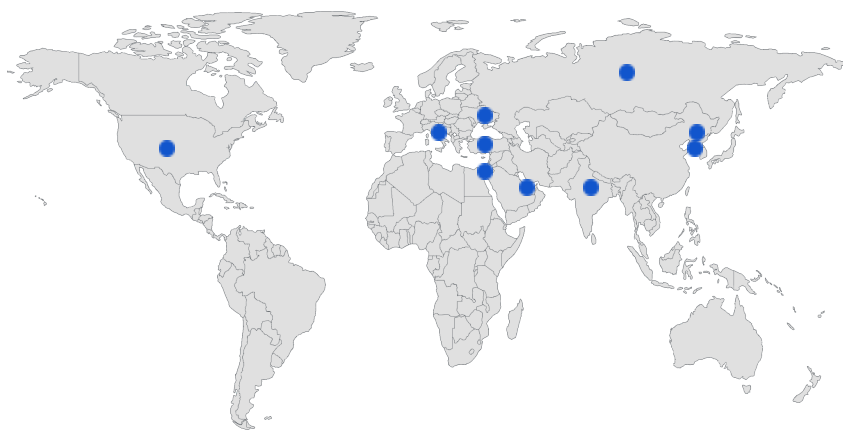


Threat Intel Report: November 20-26, 2023

Countries



Top Tags

BlackCat

Clop

Play

Cyber Toufan Operations

Corejava

Executive Summary

Actionable Information:

- **Enhanced detection and response:** Organizations must invest in advanced detection and response capabilities to counter sophisticated malware and ransomware threats. This includes adopting next-generation antivirus solutions, enhancing endpoint detection, and employing proactive threat hunting strategies.
- **Supply chain security:** The incidents involving CyberLink and TmaxSoft highlight the critical need for robust supply chain security measures. Organizations should conduct thorough security assessments of their suppliers and integrate supply chain risk management into their overall cybersecurity strategy.
- **Awareness and education:** The effectiveness of social engineering tactics in recent attacks underscores the importance of ongoing cybersecurity awareness and education programs for both employees and consumers.
- **International collaboration:** The cross-border nature of many cyber threats, including state-sponsored activities, necessitates increased international collaboration and information sharing among cybersecurity entities and law enforcement agencies.

Outlook:

The current cyber threat landscape is characterized by a diverse range of sophisticated and evolving tactics. Malware campaigns are becoming increasingly deceptive, with tactics like disguising malware as legitimate software and exploiting social engineering through fake apps. The involvement of state-sponsored groups in cyber espionage, particularly from Russia and North Korea, highlights a growing trend in geopolitical cyber warfare. The shift in focus of attacks, such as the targeting of MacOS users and the evolution of ransomware into RaaS models, indicates a broadening of threat vectors. Additionally, the significant data breaches in various sectors, including healthcare, technology, and government, underscore the critical need for enhanced cybersecurity measures and awareness. This



evolving landscape necessitates a proactive and dynamic approach to cybersecurity, emphasizing the importance of continuous monitoring, updating security protocols, and educating users about emerging threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 21% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

↓ 49% [CVE-2022-22965](#)

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

↑ 7% [CVE-2023-35078](#)

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

Israeli insurance company targeted in largest Israeli DDoS attack of 2023

+Israel +Financial Services

- An Israeli insurance company was targeted this week in a DDoS attack reaching almost 1.5M requests per second (RPS). This is the largest attack we've seen in Israel this year, and it's larger than any attacks tracked during the beginning of the Israel-Palestine conflict in October. The attack lasted over 13 hours, and came from almost 8,400 distinct IPs, primarily based in the US, Brazil, and China.

Italian business site hit in attempted ATO attack

+Italy +Business

- An Italian business site experienced an attempted account takeover (ATO) attack this week, in a three-day attack reaching 8.5M requests per day. The attacks mostly came from within Italy, as well as China and the US.

Recent Cyber Threats

Malware disguised as WinSCP through fake Google ads

+Malware

- Cybercriminals are using manipulated search results and fake Google ads to trick users into downloading [malware](#) disguised as the legitimate software WinSCP. The campaign involves redirecting users to a compromised WordPress site and then to a phishing site. The malware, delivered as a ZIP file, employs DLL side-loading and drops Python scripts for malicious activities, targeting primarily users in the U.S.

Russian FSB-linked group targets Ukraine with LitterDrifter worm

+Russia +FSB +Ukraine +LitterDrifter

- Russian cyber espionage actors, linked to the Federal Security Service (FSB), are using a USB worm called [LitterDrifter](#) to target Ukrainian entities. It's an evolution of a previous PowerShell-based USB worm and has been used in large-scale data collection efforts, with possible infections detected in several countries including the U.S., Vietnam, Chile, Poland, Germany, and Hong Kong.

Lumma C2 malware evolves with anti-sandbox technique, Google account hijacking

+Lumma

- The [LummaC2 stealer malware](#) has been updated with a novel anti-sandbox technique using trigonometry to evade detection. This technique delays the malware's activation until human mouse activity is detected, effectively bypassing most analysis systems. The malware devs have also introduced [a new feature](#) that allegedly allows cybercriminals to restore expired Google authentication cookies. This capability, if true, could enable attackers to hijack Google accounts even after the legitimate owner has logged out or their session has expired.

Konni campaign utilizes malicious Russian military document

+Konni +Russia

- The [Konni](#) campaign is distributing a Russian-language Word document equipped with a malicious macro, targeting Microsoft Windows users. This document, disguised as a Russian military operation report, deploys a remote access trojan (RAT) capable of controlling infected systems.

Corejava malware found in popular children's tablet

+Corejava

- The Dragon Touch KidzPad Y88X 10 tablet, sold on Amazon, was found to contain [Corejava](#) malware, as well as preinstalled riskware and an outdated parental control app called KIDOZ. Despite Amazon removing the product following the EFF's investigations, other KidzPad Y88X models remain on sale.

Agent Tesla malware adopts ZPAQ compression for stealth

+Agent Tesla

- A new variant of the [Agent Tesla](#) malware is using the ZPAQ archive format to evade detection and steal information from about 40 web browsers and various email clients. The use of ZPAQ, an uncommon compression format, and the .wav extension helps the malware bypass traditional security measures, making it more difficult for automatic scanning systems and sandboxes to detect.

Fake banking and government apps target Indian Android users

+India +Android

- Android users in [India](#) are being targeted by a malware campaign that uses social engineering to install fraudulent apps impersonating banks and government services. These apps, distributed via WhatsApp and Telegram, aim to capture banking details, payment card information, and other personal data. The malware, which hides its icon after installation, can intercept one-time passwords (OTPs) and send them to the attackers, significantly increasing the risk of financial fraud for the victims.

8base group enhances ransomware arsenal with new Phobos variant

+8base +Phobos

- The [8Base](#) ransomware group has incorporated a new variant of the Phobos ransomware into their attacks, which employs a three-stage payload decryption process and advanced features like .NET profiler DLL loading vulnerability and Cyrillic language to avoid detection. The Phobos variant used by 8Base includes capabilities for establishing persistence, rapid encryption, and removal of backup and shadow copies, posing a significant threat to targeted systems.

Play ransomware transforms into a RaaS model

+Play

- https://thehackernews.com/2023/11/play-ransomware-goes-commercial-now.html?&web_view=true
- The Play ransomware, also known as Balloonfly and PlayCrypt, has evolved into a Ransomware-as-a-Service (RaaS) operation. Originally exploiting Microsoft Exchange Server vulnerabilities, Play ransomware now offers a complete package for cybercriminals, including documentation, forums, technical support, and ransom negotiation support, making it a more accessible and dangerous tool for potential attackers.

Mac users targeted by Atomic Stealer via fake browser updates

+Atomic Stealer

- Atomic Stealer malware is now being distributed to Mac users through a campaign called [ClearFake](#), which uses compromised websites to push fake browser updates. This marks a significant shift in the campaign's focus, previously targeting Windows users, to now include MacOS. The malware, disguised as Safari or Chrome updates, steals credentials and files, and sends the data to a command and control server.

Data Breaches

Massive data leak from Israeli cybersecurity firm Radware

+Cyber Toufan Operations +Israel +Computing & Technology

- Cyber Toufan Operations, a politically motivated hacker group, has leaked gigabytes of sensitive data from [Radware](#), an Israeli cybersecurity company, and its customer Signature-IT. The leaked data, dumped daily on Telegram, includes personal information of millions of Israelis connected to Signature-IT's clients, such as Max Security, the Israel Innovation Authority, and the Israeli government's National Archives. The group claims to abide by a ceasefire but continues to threaten further leaks, raising concerns about the ongoing cyber warfare and the security of digital infrastructures in Israel.

BlackCat ransomware targets Autonomous Flight Technologies

+BlackCat

- [Autonomous Flight Technologies](#), known for its unmanned drone systems, has reportedly been hit by a cyberattack from the BlackCat ransomware group. The group claims to have breached AFT's data and allegedly sold it to an undisclosed foreign entity. AFT, which partners with major organizations like Airbus, NASA, NBC, and Northrop Grumman, has not yet confirmed the breach.

Idaho National Laboratory suffers major data breach

+US +Government +SiegedSec

- The [Idaho National Laboratory](#), a key U.S. national security lab, has experienced a significant data breach by the hacking group SiegedSec. The group claimed to have accessed detailed personal information of thousands of employees, including social security numbers, bank account details, and addresses. The breach, which targeted the lab's human resources application, raises serious national security concerns due to the sensitive nature of the work conducted at the lab, including cybersecurity and energy security.

Extensive leak of Turkish citizens' vaccination records

+Turkey +Healthcare

- Over 2 million [Turkish citizens'](#) vaccination records from 2015 to 2023 have been leaked. The data, which includes birth dates, doctors' full identification numbers, vaccination dates, vaccine types, and other details, was likely obtained through an information disclosure vulnerability. This breach is particularly concerning as it exposes the personal information of a significant portion of Turkey's population, including around 70% of its doctors, to potential malicious use such as identity theft and physical tracking.

\$26M crypto heist at Kronos Research

+Cryptocurrency

- [Kronos Research](#), a cryptocurrency trading and investment firm, reported a loss of \$26 million in cryptocurrency due to a cyberattack. The attack involved unauthorized access to the firm's application programming interface (API) keys, leading to the theft of 12,800 ETH distributed across six different wallets. Kronos has paused trading and initiated an investigation, assuring that all losses will be covered internally and no partners will be affected.

TmaxSoft's massive data exposure leaks over 50M records

+South Korea +Computing & Technology

- [TmaxSoft](#), a South Korean IT company specializing in enterprise software, has inadvertently leaked over 50 million sensitive records, totaling 2 TB of data. The exposed Kibana dashboard, containing employee names, emails, phone numbers, contract numbers, attachments, and internal communications, has been accessible since June

2021. This extensive data leak, which includes critical internal information, poses a significant risk for supply chain attacks, potentially affecting TmaxSoft's clients and providers. The company has not yet responded to the disclosure, and the vulnerability remains unpatched, raising concerns about the security of the data and the potential for its misuse.

Blender project under siege by DDoS attacks

+DDoS

- The open-source [Blender](#) project has been experiencing persistent DDoS attacks since Saturday. The attacks have caused significant disruption to the project's services, including its website and other online platforms. The identity of the attackers remains unknown, and the Blender team is actively working to mitigate the impact and restore normal operations.

North Korean cyber espionage targets CyberLink

+North Korea +Technology +Supply Chain

- North Korean hackers, identified as the Diamond Sleet group, conducted a supply chain attack on [CyberLink](#), a Taiwanese software company. They modified a legitimate CyberLink application installer to include malicious code, impacting over 100 devices in countries like Japan, Taiwan, Canada, and the United States. The attack, meant to conduct espionage, data theft, and financial gain, has targeted media, IT services, and defense-related entities.

Massive data breach hits Welltok, exposing millions of patients

+Healthcare +US +Clon

- [Welltok](#), a healthcare SaaS provider, experienced a data breach that exposed the personal data of nearly 8.5 million patients in the U.S. The breach occurred due to a hacked file transfer program and included sensitive information like names, email addresses, Social Security Numbers, and health insurance details. The Clon ransomware gang exploited a zero-day vulnerability in the MOVEit software, leading to this extensive data breach.

BlackCat ransomware disrupts Fidelity National Financial operations

+BlackCat +US +Financial Services

- [Fidelity National Financial](#), a major U.S. insurance company, confirmed a cybersecurity incident involving the BlackCat ransomware group. The attack forced FNF to shut down several key systems, affecting services related to title insurance, escrow, and other real estate and mortgage industry services. The full impact of the breach is still being assessed.

Cyberattack targets Bahrain government websites amid Israel-Hamas conflict

+Bahrain +Government +AI-Toufan

- The websites of [Bahrain's](#) Foreign Ministry and Information Affairs Ministry were briefly taken down by a cyberattack. A group calling itself AI-Toufan claimed responsibility, stating the attack was in retaliation for Bahrain's stance on the Israel-Hamas war. The attack included the leak of passport scans of American citizens and a Russian diplomat.

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