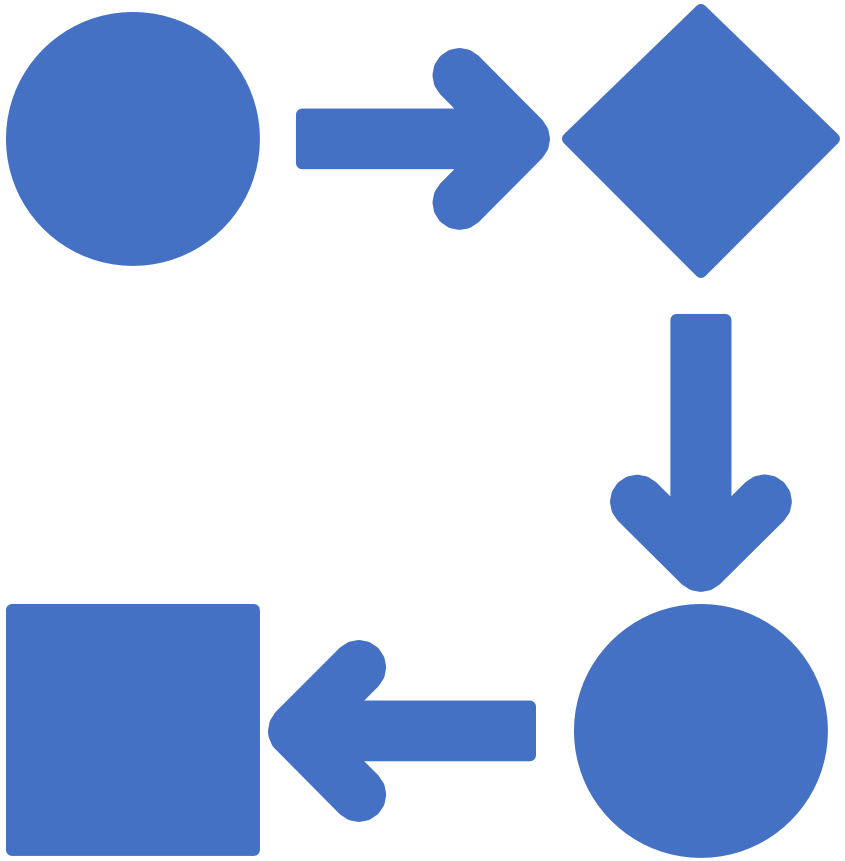
Democratic National Committee (DNC)

For 500 points

- What was the name of the of the campaign targeting ministries of foreign affairs in European countries in 2017 that APT 29 did?

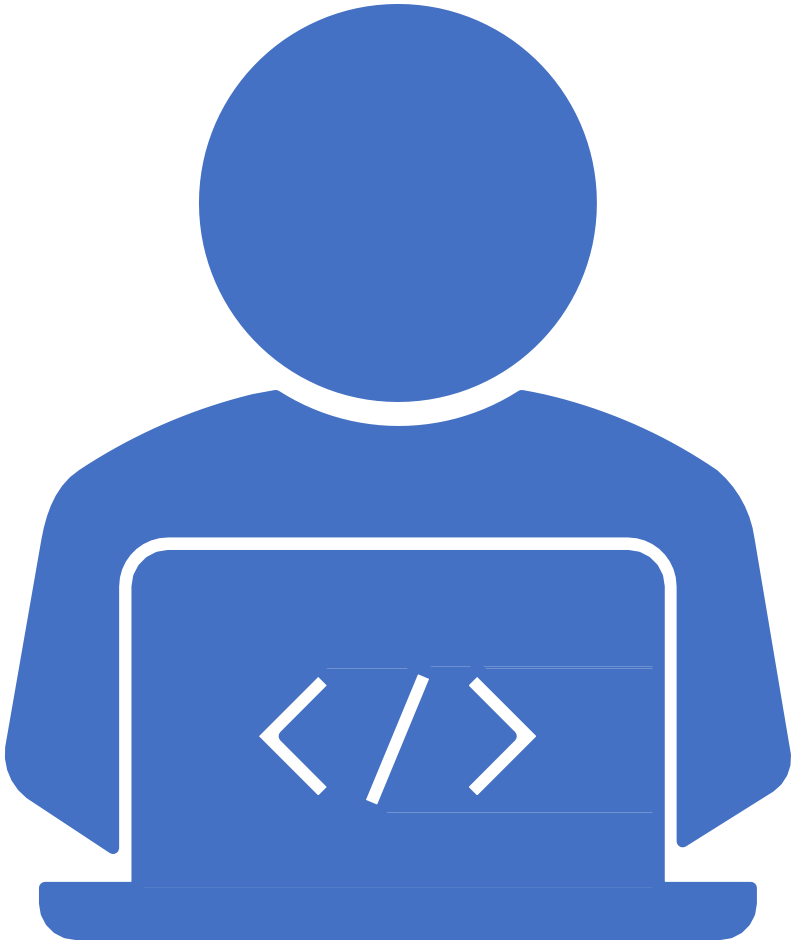
Operation GhostSecret

- APT29 utilized advanced techniques such as leveraging compromised infrastructure, utilizing PowerShell scripts for lateral movement, and employing a variety of custom and third-party tools for reconnaissance and data exfiltration.



For 100 points

- Which hacking group is believed to be associated with North Korea?



Lazarus Group

For 200 points

- Lazarus Group gained fame for its involvement in cyber-attacks targeting what type of organizations?

Financial institutions and cryptocurrency exchanges

For 300 points

What other names is Lazarus Group known by in the cybersecurity community?

Hidden Cobra and Guardians of Peace

For 400 points

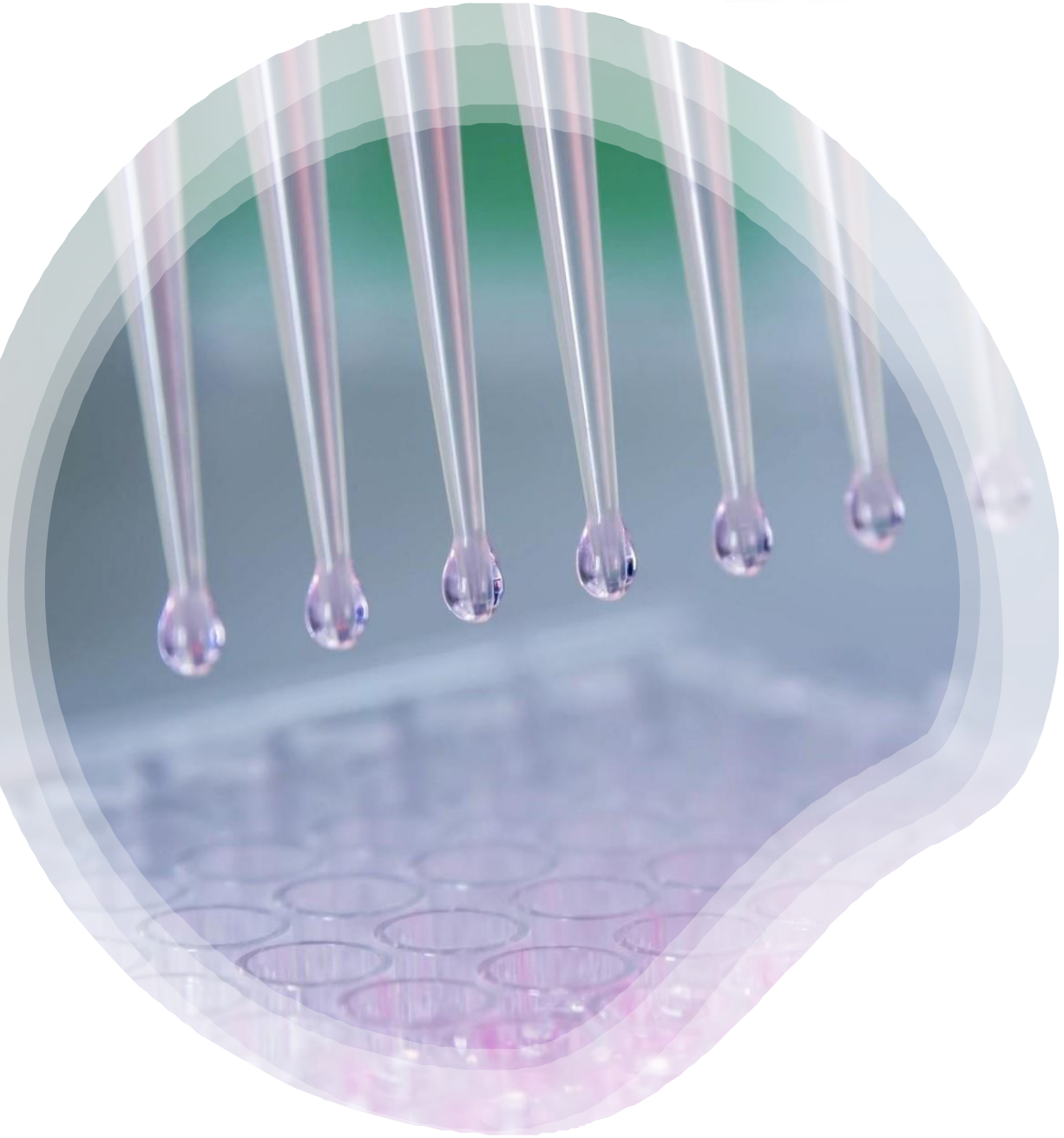
- Apart from using malware and ransomware, Lazarus Group has shown proficiency in another type of attack technique. What is it, and can you provide an example?

Spear-Phishing

- An example could be the targeted phishing emails used in the Bangladesh Bank heist.

For 500 points

- In 2020, Lazarus Group was associated with a series of cyber-attacks targeting organizations involved in COVID-19 vaccine research. What was the codename given to this campaign?



Operation Warp Speed

- The objective was likely to gather intelligence related to COVID-19 vaccine research.

Thanks for playing ☺