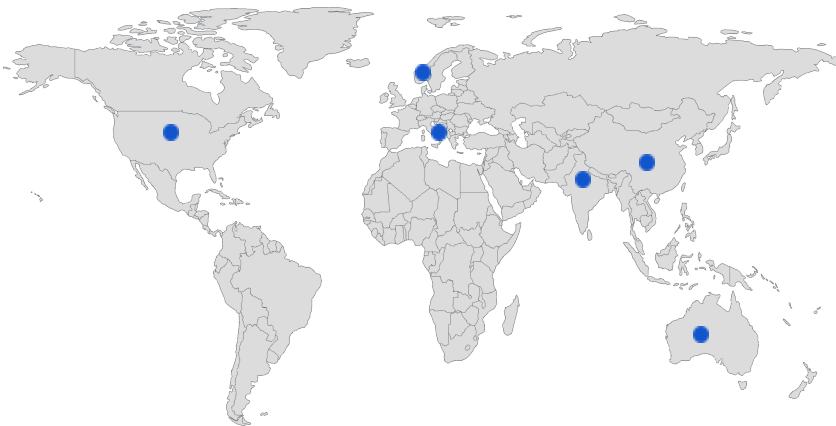


Threat Intel Report: May 20-June 2, 2024

Countries



Top Tags

Grandoreiro

APT41

Unfading Sea Haze

AllaSenha

RansomHub

Executive Summary

Actionable Information:

- *Rising Sophistication of Cyber Threats:* Attackers are increasingly using advanced techniques in malware and social engineering to breach systems. Examples include the Grandoreiro banking trojan and the AllaSenha malware variant, which demonstrate sophisticated evasion and exploitation tactics.
- *Supply Chain and Third-Party Risks:* The critical vulnerabilities discovered in AI and cloud services, such as those in Intel's OpenVINO toolkit and Llama's AI Python package, highlight the importance of securing supply chains and third-party software. The Ticketmaster data breach linked to Snowflake underscores the need for rigorous vendor management and multi-factor authentication.
- *Targeted Attacks on Critical Sectors:* Financial institutions and critical infrastructure are prime targets for sophisticated cyber campaigns, like the CatDDOS botnet and APT41's attacks on Italian industries. The healthcare and hospitality sectors also face significant risks, with breaches at Cencora and UChicago Medicine revealing major vulnerabilities.
- *Evolving Threats to Cloud and E-commerce:* Novel attack methods, such as the Linguistic Lumberjack exploit on cloud services, highlight the need for secure cloud practices. Additionally, the discovery of server-side credit card skimmers in WordPress plugins indicates persistent threats to e-commerce platforms, necessitating ongoing security audits and monitoring.

Outlook:

The landscape of cyber threats continues to evolve with increasing sophistication and targeted attacks across various sectors. The recent discovery of critical vulnerabilities in AI software, coupled with the surge in banking trojans and

malware, underscores the importance of robust cybersecurity measures. As supply chain vulnerabilities and third-party risks become more apparent, organizations must prioritize securing software dependencies and enhancing vendor management practices. The trend towards exploiting cloud services and unverified plugins calls for stringent security audits and proactive defenses. Looking ahead, the emphasis on multi-factor authentication, real-time monitoring, and regulatory compliance will be crucial in mitigating these ever-evolving cyber threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 15% [CVE-2024-27199](#)

- A path traversal vulnerability in JetBrains TeamCity

↑ 103% [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

US Real Estate Company Targeted in CRMEB Attack Attempt

+US +Real Estate +Go +CVE +CRMEB

- A US real estate company was targeted this week in attacks attempting to leverage the vulnerability CVE-2023-30185, which tracks a file upload bug in CRMEB. The attacks, which came from hacking tools written in the Go language, was probably intended to steal sensitive customer data.

US Business Site Targeted by Bad Bots

+US +Business +Bad Bots +Path Traversal

- A US business site was targeted by path traversal and automated attacks this week, coming entirely from US-based IPs. Attacking IPs had an average risk score of 56%, and leveraged vulnerability scanners to conduct these attacks.

Recent Cyber Threats

Critical Bug in Intel AI Model Compression Software

+AI

- Intel has disclosed a critical severity bug in its AI model compression software, specifically in the [Intel Distribution of OpenVINO toolkit](#). The flaw, identified as CVE-2024-22476, stems from improper input validation, or a failure to properly sanitize user input. This vulnerability affects various AI-driven applications across healthcare, automotive, and industrial sectors, posing significant risks to system integrity and data security.

Grandoreiro Banking Trojan Targets Major Financial Institutions

+Grandoreiro +Financial Services

- The [Grandoreiro](#) banking trojan has launched a widespread campaign targeting major financial institutions across Latin America and Europe. The trojan employs advanced social engineering tactics, including phishing emails and malicious macros, to steal credentials and financial information. Once inside a system, Grandoreiro uses remote access tools to exfiltrate data, posing a severe threat to the security of banks and their customers.

AI Python Package Flaw Causes Supply Chain Vulnerabilities

+AI +LLama

- A critical flaw in the widely used AI Python package, [LLama](#), has led to significant supply chain vulnerabilities. Identified as CVE-2024-34359, this flaw comes from the misuse of the Jinja2 template engine in the `llama\_cpp\_python` package, allowing attackers to exploit a hole in the package's use of Jinja2. This vulnerability highlights the importance of securing software dependencies and verifying the integrity of AI models.

Fortinet FortiSIEM Command Injection Vulnerability

+Command Injection +Fortinet

- A critical command injection vulnerability, [CVE-2023-34992](#), has been discovered in Fortinet FortiSIEM. This flaw allows attackers to execute arbitrary commands on affected systems, potentially gaining complete control over FortiSIEM installations. The vulnerability poses serious risks to organizations relying on FortiSIEM for security information and event management, necessitating immediate patching and review of system configurations.

Linguistic Lumberjack: Cloud Services Attack via Logging Endpoints

+Linguistic Lumberjack +Cloud

- A novel attack method dubbed [Linguistic Lumberjack](#) exploits logging endpoints in cloud services via Fluent Bit, identified as CVE-2024-4323. The vulnerability allows attackers to inject malicious payloads through log entries, compromising the security of cloud-based infrastructures. This attack can lead to unauthorized access and data breaches, emphasizing the need for secure logging practices and endpoint protections.

Server-Side Credit Card Skimmer Hidden in Obscure Plugin

+Skimmer +WordPress

- A sophisticated [server-side credit card skimmer](#) has been discovered hidden in an obscure WordPress plugin used by online stores. The skimmer collects credit card details during transactions and sends them to remote servers controlled by the attackers. This discovery highlights the risks of using unverified plugins and underscores the importance of regular security audits for e-commerce platforms.

UserPro Plugin Flaw Enables Account Takeover

+WordPress

- A critical vulnerability in the [UserPro](#) WordPress plugin allows attackers to take over user accounts by exploiting improper input validation. This flaw, identified as CVE-2024-35700, can be used to gain unauthorized access to sensitive information, including personal data and account credentials, by improper handling of a "secret key" used during the password reset process. Prompt updates and security patches are essential to mitigate this risk in web applications.

Spyware Found on Hotel Check-In Computers

+Hospitality +Spyware

- Spyware has been discovered on [hotel check-in computers](#), compromising the personal information of guests. The malware was designed to capture keystrokes and screen data, potentially exposing sensitive information such as credit card details and identification documents. Because of a security flaw in the spyware, these screenshots are available to anyone on the internet, not just the spyware's intended users. This breach highlights the importance of securing point-of-sale systems and implementing stringent cybersecurity measures in the hospitality industry.

CatDDoS Derivative Targets Critical Infrastructure

+CatDDoS +Botnet

- A new derivative of the [CatDDoS](#) botnet has been detected targeting critical infrastructure sectors, including energy and telecommunications. This variant utilizes advanced DDoS attack techniques, such as multi-vector attacks and amplification, to disrupt services and operations. The emergence of this threat underscores the importance of robust DDoS mitigation strategies and real-time monitoring for critical infrastructure systems.

Allasenha Malware Variant Targets Latin America

+Allakore +AllaSenha

- A new variant of the Allakore banking malware, called [AllaSenha](#), is targeting financial institutions in Latin America. This variant leverages Azure-based command-and-control (C2) infrastructure to steal banking credentials and

financial data. Allakore's advanced evasion techniques and targeting of Latin American banks highlight the evolving tactics of cybercriminals and the need for robust cybersecurity defenses in the financial sector.

Hacktivists Target Elections in India

+India +Hactivism +Government +Election

- Hactivist groups have launched cyberattacks targeting the election infrastructure in [India](#), aiming to disrupt the electoral process and undermine public confidence in the system. These attacks include website defacements, data breaches, and distributed denial-of-service (DDoS) attacks. The incidents highlight the growing threat of politically motivated cyberattacks on democratic institutions, emphasizing the need for robust election security measures.

Data Breaches

Snowflake Hack Exposes Massive Amounts of Data

+Snowflake +MFA

- A cyberattack on [Snowflake](#), a data storage company, has resulted in the exposure of data belonging to Ticketmaster and other organizations. According to Snowflake, the personal credentials of a former employee were compromised and used to access demo accounts that were not behind multi-factor authentication, leading to the breach. This has significant implications for customer privacy and security, affecting numerous organizations that rely on Snowflake's services.

Massive Ticketmaster Data Breach Affects 560M Users

+Third Party

- A substantial data breach at [Ticketmaster](#) has resulted in the personal information of 560 million users being put up for sale on the dark web. The breach was facilitated by a vulnerability in a third-party supplier—rumored to be Snowflake—underscoring the risks associated with vendor management. This incident highlights the growing threat of cyberattacks on major entertainment companies and the importance of securing third-party integrations.

APT41-Associated Actors Target Italy, Government Networks

+APT41 +Unfading Sea Haze +KeyPlug +Italy +China

- APT41, a notorious Chinese state-sponsored hacking group, has been targeting Italian industries with a new malware variant known as [KeyPlug](#). This campaign involves sophisticated spear-phishing emails and exploits for known vulnerabilities in industrial control systems. The malware facilitates data exfiltration and espionage activities, posing a significant threat to Italian industrial sectors' intellectual property and operational security.
- A Chinese hacking group known as [Unfading Sea Haze](#), associated with APT41, has been found to have hidden on military and government networks for six years. The attackers used advanced persistent threat (APT) tactics to evade detection, targeting critical infrastructure and extracting sensitive information. This long-term intrusion highlights severe vulnerabilities in critical national defense systems and underscores the need for enhanced cybersecurity measures.

Courtroom Software Backdoored by Hackers

+Backdoor +Government

- Hackers have compromised a popular [courtroom recording software](#), embedding a backdoor that could allow unauthorized access to sensitive legal proceedings. The attackers exploited a vulnerability in the software's update mechanism, potentially affecting numerous court systems worldwide. This breach could have serious implications for the integrity of judicial processes and the confidentiality of court records.

Pharma Partner Cencora Data Breach Exposes Patient Info

+Healthcare

- A data breach at [Cencora](#), a partner in the pharmaceutical industry, has exposed the information of patients on any of over a dozen medicines. The breach was caused by unauthorized access to Cencora's database, compromising

personal health information and potentially affecting patient care. This breach raises concerns about data security within the healthcare sector and the need for stricter compliance with data protection regulations.

Everbridge Data Breach Compromises Corporate Systems

+US +Australia +Norway +Software +Phishing

- [Everbridge](#), a risk intelligence and crisis management software provider, has suffered a data breach that impacted its corporate systems. The attackers gained access to Everbridge's internal network using data obtained in an earlier phishing attack, potentially compromising data from the US Army, Australia, and Norway.

UChicago Medicine Data Breach Leaks Personal Data

+Healthcare +US

- A data breach at the [University of Chicago Medicine](#) has resulted in the exposure of personal data of over 10,000 patients. The breach was caused by a phishing attack that compromised email accounts and led to the leakage of sensitive information. The incident raises significant concerns about data protection in educational institutions and the need for improved cybersecurity awareness and training.

Christie's Hit by Ransomware, Confirms Data Breach

+Retail +RansomHub

- [Christie's](#), the renowned auction house, has confirmed a data breach following an attack by a new ransomware group known as RansomHub. The attackers encrypted Christie's data and demanded a ransom for its release. The breach could compromise sensitive information related to high-value art transactions, affecting clients and potentially damaging the auction house's reputation.

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.