

Threat Intel Report: May 12-18, 2025

Countries



Top Tags

INC

Qilin

Machine1337

ScatteredSpider

DragonForce

Executive Summary

Actionable Information:

- **Ransomware and Data Extortion Surge:** Recent attacks on organizations like South African Airways, Duo Broadband, and Nova Scotia Power highlight a persistent trend of ransomware and data extortion campaigns. Threat actors are increasingly targeting critical infrastructure and service providers, exploiting vulnerabilities to disrupt operations and demand ransoms.
- **Supply Chain Vulnerabilities:** The breach of Communications Data Group, affecting Duo Broadband customers, underscores the risks associated with third-party vendors. Organizations must assess and monitor the security posture of their supply chain partners to prevent indirect breaches.
- **Government and Public Sector Attacks:** The exploitation of the GovDelivery email system to send phishing messages and the breach of the UK's Legal Aid Agency demonstrate that government entities remain prime targets. These incidents emphasize the need for robust security measures and continuous monitoring within public sector organizations.
- **Advanced Threat Techniques:** The use of steganography to deliver undetectable ransomware via JPEG images and the expansion of ClickFix attacks to Linux systems indicate that threat actors are adopting sophisticated methods to bypass traditional security defenses. Organizations should enhance their detection capabilities to identify such advanced threats.
- **Healthcare Sector Risks:** The Serviceaide breach, exposing data of 483,000 Catholic Health patients, highlights the vulnerability of the healthcare sector to cyberattacks. Given the sensitivity of healthcare data, institutions must prioritize cybersecurity investments and incident response planning.

Outlook:

The cybersecurity threat landscape continues to evolve, with attackers employing more sophisticated techniques and targeting a broader range of sectors. The convergence of advanced threat methods, such as AI-driven attacks and steganography, with traditional vulnerabilities in supply chains and public sector systems, presents a complex challenge for organizations. Proactive measures, including comprehensive risk assessments, employee training, and the adoption of advanced detection technologies, are essential to mitigate these risks. As cyber threats become more pervasive and damaging, a collaborative approach involving public and private sectors will be crucial to enhance resilience and protect critical assets.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 3,040% [CVE-2025-1974](#)

- A security issue was discovered in Kubernetes where under certain conditions, an unauthenticated attacker with access to the pod network can achieve arbitrary code execution in the context of the ingress-nginx controller. This can lead to disclosure of Secrets accessible to the controller.

↑ 217% [CVE-2025-22457](#)

- A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.6, Ivanti Policy Secure before version 22.7R1.4, and Ivanti ZTA Gateways before version 22.8R2.2 allows a remote unauthenticated attacker to achieve remote code execution.

↑ 121% [CVE-2024-2879](#)

- The LayerSlider plugin for WordPress is vulnerable to SQL Injection via the `ls_get_popup_markup` action in versions 7.9.11 and 7.10.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.

European Travel Site Targeted by ATO

+Travel +ATO

- A European airline's API login site was targeted by account takeover attacks this week, reaching 1 million attempted logins in two days. The attacks, which primarily utilized brute force techniques, came from bots.

German Telecommunications Company Hit by Automated Attacks

+Germany +Telecommunications +Bots

- A German telecommunications company was attacked by automated attacks, account takeover, cross-site scripting, and more in massive attacks this week, totaling over 15 million requests in one day. Attacks came from bots based in Germany and the Netherlands, suggesting localized botnets or IP masking.

Recent Cyber Threats

WordPress XML-RPC Leak Exposes Private Post Titles

+WordPress +Pingback

- Imperva researchers have identified a vulnerability in [WordPress's](#) XML-RPC interface that allows attackers to retrieve titles of private and draft posts. By exploiting the pingback feature, threat actors can scan for specific strings in post titles, potentially exposing sensitive information. Administrators are advised to update WordPress and disable XML-RPC if not in use.

Steganographic Ransomware Hidden in JPG Images

[+Steganography](#) [+Ransomware](#)

- Cybercriminals are employing [steganography](#) to embed fully undetectable ransomware within JPEG images. This multi-stage attack uses a disguised payload in the image to initiate a stager script, which then downloads the ransomware executable. The technique effectively bypasses traditional antivirus systems, highlighting the need for behavioral analysis tools.

ClickFix Attacks Expand to Linux Systems

[+ClickFix](#) [+APT36](#) [+Pakistan](#) [+India](#)

- [APT36](#), a Pakistan-linked threat group, is extending its ClickFix social engineering attacks to Linux systems. By impersonating India's Ministry of Defence, attackers prompt users to execute malicious commands, leading to malware infections. This marks a notable expansion from previous campaigns that primarily targeted Windows and macOS users.

GovDelivery Exploited to Send Government-Themed Scams

[+Government](#) [+US](#)

- Hackers have exploited the [GovDelivery](#) email system, used by U.S. government agencies, to send scam messages about unpaid tolls. A compromised contractor account was used to distribute emails that appeared official, redirecting recipients to malicious sites impersonating state agencies. The incident raises concerns about the security of government communication platforms.

Data Breaches

South African Airways Disrupted by Ransomware Group INC

[+South Africa](#) [+Travel](#) [+INC](#)

- The ransomware group INC has claimed responsibility for a cyberattack on [South African Airways \(SAA\)](#) on May 3, 2025. The incident temporarily disrupted the airline's website, mobile application, and several internal operational systems, which were restored later that day. SAA has not confirmed INC's claims or disclosed details about the nature of the attack or any ransom demands.

DDoSecrets Publishes 410GB of TeleMessage Breach Data

[+Telecommunications](#) [+Government](#) [+US](#)

- Distributed Denial of Secrets (DDoSecrets) has added 410GB of data from a breach of [TeleMessage](#), a company providing secure messaging solutions, to its index. The leaked data includes plaintext messages, metadata, and other sensitive information, some of which pertain to communications involving U.S. federal government officials. The breach has led to operational disruptions at TeleMessage, with its website content limited and services suspended.

Duo Broadband Customer Data Exposed via Vendor Breach

[+Qilin](#) [+Telecommunications](#)

- [Communications Data Group \(CDG\)](#), a billing vendor for Duo Broadband, notified 42,518 individuals of a data breach that occurred in February 2025. The breach exposed personal information, including names, addresses, dates of birth, and Social Security numbers of Duo Broadband customers. The Qilin ransomware group has claimed responsibility for the attack.

Nova Scotia Power Reports Customer Data Compromise

[+Canada](#) [+Utilities](#)

- [Nova Scotia Power](#), the province's largest electric utility, disclosed a cyberattack that compromised sensitive customer information, including banking details. The breach was discovered on April 25, 2025, prompting the company and its parent, Emera, to isolate affected servers. Investigations are ongoing to determine the full extent of the data compromised.

Twilio and Valve Deny Breach Amid Steam 2FA Code Leak Claims

[+Gaming](#) [+Machine1337](#)

- A threat actor known as [Machine1337](#) claimed to possess over 89 million Steam user records, including one-time access codes, and offered the data for sale. Both Twilio and Valve have denied any breaches of their systems, with Valve stating that the leaked codes were historical, time-limited, and not linked to account credentials or payment information. Investigations into the source of the data leak are ongoing.

DragonForce and Scattered Spider Target UK Retail Giants

[+UK](#) [+Retail](#) [+DragonForce](#) [+ScatteredSpider](#)

- UK retailers Marks & Spencer (M&S), Co-op, and Harrods have been targeted by coordinated cyberattacks attributed to the ransomware group [DragonForce](#) and the hacking group Scattered Spider. The attacks involved social engineering tactics, such as impersonating employees to deceive IT help desks into resetting passwords, leading to significant operational disruptions. M&S reported an estimated £60 million loss in profits and over £1 billion in market value, while Co-op faced supply chain issues and customer data compromises.

Serviceaide Breach Exposes Data of 483K Catholic Health Patients

[+Healthcare](#)

- [Serviceaide](#), a software vendor for Catholic Health, experienced a data breach between September 19 and November 5, 2024, exposing sensitive information of approximately 483,000 patients. The compromised data includes names, Social Security numbers, dates of birth, medical record numbers, patient account numbers, clinical information, provider details, and user credentials. The breach underscores the risks associated with third-party vendors in the healthcare sector.

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.