

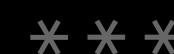
Sector Under Attack: Financial Services

Big game hunting (BGH), targeted intrusions and hacktivism remain key threats to financial institutions.



124 out of 245+
adversaries currently tracked by
CrowdStrike target Financial Services

Attack Advancements in Financial Services



↑ 25%

Increase in intrusion frequency in 2024



↑ 109%

Increase in targeted intrusions in 2024



↑ 99%

Increase in data exfiltration activity in 2023

Key Adversaries Targeting Financial Institutions



SCATTERED SPIDER ↗

This adversary targeted financial services in North America by leveraging sophisticated social engineering techniques to capture user credentials. The adversary often targets accounts belonging to IT personnel to gain access to tools that assist with lateral movement and account compromise.



BITWISE SPIDER ↗

This eCrime adversary is responsible for the development of LockBit ransomware and the StealBIT information stealer. The adversary relies on credential brute-forcing and software supply chain compromises to gain initial access.



GRACEFUL SPIDER ↗

This financially motivated eCrime group uses Clop ransomware and engages in data theft by exploiting multiple zero-day vulnerabilities in file transfer applications. The adversary targets financial entities as reflected on their dedicated leak site.

How Adversaries Achieve Their Objectives



Exploit legitimate credentials to gain access and extend presence without raising alarms



Adapt sophisticated hands-on-keyboard attacks to evade detection



Focus on cross-domain tradecraft to maintain persistence, move laterally and exfiltrate data

Questions for Defenders

- Do you know who is targeting you?
- Are you prepared for the latest adversarial tactics and techniques?
- Are all of your user credentials, cloud assets and endpoint assets protected?

Visit crowdstrike.com/adversaries or download the [CrowdStrike 2024 Threat Hunting Report](#)