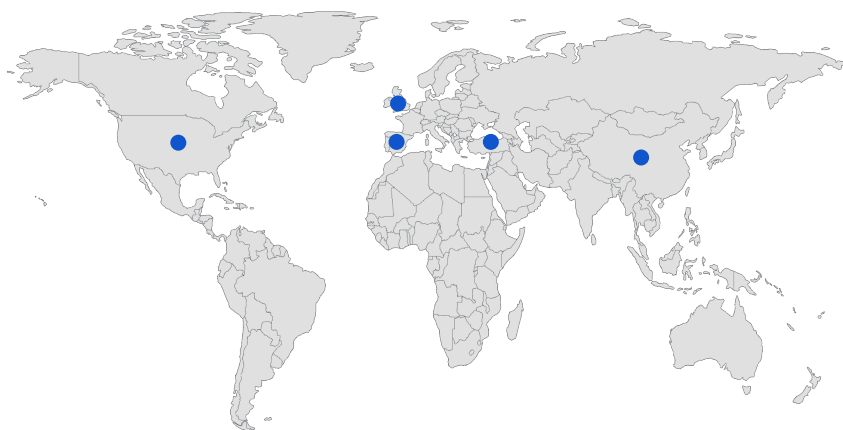


Threat Intel Report: April 21-27, 2025

Countries



Top Tags

SuperCard X

Gorilla

ELENOR-corp

Cloak

Interlock

Executive Summary

Actionable Information:

- **Healthcare Sector Under Siege:** The healthcare industry remains a prime target for cybercriminals, with multiple ransomware groups like Interlock and ELENOR-corp targeting healthcare organizations, including DaVita and Yale New Haven Health. This trend points to the increasing financial and operational risks associated with the theft of patient data and intellectual property.
- **Supply Chain Vulnerabilities:** The discovery of malicious PyPI packages and vulnerabilities in platforms like WordPress (InstaWP Connect plugin) and PyTorch emphasizes the need for heightened vigilance in securing open-source libraries and software ecosystems. These supply chain attacks have been particularly effective in delivering malware and enabling unauthorized access to sensitive systems.
- **NFC Relay Attacks and Mobile Malware:** The rise of SuperCard X and Gorilla malware, targeting Android devices and intercepting SMS for financial fraud, signals an increased risk to mobile users, particularly in banking and financial services. The malware's ability to exploit NFC technology and intercept OTPs highlights the vulnerabilities inherent in mobile ecosystems, especially through social engineering techniques.
- **Data Misuse and Privacy Concerns:** The data breach at Blue Shield of California, where sensitive health data was inadvertently shared with Google Ads, and the breach at Yale New Haven Health, involving exposed patient information, point to ongoing challenges in managing and securing personal data. Companies must prioritize data privacy and security protocols to prevent such leaks and mitigate reputational damage.

Outlook:

Looking ahead, the cyber threat landscape will likely continue to evolve with attackers increasingly focusing on leveraging social engineering techniques, exploiting misconfigurations, and targeting high-value sectors such as healthcare and finance. The expansion of ransomware groups targeting healthcare organizations, coupled with the

growth of malware-as-a-service platforms, presents a formidable challenge for defenders. As more organizations rely on cloud-based and AI-driven solutions, the potential for supply chain attacks and vulnerabilities in platforms like PyTorch and WordPress will only increase. Therefore, robust security hygiene, continuous monitoring, and timely patch management are essential to mitigate these risks.

Moreover, as data privacy issues continue to dominate headlines, regulations around data protection will likely become stricter, requiring organizations to improve their compliance efforts. With data breaches becoming more frequent and widespread, it is crucial for organizations to adopt a zero-trust security model and enhance their ability to detect and respond to attacks in real time. As mobile malware evolves, users should be increasingly cautious about the apps they install and the permissions they grant, while organizations should invest in advanced endpoint security solutions.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 48% [CVE-2024-20767](#)

- ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could leverage this vulnerability to access or modify restricted files.

↑ 25% [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.

↑ 24% [CVE-2024-3400](#)

- A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

Turkish Retail Site Attacked by 10.5M RPS DDoS Attack

+Turkey +Retail +DDoS

- A 10.5 million requests per second (RPS) application-layer DDoS attack targeted a Turkish retail site. In just nine minutes, attackers used 6,486 IP addresses to reach over 10 million RPS and attempt to disrupt luxury retail sales.

US Lifestyle Site Hit by Two-Day ATO Attack

+US +Lifestyle +ATO

- A US lifestyle site was targeted in a two-day account takeover (ATO) attack, reaching a total of 5 million requests over two days. The attacks were entirely brute-force, and came from locally-based IPs.

Recent Cyber Threats

PyPI Packages Exploit Telegram Sessions for Dark Web Sale

+PyPI +Python +Telegram +Supply Chain

- Three malicious Python packages—Quicolor, QuickColors, and ColorYi—were discovered on [PyPI](#), masquerading as legitimate color formatting libraries. These packages exfiltrate Telegram Desktop's tdata folder, enabling attackers to hijack Telegram sessions without reauthentication. The stolen session data is sold on dark marketplaces, facilitating unauthorized access to user accounts.

Chinese Cybercriminals Target U.S. and U.K. Healthcare and Manufacturing Sectors

[+China](#) [+US](#) [+UK](#) [+Healthcare](#) [+Manufacturing](#) [+Phishing](#)

- [Chinese-speaking threat actors](#) have targeted hospitals and factories in the U.S. and U.K., exfiltrating sensitive data. These financially motivated cybercriminals employ various tactics, including phishing and exploiting vulnerabilities, to gain unauthorized access to critical systems. The attacks aim to steal valuable intellectual property and disrupt operations.

SuperCard X Malware Facilitates NFC Relay Attacks on Android Devices

[+SuperCard X](#) [+Malware](#) [+Android](#)

- The [SuperCard X](#) malware-as-a-service platform targets Android devices, enabling NFC relay attacks that facilitate fraudulent ATM and point-of-sale transactions. Victims are tricked into installing malicious apps through social engineering, leading to unauthorized access to their payment card data.

Marks & Spencer Halts Online Orders Amid Cyberattack

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

- [Marks & Spencer](#) suspended all online orders following a significant cyberattack that began over the Easter weekend. The retailer experienced disruptions in online and app-based services, including contactless payments and click-and-collect orders, leading to financial losses and operational challenges. The company is working with cybersecurity experts to investigate the incident.

PyTorch Vulnerability Enables Remote Code Execution

[+Python](#) [+RCE](#) [+AI](#)

- A critical vulnerability (CVE-2025-32434) has been identified in [PyTorch](#) versions up to and including 2.5.1. The flaw exists in the torch.load() function when using the weights_only=True parameter, allowing attackers to execute arbitrary code during model deserialization. This poses significant risks, including data breaches and system compromise, particularly in cloud-hosted AI environments. The issue has been addressed in PyTorch version 2.6.0.

Gorilla Android Malware Intercepts SMS to Steal OTPs

[+Gorilla](#) [+Malware](#) [+Android](#) [+Financial Services](#)

- A sophisticated Android malware strain named [Gorilla](#) has emerged, designed to intercept SMS messages containing one-time passwords (OTPs). Operating stealthily in the background, it exploits Android's permission system to access sensitive information on infected devices. The malware primarily targets banking customers and users of services like Yandex, categorizing stolen SMS messages for easier exploitation. It establishes a persistent connection to its command and control infrastructure using WebSocket protocols, allowing real-time data exfiltration.

Cybercriminals Exploit Google OAuth Loophole to Evade Gmail Security

[+Phishing](#) [+Session Hijacking](#)

- Cybercriminals have exploited a loophole in Google's [OAuth](#) infrastructure to bypass Gmail's security measures. By manipulating OAuth tokens, they can send phishing emails that appear legitimate, tricking users into revealing their credentials. This attack highlights significant concerns about the security of Gmail users worldwide.

Vulnerability in InstaWP Connect Plugin Allows Arbitrary File Inclusion

[+WordPress](#) [+CVE](#) [+LFI](#)

- A critical vulnerability has been discovered in the [InstaWP](#) Connect plugin for WordPress, affecting versions up to and including 0.1.0.85. The flaw allows unauthenticated attackers to include and execute arbitrary files on the server via the 'instawp-database-manager' parameter. This could lead to remote code execution and compromise the affected WordPress site.

ELENOR-corp Ransomware Targets Healthcare Sector

[+ELENOR-corp](#) [+Mimic](#) [+Ransomware](#) [+Healthcare](#)

- The [ELENOR-corp](#) ransomware, a new variant of the Mimic ransomware, is targeting healthcare organizations. It features advanced capabilities, including data theft and anti-analysis techniques. This poses significant risks to healthcare providers, potentially compromising patient data and disrupting services.

Data Breaches

Blue Shield of California Exposed Health Data of 4.7 Million Members to Google

[+US](#) [+Healthcare](#)

- [Blue Shield of California](#) disclosed a data breach affecting 4.7 million members, where private health data was inadvertently shared with Google Ads due to a misconfiguration in Google Analytics. The data, tracked between April 2021 and January 2024, included sensitive information such as family size, gender, ZIP code, insurance plan type, medical claims, and search queries for healthcare providers. This information may have been used by Google for targeted advertisements, despite Google policy prohibiting the collection of private health data. Blue Shield clarified that this was not the result of malicious hacking, and no Social Security numbers, financial data, or driver's license details were compromised.

Baltimore City Public Schools Data Breach Affects Over 31,000 People

[+US](#) [+Education](#) [+Cloak](#) [+Ransomware](#)

- On February 13, 2025, [Baltimore City Public Schools](#) experienced a cybersecurity incident affecting certain IT systems within their network. The breach resulted in the exposure of sensitive personal information, including Social Security numbers, passport details, birth certificates, and other data that could be used to steal someone's identity. The criminal group known as Cloak Ransomware is suspected to be responsible for the attack.

Data Breach at Connecticut's Yale New Haven Health Affects Over 5 Million

[+US](#) [+Healthcare](#)

- [Yale New Haven Health](#), Connecticut's largest healthcare system, experienced a data breach on March 8, 2025, compromising the personal information of approximately 5.6 million patients. The breach involved unauthorized access to a network server, exposing demographic data such as names, dates of birth, contact details, race or ethnicity, and medical record numbers. Notably, Social Security numbers, financial records, and sensitive medical data were not affected. The breach has already resulted in two federal lawsuits, alleging negligence in data protection practices. The scale of the breach surpasses all patient visits across the system in 2023.

Interlock Ransomware Gang Claims DaVita Attack, Leaks Stolen Data

[+US](#) [+Healthcare](#) [+Interlock](#) [+Ransomware](#)

- The Interlock ransomware gang has claimed responsibility for a cyberattack on [DaVita](#), a leading U.S. dialysis service provider. The attackers allege to have stolen 1.51 terabytes of data from DaVita's systems. The leaked data includes sensitive information, though specific details have not been disclosed.

Cyberattack Disrupts Water Supplier in Mataró, Spain

[+Spain](#) [+Utilities](#)

- [Aigües de Mataró](#), a Spanish water supplier, suffered a cyberattack affecting its corporate systems and website. While water supply and quality control remained unaffected, personal and financial data of customers may have been exposed, leading to potential phishing risks.

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.