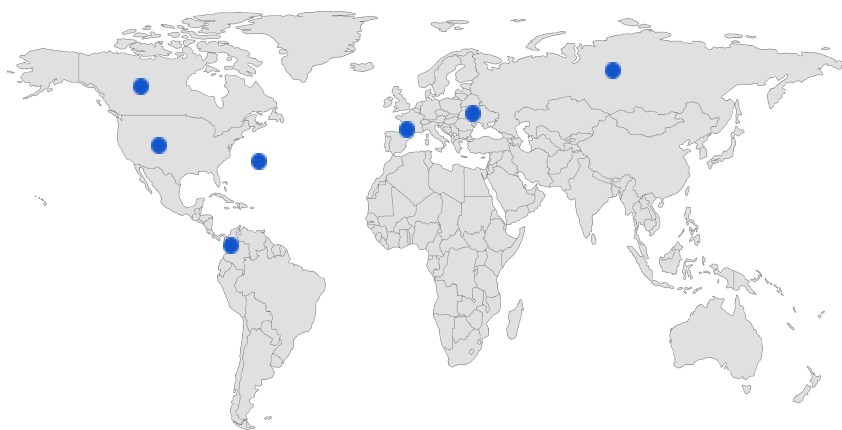


Threat Intel Report: September 18-24

Countries



Top Tags

Phantom Ghost

Clop

USDoD

NoName05716

Hacktivism

Executive Summary

Actionable Information:

- **Patch Management:** A series of vulnerabilities have been identified in products from major tech companies such as Fortinet and Juniper. Immediate patching is crucial to prevent potential exploits. Fortinet's XSS vulnerability in FortiOS and FortiProxy products and Juniper's RCE flaw in their devices stand out as particularly concerning.
- **Malware Vigilance:** There's a rising trend in malware distribution through deceptive means. Notably, cybercriminals are using a fake proof-of-concept for a vulnerability to distribute VenomRAT malware. Additionally, a malicious Python package named "colourama" has been identified, which covertly mines cryptocurrency on the victim's machine.
- **Phishing Awareness:** A targeted phishing campaign has been identified, specifically targeting Chinese-speaking users, distributing the new ValleyRAT malware. Regular training and awareness campaigns for employees can mitigate the risks associated with such targeted phishing attempts.
- **Data Management and Configuration:** Several significant data breaches have occurred due to misconfigurations and glitches. Microsoft's exposure of 38TB of data due to a misconfigured Azure storage and T-Mobile's app glitch are prime examples. Organizations must review and ensure that their data storage and management configurations are secure.

Outlook:

The cyber landscape this week highlights the importance of proactive patch management, with major companies releasing patches for critical vulnerabilities. The trend of exploiting trust, either through fake proofs-of-concept or typo-squatted software packages, underscores the evolving tactics of cybercriminals. Data breaches due to misconfigurations emphasize the need for rigorous configuration audits and reviews. Lastly, the geopolitical landscape



continues to influence cyberattacks, as seen with the DDoS attacks on Canadian airports, reportedly in response to Canada's support for Ukraine.

Organizations must remain vigilant, continuously monitor for threats, and prioritize cybersecurity awareness and training.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

📈 33% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

📈 13% [CVE-2022-22965](#)

- a RCE vulnerability in Spring programs ("Spring4Shell")

📈 45% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

Ukrainian site targeted in Russian hacktivism

+Ukraine +Gaming +Russia +Hacktivism

- This week, a Ukrainian gaming-related site was hit by application-layer DDoS reaching almost 3M requests per second (RPS) in 2 hours. The attack came from over 11K mainly Russian IP and coincides with the site raising funds to donate to the Ukrainian war effort, so the attack was almost certainly hacktivism.

Three attacks this month on US computing site, all from same attacker

+US +Computing +Path Traversal

- A US-based computing company was targeted this week by path traversal. This is the third attack this month on a site that has not frequently been targeted previously, and all attacks have come from the same online-hosted IP address.

Recent Cyber Threats

Patches released for Fortinet XSS vulnerability

+XSS +CVE

- [Fortinet](#) has released patches for a high-severity cross-site scripting (XSS) vulnerability found in its FortiOS and FortiProxy products. This vulnerability could allow attackers to execute arbitrary code, gain unauthorized access, or launch denial-of-service attacks. Users are urged to apply the patches immediately.

Imperva customers are protected out-of-the-box against CVE-2023-29183.

RCE vulnerability in Juniper devices patched

+RCE +CVE

- Thousands of [Juniper Networks](#) devices are vulnerable to a critical unauthenticated remote code execution (RCE) flaw. The vulnerability, which chains two lower-criticality vulnerabilities, can be exploited by sending a specially crafted request to the affected device. Juniper has released patches, and users are advised to update their devices promptly.

Imperva customers are protected out-of-the-box against CVE-2023-36845.

Fake PoC used to deliver malware

+Malware

- Cybercriminals are using a fake [proof-of-concept](#) (PoC) for the vulnerability CVE-2023-40477 to distribute the VenomRAT malware. The malware is delivered via malicious Microsoft Word documents that claim to contain details about the supposed vulnerability.

Crypto mining package delivered via GitHub

+Crypto

- A malicious Python package named "[colourama](#)" has been discovered, which stealthily performs cryptocurrency mining on the victim's machine. The package, a typo-squatted version of the legitimate "colorama" package, has been downloaded over 12,000 times.

ValleyRAT malware targets Chinese speakers

+Malware +Phishing

- A phishing campaign targeting [Chinese-speaking users](#) has been distributing the new ValleyRAT malware alongside Sainbox RAT and Purple Fox malware. The campaign uses invoice-themed email lures, and has been active since early 2023.

Data Breaches

Colombian government ministries targeted by Phantom Ghost

+Colombia +Government +Phantom Ghost +Ransomware

- [Colombia's](#) government ministries faced a cyberattack that disrupted their operations. The attack was attributed to the hacking group "Phantom Ghost," which claimed responsibility and demanded a ransom in exchange for not leaking sensitive information.

NC hospital breached linked to Clop MOVEit campaign

+US +Healthcare +Clop +MOVEit

- A series of cyber thefts at major [North Carolina hospitals](#) have been attributed to the Clop gang. The gang reportedly exploited a zero-day vulnerability in the MOVEit Transfer platform as part of their ongoing MOVEit campaign, which allowed the gang to steal personal data from several hospitals and healthcare providers.

TransUnion data released by hacker known as USDoD

+USDoD +Financial Services

- Threat actor "[USDoD](#)" recently exposed 3GB of data allegedly stolen from credit reporting agency TransUnion. The data contains the personal information of over 58K people globally, and goes back over a year.

Microsoft exposed 3 years worth of data via misconfigured Azure storage

+Computing & IT

- [Microsoft](#) inadvertently exposed a vast amount of sensitive internal data spanning over three years through a public GitHub repository associated with Microsoft's AI research division. Although intended for open-source code and AI image recognition models, the Azure storage was misconfigured, leading to the exposure of 38TB of data including Microsoft employees' personal computer backups, passwords to Microsoft services, secret keys, and over 30K internal Microsoft Teams messages.

T-Mobile glitch shows other people's account information

+Computing & IT

- A glitch in [T-Mobile's](#) app allowed users to view other people's account information, including customers' names, phone numbers, addresses, account balances, and credit card details. T-Mobile has confirmed the glitch was not due to any external attack, and claims it affected less than 100 customers.

Canadian airports targeted by DDoS attacks

+Canada +Transportation +NoName05716

- The [Canada Border Services Agency](#) (CBSA) confirmed that a distributed denial of service (DDoS) attack caused widespread service disruptions at several Canadian airports. The Russian hacking group NoName05716 claimed responsibility for cyberattacks targeting several Canadian organizations, including CBSA, reportedly in response to Canada's support for Ukraine.

French industrial company exposes environment file

+France +Manufacturing

- [Exail Technologies](#), a French industrial group, inadvertently exposed an environment file containing database credentials. Although the database itself wasn't publicly accessible, the exposure could have allowed attackers to access, modify, or delete sensitive data if they were able to leverage the stolen credentials.

Bermudan government attack attributed to Russian attackers

+Bermuda +Government

- The government of [Bermuda](#) experienced a cyberattack that affected all its departments' IT systems, and has attributed the attack to hackers based in Russia. While the attack disrupted internet, email, and phone services, Premier David Burt stated in a press conference that initial investigations have not found evidence of data theft.

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.



By Phone:
650-345-9000



By Fax:
888-611-7282

By mail:

Imperva Headquarters
One Curiosity Way, Suite
203 San Mateo, CA 94403