LevelBlue

TTP Briefing:
Q1 2026

Methodology

This TTP Briefing is based on threat intelligence derived directly from LevelBlue incident response engagements worldwide over the past quarter. These engagements are technology-agnostic, providing a clear view into the real-world tactics, techniques, and procedures adversaries are using today. The result is a grounded and current perspective on the evolving threat landscape facing our clients.

As LevelBlue continues integrating capabilities across Cybereason, Stroz Friedberg, Trustwave, and Alert Logic, our threat intelligence is expanding to incorporate insights from SpiderLabs and trillions of security events. For the first time, this edition reflects data from the broader LevelBlue incident response and threat intelligence ecosystem. As a result, historical comparisons are not included.

Future editions of the TTP Briefing will continue to build on this unified foundation, delivering deeper and more comprehensive insights from across LevelBlue's global incident response and threat intelligence teams.

Q1 Data overview

Top 3 impacted industries

- Financial Services (21%)
- Healthcare, Pharma, and Social Assistance (16%)
- Manufacturing (14%)

Top 3 incident types

- Business Email Compromise (39%)
- Network Intrusion (non-ransomware) (30%)
- Ransomware (26%)

Top 3 initial intrusion vectors

- Phishing/Social Engineering (58%)
- Exploited Vulnerabilities (20%)
- External Remote Services (11%)

Key takeaways – Q1 2026

Business email compromise leads to data exfil and extortion

Threat actors are leveraging oAuth tokens, acquired through phishing/social engineering, to mass exfiltrate files in SharePoint, OneDrive, and other email accounts through exposed APIs.

Social engineering pressure tactics on the rise

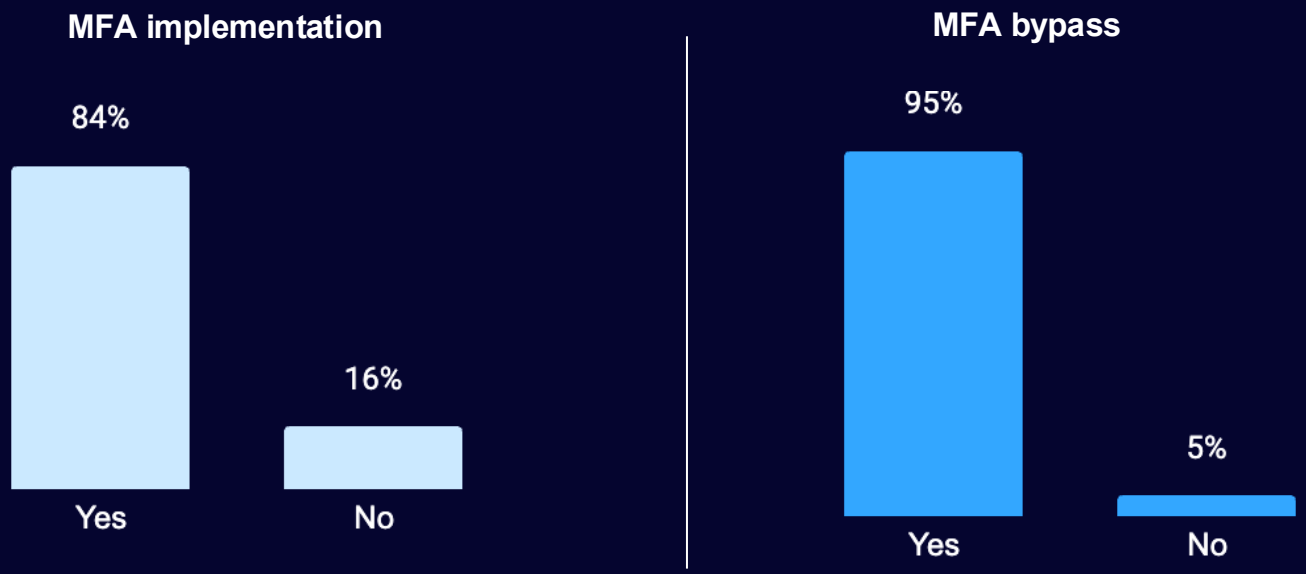
Social engineering tactics continue to grow in sophistication as threat actors leverage methods like impersonating IT on Microsoft Teams or targeting help desks to bypass defenses.

Threat actors move laterally, discretely, with AI tools

Attackers are leveraging native, internally available AI tools to effortlessly locate internal data during lateral movement. This method reduces their footprint inside a system.

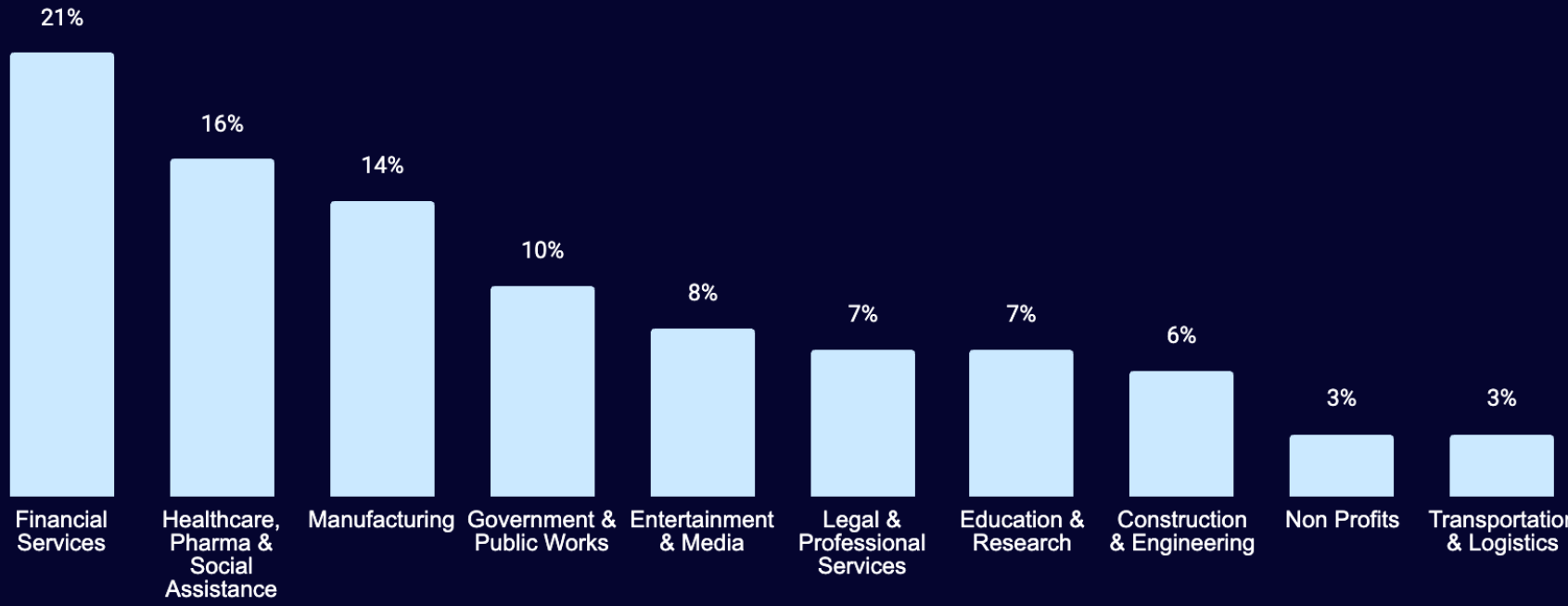
MFA implementation continues, so does bypass

Organizations continue to implement MFA, but threat actors continue to employ methods to bypass it

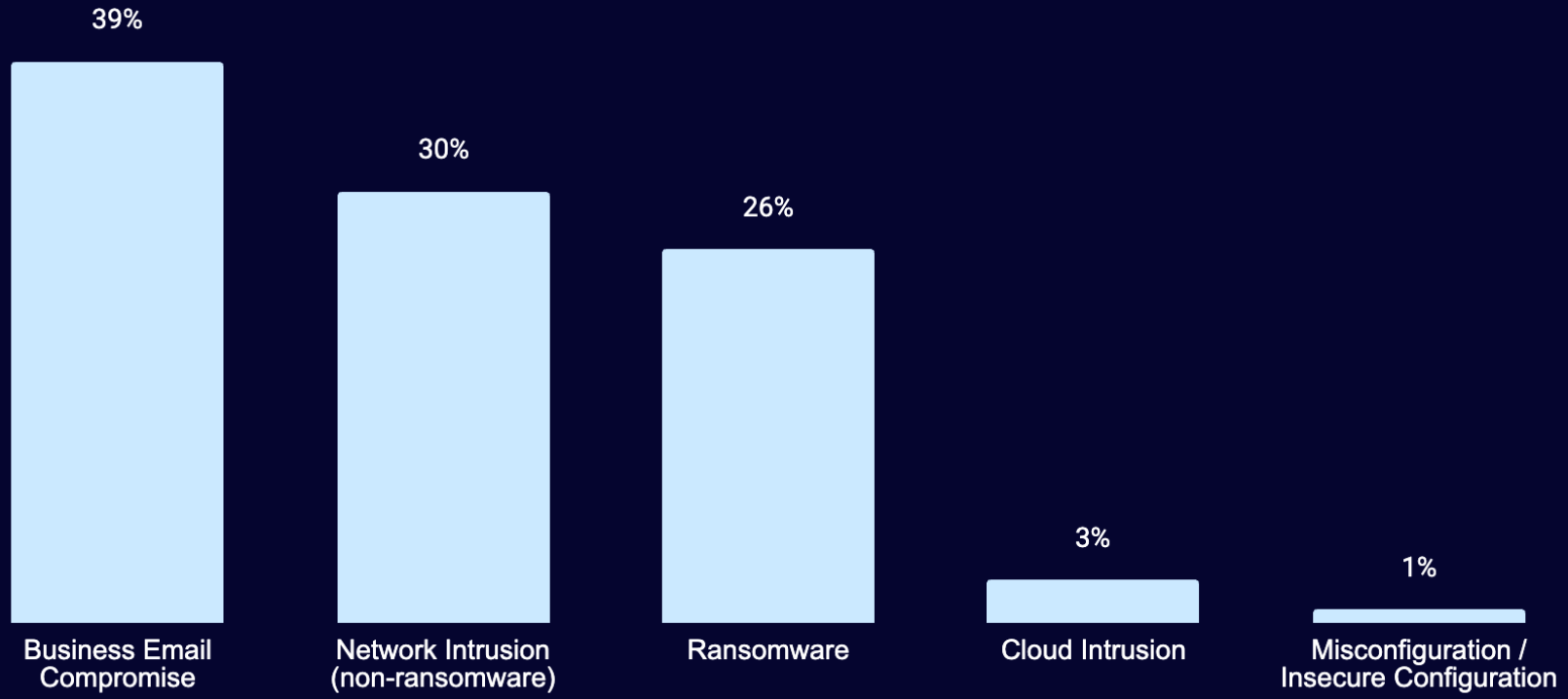


Implementing phishing-resistant MFA can help protect organizations against readily-available phishing kits and tools that intercept session tokens that threat actors leverage for MFA bypass.

Top 10 impacted industries – Q1 2026

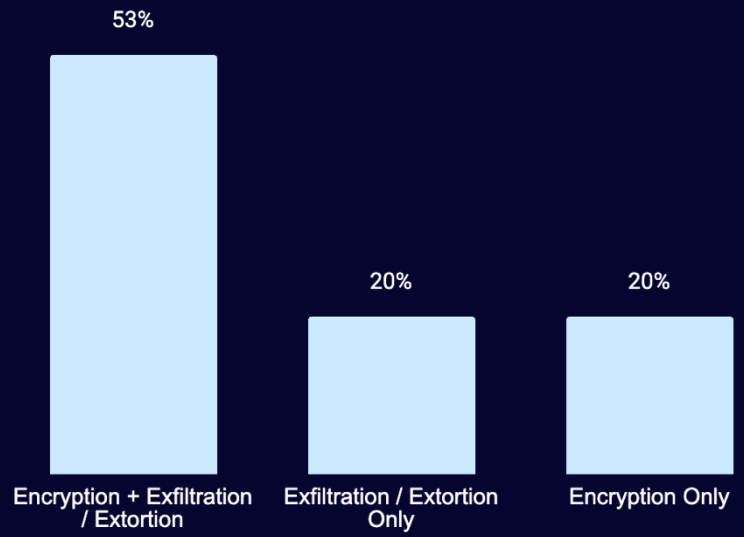


Most common incident types – Q1 2026



Ransomware Q1 2026

Attack type distribution



Top observed variants

High Activity	Others
Akira	Play
Qilin	LockBit5
ShinyHunters	DevMan
Sinobi	Chaos
Inc	Medusa

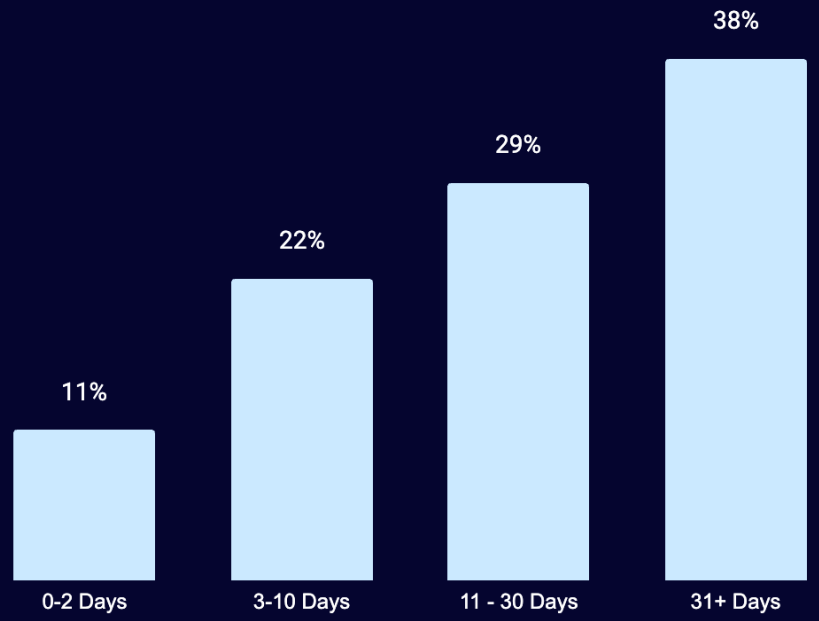
Shaming sites

Total victims in Q1: 1528

- Qilin remains most active group posting victims
- The Gentlemen rises in activity
- ShinyHunters (34 postings), did not make top 10, but higher impact

Dwell time Q1 2026 – From initial intrusion to IR kickoff

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



Dwell time benchmarks:

0-2 Days: Exceptional

3-10 Days: Above Average

11-30 Days: Below Average

31+ Days: Poor

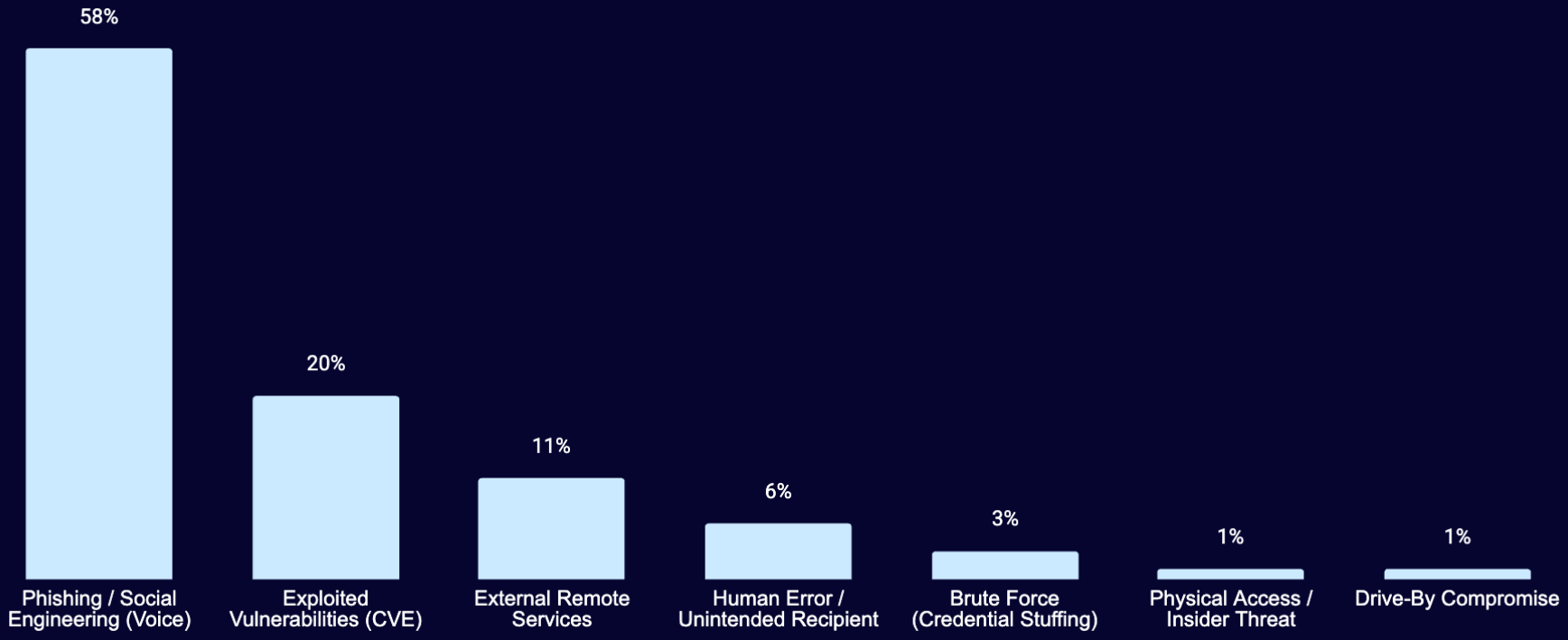
** Only applies to LevelBlue DFIR clients, excludes MDR clients*

Trends across **The Intrusion Path**

Five phases of distinct activity

Initial Intrusion Vector	Persistence	Escalation	Data at Risk	End Goal
• External recon • Entry vector • “Patient 0”	• Foothold • Internal recon • Remote access/C2	• Asset discovery • Privilege escalation • Lateral movement	• View • Access • Acquire	• Encrypt • Extort and monetize • Business interruption

1. Initial intrusion vector – Q1 2026



Most commonly observed CVEs – Q1 2026

CVE	Impacted product
CVE-2026-1731	BeyondTrust Remote Support
CVE-2025-40601	SonicWall SonicOS SSL-VPN
CVE-2025-0108	PAN-OS Authentication Bypass
CVE-2024-55591	Fortinet FortiOS
CVE-2024-53705	SonicWall SonicOS SSH
CVE-2024-53704	SonicWall SonicOS SSL-VPN

CVE	Impacted product
CVE-2024-40766	SonicWall SonicOS improper access control vulnerability
CVE-2024-40762	SonicWall SonicOS SSL-VPN
CVE-2024-23113	Fortinet FortiOS
CVE-2024-21762	Fortinet FortiOS
CVE-2021-4034	Polkit Privileged Escalation Vulnerability

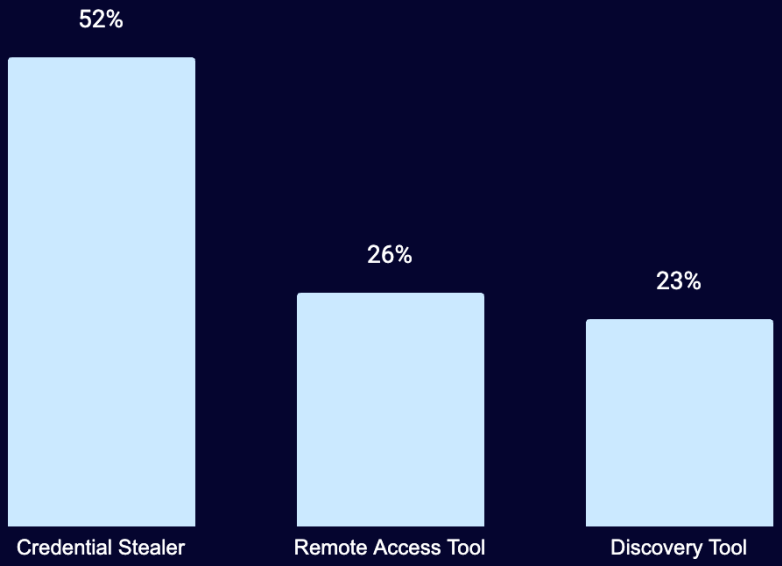
2. Persistence – Q1 2026

In cases where persistence was observed, the following malware/tools/techniques were most commonly leveraged

Name	Description
AnyDesk	Remote access tool
PSExec	Remote management tool
Advanced IP Scanner	Network discovery tool
PowerShell	Command line
GSocket	Remote access tool
Meshagent	Remote access tool
FixMe IT	Remote access tool

3. Escalation – Q1 2026

In cases where escalation was observed:

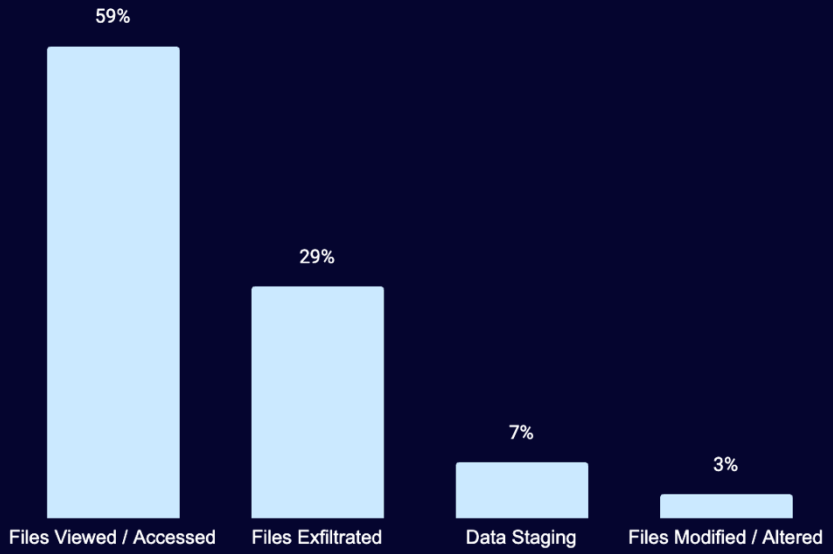


Observed tools/techniques used for escalation:

Name	Description
Powershell	Command line
Advanced IP Scanner	Network discovery tool
NetScan	Network discovery tool
Psexesvc	Remote management tool
Mimikatz	Credential stealer
TruffleHog	Tool to scan code repositories
SharpHound	Active directory exploration and exploitation framework

4. Data at risk – Q1 2026

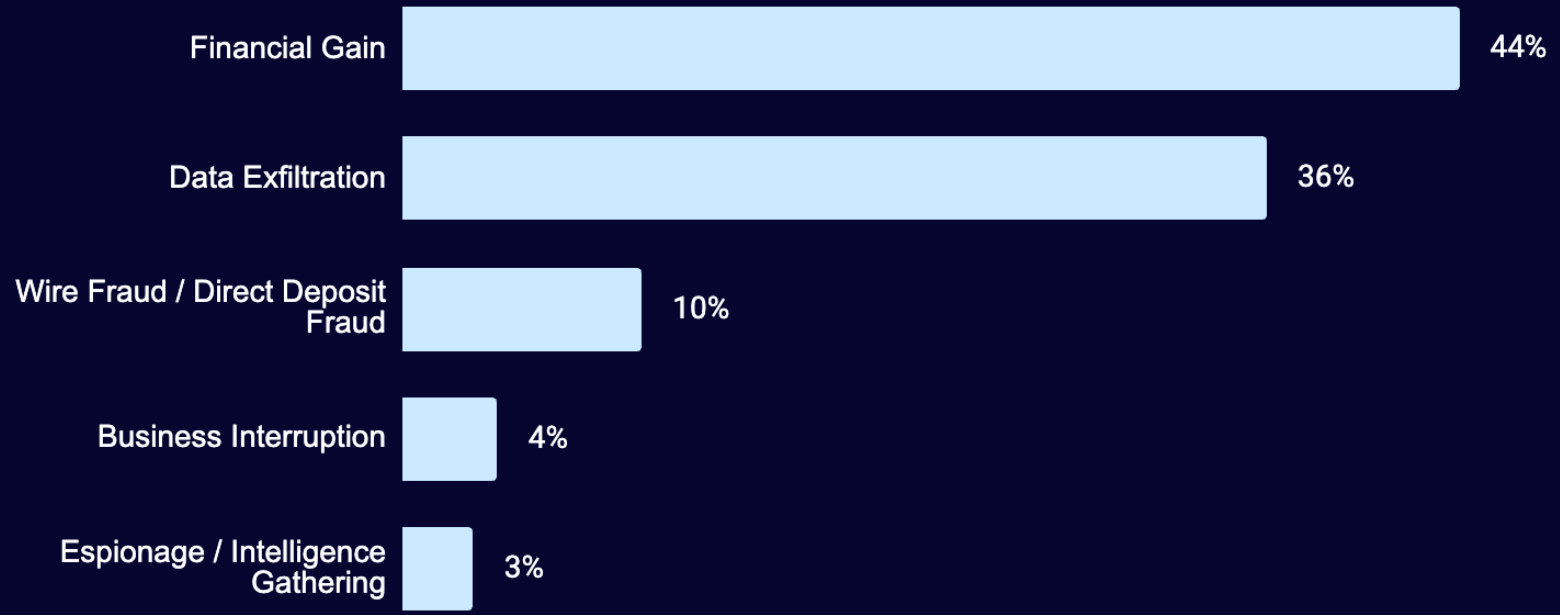
In cases where data at risk was observed:



Observed tools/techniques used for data at risk:

Name	Description
WinRar	Software for compressing and archiving files
7-Zip	Software for compressing and archiving files
MegaSync	File transfer service
WinSCP	Open-source SFTP client

5. Threat actor end goal – Q1 2026



About LevelBlue

24x7 expert assistance via response@levelblue.com

LevelBlue security solutions

LevelBlue's comprehensive portfolio delivers scalable, AI-driven protection across cloud, network, and hybrid environments.

Exposure Management

- Penetration Testing
- Vulnerability Management
- Scenario Simulations
- Threat Intelligence

Cyber Advisory & Transformation

- Strategy & Planning
- Security Assessment
- GRC Enablement
- Cloud & Platform Security Assurance
- Architecture, Integration & Remediation

Threat Detection, Investigation & Response

- Managed Detection & Response
- Managed Extended Detection & Response
- Co-Managed SOC
- Advanced Threat Hunting

Incident Readiness & Response

- Resilience Retainer
- Digital Forensics & Incident Response
- IR Plans & Tabletops
- IP Risk & Litigation Support
- Complex Cyber Investigations

Managed Network Security

- Edge Security
- Managed DDoS Protection
- Content Delivery Network
- Email Security

Managed Cloud Security

- Managed SASE / Managed SSE
- Firewall-as-a-Service
- Zero Trust Network Access
- Web App & API Protection

Proven expertise & frontline threat intel

300+
trusted DFIR experts

2,500+
cybersecurity professionals

Approved by cyber insurance carriers and brokers

50+

9000+
incidents investigated &

1K+
tabletop exercises orchestrated

8M+
Endpoints under global SOC oversight

Bleeding edge threat intel & vulnerability research via SpiderLabs

200K+
hours of pen tests delivered annually

30K+
vulnerabilities discovered per year

1K+
threat hunts conducted annually

Broad global experience

30+
years of cybersecurity experience

trillions
of events per year

billions
of threat intelligence indicators

24x7
global security operations

2500+
cybersecurity professionals

Thank You

24x7 expert assistance via response@levelblue.com