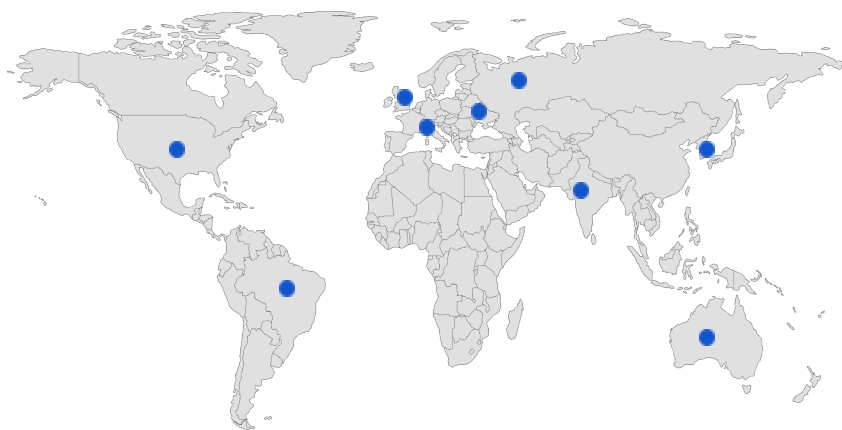


Threat Intel Report: June 5-11

Countries



Top Tags

Hacktivism

Automotive

Government

Telecom

Crypto Scam

Recent Cyber Threats

Microsoft Visual Studio Designer bug could allow malicious extensions

[+CVE](#)

- A spoofing bug found in Microsoft Visual Studio Designer ([CVE-2023-28299](#)) could allow attackers to impersonate a legitimate publisher and push malicious extensions. These extensions could steal sensitive information or change code.

Crypto scam steals over \$5M using fraudulent sites

[+Crypto Scam](#) [+Impulse Team](#)

- A cryptocurrency [scam](#), active since 2021, has leveraged over 1K websites to scam thousands of people worldwide. The scam is managed by Russian threat actors known as Impulse Team, who have collectively stolen more than \$5M.

Anonymous Sudan claims Microsoft Azure and OneDrive outages

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

- Following last week's Outlook attack, [Anonymous Sudan](#) targeted Microsoft Azure and OneDrive this week with DDoS that caused temporary outages. Microsoft has not confirmed the cause behind the outages, but Anonymous Sudan is claiming these attacks as hacktivism protesting the US' involvement in Sudanese internal affairs.

Ukrainian hacktivist group takes down Russian telecom company

[+Hacktivism](#) [+Cyber.Anarchy.Squad](#) [+Russia](#) [+Ukraine](#) [+Telecommunications](#)

- Ukrainian hacking group [Cyber.Anarchy.Squad](#) claimed an attack this week on Russian telecom provider Infotel JSC. The company provides connectivity to the Russian General Bank, and multiple major banks across Russia were unable to connect to the country's banking system following the attack. The group has targeted multiple other Russian companies since the Russia-Ukraine war began last year.

Hacking group steals almost \$3M in digital assets by impersonating journalists

+Crypto Scam +Pink Drainer +Phishing

- A hacking group known as [Pink Drainer](#) has impersonated journalists to conduct phishing attacks, stealing almost \$3M in crypto assets. The attackers posed as journalists, and conducted fake interviews which led the victims to a site instructing them to drag a verification button to their bookmarks- which then stole Discord authentication tokens.

Data Breaches

University of Manchester data breach under investigation

+UK +Education

- The [University of Manchester](#) recently warned staff and students that their data may have been stolen following an early June cyberattack on the University's networks. Currently, the organization is unsure what data may have been stolen, but an investigation into the incident has begun.

Swiss government attacked twice, with ransomware and DDoS, so far this month

+Switzerland +Government +NoName +Play

- The [Swiss government](#) recently disclosed two attacks- a ransomware attack on Swiss technology provider Xplain, and a NoName-claimed DDoS attack. The ransomware attack, claimed by the Play ransomware gang, targeted software used by the Swiss government and military, and the group dumped the data files in early June, leaking Swiss government and operational data. The DDoS attack occurred more recently, and targeted the Federal Administration service with DDoS in an effort to disrupt NATO-aligned countries.

Honda API flaws allow unrestricted access to dealer and customer data

+Automotive

- Recently, [Honda's](#) e-commerce platform for the power equipment market was found vulnerable to API flaws that allowed password reset for any account. Attackers could leverage these vulnerabilities to reset account passwords and have admin-level privileges, leading to exposure of over 21K customer orders, 3.5K dealer accounts, and 11K customers' information, among others.

Telegram bot leaks Indian vaccine data

+Indian +Healthcare

- Indian Covid vaccine site [CoWin](#) came under fire recently for a data breach that allowed a Telegram bot to release names, government IDs, and vaccination records of at least 100 people. The bot has since been taken down, and an investigation is underway into how the data was accessed.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

📈 29% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

↓ 16% [CVE-2022-22965](#)

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

↓ 20% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

South Korean retail site suffers 800K RPS DDoS attack

[+South Korea](#) [+Retail](#) [+DDoS](#)

- On June 7, a Korean retail site was hit with an application DDoS attack reaching a total of 800K RPS. The attack lasted only ten minutes, and came from 3500 total IPs from over 100 countries, including the US, Brazil, and China.

Brazilian account takeover attack targets financial site

[+Brazil](#) [+Financial](#) [+ATO](#)

- On June 6, a Brazilian financial site suffered an account takeover attack that reached 3.5M login attempts. Attackers leveraged just under 900 distinct IPs to conduct this attack, which came primarily from inside Brazil. Being a financial site, attackers could transfer money to different accounts or steal personal information if they were successful.

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