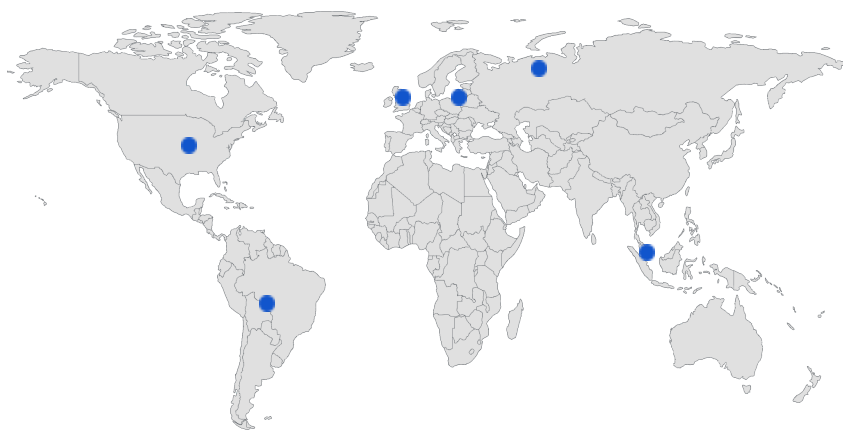


Threat Intel Report: July 5-9

Countries



Top Tags

MOVEit

NATO

Entertainment

Computing

Government

Threat Activity in Imperva

UK computing site targeted by path traversal attacks

+UK +Computing

- A UK computing site saw larger-than-average path traversal attacks on July 8. These attacks came from just 300 distinct IPs, but hit the site with almost 4M attack attempts, primarily written in Go. These attacks were blocked by Imperva protection, and unsuccessful in accessing data.

Indonesian government site attacked by DDoS

+Indonesia +Government +DDoS

- An Indonesian government site was targeted with application layer DDoS on July 9, reaching over 1M RPS. This site is frequently targeted by DDoS, and this specific attack came from 3000 distinct IPs, primarily within Indonesia. These attacks were blocked by Imperva protection, and unsuccessful in causing outages.

Recent Cyber Threats

New MOVEit SQL injection vulnerability disclosed

+MOVEit +SQL Injection +CIOP

- A new vulnerability has been disclosed in the MOVEit software, known as [CVE-2023-36934](#). This bug, a SQL injection vulnerability that allows unauthorized access to unauthenticated users, follows other recent MOVEit vulnerabilities, including one that CIOp has been exploiting in attacks.

Imperva customers are protected out of the box against this vulnerability. For more information, see [this article](#).

RomCom threat actors target Ukraine supporters at the upcoming NATO Summit

[+Russia](#) [+NATO](#) [+Ukraine](#) [+RAT](#)

- The threat actors behind the [RomCom](#) RAT are suspected of conducting phishing attacks against guests invited to the upcoming NATO Summit and organizations supporting Ukraine. The threat actors created a malicious document impersonating Ukrainian World Congress talking points, as well as a fake lobbying document supporting Ukraine, which both used RTF exploitation to connect to the victim once the document was opened.

Vilnius targeted by pro-Russia hackers amid NATO Summit

[+NoName](#) [+Russia](#) [+Lithuania](#) [+Travel](#) [+Infrastructure](#) [+NATO](#)

- DDoS group [NoName](#) has targeted Vilnius around the city's hosting of this year's NATO Summit. The group has allegedly taken down several tourism and infrastructure sites, although all are currently back up. Separately, a shopping mall's music streaming service and a local radio station were hijacked by unknown attackers to play pro-Russian propaganda.

Revolut payment flaw was exploited to steal over \$20M

[+Theft](#)

- Hackers exploited a yet-unknown flaw in [Revolut's](#) payment system that allowed them to steal over \$20M in early 2022. The breach has not yet been exposed publicly, but came from discrepancies between US and European systems that allowed money to be mistakenly refunded using the company's money when transactions were declined.

Latin American businesses targeted by new banking trojan

[+TOITON](#) [+Latin America](#) [+Trojan](#)

- Businesses in Latin America have been targeted by a new Windows-based banking trojan called [TOITON](#) since at least May of this year. The malware gathers system information, steals browser data, and checks for anti-fraud modules, along with executing malicious commands and manipulating files.

Anonymous Sudan targets US entertainment sites

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

- [Anonymous Sudan](#) has targeted entertainment sites Reddit and An Archive Of Our Own in attacks they claim are targeting American LGBTQ+ sites. Reddit is back up, but An Archive Of Our Own remains down.

Data Breaches

Gaming giant Razer investigating massive data breach

[+Gaming](#) [+US](#) [+Singapore](#)

- Gaming company [Razer](#) is investigating reports of a data breach, after someone posted on a hacker forum that they were selling stolen source code, databases, encryption keys, and backend access logins for the company's website. The validity of all of the data is unconfirmed, but the leaked accounts are confirmed valid, and Razer has reset all member passwords.

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