

Threat Intel Report: June 19-25

Countries



Top Tags

MOVEit

US

Education

Financial

Russia

Recent Cyber Threats

Microsoft Azure AD flaw can lead to account takeover

+nOAuth +Account Takeover

- An authentication implementation flaw has been discovered in Microsoft Azure AD that can lead to full account takeover. The attack, known as [nOAuth](#), affects organizations with the “Log in with Microsoft” feature on their Azure Active Directory, and can allow attackers to change their Azure AD account to administrator and take over the victim environment.

Muddled Libra threat group targets BPO industry with social engineering

+Muddled Libra +Social Engineering

- Threat actor [Muddled Libra](#) has been targeting the business process outsourcing (BPO) industry since late 2022 with social engineering attacks. The group uses the Oktapus phishing kit to target telecom and BPO companies with credential phishing and SIM swapping attacks, and is notable for their comfort talking to help desk employees over the phone to conduct successful social engineering.

SolarWinds attack group increases attacks on government and defense targets

+APT29 +Russia

- Russian-affiliated hacking group [APT29](#) has recently ramped up their credential-stealing attacks aimed at foreign ministries and diplomatic entities. The group is mainly known for the SolarWinds attacks in late 2020, and has recently used residential proxy services to obfuscate the source IPs in attacks on governments, NGOs, and defense and manufacturing targets.

Japanese crypto exchange targeted in Apple backdoor attack

+Japan +Crypto exchange +Backdoor

- A Japanese [cryptocurrency exchange](#) was targeted earlier this month in an attack deploying an Apple macOS backdoor known as JokerSpy and ultimately installing SwiftBelt, a Swift-based enumeration tool. Not much is known about the threat actor, but they leverage Python and Swift-based programs to gather data and execute commands.

Data Breaches

Pilot Credentials data breach affects multiple large airlines

+Aviation +US

- A late April hack on aviation application and recruitment portal management company [Pilot Credentials](#) was recently found to have affected multiple large airlines, including American and Southwest. The data breach stole pilots' personal information, including SSNs, drivers license and Airman Certificate numbers, and more.

Over 100K ChatGPT accounts for sale on darkweb forums in the last year

+ChatGPT +Infostealer +Malware

- In the last year, over 100K compromised [ChatGPT](#) account credentials have been listed for sale on darkweb credential marketplaces. Most have been stolen in breaches caused by the Raccoon infostealer, followed by Vidar. Many companies use ChatGPT on a daily basis, so these account breaches could lead to further data loss in large enterprises.

NYC Department of Education records affected by MOVEit breach

+US +Education +MOVEit

- The New York City [Department of Education](#) was also targeted in the recent MOVEit attacks, and they estimate 45K students' records were compromised in the breach. The stolen data includes SSNs and student evaluations, and may contain staff members' information as well.

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

February NCB breach affects Capital One customers

+US +Financial

- US financial institution [Capital One](#) recently alerted customers that a February data breach on NCB Management Services affected Capital One customers. Over 16K customers are affected by this breach, adding to the almost 500K NCB customers that were alerted in March. The stolen data may include SSNs and account numbers.

California state employees affected by MOVEit breach

+US +Education +MOVEit

- The MOVEit breach has also affected almost 770K retired [California employees](#), according to the California State Teachers' Retirement System. Personal information, including SSNs and family member data, could have been stolen.

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

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↑ 37% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

↑ 19% [CVE-2022-22965](#)

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

↑ 18% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

Attacks via hacking tools up 145%

+Hacking tool

- Attacks utilizing hacking tools have risen sharply in the past week, up 145% from previous averages. Data leakage, remote code execution, path traversal, and cross-site scripting have all shot up, passing automated attacks and business logic, which have previously remained the two most common attacks. With recent vulnerabilities like MOVEit in the news, attackers are probably trying to exploit these bugs before they are patched.

Canadian movie theater suffers DDoS attack

+DDoS +Canada +Entertainment

- A Canadian movie theater was targeted recently with an application-level DDoS attack reaching 500K RPS. The attack came from over 700 distinct IPs, which primarily came from the US and Canada. The attack was unsuccessful in causing outages, and was blocked by Imperva protection.

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