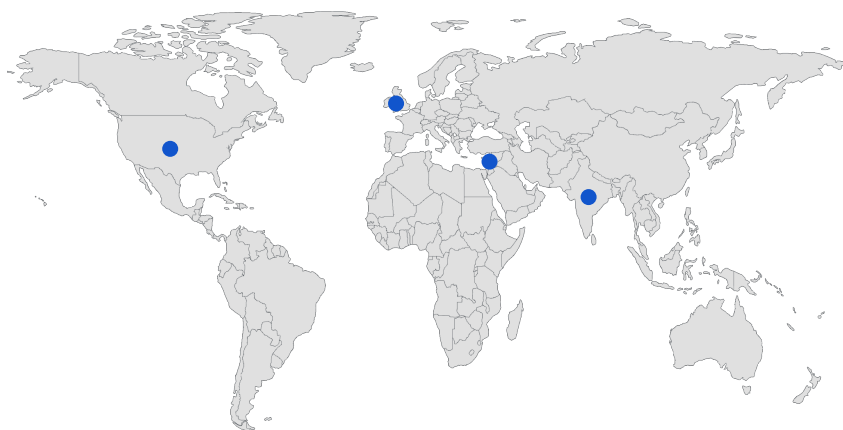


Threat Intel Report: May 26–June 1, 2025

Countries



Top Tags

NetBird

Interlock

NodeSnake

Often9

Chort

Executive Summary

Actionable Information:

- **Credential Theft and Stealth Access Tactics Expand:** Adversaries are leveraging native Windows functions like DCOM to extract NTLM credentials without deploying traditional malware, evading most EDR detection. Simultaneously, attackers are delivering remote access tools via phishing campaigns that target executives, and distributing malware through fake Google Meet pages that execute PowerShell payloads. These trends reflect a growing preference for stealthy, credential-focused attack vectors that enable lateral movement and long-term persistence.
- **Ransomware and Remote Access Threats Escalate in Education and Government:** The education sector and local governments remain top targets for ransomware groups. Interlock's deployment of the new NodeSnake RAT against UK universities demonstrates how ransomware operators are evolving their toolsets, while the Chort gang's breach of Sheboygan, WI, reveals how long ransomware attacks can go undetected and unreported. These incidents underscore the need for improved detection, incident response, and phishing defenses across under-resourced sectors.
- **API and Protocol Vulnerabilities Undermine Platform and Web Security:** This week saw major exposure of insecure system-level interfaces. A threat actor claims to have exfiltrated 428 million TikTok user records via a vulnerable API, while newly disclosed flaws in HTTP/2 and HTTP/3 protocols (CrossPUSH and CrossSXXG) allow cross-site scripting attacks by abusing shared TLS certificates. These systemic issues highlight the critical need for improved monitoring of APIs and prompt patching of underlying web infrastructure.
- **Supply Chain and Insider Threats Lead to Major Data Breaches:** Two high-impact breaches—LexisNexis and Coinbase—stemmed from weaknesses in development infrastructure and third-party partnerships. LexisNexis exposed over 364,000 individuals' personal data due to unauthorized GitHub access, while a Coinbase vendor

employee allegedly leaked sensitive customer data in exchange for bribes. These cases demonstrate the persistent risk of insider threats and underscore the importance of securing both internal and vendor environments.

- **Cloud Misconfigurations and Social Engineering Cause Massive Losses:** A publicly accessible database exposed 184 million login credentials, showing how cloud misconfigurations still lead to large-scale breaches. At the same time, Central Florida Cares Health System lost \$3.6 million due to a phishing scheme exploiting user trust in fake banking portals. As attackers continue to exploit misconfigurations and human behavior, organizations must prioritize cloud posture management and user training to close these gaps.

Outlook:

The cybersecurity landscape this week reinforces the reality that attackers are no longer reliant solely on malware to compromise systems. Instead, they are combining stealthy credential access, social engineering, and architectural flaws to achieve their goals. Ransomware continues to plague public sector entities, while data exposure through insider threats, API abuse, and cloud misconfigurations remains a persistent problem. As AI adoption, remote collaboration, and decentralization grow, organizations must harden their defenses not just at the endpoint but across APIs, cloud platforms, and human interfaces. Expect attackers to continue adapting quickly, targeting trust-based systems and overlooked attack surfaces.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 1,958% [CVE-2025-34027](#)

- The Versa Concerto SD-WAN orchestration platform is vulnerable to an authentication bypass in the Traefik reverse proxy configuration, allowing an attacker to access administrative endpoints. The Spack upload endpoint can be leveraged for a Time-of-Check to Time-of-Use (TOCTOU) write in combination with a race condition to achieve remote code execution via path loading manipulation, allowing an unauthenticated actor to achieve remote code execution (RCE).

↑ 1,945% [CVE-2025-34026](#)

- The Versa Concerto SD-WAN orchestration platform is vulnerable to an authentication bypass in the Traefik reverse proxy configuration, allowing an attacker to access administrative endpoints. The internal Actuator endpoint can be leveraged for access to heap dumps and trace logs.

↑ 1,001% [CVE-2024-11972](#)

- The Hunk Companion WordPress plugin before 1.9.0 does not correctly authorize some REST API endpoints, allowing unauthenticated requests to install and activate arbitrary Hunk Companion WordPress plugin before 1.9.0 from the WordPress.org repo, including vulnerable Hunk Companion WordPress plugin before 1.9.0 that have been closed.

Israeli Sites Targeted by Large DDoS Attacks

+Israel +DDoS +Financial Services +Healthcare +Hacktivism

- Israeli websites, including those in the financial and healthcare industries, have been increasingly targeted by distributed denial-of-service (DDoS) attacks this week, reaching up to 7.7 million requests per second (RPS) in a single attack, and a total combined volume of 22 million RPS over four days. Several IP addresses were

observed participating in all the attacks, pointing to a common attacker most likely motivated by political hacktivism.

US Entertainment Site Targeted by ATO

+US +Entertainment +ATO

- A US entertainment site was targeted by account takeover (ATO) attacks reaching over 9 million login attempts in one day. The attack focused on API login endpoints, including exposed staging environments, and likely used credential stuffing techniques with automated tools to test large volumes of stolen username-password pairs.

Recent Cyber Threats

DCOM Exploited for Stealthy Credential Harvesting

+DCOM +Windows +Credential Theft

- Threat actors are leveraging the Distributed Component Object Model (DCOM) in Windows systems to harvest NTLM credentials without deploying traditional malware. Utilizing a tool named [RemoteMonologue](#), attackers coerce NTLM authentications by exploiting specific DCOM objects, enabling lateral movement and privilege escalation while evading detection by Endpoint Detection and Response (EDR) solutions. This technique underscores the need for organizations to monitor DCOM activity and enforce strong authentication protocols.

Spearphishing Campaign Targets Financial Executives with Remote Access Tool

+Spearphishing +Financial Services +NetBird

- A sophisticated [spearphishing](#) campaign is targeting CFOs and financial executives across banks, investment firms, utilities, and insurance companies worldwide. Attackers distribute emails containing installers for NetBird, a legitimate-looking remote access tool, to gain persistent access to victim systems. The campaign's focus on high-level financial personnel increases the risk of unauthorized fund transfers and sensitive data theft.

Fake Google Meet Page Delivers PowerShell Malware

+PowerShell +RAT +Social Engineering

- Cybercriminals have created a counterfeit [Google Meet](#) page that prompts users to execute a PowerShell command under the guise of fixing a microphone permission error. This social engineering tactic leads to the download and execution of a remote access trojan (RAT), compromising the user's system. The attack highlights the importance of user awareness and skepticism towards unexpected prompts.

HTTP/2 Flaw Enables Cross-Site Scripting Attacks

+HTTP/2 +CrossPUSH +CrossSXG +XSS

- Researchers have identified vulnerabilities in the HTTP/2 and HTTP/3 protocols that allow attackers to bypass the Same-Origin Policy (SOP) through techniques dubbed [CrossPUSH and CrossSXG](#). By exploiting shared TLS certificates, attackers can inject malicious scripts into trusted websites, leading to cross-site scripting (XSS) attacks. This flaw affects a significant portion of web infrastructure, necessitating immediate attention from web administrators.

Interlock Ransomware Deploys NodeSnake RAT in University Attacks

+Interlock +NodeSnake +RAT +UK +Education

- The Interlock ransomware group is deploying a new remote access trojan (RAT) named [NodeSnake](#) to target educational institutions in the UK. Delivered via phishing emails, NodeSnake establishes persistence by masquerading as a Chrome updater and facilitates data exfiltration and ransomware deployment. The emergence of NodeSnake indicates Interlock's evolving tactics to infiltrate and compromise academic networks.

Malicious AI Tool Installers Used to Distribute Malware

+AI +Malware

- Cybercriminals are distributing [fake installers for AI tools](#), embedding malware within them to compromise systems across various industries. These counterfeit applications exploit the growing demand for AI solutions, deceiving users into installing malicious software that can lead to data breaches and system compromises. Organizations are advised to verify the authenticity of software sources before installation.

Data Breaches

Unsecured Database Exposes 184 Million Login Credentials

+Unsecure Database +Cloud Storage

- A massive data breach exposed over [184 million unencrypted login credentials](#), including emails and passwords associated with major platforms like Google, Apple, and Facebook. Cybersecurity researcher Jeremiah Fowler discovered the unsecured database, which was publicly accessible online. The breach highlights the risks associated with misconfigured cloud services and the importance of securing sensitive data.

TikTok API Exploit Allegedly Exposes 428 Million User Records

+TikTok +Often9

- A threat actor known as Often9 claims to have exploited a vulnerability in [TikTok's](#) internal API, resulting in the extraction of 428 million user records. The dataset reportedly includes email addresses, phone numbers, user IDs, and account statuses. TikTok is currently investigating the legitimacy of the breach.

Cork Protocol Suffers \$12 Million DeFi Exploit

+Cryptocurrency +DeFi +Financial Services

- The decentralized finance platform [Cork Protocol](#) experienced a security breach resulting in the theft of approximately \$12 million worth of cryptocurrency. Attackers exploited a vulnerability in the platform's smart contract related to the wstETH:weETH market. In response, Cork Protocol has paused all markets and is conducting an investigation.

LexisNexis Data Breach Exposes Personal Information of Over 364,000 Individuals

+GitHub +Data Brokerage

- [LexisNexis Risk Solutions](#) disclosed a data breach affecting more than 364,000 individuals, with compromised data including names, Social Security numbers, and driver's license details. The breach occurred via unauthorized access to the company's GitHub account used for software development. The incident raises concerns about the security practices of data brokers handling sensitive personal information.

Sheboygan Ransomware Attack Impacts Nearly 70,000 Residents

+Chort +US +Government

- The city of [Sheboygan, Wisconsin](#), reported a ransomware attack that compromised the personal data of approximately 67,000 residents, including Social Security numbers and state IDs. The Chort ransomware group claimed responsibility for the attack, which occurred in October 2024 but was disclosed in May 2025.

Florida Nonprofit Loses \$3.6M in Sophisticated Phishing Scam

+Healthcare +Social Engineering

- [Central Florida Cares Health System](#), a nonprofit managing behavioral health services, fell victim to a phishing attack resulting in a \$3.6 million loss. An employee inadvertently entered credentials into a fraudulent banking website, enabling cybercriminals to access the organization's real bank account and initiate unauthorized transfers. The incident underscores the vulnerability of healthcare nonprofits to social engineering tactics.

Coinbase Customer Data Compromised via Outsourcing Partner

+Financial Services +Cryptocurrency +India

- [Coinbase](#) experienced a significant data breach linked to its outsourcing partner, TaskUs, based in India. An employee at TaskUs was caught photographing sensitive customer information, which was allegedly shared with hackers in exchange for bribes. The breach affected nearly 70,000 customers and is expected to cost Coinbase up to \$400 million in remediation efforts.

Imperva Protection

Imperva provides comprehensive digital security solutions, including protection against threats to web applications and APIs– including security vulnerabilities, fraud, and bad bots, data security solutions, and security against disruptive network- and application-level DDoS attacks.