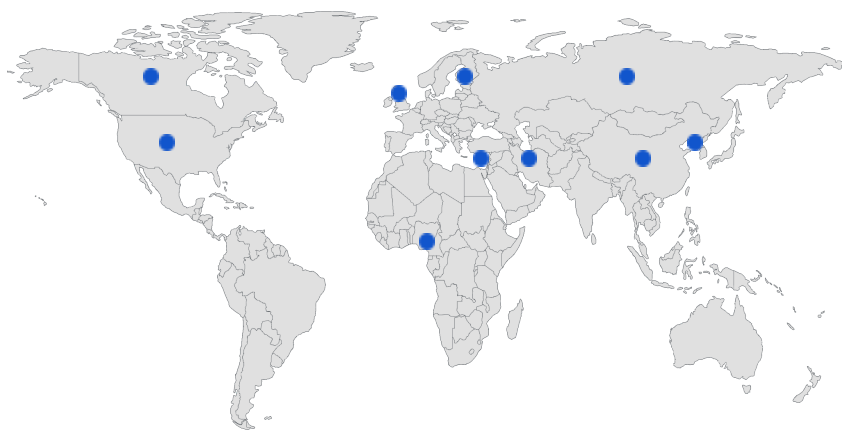


Threat Intel Report: November 6-12, 2023

Countries



Top Tags

Anonymous Sudan

MuddyWater

Bluenoroff

LockBit

Clop

Executive Summary

Actionable Information:

- *Trend in sophisticated scams and malware:* There's a noticeable increase in sophisticated scams, particularly in the cryptocurrency space. Organizations should focus on enhancing user awareness and implementing robust security measures to detect and prevent such threats. This includes educating users about the risks of unofficial apps and the importance of verifying digital assets' security.
- *Rise of targeted malware attacks:* The emergence of malware targeting specific operating systems and software packages, like macOS and Python, signifies a trend towards more targeted attacks. It's essential to maintain up-to-date security protocols and conduct regular audits of software and third-party packages used within the organization.
- *Exploitation of system vulnerabilities:* The incidents involving vulnerabilities in widely-used services like Royal Mail and Azure suggest a growing trend of attackers exploiting system weaknesses. Strengthening cybersecurity infrastructure to protect against such vulnerabilities is crucial. This involves regular system updates, vulnerability assessments, and employing advanced threat detection systems.
- *State-sponsored cyber activities and advanced malware techniques:* The increasing involvement of state-sponsored groups and the development of AI-driven malware indicate a shift towards more complex and politically motivated cyber attacks. Organizations should prepare for these advanced threats by integrating state-of-the-art cybersecurity solutions and staying informed about global cyber-political trends.

Outlook:

The cybersecurity landscape is rapidly evolving, with a clear trend towards more sophisticated and targeted attacks, including state-sponsored activities and advanced malware techniques. This evolution necessitates a proactive and



comprehensive approach to cybersecurity, encompassing user education, regular system updates, and the integration of advanced security measures. As cyber threats become increasingly complex and politically motivated, organizations must stay informed and agile, adapting their strategies to counter emerging threats and protect their digital assets effectively.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 4% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

↑ 79% [CVE-2022-22965](#)

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

↑ 47% [CVE-2023-35078](#)

- A remote unauthenticated API access vulnerability in Ivanti Endpoint Manager Mobile

Cameroon financial site targeted in DDoS attack

+Cameroon +Financial Services +DDoS

- A Cameroon-based financial site was targeted this week in an application-layer DDoS attack that reached almost 2M requests per second (RPS). Attacks came from 2800 distinct IP addresses, and targeted the site's assets directory, likely in an attempt to exhaust the site's resources or test defenses.

Swedish industrial site hit with 500% average data leakage attacks

+Sweden +Business & Industrial +Data Leakage

- A Swedish industrial site experienced a high volume of data leakage attacks this week, with attacks reaching 500% over the site's average, and primarily coming from Dutch IPs.

Recent Cyber Threats

Fake crypto app installs stealer malware

+Crypto +Malware

- Scammers deployed a fake [Ledger Live](#) app on the Microsoft Store, tricking users into downloading malware that stole Bitcoin and Ethereum funds. The sophisticated scam led to the theft of over \$768,000 in crypto assets. Microsoft has since removed the app and is investigating the breach in their app review process.

New North Korean malware targets MacOS systems

+Bluenoroff +North Korea +Malware +ObjCShells

- The Bluenoroff APT group, based in North Korea, has developed a new malware strain named [ObjCShellz](#), targeting macOS systems. This malware, similar to the Rustbucket campaign, operates as a simple remote shell executing commands on compromised systems.

Malicious Python packages found in PyPI

+Python +Malware +BlazeStealer

- Malicious Python packages containing BlazeStealer malware were found in the [Python Package Index](#) (PyPI) repository. These packages, disguised as obfuscation tools, enable attackers to control compromised systems, steal sensitive information, and even cause system crashes. The malware was downloaded 2,438 times, primarily in the US, before being removed.

Royal Mail vulnerability exposes customers to attacks

+UK

- [Royal Mail](#), the UK's largest courier company, left an open redirect vulnerability on one of its sites, exposing customers to potential phishing attacks and malware infections. This vulnerability could lead users to fake websites designed to steal credentials and credit card numbers.

New cryptomining method discovered using Azure

+Cryptomining

- A new undetectable method of cryptocurrency mining has been discovered using [Microsoft Azure's](#) automation service. This technique allows for unlimited computational resource access without incurring costs or attracting attention. The method exploits a bug in Azure's pricing calculator and leverages Azure Automation's features. Microsoft has acknowledged the issue but deemed the behavior as 'by design', raising concerns about potential misuse by threat actors for various purposes beyond crypto mining.

Iranian hackers exploiting C2 framework against Israel

+Iran +Israel +MuddyWater +Government

- Iranian state-sponsored hackers, known as MuddyWater, have been using a new command-and-control framework named [MuddyC2Go](#) against Israeli targets. Developed in Go, this tool has been active since early 2020, replacing the previously used PhonyC2. MuddyWater, linked to Iran's Ministry of Intelligence, typically initiates attacks via spear-phishing, leading to the deployment of this C2 framework for post-exploitation activities.

Python-based infostealer leverages AI

+Python +Malware +AI

- Researchers have identified a new Python-based info-stealer and hacking tool named [Predator AI](#) targeting cloud services. This tool integrates AI technology, specifically a ChatGPT-driven class, to streamline its functionality. Distributed primarily through Telegram channels linked to hacking communities, Predator AI is designed for web application attacks on technologies like WordPress and AWS SES.

Anonymous Sudan targets Cloudflare

+Anonymous Sudan +DDoS

- Anonymous Sudan launched a significant DDoS attack against [Cloudflare](#). Cloudflare confirmed that the attack took down their site for a few minutes, but said that it did not impact products or services.

Pro-Palestine hacking group disrupts Israeli flour facility

+Israel +Soldiers of Solomon

- The [Soldiers of Solomon](#), a pro-Palestinian hacktivist group, executed a targeted cyber attack on Israel's largest flour production facility, causing significant operational disruptions. The group's methods included infiltrating the plant's network systems, leading to a halt in production processes and potentially impacting the food supply chain in the region.

Data Breaches

Chinese bank operations disrupted by LockBit gang

+China +Financial Services +LockBit

- The [Industrial and Commercial Bank of China](#) (ICBC), one of the world's largest banks, faced a significant ransomware attack by the LockBit gang. This attack disrupted the bank's operations, including the clearing of

trades in the US Treasury market. The incident, which began on a Wednesday evening, forced ICBC to reroute some trades due to cybersecurity issues.

US healthcare provider discloses 2M record data breach

+Healthcare +US

- [McLaren Health Care](#), a prominent healthcare provider, disclosed a data breach impacting 2.2 million individuals. This breach involved unauthorized access to sensitive personal and medical information.

Russian insurance company breached, including GRU information

+Russia +Healthcare +Government

- [Rosgosstrakh](#), Russia's second-largest insurance company, suffered a major data breach with 400GB of sensitive data being sold online for \$50,000 in Bitcoin or Monero. The compromised data includes personal and insurance-related information of approximately 3 million individuals, including Russian military intelligence agents (GRU). The breach exposed bank statements, social security numbers, and complete bank routing information, posing significant risks to individuals and potentially the Russian government.

Canadian healthcare organization attacked by Medusa group

+Canada +Healthcare +Medusa

- The [Canadian Psychological Association](#) (CPA) was attacked by the Medusa ransomware group, which claimed responsibility on their dark web channel. The group demanded \$10,000 to delay publishing the data for a day and \$200,000 for complete deletion. The breach involved sensitive information, including psychological reports and personal data.

Chinese e-commerce site accidentally leaks data for millions of Chinese citizens

+E-Commerce +China

- An unsecured database of [Zhefengle](#), a China-based e-commerce store, exposed millions of Chinese citizen identity numbers. The database contained over 33 million orders from 2015 to 2020, including customer shipping addresses, phone numbers, and government-issued resident identity card numbers. The database was unprotected and accessible to anyone with its IP address, posing a significant privacy risk.

Scraped information of 35M LinkedIn users leaked

+USDOD +US +Government

- A hacker known as 'USDOD' leaked a database containing personal information of over 35 million [LinkedIn](#) users. The data, obtained through web scraping, includes full names, email addresses, and profile bios but notably lacks passwords. The leaked information, which includes email addresses of high-ranking US government officials and various global agencies, raises significant privacy and security concerns.

Clop ransomware gang targets Maine government in ongoing MOVEit attacks

+US +Government +MOVEit +Clop +Russia

- The [Maine government](#) experienced a significant data breach, impacting over 1.3 million individuals. This breach, attributed to a Russia-linked ransomware gang, Clop, occurred due to a vulnerability in the MOVEit file-transfer system. Sensitive data, including names, birth dates, social security numbers, and medical information, were stolen.

E-commerce site's data leaked after paying ransom

+E-Commerce +Ransomware

- [Dolly.com](#), an e-commerce platform, faced a ransomware attack and opted to pay the ransom. Despite the payment, the attackers proceeded to release the stolen data publicly. This incident underscores the risks associated with ransom payments in cyberattacks, as there is no guarantee that the attackers will honor their word.

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 mail:

Imperva Headquarters
One Curiosity Way, Suite
203 San Mateo, CA 94403