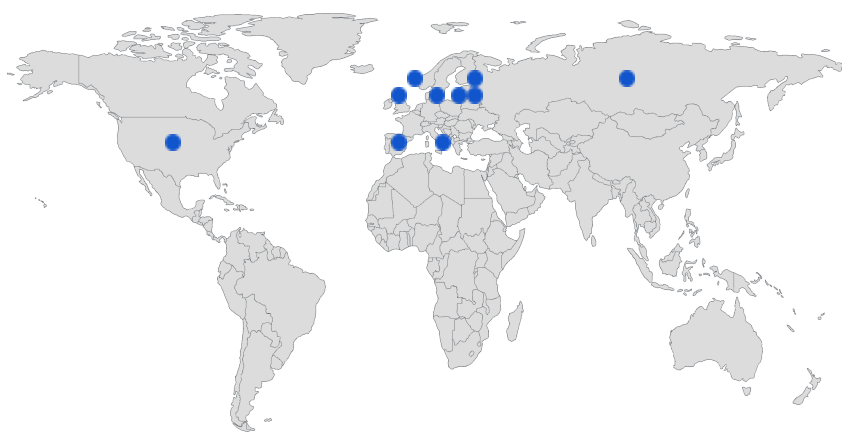


Threat Intel Report: April 29-May 5, 2024

Countries



Top Tags

DarkGate

Wpeeper

Cuttlefish

Goldoon

Cyber-Partisans

Executive Summary

Actionable Information:

- **Innovative Malware Deployment:** The use of common tools and platforms such as AutoHotkey, WordPress, and Docker indicates a trend where threat actors adapt mainstream software for malicious purposes. Monitoring and securing these tools is critical to prevent their misuse.
- **Persistent and Sophisticated Attacks:** Ongoing DDoS attacks against media outlets and novel CPU attacks demonstrate the persistence and sophistication of threats, necessitating advanced defensive strategies and real-time threat intelligence.
- **Exploitation of Old and New Vulnerabilities:** Both old vulnerabilities in D-Link devices and new vulnerabilities in R programming and Intel processors are being actively exploited, showing the importance of comprehensive vulnerability management that includes both patching and monitoring for unusual activity.
- **Increasing Use of Malware in Espionage and Data Theft:** The discovery of Cuttlefish malware targeting routers for credential theft and the extensive use of malware in the DarkGate campaign highlight the growing use of malware for espionage and comprehensive data theft.

Outlook:

The current landscape of cyber threats is characterized by an increase in the complexity and variety of attack vectors. Malware continues to evolve, leveraging both new techniques and older vulnerabilities that remain unpatched. The use of legitimate platforms and software by attackers to deploy malware presents a particularly challenging issue, as it exploits the trust and widespread use of these technologies. In response, organizations must enhance their cybersecurity frameworks to not only focus on preventive measures but also invest in detection and response.



capabilities. This includes adopting advanced security technologies, increasing cyber hygiene awareness among employees, and collaborating with global cybersecurity communities to share threat intelligence. Looking forward, we anticipate further sophistication in attacks, particularly those aimed at critical infrastructure and high-value targets, necessitating a proactive and dynamic approach to cybersecurity.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

📈 4% [CVE-2024-27199](#)

- A path traversal vulnerability in JetBrains TeamCity

📈 5% [CVE-2023-35082](#)

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

📈 7% [CVE-2023-35078](#)

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

Italian Telecommunications Site Hit By Credential Stuffing Attack

+Italy +UK +Telecommunications +ATO

- This week, an Italian telecommunications company experienced an account takeover attack reaching a collective 13M login attempts in just two days. The attack, which was primarily credential stuffing, came mostly from the UK.

Spanish Financial Site Targeted By Nordic-Based Attacks

+Spain +US +Norway +Finland +Denmark +RCE +SQLi +Protocol Manipulation +XSS

- A Spanish financial site was targeted by a large attack leveraging remote code execution (RCE), SQL injection (SQLi), protocol manipulation, and cross-site scripting (XSS) recently, leveraging about 3,300 distinct IPs. The attack primarily came from bots based in the US and several Nordic countries, including Norway, Finland, and Denmark.

Recent Cyber Threats

AutoHotkey Used in DarkGate Malware Campaign

+DarkGate +AutoHotkey +Malware

- Researchers have uncovered a new infection method employed by [DarkGate malware](#), which uses the AutoHotkey scripting language to evade Microsoft Defender SmartScreen. This malware, offered as Malware-as-a-Service (MaaS), includes capabilities like keylogging and data theft, highlighting its evasion sophistication.

Persistent DDoS Threats Against Russian Media

+Russia +Latvia +Journalism

- The Russian independent news outlet [Meduza](#) has been hit by intense DDoS attacks even after the Russian presidential elections, with attacks increasing in both scale and complexity. Meduza, which operates from Latvia due to censorship in Russia, attributed these ongoing cyber assaults to Russian governmental forces.

Novel Attacks on Intel Processors Expose Risks

+Intel +CPU

- Researchers have disclosed two new types of attacks targeting the branch predictor in [Intel processors](#), potentially affecting billions of devices. These sophisticated attacks, revealed at the ACM ASPLOS Conference, underscore significant vulnerabilities in Intel CPUs, leading to actions from Intel and AMD to address these security issues.

R Programming Language Fixes Severe Code Execution Bug

+CVE +R +Code Execution

- A critical arbitrary code execution vulnerability in the R programming language, identified as [CVE-2024-27322](#), was patched in the latest update. The flaw involved deserialization of data in a way that could allow execution of malicious code through RDS files or poisoned R packages, posing a significant threat to data integrity and security.

Wpeeper Malware Uses WordPress for Command and Control

+Malware +Wpeeper +WordPress

- The new [Wpeeper Android](#) malware utilizes hacked WordPress sites to hide its command and control (C2) servers. This novel method makes it challenging to trace back to the malware's actual communication endpoints. Wpeeper has already infected thousands of devices by presenting itself on fake app stores mimicking legitimate ones like Uptodown.

Millions of Docker Repositories Compromised with Malware

+Docker +Malware +Phishing

- Researchers have identified nearly 20% of [Docker Hub repositories](#) to be spreading malware and phishing scams. These imageless repositories serve as a front for malicious activities, embedding harmful metadata that deceives users into visiting compromised or malicious sites. This large-scale compromise shows significant misuse of Docker's platform, affecting millions of users globally.

Cuttlefish Malware Targets Routers for Credential Theft

+Cuttlefish +Malware +Turkey

- [Cuttlefish malware](#) exploits enterprise and SOHO routers to monitor and steal authentication data from network traffic. Active since at least July 2023, this malware uses proxy or VPN tunnels to exfiltrate data stealthily and has been actively infecting systems primarily in Turkey. It uses complex techniques like DNS and HTTP hijacking to facilitate further malicious activities.

Goldoon Botnet Exploits Old D-Link Vulnerability

+Goldoon +Botnet +CVE

- Researchers have reported a resurgence of the [CVE-2015-2051](#) vulnerability in D-Link devices being exploited by a new botnet named [Goldoon](#). This botnet enables remote attackers to take over devices, launching further attacks such as DDoS. The malware associated with this botnet has been engineered to avoid detection and ensure persistence on compromised devices.

Data Breaches

Belarusian KGB Website Compromised by Hacktivists

+Belarus +Government +Hacktivism +Cyber-Partisans

- [Belarus' main security service](#), the KGB, experienced a prolonged website outage lasting two months due to a cyberattack by the Belarusian Cyber-Partisans. This group, composed of exiled Belarusian tech specialists, claims to oppose President Lukashenko's regime. They leaked data including the personal details of over 8,600 KGB agents and published sensitive server logs and administrator details online, aiming to expose and disrupt operations within the Belarusian government.

Data Breach Lawsuit Hits Maine Accounting Firm BerryDunn

+US +Financial Services +Third-Party

- [BerryDunn](#), a Portland-based accounting firm, faces multiple lawsuits following a data breach impacting 1.1 million individuals. The exposed information includes names and Social Security numbers. This breach, attributed to a third-party vendor mishap, has sparked significant legal action, underscoring the critical need for stringent data security measures in third-party partnerships.

Massive Data Breach Affects Over 1 Million NYC Students

+US +Government +Education +Third-Party

- In New York City, a cyberattack on a former software vendor for the [Department of Education](#) has now been found to affect over 1 million current and former students. The breach- initially reported to impact around 800,000 individuals- has grown, prompting the DOE to offer two years of free credit monitoring and identity protection services. The compromised information includes student names, birth dates, ethnicities, academic records, and school enrollments.

UnitedHealth Faces Senate Over Security Lapses Leading to Data Breach

+US +Healthcare +MFA

- [UnitedHealth's](#) CEO testified before the U.S. Senate, revealing that a lack of multifactor authentication allowed hackers to breach its subsidiary, Change Healthcare. The incident led to the theft of over six terabytes of sensitive data, including medical records, affecting a vast number of patients and healthcare professionals. UnitedHealth has since paid a \$22 million ransom, but sensitive patient records have surfaced on the dark web, highlighting the ongoing challenges and significant costs associated with cybersecurity in healthcare.

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