

Threat Intel Report: May 29-June 5

Countries



Top Tags

Healthcare

Retail

Automotive

Financial

Travel

Recent Cyber Threats

MoveIt file transfer vulnerability causes massive hack

+SQL injection +CVE

- A recent vulnerability in the MoveIt transfer service ([CVE-2023-34362](#)) has wide-reaching implications. This SQL injection vulnerability could allow an unauthenticated attacker to gain unauthorized access to MOVEit Transfer's database. This vulnerability was promptly exploited by potentially Russian threat actors in hacks on multiple large organizations, and as of May 31, there are 2,500 vulnerable MoveIt instances exposed to the internet.

Imperva Cloud WAF protects against critical vulnerabilities, including this one.

Spyware on Google Play store downloaded 450M times

+Malware +SpinOk

- [SpinOk](#) malware has been found in Google Play apps with over 450M collective downloads. This malware uses minigames to grab interest, and runs spyware in the background to steal personal information.

\$35M in crypto stolen from Atomic Wallet users

+Crypto Theft

- [Atomic Wallet](#) is investigating thefts of over \$35M in crypto in early June. The company is investigating the source of the issue, but took their download server offline in case it's a software breach.

Russia alleges US intelligence hacked iPhones

+Russia +US +CE

- A Russian cybersecurity firm claims US intelligence agencies hacked iPhones beginning in 2019, using an iMessage exploit to perform remote code execution. Apple claims they were not involved in any backdoor creation.

Anonymous Sudan claims responsibility for a Microsoft outage

+Anonymous Sudan

- [Anonymous Sudan](#) claimed responsibility for a Microsoft outage that took the web-based Microsoft 365 site down for a few hours. Anonymous Sudan claims this is the beginning of a targeted campaign against US infrastructure, in retaliation for US State Department comments on Sudan.

Data Breaches

Burton snowboards alerts customers of data stolen in data breach

+US +Retail

- [Burton Snowboards](#) recently alerted customers of a February data breach, which may have stolen SSNs and financial account information. The incident occurred in early February, forcing the company to cancel orders amid what was reported as a system outage.

Harvard Pilgrim Health Care data breach affects 2.5M customers

+US +Healthcare

- [Harvard Pilgrim Health Care](#) (HPHC) recently disclosed a data breach in April that exposed over 2.5M customer records. The attackers maintained access to HPHC records for almost a month before the breach was discovered. The files stolen contained personal information, including SSNs, taxpayer records, and healthcare information.

Additional misconfigured Toyota servers exposed customer data

+Japan +Australia +Automotive

- Two more misconfigured [Toyota](#) servers have been discovered, as part of an investigation following servers discovered earlier this year that leaked user location data for almost a decade. The new servers exposed the personal information of Toyota customers in Asia and Australia between 2016 and 2023.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

⬆ 20% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

⬆ 12% [CVE-2022-22965](#)

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

⬇ 25% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

Nigerian financial site targeted with path traversal

+Nigeria +Financial

- This week, a Nigerian financial site was targeted twice with path traversal attacks. Attacks came mainly from US-based IPs, and reached a total of almost 8M requests. Attackers used 5500 distinct IPs, which had an average risk score of 40%.

Mexican travel API suffered API violations

[+Mexico](#) [+Travel](#)

- A Mexican travel API site was targeted on June 1 with API violations reaching 6.5M requests. The attacks collectively came from 313K IPs, mostly based in Mexico.

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