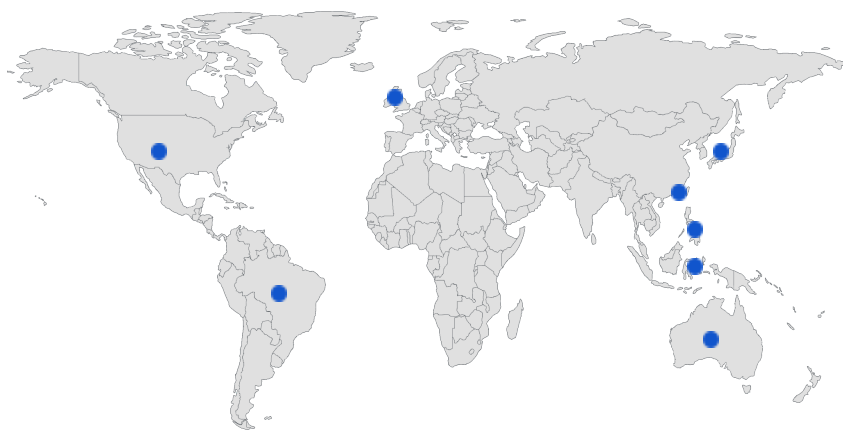


Threat Intel Report: June 26 - July 4

Countries



Top Tags

ALPHV

Ransomware

CI0p

Anonymous Sudan

MOVEit

Recent Cyber Threats

Node.js registry susceptible to manifest confusion attack

+Manifest Confusion

- A [Node.js](#) registry is susceptible to a manifest confusion attack that could allow threat actors to conceal malware in project dependencies or perform arbitrary script execution. Manifest and package metadata are never cross referenced, leading to unexpected behavior when they don't match.

DDoSia threat actors update malware for broader audience

+DDoSia +Malware

- The threat actors behind the [DDoSia](#) attack tool have created a new version that conceals the list of targets, showing that the tool is actively maintained by operators. They're also attempting to make the malware compatible with multiple operating systems, in an attempt to market to a broader audience.

RedEnergy ransomware group targets Brazil, Philippines

+RedEnergy +Energy +Telecom +Machinery +Brazil +Philippines

- A ransomware group known as [RedEnergy](#) has been targeting energy, telecom, and machinery sites in Brazil and the Philippines via LinkedIn pages. The goal appears to be data theft and encryption, as the attackers exfiltrate sensitive information and charge users to recover encrypted data.

WordPress plugin vulnerable to compromise

+WordPress +Plugin exploitation

- The Ultimate Member [WordPress](#) plugin is being exploited by attackers to compromise sites. The vulnerability allows attackers to bypass security measures and register fake admin accounts, and is tracked as CVE-2023-3460.

Data Breaches

Anonymous Sudan claims to have 30M Microsoft customer accounts

[+Anonymous Sudan](#) [+DDoS](#)

- [Anonymous Sudan](#) claims to have stolen 30M customer accounts in their attack on Microsoft's servers, and are asking \$50,000 USD for the full database. Microsoft denies these claims, and says the data is an aggregation of older data from a third-party breach.

Taiwan Semiconductor Manufacturing Company denies LockBit attack

[+Taiwan](#) [+LockBit](#) [+Ransomware](#) [+Computing](#)

- Taiwan Semiconductor Manufacturing Company ([TSMC](#)) denies a recent LockBit ransomware attack, which claimed to have access to various internal systems. Lockbit is demanding \$70M for the stolen data, but TSMC claims the attack actually affected an IT supplier and doesn't affect any internal functions.

Port of Nagoya operations shut down by ransomware attack

[+Japan](#) [+Ransomware](#)

- The Port of [Nagoya](#), the largest and busiest port in Japan, has been targeted in a ransomware attack that currently impacts the operation of container terminals. The port administrative authority is meeting with police to remedy the problem, and no further information is currently available about the attack. So far, this seems to be the largest attack the port has dealt with.

Nickelodeon animation data leaked in Discord server

[+Entertainment](#)

- [Nickelodeon's](#) animation department allegedly leaked 500 GBs of series porches, scripts, music, and more in a private Discord server in an event dubbed the Nickelodeon GigaLeak. Most of the data seems to have been removed from the internet so far.

Dublin Airport targeted by CI0p gang

[+Travel](#) [+CI0p](#) [+MOVEit](#)

- Over 2K [Dublin Airport](#) employees have had personal information stolen by the CI0p ransomware gang in their ongoing MOVEit exploitation attacks. The attacks stole pay and benefits information via a breach into a third-party supplier called Aon. Aon also serves Cork Airport, but it's unknown if their data is affected at this time.

Imperva customers are protected out-of-the-box against CVE-2023-34362.

Australian government data leaked in law firm attack

[+Australia](#) [+Law & Government](#) [+ALPHV](#)

- Sensitive government information has been stolen from Australian law firm [HWL Ebsworth](#) in a recent ALPHV attack that stole 3.6TB of data. 1.1TB of this data has been posted so far. At least 60 Australian government agencies have used the law firm in the past decade, including the police, Prime Minister, and Defence Department, although the full impact of the breach is currently unknown.

ALPHV targets British hospital group

[+UK](#) [+Healthcare](#) [+ALPHV](#)

- ALPHV has also targeted [Barts](#), a British group of hospitals, in a recent attack that British cybersecurity officials are currently investigating. Attackers published files they claimed to have stolen from the group, but more details or verification about the attack are currently unknown.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 42% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

↓ 51% [CVE-2022-22965](#)

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

↓ 40% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

US retail sites see higher-than-average bot attacks on Independence Day

+US +Retail +Automated Attack

- Bot attacks on US retail sites were higher than average on July 4th due to the Independence Day holiday. Retail sites often run promotions on this holiday, leading to higher traffic, which bots can leverage to go unnoticed, scrape data, or steal information.

Indonesian retail site targeted by almost 1M RPS DDoS attack

+Retail +DDoS

- An Indonesian retail site was targeted by an almost 1M RPS DDoS attack this week, coming from about 2600 distinct IPs. The attack was blocked by Imperva protection, and unsuccessful in interrupting service.

Policies & Regulations

Instagram Threads will not be launched in EU over data privacy concerns

+Data Privacy +EU

- Instagram [Threads](#), the upcoming Twitter competitor from Meta, will not be launched in the European Union due to privacy concerns. Ireland's Data Protection Commission confirmed that the app will not be released in the EU at this point over concerns about the wide range and security of user data the app collects.

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