

Threat Intel Report: 15-21 May

Imperva Threat Research



Recent Cyber Threats

KeePass vulnerability leaks master password in plaintext

+CVE

- A new vulnerability in KeePass ([CVE-2023-32784](#)) allows attackers to exploit a master password in plaintext. Successful execution requires the attacker to already have compromised the victim's computer, and the password must be typed, not copied from the clipboard.

Android phones susceptible to fingerprint brute force attack

+China +Android +Brute-Force

- A new attack presented by researchers in China, called [BrutePrint](#), brute-forces fingerprints on Android smartphones to bypass user authentication. The attack leverages inadequate biometric protection to conduct a man-in-the-middle attack and copy fingerprint images.

Anonymous Sudan targets Ukraine, UAE

+Anonymous Sudan +Israel +UAE +Ukraine

- [Anonymous Sudan](#) continues to target the Middle East, with recent attacks on both Israel and the United Arab Emirates. The group pivoted to target the UAE on May 20, after brief attacks on Ukraine after Zelenskyy commented at the Arab Summit.

Targeted hacking campaign found on Southeast Asian servers

+China +Southeast Asia +Government +Aviation +Education +Telecom

- A [backdoor](#) has been found in Southeast Asian government, aviation, education, and telecom organizations as part of a new, highly targeted hacking campaign. The backdoor, which may have been active as far back as 2018, ultimately deploys ZXShell, which has been tied to several Chinese hacking groups.

Android vulnerability enables memory management attacks

+CVE

- CISA recently alerted about a Samsung vulnerability ([CVE-2023-21492](#)) that is leveraged to bypass Android address space layout randomization and exploit memory management issues.

Fake CapCut software downloads distribute stealer malware

+Malware

- A new malware distribution campaign has been found impersonating the [CapCut](#) video editing program. Fake websites offer free downloads of the program, which then install Offx Stealer and Redline Stealer malware on the victim's computer.

Data Breaches

Eyewear company customer data leaked for free

+Retail

- [Luxottica](#) confirmed a 2021 data breach exposed over 70M customers' records after a database was posted recently on hacker forums. The data contains personal information, including addresses and birthdates, and was posted for free in mid May, making the data extremely accessible to attackers.

Indian apparel company leak exposes 1.5M women's records

+India +Retail

- Customer data from Indian clothing company [Zivame](#) was recently listed for sale, exposing the data of over 1.5M customers. Although the company has yet to confirm the breach, the sample data was confirmed to be accurate, and the breach exposes personal data and physical addresses of primarily female customers.

DISH probably paid ransom in February ransomware attack

+US +Telecom & ISP

- [DISH networks](#) recently confirmed a February ransomware attack that exposed 300K people's records, including drivers license numbers. The network's letter says that it received confirmation that the data was deleted, which implies the company paid the requested ransom.

Sysco data breach may expose SSNs and bank account numbers

+US +Food & Beverages

- [Sysco](#) recently alerted over 125K people that their data may have been exposed in a recent data breach that went undetected for almost two months. The data of current and former employees may include social security and bank account numbers.

PharMerica data breach exposes 2M records

+US +Healthcare

- US healthcare company [PharMerica](#) data recently alerted customers that their data may have been compromised in a March attack claimed by the Money Message ransomware group. The group claimed to have 2M records, including social security numbers.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↑18% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

↓16% [CVE-2022-22965](#)

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

↓44% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

Indonesian government site under persistent DDoS

+Indonesia +DDoS +Law & Government

- An Indonesian government site has been frequently targeted by application DDoS since the beginning of May. Although attacks have been consistent, they've been relatively low-level for the first half of the month, and increased intensity on the 14th. Attacks came from an average of only 2200 distinct IPs per day, primarily based in the US and Indonesia.

Spanish news site targeted by path traversal

+Spain +Path Traversal +News

- For three days, a Spanish news site was attacked with path traversal that reached over 2M requests per day. Attacks overwhelmingly came from Germany and probably intended to access restricted or sensitive content to gain personal information or paywalled content.

Policies & Regulations

G7 leaders express concern over digital security

+G7 +EU +Security

- The G7 leaders recently released a [statement](#) on economic security, which expressed concern about regulations that localize or allow governments to access data without appropriate protections. The G7 promised to counter malicious practices in the digital sphere going forward.

Meta charged record EU fine in data privacy violation

+EU +Security

- The EU imposed a \$1.3 billion fine on Facebook parent company [Meta](#) for transferring European user data to US servers. This action, which violates EU data privacy rules, is the highest EU data protection fine ever imposed.

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.