EXTRAHOP

ExtraHop Global Threat Landscape Report

Financial Services Edition

Table of Contents

Key Findings

AVERAGE NUMBER OF RANSOMWARE INCIDENTS IN THE LAST 12 MONTHS:

5-6

MOST DETECTED THREAT ACTOR IN FINANCIAL SERVICES:

RansomHub

THE COST OF COMPROMISE:

$3.8M
average ransomware payment

36 hours
average downtime per incident

THE WINDOW OF OPPORTUNITY:

~12 days
attacker dwell time before ransomware deployment

17 days
average time to respond and contain incidents from initial detection

The Shift Redefining Cybersecurity in Financial Services

A growing number of companies in the financial sector are confronting a troubling reality: Attacks are becoming increasingly sophisticated, persistent, and coordinated, often leading to severe setbacks when it comes to ROI and growth.

According to The ExtraHop 2025 Global Threat Landscape Report, financial services organizations experienced an average of 5-6 ransomware incidents in the last year. With these attacks came increasing ransomware payments, which surged to an average of $3.8 million, up a million dollars from the previous year.

These organizations also found themselves experiencing an average of 36 hours of downtime per cyber incident, disrupting operations and preventing customers from accessing services.

With these cascading costs often came customer churn, reputational damage, and increased insurance premiums that eroded margins and stalled strategic initiatives.

The reality is that threat actors are relentless and resourceful. Financial breaches are no longer a matter of *if* but *when* — and the magnitude of their impact depends on how quickly security teams can detect and contain them.

A 2025 cyberattack on TransUnion exposed the personal details of approximately 4.4 million U.S. consumers, including names, birthdates, social security numbers, and contact information, leading to millions in losses (e.g., settlements, fines, customer churn).

2025
$3.8M
THE AVERAGE
ransom

2024
$2.8M
THE AVERAGE
ransom

The Cybersecurity Landscape

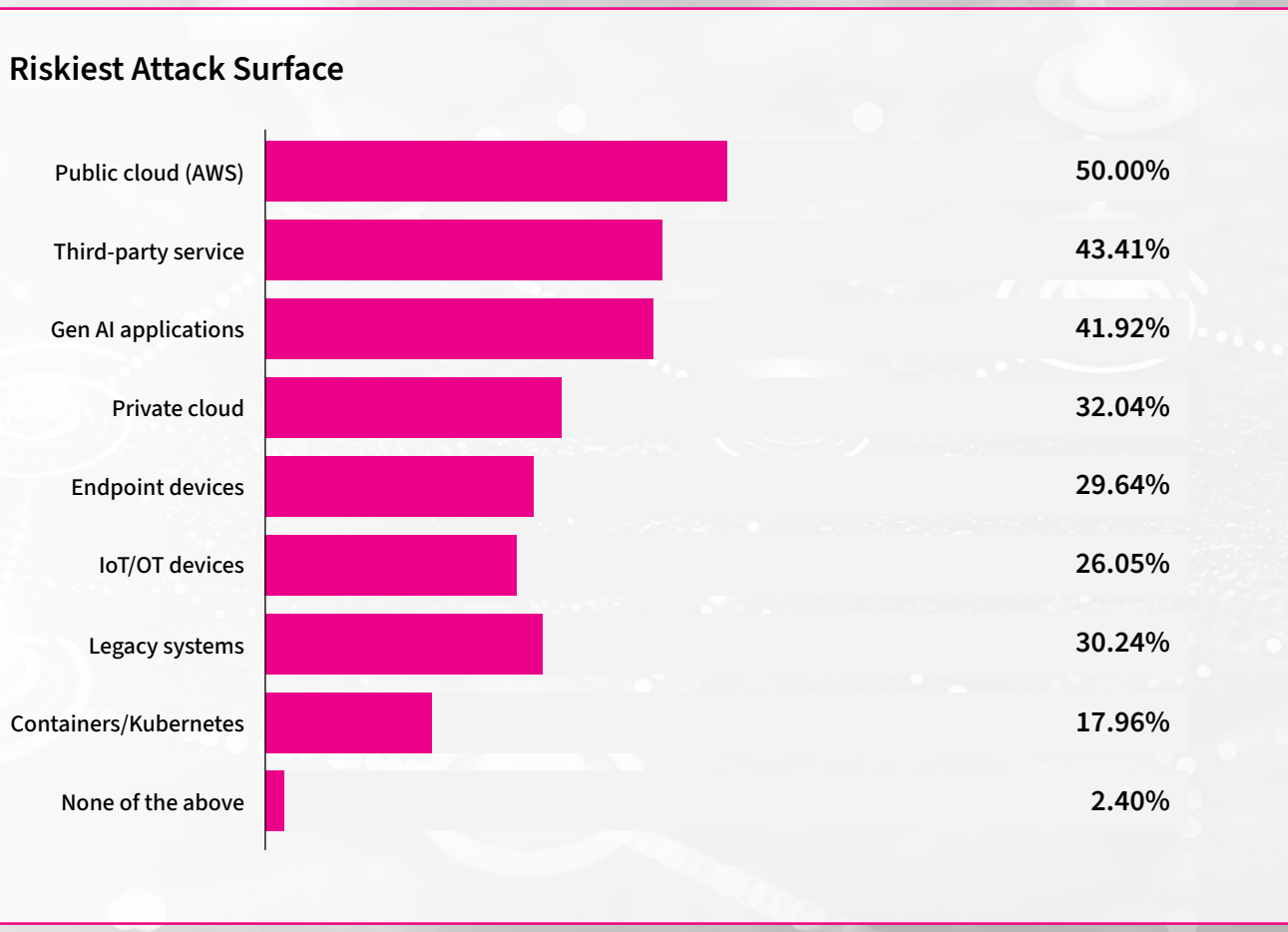
AN EXPANDING ATTACK SURFACE

Financial institutions are confronting a rapidly expanding attack surface, making defense even more difficult. Every new cloud deployment, API, and endpoint creates additional risk and more entry points for threat actors.

Public cloud infrastructure presents the highest perceived risk (50.00%), according to the data. Most financial institutions now run in multi-cloud or hybrid environments, amplifying oversight gaps and complicating security enforcement.

Third-party and supply chain integrations are the second-highest risk (43%), which comes as no surprise for an industry so reliant on external vendors.

In 2023, threat actors **exploited the MOVEit file transfer application** to compromise numerous financial institutions, including wealth management groups and pension fund entities, resulting in multi-million dollar losses, mass customer data compromise, regulatory scrutiny, and protracted litigation.



PROLIFERATING THREATS

Threat actors target financial services for their high-value data, infrastructure that underpins global commerce, and the potential for lucrative disruption. Understanding who these threat actors are, how they operate, and what they prioritize is essential to staying ahead.

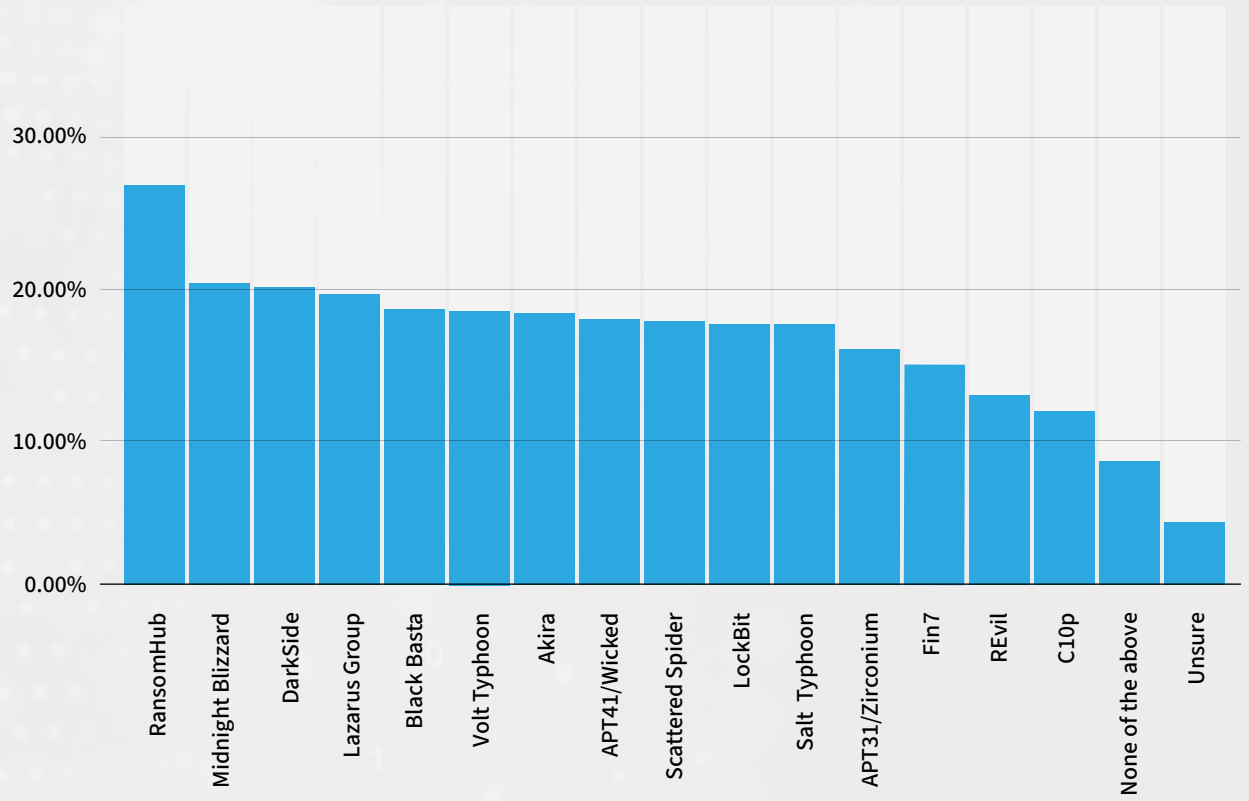
According to the findings, threat actors, including RansomHub, Midnight Blizzard (a.k.a Apt29/ Nobellium/Cozy Bear), Darkside, Black Basta, and Volt Typhoon have relentlessly pursued financial institutions over the past 12 months.

RANSOMHUB

In that time, more than a quarter of financial institutions detected RansomHub in their environments.

RansomHub targets *high-value* financial institutions, including investment firms, credit unions, and wealth management firms, by exploiting public-facing services or using sophisticated spearphishing to harvest authorized credentials.

Most Detected Threat Actors Groups in Financial Services



Once inside, RansomHub deploys custom tools and Living-off-the-Land (LotL) techniques to escalate privileges and harvest additional credentials. From there, RansomHub moves laterally via standard protocols, like Remote Desktop Protocol (RDP) and PowerShell, blending in with legitimate network traffic to remain undetected.

Despite the dismantling of RansomHub's infrastructure in early 2025, the underlying threat remains. Former affiliates have re-branded under new RaaS umbrellas, leveraging their established playbooks for initial access and internal network traversal to target the banking sector.

MIDNIGHT BLIZZARD

20.06% of financial services organizations detected the nation-state group Midnight Blizzard, which targets major financial services conglomerates and wealth management firms.

Midnight Blizzard often gains initial access through password spraying attacks, dormant accounts lacking multi-factor authentication, or spearphishing lures. The group then uses a sophisticated lateral movement strategy that abuses valid accounts to hijack or register malicious applications, enabling long-term persistence while bypassing traditional security controls.

Midnight Blizzard specializes in intelligence collection, focusing on access to executive communications, identity systems, and data — information that can influence markets, policy, and geopolitical outcomes.

Midnight Blizzard remains active against financial services organizations, prioritizing access to executive communications and identity systems. The group frequently abuses dormant accounts and weak authentication controls to evade detection, increasing the likelihood of regulatory notifications, compliance exposure, and costly remediation efforts.

Threat Actors' Tactics

GAINING INITIAL ACCESS

Gaining entry is rarely the hurdle for threat actors. They typically breach financial institutions via well-known vectors: phishing, unpatched software, stolen credentials, third-party vulnerabilities, misconfigurations, and insider threats.

More than a quarter of financial sector decision-makers cite phishing and social engineering as the most common initial access methods, allowing attackers to, at minimum, access sensitive accounts ahead of detection.

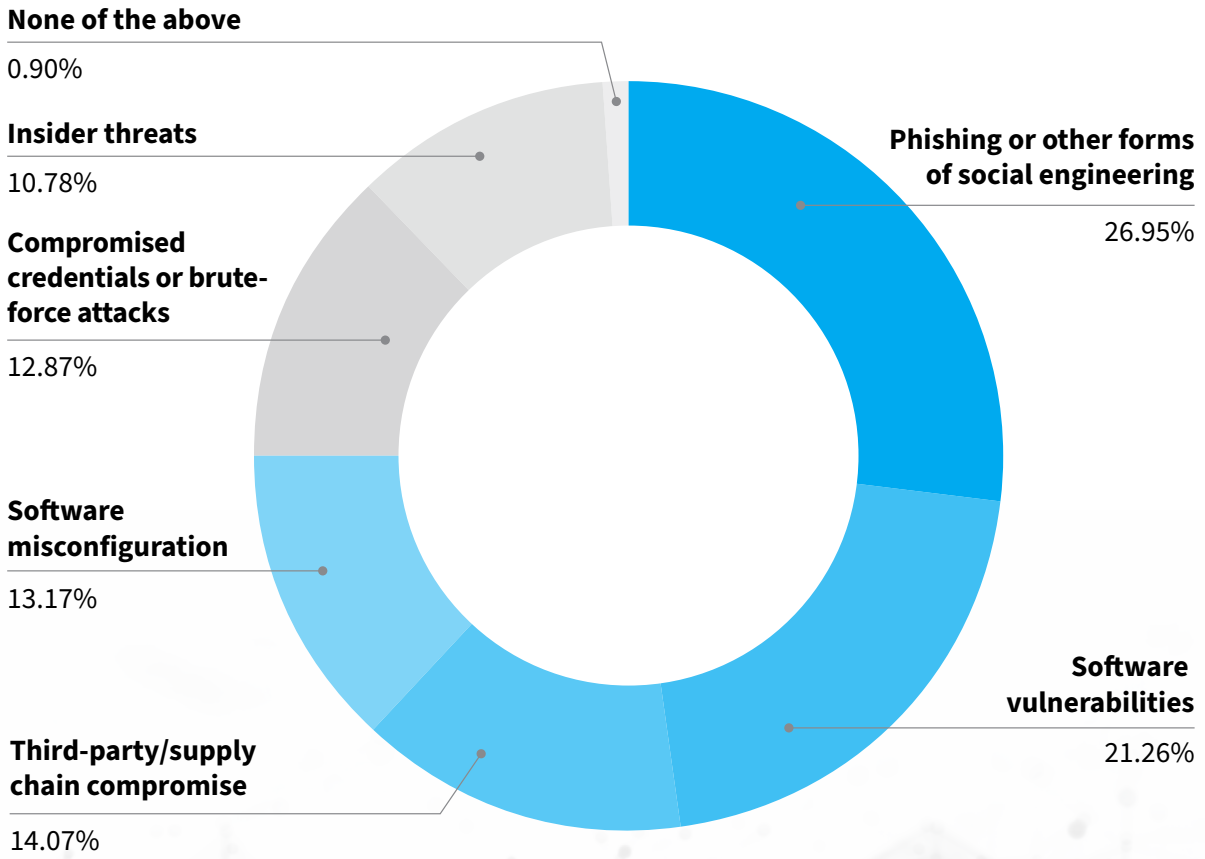
The second-most common entry point (21.26%), software vulnerabilities often provide the unpatched gaps attackers need to establish a foothold and maintain persistence.

Threat actors are also increasingly using compromised credentials and brute-force attacks (13%) to mimic authorized users and gain access. Once inside, those compromised credentials make it easier for them to continue carrying out their attacks undetected, as they blend in with normal activity.

Critically, credentials unlock deeper pathways into the infrastructure. In cloud environments, a single login can authenticate across multiple platforms and services, expanding what attackers can reach in a given environment.

All of these methods permit discreet entry, setting the stage for lateral movement.

Most Common Initial Points of Entry for Attackers Targeting Financial Services



MOVING LATERALLY

After entry, attackers may begin lateral movement, the process of navigating internal systems to escalate privileges, map assets, and expand access while remaining undetected. This stage is often the most impactful, occurring during dwell time — the period between initial compromise and detection — when attackers have the freedom to explore and position themselves for maximum effect.

Prior to a ransomware incident, financial services organizations believe that threat actors have access to their systems for about 12 days, on average.

To stay under the radar while moving laterally, LockBit leverages tools like PsExec, Cobalt Strike, and Group Policy Objects (GPOs) to deploy ransomware at scale. Similarly, the Akira group blends lateral movement with routine administrative workflows using legitimate remote access tools.

LEVERAGING ORGANIZATIONAL WEAKNESSES

Detection often comes too late.

On average, financial services organizations require seventeen days to respond to and contain security alerts. This gives threat actors time to escalate their activity.

Consider the impact delayed detection could have in the event of a ransomware attack: According to the data, nearly a quarter of ransomware attacks are detected only during or after data exfiltration has begun. By this point, the incident has transitioned from a containment challenge to a massive liability.

Once data exfiltration begins, a bank is no longer just tracking down a threat; it is facing mandatory disclosure requirements, potential regulatory fines, and the permanent loss of client trust as sensitive intellectual property or personal data enters the hands of criminals.

How Financial Services Organizations Can Fight Back

Disrupting the attack chain early is key to shrinking the time that attackers have to move laterally, escalate privileges, and exploit assets.

Essential to this effort is comprehensive network visibility, enabling organizations to detect threats quickly, halt unauthorized activity, and protect core systems and data.

Limited visibility is the top challenge (42.22%) hindering financial services' timely response to threats.

DETECT THREATS FASTER

Traditional security often fails because it focuses almost exclusively on the "front door," only monitoring the north-south traffic entering and exiting the network. Cyberattackers capitalize on this by seeking out internal "blind spots" within the east-west corridor, where traffic flows between servers and applications.

Once a perimeter is breached, the network's interior often becomes a dark zone where attackers can move undetected, masquerading as legitimate internal communications to navigate from an initial foothold toward high-value assets.

Effective detection, therefore, requires more than just guarding the gate; it demands an intimate understanding of attacker behavior and the specific tactics needed to disrupt their progression.

COMPROMISING HIDDEN OR UNMANAGED DEVICES

Threat actors exploit hidden or unmanaged devices to bypass controls and escalate privileges.

Shadow IT, Bring Your Own Device (BYOD), and IoT sensors often exist beyond the borders of traditional inventories, creating opportunities for exploitation. To secure the network, security teams need to maintain real-time inventory, preventing attackers from leveraging overlooked resources.

- ✓ Use passive monitoring of all network communications to build a real-time comprehensive asset inventory.
- ✓ Ensure the discovery process captures every connected device, including unmanaged, BYOD, and IoT assets, without requiring software installations.
- ✓ Classify every asset automatically based on its observed function and communication patterns within the network.
- ✓ Establish a behavioral "normal" for each classification to facilitate the identification of subtle deviations.
- ✓ Set triggers to alert security teams the moment a device joins the network or its behavior shifts from its assigned role.

BLENDING IN WITH LEGITIMATE ACTIVITY

Adversaries also maintain invisibility by integrating lateral movement with legitimate activity, making use of the following practices.

HIDING IN ENCRYPTED TRAFFIC

Attackers conceal lateral movement in encrypted traffic, exploiting the fact that most network traffic is encrypted and that traditional tools cannot inspect what's inside.

Both CISA and NIST have identified these encrypted gaps as major security vulnerabilities. To avoid remaining blind to the majority of internal communications, financial organizations need the capability to decrypt and analyze traffic.

STEALING CREDENTIALS AND TOOL ABUSE

Adversaries exploit stolen credentials and legitimate tools to make their actions appear normal. To unmask the adversary's efforts to blend into the environment, organizations need to be able to follow identities across the environment, seeing what they're doing.

Prioritizing high-value identities lets teams track compromised accounts, detect reconnaissance, map lateral movement, and contain incidents.

EXPLOITING SILOED TOOLS

By exploiting siloed tools and uncorrelated alerts, attackers move laterally and evade detection. To counter this, integrating network telemetry provides the contextualized data necessary to validate threats faster. When paired with native security platform integrations, teams can leverage EDR agents for automated detection and containment, effectively eliminating the attacker's head start.

Stop Threats Before They Strike

For businesses in financial services, a breach is a matter of *when*, not *if*.

The ultimate defense is early-stage detection. By intercepting attackers as they move throughout the network, organizations can disrupt the kill chain after entry, but before adversaries secure high-value targets or execute their final objectives.

Faster detection during this critical window helps financial services organizations neutralize threats, limit operational disruption, and reduce the financial fallout from modern cyberattacks.

Learn how ExtraHop helps financial services customers like BAC Credomatic — the largest financial institution in Central America — stop threats in their tracks.

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.

EXTRAHOP®