

# Intro to Threat Intelligence

---

By Kedric Salisbury

BYU CSA

# What is Threat Intelligence?

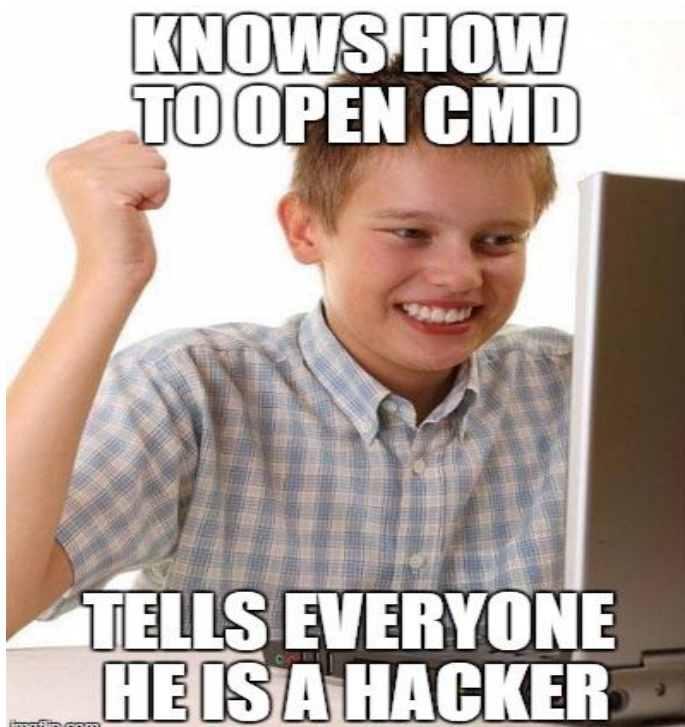






# Threat Intelligence

- Threat intelligence is the collection, analysis, and dissemination of information about potential cybersecurity threats.
- Importance:
  - Proactive Defense
  - Risk Mitigation
  - Incident Response Enhancement
- Real-world example:
  - Phishing campaigns with TTPs (tactics, techniques, and procedures)
  - Lazarus Group (Advanced Persistent Threat from North Korea) NFT phishing websites



## Classifications

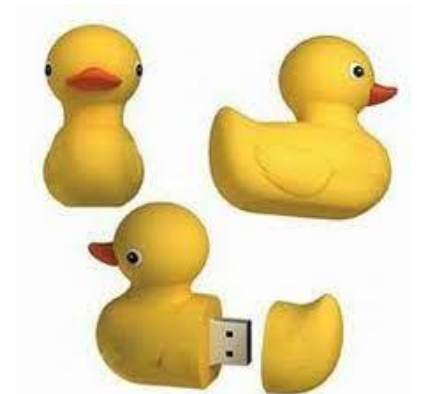
- Script kiddies
- Hacktivists
- Criminal Syndicates
- Advanced Persistent Threats (APTs)
- Insiders
- Competitors





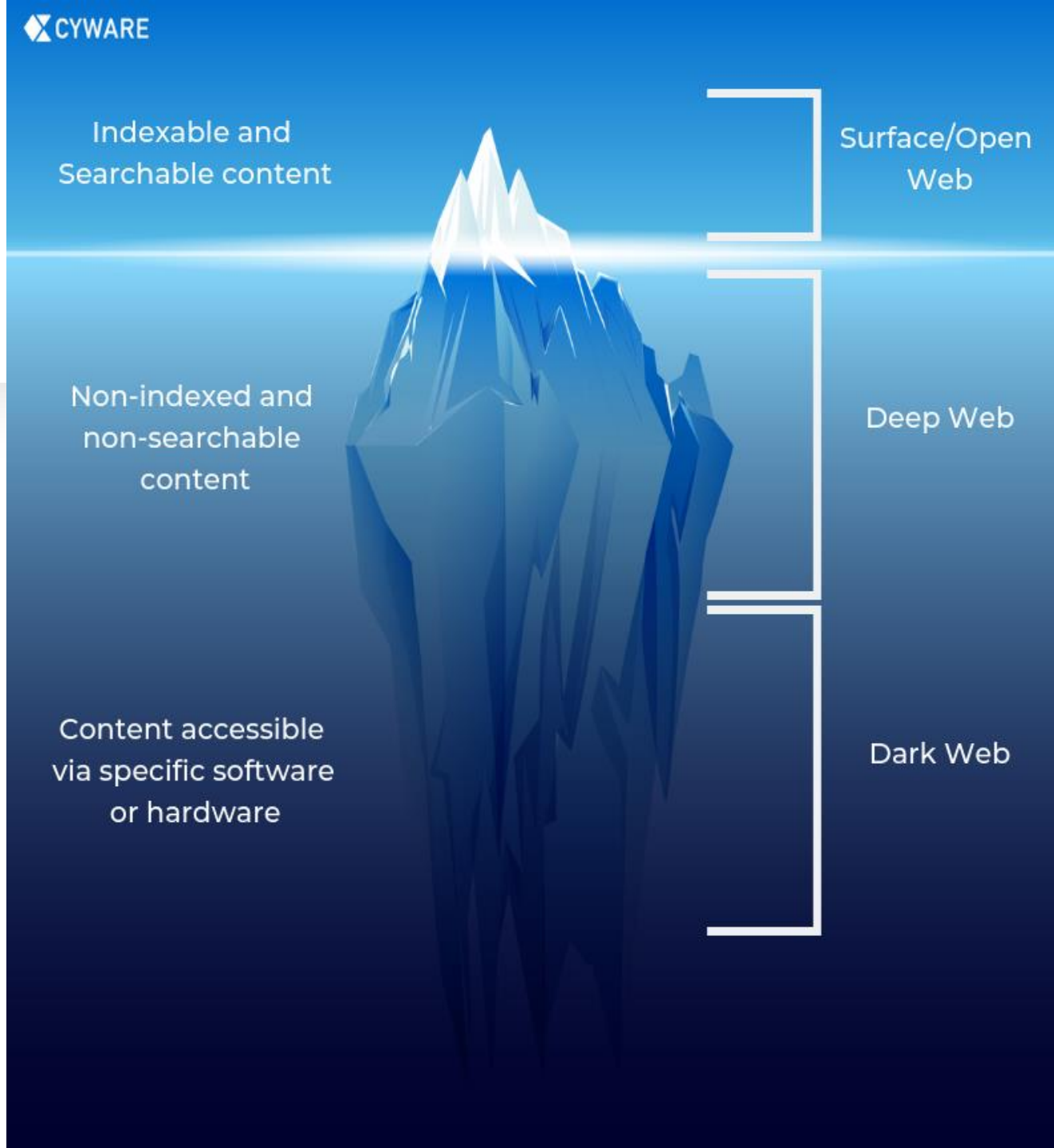
# Threat Vectors

- Email and Social Media
- Direct Access
- Wireless Networks
- Removable Media
- Cloud
- Third-Party Risks



# Sources

- Open Source
- Commercial
- Government
- Internal Data
- Dark Web
- Rated on Reliability and Trustworthiness



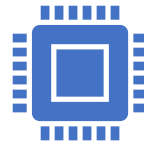
# Threat Intelligence Lifecycle



Planning and  
Direction



Collection



Processing and  
Analysis



Dissemination



Feedback and  
Improvement



# Application

Threat Analyst

Security Consultant

Incident Responder

Cybersecurity Engineer

Threat Researcher

Information Security Manager

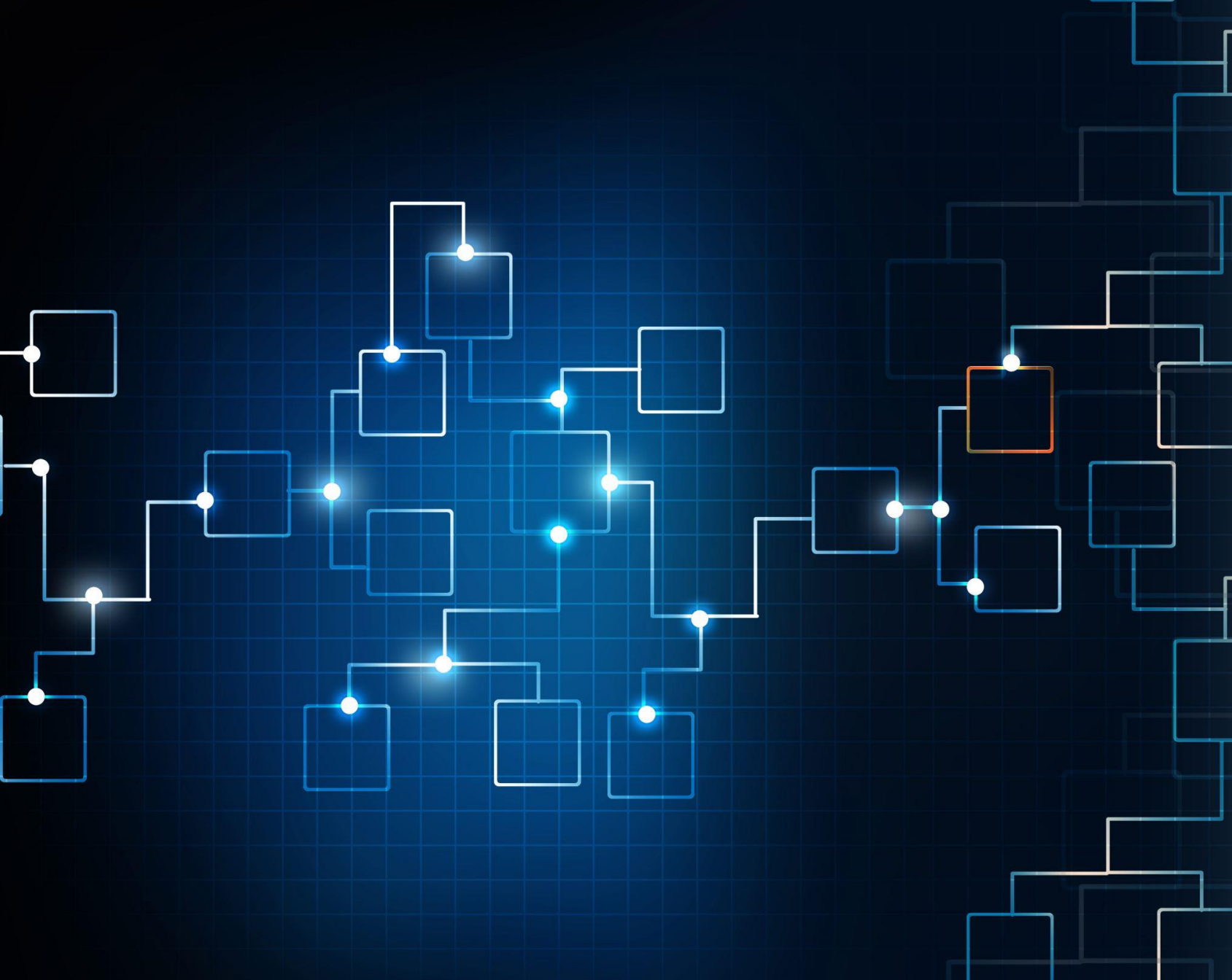
Cyber Threat Intelligence Analyst

Security Operations Center (SOC) Analyst

Penetration Tester (Ethical Hacker)

Cybersecurity Policy Analyst






# Threat Intelligence Emphasis Meetings

1. Basics of Threat Intelligence
2. Intelligence Collection and Analysis
3. Dark Web Monitoring
4. TTPs and APTs

# Activity Suggestion



[About](#) ▾ [Initiatives](#) ▾ [Supporters](#) ▾ [Blog](#) ▾ [Shop](#)


[Get Involved](#)

## We crowdsource OSINT to help find missing people.

Become a Part of the Solution

Trace Labs is a nonprofit organization whose mission is to accelerate the family reunification of missing persons while training members in the tradecraft of open source intelligence (OSINT).

[Get Involved](#)





Questions or  
Suggestions?

# Activity Time



---

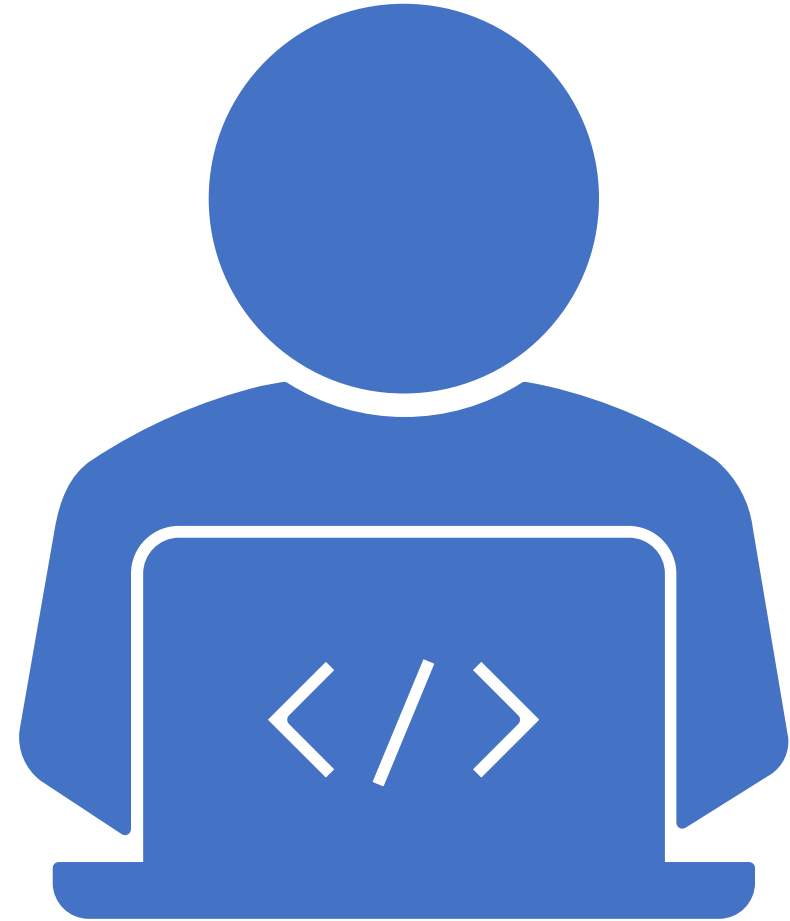
**Who are these Hacker groups?**



# 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?



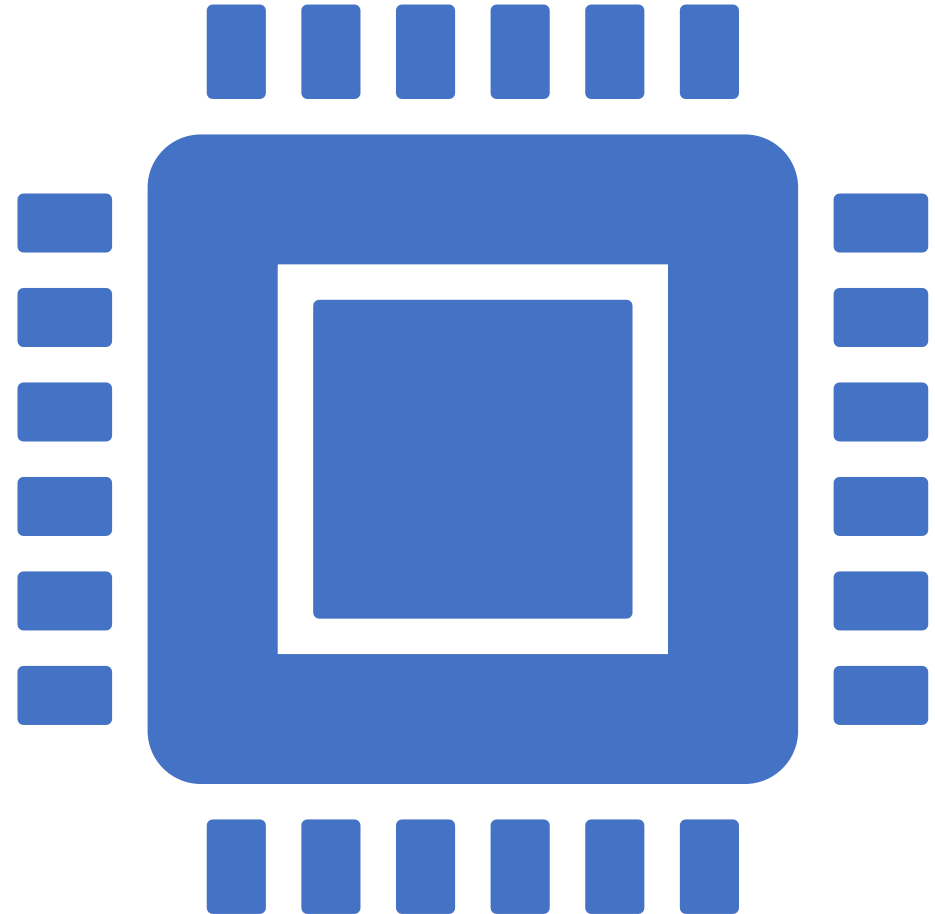
# In 2008

- 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.



The image features decorative curved lines in the corners. In the top right corner, there is a thick, multi-layered arc in shades of green and blue. In the bottom left corner, there is a similar thick, multi-layered arc in shades of green and blue.

# SONY

Sony - 2011



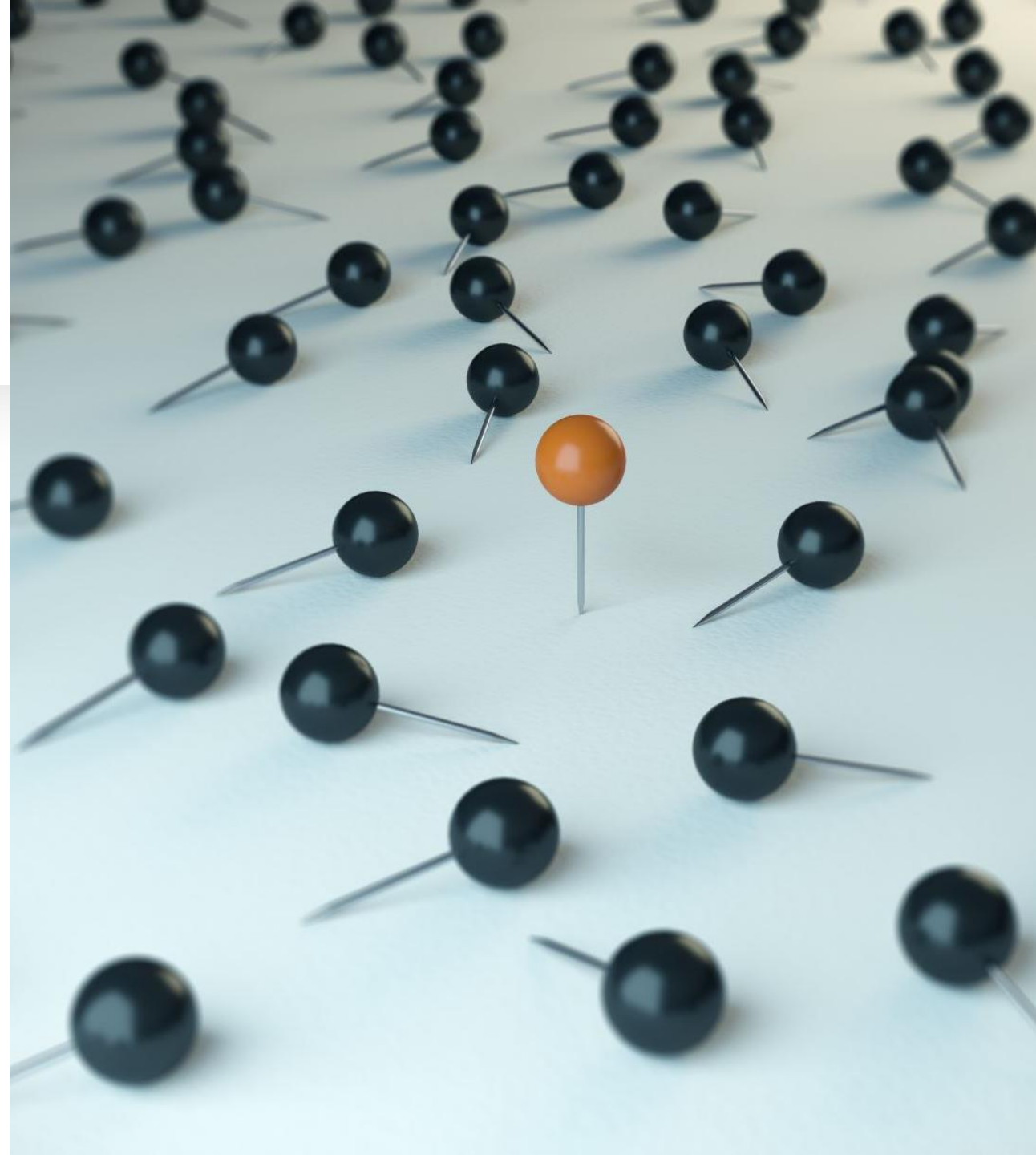


For 500 points

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

---

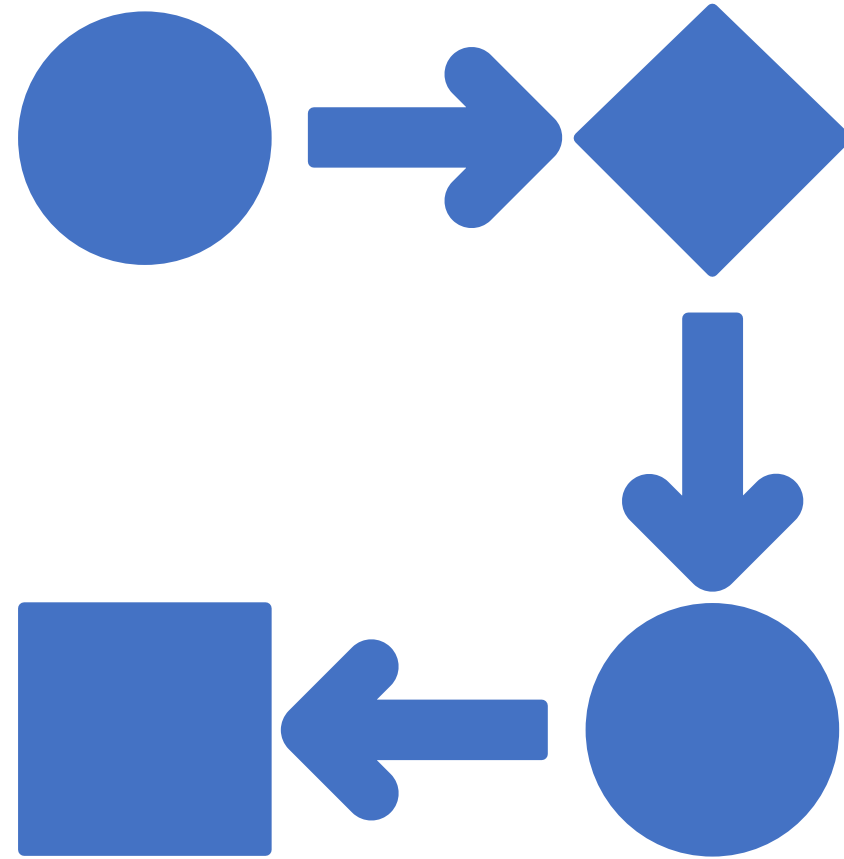
- What was the name of the of the campaign targeting ministries of foreign affairs in European countries in 2017 that APT 29 did?



# Operation GhostSecret

---

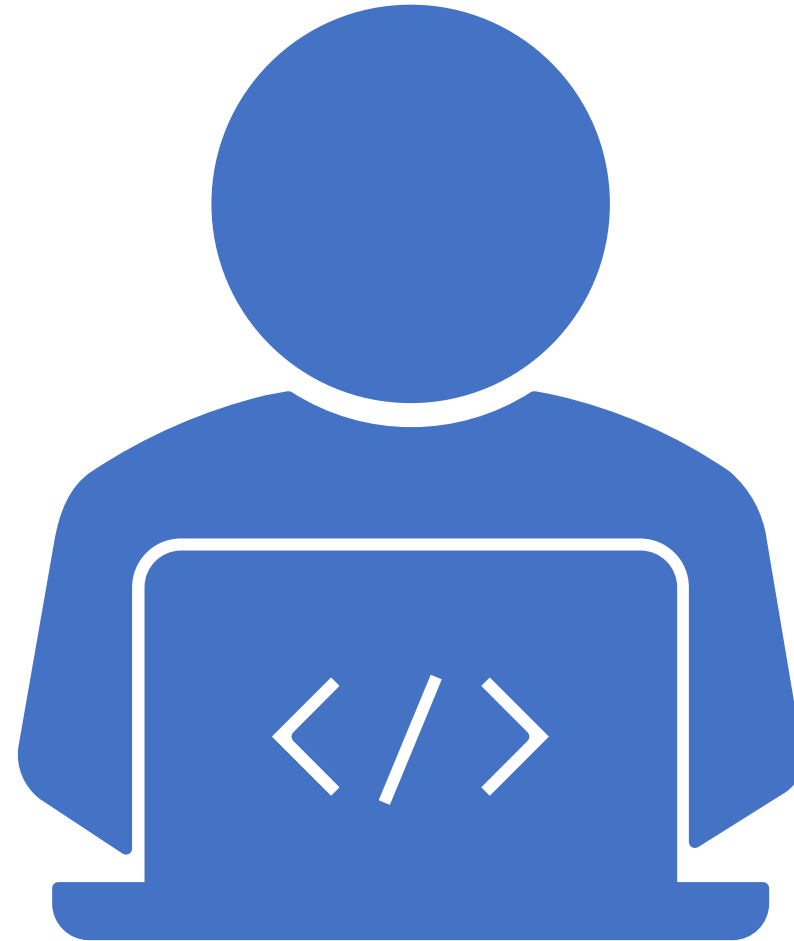
- APT29 utilized advanced techniques such as leveraging compromised infrastructure, utilizing PowerShell scripts for lateral movement, and employing a variety of custom and third-party tools for reconnaissance and data exfiltration.



# 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

---

What other names is Lazarus Group known by in the cybersecurity community?  
For 300 points



# Hidden Cobra and Guardians of Peace



# For 400 points

---

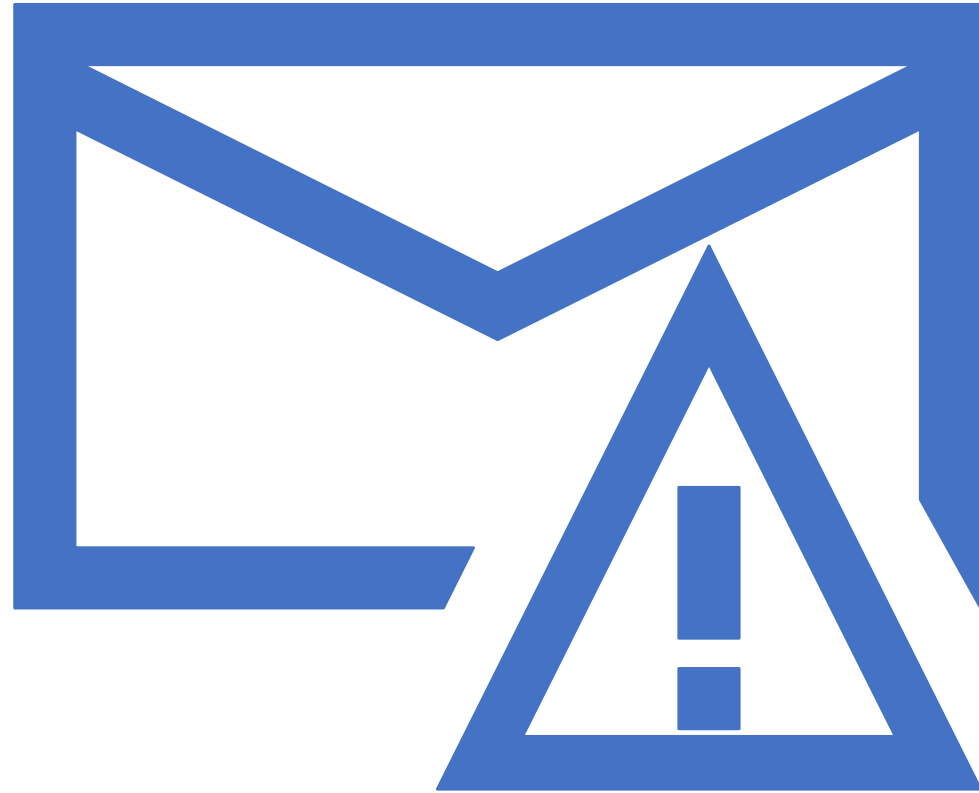
- Apart from using malware and ransomware, Lazarus Group has shown proficiency in another type of attack technique. What is it, and can you provide an example?



# Spear- Phishing

---

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



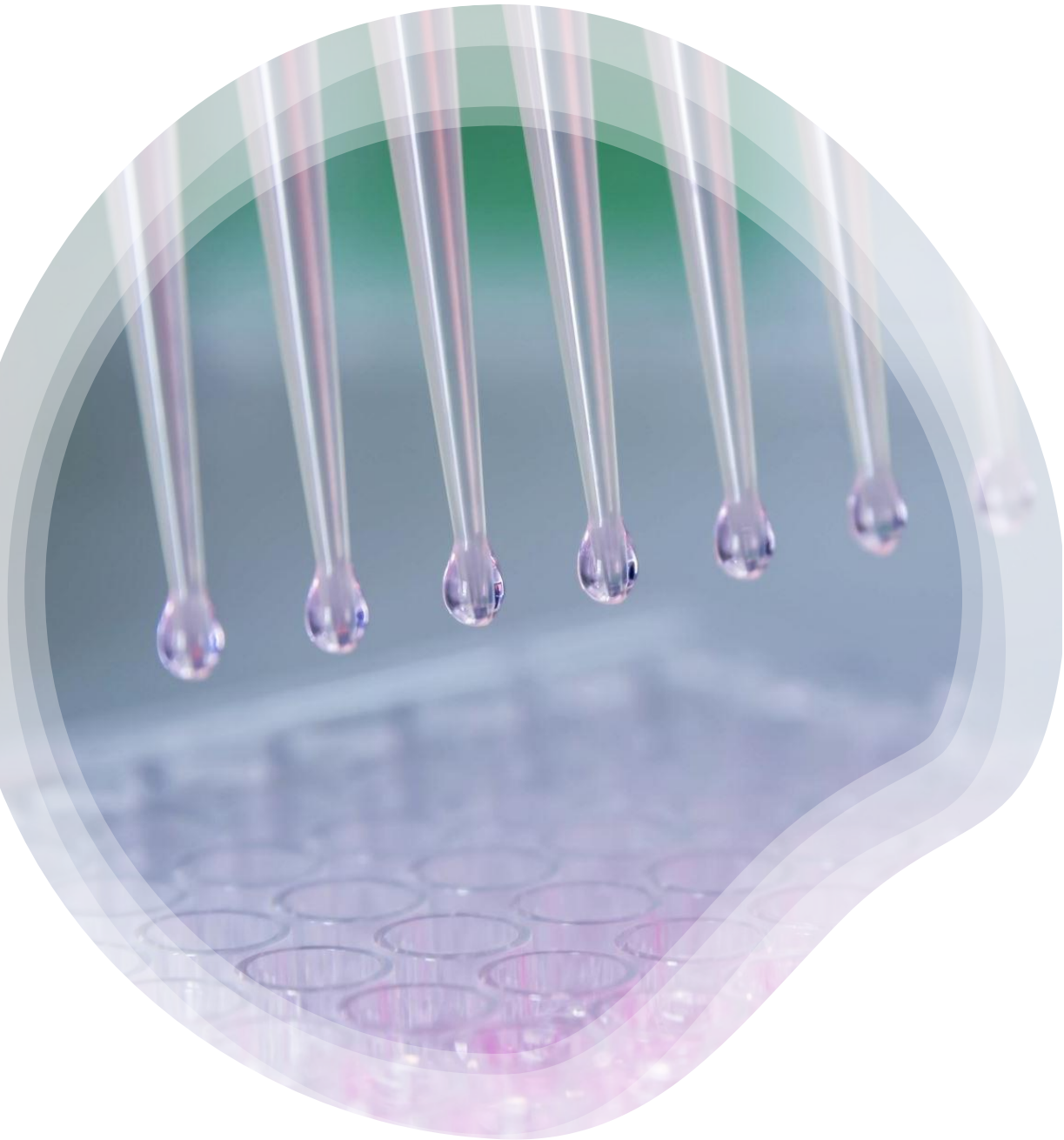


# For 500 points

---

- 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.

I hope you enjoyed  
the game 😊

