LevelBlue

TTP Briefing:
Q2 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.

This edition also incorporates threat intelligence from LevelBlue's recently integrated teams, including SpiderLabs, which broadens the dataset behind our findings.

Q2 data overview

Top 3 impacted industries

- Financial Services (28%)
- Education & Research (13%)
- Legal & Professional Services (11%)

Top 3 incident types

- Business Email Compromise (45%)
- Network Intrusion (non-ransomware) (20%)
- Cloud Intrusion (15%)

Top 3 initial intrusion vectors

- Phishing/Social Engineering (65%)
- External Remote Services (9%)
- Valid Accounts / Credential Abuse (7%)

Key takeaways – Q2 2026

Token and machine identity abuse leads to software supply chain concerns

OAuth token and machine identity abuse attacks continue to evolve as threat actors apply them to vendor integrations, leading to software supply chain incidents like those of Klue, Vercel, and the Shai-Hulud campaign.

Everything old is new again: ClickFix social engineering

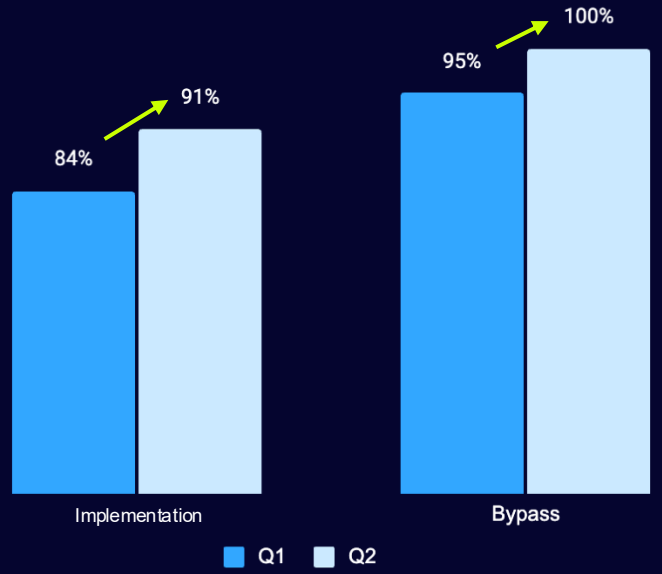
ClickFix social engineering resurged in Q2. Victims are tricked into pasting attacker-supplied commands, typically through fake CAPTCHA or error-fix prompts, allowing attackers to bypass email security controls because the user executes the payload themselves.

Threat actors moving faster, decreasing time in victim networks

Attackers are compressing the intrusion path. Average dwell time dropped in Q2, driven in part by threat actors moving from initial access to exfiltration in days rather than weeks, shrinking the window defenders have to detect and evict them before data leaves the network.

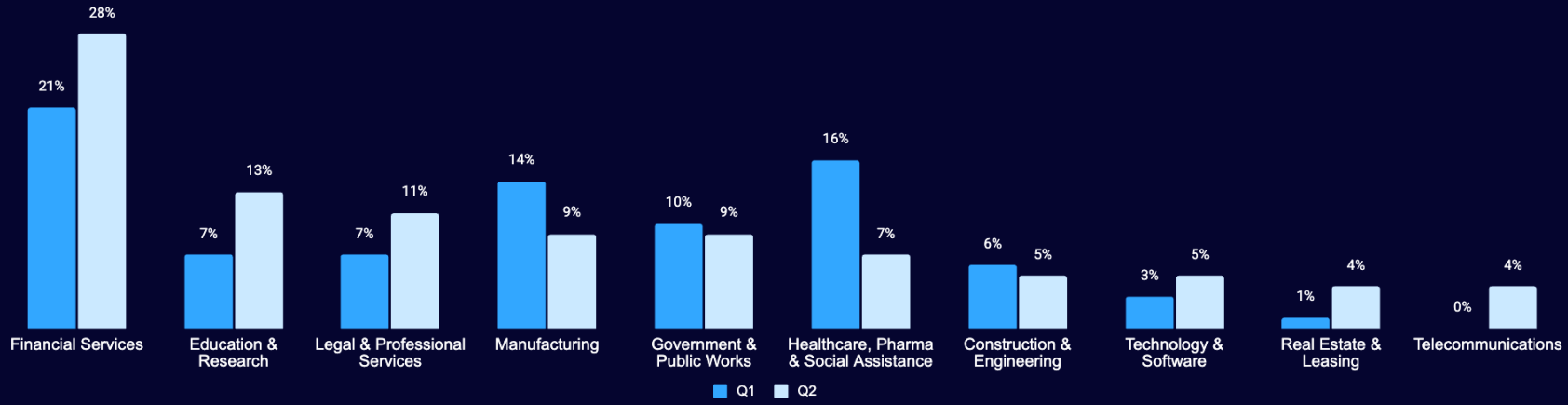
MFA bypass hits 100%

Whether it was overcome by sophisticated phishing kits, unique social engineering tactics, or circumvented by valid OAuth tokens or API keys, threat actors bypassed MFA in every BEC where it was enabled.

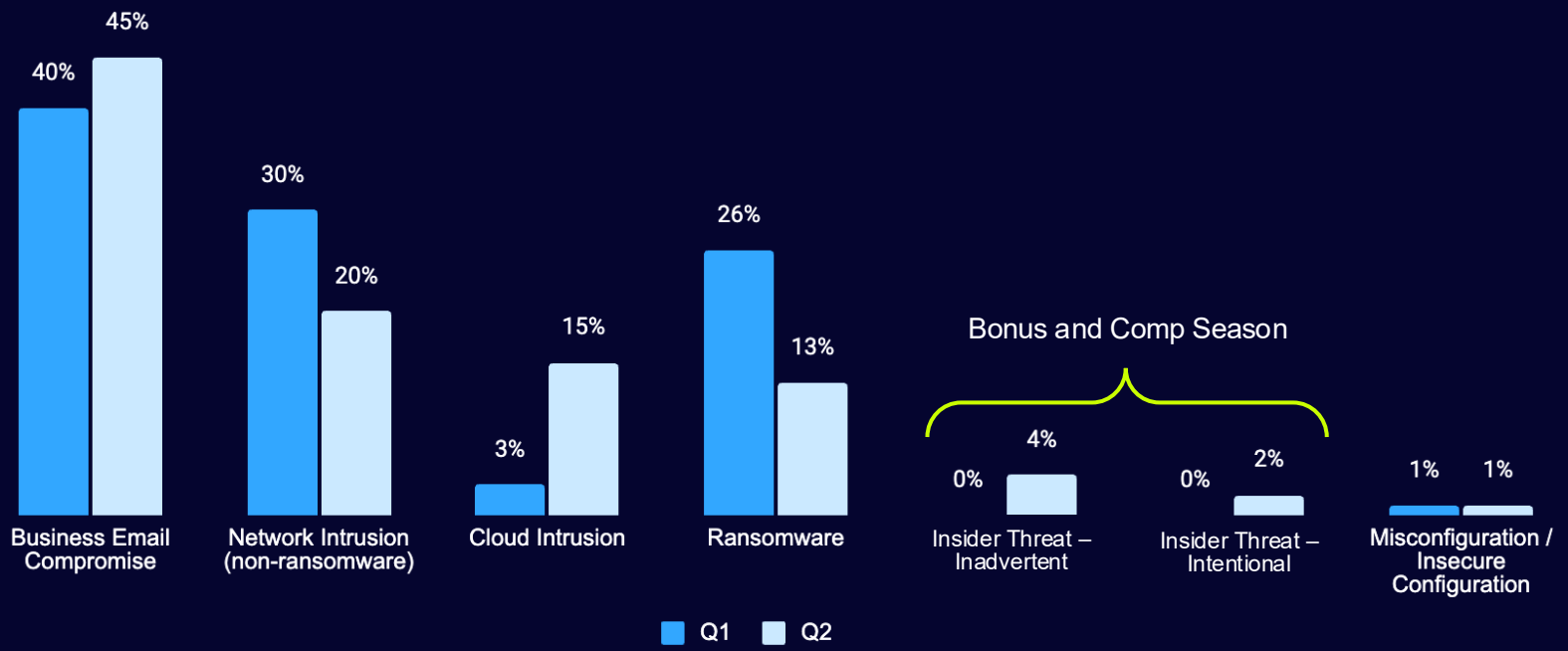


Implementing phishing-resistant MFA can help protect organizations against readily available phishing kits that intercept session tokens, enabling MFA bypass.

Top 10 impacted industries over time



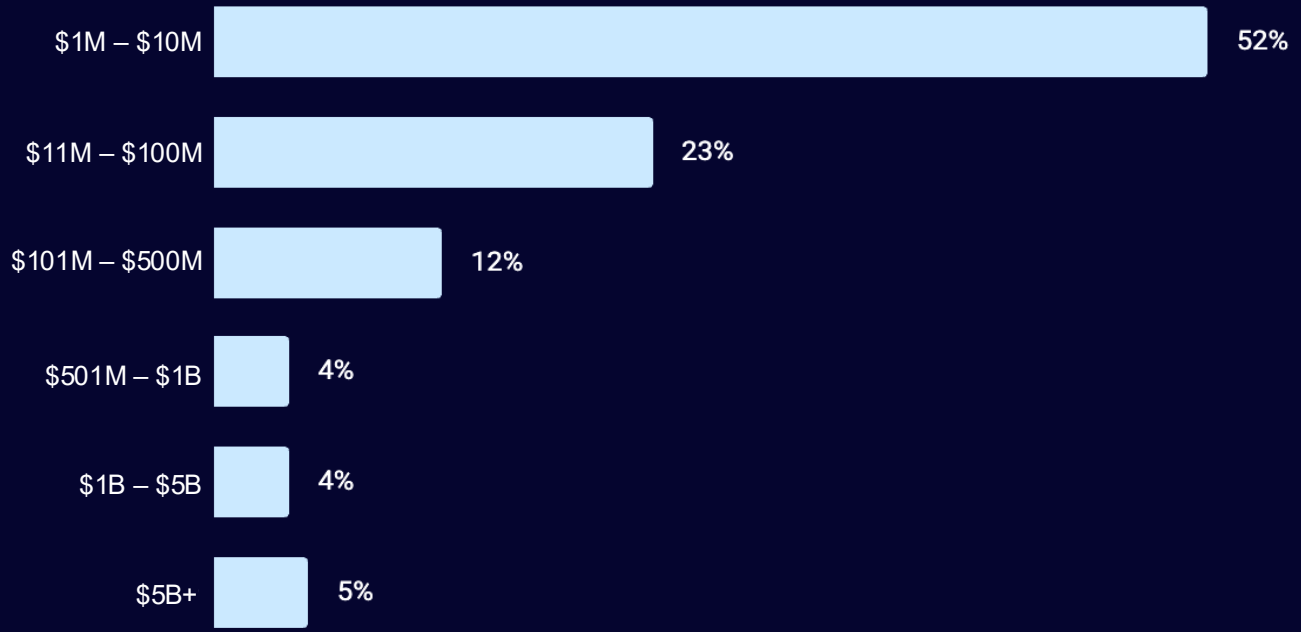
Most common incident types over time



LevelBlue

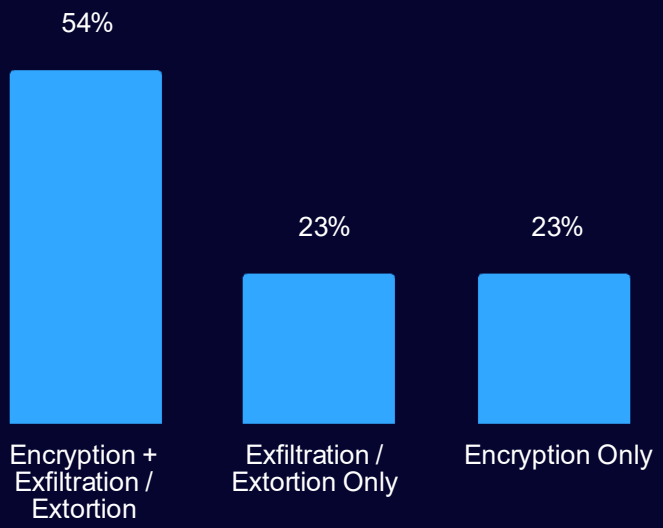
Company size – Q2

Based on revenue



Ransomware Q2 2026

Attack type distribution



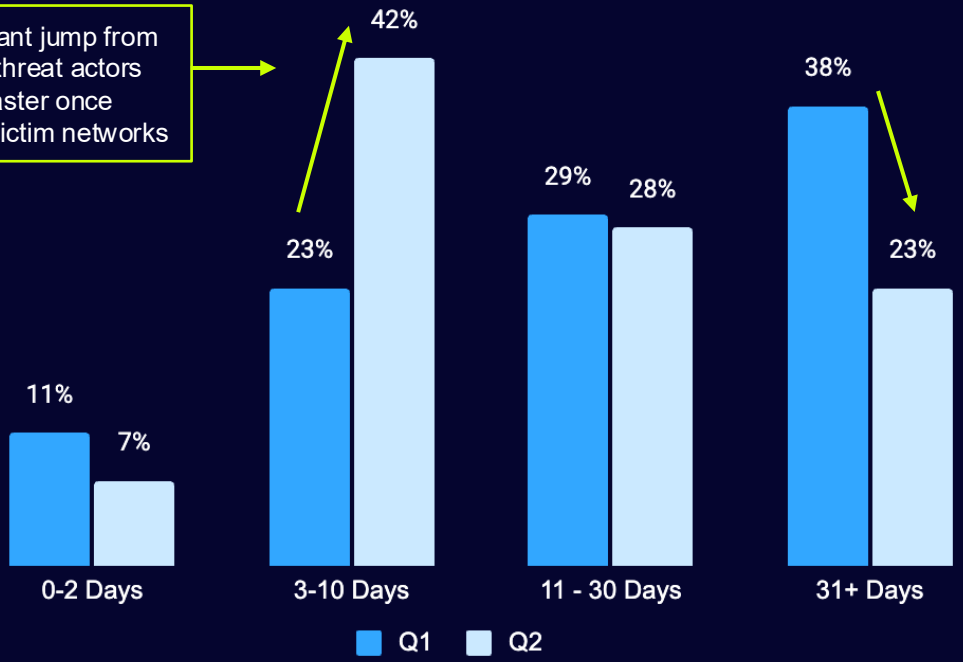
Top observed variants

High Activity	Others
Akira	World Leaks
INC	ShinyHunters
Icarus	Play
	LockBit5.0
	Blackfile
	DragonForce
	SecP0

Dwell time over time – From initial intrusion to IR kickoff

Measured from the initial date of compromise until IR team engagement (excludes MDR clients)

Significant jump from Q1, as threat actors move faster once inside victim networks



Dwell time benchmarks:

0-2 Days: Exceptional

3-10 Days: Above Average

11-30 Days: Below Average

31+ Days: Poor

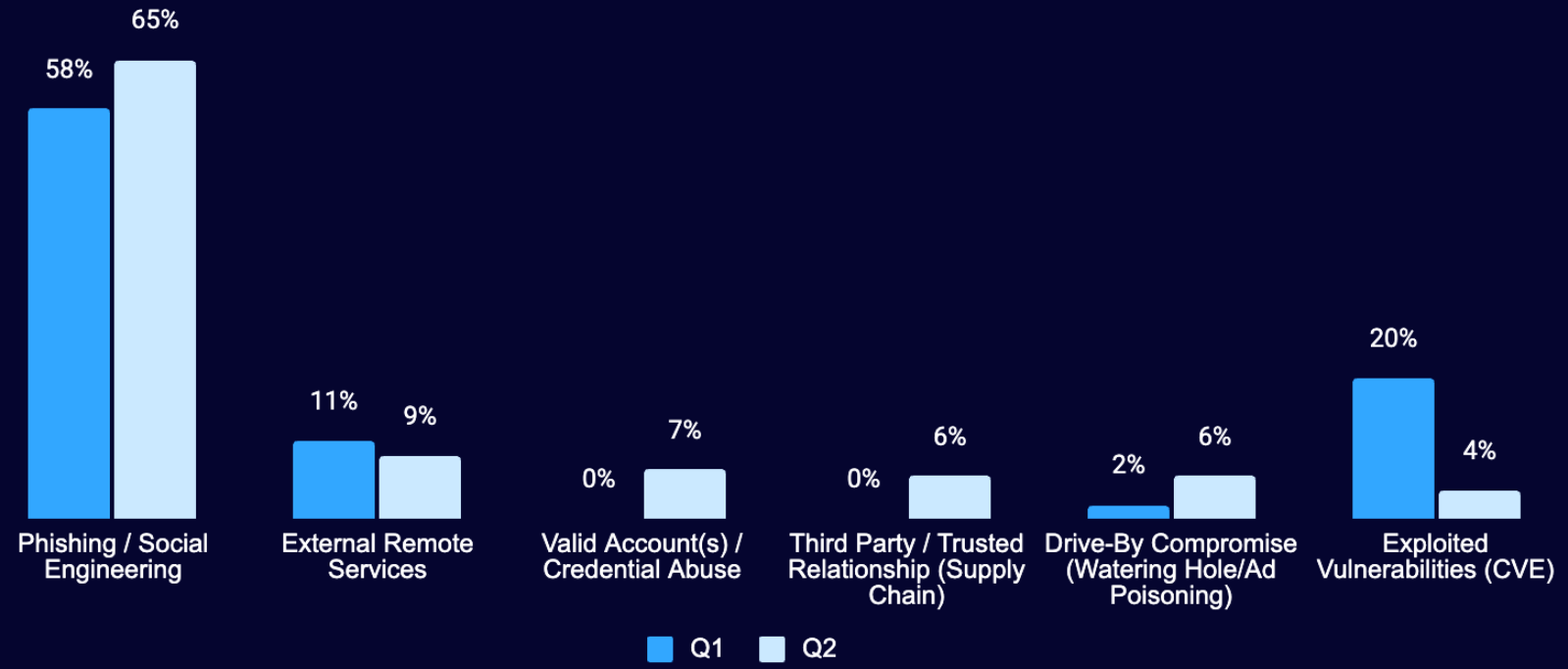
LevelBlue

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” • Phishing Email	• 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 over time



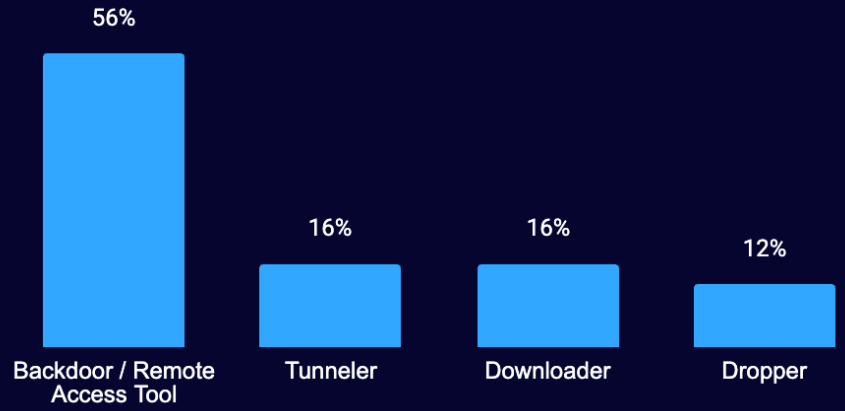
Most commonly observed CVEs – Q2 2026

CVE	Impacted product
CVE-2026-1281	Ivanti Endpoint Manager Mobile Unauthenticated remote code execution
CVE-2026-1340	Ivanti Endpoint Manager Mobile Unauthenticated remote code execution
CVE-2026-24858	Fortinet FortiAnalyzer authentication bypass
CVE-2026-41089	Windows Netlogon stack-based buffer overflow

CVE	Impacted product
CVE-2025-59718	Fortinet FortiOS improper verification of cryptographic signature
CVE-2025-59719	Fortinet FortiWeb improper verification of cryptographic signature
CVE-2025-62631	Fortinet FortiOS insufficient session expiration vulnerability
CVE-2024-55591	FortiOS authentication bypass
CVE-2023-20269	Cisco ASA remote access

2. Persistence – Q2 2026

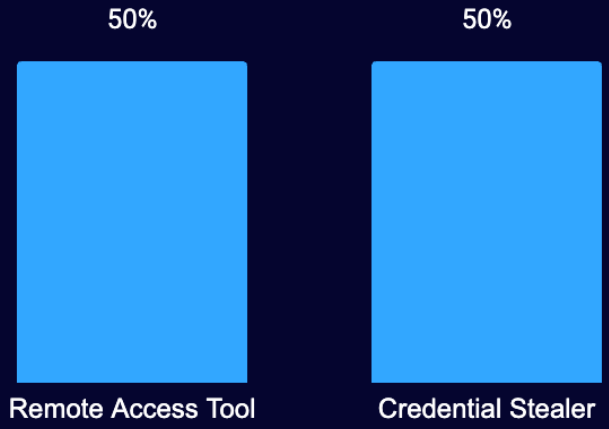
In cases where persistence was observed, the following malware/tools/techniques were most commonly leveraged



Name	Description
AnyDesk	Remote access tool
PSExec	Remote management tool
PowerShell	Command line
Frpc.exe	Tunneler

3. Escalation – Q2 2026

In cases where escalation was observed:

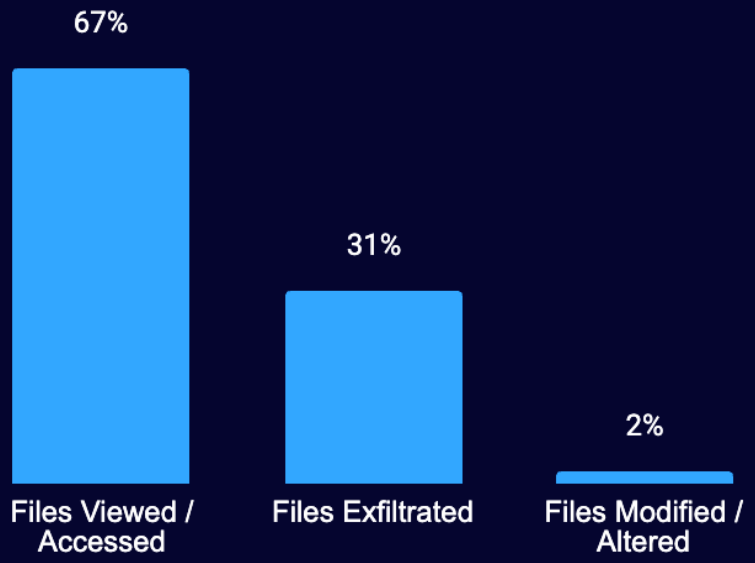


Observed tools/techniques used for escalation:

Name	Description
Powershell	Command line
NetScan	Network discovery tool
Psexesvc	Remote management tool
Mimikatz	Credential stealer
Kali	Penetration testing framework

4. Data at risk – Q2 2026

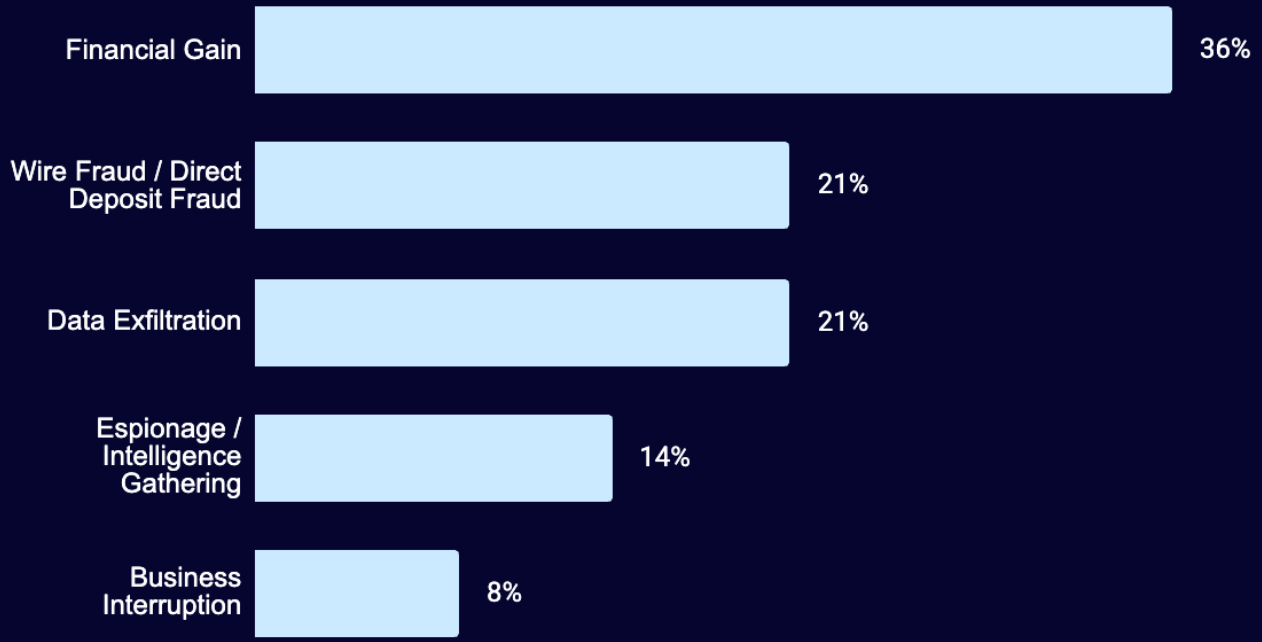
In cases where data at risk was observed:



Observed tools/techniques used for data at risk:

Name	Description
Rclone	Command-line program for file management
7-Zip	Software for compressing and archiving files
GraphAPI	Intermediary allowing program to request data or services from Microsoft

5. Threat actor end goal – Q2 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 and 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 and 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

LevelBlue

Secure What's Next.