INSIGHTS FOR SOC TEAMS

ANY RUN

Q1 2026 Cyber Risk Report

About ANY.RUN

ANY.RUN delivers award-winning malware analysis and threat intelligence solutions designed to reduce uncertainty in security operations and enable faster, more confident response to critical threats.

Trusted by over 600,000 security professionals in 15,000 organizations, ANY.RUN supports security teams at leading companies worldwide in managing cyber risks.

Report Methodology

This report is based on **2,101,483 malware and phishing investigations** from Q1 2026 conducted inside ANY.RUN's Interactive Sandbox.

The data reflects actual security operations, focusing on how attacks behave in practice: How access is gained and and how long it takes to reach impact.

The report identifies critical breakdown points:

- Where threats are missed despite detection
- When response is delayed due to lack of clarity
- Where cyber risk accumulates unrecognized

This provides a view of cyber risk aligned with business impact, highlighting where and why organizations lose control.

Executive Summary

1

Early-stage compromise is an unmanaged risk

Initial compromise increased by 84% and loader-based entry by 98.3%, indicating attackers' growing reliance on tools to establish access for follow-on activity.

2

Identity is the most exposed layer

Credential theft grew by 14.7% and surveillance by 34.4%, showing that attackers are operating through valid access with limited visibility.

3

Phishing focuses on immediate access

Session interception tools such as Sneaky2FA (+76.8%) and EvilProxy (+17.7%) allow attackers to gain access instantly.

4

Persistent access introduces long-term exposure

Windows service abuse for persistence grew by 89.3%, increasing the likelihood that access remains after response and leads to repeat compromise.

5

Tooling fragmentation is increasing coverage gaps

AgentTesla grew by 87.9% while Lumma dropped by 45.9%, showing rapid rotation across malware families and reducing predictability.

6

Attacks are narrowing around high-impact vectors

Email-based delivery exceeds 49%, and executable files are increasing, creating dependency on a limited set of vectors that drive most risk.

7

Malicious activity is hiding in normal operations

PowerShell (+17.4%) and JavaScript (+58.4%) are used to execute attacks within trusted environments.

Key Stats CISOs Need to Know

Understanding the speed and vectors of modern attacks is crucial for prioritizing defenses and building effective security strategies.

+14.7%

Credential Theft

Increase in Q1 2026 in attacks targeting user credentials.

+98.3%

Loader-Based Attacks

Significant growth in initial compromise via loaders.

+58.4%

Rise in LOLBAS Attacks

Based on the number of T1059.007 detections in Q1 2026.

16 sec

LOTL Execution

Median time for attackers to utilize native system tools.

21 sec

Persistence

Median time for attackers to establish long-term access.

49.5%

Email-Initiated Attacks

Percentage of attacks originating from email vectors.

Trend 1: Initial Compromise Is Now the Primary Point of Failure

The most critical shift in Q1 2026 is that **attacks are determined at the moment of entry**, while that same moment is becoming harder to recognize and act on.

Initial Compromise: Structural Blind Spot

The Scale of the Trend

Initial compromise increased by **+84%**. This points to a clear expansion in attacks designed to establish footholds rather than deliver immediate payloads. Loaders are used to gain controlled execution, assess the environment, and enable follow-on actions, including resale of access.

+98.3%

Increase in Loader-Based Attacks in Q1 2026

This aligns with the growing role of access brokers in the threat landscape. Compromised endpoints are no longer the end goal of an attack. They are an asset that can be reused, transferred, or monetized. As a result, the volume of initial access attempts increases, and the barrier to launching follow-on attacks decreases.

Why SOCs Are Struggling

Activity Blends into Trusted System Behavior

Use of PowerShell and JavaScript (+17.4% and +58.4%) makes malicious execution indistinguishable from legitimate operations at entry.

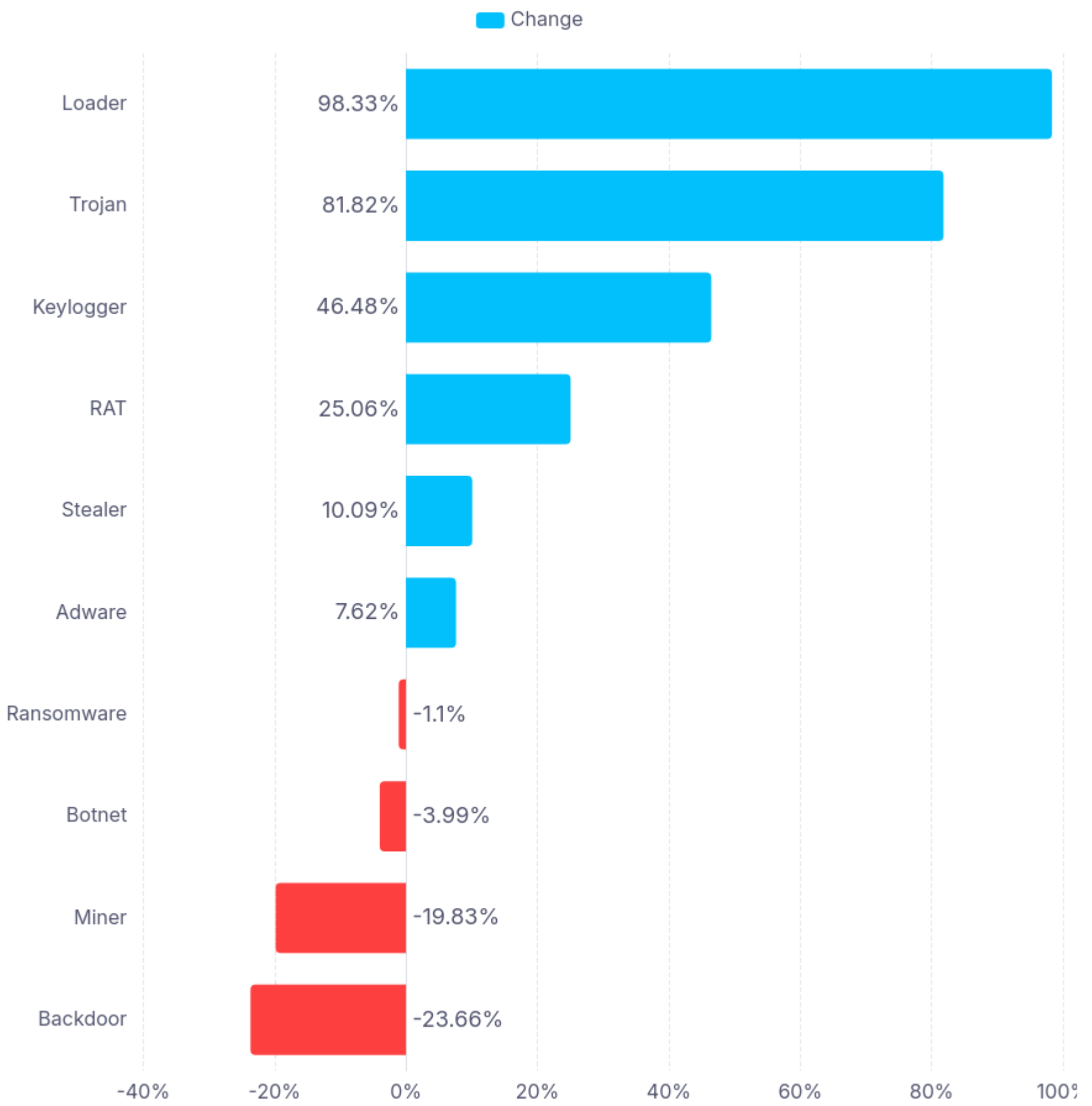
No Clear Malicious Artifact to Trigger Response

Absence of binaries removes high-confidence indicators that SOC workflows depend on for escalation.

Escalation is Delayed Until Later Stages

Malicious intent becomes visible only after multiple steps, by which point access and persistence are already established.

Malware Type Detections: Q4 2025 vs. Q1 2026



Strategic Shift: What CISOs Need to Change

CISOs need to reduce the value of initial access by limiting what loaders can actually achieve, enforce strict privilege boundaries, isolate user environments, and constrain outbound communication so early footholds can’t be expanded, validated, or monetized.

> Initial access must be treated as a high-risk condition at the moment it occurs, even when signals are incomplete or ambiguous. Speed of interpretation becomes the primary control mechanism.

Where to Focus Effort

1

Constrain initial execution context

Limit what can run and from where to reduce loader execution paths early.

2

Restrict outbound communication

Block unknown external connections to prevent payload retrieval and access validation.

3

Enforce least privilege by default

Minimize user rights to limit escalation and lateral movement after execution.

4

Isolate high-risk user activity

Contain browser and email activity in controlled, isolated environments.

Trend 2: Identity Has Become the Primary Attack Surface

Attackers are shifting from exploiting systems to operating through identity, **using valid credentials to access and control environments**. This reduces visibility while enabling a sustained focus on establishing, validating, and maintaining access rather than immediate disruption.

Identity Under Attack: Data and Implications

What Changed in Q1

Instead of forcing entry through vulnerabilities, attackers gain access through credentials and then act within legitimate sessions. This shifts the point of control from infrastructure to identity, while reducing the visibility of malicious activity.

Objective	Q4 2025	Q1 2026	Change
Credential Theft	43,220	49,569	+14.7%
Surveillance	9,077	12,198	+34.4%

Credential theft increased by **+14.7%**, surveillance activity grew by **+34.4%**, and Remote Access Trojans (RATs) increased by **+25.1%**. Together, these trends show a coordinated shift toward establishing, validating, and maintaining access rather than triggering

Business Security Impact

Harder to Detect Takeover

No failed logins or exploit attempts to trigger alerts when access is gained through valid credentials.

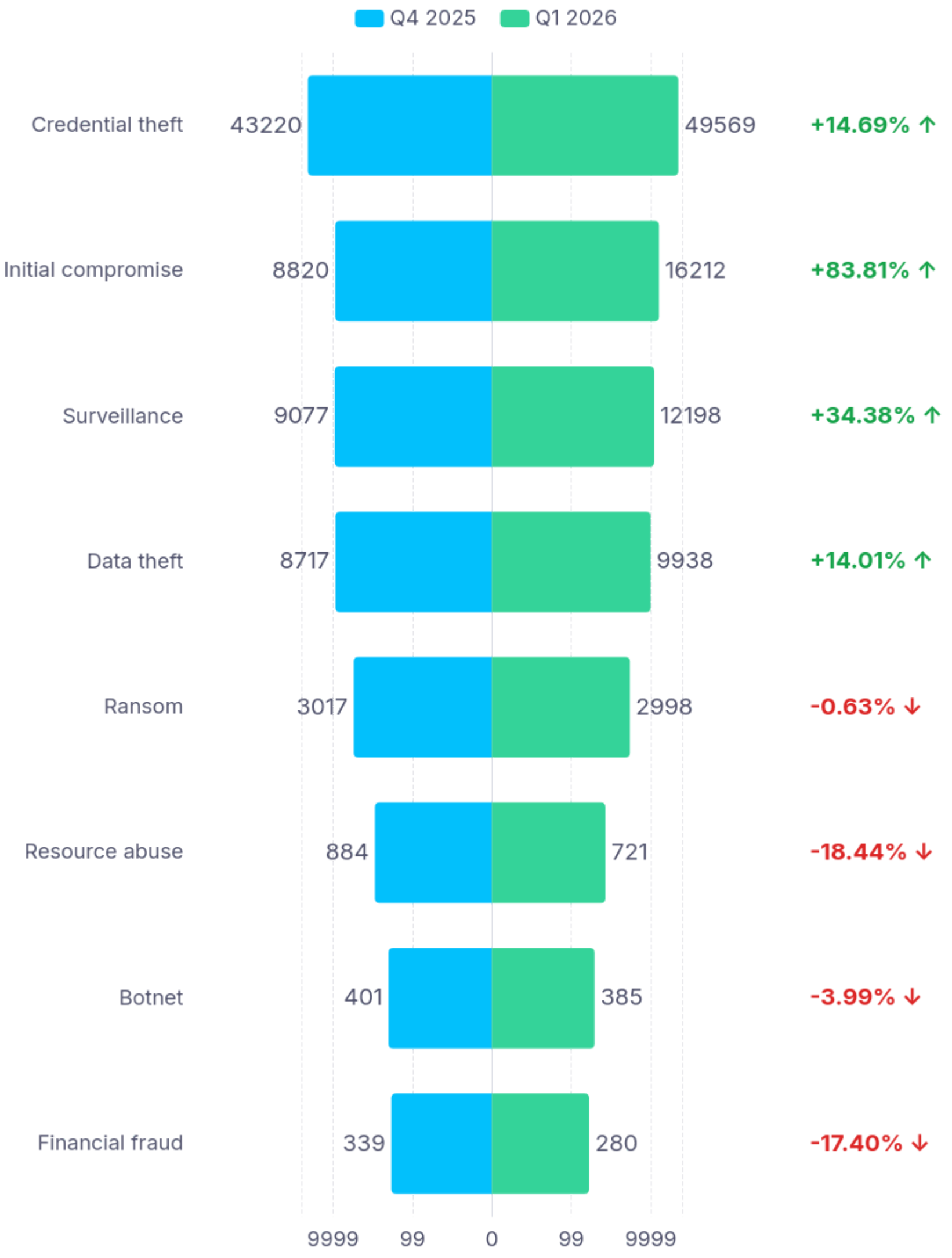
Fraud & Data Access Risk

Valid sessions allow direct interaction with sensitive systems without triggering alerts.

Complex Attribution

Actions are tied to legitimate users, not external actors, increasing operational risk and incident cost.

Cyber Threats by Attack Objective: Q4 2025 vs Q1 2026



Strategic Shift: What Needs to Change for Identity

Identity can no longer be treated as a control that is validated only at login. Access must be continuously evaluated based on behavior, context, and usage.

The priority shifts from authentication assurance to ongoing access validation.

Where to Focus Effort

1

Monitor identity behavior after authentication

Track how accounts are used, not just how they log in.

2

Correlate identity with endpoint and session activity

Link user actions to device behavior and system interaction.

3

Prioritize credential exposure and access anomalies

Treat suspicious access patterns as high-risk signals, even without clear compromise.

3 steps to building defense against phishing-based identity compromise

Learn practical steps CISOs can use to strengthen phishing detection across monitoring, triage, and response to reduce risk and improve SOC performance.

Read more →

Trend 3: Phishing Is Aiming for Immediate Access

Phishing has shifted from collecting credentials to obtaining direct, authenticated access. Attackers try to **gain control of a live session at the moment of user interaction**.

Phishing Moves from Credential Theft to Session Control

Phishing kits have become industrialized and focused on session interception. They proxy authentication flows, allowing users to log in and complete MFA while the session is captured and transferred to the attacker.

Established Kits Growing Rapidly

Phishkit	Q1 Change
Sneaky2FA	+76.8%
EvilProxy	+17.7%

New Kits Reaching Operational Scale

Phishkit	Q1 Detections
FlowerStorm	3,376
EvilTokens	683

Emerging blind spot: token-based phishing via OAuth flows

Phishing kits like **EvilTokens** exploit OAuth flows (e.g., Microsoft 365 Device Code) to gain access without stealing credentials. Users approve legitimate logins, and attackers receive access tokens directly.

Read more →

Business Implications

Reduced Detection Window

No gap between compromise and active use means traditional alerts are not triggered in time.

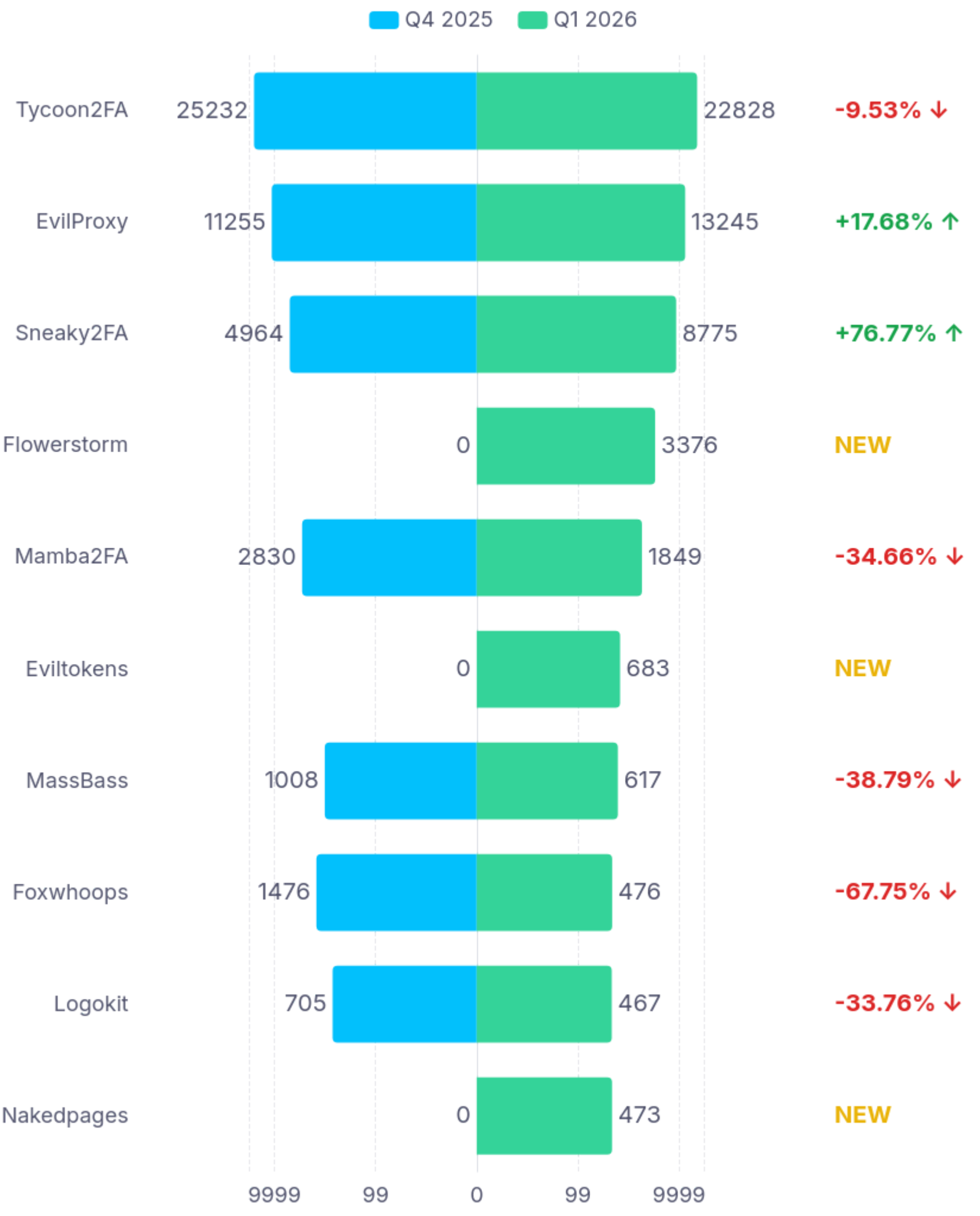
MFA No Longer Sufficient

MFA no longer acts as a reliable barrier on its own. Higher success rates for attackers result.

Immediate Account Takeover

Attackers get access at the moment of user interaction without a delay between compromise and active use.

Phishing-as-a-Service Kit Detections: Q4 2025 vs. Q1 2026



Strategic Shift: What Needs to Change for Phishing

Phishing defense can no longer focus only on preventing credential theft. The priority shifts to controlling what happens **after authentication** and detecting misuse of valid sessions.

Security Investment Priorities

1

Phishing-resistant authentication

Adopt FIDO2 or hardware-backed methods that reduce exposure to session interception.

2

Session-level detection and response

Enable monitoring and rapid termination of suspicious sessions and token activity.

3

OAuth and application access governance

Control and audit third-party app permissions and token issuance.

4

Integrated identity and access telemetry

Combine authentication, session, and endpoint data for faster investigation and response.

Trend 4: Persistence Is Moving Deeper and Becoming Harder to Eradicate

Persistence has evolved beyond staying on a machine. It now **embeds access in a way that survives investigation,** blends into normal operations, and allows attackers to re-enter even after partial remediation.

Persistence: Deeper, Stealthier, Harder to Remove

Persistence is becoming less event-driven and more structural. Removing the initial payload or access vector is no longer sufficient. The attacker may still retain control through embedded mechanisms. This shifts the problem from "detect and remove" to "detect, verify, and continuously ensure removal."

Technique	Q4 2025	Q1 2026	Change
T1543.003 (Windows Service)	2,621	4,962	**+89.3%**
T1547.001 (Registry Run Keys)	11,559	13,291	**+15%**
T1569.002 (Service Execution)	10,046	12,877	**+28.2%**

Attackers are moving away from visible techniques and integrating into system services and configuration layers that survive reboots, avoid obvious indicators of compromise, and blend into legitimate system behavior.

21 sec

Median Time-to-Persistence

Business Implications

Longer Dwell Time inside Systems

Attackers maintain access across extended periods, increasing the scope of potential damage.

Incomplete Remediation

Systems may appear clean while persistence remains active, creating false confidence in response.

Repeat Compromise

Attackers can re-enter without repeating initial access steps, increasing operational cost.

Strategic Shift: What Needs to Change for Persistence

Persistent access must be treated as a long-term risk, not merely a technical artifact of an incident. The objective shifts from removing visible threats to proactively verifying that all embedded access mechanisms have been fully eliminated.

Where to Focus Effort

1

Deep endpoint visibility and forensics

Invest in solutions capable of detecting service abuse, registry changes, and other low-visibility persistence mechanisms.

2

Continuous integrity monitoring

Establish baselines for critical system configurations and implement alerting for any unauthorized deviations.

3

Post-incident validation workflows

Develop and enforce processes that confirm full remediation and eradication, beyond initial containment.

4

Extended detection coverage for persistence

Prioritize solutions that address service-based mechanisms and stealthy system modifications.

Trend 5: Rapid Malware Rotation is Weakening Detection

The malware landscape is becoming more dynamic and less predictable, with **activity spreading across multiple families** rather than concentrating around a few dominant ones. This shift increases the likelihood that threats bypass detections.

No Dominant Malware Family Is Increasing Exposure

Attackers are no longer dependent on specific malware families to reach their objectives. The same outcomes, such as credential theft, access, or persistence, can be achieved using different tools with minimal changes in execution.

When one family becomes less effective or more detectable, it is quickly replaced.

Growing Families

Family	Change
AgentTesla	+87.9%
Vidar	+66.1%
LokiBot	+75.5%
Stealc	+21.5%
DCRAT	+19.3%

Declining Families

Family	Change
Lumma	-45.9%
HijackLoader	-39.9%
XWorm	-26.3%

Risk Implications

Unstable Detection Coverage

Rapid rotation of malware families reduces effectiveness of signature-based detection, increasing likelihood of missed threats.

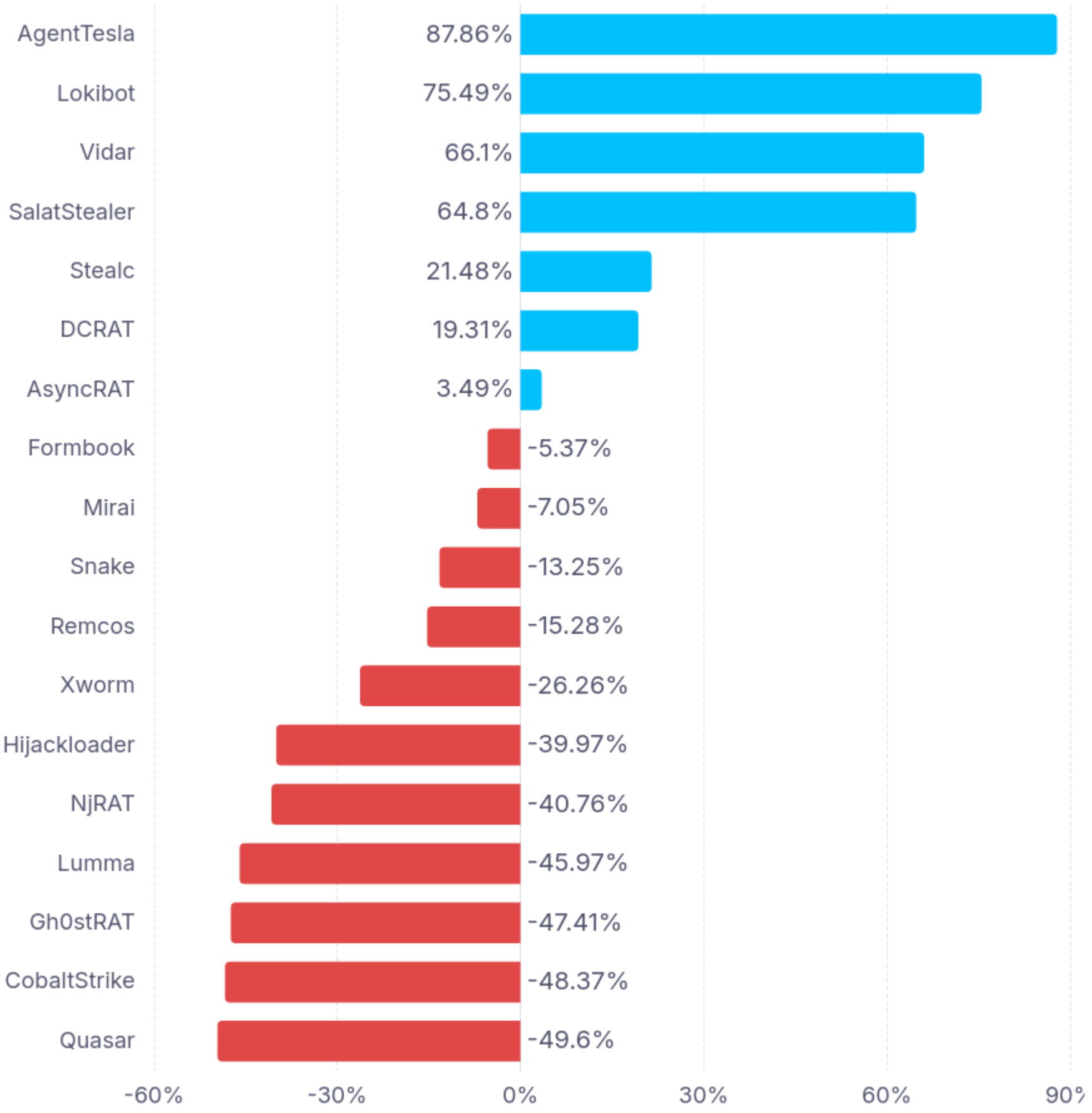
Tool-Agnostic Attacks Rising

Attackers achieve consistent objectives using different tools, making detection based on tooling increasingly unreliable and incomplete.

Credential Exposure as Primary Risk

High growth in families designed for harvesting access means credential exposure must be treated as an immediate incident-level event.

Malware Family Detections: Q4 2025 vs. Q1 2026



Strategic Shift: What Needs to Change for Malware Detection

Detection can no longer depend on malware family tracking, as attackers continuously rotate tools to achieve the same outcomes. What remains consistent is behavior, such as credential access, execution, persistence, which must become the core detection layer.

Where to Focus Effort

1

Prioritize behavior over family attribution

Focus on what the malware does, such as credential access, data collection, or persistence, rather than what it is called.

2

Detect common outcomes across different tools

Identify patterns like credential harvesting, command execution, and data exfiltration that remain consistent despite tooling changes.

3

Continuously validate detection coverage

Regularly assess whether new and emerging families are being detected, not just known ones.

4

Correlate activity across signals

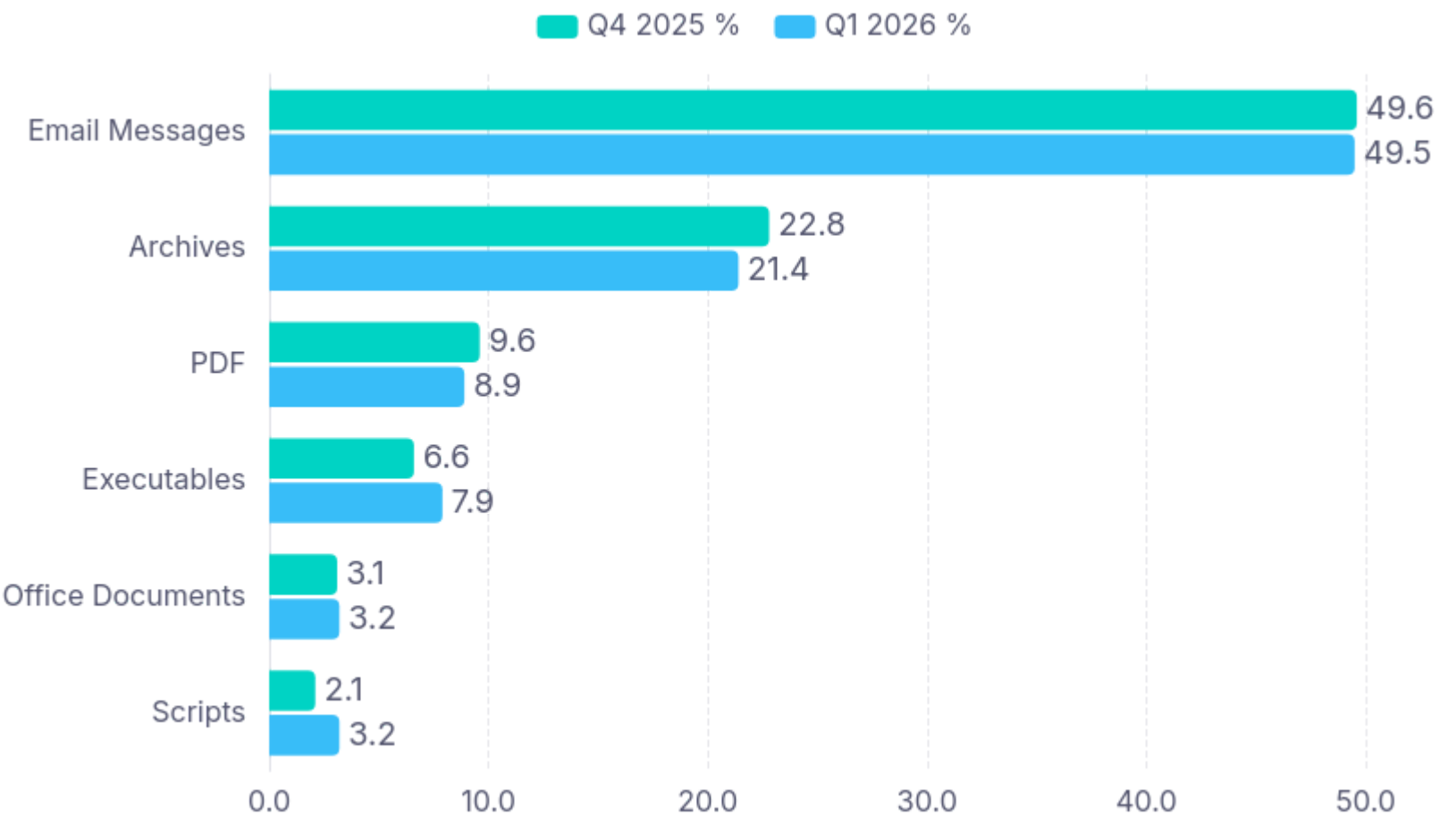
Link endpoint behavior, identity activity, and network traffic to reduce dependence on single indicators.

Trend 6: Delivery Formats Are Consolidating Around Email and Direct Execution

Delivery methods are becoming less diverse and increasingly standardized around what works at scale. As a result, a **small number of vectors now drive a majority of risk**, amplifying the consequences of any weakness in these channels.

Risk Is Concentrating in a Small Number of Vectors

The way malicious content is delivered is becoming **more concentrated, not more diverse**. Attackers are standardizing on formats that maximize reach, compatibility, and execution success. The entry point is predictable, but harder to control due to scale.



Key Trends

Email-based delivery is becoming more dominant and refined, now accounting for **over 49%** of all observed cases. This turns email into a structural dependency, where control gaps have a disproportionately high impact on overall security.
Archive-based attacks follow a similar pattern. Despite a slight decline from **22.8% to 21.4%,** they remain a core delivery mechanism, which indicates sustained effectiveness rather than reduced relevance.

Direct compromise through executable files is increasing. The rise to 7**.9%** suggests continued reliance on compiled payloads, likely supported by improved obfuscation and delivery techniques.

Strategic Shift: What Needs to Change for Delivery

As attack delivery concentrates around a small number of vectors, control must shift from broad coverage to depth of inspection and response at these critical entry points. The priority is to reduce risk where it is most likely to originate.

Investment Priorities

Advanced Email Security

Capabilities that scan message context, attachments, and embedded content.

Interactive Sandboxing

Immediate inspection of files and links to understand execution behavior.

Integrated Detection Pipelines

Connecting email, endpoint, and network signals for faster investigation.

User Interaction Visibility

Monitoring how users engage with content to identify high-risk actions early.

Strategic Direction

Risk is no longer evenly distributed across entry points. Organizations that invest in deeper visibility and faster response at the most common vectors will significantly reduce overall exposure. Those that spread controls evenly will leave critical entry paths underprotected.

Trend 7: Execution is Shifting Toward Native System Tools

Attackers are increasingly **using tools that already exist inside victims' environments**. Activity that would previously stand out as foreign now appears as part of normal system or administrative behavior.

Living Off the Land: Execution Trends and Consequences

Execution is becoming harder to distinguish from legitimate activity. The same tools used for administration, automation, and system management are now used to execute attacks. This reduces the effectiveness of controls that identify malicious indicators.

What Changed in Q1

Technique	Change
T1059.001 (PowerShell)	**+17.4%**
T1059.007 (JavaScript)	**+58.4%**

Operational Consequences

Higher Alert Ambiguity

Common tools generate high volumes of activity, making it difficult to isolate malicious use from legitimate administration.

Increased Analyst Workload

More effort is required to determine intent behind each execution event, slowing down triage and response.

Delayed Decisions

Uncertainty slows down escalation and response, directly impacting the ability to act in early attack stages.

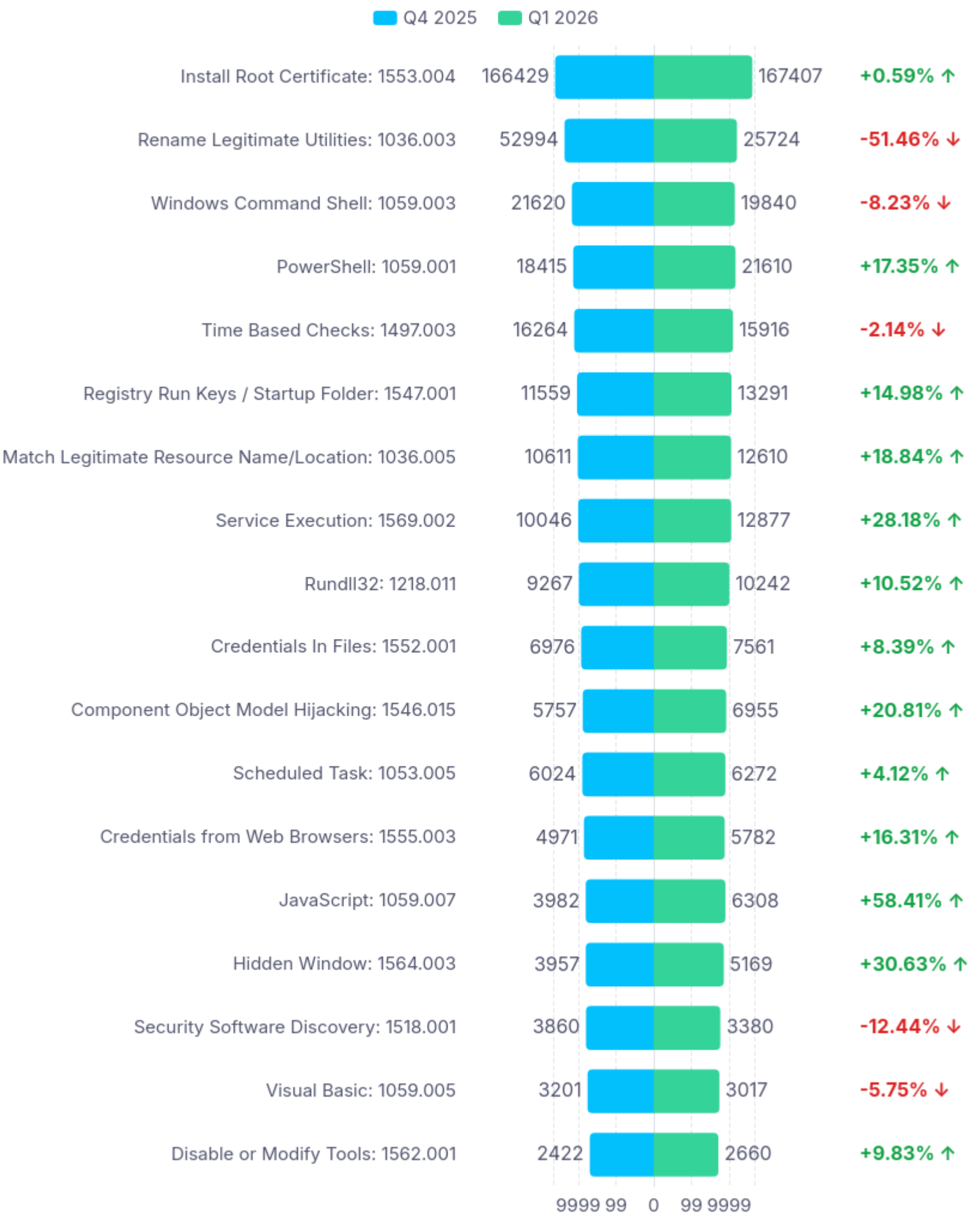
Business Impact

The shift to native execution changes how risk develops:

- **Higher likelihood of undetected execution**
  Malicious actions blend into normal system activity
- **Delayed response to active attacks**
  Execution is not recognized as malicious at the moment it occurs
- **Increased operational load on SOC teams**
  More time is required to interpret activity

In practice, organizations are observing execution activity but lack the clarity to act on it immediately.

MITRE ATT&CK TTP Detections: Q4 2025 vs. Q1 2026



Strategic Shift: What Needs to Change for Execution

Execution analysis can no longer rely on tool identification. The priority shifts to how native tools are used and whether that behavior aligns with expected activity.

Where to Focus Effort

1

Deep process visibility

Capture full execution chains and command details across endpoints.

2

Behavioral analytics

Detect deviations from established baselines of native tool usage.

3

Execution chain reconstruction

Tools to quickly understand what a script or command actually does.

4

Integrated telemetry

Combine execution data with user and session context for faster decisions.

Strategic Direction

Control over execution depends on distinguishing intent within legitimate tools. Organizations that can interpret how native tools are used will identify malicious activity earlier and reduce exposure.

Cyber Risk Is Becoming Continuous, Less Visible, and More Expensive

The key trend in Q1 2026 is how **risk behaves in organizations,** moving from isolated incidents to continuous exposure.

Six Dimensions of Continuous Risk

1

The Cost of Being "Late" Is Increasing

Early-stage activity no longer provides clear signals. Entry points look legitimate, execution blends into normal operations, and alerts lack context. Decisions are delayed, attackers move forward without resistance, and incident scope grows, which is consistent with an 84% initial compromise increase.

2

Trust Is Being Exploited as an Attack Vector

Attackers operate through authenticated sessions, valid credentials, and normal user behavior. Credential theft (+14.7%), surveillance (+34.4%), and session-based phishing (Sneaky2FA +76.8%) show access is easier to obtain and harder to tell from legitimate activity.

3

The Window to Prevent Impact Is Shrinking

Attackers reduce time between entry and meaningful impact. Access is established earlier, execution is immediate, and response is slowed by uncertainty. This mismatch means incidents are contained later and recovery becomes more complex.

4

Compromise Is Harder to Fully Remove

Service mechanisms abuse (+89.3%) and rise in persistence attempts via Registry Run Keys (+15%) indicate attackers anchor access deeper. This leads to incomplete remediation, repeated access without new intrusion, and extended incident lifecycles.

5

Recovery Is No Longer Guaranteed

Attackers increasingly target the ability to recover, not just the systems themselves. Longer downtime, disrupted recovery processes, and higher restoration costs result. Even when backups exist, they may not be immediately usable or accessible.

6

The Threat Landscape Is Less Predictable

New phishing kits appear and scale within a single quarter. Malware families rise and fall quickly. Actor activity shifts unpredictably and attackers keep changing tools. This reduces the value of historical threat prioritization and static detection.

Strategic Priorities for Q2 2026

Security effectiveness is increasingly determined by how well organizations adapt to changes in attacker behavior. These priorities highlight the critical areas where focus and investment will have the greatest impact on reducing risk.

1. Reduce the Business Value of Initial Access

Ensure that early-stage footholds cannot be converted into meaningful access, lateral movement, or monetizable assets across the environment. Achieving this requires strict execution controls, limited outbound communication, and isolation of user environments.

2. Establish Identity as a Continuous Control Layer

Shift from point-in-time authentication to continuous validation of user and session behavior across systems, applications, and access contexts. Effective control depends on correlating identity signals with endpoint and session activity to detect misuse within legitimate access.

3. Concentrate Security Investment on Primary Attack Vectors

Reallocate resources toward dominant entry points such as email and user-driven execution, where risk is most concentrated and consistently exploited. Greater depth of inspection is needed, including interactive sandbox analysis of files and links.

4. Align Detection with Attacker Objectives, Not Tooling

Prioritize visibility into access, persistence, and data movement rather than reliance on identifying specific malware families or known indicators. A shift toward behavioral detection and integration of threat intelligence enables tracking of attacker activity across changing tools.

5. Optimize Security Operations for Decision Speed

Reduce time from signal to action by integrating context across systems and enabling faster, more confident response to early-stage activity. Success depends on unified visibility, automated enrichment, and the ability to quickly reconstruct execution chains and intent.

Bottom Line: Understanding Early Is the New Security Imperative

> The Q1 2026 landscape shows a clear transition: **Cyber risk is becoming continuous, less visible, and more expensive** to control. The critical capability is no longer just seeing threats, but understanding them early enough to act before they turn into business impact.

Organizations That Will Succeed

- **Validate early-stage activity quickly**, before uncertainty becomes compromise
- **Reduce uncertainty in investigations** through behavioral analysis and threat intel
- **Act before escalation**, contain attacks before they expand
- **Continuously evaluate identity** throughout the session, not just at login
- **Treat persistence as a core part of the attack** lifecycle, not a secondary concern

Organizations That Will Struggle

- **Detect incidents late**, after access is already established and expanded
- **Absorb higher costs from wider incident scope** and longer dwell times
- **Operate with reduced confidence** in their ability to contain threats
- **Rely on historical threat models** that cannot track the pace of change
- **Face incomplete remediation** and repeat compromise from embedded persistence

Security effectiveness in Q2 2026 is determined by how quickly an organization can understand what is happening and act before the attacker establishes control. Speed of understanding is the new competitive advantage.

Power Your Business Security with ANY.RUN

ANY.RUN’s solutions are used by more than **15,000 businesses** across multiple industries, such as finance, manufacturing, healthcare, and technology, including **74 of Fortune 100 companies**.

Interactive Sandbox helps **SOC & MSSP teams** identify malware & phishing targeting Windows, Linux, macOS, and Android systems. It provides capabilities for fast, hands-on investigations for **streamlined triage and informed response**.

ANY.RUN's Threat Intelligence delivers **rich, real-time info on active cyber attacks**, to expand threat coverage, accelerate alert validation, and power proactive defense.

Integrate ANY.RUN to stay ahead of threats →