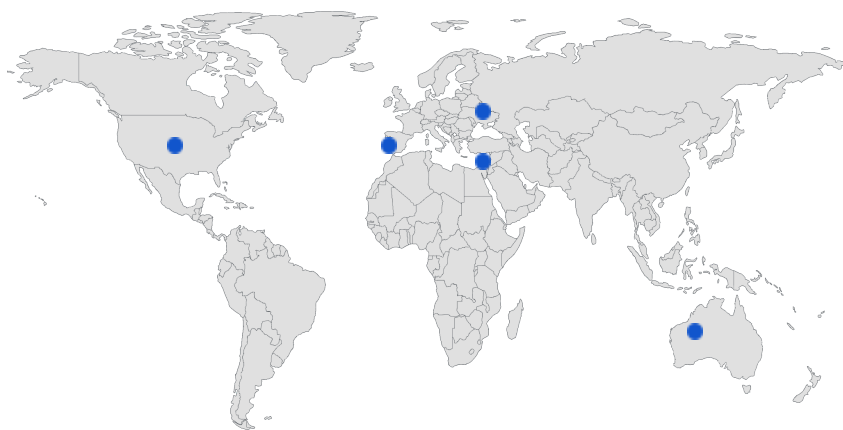


Threat Intel Report: September 5-10

Countries



Top Tags

ALPHV

LockBit

Ragnar Locker

APT28

Executive Summary

Actionable Information:

- Update any Apple devices to protect against attacks from the dangerous Pegasus spyware.
- Organizations, especially those in the financial and retail sectors, should bolster their API security measures and regularly monitor for unusual activity.
- Ensure systems are updated and patched against the latest known vulnerabilities.
- Implement robust cybersecurity training for employees to recognize and report potential phishing attempts and other malicious activities.
- Engage in continuous monitoring and threat intelligence to stay ahead of emerging threats and adapt security postures accordingly.

Outlook:

The cyber landscape remains volatile, with attackers continuously evolving their tactics. As threats become more sophisticated, organizations must stay vigilant, investing in advanced security measures and fostering a culture of cybersecurity awareness. The collaboration between industries and cybersecurity firms will be pivotal in countering future threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

📈 14% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

📈 54% [CVE-2022-22965](#)

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

📈 7% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

DDoS attack targets web-hosting site

+Computing & IT

- On September 6, a web-hosting site was targeted by network-layer DDoS, which reached a peak of 377 GBPS. This site is frequently targeted by DDoS, and this attack is the sixth-highest attack the site has seen this year.

Grocery store suffers API violation attacks

+US +Retail

- A US-based grocery store experienced API violations much higher than usual for three days this week. The attacks, which can potentially expose sensitive customer data or disrupt online services, came primarily from US-based IPs.

Recent Cyber Threats

Graphic design programs exploited for crypto mining

+Crypto mining

- Cybercriminals are utilizing weaponized Windows installers to target [graphic designers](#), likely because they use computers with powerful graphics cards and GPUs. The malicious installers, hidden in legitimate installers for programs like Adobe Illustrator, Autodesk 3ds Max, and SketchUp Pro, are then used to mine cryptocurrency.

Apple fixes dangerous zero-days

+CVE +Pegasus +NSO Group

- Apple has released emergency updates to address two zero-day vulnerabilities that have been exploited to deliver NSO Group's [Pegasus](#) spyware. This spyware is extremely dangerous, with the ability to deploy the malware without any interaction from the victim.

Pandora botnet hijacks Android home devices

+Pandora +IOT

- A new variant of the Mirai botnet, named '[Pandora](#)', has been discovered hijacking Android-based Internet of Things (IoT) devices. The compromises likely come from malicious firmware updates or installing apps to watch pirated video content.

Eight vulnerabilities found in Cisco IOT platforms

+CVE +IOT

- [Cisco](#) identified eight security vulnerabilities in the Open Automation Software (OAS) Industrial IoT data platform. These vulnerabilities could potentially allow attackers to execute arbitrary code or disrupt the normal operations of the platform.

BlueShell malware targets computers to steal information

+BlueShell

- A new malware strain named [BlueShell](#) has been detected targeting Windows, Linux, and Mac systems. This cross-platform malware is designed to steal information and execute malicious commands on the infected systems.

Data Breaches

Israeli hospital data leaked by ransomware group

[+Israel](#) [+Healthcare](#) [+Ragnar Locker](#)

- The Ragnar Locker ransomware group claimed responsibility for a cyberattack on [Mayanei Hayeshua Medical Center](#) in Tel Aviv, subsequently leaking patient data online. The group claims that the requested ransom was not paid within a month, leading to the leaked data. The affected data potentially includes top politicians, government officials, and religious leaders.

Hotel booking platform found exploited for financial gain

[+Travel](#)

- Multiple vulnerabilities were discovered and exploited in a [hotel booking platform](#), though the threat actor has not been identified, although researchers believe it's part of a larger coordinated effort for financial gain.

Patient data compromised in J&J breach

[+Healthcare](#)

- A data breach has been reported at a [Johnson & Johnson](#) subsidiary, where patient data was compromised. Although the incident has not been fully investigated, it could affect the data of up to 1.6M patients.

LockBit takes down Spanish networks

[+Spain](#) [+LockBit](#)

- The LockBit ransomware group launched a cyberattack that disrupted networks across [Seville](#), Spain. Local authorities and cybersecurity teams are actively working to restore the affected systems, but they claim they will not pay the \$1.5M ransom.

Sabre compromised by Dunghill Leaks gang

[+Travel](#) [+Dunghill Leaks](#)

- The Dunghill Leaks ransomware gang claimed responsibility for a data breach at [Sabre](#), a major travel technology company. The group claims to have 1.3TB of data, and the company is working to verify the claims.

Dental service compromise impacts up to 130K pediatric patients

[+Healthcare](#)

- [Just Kids Dental](#) reported a cyberattack that potentially impacted around 130,000 individuals. The dental service is reaching out to affected parties and seems to have paid the ransom in exchange for the deletion of compromised data.

Dating app targeted in destructive cyberattack

[+Adult](#)

- The dating app [Coffee Meets Bagel](#) experienced an outage, which they attributed to a destructive cyberattack. The company has not yet confirmed whether this was a ransomware attack, but did say that attackers purposely deleted data.

Ukraine CERT counters APT28 attack

[+Ukraine](#) [+Government](#) [+APT28](#)

- Ukraine's [Computer Emergency Response Team \(CERT\)](#) claims to have countered an intrusion attempt by the APT28 hacking group. The intrusion started with a phishing email containing a link to a malicious ZIP archive, which, when clicked, activates the infection chain.

\$40M stolen from online casino

+Gambling +Cryptocurrency

- The online cryptocurrency casino, [Stake.com](#), reported a heist in which approximately \$40 million was stolen. The attackers stole funds from Ethereum and Binance Smart Chain hot wallets, and all other wallets seem to be untouched.

Australian pathology clinic compromised in possible ALPHV attack

+Australia +Healthcare +ALPHV

- Melbourne-based pathology clinic, [TissuPath](#), suffered a cyberattack, leading to a breach of patient data. The breach may have stolen up to ten years' worth of pathology referral letters, which include patient information. The attack has been linked on the darkweb to attack group ALPHV, but the company has not yet publicly attributed the attack.

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