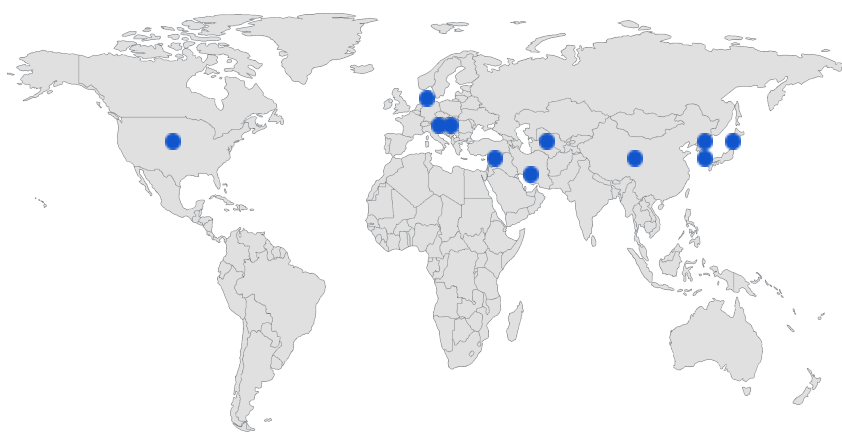


Countries



Top Tags

Rhysida

ALPHV

Qilin

Lazarus Group

Cyber Avengers

Executive Summary

Actionable Information:

- *Advanced persistent threats (APTs):* Government entities, particularly in Afghanistan, are being targeted by sophisticated APTs using tools like HrServ web shells, indicating a rise in state-sponsored cyber espionage.
- *Privilege escalation and zero-day exploits:* Flaws in widely used platforms like Google Workspace and Chrome are being exploited for unauthorized access and privilege escalation, emphasizing the need for continuous monitoring and rapid patching.
- *Ransomware trends:* The healthcare sector, as seen with Henry Schein, and critical infrastructure like energy and utilities, are increasingly targeted by ransomware groups like Rhysida and Daixin Team. This trend highlights the need for robust cybersecurity defenses in these sectors.
- *Supply chain attacks:* The Lazarus Group's new strategy targeting software flaws in supply chains, as seen in South Korea, underscores the growing threat to global supply chains.
- *Third-party risks:* Incidents like the Dollar Tree data breach via a service provider stress the importance of securing third-party connections and vendor risk management.

Outlook:

The current landscape of cyber threats reveals a diverse range of sophisticated attacks targeting critical sectors and infrastructure. State-sponsored activities, particularly APTs, are increasingly focusing on government and defense-related targets, leveraging advanced tools and techniques. The rise in ransomware attacks against healthcare and energy sectors signifies a worrying trend where attackers capitalize on the critical nature of these services. Additionally, the exploitation of vulnerabilities in widely used software and platforms points to an urgent need for organizations to prioritize cybersecurity hygiene, including regular updates and patches. Supply chain attacks and

third-party vulnerabilities remain significant concerns, highlighting the interconnected nature of cyber risks in the modern digital ecosystem. Overall, the outlook calls for heightened vigilance, proactive defense strategies, and collaborative efforts to mitigate these evolving cyber threats.

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

📈 94% [CVE-2022-22965](#)

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

📈 20% [CVE-2023-35078](#)

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

Irish-originating attack targets Israel military site

+Israel +Government +RCE

- An Israeli military site was targeted this week with attempted remote code execution attacks. Attack attempts came primarily from Ireland, with only 232 IPs involved. Given the location, target, and limited scope of the attack, this was almost certainly attempted hacktivism as part of the Israel-Palestine conflict.

US education site under attack

+US +Education +RCE +SQLi

- A US education site was hit this week with attempted remote code execution and SQL injection attacks at rates 1100% above average. Attacks came from almost 65,000 US-based IP addresses.

Recent Cyber Threats

APT attack targets Afghan government with web shell

+Afghanistan +Government

- A new web shell named HrServ, part of a suspected APT attack, targeted an unspecified government entity in [Afghanistan](#). The web shell, embedded in a DLL named "hrrserv.dll," exhibits sophisticated features like custom encoding methods for client communication and in-memory execution.

Google Workspace's domain-wide delegation flaw exposed

+Privilege escalation

- Researchers discovered a design flaw in [Google Workspace's](#) Domain-Wide delegation feature, named DeleFriend, which could enable privilege escalation and unauthorized access to Workspace APIs without Super Admin privileges. This flaw poses a significant risk to organizations using Google Workspace, highlighting the need for vigilant security practices.

Critical vulnerability in Ray AI framework allows OS access

+AI

- A critical vulnerability in the [Ray](#) open-source AI framework, identified as [CVE-2023-48023](#), could allow attackers to gain operating system access to all nodes. This flaw, due to inadequate authentication enforcement, poses a significant threat to users of the Ray AI framework, emphasizing the importance of timely security updates.

Google Chrome zero-day under active exploitation

+Zero-day

- [Google Chrome](#) experienced a zero-day vulnerability, tracked as [CVE-2023-6345](#), which was actively exploited in the wild. This high-severity integer overflow bug in the Skia graphics library underscores the ongoing challenges in protecting widely used software from sophisticated cyber threats.

Latest variant of DJVU ransomware spreads via cracked software

+DJVU +Xaro +Ransomware

- The DJVU ransomware strain's new variant, [Xaro](#), is being distributed through cracked software. This variant encrypts files and demands ransom, posing a significant threat to users downloading software from untrusted sources.

Zoom Rooms service accounts vulnerability exploited

+Zoom

- A vulnerability in [Zoom Rooms service accounts](#) could have been exploited to gain unauthorized access to Zoom tenants. An attacker could use the account to gain access to confidential information in Team Chat, Whiteboard, and other Zoom applications.

SugarGh0st RAT targets Uzbekistan and South Korea

+SugarGh0st +Uzbekistan +South Korea

- Researchers discovered a malicious campaign, likely starting in August 2023, delivering a new remote access trojan (RAT) dubbed [SugarGh0st](#). This likely Chinese campaign targeted the Uzbekistan Ministry of Foreign Affairs and users in South Korea, indicating a significant threat to governmental and individual cybersecurity.

LogoFAIL attacks exploit EFI bootkits

+UEFI +LogoFAIL

- Multiple security vulnerabilities, collectively named [LogoFAIL](#), affect image-parsing components in EFI code from various vendors. These vulnerabilities could be exploited to hijack the booting process and deliver bootkits, posing a significant threat to the integrity of the booting process in various devices.

ChatGPT's training data exposed

+AI

- Researchers discovered a simple technique to extract training data from [ChatGPT](#), including personal information. By prompting ChatGPT to repeat certain words indefinitely, the AI began to output memorized data, raising significant privacy concerns.

Lazarus Group's new supply chain attack strategy

+Lazarus Group +North Korea +South Korea

- The [Lazarus Group](#), linked to North Korea, exploited a zero-day flaw in MagicLine4NX software to launch supply chain attacks, codenamed Operation Dream Magic. The attacks, primarily targeting South Korean organizations, involved a watering hole technique and aimed at data exfiltration and system control.

Serbian government critics targeted by advanced spyware

+Serbia +Government +Spyware

- Pro-democracy activists in [Serbia](#) were targeted with military-grade spyware, suspected to be Pegasus, sold by NSO Group. The attacks, which were unsuccessful due to updated iOS software on the victims' iPhones, are part of a concerning trend of state-sponsored surveillance against political critics.

Japan's space agency hit by cyberattack

+Japan +Government +Aerospace

- [Japan's Space Exploration Agency](#) (JAXA) reported a cyber incident suspected to involve a breach in its Active Directory. The agency had to shut down parts of its network for investigation. This incident adds to JAXA's challenges, both in cyberspace and space missions, highlighting the growing cyber threats in the aerospace sector.

Data Breaches

General Electric's development environment compromised

+Engineering

- [General Electric](#) is investigating a breach in their development environment by a threat actor named IntelBroker, who claims to have stolen sensitive data, including military information.

Iranian-backed cyber group targets Pennsylvania Water Authority

+Iran +US +Utilities +Cyber Avengers

- The [Municipal Water Authority](#) of Aliquippa, Pennsylvania, was hacked by an Iranian-backed cyber group, Cyber Av3ngers. The attack targeted a booster station but did not compromise the water supply.

Rivers Casino suffers major data breach

+Gambling

- [Rivers Casino Des Plaines](#) reported a cyber incident where fraudsters stole sensitive customer and employee information, including social security and driver's license numbers.

Rhysida ransomware targets multiple energy giants

+Rhysida +China +Slovenia +Energy

- The Rhysida ransomware group claimed to have hacked [China Energy Engineering Corporation](#), stealing a large amount of sensitive data. The group is auctioning the data for 50 BTC and threatens to release it publicly.
- [Holding Slovenske Elektrarne](#), Slovenia's largest power generation company, suffered a ransomware attack that encrypted files but did not disrupt power production. The attack, also attributed to the Rhysida ransomware group, emphasizes the cyber vulnerabilities of critical energy infrastructure.

Daixin Team claims attack on Texas municipal water district

+Daixin Team +US +Utilities

- The Daixin Team group claims to have hacked the [North Texas Municipal Water District](#), threatening to leak stolen data including internal documents and personnel details. The ransomware gang claims the theft of board meeting minutes, internal project documentation, personnel details, audit reports, and more.

Henry Schein targeted by ALPHV ransomware twice

+Healthcare +ALPHV

- [Henry Schein](#), a major healthcare company, reported two cyberattacks by the ALPHV ransomware gang, one in October and another in November. The attacks disrupted their systems and led to the theft of 35 terabytes of sensitive data, demonstrating the persistent threat of ransomware in the healthcare sector.

Prolonged espionage campaign against chipmaker NXP

+Netherlands +Technology +China +Chimera

- [NXP](#), a Netherlands-based chipmaker, was infiltrated by the Chinese espionage group Chimera for over two years. The hackers looted sensitive information, including chip designs, without detection.

Qilin ransomware strikes automotive supplier Yanfeng

+Qilin +Automotive

- [Yanfeng Automotive Interiors](#), a leading automotive parts supplier, was attacked by the Qilin ransomware group. The breach affected major automakers and disrupted production at Stellantis' North American plants, underscoring the growing cyber threats in the global automotive supply chain.

Dollar Tree affected by third-party data breach

+Retail +US

- A significant data breach at Zeroed-In Technologies, a service provider for [Dollar Tree](#), led to the exposure of personal information of nearly 2 million individuals. This incident, which involved sensitive data of Dollar Tree and Family Dollar employees, underscores the vulnerability of retail chains to cyber incidents involving third-party vendors.

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