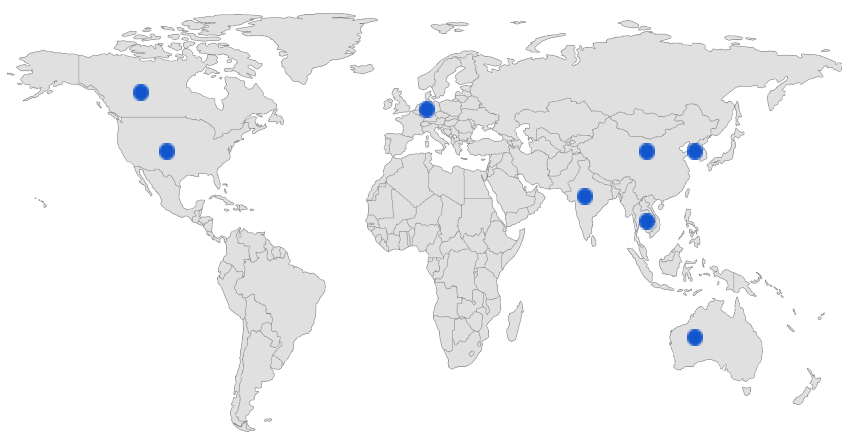


# Threat Intel Report: October 2 - 8, 2023

## Countries



## Top Tags

ALPHV

SiegedSec

RansomedVC

Balada Injector

APT41

## Executive Summary

### Actionable Information:

- **Software and Platform Vulnerabilities:** Regularly update and patch widely-used software, platforms, and IoT devices to address recent critical vulnerabilities.
- **Firewall and Protection Systems:** Review and strengthen configurations of firewall and DDoS protection systems to address identified logic flaws and bypass techniques.
- **Botnet and Malware Activity:** Bolster defenses against the rising aggressive botnet attacks and stay vigilant against new malware strains targeting popular platforms.
- **Data Security and Management:** Tighten security protocols around data storage, access, and transmission to prevent breaches and inadvertent exposures.
- **Ransomware Preparedness:** Prioritize regular backups, employee training, and proactive security measures to mitigate the increasing threat of ransomware attacks.

### Outlook:

The cyber landscape continues to evolve with a mix of software vulnerabilities, malware attacks, and data breaches. Organizations are advised to stay updated on patches, especially for widely-used software like WS\_FTP and Linux distributions. The rise of new Mirai botnet variants indicates a continued focus on IoT devices, while targeted attacks on specific platforms like WeChat and WordPress highlight the need for vigilance across various digital touchpoints. Data breaches, such as those experienced by the National Logistics Portal and the DC Board of Elections, underscore the importance of securing sensitive information and ensuring robust cybersecurity measures.

## Threat Activity in Imperva

### Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 12% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

↓ 14% [CVE-2022-22965](#)

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

↑ 10% [CVE-2023-35082](#)

- An authentication bypass vulnerability in Ivanti

### Korean gambling site hit by 2.6M RPS attack

+Gambling +Korea

- A Korean gambling site was targeted this week with application DDoS reaching 2.6M RPS, and coming from 7K IPs. This is part of an upward trend in application DDoS over the past few weeks.

### Data leakage from hacking tools rises 100%

+Canada +Australia +Business +Financial Services

- Hacking tools conducting data leakage attacks rose almost 100% in the second half of this week. Attacks primarily targeted Canadian and Australian sites in the Business and Financial Services industries.

## Recent Cyber Threats

### WS\_FTP gets crucial update

+CVE

- [WS\\_FTP](#), a widely-used file transfer software, has addressed multiple critical vulnerabilities in its software, including one ranked 10 out of 10 on the CVSS severity scale. Users are urged to apply the patch immediately to prevent potential exploitation, as mass exploitation has begun.

*Imperva customers are protected against this vulnerability.*

### Cloudflare's firewall bypassed due to logic flaws

+DDoS

- Attackers have found a way to bypass [Cloudflare's](#) firewall and DDoS protection due to certain logic flaws. The organization's usage of open infrastructure, which accepts connections from all users, is the root cause of the problem, which only requires an attacker to make a free account.

### Rise of new Mirai botnet variants

+Mirai +DDoS +Botnet

- A new wave of [Mirai](#) botnet variants, including HailBot, KiraiBot, and CatDDoS, has been observed launching aggressive attacks. These botnets continue the legacy of the original Mirai, targeting IoT devices.

### New critical Linux vulnerability

+Linux +CVE

- A significant bug named "[Looney Tunables](#)" has been identified in major Linux distributions. The bug allows attackers to gain root privileges by exploiting a buffer overflow weakness in the GNU C Library's ld.so dynamic loader.

## **WeChat users targeted by Chinese APT actors**

**+APT41 +China**

- Chinese Advanced Persistent Threat (APT) group [APT41](#) has been observed targeting WeChat users since at least 2018. The campaign aims to extract sensitive information from unsuspecting users of the popular messaging app.

## **Confluence faces privilege escalation bug**

**+CVE +Privilege escalation**

- A critical privilege escalation bug has been identified in [Confluence](#), prompting urgent patching. The bug affects on-premises instances of Confluence Server and Confluence Data Center, and allows attackers to create and abuse admin accounts within the software.

*Imperva customers are protected against this vulnerability.*

## **GoldDigger Android trojan targets bank accounts**

**+GoldDigger +Trojan +Vietnam +Financial Services**

- A new Android trojan named [GoldDigger](#) has been discovered, which drains victims' bank accounts. The trojan has been active since at least June 2023, and is currently targeting users of over 50 Vietnamese banking apps.

## **Android devices infected with malware during production**

**+Malware +BADBOX +Triada +China**

- A significant number of devices used by retailers have been found to be infected with malware. The scheme, known as [BADBOX](#), deploys the Triada malware as a backdoor on various Android devices during the supply chain process in China.

## **Balada Injector strikes WordPress plugin**

**+Malware +WordPress +Balada Injector**

- The [Balada Injector](#) malware is targeting an unpatched TagDiv plugin used in the Newspaper theme for WordPress. Site administrators are advised to update the plugin immediately to fend off potential attacks.

# **Data Breaches**

## **National Logistics Portal data exposed**

**+India +Government**

- A significant data leak was reported at the Indian [National Logistics Portal](#), exposing sensitive information. The newly-created portal, which manages port operations, accidentally left encryption keys and AWS S3 buckets exposed.

## **Telecom standards body breached**

**+Telecommunications**

- [ETSI](#), a European telecommunications standards organization, suffered a cyberattack, resulting in the theft of its user database. It is not clear whether the attack was financially motivated, or if the hackers acquired the list of users for espionage purposes.

## **Virginia school district faces LockBit threat**

**+Education +US +LockBit**

- [Fauquier County School District](#) in Virginia was targeted by the LockBit ransomware. The school district was able to stay open, and claims that the impact has been minimal.

## **Motel One hit by ALPHV ransomware**

**+ALPHV +Germany +Travel**

- The hotel chain [Motel One](#) became a victim of the AlphV ransomware attack. The group claims to have stolen 6TB worth of internal data, containing reservations from the last three years.

## San Francisco transportation agency exposes driver data

**+US +Transportation**

- The [Metropolitan Transportation Commission](#) in San Francisco inadvertently exposed 26K files including drivers' plate numbers and addresses. The misconfigured AWS buckets exposed data from 2016 to 2021.

## NATO's unclassified sites under attack

**+NATO +SiegedSec +Government**

- The [North Atlantic Treaty Organization](#) (NATO) is currently investigating claims made by a hacking group named SiegedSec, which alleges to have stolen 9 GB of data from several unclassified NATO websites.

## Alleged sale of FBI data

**+US +Government**

- Classified data from the FBI's [Law Enforcement Enterprise Portal](#) (LEEP) is allegedly up for sale, putting sensitive information at risk. The alleged FBI LEEP data sale can mean critical information used by US law enforcement agencies, intelligence groups, and criminal justice organizations is at risk of being misused by cybercriminals.

## 23andMe user data compromised

**+Healthcare**

- The genetic testing company [23andMe](#) confirmed that data from a subset of its users was compromised, though its systems were not breached. Attackers scraped information from a feature called DNA Relatives; the compromised data was then posted on BreachForums, with claims of containing information about Ashkenazi Jews and other ethnicities.

## DC Board of Elections data stolen

**+US +Government +RansomedVC**

- The [DC Board of Elections](#) is investigating a data breach after claims from attack group RansomedVC. The group claims to have stolen 600K records, which the Board of Elections has confirmed.

---

## 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