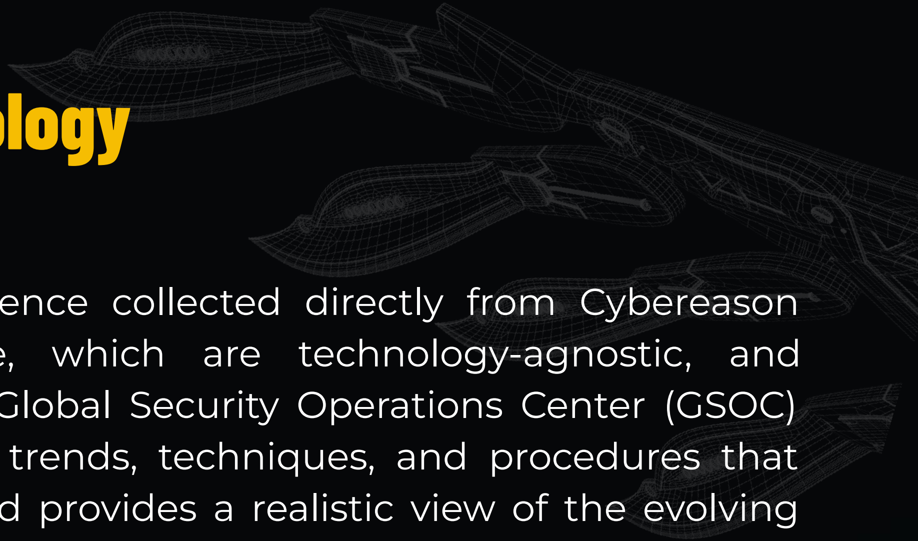
cybereason

TTP Briefing:

January - May 2025

Methodology



This TTP Briefing is based on threat intelligence collected directly from Cybereason incident response engagements worldwide, which are technology-agnostic, and supplemented with data from a selection of Global Security Operations Center (GSOC) detections. This approach reflects the attack trends, techniques, and procedures that Cybereason is currently seeing in the wild, and provides a realistic view of the evolving threat landscape for our clients.

Data Overview

Top 3 Impacted Industries

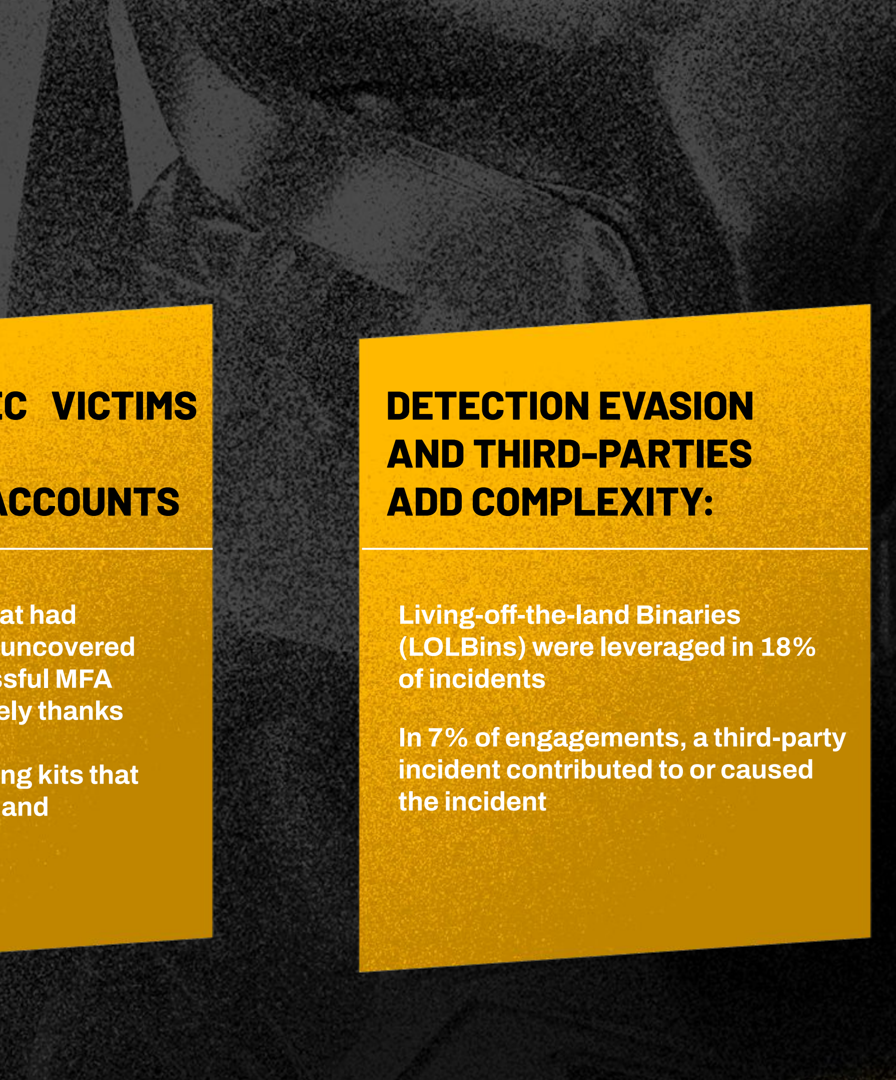
- Financial Services (18%)
- Manufacturing (16%)
- Technology & Software (11%)

Top 3 Threat Incident Types

- Business email Compromise (41%)
- Ransomware (28%)
- Cloud Intrusion (13%)

Top 3 Initial Intrusion Vectors

- Phishing/Social Engineering (46%)
- Valid Accounts /Credential Abuse (16%)
- Exploited Vulnerabilities (14%)



KEY TAKEAWAYS

H1 2025

MOST (76%) ORGANIZATIONS HAD EDR IN PLACE

Additionally, EDR bypass techniques were only identified in rare (< 5%) instances. Despite that, attackers still succeeded in compromising the victim.

Most commonly, EDR triggered alerts but organizations didn’t properly respond.

ONLY 36% OF BEC VICTIMS HAD MFA ON COMPROMISED ACCOUNTS

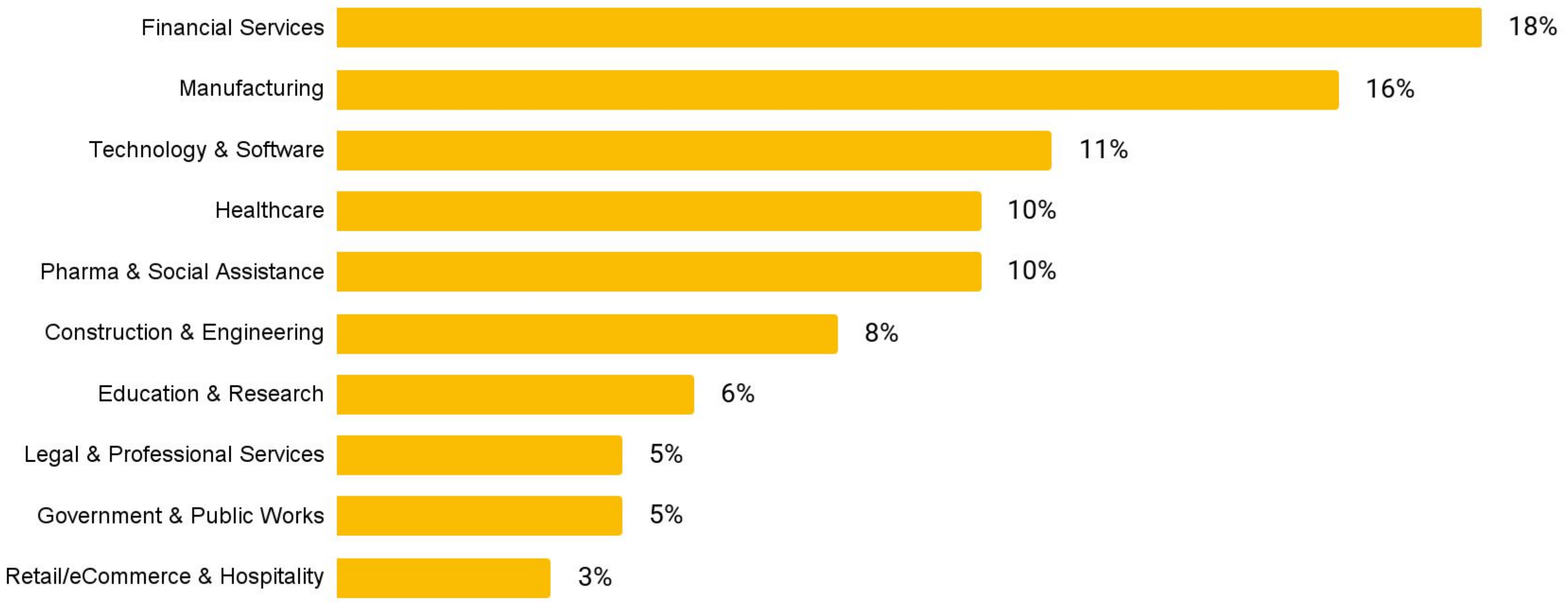
Within BEC cases that had MFA, investigations uncovered a high rate of successful MFA bypass (> 50%) largely thanks to readily available sophisticated phishing kits that capture MFA tokens and credentials.

DETECTION EVASION AND THIRD-PARTIES ADD COMPLEXITY:

Living-off-the-land Binaries (LOLBins) were leveraged in 18% of incidents

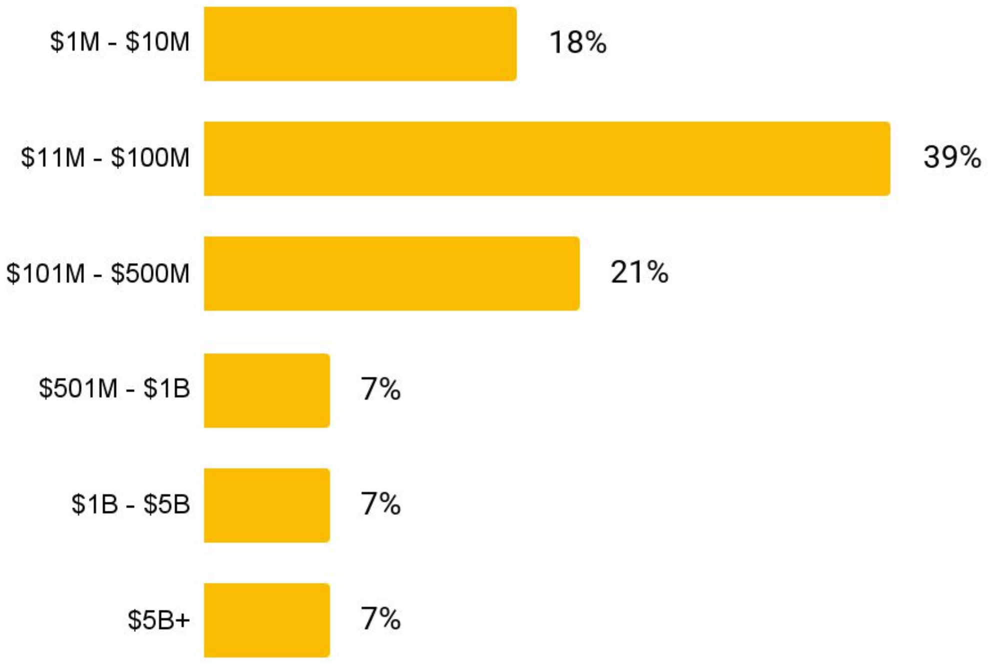
In 7% of engagements, a third-party incident contributed to or caused the incident

Top 10 Impacted Industries

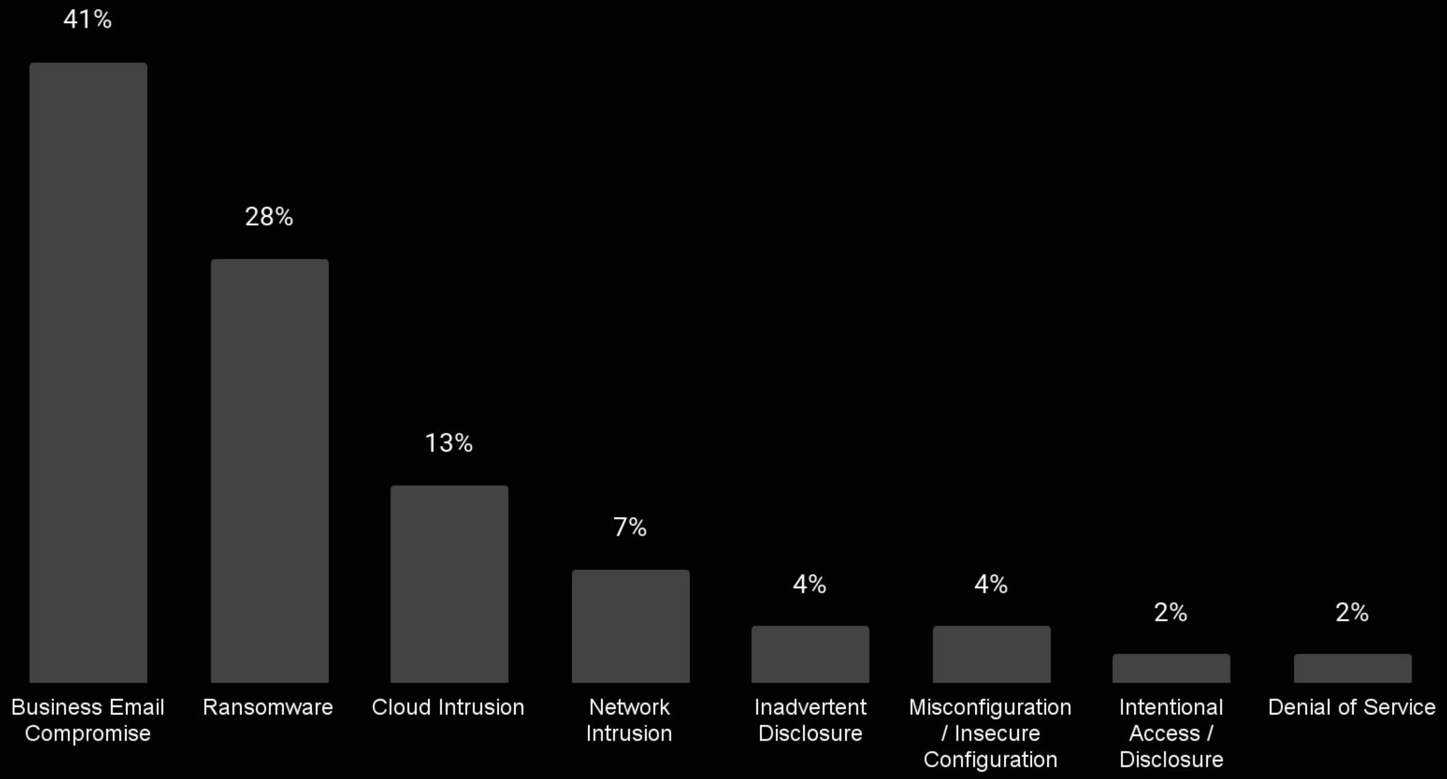


Company Size

Based on revenue

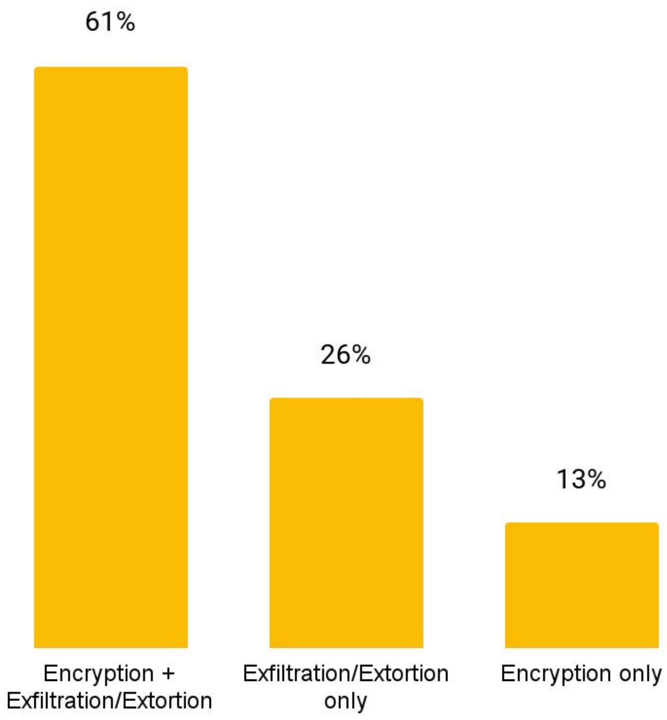


Most Common Incident Types



Ransomware

Attack Type Distribution



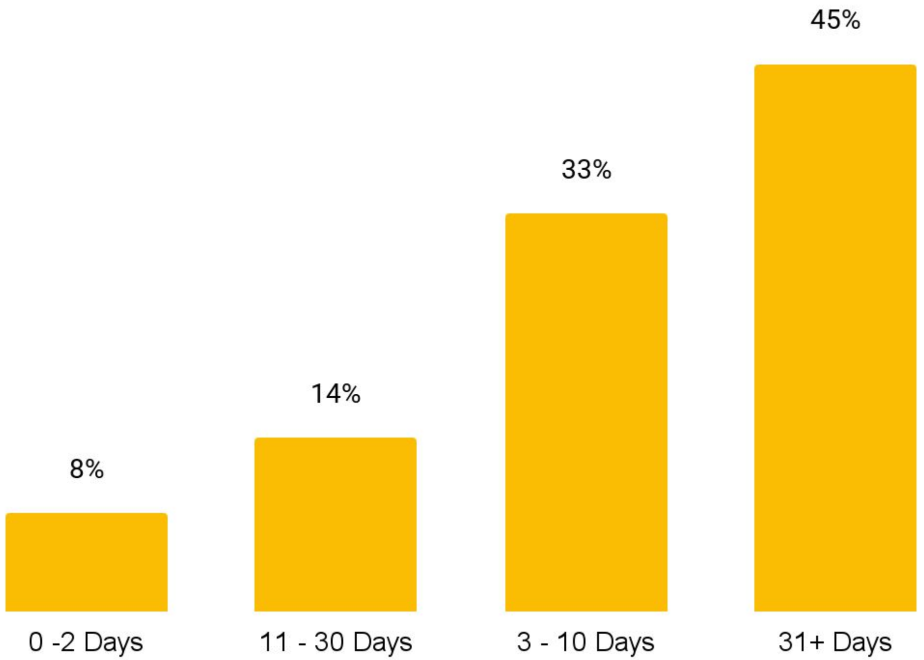
Top Observed Variants

High Activity:	Others:
Akira	Bootkit
Inc	Cactus
Play	BlackNevas
SafePay	GandCrab
Medusa	Makop
Qilin	Ransomhouse
	Mimic
	SECP0

Dwell Time

From Initial Intrusion to IR Kickoff

Measured from the initial date of compromise until Cybereason IR team engagement.



Dwell Time Benchmarks:

0-2 Days: Exceptional

3-10 Days: Above Average

11-30 Days: Below Average

31+ Days: Poor

* *Only applies to Cybereason Consulting clients, excludes MDR clients*

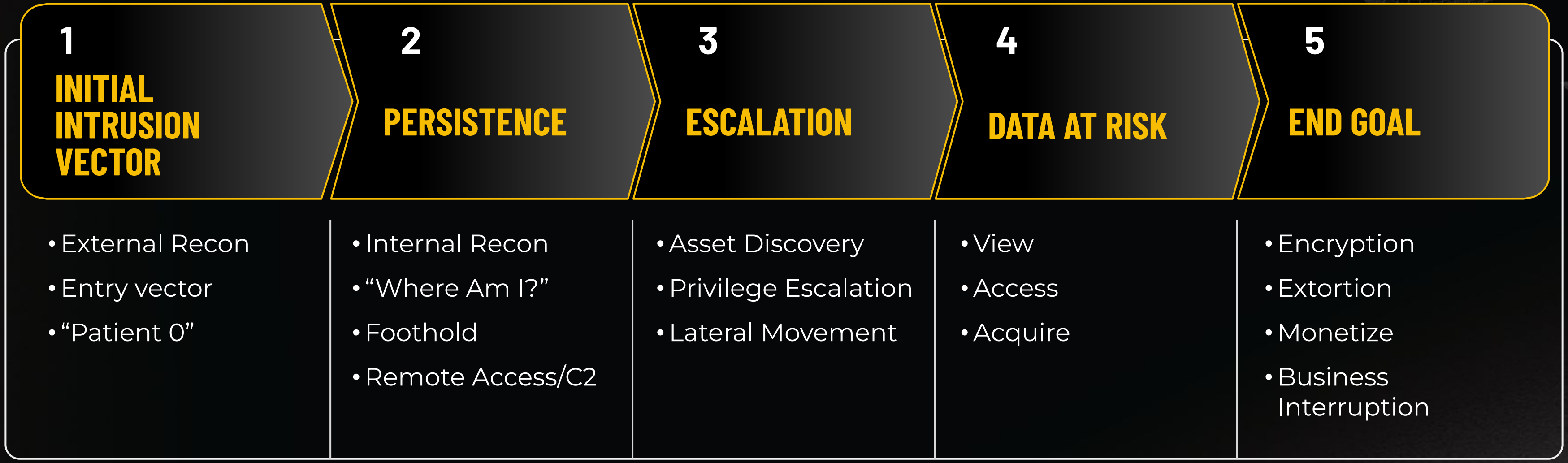
cybereason

Most Commonly Observed CVEs

CVE	Impacted Product
CVE-2024-55956	Cleo Harmony
CVE-2022-41335	Fortinet FortiOS
CVE-2022-42475	FortiOS SSL-VPN
CVE-2024-57727	SimpleHelp Remote Support Software
CVE-2023-34362	MOVEit Transfer
CVE-2016-0099	Microsoft Windows Secondary Logon Elevation of Privilege
CVE-2023-20269	CISCO Adaptive Security Appliance

Trends Across The Intrusion Path

Five Stages of Distinct Activity



1 **INITIAL INTRUSION VECTOR**

- External Recon
- Entry vector
- “Patient 0”

2 **PERSISTENCE**

- Internal Recon
- “Where Am I?”
- Foothold
- Remote Access/C2

3 **ESCALATION**

- Asset Discovery
- Privilege Escalation
- Lateral Movement

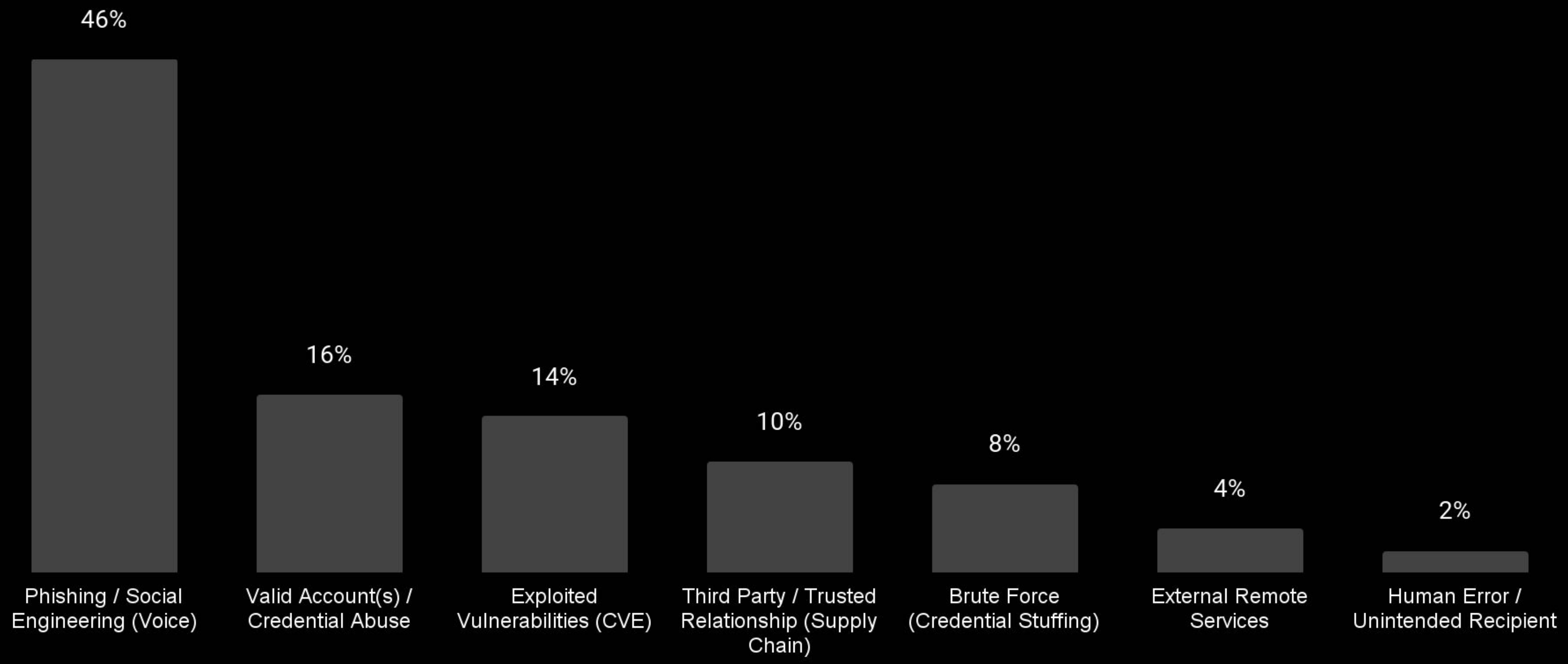
4 **DATA AT RISK**

- View
- Access
- Acquire

5 **END GOAL**

- Encryption
- Extortion
- Monetize
- Business Interruption

1 - Initial Intrusion Vector



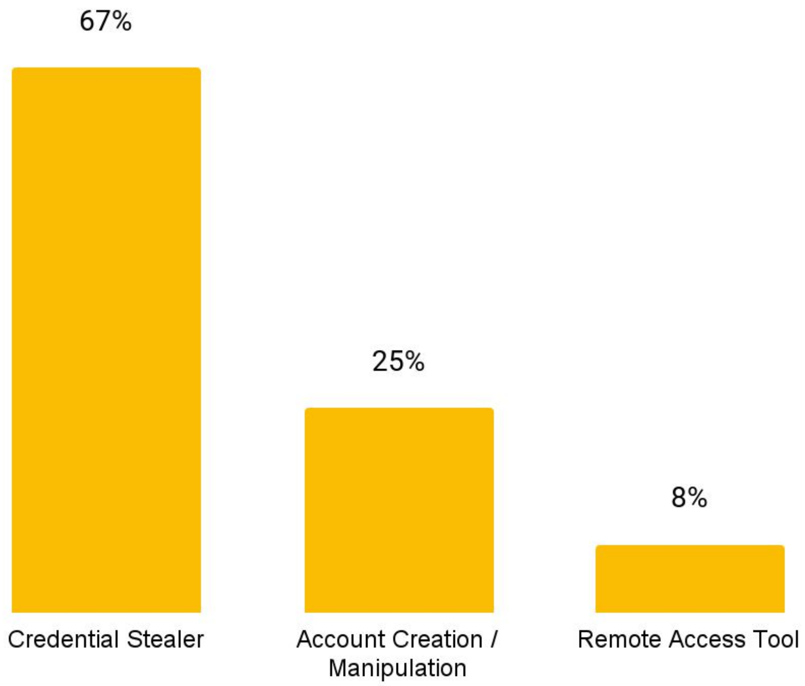
2 - Persistence

In cases where Persistence was observed, the following Malware/Tools/Techniques were most commonly leveraged

Name	Description
AnyDesk	Remote access (desktop) software
Webshell	Remote access and command script
Level RMM	Remote access (desktop) and monitoring software
psexesvc.exe	Remote command execution (LOLBin)
Meshagent	Remote access (desktop) software
ScreenConnect	Remote access (desktop) software
SplashTop	Remote access (desktop) software
Abuse of VPN	Technique to leverage VPN access
schtasks.exe	Scheduled Tasks / Job scheduler (LOLBin)

3 - Escalation

In cases where Escalation was observed:

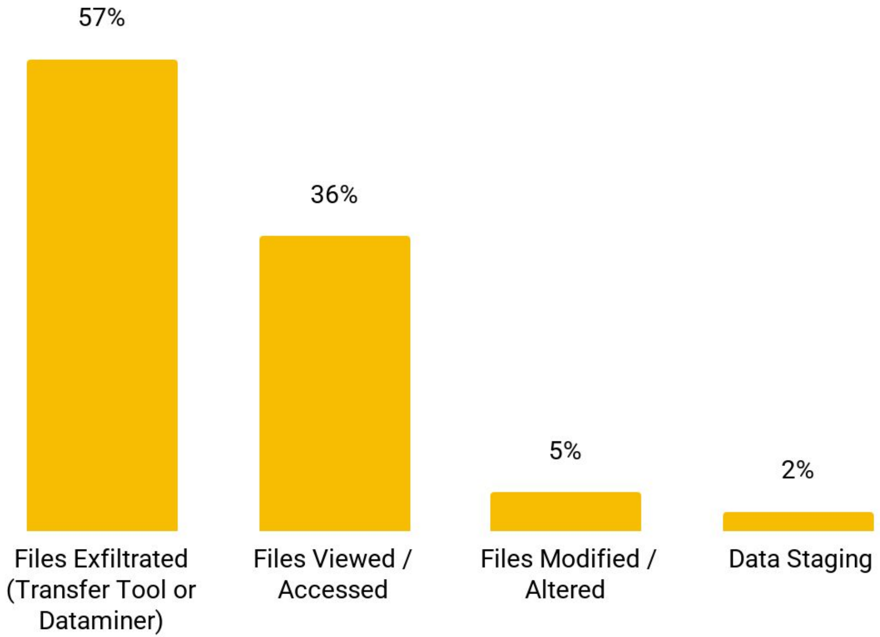


Observed Tools/Techniques used for Escalation:

Name	Description
Mimikatz	Credential stealer
LSASS Dump	Technique for extracting credentials
TruffleHog	Tool to scan code repositories
OpenSSH Authentication Agent	Program that stores private keys for SSH authentication
Net User Command	Command to manage user accounts

4 - Data at Risk

In cases where Data at Risk was observed:

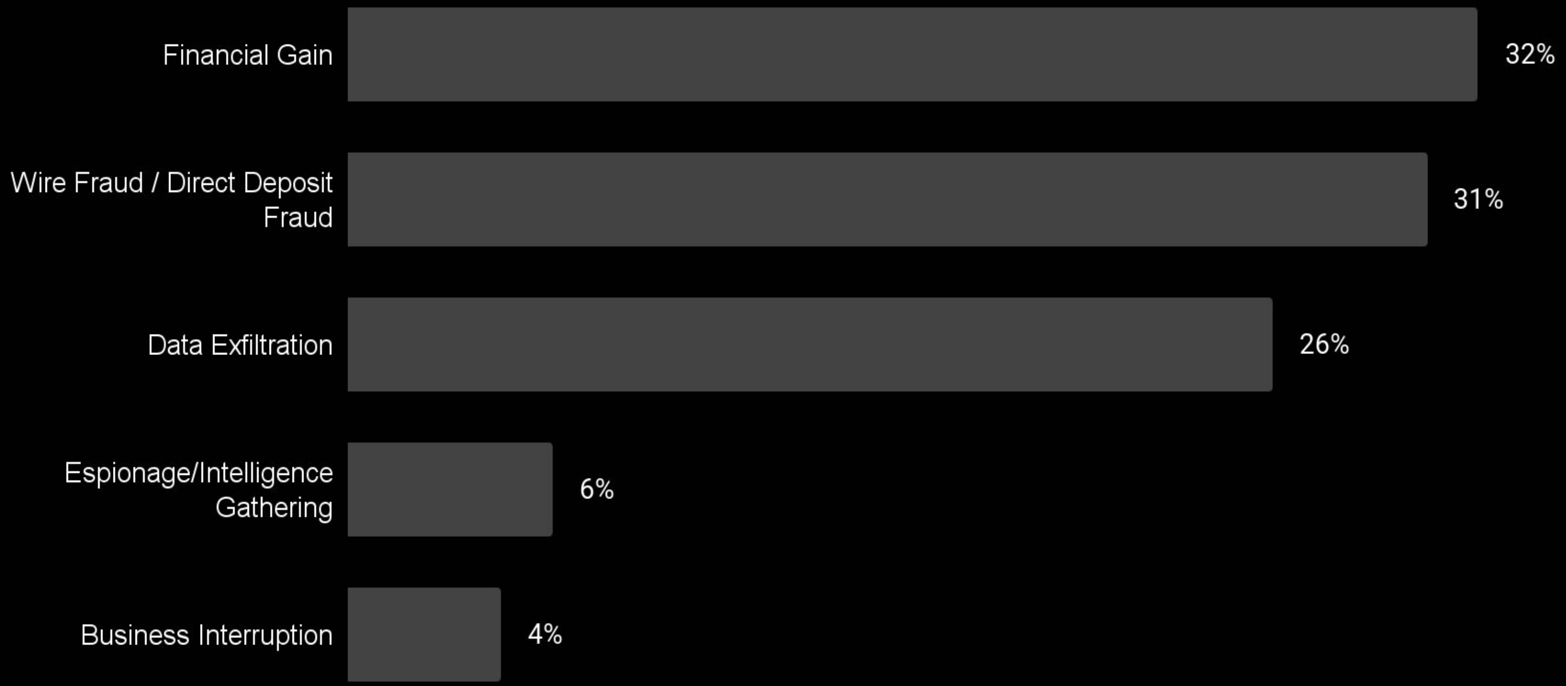


Observed Tools/Techniques for Data at Risk:

Name	Description
RClone	Command-line program for file management
WinSCP	Open-source SFTP client
couchdrop.io	SFTP server and client
WinRAR	Software for compressing and archiving files
Exfiltration Over C2 Channel	Technique to transfer data over C2 channel

cybereason

5 - Threat Actor End Goal



About Cybereason

TRUSTED INCIDENT RESPONSE TEAM

FRONTLINE EXPERTISE TO ELEVATE YOUR CYBER PREPAREDNESS AND RESILIENCE

BATTLE-TESTED EXPERTISE

7000+
Incident response investigations

200K+
Hours of offensive security engagements

~500
Tabletop exercises orchestrated

Relationships with 100s of law firms and insurance carriers

HOLISTIC EXPOSURE MANAGEMENT

300+
experts versed in infrastructure, applications, systems, and endpoints including OT/IoT and emerging tech

60+ elite DFIR investigators
with eDiscovery, managed review, breach notification and expert witness expertise

ELITE THREAT INTEL & SECURITY RESEARCH

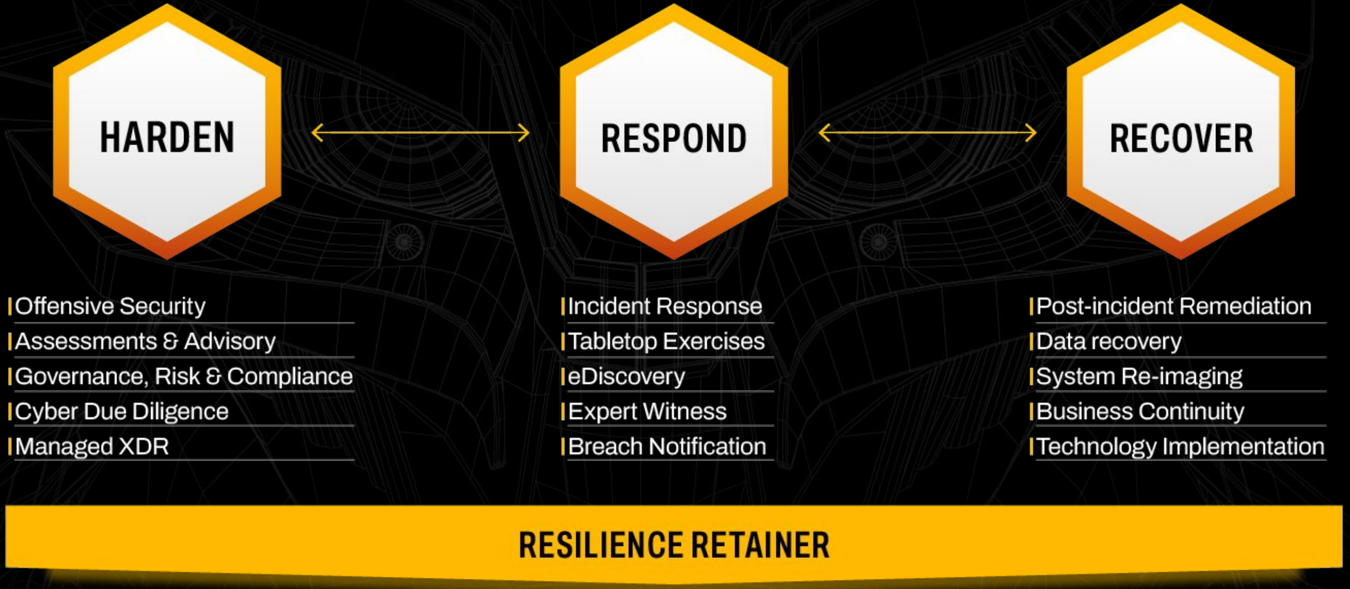
30K+ vulnerabilities
discovered annually

6M+ endpoints
under management

MXDR platform
able to ingest 100s of cloud, SaaS, EDR telemetry

PREPAREDNESS & RESILIENCE SOLUTIONS

50+ SERVICES TO HANDLE THE ENTIRE LIFECYCLE OF A CYBER INCIDENT



HARDEN

- Offensive Security
- Assessments & Advisory
- Governance, Risk & Compliance
- Cyber Due Diligence
- Managed XDR

RESPOND

- Incident Response
- Tabletop Exercises
- eDiscovery
- Expert Witness
- Breach Notification

RECOVER

- Post-incident Remediation
- Data recovery
- System Re-imaging
- Business Continuity
- Technology Implementation

RESILIENCE RETAINER

cybereason

24x7 expert assistance via response@cybereason.com