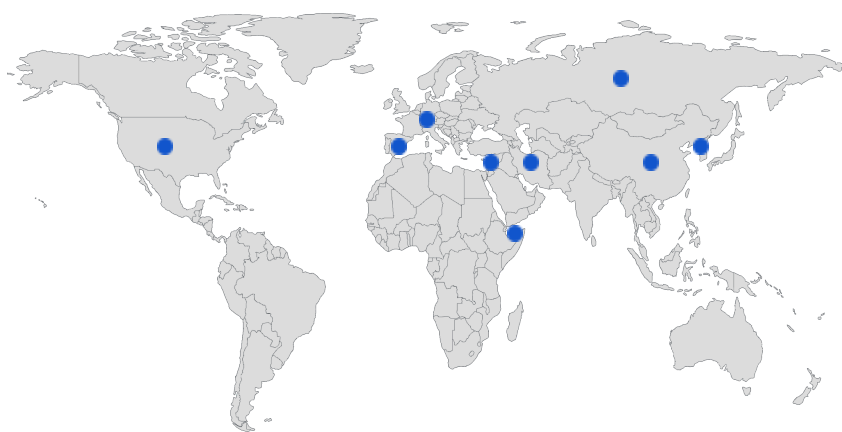


Threat Intel Report: February 19-25, 2024

Countries



Top Tags

LockBit

CharmingKitten

ALPHV

Cactus

Black Basta

Executive Summary

Actionable Information:

- **Global Law Enforcement Success:** The international crackdown on the LockBit ransomware group underscores the effectiveness of coordinated law enforcement efforts in combating cyber threats. Organizations should remain vigilant and ready to collaborate with authorities.
- **Emerging Threats and Vulnerabilities:** The discovery of the MonikerLink bug in Microsoft Outlook highlights the critical need for timely software updates and patch management, and the introduction of M.O.R.E ransomware and a macOS backdoor developed in Rust signals a diversification in attack vectors, emphasizing the need for cross-platform security solutions. Additionally, VoltSchemer's exploitation of wireless chargers as attack vectors and SSH-Snake's network propagation capabilities underscore the importance of securing both hardware and network infrastructure.
- **Targeted Cyber-Espionage:** The activities of state-aligned groups like Charming Kitten and TAG-70, targeting specific geopolitical interests, underscore the necessity for sector-specific threat intelligence and defense strategies.
- **Ransomware and Data Breaches:** Incidents involving ALPHV, Cactus ransomware, and the Wyze camera breach highlight the ongoing risk of ransomware and the need for robust data protection and incident response plans.

Outlook:

The current cybersecurity landscape is characterized by an increasing sophistication of threat actors, leveraging both technological vulnerabilities and geopolitical tensions to conduct espionage, disrupt services, and steal sensitive data. The rise in cross-platform malware and the use of innovative attack vectors, such as exploiting wireless charging

technology, indicate that threat actors are continually evolving their tactics to bypass traditional security measures. As such, organizations must adopt a proactive and comprehensive security posture, integrating advanced threat detection, response capabilities, and cybersecurity awareness training to mitigate these risks. Looking ahead, the collaboration between private sector entities and law enforcement will be crucial in dismantling threat actor infrastructure and disrupting cybercriminal activities. Additionally, the focus on securing emerging technologies and addressing supply chain vulnerabilities will be paramount in preventing future attacks and safeguarding global digital infrastructure.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 34% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

↓ 1% [CVE-2023-35078](#)

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

↑ 2% [CVE-2023-35082](#)

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

Spanish Financial Site Targeted in ATO Attack

+Spain +Financial Services +ATO

- A Spanish financial site saw an attempted account takeover (ATO) attack this week. The attack came primarily from within Spain and leveraged over 294,000 IPs. 63% of the logins in this attack came from previously compromised login information.

Israel Financial Site Hit By DDoS

+Israel +Financial Services +DDoS

- A frequently targeted Israeli insurance site was hit this week with a DDoS attack reaching over 800K requests per second (RPS). This attack came from about 2,000 IPs, primarily in the US and Brazil.

Recent Cyber Threats

Global Crackdown Disables LockBit Ransomware Operations

+LockBit

- A coordinated international law enforcement effort has significantly disrupted the [LockBit](#) ransomware group. This operation, named Operation Cronos, seized the group's infrastructure, dark-web sites, and obtained crucial data on its members, effectively rendering LockBit inoperative. LockBit, known for attacking thousands of entities worldwide and causing billions in damages, has been one of the most harmful ransomware groups in recent years. The crackdown also led to arrests and sanctions against group members, although the group has since attempted to [resurface](#).

Exploiting Outlook with MonikerLink

+MonikerLink +Microsoft

- A critical bug named [MonikerLink](#) has been discovered in Microsoft Outlook, allowing attackers to execute malware through specially crafted emails. This vulnerability poses a significant threat as it can bypass traditional security measures, potentially leading to unauthorized data access and system control. Microsoft has issued patches, urging users to update their systems promptly to mitigate the risk.

Charming Kitten's BASICSTAR Backdoor Targets Middle East Experts

+CharmingKitten +BASICSTAR +Iran

- Iranian cyberespionage group [Charming Kitten](#) employs a new backdoor, BASICSTAR, targeting Middle East policy experts through fake webinar portals. This campaign, linked to Iran's Islamic Revolutionary Guard Corps, aims to harvest sensitive information from compromised hosts.

M.O.R.E: A Cross-Platform Ransomware Menace

+M.O.R.E +Ransomware +MacOS +Windows +Linux

- The dark web introduced [M.O.R.E](#) (Multi OS Ransomware Executable), a tool claiming swift encryption across Windows, MacOS, and Linux systems. This development signifies an evolution in ransomware threats, targeting a broader range of operating systems for more extensive impact.

New macOS Rust-Based Backdoor Linked to Ransomware Operators

+Rust +MacOS +Malware

- Security researchers have uncovered a new backdoor affecting MacOS systems, uniquely developed in the [Rust](#) programming language. This discovery suggests a potential link between the backdoor's operators and a known Windows ransomware group. The backdoor exhibits capabilities that could allow attackers to execute arbitrary code and maintain persistent access on infected MacOS devices.

VoltSchemer Leverages Wireless Chargers as Attack Vectors

+VoltSchemer

- Newly discovered [VoltSchemer](#) attacks exploit wireless chargers to inject voice commands or cause physical damage to devices by leveraging the charger's magnetic field. This innovative attack vector showcases the potential security risks associated with wireless charging technology.

SSH-Snake: New Network Mapping Tool Discovered

+SSH-Snake +Worm

- [SSH-Snake](#) is a self-modifying worm that uses SSH credentials found on compromised systems to propagate through networks. Released on January 4, 2024, it actively searches for credentials in known locations and shell history files, initiating connections with command and control locations to facilitate further malicious activities.

KONNI Malware Compromises Russian Consular Software

+KONNI +North Korea +Russia +Malware

- A malware sample, uploaded to VirusTotal in mid-January 2024, has been linked to North Korea and targets the Russian Ministry of Foreign Affairs. The malware, identified as [KONNI](#), has been used in similar activities since 2014. It was found within a backdoored installer for software presumably used internally by the Russian Ministry of Foreign Affairs, specifically for consular report management.

Rhadamanthys Stealer Phishing Campaign Hits Oil & Gas Industry

+Rhadamanthys Stealer +Phishing +Oil & Gas

- A sophisticated phishing campaign is targeting the oil and gas sector with [Rhadamanthys Stealer](#), a Malware-as-a-Service (MaaS) information stealer. Following the recent takedown of the LockBit ransomware group, this campaign utilizes the newly updated Rhadamanthys Stealer to bypass secure email gateways, employing tactics that lead victims through several redirects to download the malware from a GitHub repository.

Hackers Target Israeli El Al Flights in Mid-Air Hijack Attempt

+Israel +Somaliland +Aviation

- Israel's [El Al](#) airline claims hackers attempted to hijack the communication networks of two flights from Thailand to Israel, aiming to divert the aircraft. The incidents involved flights from Phuket and Bangkok to Ben-Gurion Airport, with pilots receiving false instructions from "hostile elements" suspected to be based in Somaliland. The pilots, suspecting foul play, switched communication channels to verify their routes, allowing the flights to continue safely.

Data Breaches

Chinese Contractor iSoon Leaks Sensitive Documents

+China +Government

- Internal documents leaked from [iSoon](#), a Chinese hacking contractor, reveal a disaffected workforce involved in hacking operations for the Ministry of Public Security. The leaked documents include technical details about malware and command-and-control infrastructure, indicating iSoon's involvement in cyber-espionage activities targeting regional governments and possibly NATO.

ALPHV Ransomware Targets LoanDepot and Prudential Financial

+ALPHV +Financial Services

- The [ALPHV](#) ransomware gang has claimed responsibility for breaching the networks of Prudential Financial and LoanDepot, placing them on its dark web leak site. The incident at LoanDepot resulted in the theft of personal information of at least 16.6 million individuals. Prudential Financial also reported a breach that compromised employee and contractor data, though customer data was not believed to be affected.

Russia-Linked Hackers Target Embassies for Espionage

+TAG-70 +Russia +Iran +Europe +Government

- A Russia-aligned hacking group, tracked as [TAG-70](#), exploited a vulnerability in the Roundcube webmail server to conduct espionage against European government and military agencies, as well as Iranian embassies in Russia. The campaign aimed to collect intelligence on European political and military activities.

Cactus Ransomware Gang Hits Schneider Electric

+Cactus +Electricity

- The [Cactus](#) ransomware gang has claimed to have stolen 1.5TB of data from Schneider Electric, an energy management and industrial automation firm. The breach, which initially seemed to affect Schneider Electric's Sustainability Business division, led to outages on the Resource Advisor cloud platform. The gang has published a sample of the allegedly stolen data, including passports and company documents, as proof of the hack.

Wyze Camera Breach Exposes 13,000 Users' Camera Feeds

+Security

- A security breach at [Wyze](#) allowed approximately 13,000 users to inadvertently access images and videos from other users' cameras due to a system overload and incorrect device ID mapping. The issue, which occurred during a service restoration process, has prompted Wyze to implement additional security measures, including a new layer of verification before connecting users to event videos.

North Korean Hackers Conduct Defense Sector Supply Chain Attack

+Lazarus +North Korea +South Korea +Germany +Government

- German and South Korean intelligence services have warned of a North Korean cyber-espionage operation targeting the global defense sector. The operation, involving the [Lazarus](#) group, aimed to steal military technology information. The attack exploited a network server of a maritime and shipping technologies research center, using sophisticated techniques for lateral movement and data theft.

FixedFloat Crypto Exchange Hacked

+Crypto

- [FixedFloat](#), a Bitcoin and Ethereum exchange, suffered a wallet-drainer attack resulting in the theft of at least \$26 million worth of cryptocurrencies. The breach led to frozen transactions and missing funds, with the stolen assets being transferred to various addresses before moving to the eXch exchange. FixedFloat has confirmed the external attack and denied any insider involvement.

Hack Affects 24 Million Eye Doctor Patients

+Healthcare

- [Medical Management Resource Group](#) reported a hack affecting nearly 2.4 million patients of its eye doctor practice clients. The November incident compromised sensitive patient information, including contact details, medical records, and for some, Social Security numbers and insurance information. The breach is part of a surge in incidents involving third-party healthcare service providers.

Das Team AG Falls Victim to Black Basta Ransomware

+Recruiting +Black Basta +Switzerland

- [Das Team AG](#), a Swiss job placement agency, confirmed a cyberattack by the Black Basta ransomware group. The attack targeted the company's website, with DAS Team AG working to minimize consequences and informing law enforcement. The breach is part of a trend where recruitment industries become prime targets for cyber threats due to the sensitive data they manage.

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