

Threat Intel Report: 22-28 May

Imperva Threat Research



Recent Cyber Threats

Lazarus Group targets Windows IIS servers

+North Korea

- North Korea-based [Lazarus Group](#) hackers are targeting Windows Internet Information Services web servers to access corporate networks, exploiting misconfigurations to create malicious files. The group's main goal is financial gain, but they also conduct espionage for North Korea.

New trojan GobRAT targets Japanese linux routers

+Japan

- A new Golang remote access trojan called [GobRAT](#) has been seen targeting Linux routers based in Japan. The trojan collects information from the machine, reads and writes files, and attempts to log in to services on other machines.

.zip domains create new attack vectors for social engineering

+Social Engineering

- Attackers are emulating file archive systems in a web browser when a victim visits a [.zip domain](#), in a new attack leveraging the new domain extensions. The attack could use social engineering and steal credentials and personal files.

Hacking campaign since 2021 targets US and Guam critical infrastructure

+China +US +Guam +Critical Infrastructure

- Allegedly Chinese state-sponsored hackers have conducted a hacking campaign since 2021 that targeted critical infrastructure in the US and Guam. The group is nicknamed [Volt Tycoon](#), seems to be laying the groundwork for future offensive attacks, and access to a key location in the Pacific may help China in a military conflict in the region.

Data Breaches

Tesla whistleblower releases 100GB of internal data

+Automotive

- A [Tesla](#) whistleblower dumped 100GB of internal data, including thousands of Autopilot safety complaints, crash reports, and the personal data of over 100,000 current and former employees, including Elon Musk. The information was sent to a German newspaper, which has not yet verified the documents- but if confirmed, Tesla could be fined up to \$3.5B.

NHS tracked and shared patient data without consent

+UK +Healthcare

- A tracking tool discovered in 20 [NHS](#) trust websites was found to collect granular browsing information, including health webpages visited and details about when the user booked appointments or ordered prescriptions. This data, which was collected and shared with FaceBook parent company Meta without consent, could collectively reveal personal health details about the user.

Dental and ID data exposed in MCNA breach

+US +Healthcare

- Dental benefits company [MCNA](#) recently notified customers that a late February data breach exposed government IDs, including SSNs and drivers license information, as well as dental data. Almost 9M people are affected by this breach, which was caused by an unnamed third party.

Metropolitan Opera House data breach exposes 45,000 records

+US +Arts

- The [Metropolitan Opera House](#) is under fire for compromising the personal information of 45,000 employees and customers. The breach originally occurred in December, and took down the website for more than 30 hours.

Swiss company ABB attacked by Black Basta ransomware group

+Switzerland +Manufacturing +Black Basta

- Swiss manufacturing company [ABB](#) recently suffered a ransomware attack in early May that targeted the company's Windows Active Directory. The attack was reportedly conducted by the Black Basta ransomware group, but the company has not been added to the group's leak website, which implies they may still be in negotiations or have paid a ransom.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 12% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

↑ 24% [CVE-2022-22965](#)

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

↑ 125% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

Anonymous Sudan targets Israeli education site

+Israel +Education +Anonymous Sudan

- On May 24, an Israeli academic site suffered an application DDoS attack that reached almost 1.2M RPS. The attack was conducted by Anonymous Sudan and came from about 20,000 distinct IPs.

UK computing site targeted by path traversal and RCE

+UK +Computing & IT

- A UK computing site was targeted on May 27 by path traversal and RCE attacks that totaled 4.3M requests. The attacks came from just 300 US-based IPs, meaning attackers conducted targeted, specific attacks in an attempt to exfiltrate information.

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.

Imperva Headquarters

One Curiosity Way, Suite 203
San Mateo, CA 94403

Telephone: 650-345-9000

Fax: 888-611-7282