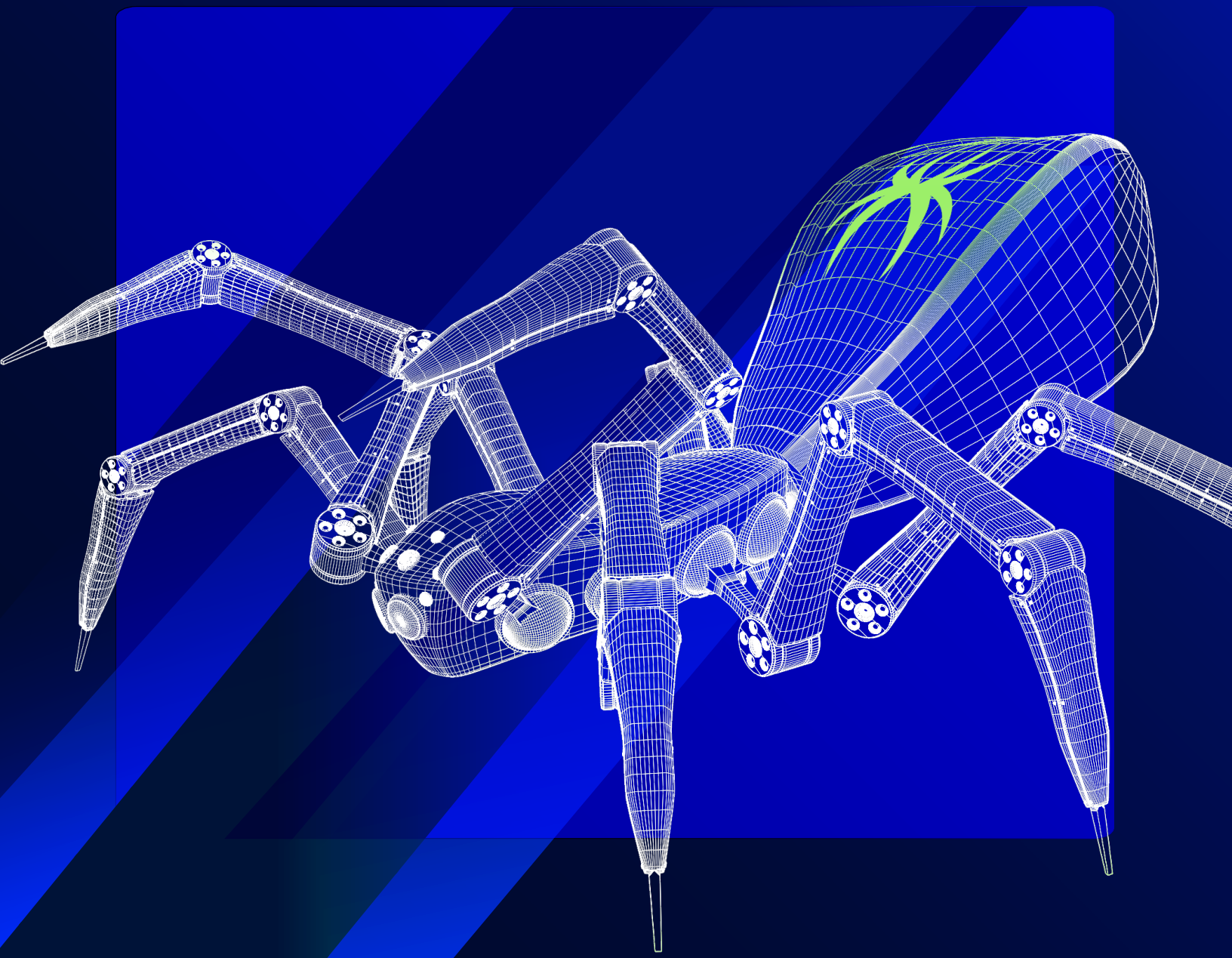
LevelBlue SpiderLabs

TTP Briefing Q3 2026:

Trusted access fuels data theft



LevelBlue SpiderLabs

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 SpiderLabs, which broadens the dataset behind our findings.

Key takeaways

01

Data exfiltration becomes the focus for attackers:

Data exfiltration now appears in 83% of intrusion cases, while encryption is at 67%. Both held at 77% in Q2. This indicates that attackers see the data itself as their leverage and are spending less time looking at it before they take it.

02

Identity is the thread through the intrusion:

Valid accounts increased this quarter, along with the use of credential stealers. Attackers holding legitimate credentials can blend into normal activity and need little malware, making them harder to spot.

03

Exploitation is back, and initial access diversifies:

Internet-facing flaws have become a more common initial access route as CVEs and external remote services were more exploited in Q3. Attackers are using a wider mix of entry points, including flaws like Metabase.

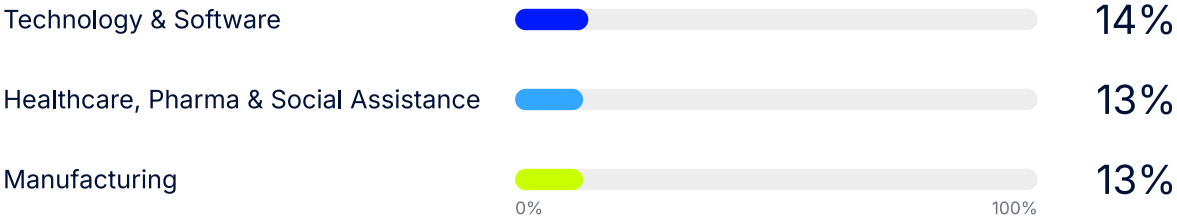
© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

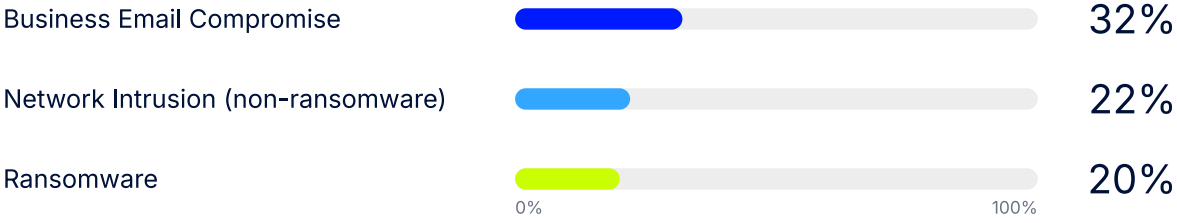
Quarterly data overview

What our IR teams saw this quarter: who was targeted, how attackers got in, what they did once inside, and how fast they moved. Each section closes with guidance defenders can act on now.

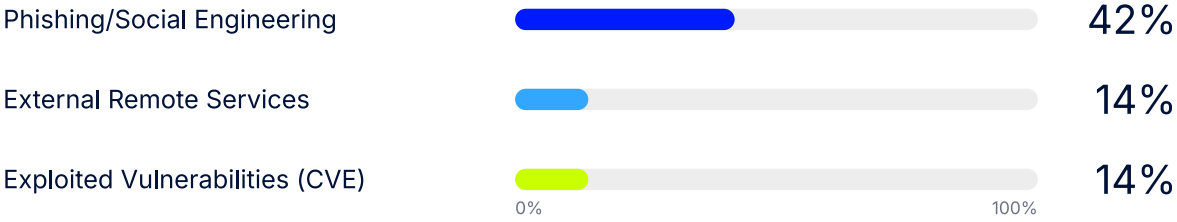
TOP 3 IMPACTED INDUSTRIES



TOP 3 INCIDENT TYPES



TOP 3 INITIAL INTRUSION VECTORS



Top 3 categories shown; percentages do not total 100%.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

MFA bypass

MFA is close to universal among the organizations we respond to, yet it no longer stops business email compromise. In Q3, threat actors bypassed MFA in 79% of BEC incidents where it was enabled.

MFA IMPLEMENTATION

84% → 91% → 90%

Q1 → Q2 → Q3 2026

MFA BYPASS

95% → 100% → 79%

Q1 → Q2 → Q3 2026

Although MFA remains widely deployed, attackers are increasingly sidestepping it through vishing, convincing victims to enroll an attacker-controlled device on their account. Because the victim approves the registration, the access appears legitimate, reflecting a shift from token interception to abuse of trusted device enrollment.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

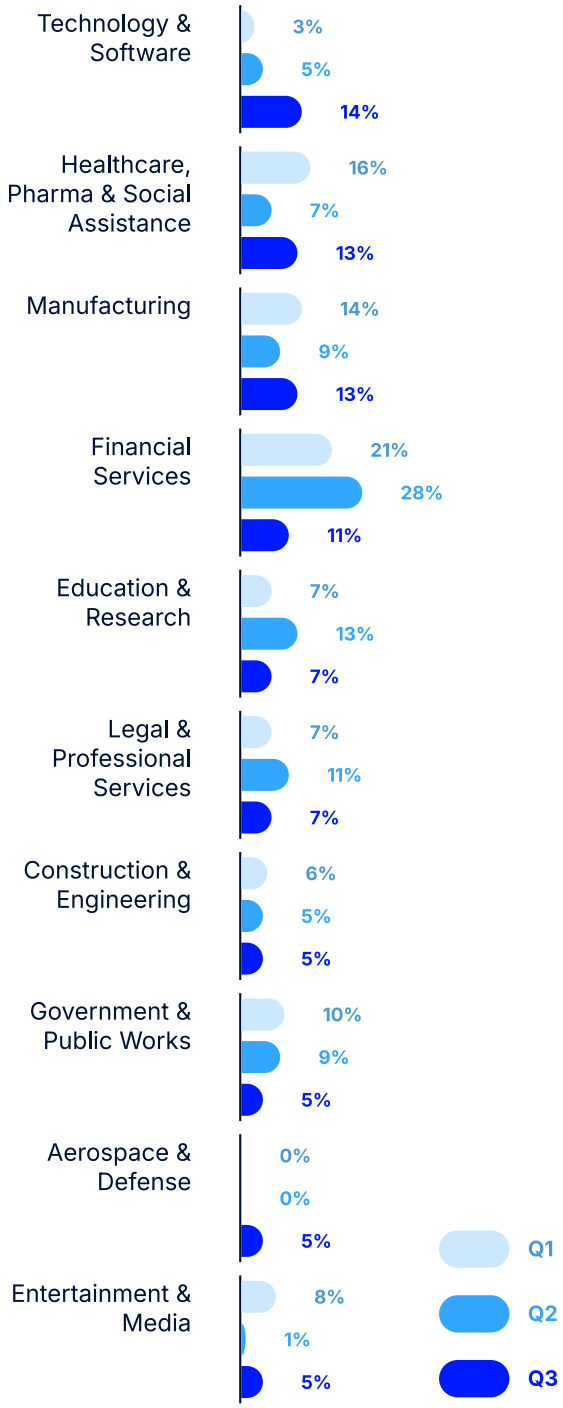
LevelBlue SpiderLabs

Top 10 impacted industries over time

Targeted industries shifted in Q3. Financial services, the most impacted sector for the last several quarters, dropped to fourth. Technology & software surged to the top spot, while healthcare and manufacturing tied for second. The takeaway is simple: no industry is off limits, and every sector should be investing in cyber resilience.

Technology & Software spike:

We observed an increase in compromised custom software and applications via exposed API keys, a trend that became more common in Q3 as threat actors used AI to hunt for exposed keys as an entry point into custom technologies. Because API keys are often long-lived, over-permissioned, and bypass MFA, a single exposed key can give direct access to sensitive data and connected systems. That reach, which can extend to a provider's customers, makes the sector an attractive target.



© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

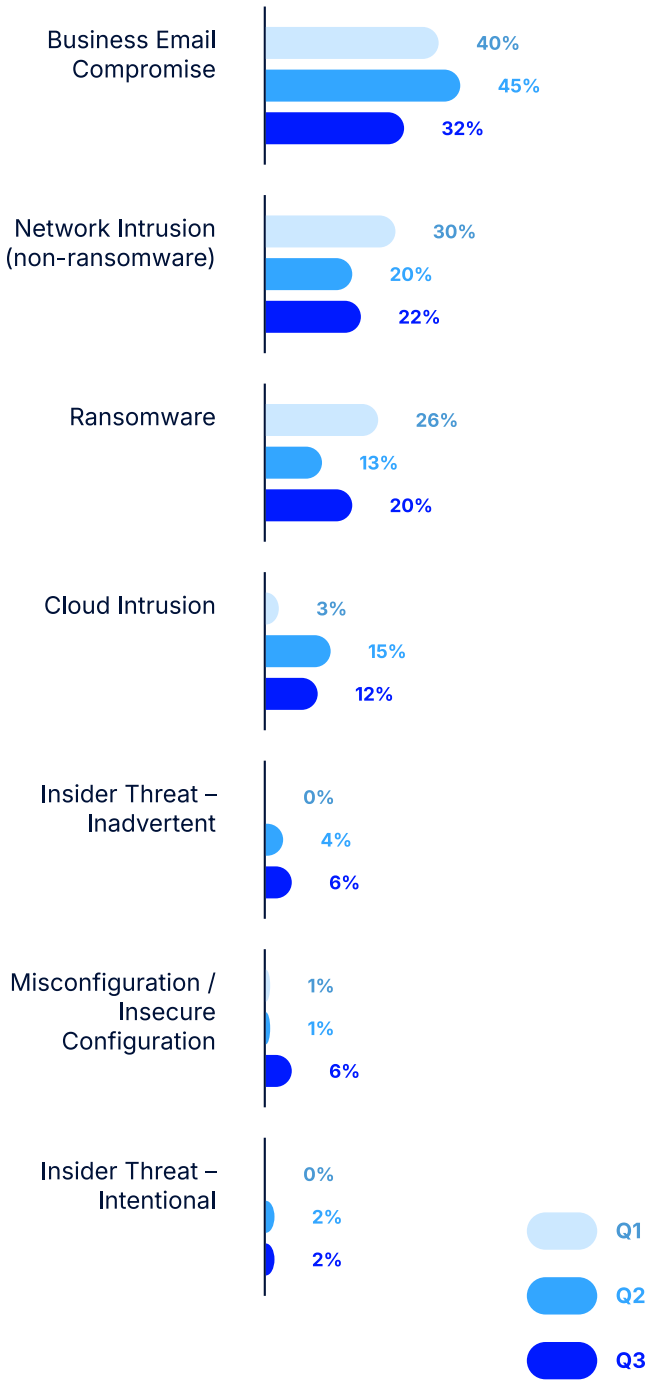
Most common incident types over time

BEC still leads, but the mix is shifting:

Business email compromise remained the most common incident type at 32% of engagements, down from 45% in Q2. Its share is shrinking because other incident types are growing, not because BEC is going away; with MFA bypassed in 79% of BEC cases where it was enabled, mailbox takeover remains a reliable payday.

Key takeaway:

Detection built around encryption events will miss a growing share of intrusions. Watch for large outbound transfers, unusual archive creation, and new cloud storage destinations.



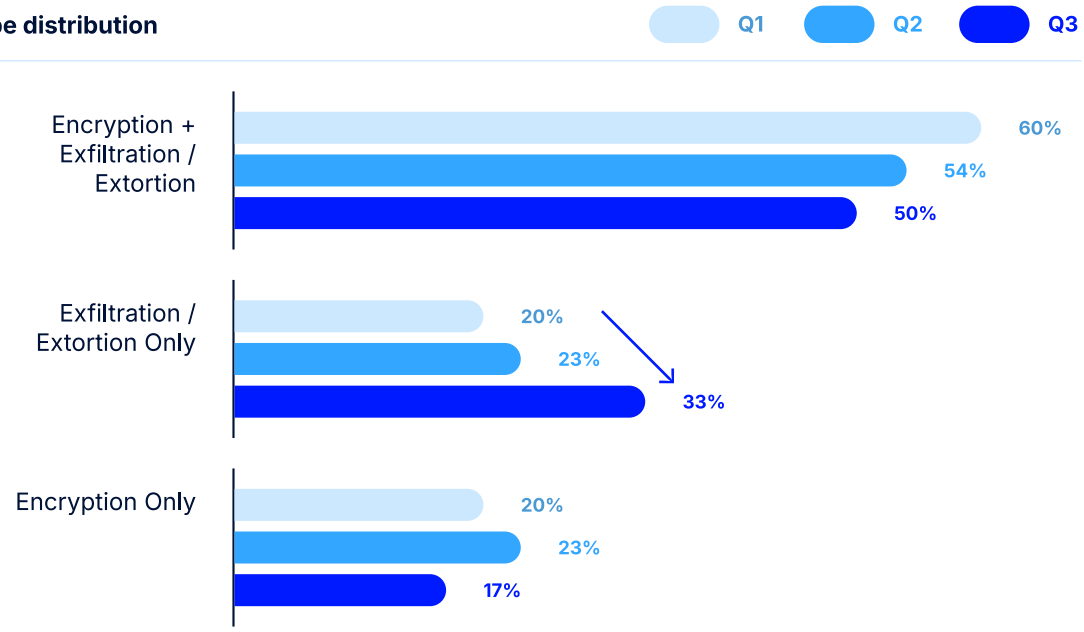
© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Dive into intrusions

Breakdown of ransomware variants and extortion groups. Threat actors are still leveraging encryption, but we have seen a surge in data exfiltration and extortion only.

Attack type distribution



Top observed variants and extortion groups

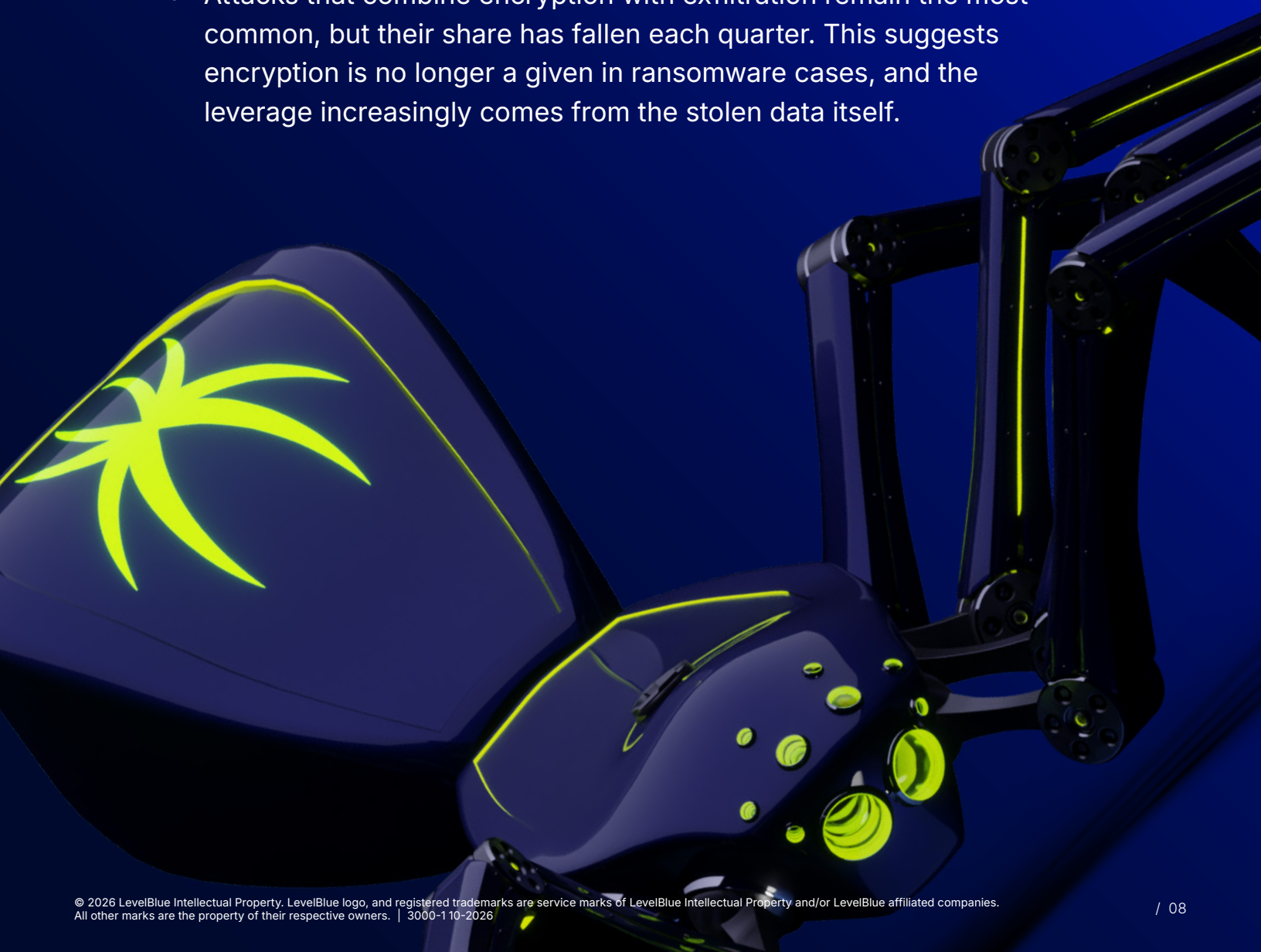
High Activity	Others
Akira	The Gentlemen
ShinyHunters	Icarus
Qilin	Play
INC	Termite
Helix	Chaos
	RansomHouse/Rabbit
	SilentTrouble
	Settra

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Key takeaway 1: Data exfiltration becomes the focus for attackers

- Exfiltration/extortion-only attacks were the fastest-growing category in Q3, with attackers stealing data and threatening to publish it without deploying ransomware.
- Attacks that combine encryption with exfiltration remain the most common, but their share has fallen each quarter. This suggests encryption is no longer a given in ransomware cases, and the leverage increasingly comes from the stolen data itself.



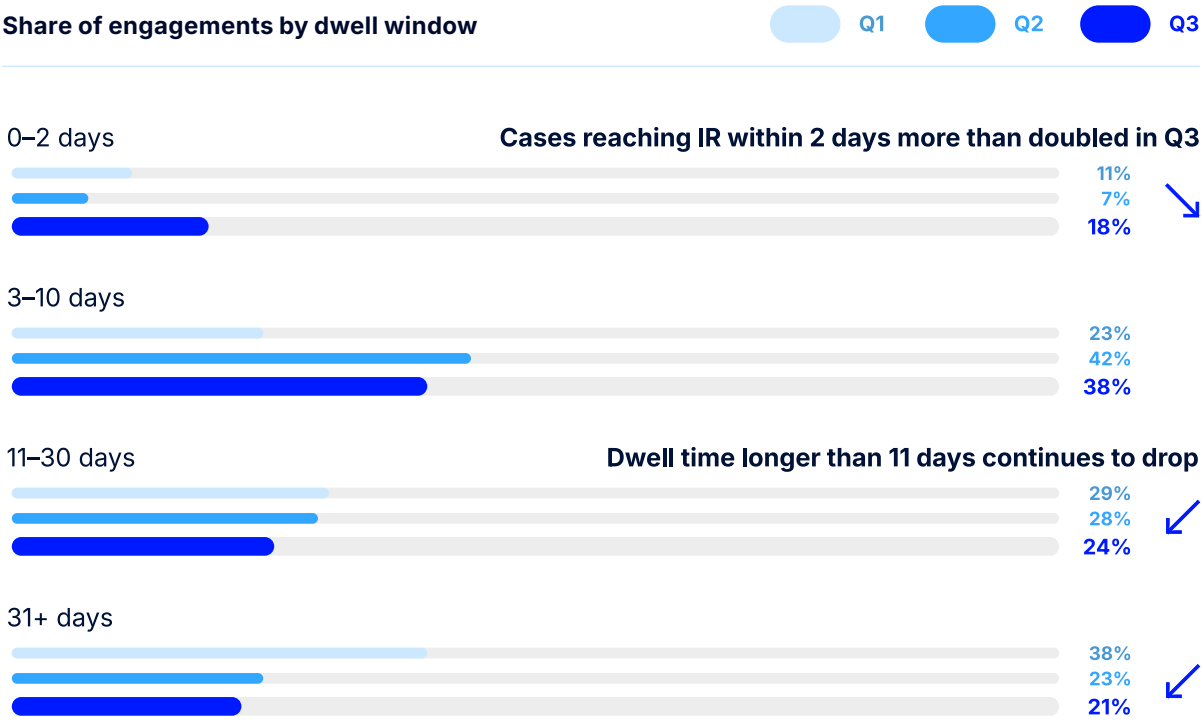
© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Dwell time: Initial intrusion to IR kickoff

Dwell time measures the gap between an attacker's first foothold and the moment our IR team is engaged, the clock defenders are racing against. This quarter it kept shrinking. Shorter windows can mean faster detection, faster attacker execution, or both, and in Q3 we saw plenty of the latter.

Share of engagements by dwell window



WHAT THE SHIFT SAYS

Attackers are executing faster than we have ever seen. Some intrusions now play out in hours instead of days, with threat actors using AI tools to move through networks. Detection is improving, but so is attacker speed.

56%

of engagements began within 10 days of compromise, up from 49% in Q2.

DATA NOTE

Dwell time is measured from the initial date of compromise to the date LevelBlue IR is engaged. Engagements involving LevelBlue MDR clients are excluded.

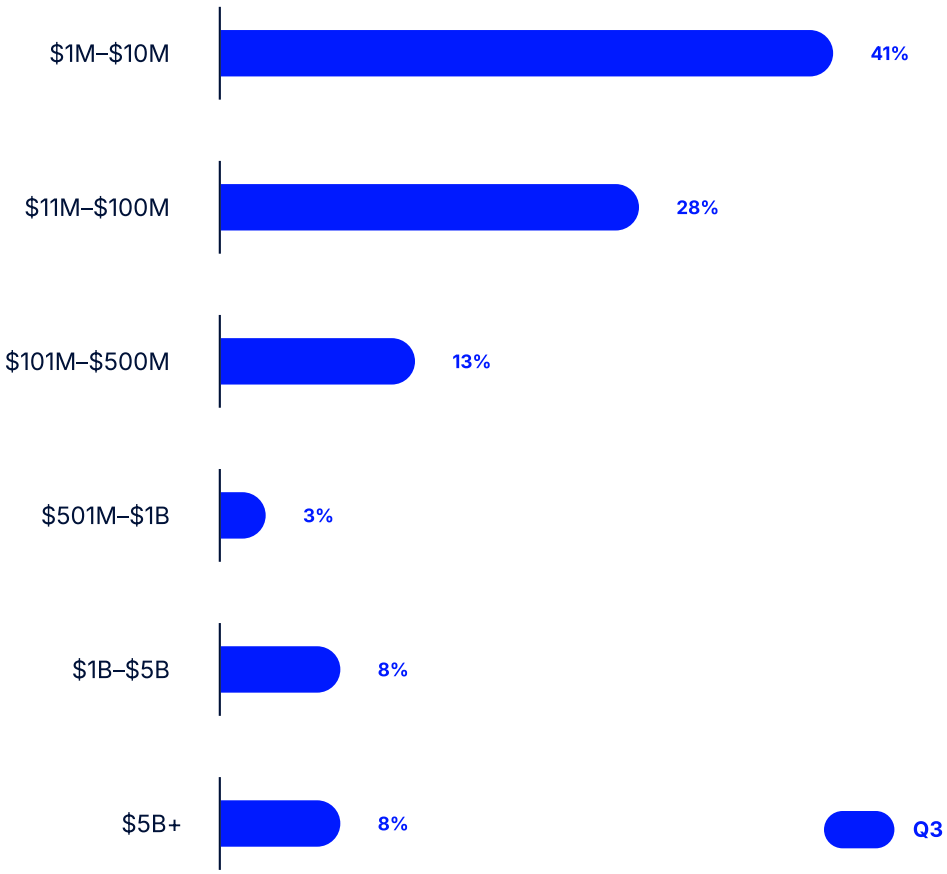
© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Company size

Organizations with $1M–$100M in revenue accounted for the largest share of incidents. Threat actors increasingly see mid-market companies as high-value, lower-resistance targets, with valuable data but rarely an enterprise-scale security team.

Based on revenue



© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Five phases of distinct activity: Trends across the intrusion path

01

Initial intrusion vector

External recon · Entry vector · Patient 0 · Phishing email

02

Persistence

Foothold · Internal recon Remote access/C2

03

Escalation

Asset discovery · Privilege escalation Lateral movement

04

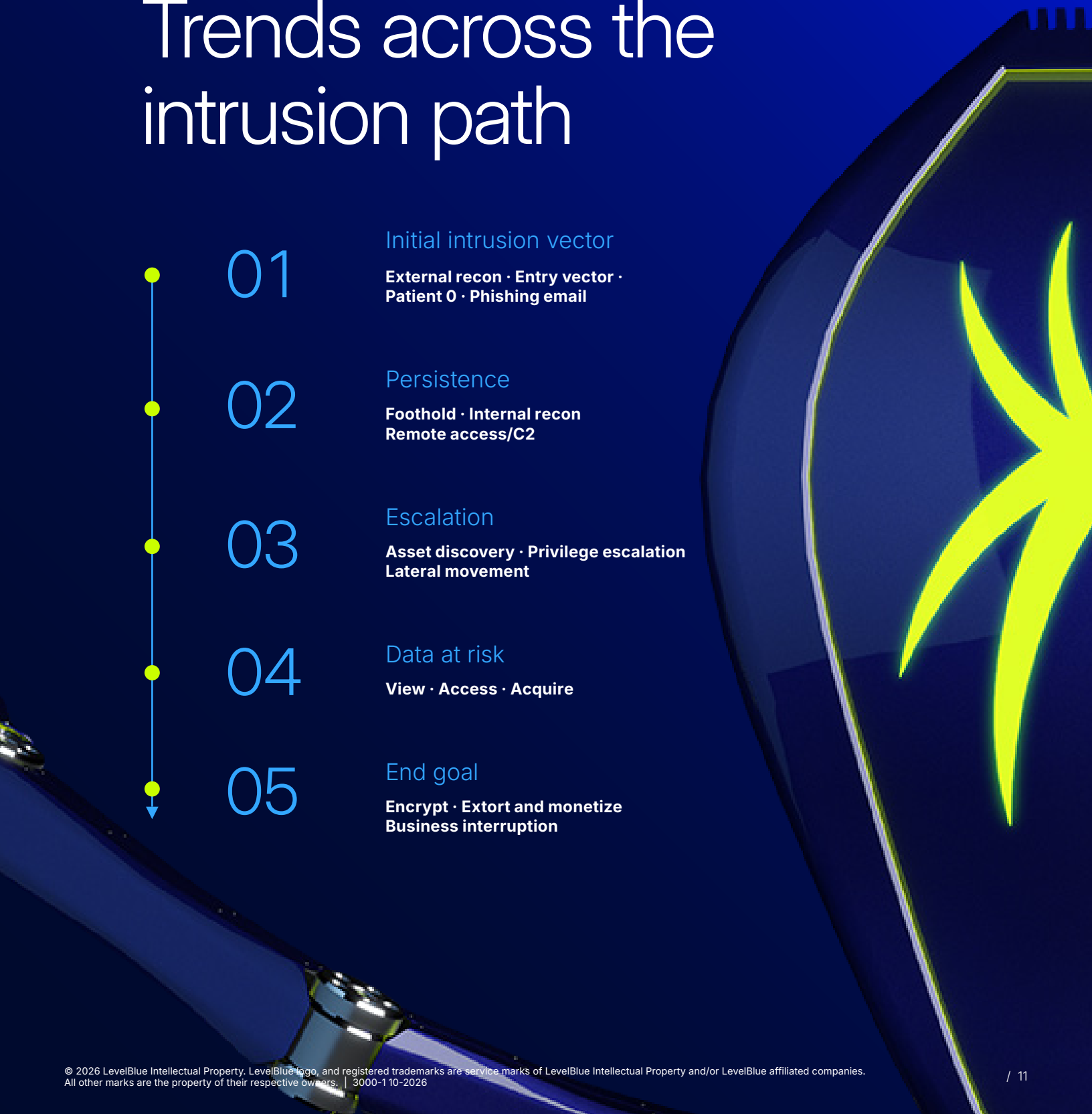
Data at risk

View · Access · Acquire

05

End goal

Encrypt · Extort and monetize Business interruption



© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 3000-1 10-2026

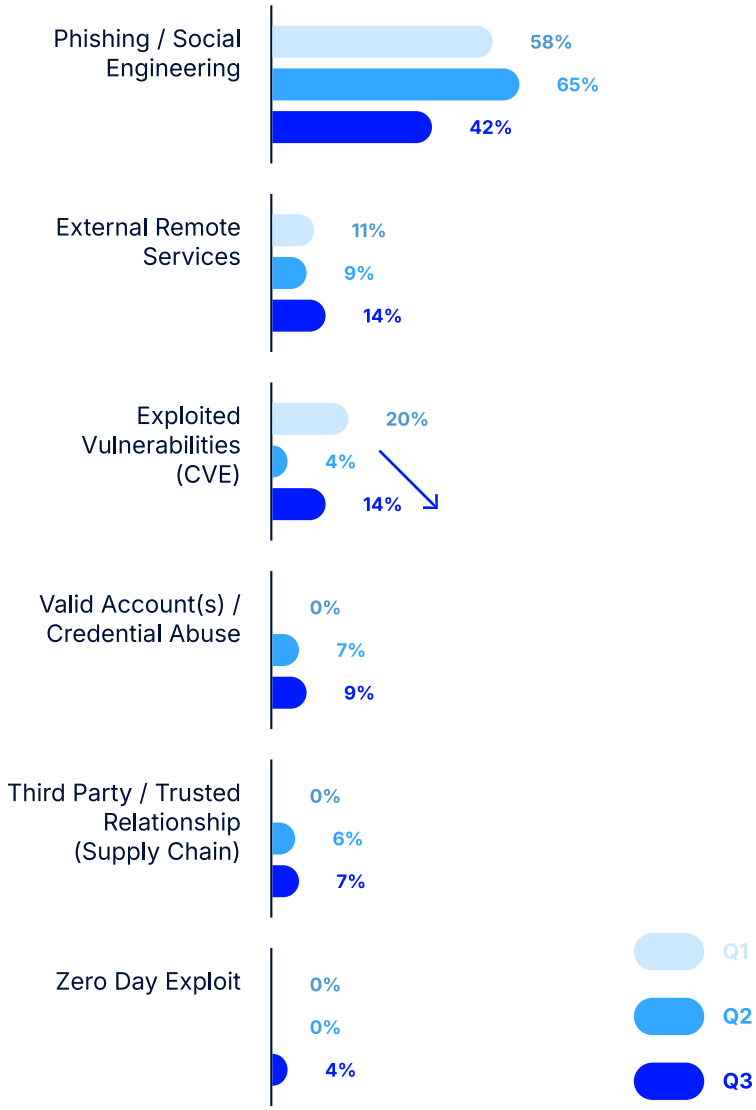
LevelBlue SpiderLabs

Stage 1
Initial intrusion vector over time

How threat actors are gaining access to networks and where the intrusion begins, including external reconnaissance and entry vector.

Phishing still dominates, but the door is widening:

Phishing remained the top initial intrusion vector in Q3 at 42%, down from 65% in Q2. External remote services (RDP, VPN) and exploited vulnerabilities tied for second at 14% each. Together, those two internet-facing routes now account for more than a quarter of initial access.



© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Key takeaway 2: Identity is the thread through the intrusion

- Valid-account abuse has grown each quarter. It is still a small share of initial access, but the direction is clear.
- Social engineering often ends in stolen identities. Phishing/social engineering remains the most common way in, and that category includes vishing and help-desk impersonation. Many of those cases result in stolen credentials or tokens, so identity likely plays a larger role than the valid accounts bar alone shows.



© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Most commonly observed CVEs

A patching priority list, not an index:
These are the vulnerabilities our IR teams saw actively exploited in real incidents this quarter, which makes them a sharper patching priority list than any CVSS score.

CVE	Impacted product
CVE-2026-0257	Palo Alto Networks PAN-OS GlobalProtect authentication bypass
CVE-2026-25639	Axios (JavaScript HTTP client) denial of service
CVE-2026-72898	Metabase unauthenticated SQL injection
CVE-2025-13407	Gravity Forms WordPress plugin unauthenticated arbitrary file upload
CVE-2024-40762	SonicWall SonicOS SSLVPN weak PRNG in authentication token generator
CVE-2024-40766	SonicWall SonicOS SSLVPN improper access control
CVE-2024-53704	SonicWall SonicOS SSLVPN authentication bypass
CVE-2024-53705	SonicWall SonicOS server-side request forgery (SSRF)
CVE-2022-26923	Microsoft Active Directory Domain Services elevation of privilege

INSIDE THE CVE NUMBERS:

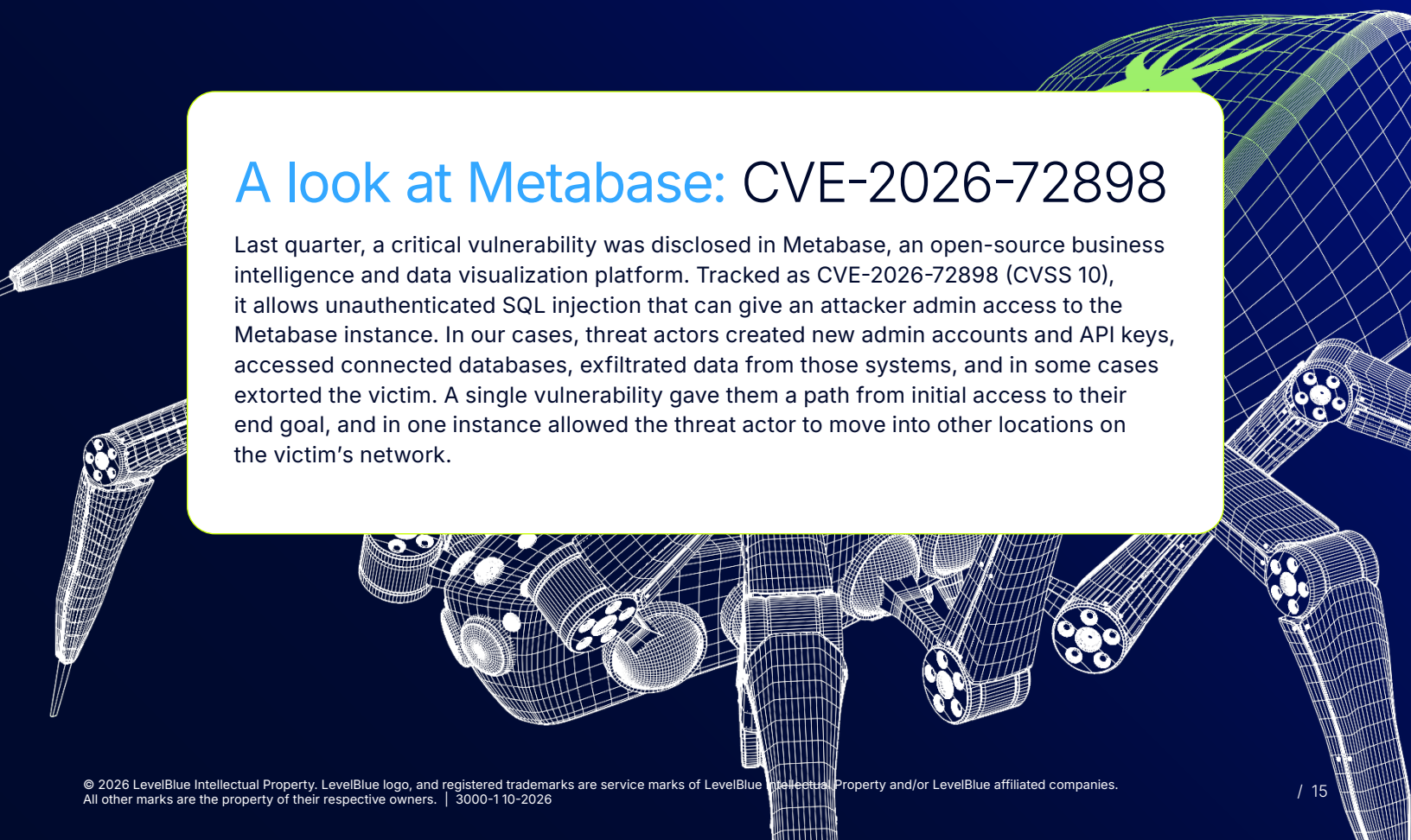
Inventory internet-facing business applications, not just network appliances. If it touches sensitive data and faces the internet, it belongs on the emergency patch list.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Key takeaway 3:
Exploitation is back, and initial access diversifies

- While social engineering remains a top concern, internet-facing flaws have increased as an initial access route, with CVEs and external remote services both rising in Q3. Attackers are using a wider mix of entry points, including vulnerabilities like Metabase.



A look at Metabase: CVE-2026-72898

Last quarter, a critical vulnerability was disclosed in Metabase, an open-source business intelligence and data visualization platform. Tracked as CVE-2026-72898 (CVSS 10), it allows unauthenticated SQL injection that can give an attacker admin access to the Metabase instance. In our cases, threat actors created new admin accounts and API keys, accessed connected databases, exfiltrated data from those systems, and in some cases extorted the victim. A single vulnerability gave them a path from initial access to their end goal, and in one instance allowed the threat actor to move into other locations on the victim's network.

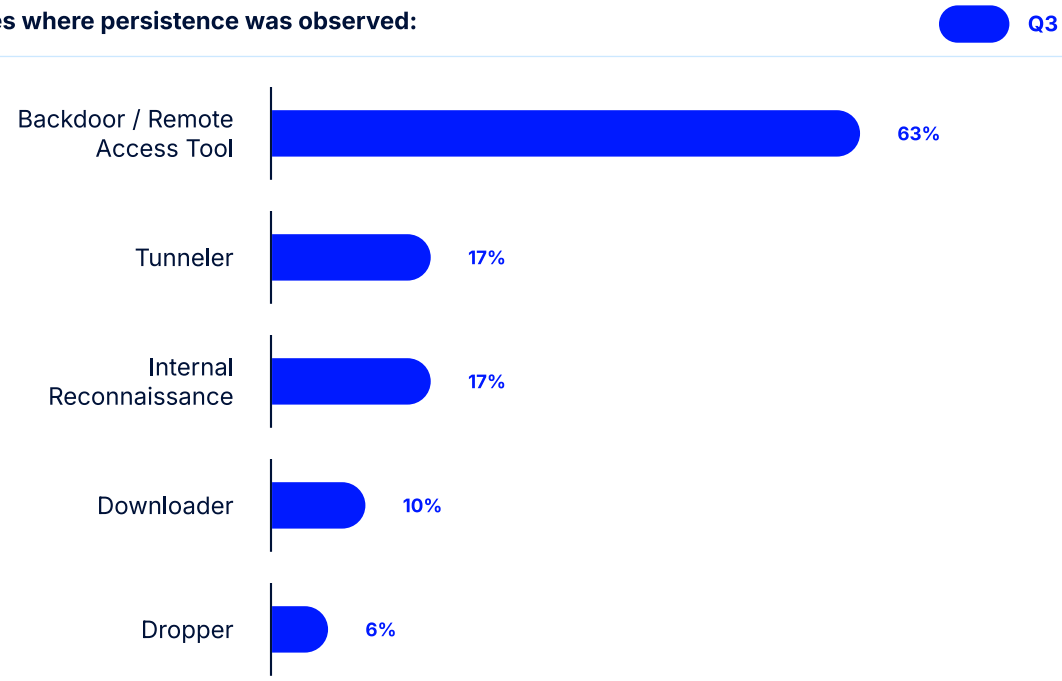
© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Stage 2
Persistence

Steps threat actors take to ensure access to a network once inside. How they are gaining a foothold, internal reconnaissance, and gaining remote access.

In cases where persistence was observed:



Observed tools/techniques used for persistence

Name	Description
NetScan	Network discovery tool
PowerShell	Command line
Matanbuchus	Malware-as-a-Service
ScreenConnect	Remote access tool
MeshAgent.exe	Remote access tool
Cloudflare Tunnel	Cloud-based threat protection platform

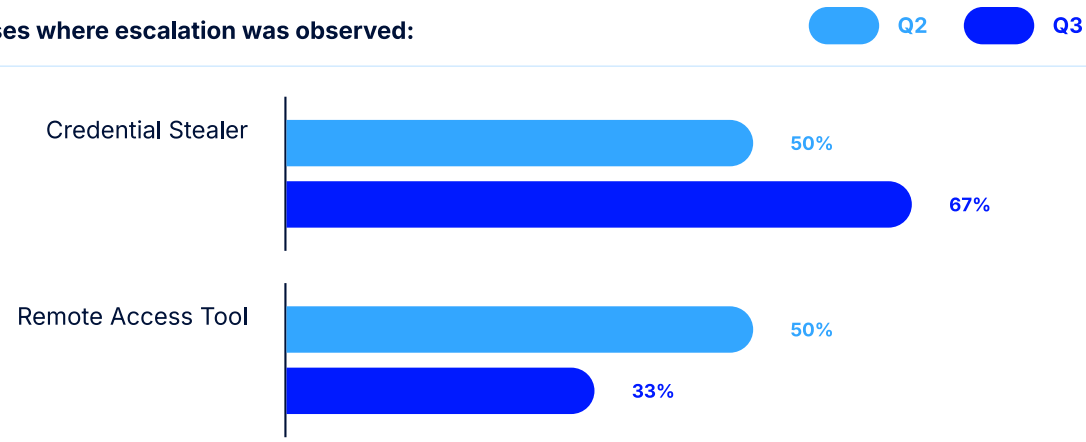
© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Stage 3 Escalation

Threat actors escalate capabilities during this stage of the intrusion path. They are performing asset discovery, privilege escalation, and executing lateral movement.

In cases where escalation was observed:



Observed tools/techniques used for escalation

Name	Description
PSEXESVC	Remote management tool
Mimikatz	Credential stealer
Kali Linux	Penetration testing operating system
DCSync	Credential stealer
Msconfig.exe	System configuration tool used to disable services and startup items
NetExec	Penetration testing framework

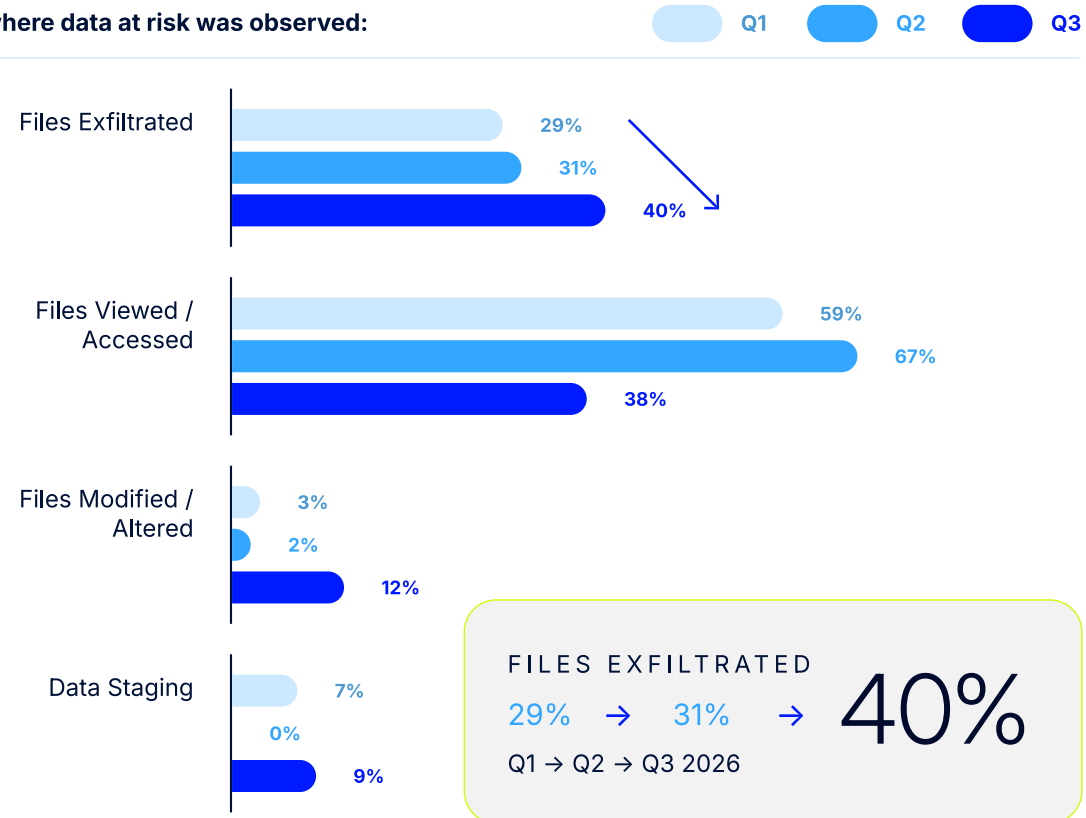
© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Stage 4
Data at risk

Data officially at risk. What was accessed and how?

In cases where data at risk was observed:



FILES EXFILTRATED

29% → 31% → 40%

Q1 → Q2 → Q3 2026

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
MEGAsync	File transfer service
WinRAR	Software for compressing and archiving files
WinSCP	Open-source SFTP client

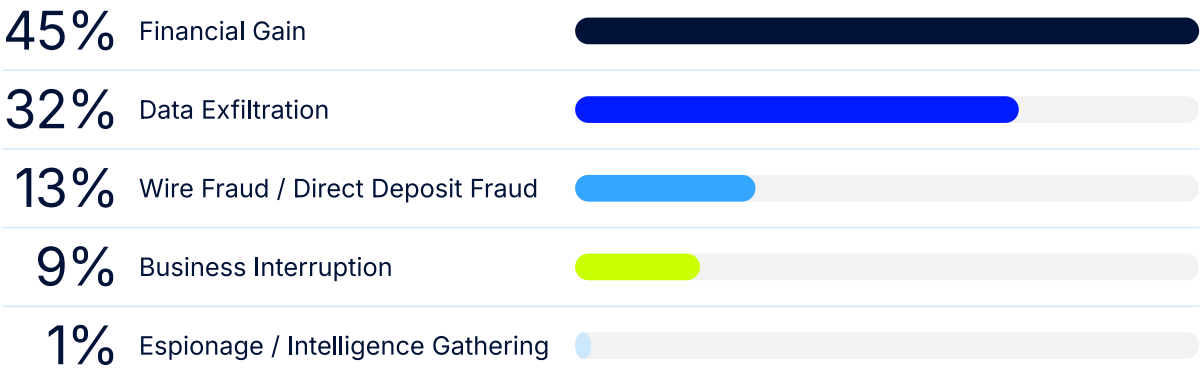
© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue SpiderLabs

Stage 5
Threat actor end goal

Every intrusion technique eventually serves one of these outcomes. Knowing which goal is trending helps prioritize defenses around what attackers are actually trying to accomplish.

Share of intrusions by end goal



77%

of intrusions aimed at Financial Gain (45%) or Data Exfiltration (32%).

Q3 2026 • TOP END GOALS

Espionage / Intelligence Gathering accounted for just 1%, the smallest share this quarter.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026

LevelBlue

Defender priorities: 5 actions for Q4

01

Defend the session, not just the login:

Deploy phishing-resistant MFA, then shorten token lifetimes, monitor session tokens continuously, and enforce conditional access.

02

Govern third-party app consent:

Restrict user consent to OAuth apps, review existing grants, and rotate API keys used by vendor integrations.

03

Patch the edge on an emergency cadence:

Treat VPNs, firewalls, and internet-facing apps as the front line; lock management interfaces to trusted networks.

04

Detect data leaving, not just data locked:

Alert on bulk exfiltration, archive staging, and new remote management tools, not only on encryption.

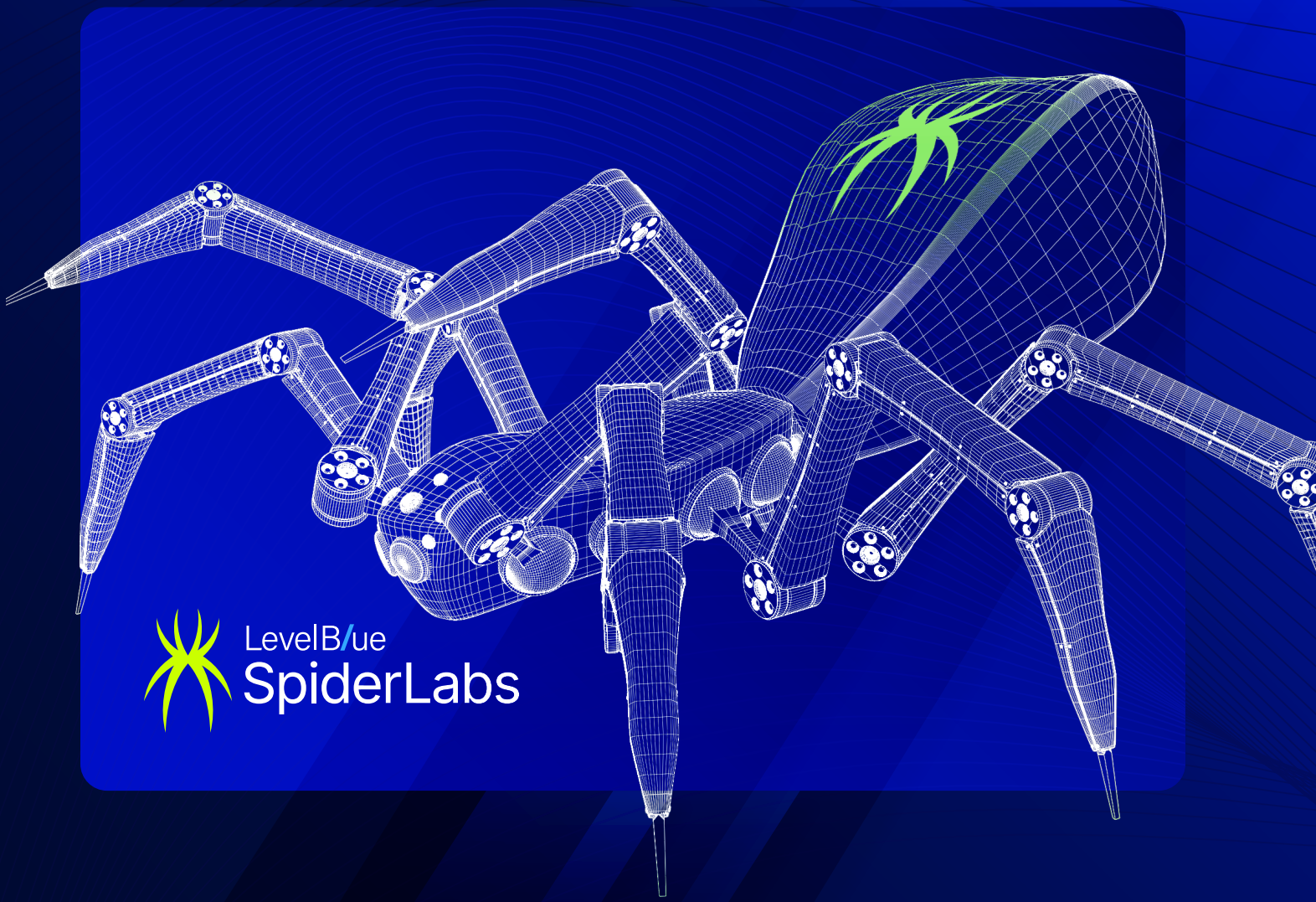
05

Plan for hours, not weeks:

Pre-authorize containment actions and keep an IR retainer in place so response starts the moment an alert fires.

For more information about this report, contact a LevelBlue expert at **levelblue.com/irr**

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 3000-1 10-2026



levelblue.com
levelblue.com/irr

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies.
All other marks are the property of their respective owners. | 3000-1 10-2026