

Threat Intel Report: 12-18 June

Countries



Top Tags

Anonymous Sudan

Clop

Financial

Computing & IT

Government

Recent Cyber Threats

Anonymous Sudan, Killnet, REvil join forces against US and European financial sites

+Financial +Anonymous Sudan +Killnet +REvil

- Anonymous Sudan, Killnet, and REvil announced plans to collectively [target](#) the US and European banking systems over the weekend, including Swift, the European Investment Bank (EIB), and the US Federal Reserve. The groups aim to use DDoS to stop the flow of money that supports Ukraine. As of June 19, the EIB site was down, and the bank acknowledged that it was a cyber attack.

New toolkit discovered targeting Apple systems

+Backdoor +Spyware

- A new toolkit has been discovered targeting [macOS](#) systems, dating back to early April of this year. The attacks consist of three separate Python backdoors that collectively run commands, download and execute files, and potentially run spyware on the victim device. Researchers don't currently know who is behind these attacks, or how they gain initial access.

Microsoft confirms outages were caused by DDoS attacks

+DDoS +Anonymous Sudan

- Microsoft recently [confirmed](#) that last week's Azure and Outlook outages were caused by an application-layer DDoS attack, linking them to an unnamed actor Microsoft is tracking as Storm-1359. Microsoft has not linked Storm-1359 to Anonymous Sudan, but the group publicly claimed these attacks last week.

Data Breaches

Clop gang exploits MOVEit vulnerability, US government targeted

+US +Russia +Government +Clop

- The suspected Russian ransomware gang Clop has recently joined the list of actors exploiting the recent MOVEit vulnerability, and have listed thirteen newly targeted organizations on their leak site, including the Shell oil and gas company, United Healthcare, and the University of Georgia. CISA also recently confirmed that several US government agencies, including the [US Department of Energy](#) and USDA, have been targeted as well, although Clop claims to delete any stolen government data.

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

Driver's license data stolen by Clop gang

+US +Government +Clop

- Oregon's Department of Transportation recently confirmed 3.5M driver's license records were compromised in an early June hack related to the MOVEit vulnerability. Similarly, the Louisiana Office of Motor Vehicles confirmed an attack that potentially stole the personal data of everyone with a Louisiana driver's license. Ransomware gang Clop is assumed to be behind these attacks as well.

Ransomware gang threatens to leak Reddit data

+BlackCat

- The [BlackCat](#) ransomware gang claims to have stolen 80Gb of data from Reddit in a February breach that accessed internal data, including source code and employee data, via a phishing attack. The BlackCat gang is now threatening to leak the data if Reddit doesn't pay the requested \$4.5M bounty.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 32% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

↓ 7% [CVE-2022-22965](#)

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

↑ 47% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

MOVEit attacks on the rise

+Computing & IT

- Imperva has seen a sharp spike in MOVEit-related attacks recently, after a dip late last week. Attacks over the weekend are 40% higher than last week, and have primarily targeted US-based sites in the computing industry.

Imperva customers are protected out-of-the-box against CVE-2023-34362. All attacks have been mitigated by Imperva.

Data leakage attack targets US-based business site

+Business +US +Hong Kong +Business

- A US-based business site was targeted in mid June with data leakage and path traversal attacks. Attacks came from just 800 Hong Kong-based IP addresses, which points to this being a targeted attack. All attacks were blocked by Imperva, and unsuccessful in exfiltrating data.

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