Q 1. What was the dominant ransomware family that impacted the healthcare industry in 2020?

Question 1 10 pts

What was the dominant ransomware family that impacted the healthcare industry in 2020?

- ○ Labyrinth
- ○ CryptoLocker
- ○ CryptoFreeze
- ○ Maze

Maze.

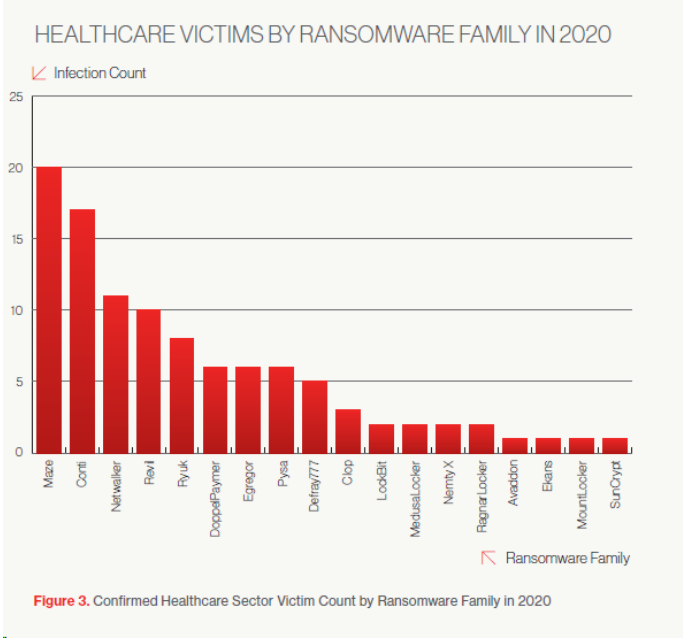


Figure 3. Confirmed Healthcare Sector Victim Count by Ransomware Family in 2020

Q 2. Which industry was targeted with the highest number of ransomware-associated data extortion operations?

Question 2 — 10 pts

Which industry was targeted with the highest number of ransomware-associated data extortion operations?

- ○ Agriculture
- ○ Industrial and Engineering
- ○ Construction
- ○ Education

Industrial and Engineering

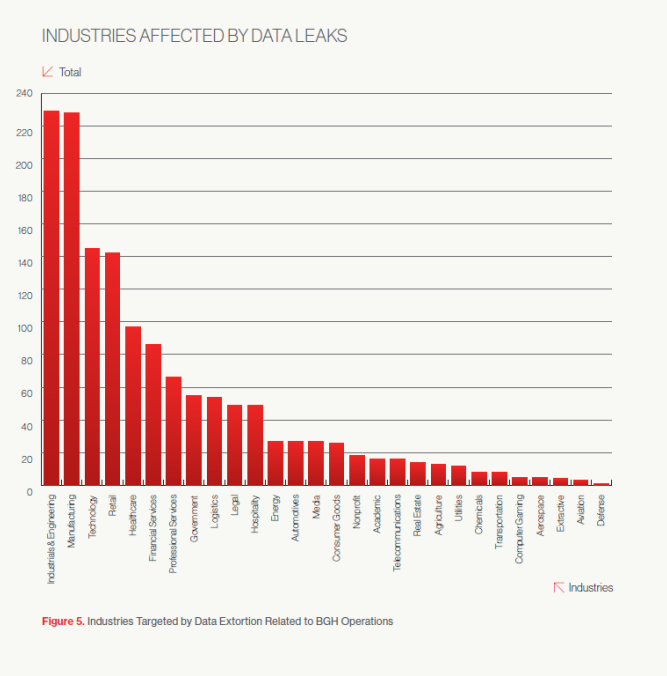
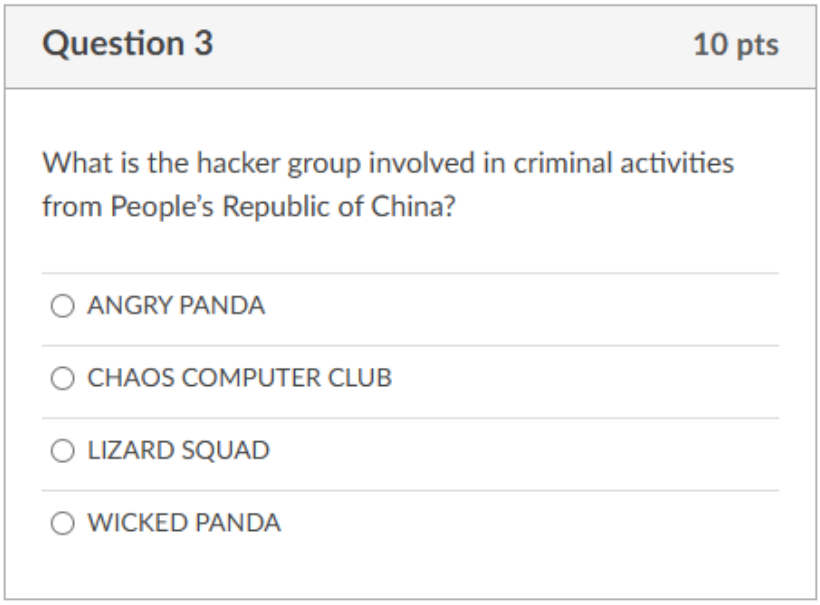


Figure 5. Industries Targeted by Data Extortion Related to BGH Operations

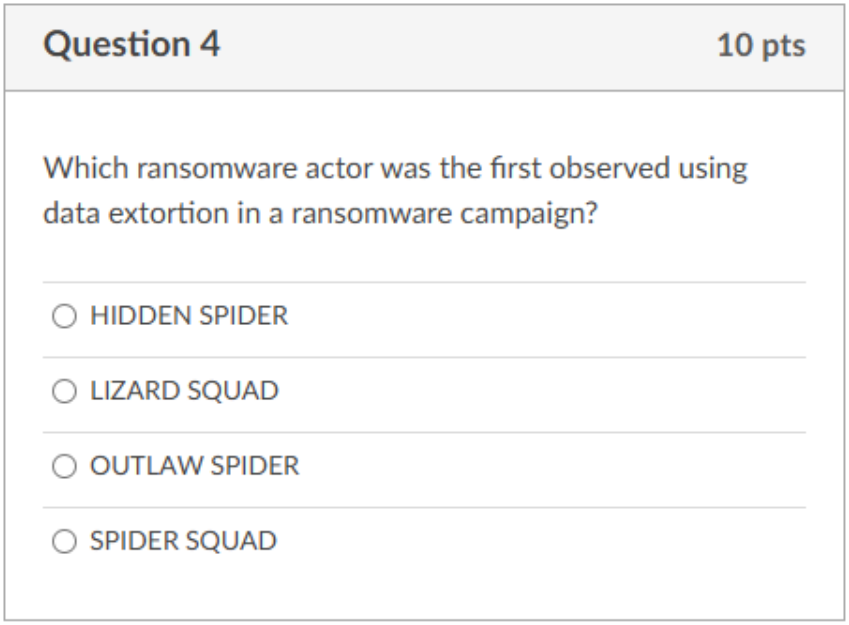
Q 3. What is the hacker group involved in criminal activities from People's Republic of China?

Wicked Panda



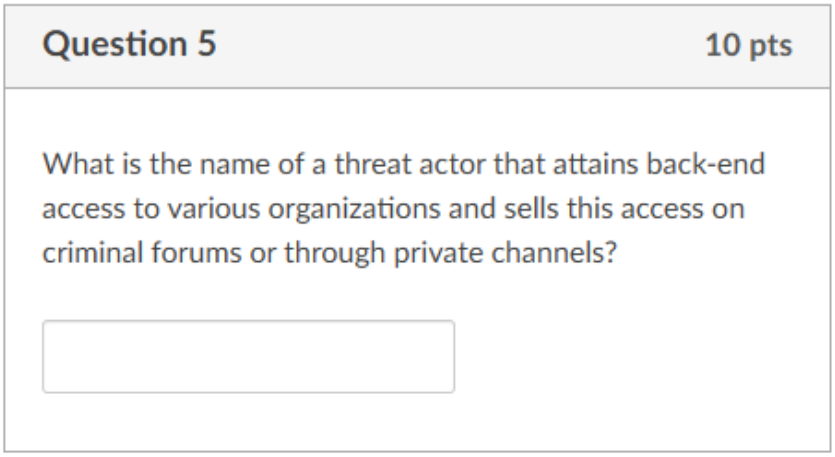
Q 4. Which ransomware actor was the first observed using data extortion in a ransomware campaign?

Outlaw spider



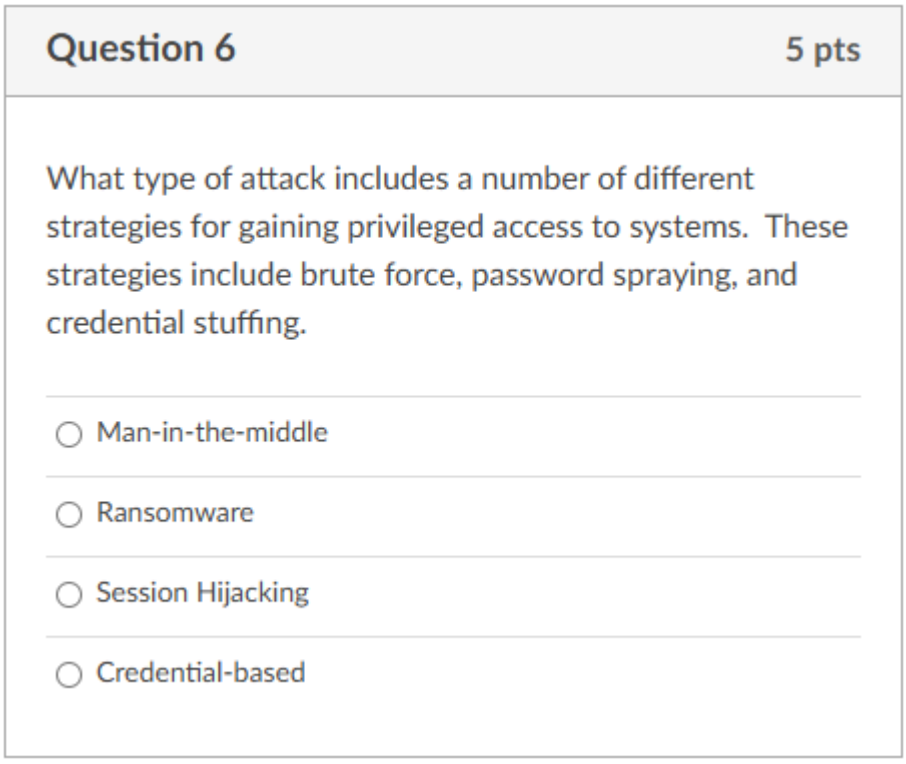
Q 5. What is the name of a threat actor that attains back-end access to various organizations and sells this access on criminal forums or through private channels?

Access Brokers / Initial Access Brokers



Q 6. This type of attack includes a number of different strategies for gaining privileged access to systems. These strategies include brute force, password spraying, and credential stuffing.

Session hijacking



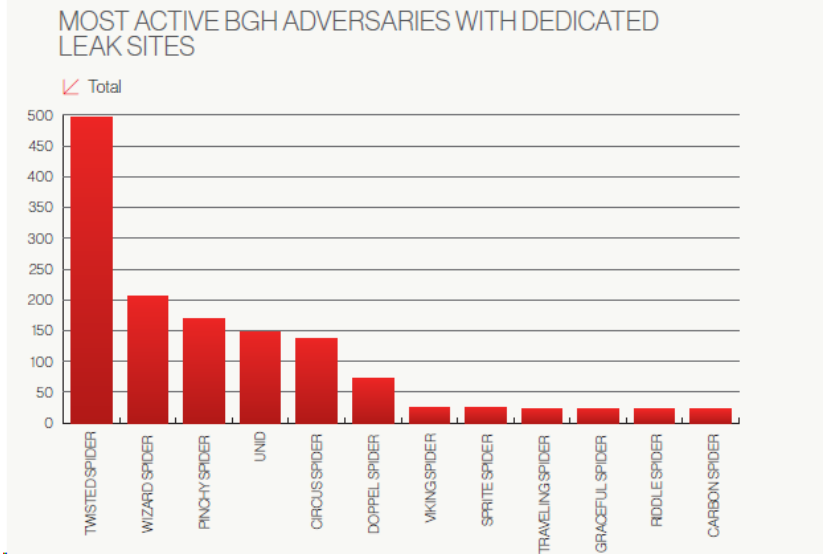
Q 7 Who is credited for the heavy adoption of data extortion in ransomware campaigns?

Question 7 10 pts

Who is credited for the heavy adoption of data extortion in ransomware campaigns?

- ○ TWISTED SPIDER
- ○ LIZARD SQUAD
- ○ SPIDER SQUAD
- ○ ANGRY SPIDER

TWISTED SPIDER



Q 8. According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020?

Question 8 10 pts

According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020?

79%

The growth in intrusion numbers has been driven in large part by the proliferation of eCrime activity. As shown in Figure 2, eCrime intrusions made up 79% of all attributable intrusions uncovered by OverWatch in 2020.

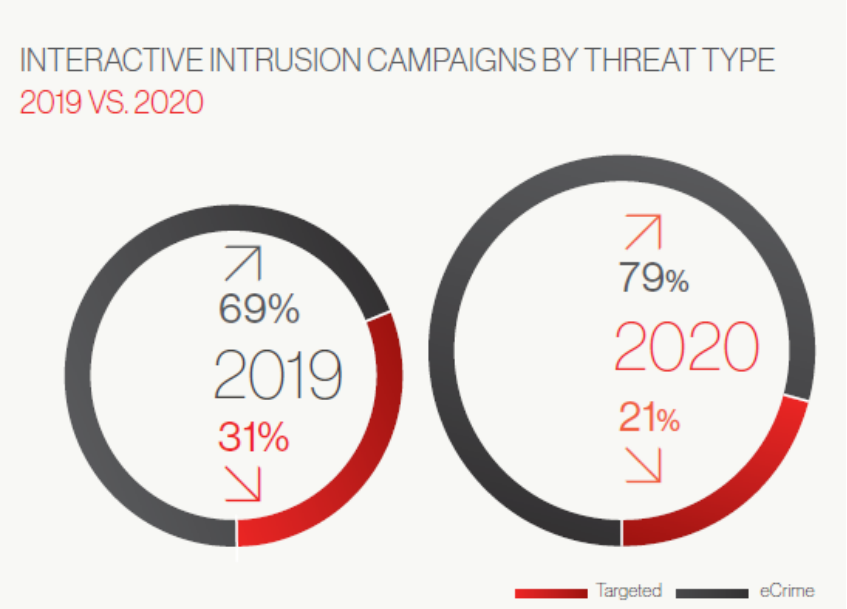


Figure 2. Relative Frequency of Targeted and eCrime Intrusions Uncovered by OverWatch, 2019 vs. 2020

Q 9 . Who was the most reported criminal adversary of 2020?

WIZARD SPIDER

Question 9 **10 pts**

Who was the most reported criminal adversary of 2020?

- ○ OUTLAW SPIDER
- ○ GHOST SPIDER
- ○ WIZARD SPIDER
- ○ LIZARD SQUAD

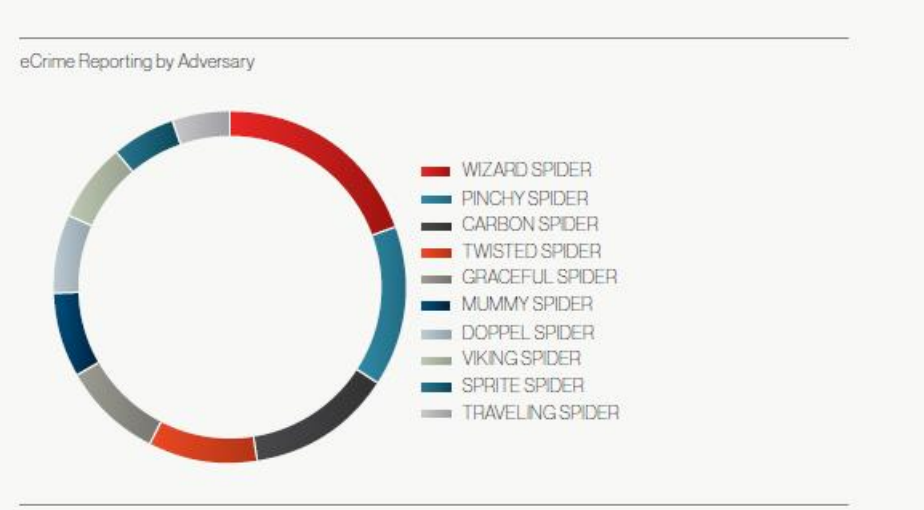


Figure 6. eCrime Reporting by Adversary in 2020

Q 10. What are the three parts of the eCrime ecosystem that CrowdStrike highlighted in their report?

1.service -
2.distribution -
3.monetisation -

Question 10 10 pts

What are the parts of the eCrime ecosystem that CrowdStrike highlighted in their report?

- [ ] Distribution
- [ ] Services
- [ ] Monetization
- [ ] Infrastructure

Q 11. What is the name of the malicious code used to exploit a vulnerability in the SolarWinds Orion IT management software?

Sunburst by StellarParticle

Question 11 — 5 pts

What is the name of the malicious code used to exploit a vulnerability in the SolarWinds Orion IT management software?

- ○ BITPAYMER
- ○ SUNBURST
- ○ MAZE
- ○ CRYPTOLOCKER