DEEPWATCH™



2026 DEEPWATCH FRONTLINE REPORT:

The Precision Mandate

A Year of Edge Exploitation, Identity Shifts, and Evasive Maneuvers

Published by: Deepwatch ATI Team
Date: March 2026

EXECUTIVE SUMMARY



2025: The Year of the Edge-to-Identity Pivot

In 2025, Deepwatch observed a transition from broad, opportunistic attacks to highly targeted "Edge-to-Identity" campaigns. By weaponizing zero-day vulnerabilities in edge gateways (VPNs/Firewalls) and bypassing the "Human Firewall" through sophisticated social engineering, adversaries achieved unprecedented access with surgical precision and minimal noise.

The Three Defining Pillars of 2025:

- **The Exploitation of the Edge:** The year was bookended by critical exploits in Ivanti, Cisco, and Oracle EBS. Adversaries moved "upstream," targeting the very appliances designed to secure the perimeter. This trend culminated in October with the attacks on Oracle EBS, proving that even internal ERP systems are now high-leverage targets for mass extortion.
- **The Identity Crisis & "Self-Infection":** As technical perimeters hardened, attackers turned to the user with devastating new TTPs. ClickFix (Pastejacking) became the breakout tactic of the year, tricking users into executing malicious code under the guise of "fixing" their browsers. Simultaneously, the TamperedChef campaign weaponized trusted developer tools (Node.js), using legitimate digital signatures to bypass EDR and remain dormant for months before activation.
- **The Extortion Evolution:** Ransomware matured into a data-theft enterprise. While encryption remains a threat, "extortion-only" models became the primary monetization strategy. The transition of elite affiliates from the dissolved Black Basta group into more agile clusters like SafePay and CACTUS signaled a move toward "Precision Extortion," where data exposure is the primary leverage.

The 2026 Strategic Mandate

The "NX Breach" in late 2025, served as a harbinger for the year ahead. As we move into 2026, the battleground is shifting toward Agentic AI—where autonomous bots navigate networks with human-like decision-making. To survive this acceleration, organizations must move beyond reactive security.

The following report outlines the move towards a Precision MDR model, integrating identity-aware detection, edge visibility, and an AI-driven response to out-pace tomorrow's adversaries.

TABLE OF CONTENTS

Executive Summary 2

Top Threats of 2025 4

Threat Vector 1: 5
The Edge Under Siege
Defending the Broken Perimeter

Threat Vector 2: 6
Ransomware's New Playbook
From Mass Encryption to Precision Extortion

Threat Vector 3: 7
The Human Firewall
Weaponizing Trust and Identity

Threat Vector 4: 8
Malware Evolution & Nation-State Nexus
Stealth and Sophistication

Threat Vector 5: 9
Customer Awareness & Advisory Analysis
Real-World Response: Recognition, Impact, and Resolution

- **Case Study 1:** 9
  The Ivanti "Credential Harvest"
- **Case Study 2:** 10
  The "Arcane Door" Campaign: Cisco ASA Exploitation
- **Case Study 3:** 10
  NX Breach: The "AI Agent Betrayal"
- **Case Study 4:** 11
  Oracle EBS Zero-Day: The Graceful Spider Strike
- **Case Study 5:** 11
  React & Next.js Server Component Flaws

2026 Forecast Analysis 12

Final Assessment 12



TOP THREATS OF 2025

Accelerated Evolution and Rapid Tactic Development

Advanced social engineering tactics, double extortion, edge device exploitation, software supply chain attacks, AI accelerated attacks... 2025 was a year full of evolving and ever changing tactics. As the threat actors grow and evolve, we grow and advance our capabilities to counter them.

- **Scattered Spider & Identity Hijacking:** Advanced social engineering targeting IT admins and vSphere environments.
- **Ransomware Evolution (Basta, Akira, Qilin, FOG):** High-speed encryption and "double extortion" tactics.
- **Edge Device Zero-Days:** Continuous exploitation of Ivanti, Cisco, and Fortinet appliances.
- **Living-Off-The-Land (LOTL):** Abuse of legitimate tools like ScreenConnect, SimpleHelp, and AnyDesk.
- **Supply Chain Infiltration:** The "Shai-Hulud" npm campaign and other developer-targeted attacks.
- **TamperedChef:** Victims lured through malvertising download trojanized tools, often signed with Extended Validation (EV) certificates, making them appear "safe" to Windows SmartScreen. These installers silently drop a legitimate node.exe binary and an obfuscated JavaScript file. Because node.exe is a trusted developer tool, its execution is frequently overlooked by security filters.
- **ClickFix (aka "Pastejacking" or "Fake CAPTCHA"):** In 2025, ClickFix emerged as the breakout social engineering threat, it became the second most frequent initial access vector globally, trailing only behind traditional phishing.



THREAT VECTOR 1:
THE EDGE UNDER SIEGE

Defending the Broken Perimeter

The year began and ended with a crisis in edge security. Adversaries, particularly China-linked groups like UNC5337, specialized in weaponizing VPN and network gateway vulnerabilities.

Ivanti Connect Secure (CVE-2025-0282): Early in 2025, a massive wave of exploitation targeted Ivanti appliances to deploy the "SPAWN" malware family. These attacks were characterized by their ability to survive reboots and evade traditional EDR by living entirely within the appliance's firmware.

Cisco ASA & FTD (CVE-2025-20333): In Q3, the "ArcaneDoor" campaign leveraged critical zero-days in Cisco VPN web servers. These flaws allowed unauthenticated root access, enabling nation-state actors to monitor encrypted traffic and exfiltrate credentials without ever touching the internal network.

The SonicWall Surge: Throughout the summer, Akira ransomware affiliates targeted unpatched SonicWall SSL VPNs, often moving from initial breach to domain controller compromise in under 12 hours.

Oracle EBS: Oracle EBS faced critical threats led by CVE-2025-61882, a 9.8 CVSS RCE vulnerability that allowed the CL0P group to conduct mass data exfiltration. By bypassing authentication in the BI Publisher component, attackers gained full system control, leveraging unpatched ERP systems as high-value targets for ransomware. This trend highlighted a major shift toward targeting the financial and supply chain cores of global enterprises through internet-facing legacy flaws.

SharePoint: Dubbed "ToolShell" primarily refers to a sophisticated, chained cyberattack that targeted on-premises Microsoft SharePoint servers in mid-2025, The situation escalated following the public release of proof-of-concept (PoC) exploits, with real-world attacks observed shortly thereafter. Following the discovery of these CVEs, Deepwatch published a blog post that provided an overview of the vulnerabilities, including key information and initial insights of the attacks.

THREAT VECTOR 2:
RANSOMWARE'S NEW PLAYBOOK

Ransomware groups in 2025 continued to mature into highly organized criminal enterprises. The "Ransomware-as-a-Service" (RaaS) model evolved to prioritize "data-theft-first" strategies.

From Mass Encryption to Precision Extortion

FOG Ransomware: Emerging in April, FOG specialized in masquerading as legitimate software installers. They focused heavily on the educational and healthcare sectors, using localized language to pressure victims.

Interlock & Qilin: These groups dominated the mid-year landscape. Interlock introduced a new Remote Access Trojan (RAT) that bypassed CAPTCHAs, while Qilin successfully targeted Managed Service Providers (MSPs) to achieve a "one-to-many" impact.

RansomHub & Betruger: RansomHub remained a top-tier threat by integrating the Betruger backdoor, allowing for long-term persistence even after a ransom was paid or a system was restored.

BlackBasta: The dissolution of Black Basta in early 2025 did not end the threat; instead, it triggered a fragmented migration of elite cybercriminals and highly specialized tactics across the RaaS (Ransomware-as-a-Service) landscape. Groups like CACTUS, SafePay, and DragonForce all share significant technical DNA with the old Conti and Black Basta codebases.

The Evolution of TTPs (Tactics, Techniques, and Procedures)

- BYOVD (Bring Your Own Vulnerable Driver): The most dangerous evolution in 2025–2026 is the embedding of vulnerable drivers (like NsecSoft NSecKrnl) directly into the payload. This allows the ransomware to kill EDR and antivirus processes (CrowdStrike, Sophos, SentinelOne) from the kernel level before encryption starts.
- Teams Phishing & Vishing: A social engineering "triple-threat." Attackers flood an employee with spam, call them pretending to be IT (vishing), and then initiate a Microsoft Teams chat to "help" them. They use this trust to have the user install RMM tools (like Quick Assist or AnyDesk) or execute a malicious Python script via cURL.
- MFA-Bypass via Session Hijacking: Instead of trying to crack passwords, actors now focus heavily on stealing session cookies from browsers to bypass Multi-Factor Authentication entirely, often using custom Infostealers before deploying the ransomware.

CHAPTER 3:
THE HUMAN FIREWALL

Weaponizing Trust and Identity

As technical perimeters hardened, threat actors focused on the most vulnerable link: *the user*.

Scattered Spider: This group remained a persistent thorn in the side of enterprise security. Their tactics evolved to include "MFA Fatigue 2.0," where they used AI-generated voice clones to trick help desk employees into resetting credentials.

SEO Poisoning & Fake IT Tools: A major trend in August involved malicious advertisements for tools like "ManageEngine" and "ChatGPT" apps. IT administrators searching for professional software were led to trojanized installers that delivered the Bumblebee malware.

DPRK Fake IT/Candidate: Throughout 2025 there was a widespread, government-backed scheme where North Korean IT workers used fake or stolen identities to secure remote jobs with global companies mainly in the U.S. to generate hundreds of millions in revenue to support North Korea's agenda.

iCloud and Salesforce Exploits: Late in the year, "Calendar Lures" became a widespread phishing tactic. By injecting malicious invites into iCloud and Outlook calendars, attackers bypassed email filters to deliver credential-harvesting links.



THREAT VECTOR 4:
MALWARE EVOLUTION & NATION-STATE NEXUS

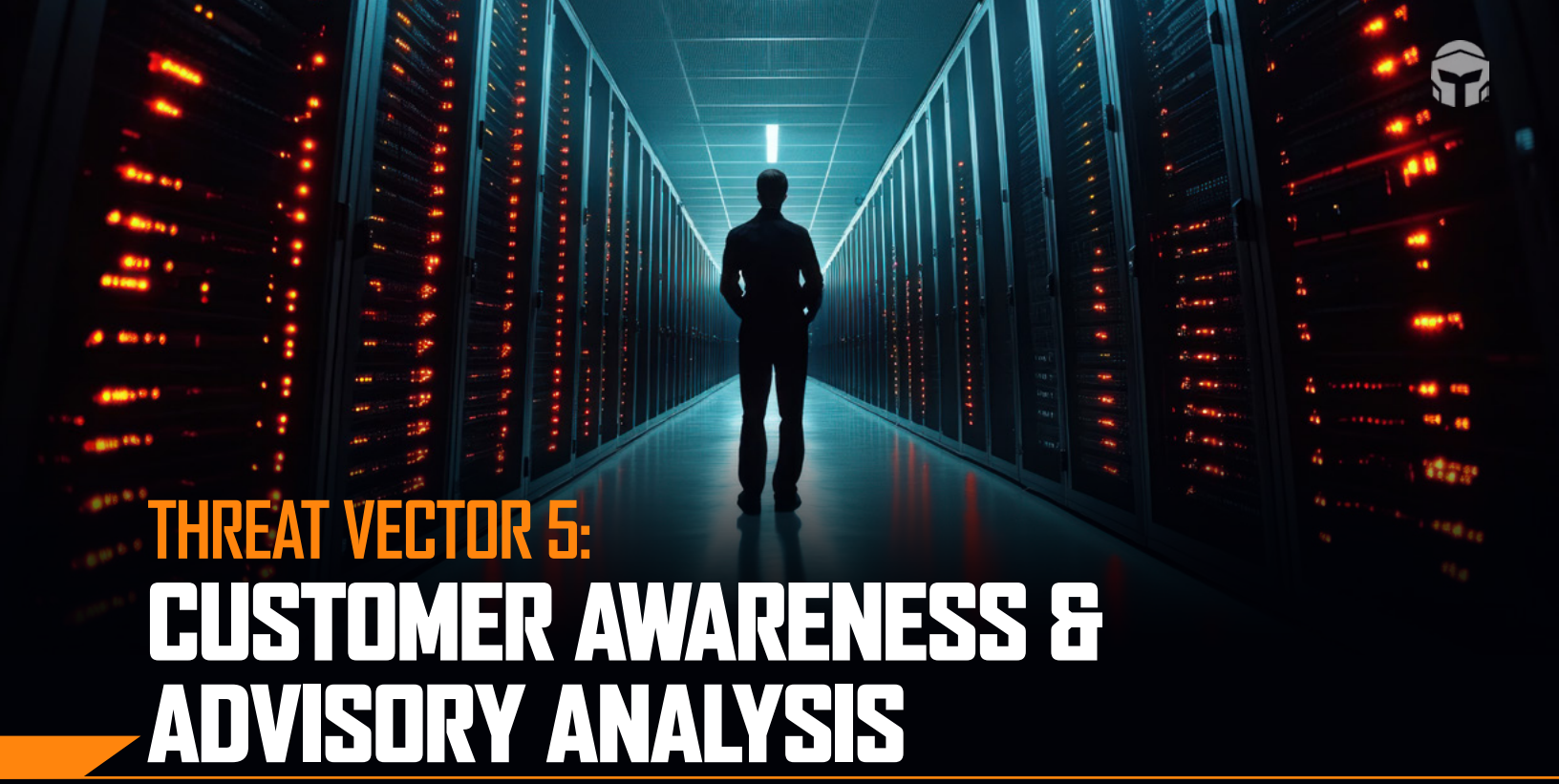
Stealth and Sophistication

The Shai-Hulud Supply Chain Attack: In September, a massive supply chain attack was discovered in the npm registry. Dubbed "Shai-Hulud," it targeted federal contractors by infiltrating open-source dependencies used in secure development environments.

Infostealer Dominance: Lumma Stealer and Rhadamanthys continued to dominate the "underground economy." These tools became more modular, adding features to specifically target cryptocurrency wallets and browser-based password managers.

North Korean (DPRK) Targeting: Groups like Moonstone Sleet shifted focus to IT developers, using fake job interviews and technical assessments to trick engineers into running malicious "coding challenges" that compromised corporate laptops.





THREAT VECTOR 5:
CUSTOMER AWARENESS & ADVISORY ANALYSIS

Real-World Response: Recognition, Impact, & Resolution

In 2025, Deepwatch's Adversary Tactics and Intelligence (ATI) team issued several critical advisories. These events represent the "front lines" of the year's most significant security challenges. Below is an analysis of how these threats materialized and how affected organizations navigated the road to recovery.

01

JANUARY 2025
The Ivanti "Credential Harvest"

THE EVENT:

Suspected Chinese threat actors exploited a zero-day vulnerability (CVE-2025-0282) in **Ivanti Connect Secure** appliances. The goal was stealthy data exfiltration and long-term credential harvesting.

RECOGNITION:

Anomalous Logins:

Affected parties first recognized the event through unusual VPN login patterns occurring at non-standard hours from geographically improbable locations.

- **File Integrity Monitoring:** Deepwatch identified unauthorized modifications to the appliance's underlying system files, which were being used to host a custom webshell.

OVERCOMING THE EVENT:

- **Hard Resets & Patching:** Mitigation required a full factory reset of the hardware to ensure no persistence remained in the firmware, followed by the immediate application of the vendor's emergency XML mitigation file.
- **Credential Rotation:** Organizations implemented a mandatory global password reset and revoked all active OAuth tokens to neutralize the harvested credentials.

02

SEPTEMBER 2025

The "ArcaneDoor" Campaign: Cisco ASA Exploitation

THE EVENT:

A sophisticated espionage campaign (Storm-1849) utilized two critical vulnerabilities (CVE-2025-20333 and CVE-2025-20362) to gain unauthorized root access to **Cisco ASA** devices.

RECOGNITION:

Egress Traffic Analysis:

The breach was recognized by detecting small, encrypted "heartbeat" packets sent to previously unknown command-and-control (C2) servers.

- **Memory Forensics:** Deepwatch ATI experts utilized memory forensics to identify the "RayInitiator" and "LINE VIPER" malware families running in the device's volatile memory, which did not leave a footprint on the physical disk.

OVERCOMING THE EVENT:

- **iSegmentation:** Affected parties immediately isolated the management interface of their edge devices from the public internet.
- **Firmware Verification:** Organizations utilized Cisco's software integrity validation tools to confirm the authenticity of the running OS image before performing a clean re-install of the patched firmware.

03

SEPTEMBER 2025

NX Breach: The "AI Agent Betrayal"

THE EVENT:

A landmark supply chain attack on the NX package ecosystem. Threat actors infiltrated the build pipeline and utilized integrated AI tools (like Gemini and Claude) to automate the reconnaissance of internal developer environments.

RECOGNITION:

API Overuse:

Developers noticed an unexpected spike in AI API calls associated with their build service accounts.

- **Behavioral Detections:** Security teams recognized "betrayal" when AI agents began requesting access to sensitive environment variables and internal documentation repositories that were outside their normal scope.

OVERCOMING THE EVENT:

- **"Human-in-the-Loop" Verification:** Organizations moved to a strict "manual approval" phase for all AI-generated code and configuration changes within the CI/CD pipeline.
- **Secrets Management:** All API keys and secrets exposed to the AI environment were rotated, and stricter IAM policies were enforced to limit AI agents to "read-only" access for non-essential repositories.

04

OCTOBER 2025

Oracle EBS Zero-Day: The Graceful Spider Strike

THE EVENT:

The threat group **Graceful Spider** (linked to Cl0p) exploited a critical RCE vulnerability (CVE-2025-61882) in **Oracle E-Business Suite (EBS)** for mass extortion.

RECOGNITION:

System Latency:

Users reported significant slowdowns in financial reporting modules.

- **Endpoint Detection:** Deepwatch's Precision MDR flagged unauthorized Java processes spawning cmd.exe—a classic sign of exploitation in the EBS environment.

OVERCOMING THE EVENT:

- **WAF Shielding:** Before a patch was fully deployed, organizations used Web Application Firewalls (WAFs) to block the specific URI patterns used in the exploit's payload.
- **Emergency Patching:** Once the Oracle "Critical Patch Update" was released, teams performed weekend-long emergency maintenance cycles to patch the enterprise resource planning (ERP) systems.

05

DECEMBER 2025

React & Next.js Server Component Flaws

THE EVENT:

Max-severity (10.0) RCE flaws (CVE-2025-55182) were discovered in **React 19** and **Next.js 15/16**. Attackers used insecure deserialization in Server Components to execute code on the web server.

RECOGNITION:

Payload Signature Matching:

Deepwatch ATI recognized the threat by identifying specific malformed JSON/RSC payloads being sent to public-facing web applications.

- **Internal Vulnerability Scanning:** Automated scanners identified outdated versions of the frameworks in "shadow IT" projects that had bypassed traditional review processes.

OVERCOMING THE EVENT:

- **Framework Upgrades:** Affected parties prioritized the upgrade to React 19.1 and Next.js 16.0.2, which introduced hardened deserialization logic.
- **Input Validation:** Developers implemented stricter schema validation for all incoming React Server Component (RSC) requests to prevent unauthenticated server compromise.

FORWARD RECON

2026 FORECAST ANALYSIS

As we look toward 2026, the Deepwatch ATI team predicts the following trends:

1. **Agentic AI Attacks:** Threat actors will move beyond using AI for phishing emails to deploying "Agentic AI" bots that can autonomously perform reconnaissance, exploit vulnerabilities, and navigate internal networks with human-like decision-making.
2. **SaaS-to-SaaS Attacks:** With more data moving to the cloud, we expect a surge in attacks that leverage OAuth token theft to move laterally between SaaS platforms (e.g., from Salesforce to Slack to Google Workspace) without ever touching an endpoint.
3. **The Rise of "Disruption-as-a-Service":** Driven by geopolitical tensions, we anticipate more "pseudo-ransomware" attacks where the goal is not profit but the destruction of data and disruption of critical services, masked as criminal activity.
4. **Supply Chain 3.0:** Attacks will move further "upstream," targeting the AI models themselves (Data Poisoning) and the automated CI/CD pipelines used to train them.

THE PRECISION MANDATE

FINAL ASSESSMENT

The 2025 threat landscape proved that "defensibility" is a moving target. The sheer volume of edge vulnerabilities combined with the relentless targeting of identities has made traditional detection insufficient. Organizations must move toward a **Precision MDR** approach, integrating identity-aware detections with deep visibility into edge devices. As we enter 2026, the battle will be won by those who can automate their defenses as fast as the adversaries automate their attacks.





DEEPWATCH™

Deepwatch® is the leader in Precision MDR powered by AI and humans. We amplify human expertise with AI insights to reduce the risks that matter most to your business. Our protection is proactive, preemptive and responsive, tuned to your business, with no black boxes, and watched by experts 24/7/365.

Learn more: **www.deepwatch.com**

Follow us:

Blog | LinkedIn | Facebook