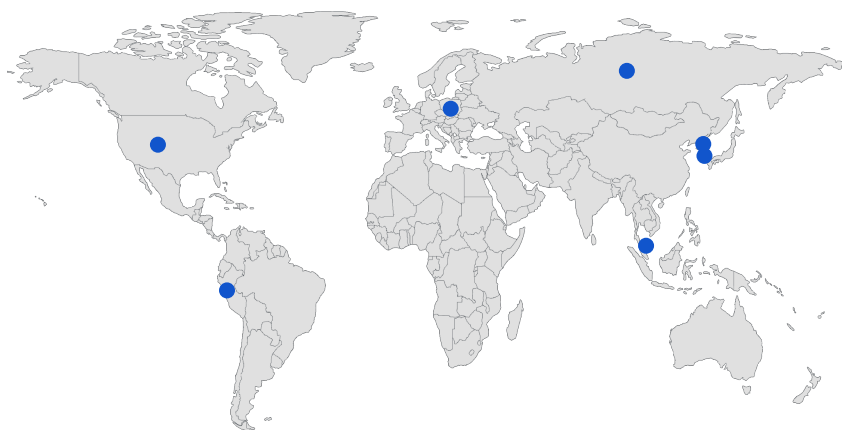


Threat Intel Report: April 28-May 4, 2025

Countries



Top Tags

Lazarus Group

Venom Spider

NoName057(16)

Conti

Rhysida

Executive Summary

Actionable Information:

- **Infostealer Malware Surge Across Sectors:** Multiple campaigns this week highlight the growing use of infostealer malware for credential harvesting. Lazarus Group (North Korea) targeted gamers with Ageostealer; Venom Spider (Russia) deployed More_eggs against HR departments; and Gremlin infostealer was introduced on Russian cybercrime forums. This surge underscores attackers' focus on stealing credentials at scale across diverse industries, from gaming to business operations.
- **Exploitation of Critical Vulnerabilities:** High-severity vulnerabilities are being actively disclosed, with one notable SQL injection flaw (CVE-2025-46337, CVSS 10.0) in the PHP ADOdb library threatening web applications globally. Similarly, an authentication bypass in Zimbra's GraphQL API could allow account takeovers. These critical flaws represent major risks to applications relying on popular libraries and APIs.
- **Critical Infrastructure and Government Targets Remain Under Siege:** Several incidents show persistent ransomware and cyberattacks against critical services. Conti attacked Kuala Lumpur Airport; Rhysida ransomware hit Peru's government; and Poland's PESEL identification system suffered a cyber incident. These incidents demonstrate attackers' interest in disrupting public sector and critical infrastructure globally.
- **DDoS and Hacktivist Activity Targeting National Services:** The Netherlands experienced widespread DDoS disruptions affecting banks and government websites, reportedly by Russian hacktivist group NoName057(16). The volume and coordination of attacks against national digital infrastructure indicate increasing hacktivist-driven geopolitical activity.
- **Third-Party and Supply Chain Vulnerabilities Exposed:** Data breaches at Ascension (via a third-party vendor) and Verisource (exposing 4 million applicants) highlight third-party risk as a key attack vector. Organizations

relying on vendors for sensitive data processing must prioritize third-party security assessments to reduce exposure.

- **Telecommunications Data at Risk:** The breach of 40 million SK Telecom customers underscores the high-value target telecommunications companies represent. Large troves of subscriber data are being compromised, amplifying risks of fraud, identity theft, and downstream attacks leveraging exposed information.

Outlook:

This week's cyber events reinforce a growing convergence of credential theft, critical infrastructure disruption, and third-party exploitation as dominant attack themes. Attackers are shifting toward multi-pronged campaigns that combine social engineering, supply chain compromises, and exploitation of high-severity vulnerabilities to maximize impact. The prevalence of infostealer malware across unrelated sectors signals an expanding criminal economy focused on credentials as a primary commodity. Meanwhile, state-linked and hacktivist activity continues to erode trust in critical infrastructure and national systems. Looking ahead, organizations must prioritize patching critical vulnerabilities, strengthening API and supply chain defenses, and deploying proactive threat detection to navigate an increasingly multifaceted cyber threat landscape.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 210% [CVE-2024-45195](#)

- Direct Request ('Forced Browsing') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 18.12.16.

↑ 193% [CVE-2024-21893](#)

- A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.

↑ 73% [CVE-2024-9465](#)

- An SQL injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to reveal Expedition database contents, such as password hashes, usernames, device configurations, and device API keys. With this, attackers can also create and read arbitrary files on the Expedition system.

DDoS Attacks on the Rise

+DDoS

- DDoS attacks have risen 100% since 2024, with several attacks per month now reaching over 5 million requests per second (RPS), which previously happened only twice in all of 2024. Attacks primarily target Financial Services and Business sites, which collectively account for almost 50% of all DDoS attacks.

US-Based Financial Services Site Hit by Automated Attacks

+US +Financial Services +Bad Bots

- A US-based financial services site was targeted by a wave of automated attacks this week, surpassing 10 million requests over a span of just two days. Most of these attacks were driven by vulnerability scanning tools, originating primarily from within the US. The intensity of the attack highlights the growing trend of automated tools being used for reconnaissance and exploitation attempts on financial institutions.

Recent Cyber Threats

Lazarus Group Targets Gamers with Ageostealer Malware Masquerading as Gaming Company

+North Korea +Lazarus +Ageostealer +Infostealer malware

- The North Korea-linked [Lazarus Group](#) conducted a social engineering campaign targeting gamers by creating fake gaming company accounts on social media platforms and gaming forums. The fake accounts promoted "game giveaways" and offered free game cheats or hacks to lure gamers into downloading malware called Ageostealer. Ageostealer is an information stealing malware that is able to harvest login credentials from over 50 gaming platforms and services. By masquerading as legitimate gaming companies offering free games and cheats, the Lazarus Group was able to deceive gamers into infecting their own devices. This campaign shows how cyber threat actors leverage people's interests like gaming to trick them into downloading malware.

Airplay Vulnerabilities Allow iPhone and Mac Hacking Via WiFi

+MacOS +Airplay

- Researchers discovered vulnerabilities in Apple's [Airplay](#) technology that could allow attackers to hack nearby iPhones, iPads, and Macs by broadcasting malicious WiFi signals. The flaws affect devices running iOS 15.4 or macOS Monterey 12.3. By setting up a WiFi network with a specially crafted SSID name, attackers can exploit the Airplay implementation to gain remote code execution on victims' devices. The researchers demonstrated how a \$100 WiFi module could be used to create the malicious WiFi access point to exploit any Apple devices that have WiFi and Bluetooth enabled and are in proximity. Apple has patched the flaws in iOS 15.4.5 and macOS 12.4 updates.

Gremlin Infostealer Being Sold on Cybercrime Forums

+Gremlin +Russia +Infostealer Malware

- A new information stealing malware called [Gremlin](#) is being advertised and sold on Russian cybercrime forums. Gremlin is able to harvest credentials from browsers, cryptocurrency wallets, VPNs, messaging applications, and more. It is being sold for about \$100 and advertised as having enhanced capabilities for stealing browser cookies, history, passwords, crypto wallet keys, and VPN credentials. Gremlin is the latest example of increasingly sophisticated malware being developed and sold to cybercriminals to steal sensitive information from victims. Its wide collection of exfiltration capabilities makes it a dangerous new infostealer threat globally across many industries.

Zimbra Collaboration Platform Vulnerable to GraphQL API Account Takeover

+GraphQL +API

- Researchers disclosed a vulnerability in the GraphQL API of [Zimbra Collaboration](#) that could allow attackers to take over user accounts. By exploiting an authentication bypass, attackers could submit malicious GraphQL queries to edit user account information and reset account passwords. Successful exploitation of this flaw would give attackers full access and control over the compromised email accounts. The vulnerability highlights the security risks of improper access controls in GraphQL APIs, which can enable account takeover and data exfiltration if not properly secured.

Venom Spider APT Group Targets HR in More_eggs Malware Campaign

+Russia +Venom Spider +More_eggs +Infostealer Malware +Business

- Researchers uncovered a new campaign from the Russia-linked [Venom Spider APT](#) group targeting human resources and recruiting firms with a variant of the More_eggs malware. The emails contained job interview invitations laced with macros that installed the information-stealing malware if enabled. More_eggs is able to exfiltrate system information, files, and credentials from infected machines. By compromising HR and recruiting employees, Venom Spider appears to be attempting to infiltrate the networks of technology companies. The campaign highlights the risks of targeted phishing emails and how threat actors like Venom Spider are evolving techniques to breach corporate networks by going after soft targets like HR.

Critical SQL Injection Flaw Discovered in PHP ADODB Library

+SQL Injection +CVE +PHP

- Researchers disclosed a critical severity SQL injection vulnerability, tracked as [CVE-2025-46337](#), impacting the ADOdb PHP library for database abstraction. The flaw has a CVSS score of 10.0 and could enable remote code execution if exploited. The SQL injection issue is due to improper input sanitization in the library. This would allow attackers to inject malicious SQL queries and commands and takeover the database server. The ADOdb PHP library is used in many web applications and services for database connectivity. The high severity SQL injection flaw highlights the need to sanitize user-supplied input in order to prevent compromise from injection attacks.

Data Breaches

Conti Ransomware Gang Claims Attack on Malaysia's Kuala Lumpur Airport

[+Malaysia](#) [+Travel](#) [+Conti](#)

- The [Conti](#) ransomware gang claims to have hacked and encrypted systems at Malaysia's Kuala Lumpur International Airport. The group leaked data allegedly stolen from the airport on their dark web site after ransom negotiations failed. The impacted data includes security scans, terminal maps, and internal network information. The attack impacted display systems at the airport causing flight delays. This incident exemplifies the disruption ransomware can cause to critical infrastructure like transportation.

DDoS Attacks Disrupt Online Services in Netherlands

[+Netherlands](#) [+Russia](#) [+DDoS](#) [+NoName057\(16\)](#)

- A series of distributed denial-of-service (DDoS) attacks disrupted online services and websites in the [Netherlands](#) this week. The attacks flooded servers with junk traffic, causing outages at the tax authority, major banks, and other online services. This led to widespread disruptions for Dutch consumers and businesses. Although unconfirmed, several of the incidents have been publicly claimed by the Russian hacktivist group NoName057(16). The attacks in the Netherlands show how DDoS can be an effective disruptive tool, as many organizations still lack adequate mitigation. The outages highlight the need for DDoS protections and redundant infrastructure to maintain availability during volumetric attacks.

Cyber Incident Impacts Poland's PESEL Citizen Identification System

[+Poland](#) [+Government](#)

- An undisclosed cyber incident impacted [Poland's PESEL](#) citizen identification database system. PESEL contains personal data records on Polish citizens and foreign residents used for identification purposes. While authorities said no personal data was compromised, the system was taken offline to investigate the breach. The incident showcases cyber risks to critical government infrastructure like national identification systems which contain highly sensitive information. Breaches of such systems can enable identity theft and other fraud by exposing citizens' data.

Rhysida Ransomware Gang Claims Hack of Peru Government Networks

[+Peru](#) [+Government](#) [+Rhysida](#)

- The [Rhysida](#) ransomware gang claims to have breached and encrypted the networks of the Peru government. The group said it stole large amounts of data and demanded a ransom payment in return for a decryptor and to prevent leak of the stolen files. This attack impacted numerous government agencies and led to temporary shutdown of state online services. The incident exemplifies the risks ransomware poses to government networks, potentially disrupting vital services for civilians. Ransomware operators like Rhysida often leverage stolen data to pressure victims into paying extortion demands. Attacks on critical infrastructure demonstrate how ransomware has become a severe threat for governments globally.

Ascension Discloses Data Breach After Hacking of Third-Party Vendor

[+US](#) [+Healthcare](#) [+Third-Party](#)

- [Ascension](#), a large US health system, disclosed a data breach impacting patients after one of its third-party vendors suffered a cyberattack. The breach exposed protected health information like patient names, dates of birth, phone numbers, and medical record numbers. However, no Social Security numbers, financial data, or

diagnosis/treatment information was accessed. The incident highlights the risks associated with third-party vendors who can provide an avenue for attackers to access sensitive data. Healthcare providers often have little visibility or control over vendors' security posture. This breach of Ascension patient data via a hacked vendor shows the need for healthcare entities to ensure rigorous security assessments of all third-parties.

Data Breach at Verisource Exposes 4 Million Job Applicants

+Business +HR

- Background screening firm [Verisource](#) disclosed a data breach impacting 4 million job applicants after discovering unauthorized access to its systems. Exposed data included names, addresses, dates of birth, and Social Security numbers of applicants. The company provides background check and employment screening services. This breach highlights risks for sensitive personal information stored by HR service firms. Attackers often target such companies to access large troves of people's data for identity theft and other fraud. Though the method of attack is unknown, the Verisource breach again demonstrates the need to properly secure and encrypt highly sensitive data like SSNs and background check files.

SK Telecom Suspends New Subscribers After Data Breach

+South Korea +Telecommunications

- South Korean telecom provider [SK Telecom](#) halted onboarding new subscribers as it responds to a data breach impacting an estimated 40 million users. The company said both current and departed customers across its mobile, IPTV, and internet services had personal data exposed by unauthorized access. Information compromised included names, home addresses, phone numbers, and service subscription details. However, more sensitive data like financial information was not affected. The temporary signup suspension allows SK Telecom to investigate the breach's scope and prevent further damage as it comes under increased scrutiny. The large-scale compromise of telecom user records in South Korea underscores threats to telcos holding vast customer data.

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.