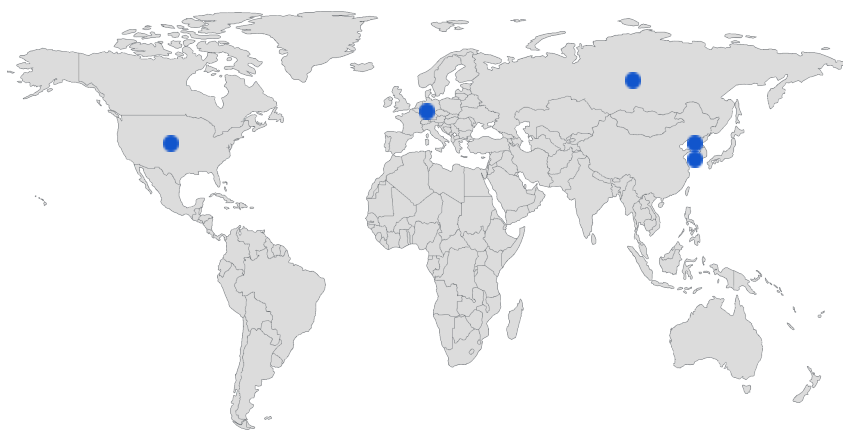


Threat Intel Report: May 13-19, 2024

Countries



Top Tags

FIN7

LockBit

Black Basta

Ebury

Turla

Executive Summary

Actionable Information:

- *Increased Use of Legitimate Platforms for Malicious Activity:* Cybercriminals are exploiting trusted platforms like Google Ads, cloud storage, and social media to distribute malware and conduct malicious activities. This trend makes malicious links and files appear more legitimate and harder to detect, increasing the success rate of attacks.
- *Sophisticated Techniques to Evade Detection:* There is a growing use of advanced methods like steganography (embedding malware within images) and remote code execution exploits. These techniques allow attackers to bypass traditional security measures, emphasizing the need for advanced and adaptive detection technologies.
- *Persistent and Evolving Ransomware Threats:* Ransomware campaigns, such as those by LockBit Black and Black Basta, are employing large-scale phishing and social engineering tactics to maximize infection rates. These campaigns highlight the importance of comprehensive email security solutions and continuous user education to recognize and avoid phishing attempts.
- *Targeted Attacks on Critical Sectors:* Healthcare, technology, and government sectors are frequently targeted, with significant breaches leading to severe operational and financial impacts. This underscores the necessity for sector-specific cybersecurity strategies and robust protection of critical infrastructure.
- *Exploitation of Vulnerabilities in Widely Used Technologies:* Vulnerabilities in commonly used devices and software, such as D-Link routers and GE ultrasound devices, are being actively exploited. Immediate patching and vulnerability management are crucial to prevent exploitation and ensure system integrity.

Outlook:

The recent trends in cyber threats and data breaches reveal a landscape marked by increasing sophistication and scale. Cybercriminal groups like FIN7 and LockBit Black are adopting more legitimate-looking methods, such as leveraging Google Ads and personalized phishing emails, to deceive targets and spread malware. The use of steganography and exploitation of zero-day vulnerabilities further complicate detection and defense efforts. Healthcare, technology, and government sectors remain prime targets, with significant breaches impacting essential services and sensitive data.

As state-sponsored and financially motivated cybercriminals continue to evolve their tactics, the need for proactive and comprehensive cybersecurity strategies becomes more urgent. Enhanced user awareness, advanced threat detection technologies, and stringent data protection measures are critical in mitigating the impact of these threats. The ongoing adaptation of attack methods by adversaries suggests that organizations must remain vigilant and adaptive in their cybersecurity defenses to protect against the ever-changing threat landscape.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 35% [CVE-2024-27199](#)

- A path traversal vulnerability in JetBrains TeamCity

↓ 6% [CVE-2023-35078](#)

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

↓ 7% [CVE-2023-35082](#)

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

German Automotive Site Under Bot Attack

+Germany +Automotive +Bad Bots

- A German automotive site was targeted this week by bad bots in an almost 4M request attack. The attack came from IPs based in Germany, and targeted URLs connected to credentials and access management, as well as attempting to fingerprint the site's technology stack.

US Retail Site Targeted by ATO

+US +Retail +ATO +API

- A United States retail site was hit this week with an attempted account takeover (ATO) attack, reaching 2M malicious logins over two days. The credential stuffing attack, coming entirely from the Netherlands, targeted an API site.

Recent Cyber Threats

FIN7 Utilizes Google Ads for Malicious Payload Distribution

+FIN7

- The [FIN7](#) cybercriminal group has adopted a new tactic, leveraging trusted brand names and sponsored Google ads to distribute malicious MSIX payloads. By purchasing Google ads, FIN7 can make their malicious links appear

legitimate to unsuspecting users. This strategy increases their reach and the likelihood of successful malware installations, posing significant risks across multiple industries globally.

Steganography Employed in Malicious Go Binary via PyPI

+Go +PyPI

- Cybercriminals are now embedding [malicious Go binaries](#) within images using steganography, specifically targeting the Python Package Index (PyPI) as their distribution platform. This sophisticated method allows attackers to conceal malware within seemingly innocuous files, making detection by traditional security measures challenging. Developers who download these compromised packages face the risk of inadvertently executing malicious code, which could compromise their systems and data integrity.

LockBit Black Ransomware Campaign via Email

+LockBit Black

- A widespread phishing campaign has been identified, distributing [LockBit Black](#) ransomware via millions of email messages. This campaign targets a broad range of industries, exploiting the high volume of emails to maximize infection rates. The LockBit Black ransomware is known for its encryption capabilities and ransom demands, which can cause severe operational and financial damage to affected organizations. The scale and impact of this campaign highlight the persistent threat of ransomware to global enterprises.

Black Basta Ransomware Operators' Social Engineering Campaign

+Black Basta

- The [Black Basta](#) ransomware group has been linked to an ongoing social engineering campaign that targets multiple industries. This campaign employs sophisticated tactics, such as personalized phishing emails, to deceive recipients into compromising their systems. Once access is gained, the ransomware is deployed, encrypting valuable data and demanding ransom payments. This highlights the need for enhanced cybersecurity awareness and training to mitigate such threats, as well as the importance of implementing advanced email security measures to detect and block phishing attempts.

Ebury Malware Compromises 400,000 Linux Servers

+Ebury +Linux

- Researchers have discovered that the [Ebury](#) malware, previously thought dormant, has compromised approximately 400,000 Linux servers worldwide. This malware is used to steal SSH credentials and redirect network traffic, facilitating cryptotheft and other financial crimes. The large-scale compromise underscores the ongoing threat to Linux server environments and the importance of robust security practices.

RCE Zero-Day Exploit in D-Link EXO AX4800 Routers

+RCE +Routers

- A proof-of-concept (PoC) exploit has been released for a remote code execution (RCE) zero-day vulnerability in [D-Link EXO AX4800 routers](#). This critical flaw allows attackers to execute arbitrary code remotely, potentially gaining full control over the affected devices. Users of these routers are urged to apply available patches immediately to mitigate the risk of exploitation.

Russian Cybercriminals Exploit Legitimate Services for Malicious Activities

+Russia

- [Russian cybercriminals](#) are increasingly using legitimate services to conduct malicious activities. These services include cloud storage, social media platforms, and online communication tools, which they exploit to evade detection and enhance the effectiveness of their attacks. The misuse of legitimate services by these actors complicates efforts to identify and mitigate threats, highlighting the need for enhanced monitoring and security measures.

Multiple Vulnerabilities Found in GE Ultrasound Devices

+Healthcare

- A recent report identified 11 vulnerabilities in [GE ultrasound devices](#), which could be exploited by attackers to gain unauthorized access, alter device functionality, or compromise patient data. These vulnerabilities pose significant

risks to healthcare providers, emphasizing the need for immediate remediation and robust security measures to protect medical devices and sensitive patient information.

Quick Assist Misused in Social Engineering Leading to Ransomware

+Social Engineering

- Threat actors are misusing [Microsoft's Quick Assist](#) tool in social engineering attacks that lead to ransomware infections. By convincing victims to use Quick Assist, attackers gain remote access to their systems, allowing them to deploy ransomware and encrypt critical data. This tactic underscores the importance of user awareness and caution when receiving unsolicited assistance requests.

Data Breaches

Newsquest Media Group Websites Defaced in Cyber Attack

+UK +Journalism

- The websites of [Newsquest Media Group](#), a prominent British newspaper publisher, were defaced in a recent cyber attack. The attackers replaced website content with unauthorized messages, causing significant disruption to the publisher's online presence. The motive behind the attack remains unclear, and efforts are underway to restore normal operations and strengthen security measures.

NHS Ransomware Attack Linked to Arcserve UDP Vulnerability

+UK +Arcserve

- The recent ransomware attack on the UK's [National Health Service](#) (NHS) was traced to vulnerabilities in Arcserve's UDP backup software. Attackers exploited these weaknesses to gain access to the network, leading to significant disruptions in healthcare services. This incident highlights the critical importance of securing backup solutions, especially in sectors as vital as healthcare, to prevent similar attacks in the future. Ensuring robust cybersecurity measures for backup and recovery systems is essential to safeguard against ransomware threats.

Turla Suspected in European Government Malware Attack

+Turla +Government

- [Turla](#), a suspected Russian state-sponsored hacking group, is believed to be behind a backdoor malware attack targeting a European government. The malware allows remote access and data exfiltration, posing a significant threat to national security. This incident highlights the persistent threat posed by state-sponsored actors to government institutions.

Kimsuky Hackers Deploy New Linux Backdoor in South Korea Attacks

+Kimsuky +South Korea +North Korea

- The [Kimsuky](#) hacking group has deployed a new Linux backdoor in attacks targeting South Korean entities. This backdoor allows attackers to maintain persistent access and execute commands on compromised systems. The campaign underscores the ongoing cyber threat from North Korean-linked groups and the need for vigilant cybersecurity defenses.

WebTPA Data Breach Impacts 2.4 Million Insurance Policyholders

+Healthcare

- A data breach at [WebTPA](#), a third-party administrator for insurance companies, has exposed the personal information of 2.4 million insurance policyholders. The compromised data includes names, Social Security numbers, and health information. The breach highlights the risks associated with third-party service providers and the importance of stringent data protection measures.

OmniVision Discloses Data Breach Following Ransomware Attack

+Technology & Manufacturing

- [OmniVision](#), a leading image sensor manufacturer, has disclosed a data breach following a ransomware attack in 2023. The breach resulted in the exposure of sensitive data, including personal information and intellectual property. This incident emphasizes the growing threat of ransomware to high-tech companies and the need for comprehensive cybersecurity strategies.

MediSecure Ransomware Attack Disrupts Medical Services

+Healthcare +Software +Australia

- [MediSecure](#), an Australian medical software provider, suffered a ransomware attack that disrupted its services. The attack affected the company's ability to provide electronic prescription services, impacting healthcare providers and patients. The incident underscores the critical need for robust cybersecurity measures in the healthcare sector to ensure the continuity of essential services.

Tri-City Herald Data Breach Affects Thousands of Customers

+US +Journalism

- [The Tri-City Herald](#), a local newspaper in Washington state, experienced a data breach affecting thousands of its customers. The breach exposed personal information, including names and contact details. The incident highlights the ongoing cyber threat to media organizations and the importance of protecting customer data.

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