EXTRAHOP®

The Global Threat Landscape:

A Guide to Today's Most Active Threat Actors

Table of Contents

Key Findings

THREAT ACTORS DETECTED IN ORGANIZATIONAL NETWORKS (PAST 12 MONTHS)

RansomHub	**26.82%**
LockBit	**26.54%**
DarkSide	**25.71%**
APT41/Wicked Panda/Double Dragon/Brass Typhoon	**24.04%**
Black Basta	**23.43%**

Additional threat actors detected

Midnight Blizzard/Apt29/Nobelium/Cozy Bear	23.32%	Akira	19.60%
Scattered Spider	21.99%	REvil	18.05%
Volt Typhoon	21.65%	Apt31/Zirconium	17.21%
Lazarus Group	21.54%	Cl0p	14.83%
Salt Typhoon	20.27%	FIN7	13.83%

ATTACK SURFACES WITH THE HIGHEST PERCEIVED RISK

Public cloud	53.80%
Third-party services	43.70%
Generative AI applications	41.87%

MOST COMMON INITIAL ATTACK VECTORS

33.65%
Phishing/social engineering

19.43%
Software vulnerabilities

13%
of organizations only discover threat actors at the encryption phase

The Industrialization of Threat Groups

Modern cyber warfare has moved far beyond the image of the isolated hacker. Today's threat landscape is dominated by prolific threat actors who operate with the discipline and sophistication of Fortune 500 companies.

These groups are no longer just opportunistic; they are highly collaborative, organized, and strategic, often maintaining dedicated research and development (R&D) departments and tracking success through rigorous key performance indicators (KPIs). By leveraging dedicated infrastructure and tested playbooks, they have transformed cyberattacks into repeatable, industrialized workflows designed to maximize speed, scale, and persistence.

While data from the Global Threat Landscape Report confirms that a few actors are responsible for a disproportionate share of global activity, their reliance on standardized processes creates a significant tactical vulnerability. Their operations are not as well concealed as they believe; even as malware and specific tools evolve, the underlying workflows leave consistent evidence. Understanding these operational fingerprints helps track and disrupt even the most sophisticated adversaries.

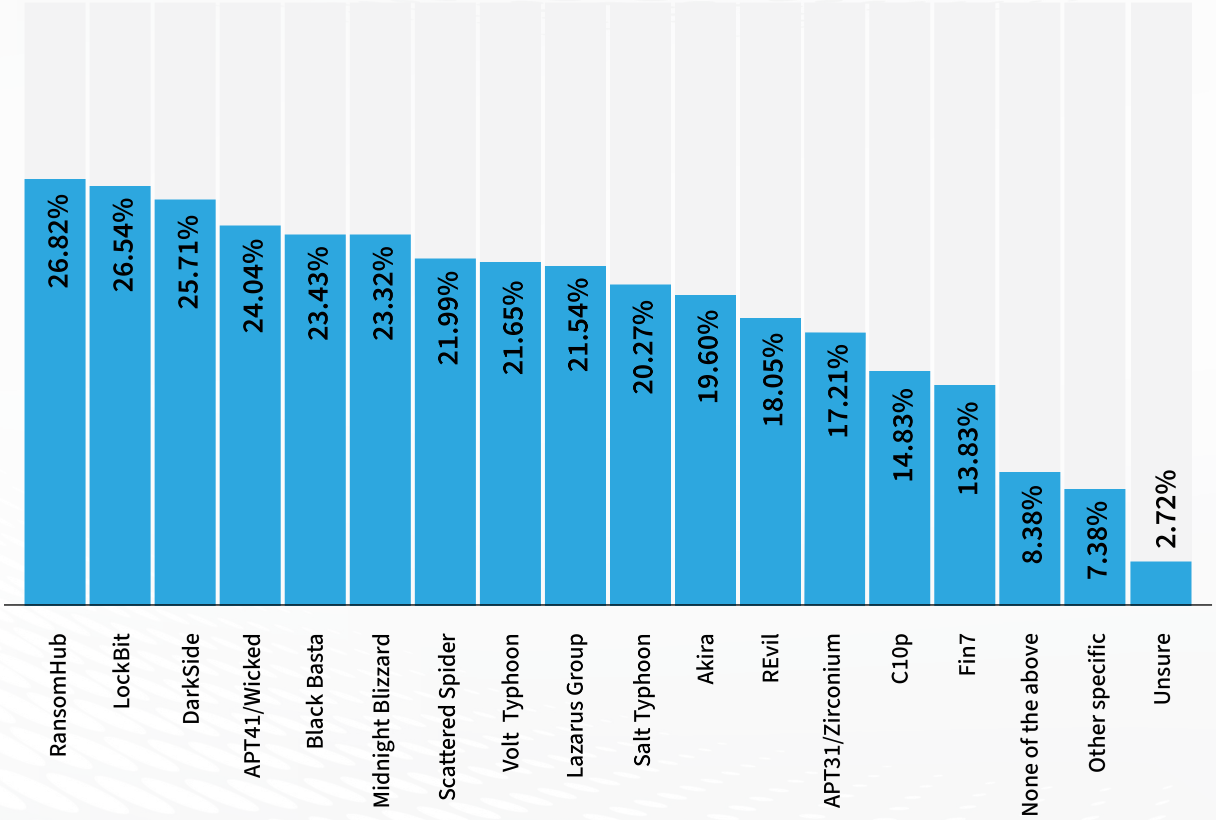
Top Threat Actors in 2025

A closer look at these actors reveals patterns in tactics, prevalence, and impact. Certain actors are consistently visible across networks. For instance, ransomware operators and state-linked actors dominate activity, as demonstrated by the data.

This dominance is marked by a clear evolution in threat actor maturity. In 2025, the ransomware sector pivoted from high-frequency campaigns to campaigns designed for high-yield outcomes; though total incidents slowed, the financial severity of each breach spiked. This shift signals a move toward "surgical" extortion, where attackers invest heavily in credential harvesting and lateral movement to ensure maximum operational paralysis.

U.S. government and independent cybersecurity analyses confirm that RansomHub moves laterally through unpatched internet-facing applications, ensuring their activity blends in with legitimate network traffic.

Most Detected Threat Actors



A Deeper Dive into the Top Reported Threat Actors

RANSOMHUB

RansomHub operates via Ransomware-as-a-Service with a focus on rapid execution. The group commonly exploits public-facing vulnerabilities and third-party access for initial entry.

Once inside, affiliates move quickly, deploying ransomware within three days. Their operations prioritize high-value targets such as backup systems, compressing the attack window and increasing their leverage.

LOCKBIT

LockBit gains initial access primarily through phishing and credential theft, bypassing perimeter defenses. It also exploits unpatched servers, applications, and third-party systems.

After establishing access, the group automates lateral movement to propagate ransomware, achieving rapid domain-wide spread that can outpace manual containment efforts.

DARKSIDE

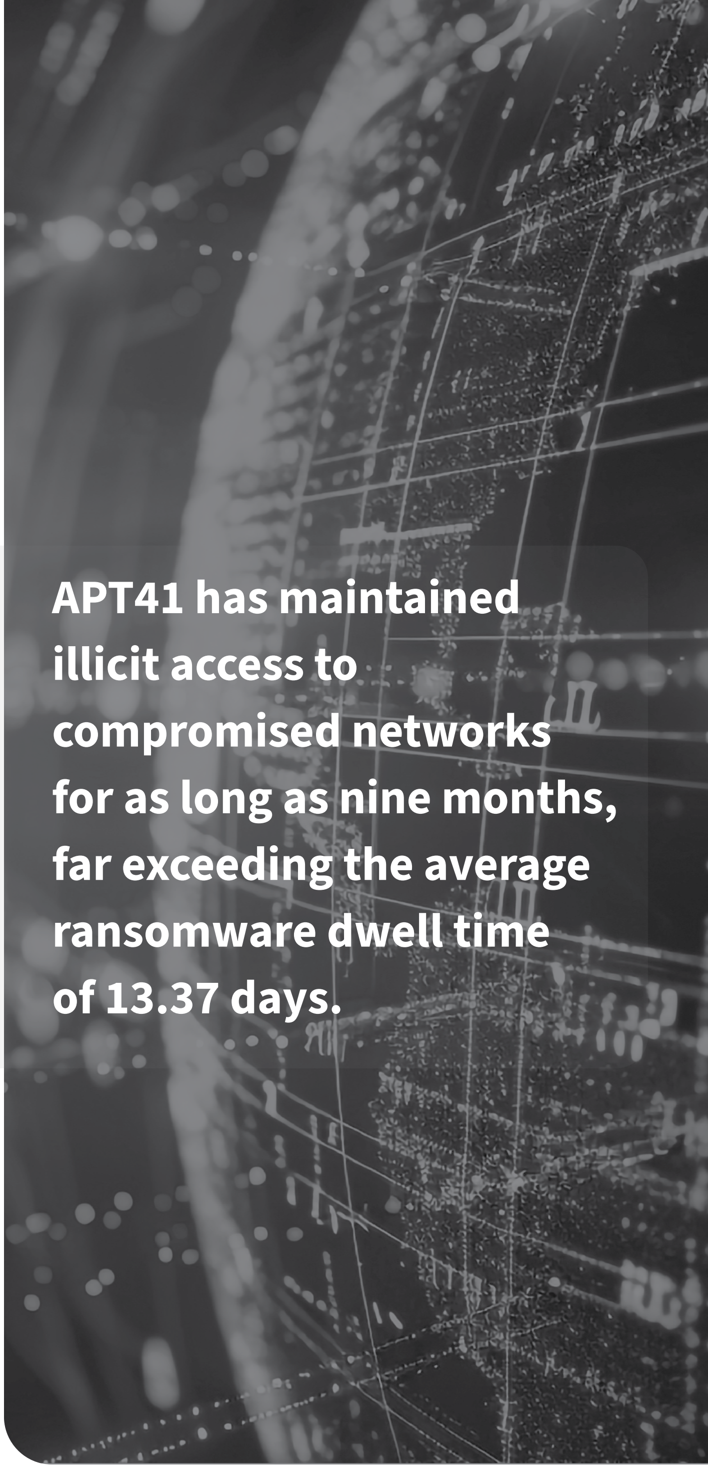
DarkSide employs a "big game hunting" approach, selecting high-value targets where a breach can create significant disruption and strategic advantage.

DarkSide frequently gains access via purchased credentials or by exploiting VPN and RDP vulnerabilities, granting legitimate-looking access that bypasses perimeter defenses. After infiltration, the group moves laterally to identify critical business systems — including data repositories and backup infrastructure — before deploying ransomware.

APT41

APT41 blends nation-state espionage with financially motivated attacks. The dual focus encourages prolonged presence; these attackers maintain access for months, far exceeding typical ransomware dwell times.

Persistence allows APT41 to adapt tactics, probe defenses, and exploit emerging opportunities within compromised networks, extending the reach and severity of each intrusion, making detection and remediation more complex.



APT41 has maintained illicit access to compromised networks for as long as nine months, far exceeding the average ransomware dwell time of 13.37 days.

BLACK BASTA

Black Basta prioritizes speed and disruption over long-term persistence. The group disables endpoint defenses using custom "EDR-Killers," blinding security teams early in the attack chain.

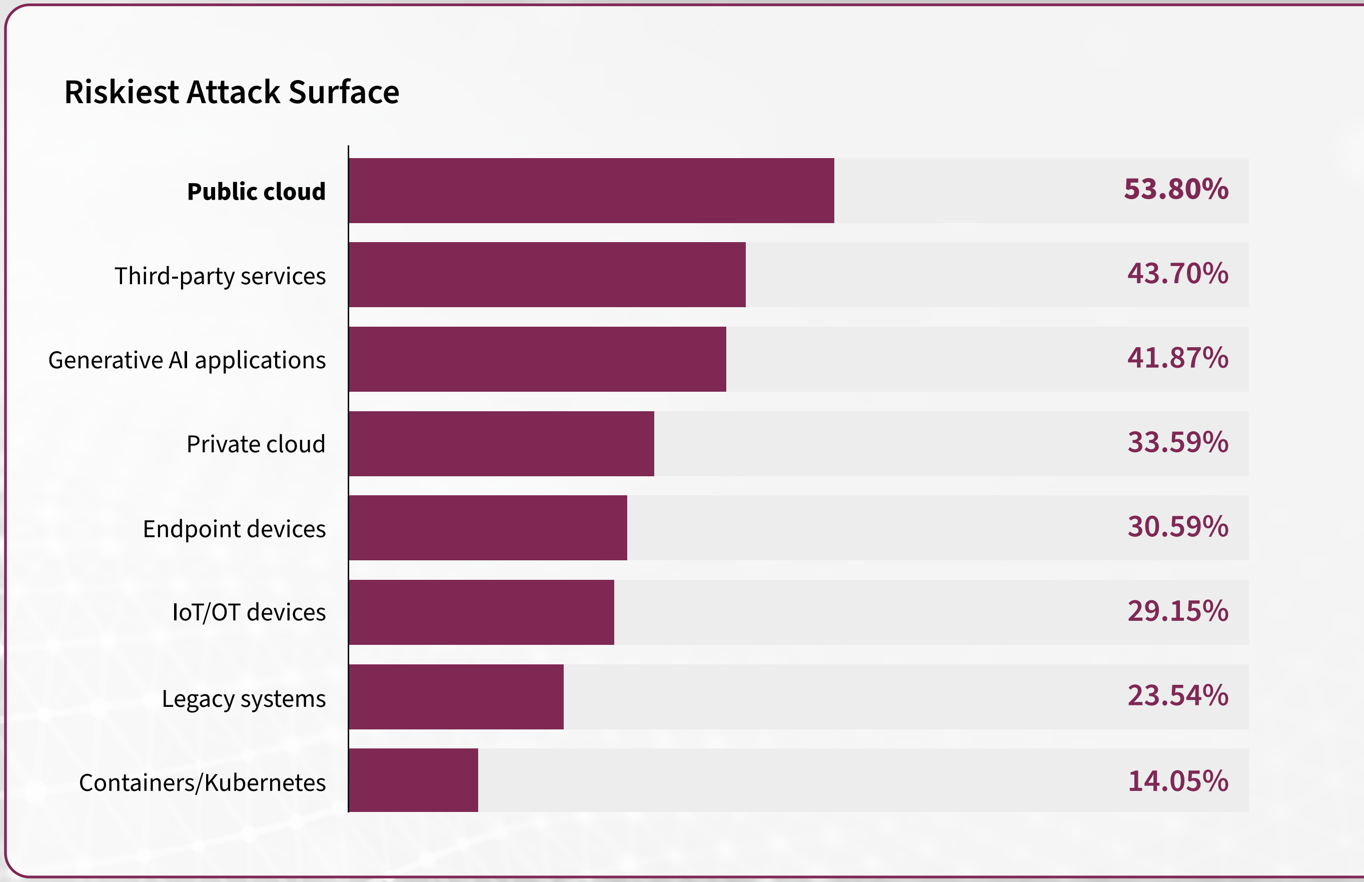
Domain-wide encryption can occur within hours of initial access, leaving organizations with minimal time to respond before attackers achieve their objectives.

Commonly Exploited Attack Surfaces

Knowing which attack surfaces threat actors target most helps guide attribution-driven response.

Public cloud (53.8%), third-party services (43.7%), and generative AI applications (41.9%) are consistently cited as the highest risk.

The complexity and fragmented ownership of these environments create visibility gaps that attackers readily exploit to gain access and move laterally.



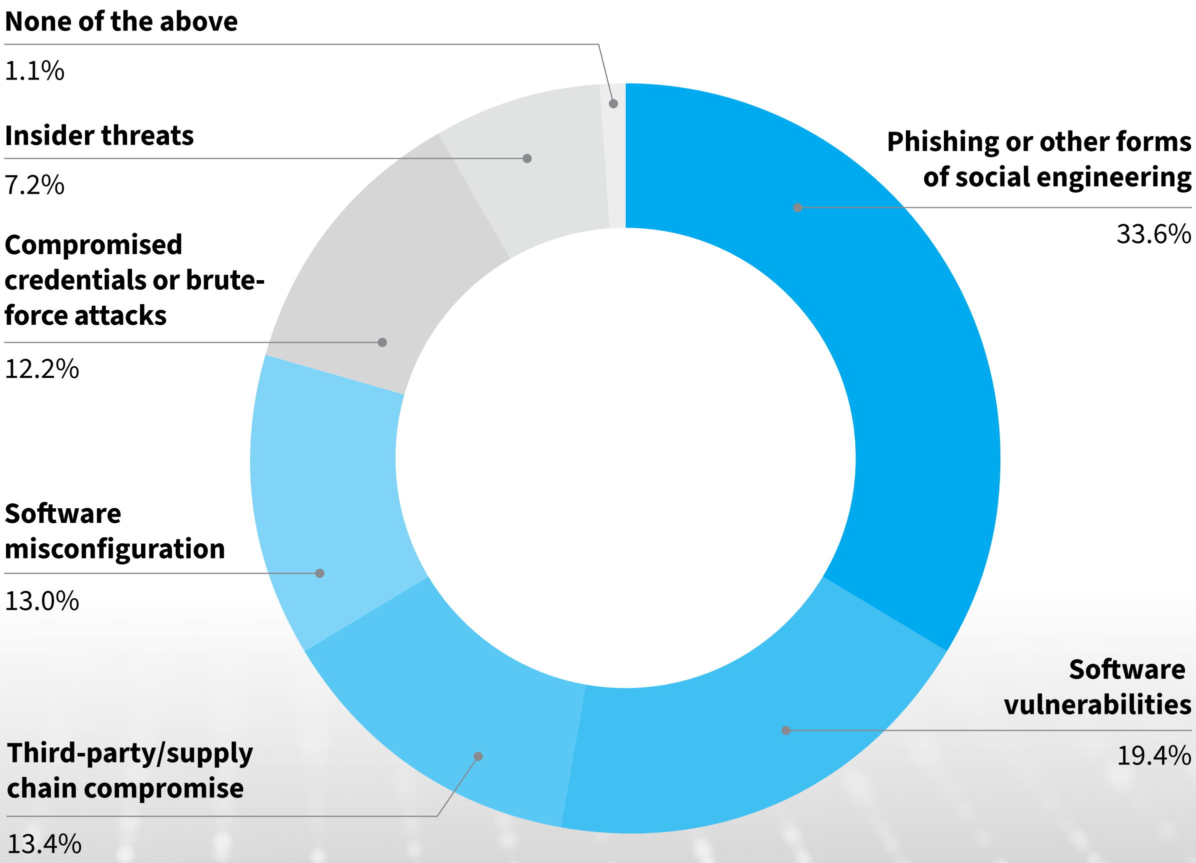
Initial Access Through Proven Methods

Threat actors continue to favor proven initial access techniques over novel exploits.

- **Phishing and social engineering** remain the most common entry points, exploiting human trust to bypass perimeter defenses.
- **Software vulnerabilities** represent the second most common access vector. Unpatched systems provide direct access, without requiring authentication or social engineering.
- **Compromised credentials** are also increasingly becoming a primary entry point for threat actors.

Midnight Blizzard's breach of Microsoft's email system led to exfiltration of correspondence between U.S. Federal Civilian Executive Branch (FCEB) agencies, demonstrating how compromised credentials provide persistent access to sensitive government information.

Most Common Initial Points of Entry for Attackers



The Detection Gap

Most organizations detect attackers too late. Nearly a third (30.6%) only recognize ransomware attacks during or after data exfiltration begins.

Delayed detection increases the amount of time attackers have to map environments, escalate privileges, and position themselves for maximum impact.

Aligning Defense Strategies with Real-World Threats

Different threat actors pursue different objectives — some favor speed and disruption, while others focus on stealth and persistence. For instance, RansomHub and DarkSide compress attack timelines to maximize immediate impact, while APT41 and Midnight Blizzard maintain prolonged access, gathering intelligence and adapting to defensive responses.

Attributing the threat actor clarifies their “endgame.” By understanding the adversary’s unique playbook, defenders can anticipate operational moves and deploy more effective, context-aware countermeasures.

Black Basta disables endpoint defenses and completes domain-wide encryption within hours, highlighting how delayed detection leaves minimal time to intervene.

Stop Attacks by Detecting Threat Actors Early

Once attackers gain access to the network, most traditional tools are blind to their activities. Yet, lateral movement, reconnaissance, and privilege escalation generate network signals that defenders can act on.

By analyzing east-west traffic, defenders can reveal who the threat actors are and how they operate. Detecting them early prevents data exfiltration and encryption, stopping even the most prolific and advanced attackers — before damage occurs.

For a deeper analysis of today's most impactful threat actors and the behaviors that expose them, explore the ExtraHop Global Threat Landscape Report.

About ExtraHop

ExtraHop turns the network — the enterprise's ultimate source of truth — into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that "thinks," analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.