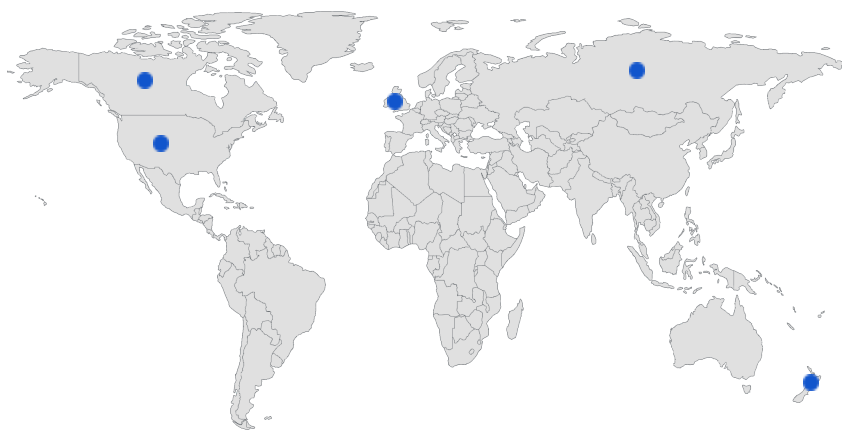


Threat Intel Report: September 11-17

Countries



Top Tags

Pegasus

ALPHV

Bian Lian

NoEscape

Scattered Spider

Executive Summary

Actionable Information:

- Organizations using the 'ncurses' library in Unix-based systems should immediately apply the update provided by Microsoft to address the vulnerabilities known as CVE-2023-29491.
- Companies should be wary of the misuse of Extended Validation (EV) certificates by malware and implement measures to detect and counteract spear-phishing campaigns.
- Users of N-able's "Take Control" agent should apply patches to protect against the vulnerability CVE-2023-27470, which could allow arbitrary code execution on Windows systems.
- Adobe PDF Reader users should promptly update their software to protect against the zero-day vulnerability CVE-2023-26369.
- Developers and organizations using GitHub should be aware of the potential for Repojecting and take steps to secure their repositories against unauthorized access.

Outlook:

The recent surge in cyberattacks underscores the evolving nature of cyber threats. With attackers employing a range of sophisticated techniques, from ransomware to spear-phishing, organizations must remain proactive in updating and patching their systems. Continuous cybersecurity training for employees and collaboration between industries and cybersecurity firms will be crucial in navigating this challenging landscape. As cybercriminals continue to target various sectors, from transportation to finance, a unified and informed approach to cybersecurity will be essential in mitigating risks.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 15% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

↓ 47% [CVE-2022-22965](#)

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

↓ 13% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

Largest application DDoS attack of 2023 targets financial site

+DDoS +Financial Services

- This week, a financial services site was targeted in an application-layer DDoS attack that reached almost 5M RPS in less than two hours. This attack is now the largest application-layer DDoS attack Imperva has seen this year, shattering the previous 3M RPS record, which was set just weeks ago. This attack came from just 845 IPs, of which the majority were based in Brazil and Mexico.

US computing site attacked by path traversal

+US +Computing +Path Traversal

- A US-based computing site was targeted with path traversal attacks this week that reached almost 3M attack attempts. The site is not frequently targeted by attackers, so this is unique, and likely a pinpointed attack.

Recent Cyber Threats

MGM cyberattack claimed by Scattered Spider

+Scattered Spider +Gambling +US +ALPHV

- [MGM Resorts](#) experienced a cyberattack, leading them to shut down their IT systems as a precautionary measure. The ransomware group Scattered Spider has claimed responsibility for the attack, and allegedly used ALPHV malware to conduct the attack after conducting a social engineering attack to get in.

Microsoft discloses vulnerabilities in ncurses library

+CVE

- Microsoft discovered vulnerabilities in the 'ncurses' library, which is widely used in Unix-based systems, potentially affecting numerous applications. The vulnerabilities, collectively tracked as [CVE-2023-29491](#), have been addressed in a recent update.

Stealer malwares misuse extended validation certificates

+Malware

- [RedLine and Vidar](#) stealers have been found to misuse Extended Validation (EV) certificates to deploy ransomware, enhancing their credibility and success rate in spear-phishing campaigns.

N-able vulnerability could delete Windows files

+CVE

- N-able's "Take Control" agent, a remote management tool, was found to have vulnerabilities that could allow attackers to execute arbitrary code. Tracked as [CVE-2023-27470](#), the issue relates to a Time-of-Check to Time-of-Use (TOCTOU) race condition vulnerability, which, when successfully exploited, could delete arbitrary files on a Windows system.

WebEx users targeted in malvertising campaign

[+BatLoader](#) [+Malware](#)

- A malvertising campaign has been targeting [WebEx](#) users, dropping a malware named "BatLoader" onto their systems. The malware is distributed via a fake WebEx ad that looks incredibly realistic.

Russian journalist infected with Pegasus malware

[+NSO Group](#) [+Pegasus](#) [+Russia](#) [+News](#)

- The CEO of [Meduza](#), a Russian news outlet critical of the Kremlin, was reportedly targeted with the notorious Pegasus spyware. The spyware was installed when the CEO was in Berlin, and this is the first known incident of a Russian citizen infected with NSO Group's Pegasus malware.

New 3AM ransomware used as LockBit backup

[+LockBit](#) [+3AM](#)

- A new ransomware named "[3AM](#)" has been identified. This ransomware was used as an alternative by attackers when their attempt to deploy LockBit ransomware was thwarted.

PDF reader vulnerability can lead to code execution

[+CVE](#) [+Remote Code Execution](#)

- Adobe has identified a critical zero-day vulnerability in its PDF Reader, which is currently being exploited in the wild. The vulnerability, tracked as [CVE-2023-26369](#), can be used to launch code execution attacks.

GitHub exploit could conduct repojacking attack

[+Repojacking](#)

- A new exploit could allow an attacker to exploit a race condition within [GitHub's](#) repository creation and username renaming operations. This technique could be used to perform a Repojacking attack, or hijacking popular repositories to distribute malicious code.

Wiki-Eve attack technique can steal passwords over Wi-Fi

[+BFI](#)

- A new attack technique named "Wiki-Eve" has been discovered, which can steal numerical passwords over Wi-Fi networks at an accuracy rate of over 90%. Wiki-Eve exploits BFI (beamforming feedback information), which allows devices to send feedback about their position to routers so they can direct their signal more accurately. The information contains data in cleartext form, meaning that this data can be intercepted and used without requiring hardware hacking or cracking an encryption key.

Data Breaches

Anonymous Sudan targets Telegram

[+Anonymous Sudan](#)

- Anonymous Sudan launched a DDoS attack on [Telegram](#) in retaliation to the site suspending their account. Although the reason for the original ban is unknown, the group has since started a new page.

Mississippi community college attack under FBI investigation

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

- [Hinds Community College](#) in Mississippi suffered a cyberattack, prompting an investigation by the FBI. The attack led to a complete shutdown of the college's systems.

New Zealand transportation system targeted by ransomware

+New Zealand +Transportation

- [Auckland Transport's](#) HOP system in New Zealand was impacted by a suspected ransomware attack. The incident affected commuter's payment cards, and the transportation agency confirmed that it seemed to be isolated, and does not affect travel.

UK police bureau compromised in third-party breach

+UK +Government

- A ransomware attack on a third-party supplier led to data compromise for the [Greater Manchester Police](#) in Britain. Although financial data was not affected, there are concerns over undercover officers' data being included.

US-Canada water commission attacked by NoEscape

+NoEscape +US +Canada +Government

- The NoEscape ransomware group has claimed an attack on the [International Joint Commission](#), which manages water systems on the border of the US and Canada. The group claims to have stolen 80GB of data containing 50K confidential files.

Airbus data exposed after IT account hacked

+Transportation

- [Airbus](#) experienced a data leak after an attacker accessed its internal web portal via a Turkish IT account. The breach has exposed sensitive information, including the information of over 3K Airbus vendors.

Auto sites compromised in VIN-harvesting spree

+Automotive

- Several [automaker](#) sites were compromised by cybercriminals who used bots to harvest Vehicle Identification Numbers (VINs) and information about the owner of the car. Over 15K accounts are currently for sale, at about \$2 each.

\$27M stolen in suspected crypto hack

+Crypto

- [CoinEx](#), a cryptocurrency exchange, is suspected of being hacked after \$27M in crypto was transferred to an unknown wallet with no transaction history. The incident is still under investigation.

Save the Children data stolen by Bian Lian

+Bian Lian

- The charity [Save the Children](#) was targeted by the Bian Lian ransomware group. The group claims to have stolen 6.8TB of data, including financial, personal, and medical information.

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