infinitum IT
Power of Integrated Security

MDR Insights

"December"

infinitumitlabs

Content

MDR REPORT

As Infinitum IT MDR team, we are pleased to provide you December trends, current news, the most common attack vectors and many new developments in the cyber world, including TTPs used by APT Groups. This report allows you to follow current events and analyze the situation with various graphs.

This report provides you ;

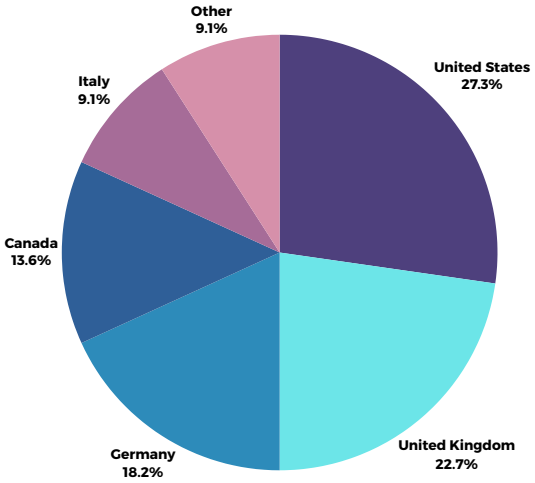
- Data on ransomware groups and graphical representation of their activity this month
- Emerging vulnerabilities
- This month's risk analysis graph
- Graph of product families with the most patches
- Infinitum IT MDR team presents the most common TTPs and their descriptions in our customer environment.
- Various attack vectors grouped by risk level
- Our current news section will help you stay up to date.

This MDR report provides an analysis of threats and security incidents detected in our company's information systems. The report covers topics such as summary and impact of incidents during the period under review, type and source of threats, status of security measures and recommendations.

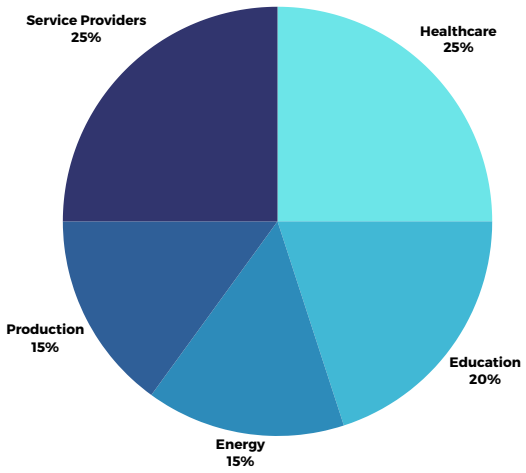
Ransomware Groups

1. ALPHV Ransomware Group

Attack Graph by Country



Attack Graph by Sectors

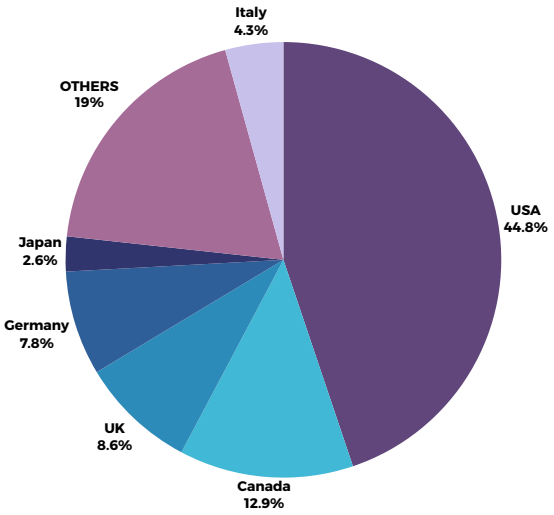


The Alphv ransomware group is a cybercrime group that first emerged in November 2021 and has been described as the first major ransomware family written in the Rust programming language. The group targets organizations all over the world, but with a particular focus on companies in North America, Europe and Asia. Targeted sectors include healthcare, finance, utilities and energy.

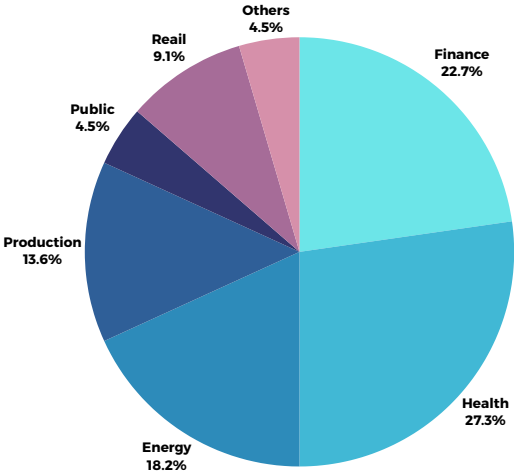
Alphv uses a variety of methods to carry out its attacks. These include malicious email, phishing attacks and security vulnerabilities. After carrying out the attacks, the group demands a ransom from victims to retrieve the encrypted data. Ransom demands are usually in the range of several million dollars.

2. Play Ransomware Group

Attack Graph by Country



Attack Graph by Sectors



Since its inception, the Play ransomware group has attracted attention by specifically targeting businesses and government organisations in the US, UK, Canada, the Netherlands, Brazil, Argentina, Germany, Belgium and Switzerland. Security experts believe that the Play ransomware group is linked to Russia. The group is also known by the name PlayCrypt and was created by the Balonfly team, which Symantec is monitoring. The ransomware locks victims' files by adding the ".play" extension after encrypting the files.

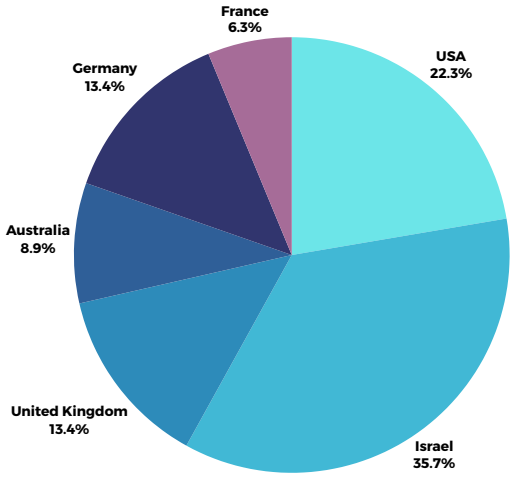
The ransom note contains the word "PLAY" and contact details left by the group responsible for the attack. The group used two new tools specially developed to support their attacks: The first is the Volume Shadow Copy Service (VSS) and the second is Grixbat.

As the Play ransomware group remains active in the ransomware environment, their actions have not been static. In-depth research has unveiled a clear pattern of the group continuously refining their tactics and enhancing their toolkit. This persistence underscores their commitment to perpetuate their presence and expand their influence.

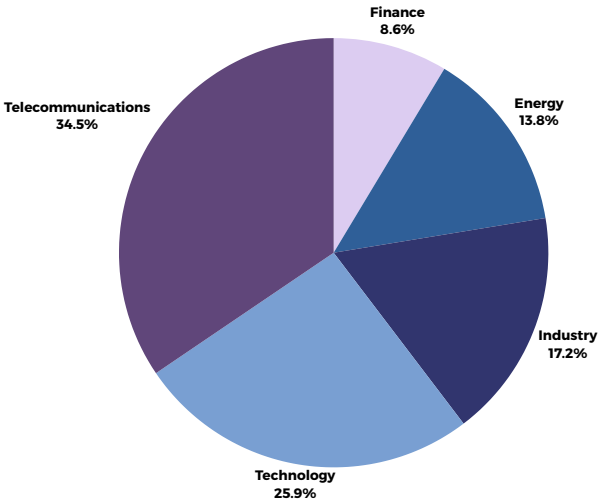
In their quest to achieve these objectives, the Play ransomware group has exhibited an adeptness at leveraging new vulnerabilities and incorporating fresh tools into their attacks. Notably, they have targeted vulnerabilities such as ProxyNotShell, OWASSRF, and Microsoft Exchange Server Remote Code Execution. Furthermore, they have introduced innovative components into their arsenal, including Grixba, a proprietary network scanner and information-stealer, as well as the open-source VSS management tool AlphaVSS.

3. GhostLocker Ransomware Group

Attack Graph by Country



Attack Graph by Sectors



GhostLocker is a sophisticated Ransomware-as-a-Service (RaaS) software introduced by hacktivist group GhostSec. Unlike traditional ransomware derivatives, GhostLocker is designed as an enterprise-grade lockdown software that prioritises security and efficiency above all else. This cutting-edge encryptor is marketed to infiltrate well-established telecommunications companies, surveillance systems and Internet of Things (IoT) devices.

GhostLocker's unique selling points include encryption capabilities, military-grade security measures, and a control panel that facilitates the creation of ransomware encryptors and decryptors. The ransomware encrypts data with the .ghost extension and self-deletes itself when encryption is complete.

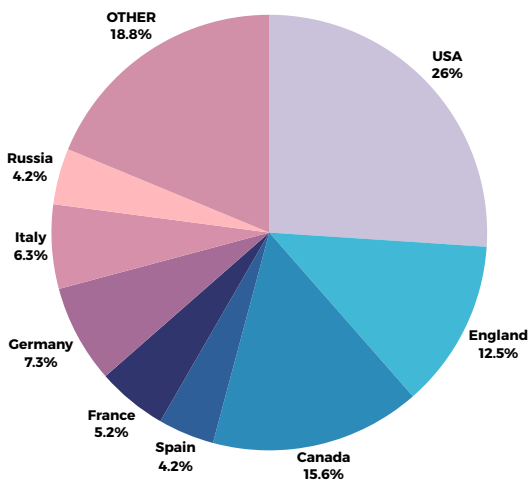
Key features include its undetectable nature, strong encryption and ease of negotiation by the GhostLocker team. In particular, it features advanced web panels, faster encryption with reduced file sizes and increased recovery cost if payment is not made within 2 days.Failure to pay leads to permanent deletion of data.The malware involves the creation of a malicious executable file within a Temp directory after execution.

After execution, the malware generates a malicious executable, Python modules, and DLL files within a Temp directory. The directory hosts the executable file alongside the requisite libraries for its functioning. Python modules are integrated into the executable file within the Temp directory, enabling encryption operations utilizing Python libraries. This strategy aims to reduce the detection rate by security products.

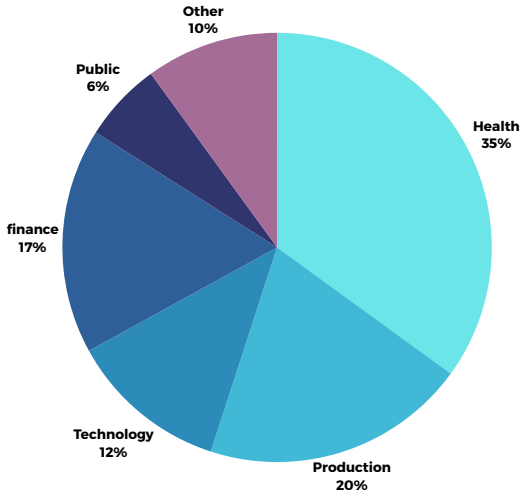
GhostLocker fide software restricts its use in medical or educational systems. There is no specific country where it is infected, it allows widespread use between various countries and systems.

4. LockBit Ransomware Group

Attack Graph by Country



Attack Graph by Sectors



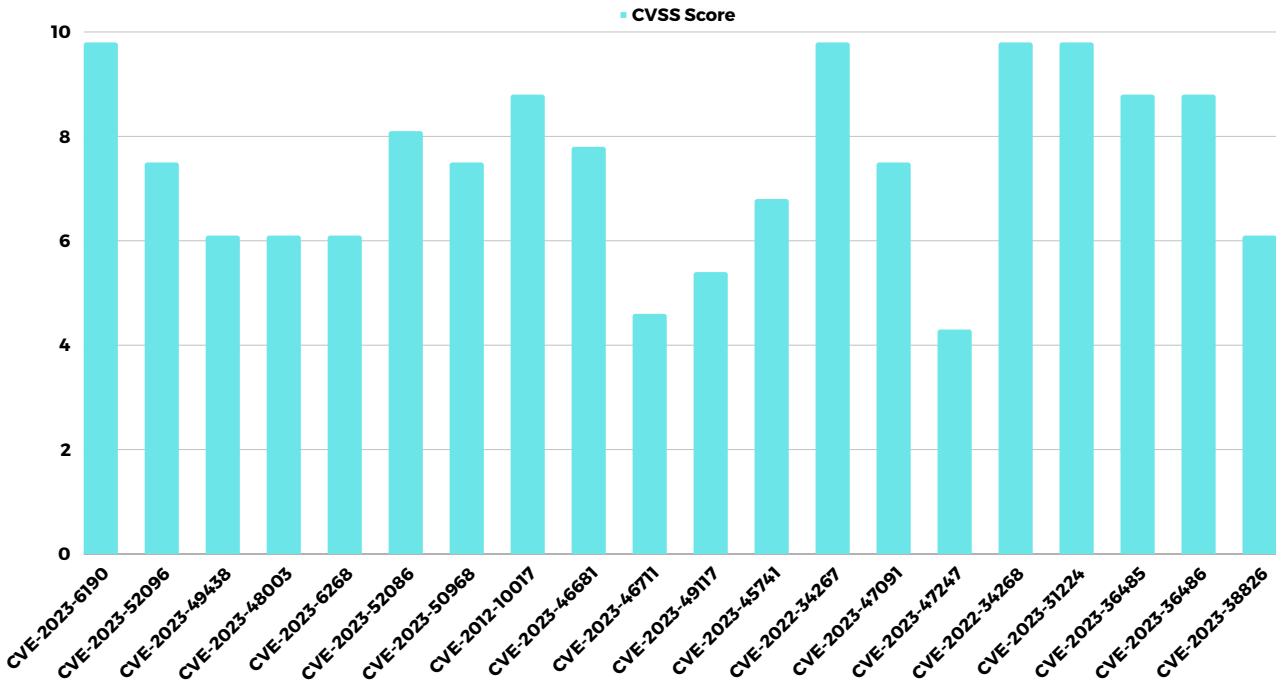
December 2023 has been very active for the ransomware group LockBit. Their focus on the healthcare sector is of particular concern, demonstrating their willingness to exploit weaknesses that can have serious consequences for individuals and healthcare systems. The increasing frequency of Cyber attacks in the healthcare sector highlights the need for urgent measures to protect sensitive patient information and ensure the uninterrupted delivery of critical medical services.

LockBit's various attacks on sectors such as energy, industry, government, technology and construction show that they target infrastructure, economic stability and national security. The high number of attacks categorized as "OTHER" raises possible concerns about unexpected and non-traditional targets. This highlights the urgent need for comprehensive cybersecurity strategies across all industries to mitigate effective risks.

The focus of LockBit attacks on countries with developed economic and political influence, such as the US, UK, France and Canada, demonstrates the group's willingness to target these countries. These attacks not only cause financial losses, but also affect key sectors in the global arena, causing a range of problems. Furthermore, LockBit's willingness to discover weaknesses in other countries poses a challenge for international efforts to effectively disrupt its activities. This highlights the importance of global cooperation and cybersecurity measures to counter the changing threat landscape posed by groups like ransomware.

The examples experienced in December 2023 show how active and dangerous LockBit is in the cybersecurity landscape. Organizations should be vigilant about implementing strong cybersecurity measures to protect themselves from ransomware attacks.

Top Trending CVEs of December 2023



	CVEs	Published	Description
Critical	CVE-2023-6190	2023-12-27	Improper Input Validation vulnerability in İzmir Katip Çelebi University University Information Management System allows Absolute Path Traversal.This issue affects University Information Management System: before 30.11.2023.
	CVE-2022-34267	2023-12-25	An issue was discovered in RWS WorldServer before 11.7.3. Adding a token parameter with the value of 02 bypasses all authentication requirements. Arbitrary Java code can be uploaded and executed via a .jar archive to the ws-api/v2/customizations/api endpoint.
	CVE-2022-34268	2023-12-25	An issue was discovered in RWS WorldServer before 11.7.3. /clientLogin deserializes Java objects without authentication, leading to command execution on the host.
	CVE-2023-31224	2023-12-25	There is broken access control during authentication in Jamf Pro Server before 10.46.1.

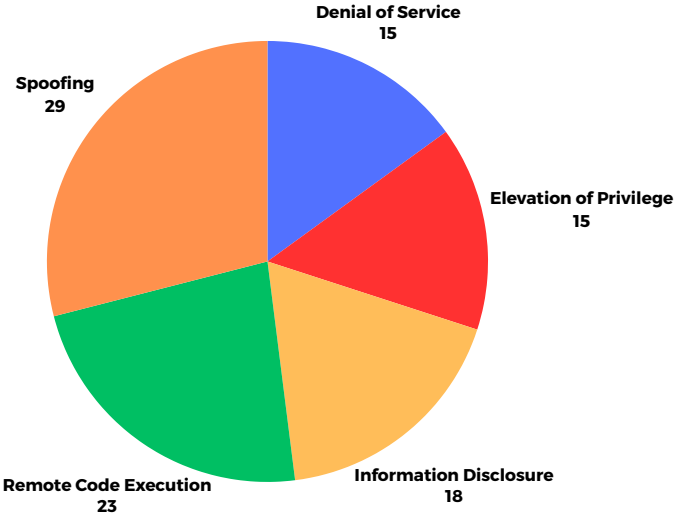
High

CVEs	Published	Description
CVE-2023-52096	2023-12-26	SteVe Community ocpp-jaxb before 0.0.8 generates invalid timestamps such as ones with month 00 in certain situations (such as when an application receives a StartTransaction Open Charge Point Protocol message with a timestamp parameter of 1000000). This may lead to a SQL exception in applications, and may undermine the integrity of transaction records.
CVE-2023-52086	2023-12-26	resumable.php (aka PHP backend for resumable.js) 0.1.4 before 3c6dbf5 allows arbitrary file upload anywhere in the filesystem via ../ in multipart/form-data content to upload.php. (File overwrite hasn't been possible with the code available in GitHub in recent years, however.)
CVE-2023-50968	2023-12-26	Arbitrary file properties reading vulnerability in Apache Software Foundation Apache OFBiz when user operates an uri call without authorizations. The same uri can be operated to realize a SSRF attack also without authorizations. Users are recommended to upgrade to version 18.12.11, which fixes this issue.
CVE-2012-10017	2023-12-26	A vulnerability was found in BestWebSoft Portfolio Plugin up to 2.04 on WordPress. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. Upgrading to version 2.06 is able to address this issue. The patch is named 68af950330c3202a706f0ae9bbb52ceaa17dda9d. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-248955.

Medium

CVEs	Published	Description
CVE-2023-49438	2023-12-26	An open redirect vulnerability in the python package Flask-Security-Too <=5.3.2 allows attackers to redirect unsuspecting users to malicious sites via a crafted URL by abusing the ?next parameter on the /login and /register routes.
CVE-2023-48003	2023-12-26	An open redirect through HTML injection in user messages in Asp.Net Zero before 12.3.0 allows remote attackers to redirect targeted victims to any URL via the '<meta http-equiv="refresh"' in the WebSocket messages.
CVE-2023-6268	2023-12-26	The JSON Content Importer WordPress plugin before 1.5.4 does not sanitise and escape the tab parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin
CVE-2023-46711	2023-12-26	VR-S1000 firmware Ver. 2.37 and earlier uses a hard-coded cryptographic key which may allow an attacker to analyze the password of a specific product user.

December 2023 Risk Analysis



Drawing upon the numerical data derived from our December risk analysis, we can discern critical trends and emerging threats that demand immediate attention. This data provides a comprehensive perspective on the array of attack vectors and techniques that potential adversaries may exploit during this specific timeframe.

RCE attacks now account for a significant 23% of the identified risks, representing a concerning uptick in their prevalence. RCE remains a serious concern as it grants malicious actors the ability to execute code on vulnerable systems remotely, potentially resulting in unauthorized access, data breaches, or even the complete compromise of critical infrastructure. Hence, organizations must maintain vigilant monitoring and swift remediation of potential RCE vulnerabilities.

Elevation of Privilege (EoP) emerges as another significant risk, constituting 15% of the analyzed threats. EoP attacks involve threat actors attempting to escalate their privileges within a system, seeking access to resources and capabilities beyond their authorized level. To mitigate the impact of EoP attacks, organizations should rigorously enforce robust access controls and adhere to the principle of least privilege.

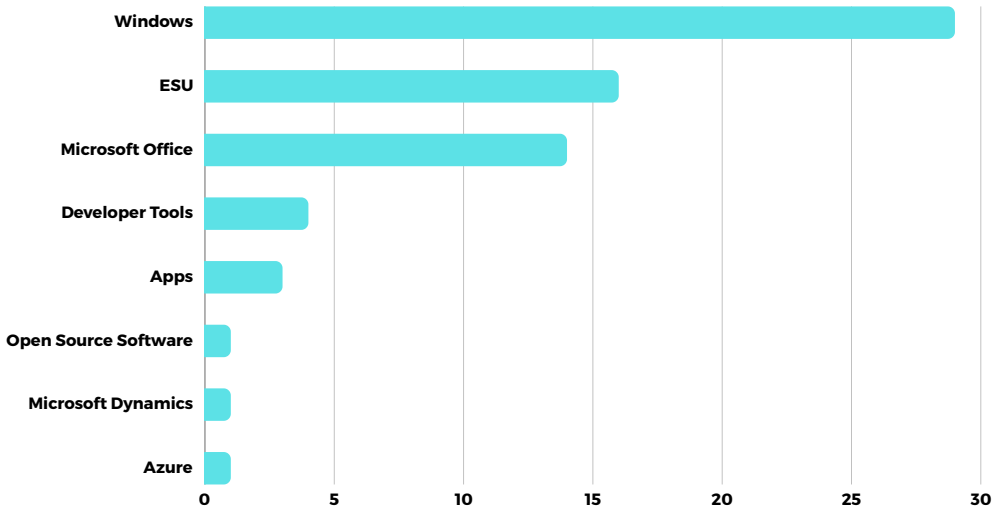
Meanwhile, Denial of Service (DoS) attacks, contributing to 15% of the identified risks, continue to pose a substantial threat. DoS attacks aim to overwhelm a system, network, or application with an excessive volume of traffic, rendering it unresponsive or inaccessible to legitimate users. Effectively countering DoS attacks requires meticulous network capacity planning, traffic filtering, and the deployment of distributed denial-of-service (DDoS) protection mechanisms.

Information Disclosure, making up 18% of the identified risks, signifies the inadvertent or unauthorized exposure of sensitive data to unauthorized entities. Such incidents can result from unsecured configurations, weak authentication, or other vulnerabilities, potentially leading to regulatory non-compliance, reputational damage, and financial losses. Organizations must prioritize data protection through robust encryption, access controls, and regular security assessments.

Lastly, Spoofing attacks, contributing to 29% of the identified risks, encompass malicious actors' attempts to conceal their identities or manipulate data packets to deceive systems or users. Implementing robust authentication mechanisms, such as multi-factor authentication, is crucial in mitigating the risks associated with Spoofing attacks.

Navigating the ever-evolving cybersecurity landscape in December demands vigilance, adaptability, and proactive measures. Staying ahead of emerging threats and vulnerabilities is essential for safeguarding organizational assets and ensuring robust security posture.

Patches by Product Family, December 2023



December 2023 Patch
The final Patch Tuesday of 2023 saw a flurry of fixes, with various product families getting their share of TLC. While the number of patches was lower than usual, the severity of some addressed vulnerabilities shouldn't be underestimated.

Microsoft ESU Takes the Lead: Extended Security Updates, keeping older Windows versions alive, received the most attention with 18 patches. This highlights the ongoing need for security even in outdated systems.

Windows Holds Its Ground: Despite ESU stealing the spotlight, Windows itself received 7 crucial patches, addressing vulnerabilities in core components like networking and kernel drivers.

Cloud Concerns Addressed: Azure, Microsoft's cloud platform, saw 3 patches tackling potential information disclosure and elevation of privilege issues. Cybersecurity in the cloud remains paramount.

Office Gets Polished: Although only 3 patches, Office updates focused on fixing critical remote code execution (RCE) vulnerabilities, especially concerning Word and Excel. Keeping productivity tools secure is essential.

Beyond Microsoft: Adobe also joined the patching party, addressing 13 critical vulnerabilities across various software, including Flash Player (finally!).

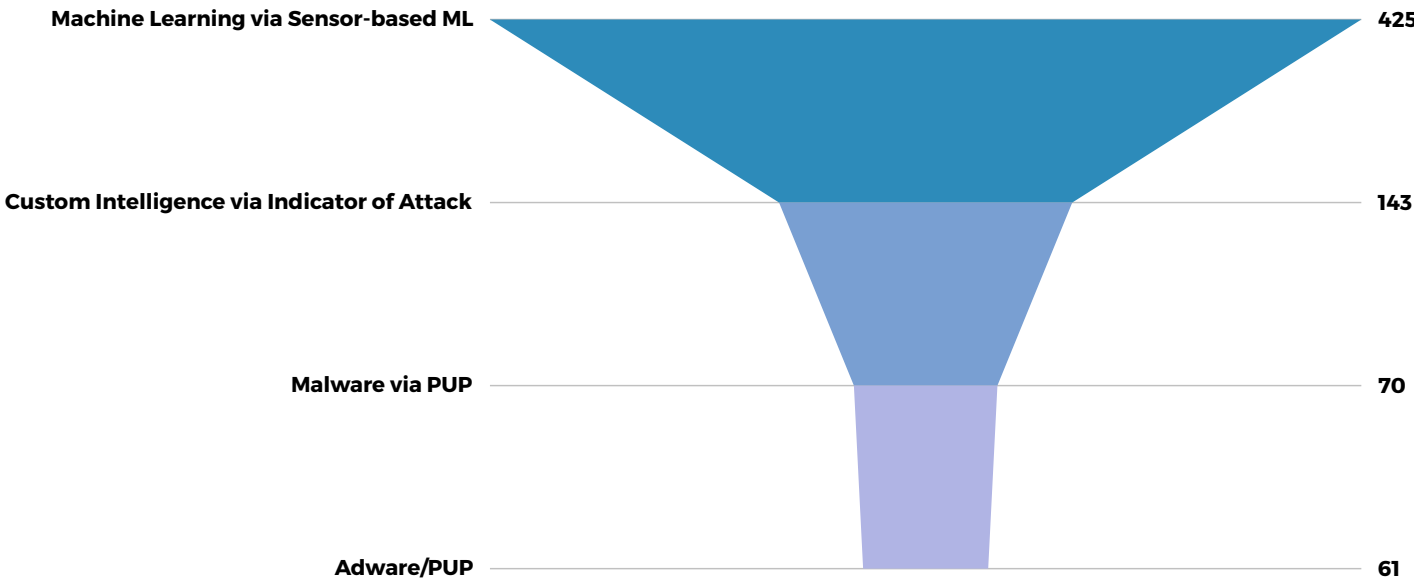
The Numbers Game: In total, December 2023 saw 34 vulnerabilities patched, including a single publicly disclosed zero-day affecting AMD processors. While lower than average, the severity of some flaws emphasizes the importance of timely patching.

Remember: Patching isn't just about numbers. Prioritize critical fixes and focus on high-impact products within your environment.

Stay vigilant: December may be over, but the patching journey continues. Keep your systems updated and be prepared for future vulnerabilities.

The Most Common TTPs

This section contains the most common TTPs we have encountered in the last 30 days in our own customer environment.



In this monthly MDR report, we present an analysis of the data obtained from our customers' cybersecurity systems. The graphic includes information on the Detection Counts for various categories:

Machine Learning via Sensor-based ML: 425

Sensor-based Machine Learning played a crucial role, with 158 instances of threat detection. This reflects the effectiveness of our machine learning algorithms deployed in the client environments.

Custom Intelligence via Indicator of Attack: 143

Instances of custom intelligence based on indicators of attack further emphasize our commitment to proactively identifying and mitigating potential cybersecurity threats. The count of 140reflects a targeted approach to threat detection.

Malware via PUP (Potentially Unwanted Program): 70

Detection of malware through Potentially Unwanted Programs indicates vigilance against unwanted and potentially harmful software, with 62 instances identified.

Machine Learning via Adware/PUP: 61

Adware (advertising-supported software) and PUPs (Potentially Unwanted Programs) are typically considered unwanted software because they often display intrusive advertisements or collect user data without clear consent.

This monthly analysis provides valuable insights into the effectiveness of our cybersecurity measures, showcasing a proactive and multi-faceted approach to safeguarding our clients' environments.

Common Types Attack Vectors

Risk Severity

Critical **High** **Medium**

Adversary in the Middle (AiTM)

An attacker typically targets the communication between client and server, aiming to modify or extract data from transactions. A common approach is for the attacker to position themselves in the communication channel, usually between the client and the server.

XSS Targeting Non-Script Elements

This type of attack falls under Cross-Site Scripting (XSS), where malicious scripts are injected into elements that are typically not expected to host scripts (for example, <img> image tags, < !-CDATA-> comments in XML documents, etc.). These special tags may not typically be subject to the same input validation, output validation and other content filtering processes, allowing the attacker to pass through application components and launch an XSS attack through unexpected elements. Like all remote attacks, the difference between the ability to launch an attack and the remote attacker's ability to collect and interpret the results of that attack is important.

Command Line Execution through SQL Injection

The attacker injects data into the command line using standard SQL injection methods. This can be done directly by misuse of directives such as MSSQL_xp_cmdshell, or indirectly by injecting the data into the database in a way that is acceptable. Then, an unethical backend application (or it could be part of the functionality of the same application) pulls the injected data stored in the database and uses it as command line arguments without proper validation. The malicious data escapes from the data plane to be executed on the host by hosting new commands.

Install Malicious Extension

An attacker installs a malicious plugin directly into existing trusted software or tricks the user into installing it. This is intended to achieve various negative technical effects.

Manipulating State

The attacker changes the state information stored by the target software or causes a state transition in the hardware. When successful, the target uses this affected state to operate in an unintended way. State management in software applications contains important information about the user, such as usernames, payment information, browsing history. An attacker can manipulate this information and use it to elevate privileges, perform fraudulent operations or change the flow of the application. In case of a logic error in the hardware, the attacker can cause an undefined state on the system, which can lead to service interruption or leakage of security data

Voice Phishing

The attacker targets users with a phishing attack to provide account passwords or sensitive information. Voice Phishing is a social engineering technique where the attack is initiated with a voice call instead of an email. The user is tricked into providing sensitive information verbally by a person posing as a legitimate employee of the organization the attacker claims to be. Voice Phishing differs from standard Phishing attacks in that typically the user does not interact with a website to provide sensitive information.

Email Injection

An attacker manipulates the headers and content of an email message using protocol-specific delimiter characters to inject data.

File Manipulation

By changing file contents or properties, the attacker causes the application to malfunction. These attacks aim to destabilize applications, expose sensitive information and execute arbitrary code with application privileges.

BlueSmacking

An attacker intends to create a DoS (Denial of Service) by sending large packets to Bluetooth-enabled devices over the L2CAP protocol using Bluetooth flooding. This attack must be performed in close proximity to a Bluetooth-enabled device.

ThreatBlade

Automated Testing

The automated platform helps red teams to be more efficient; they can run automated testing operations at scale and benefit from the rich performance data that scaled automation brings.

Audit and Compliance

Use the platform to reduce your compliance and regulatory burden by mapping regulatory and compliance controls, conducting continuous tests, mapping the data from those tests to your compliance framework, and training your auditors.

Security Operations

Use the MITRE ATT&CK framework and up-to-date threat intelligence about adversary tactics, techniques, and procedures to facilitate threat-informed defense operations across the enterprise, gaining data-driven control over your security program to ensure that you detect and prevent the adversary when the time comes.

Ransomware Defense Assessment

ThreatBlade's Ransomware Defense Assessment evaluates your organization's ability to detect, contain, and remediate ransomware within your environment—before it produces costly harm.

Red, Blue, and Purple Teams

Teams use ThreatBlade's library of adversary emulations to exercise and validate specific security controls, building on the MITRE ATT&CK framework and ThreatBlade library with new threat intelligence from the outside or which the security team itself generates.

Adversary Emulation Exercise

This test provides the benefit of experiencing a sophisticated targeted attack without the actual damage of a real incident.

MDR Health Check

ThreatBlade provides real-time malware simulations on your inventory with experienced experts and innovative technology. **The free MDR Health Check** is like a stress test to measure how robust your shield is against threats you may face in the field. Our test results show how much of your security service is alert to real-world threats. This valuable information helps you finalize and improve your security strategies and protocols.

As InfinitumIT, at the end of MDR Health Check, we provide you with a customized report. This report will evaluate the performance, effectiveness and maturity level of the SOC or MDR service you have provided. The report provides detailed information on gaps, improvements and potential threats. As a result, you can clarify the limits of your security measures and direct your security investments in the most effective way.

Click the link below to take advantage of our free MDR Health Check service.

https://www.infinitumit.com.tr/ucretsiz-mdr-health-check/

News

FBI Releases Free Decryption Tool Disabling BlackCat Ransomware

The US Department of Justice (DoJ) announced the BlackCat ransomware operation and released a decryption tool for more than 500 victims to regain access to their files. The FBI used an undercover human resource to hack the BlackCat group, gaining access to the web panel controlled by the group where the victims were controlled. This international operation, with legal assistance and cooperation from the United States, Germany, Denmark, Australia, the United Kingdom, Spain, Switzerland and Austria, is an example of a counter-ransomware operation. The FBI's intervention comes as BlackCat has become one of the most widespread ransomware in the world. As part of the operation, the FBI announced that it had recovered $68 million in ransom demands and gained significant insight into BlackCat's computer network. It was also observed to have various effects, including disabling TOR sites by collecting 946 public/private key pairs.

QakBot Malware Reappears: Targeting the Hospitality Industry with Innovative Tactics

Microsoft tarafından keşfedilen yeni bir QakBot zararlı yazılım saldırısı, komuta kontrol (C2) ağının çökertilmesinden üç aydan fazla bir süre sonra tespit edildi. 11 Aralık 2023'te başlayan bu kampanya, konaklama endüstrisini hedef almıştır. Saldırı, kullanıcılara IRS çalışanını taklit eden birinden gelen phishing mesajlarıyla gerçekleşiyor. Mesajlarda bulunan PDF, QakBot'u içeren dijital imzalı bir Windows Installer dosyasını indiren bir URL içeriyor. Kampanyanın ilk gününde oluşturulan yük, daha önce görülmemiş 0x500 sürümüyle yapılandırılmıştır. QakBot'un geri döndüğünü ve AES şifrelemesini kullanan bir 64-bit ikili olduğunu belirten Zscaler ThreatLabz, QakBot'un yeni taktiklerle tekrar ortaya çıktığını ifade ediyor. Daha önce etkisiz hale getirilen Operation Duck Hunt çabasının bir parçası olan QakBot, bu kez önceki kampanyalardaki hacim ve ölçekte olmadan geri dönmüştür. Uzmanlar, kolluk kuvveti müdahalesinin QakBot'un operasyonları üzerinde hala etkili olduğunu belirtiyorlar. Bu olaylar, organizasyonların phishing kampanyalarına karşı dikkatlerini artırmalarını ve güvenlik önlemlerini güncel tutmalarını vurgulamaktadır.

Russian APT28 Hackers Target 13 Countries in Ongoing Cyber Espionage Campaign

The Russian state-sponsored cyber threat actor APT28, or ITG05, has been observed using deceptive tactics in a cyber espionage campaign linked to the Israel-Hamas conflict. ITG05 is known by various aliases and uses a special backdoor called "HeadLace". The campaign targets organizations in at least 13 countries, with APT28 this time targeting European organizations affecting humanitarian aid allocation. The attackers are using forged documents that appear to be associated with the United Nations, the Bank of Israel, the US Congressional Research Service, the European Parliament, a Ukrainian think tank and the Azerbaijan-Belarus Intergovernmental Commission. The campaign exploits the WinRAR bug (CVE-2023-38831) in RAR archives to deliver the HeadLace backdoor. This is a deviation from APT28's previous tactics. These events highlight APT28's efforts to obtain advanced information on international security and humanitarian issues.

Kyivstar - Ukraine's Largest Telecom Operator Suffers Massive Cyber Attack

Ukraine's leading telecom operator Kyivstar has suffered a severe cyber attack, causing disruptions to mobile and internet services to customers. The attack affected the entire country and had a significant impact on the capital. Kyivstar explained that the attack was a consequence of the ongoing war with Russia and reported the incident to law enforcement and state services. The company has not yet provided details on the nature and effects of the attack. It says subscribers' personal data was not breached. Kyivstar said it would compensate all subscribers and corporate customers as soon as services return to normal. The pro-Russian hacktivist group KillNet and the security service Solntsepyok claimed responsibility for the attack via Telegram, but did not provide additional evidence to support these claims. Kyivstar warns users to be wary of fraud attempts and emphasizes that official news will come from the company's official pages.

infinitum IT
Power of Integrated Security

MDR Insights

"December"

infinitumitlabs