

Threat Intel Report: June 2-8, 2025

Countries



Top Tags

PuTTY

Lumma

ASyncRAT

SocGhosh

Qilin

Executive Summary

Actionable Information:

- **Clipboard Injection Malware on the Rise:** Multiple campaigns this week leveraged clipboard hijacking via fake CAPTCHA pages and phishing sites. HuluCaptcha, a new framework mimicking Cloudflare CAPTCHA screens, was used to trick users into pasting PowerShell commands that deploy Lumma, Aurotun, or AsyncRAT. Fake DocuSign and Booking.com pages employed similar tactics. This approach reflects a broader trend in socially engineered clipboard manipulation targeting non-technical users through visually trusted interfaces.
- **Supply Chain Threats Target WordPress and NPM Ecosystems:** Malicious JavaScript embedded in fake NPM packages is being used to harvest Ethereum wallet credentials from developers. Simultaneously, a rogue WordPress plugin disguised as a caching tool ("wp-runtime-cache") was discovered stealing admin credentials. These incidents highlight ongoing supply-chain risks in open-source and content management platforms, where threat actors exploit implicit trust in widely adopted tools.
- **Use of LOLBINs and Living-off-the-Land Techniques Expanding:** Trojanized PuTTY clients, abusing ssh.exe as a LOLBIN, were observed deploying persistent backdoors that launch disguised payloads like dllhost.exe. These techniques bypass traditional detection and highlight increased sophistication among attackers prioritizing stealth and durability within Windows environments.
- **Credential-based Attacks Dominate Consumer Services:** The North Face suffered a large-scale credential stuffing attack that exposed customer PII but not payment data. The ColoCloud breach stemmed from a vulnerable third-party SSO integration (Virtualizor), leaking thousands of customer records. These incidents reinforce that credential reuse and third-party vulnerabilities remain critical weak points in both retail and infrastructure services.

- **Ransomware Groups Continue to Target High-Value Data:** The Qilin ransomware group continues aggressive activity, breaching both Next Step Healthcare and Lee Enterprises. Exfiltrated data includes highly sensitive medical and financial information, with over 50,000 individuals affected across both attacks. Meanwhile, Sensata Technologies also disclosed a ransomware breach compromising health, financial, and identity data. These incidents confirm that ransomware operators are shifting focus toward sectors with rich PII stores and limited downtime tolerance.

Outlook:

This week's threats reflect a clear convergence of supply-chain exploitation, credential harvesting, and evasive persistence methods. Clipboard-based malware delivery is becoming a favored vector due to its simplicity and user-driven execution path, making it difficult to detect with traditional AV tools. At the same time, the surge in attacks leveraging trusted platforms—like NPM, WordPress, and SSO tools—shows that attackers are continuing to exploit gaps in dependency chains and administrative oversight. The Qilin ransomware group's repeated targeting of healthcare and media providers, along with the appearance of enriched datasets from previous breaches (e.g., AT&T), signals that adversaries are capitalizing on previously stolen data to amplify current campaigns. Organizations must tighten endpoint protections, audit third-party tools, and monitor user behavior to prevent exploitation of these attack vectors.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 1,364,886% [CVE-2025-4322](#)

- The Motors theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 5.6.67. This is due to the theme not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user passwords, including those of administrators, and leverage that to gain access to their account.

↑ 4,333% [CVE-2025-27007](#)

- Incorrect Privilege Assignment vulnerability in Brainstorm Force SureTriggers allows Privilege Escalation. This issue affects SureTriggers: from n/a through 1.0.82.

↑ 468% [CVE-2024-7399](#)

- Improper limitation of a pathname to a restricted directory vulnerability in Samsung MagicINFO 9 Server version before 21.1050 allows attackers to write arbitrary file as system authority.

Recent Cyber Threats

Trojanized PuTTY SSH Client Turns Malware Launcher

+PuTTY +LOLBIN

- Threat researchers have observed attackers distributing trojanized versions of [PuTTY](#) and abusing Windows' native OpenSSH (ssh.exe) as a trusted LOLBIN to establish stealthy, persistent backdoors. The malicious loader, disguised as legitimate ssh activity, launches a secondary payload camouflaged as dllhost.exe, enabling covert remote access. This tactic helps adversaries evade detection tools while maintaining command-and-control communications with compromised systems.

HuluCaptcha: Fake CAPTCHA Deploys Info-Stealer RATs

+CAPTCHA hijacking +HuluCaptcha +Lumma +Aurotun

- A new fake captcha framework dubbed [HuluCaptcha](#) lures victims with Cloudflare-like CAPTCHA prompts, then hijacks the clipboard to copy a malicious PowerShell command. Users who paste the command into Win+R unknowingly deploy malware—observed delivering stealers like Lumma and Aurotun. The code injection comes from compromised WordPress sites, highlighting widespread supply-chain origins.

Fake Booking Sites Push AsyncRAT via Clipboard Trick

+AsyncRAT +CAPTCHA hijacking

- Since mid-May, users redirected from ads or social media to fake Booking.com pages face [deceptive CAPTCHA prompts](#) that hijack their clipboard. Victims prompted to paste and run a PowerShell command in the Windows Run dialog are infected with AsyncRAT, a remote-access Trojan capable of data theft. Obfuscated domains rotate every 2–3 days to evade blocking.

NPM Poisoning Targets Ethereum Wallet Keys

+NPM +Cryptocurrency

- Cybersecurity teams uncovered obfuscated JavaScript in [malicious NPM packages](#) designed to steal Ethereum wallet private keys and seed phrases. These systematically connect to remote C2 servers in multi-stage attacks, exploiting developer trust in open-source ecosystems. The campaign underscores growing crypto-targeted supply-chain risks in developer environments.

Phishing with Fake DocuSign Clones Deploys NetSupport RAT

+Phishing +SocGhosh +NetSupport RAT

- Security analysts report a phishing campaign using fake DocuSign (and Gitcode) [clone sites](#). Once users trigger a CAPTCHA, malicious PowerShell scripts are copied to the clipboard and executed via Win+R. This multi-stage downloader fetches additional payloads, culminating in the deployment of NetSupport RAT for remote control. Attack resembles past SocGhosh campaigns.

Fake WordPress Caching Plugin Hijacks Admin Logins

+WordPress +Plugin +Credential Stealing

- A malicious [WordPress plugin](#) posing as a caching tool—wp-runtime-cache—was discovered stealing administrator credentials from infected sites. Unlike legitimate plugins, it contains no listed author or version information and hides itself from the WordPress dashboard to avoid detection. The plugin quietly exfiltrates login credentials using obfuscated JavaScript embedded within its PHP files and transmits stolen data to an attacker-controlled domain. Distribution methods remain unclear but likely involve phishing, nulled plugin repositories, or compromised admin accounts.

Data Breaches

Next Step Healthcare Breach Exposes Medical, Financial Data

+Healthcare +US +Qilin

- In July 2024, the Qilin ransomware gang allegedly breached [Next Step Healthcare's](#) network, stealing over 12,090 records—including SSNs, medical records, drivers' licenses, credit/debit card details, and financial account data. Affected states include Massachusetts (10,041 people) and New Hampshire (1,697). Qilin posted the stolen data but it's unclear whether a ransom was paid.

ColoCloud SSO Error Leads to Exposure of Customer Credentials

+Technology +Third-Party

- In May 2025, ColoCrossing's [ColoCloud VPS](#) service suffered a breach due to a flaw in its single sign-on system. This vulnerability allowed attackers to extract approximately 7,200 user records, including email addresses, full names, and MD5-Crypt hashed passwords. The breach was caused by a vulnerability in

Virtualizor, which is a third-party tool used by ColoCloud, meaning other providers using Virtualizor are likely vulnerable as well.

The North Face User Data Exposed in Large-Scale Credential Stuffing Attack

[+Retail](#) [+eCommerce](#) [+Credential Stuffing](#)

- On April 23, 2025, [The North Face](#) detected a credential-stuffing campaign targeting its e-commerce platform, where stolen login credentials (usernames and passwords) were used en masse. Investigators confirmed that personal data (names, email addresses, shipping addresses, phone numbers, dates of birth, and purchase histories) had been accessed. No payment card data was compromised, as transactions are handled externally via a tokenization provider. The company has reset affected user passwords and is notifying customers, urging them to implement strong, unique passwords and MFA.

Mass AT&T Data Leak Includes Plaintext SSNs & ID Details

[+Telecommunications](#) [+Russia](#)

- Beginning May 15 and resurging on June 3, 2025, threat actors posted a data trove of ~86 million [AT&T customer records](#) on Russian cybercrime forums. The dataset includes decrypted SSNs (~44 million), birthdates, phone numbers, addresses, emails, and possibly other PII—taking previous leaks from the 2021 ShinyHunters and April 2024 Snowflake breach to another level. While AT&T is investigating, analysis indicates this appears to be a cleaned and enriched version of the earlier breach, now with plaintext SSNs and DOBs, which significantly increases identity theft risk. Customers are being advised to monitor credit reports, set up alerts or freezes, and remain vigilant against fraud.

Lee Enterprises Hit By Qilin Ransomware, Exposing Employee Data

[+Qilin](#) [+News](#)

- In early February 2025, [Lee Enterprises](#)—operator of over 70 local newspapers—was struck by the Qilin ransomware gang, which encrypted networks, disrupted printing operations, website services, advertising, and freelancer payroll. Qilin claims to have stolen approximately 350 GB of data before threatening release if no ransom was paid. Subsequent breach reports indicate nearly 40,000 current and former employees had SSNs, names, emails, and financial data exfiltrated.

Sensata Suffers Ransomware Breach That Compromises Highly Sensitive PII

[+Technology](#) [+US](#)

- Between March 28 and April 6, 2025, [Sensata Technologies](#) was infiltrated by ransomware actors who encrypted internal systems, disrupted operations—including shipping and manufacturing—and exfiltrated sensitive personal data. The breach impacted names, SSNs, tax and government ID numbers, financial account and payment card data, medical and health insurance information, and dates of birth.

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.