infinitum IT
Power of integrated Security

MDR Insights

"November"

infinitumitlabs

Content

Ransomware Groups..........03
NoEscape Ransomware Group 03
8Base Ransomware Group 04
Play Ransomware Group 05
LockBit Ransomware Group 06
Top Trending CVEs of November 2023..........07
Windows SmartScreen Security Feature Bypass Vulnerability..........07
Windows Desktop Window Manager Local Privilege Escalation Vulnerability..........08
Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability..........09
Microsoft Protected Extensible Authentication Protocol Vulnerability..........10
Windows Pragmatic General Multicast Remote Code Execution Vulnerability..........11
November 2023 Risk Analysis..........12
Patches by Product Family, November 2023..........13
The Most Common TTPs..........14
Common Types of Attack Vectors..........15
ThreatBlade 16
MDR Health Check..........16
News..........17

MDR REPORT

As Infinitum IT MDR team, we are pleased to provide you November 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.

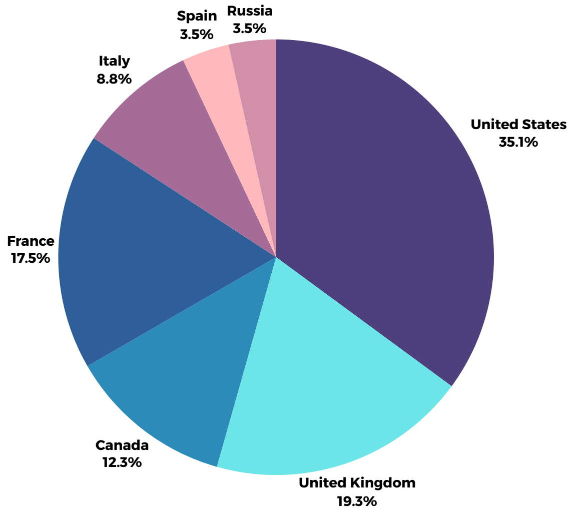
This MDR report provides an analysis of threats and security incidents detected in our company's information systems. The report covers topics such as summary and impact of incidents during the period under review, type and source of threats, status of security measures and recommendations.

Ransomware Groups

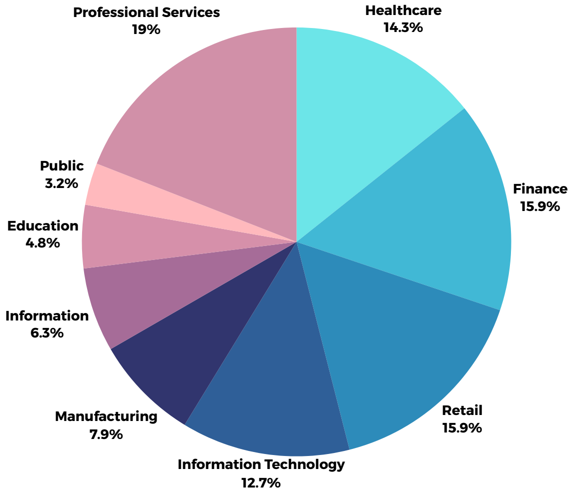
1. NoEscape Ransomware Group

Total Number of Attacks: 30

Attack Graph by Country



Attack Graph by Sectors



The latest data for November unveils a significant transformation in the ransomware landscape, particularly with the emergence of NoEscape, following in the footsteps of the notorious Avaddon ransomware that surfaced in early 2019. Avaddon was known for its double-extortion tactics, threatening to release stolen data while encrypting victims' files. It targeted a wide array of sectors, including health, government, finance, law, hospitality, education, and retail. Interestingly, some of Avaddon's affiliates targeted individual entities rather than major corporations.

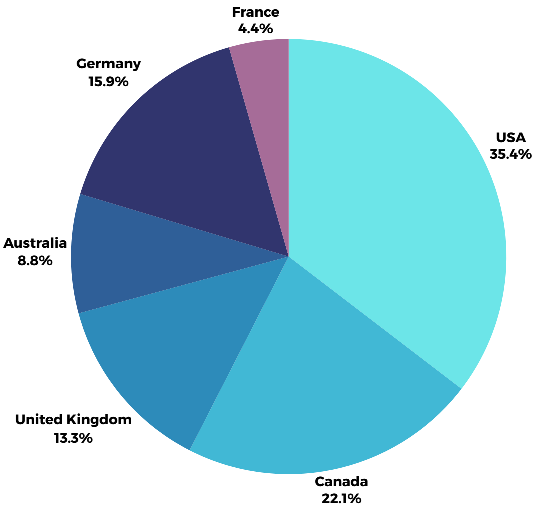
Avaddon had mechanisms to avoid attacks in specific countries within the former Soviet Union, particularly those aligned with Russia. However, in 2021, Avaddon ceased operations, providing decryption keys to all victims. This pause marked the emergence of NoEscape in June 2023, showcasing strikingly similar tactics and operations to Avaddon.

November's data highlights the resurgence of ransomware threats. NoEscape's emergence raises serious concerns in the cybersecurity realm. This strategic shift emphasizes the need to strengthen cybersecurity measures not only in prominent nations but also in regions where vulnerabilities often go unnoticed.

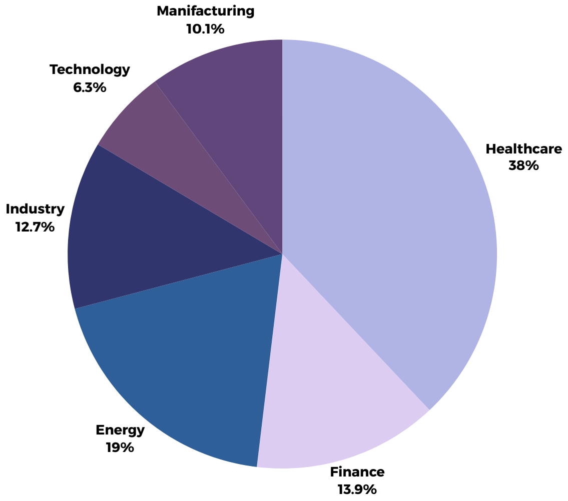
2. 8Base Ransomware Group

Total Number of Attacks: 42

Attack Graph by Country



Attack Graph by Sectors



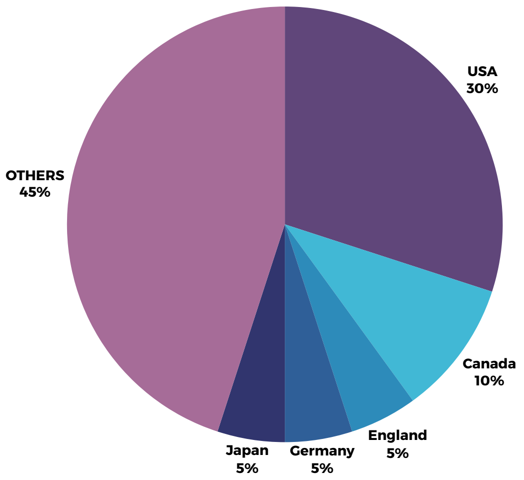
Recent data regarding the 8BASE Ransomware Group in November sheds light on their evolving targeting patterns and global reach, reflecting a significant and concerning cyber threat. Examination of sectoral attack data for November indicates a wide array of interests, with the construction, health, energy, and industry sectors each experiencing three to four attacks. This suggests 8BASE continues its indiscriminate targeting, aiming to disrupt critical infrastructure and services across diverse industries. The notable number of attacks categorized as "OTHER" hints at potential exploration of unconventional targets or an expansion beyond traditional sectors, indicative of their adaptability.

Analyzing country-specific data for November highlights the USA as the primary target, encountering 14 attacks. The USA's standing as a global economic and technological hub renders it an appealing target for cybercriminals seeking financial gain or intending to sow widespread chaos. Meanwhile, Canada, the UK, and the UAE faced two to three incidents each, underscoring the group's international impact. Singular attacks in countries like France emphasize the group's willingness to diversify targets. Moreover, the considerable number of attacks attributed to "OTHER" countries points to 8BASE's active pursuit of victims in lesser-known regions, possibly exploiting weaker cybersecurity defenses prevalent in those areas during November.

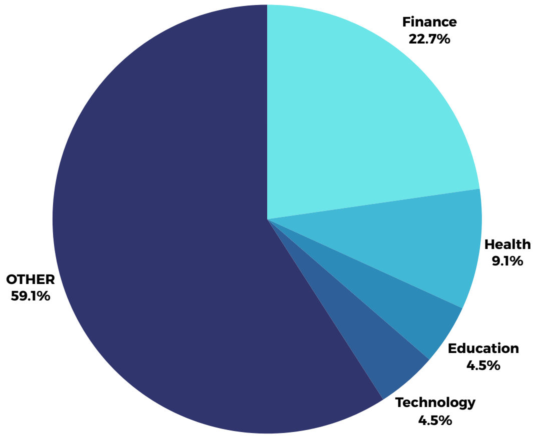
3. Play Ransomware Group

Total Number of Attacks: 53

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.

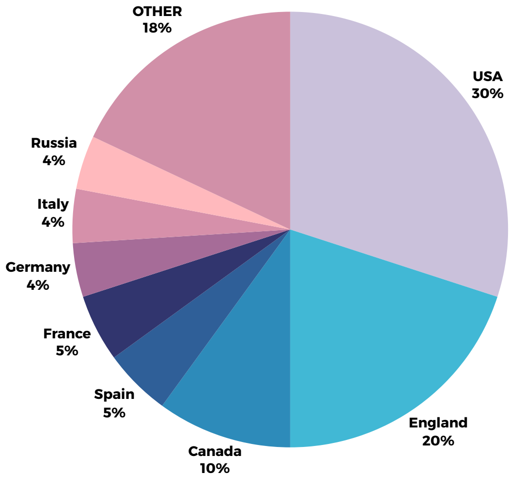
In their quest to achieve these objectives, the Play ransomware group has exhibited an adeptness at leveraging new vulnerabilities and incorporating fresh tools into their attacks. Notably, they have targeted vulnerabilities such as ProxyNotShell, OWASSRF, and Microsoft Exchange Server Remote Code Execution. 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.

To protect against this evolving threat landscape and the potential ties to other ransomware families, organizations must remain vigilant, continuously update their security measures, and leverage threat intelligence as an essential defense mechanism. Staying proactive and informed is paramount in fortifying defenses against the multifaceted and interconnected threats presented by ransomware groups like Play.

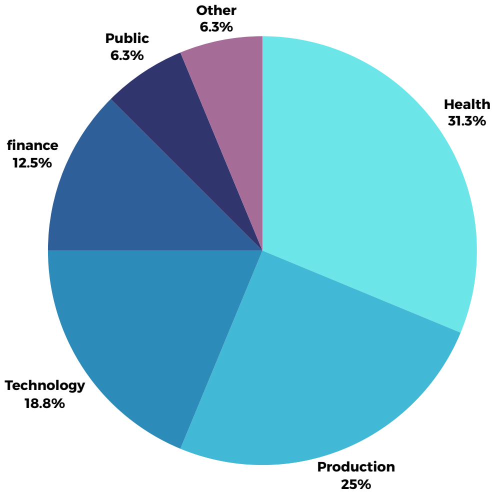
4. LockBit Ransomware Group

Total Number of Attacks: 104

Attack Graph by Country



Attack Graph by Sectors



In today's digital age, cyber security threats are becoming increasingly sophisticated and one of the leading names among these threats is the LockBit ransomware group. LockBit is known as a type of ransomware that infiltrates computer systems, encrypts files and then demands a ransom. This malware group stands out as a player in many cyber attacks known for its malicious actions.

The LockBit ransomware group is notable for its advanced technical skills and constantly evolving attack strategies. This group is generally known for its sophistication in the methods used to infiltrate and encrypt target systems. They are also known for their ability to quickly target weaknesses discovered by cyber security experts.

They often target large-scale corporate networks and organise attacks against companies operating in finance, healthcare, energy and other critical sectors. This group has the ability to create a global impact, often directing their attacks at multiple international companies.

It infiltrates target systems using social engineering tactics. They use methods such as email spoofing, malicious links, and malicious file attachments to trick users into logging into systems. They also use sophisticated encryption algorithms to render files inaccessible and then attempt to gain financial gain from victims by transmitting ransom demands.

Top Trending CVEs of November 2023

Windows SmartScreen Security Feature Bypass Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-36025	8.2	High	Security Feature Bypass

The vulnerability allows for a threat actor to bypass Windows Defender SmartSceen check and their associated prompts. To successfully exploit this vulnerability a threat actor would need to social engineer a victim into clicking a specially crafted Internet Shortcut (.URL) or a hyperlink pointing to a compromised Internet Shortcut file.

Mitigations

- Microsoft has released a security update to address this vulnerability. Installing this update will help prevent this vulnerability from being exploited.

- Windows SmartScreen is a built-in security feature that evaluates applications for their trustworthiness. Enabling this feature can help prevent malicious software or other security risks from being installed on a computer.

- Only download applications from trusted sources. Applications downloaded from untrusted sources may contain malicious software.

- A firewall or security software can help protect your computer from malicious software and other security threats.

Windows Desktop Window Manager (DWM) Local Privilege Escalation Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-36033	7.8	High	Elevation of Privilege

CVE-2023-36033 is a critical security vulnerability in the Windows Desktop Window Manager (DWM) that could allow an attacker to elevate their privileges on a vulnerable system. This vulnerability could allow an attacker to take control of a system, install malware, or steal sensitive data.

This vulnerability is caused by a flaw in the way the DWM handles certain types of memory requests. An attacker could exploit this vulnerability by sending specially crafted requests to the DWM, which could cause the DWM to elevate the attacker's privileges.

This vulnerability is remotely exploitable, meaning that an attacker could exploit it from a remote location. An attacker could exploit this vulnerability by sending specially crafted requests to the DWM via a web page, email, or other remote resource.

Mitigations

- Microsoft has released a security update to address this vulnerability. Installing this update will help prevent this vulnerability from being exploited.
- A firewall or security software can help protect your computer from malicious software and other security threats.
- Do not click on links or open attachments from unknown senders.
- Make sure you have the latest updates for all of your software, including your operating system, web browser, and security software.

Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-36036	7.8	High	Elevation of Privilege

CVE-2023-36036 is a critical security vulnerability in the Windows Cloud Files Mini Filter Driver that could allow an attacker to elevate their privileges on a vulnerable system. This vulnerability could allow an attacker to take control of a system, install malware, or steal sensitive data.

This vulnerability is caused by a flaw in the way the Cloud Files Mini Filter Driver handles certain types of requests. An attacker could exploit this vulnerability by sending specially crafted requests to the driver, which could cause the driver to elevate the attacker's privileges.

This vulnerability is remotely exploitable, meaning that an attacker could exploit it from a remote location. An attacker could exploit this vulnerability by sending specially crafted requests to the driver via a web page, email, or other remote resource.

Mitigations

- The best way to mitigate this vulnerability is to install the security update from Microsoft. This update will patch the flaw in the Cloud Files Mini Filter Driver that is exploited by this vulnerability.

  To install the security update, follow these steps:
  Click the Start button.
  Select Settings.
  Select Update & Security.
  Select Windows Update.
  Check for updates.

- A firewall or security software can help protect your computer from malicious software and other security threats. A firewall can help prevent malicious software from entering your computer by filtering network traffic. Security software includes a variety of tools designed to protect your computer from malicious software and other threats.

- Make sure you have the latest updates for all of your software, including your operating system, web browser, and security software. These updates often include security patches that can help protect your computer from vulnerabilities like CVE-2023-36036.

Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-36028	9.8	Critical	Remote Code Execution

CVE-2023-36028 is a critical security vulnerability in the Microsoft Protected Extensible Authentication Protocol (PEAP) that could allow an attacker to execute arbitrary code on a vulnerable system. This vulnerability could allow an attacker to take control of a system, install malware, or steal sensitive data.

This vulnerability is caused by a flaw in the way the PEAP protocol handles certain types of requests. An attacker could exploit this vulnerability by sending specially crafted requests to a PEAP server, which could cause the server to execute arbitrary code.

This vulnerability is remotely exploitable, meaning that an attacker could exploit it from a remote location. An attacker could exploit this vulnerability by sending specially crafted requests to a PEAP server via a web page, email, or other remote resource.

Mitigations

- If you do not need to use PEAP authentication, you can disable it to mitigate this vulnerability. To disable PEAP authentication, follow these steps:

  1.Open the Group Policy Editor.
  2.Navigate to the following path:

  Computer Configuration\Policies\Administrative Templates\Network\Network Connections\IEEE 802.1X\PEAP

  3. Double-click the "Allow PEAP authentication" policy.
  4. Set the policy to "Disabled".
  5. Click "Apply" and "OK".

- A firewall or security software can help protect your computer from malicious software and other security threats. A firewall can help prevent malicious software from entering your computer by filtering network traffic. Security software includes a variety of tools designed to protect your computer from malicious software and other threats.

Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-36397	9.8	Critical	Remote Code Execution

CVE-2023-36397 is a critical security vulnerability in the Windows Pragmatic General Multicast (PGM) protocol that could allow an attacker to execute arbitrary code on a vulnerable system. This vulnerability could allow an attacker to take control of a system, install malware, or steal sensitive data.

This vulnerability is caused by a flaw in the way the PGM protocol handles certain types of messages. An attacker could exploit this vulnerability by sending specially crafted messages to a PGM server, which could cause the server to execute arbitrary code.

Mitigations

- If you do not need to use PGM, you can disable it to mitigate this vulnerability. To disable PGM support, follow these steps:
  1. Open the Group Policy Editor.
  2. Navigate to the following path:

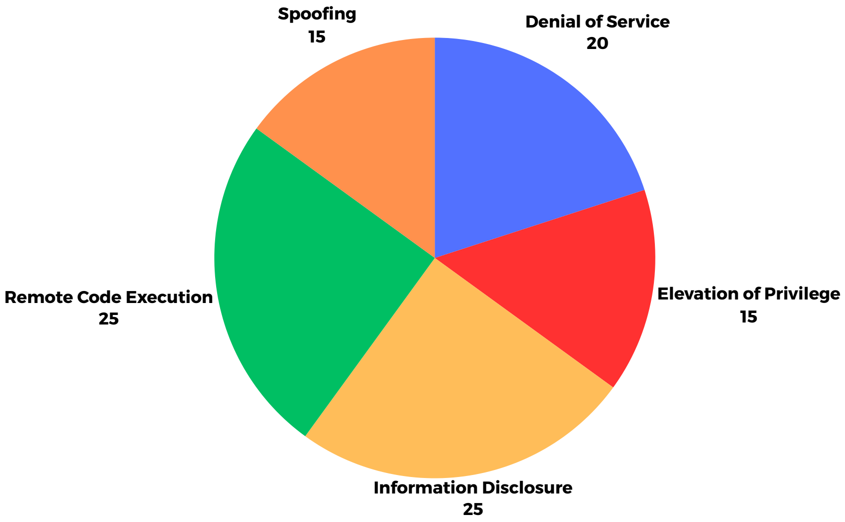
Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Windows Sockets (Winsock)

3. Double-click the "Enable IPv6 for all interfaces" policy.
4. Set the policy to "Disabled".
5. Click "Apply" and "OK".

- A firewall or security software can help protect your computer from malicious software and other security threats. A firewall can help prevent malicious software from entering your computer by filtering network traffic. Security software includes a variety of tools designed to protect your computer from malicious software and other threats.

To configure a firewall, follow these steps:
1. Open the Control Panel.
2. Select System and Security.
3. Select Windows Firewall.
4. Select Allow an app or feature through Windows Firewall (or Allow an app through Windows Firewall with Advanced Security).
5. Select Change settings.
6. Allow the app or feature that you want to allow through the firewall.

November 2023 Risk Analysis



Drawing upon the numerical data derived from our November 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 25% 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.

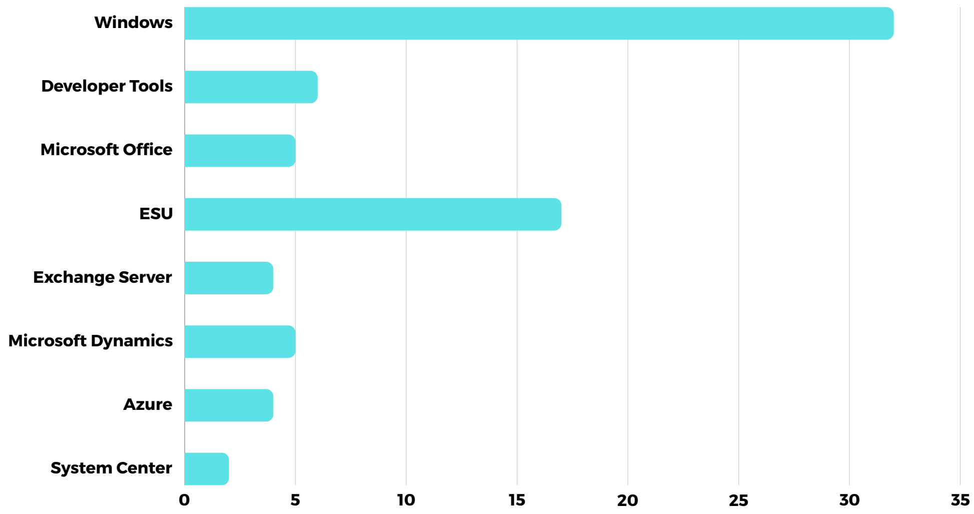
Meanwhile, Denial of Service (DoS) attacks, contributing to 20% of the identified risks, continue to pose a substantial threat. DoS attacks aim to overwhelm a system, network, or application with an excessive volume of traffic, rendering it unresponsive or inaccessible to legitimate users. Effectively 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 25% 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 15% 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 November 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, November 2023



The distribution of Microsoft security updates in November 2023 reveals a slightly different picture than previously analyzed. While Windows still holds the top spot with 32 patches, showcasing Microsoft's continued focus on safeguarding its flagship operating system, other product families demonstrate increased attention.

Developer Tools, essential for building the software we rely on daily, saw a substantial increase to 6 patches, highlighting Microsoft's commitment to securing the development ecosystem. Similarly, Exchange Server, a critical communication tool for many organizations, received 4 patches, emphasizing its security importance.

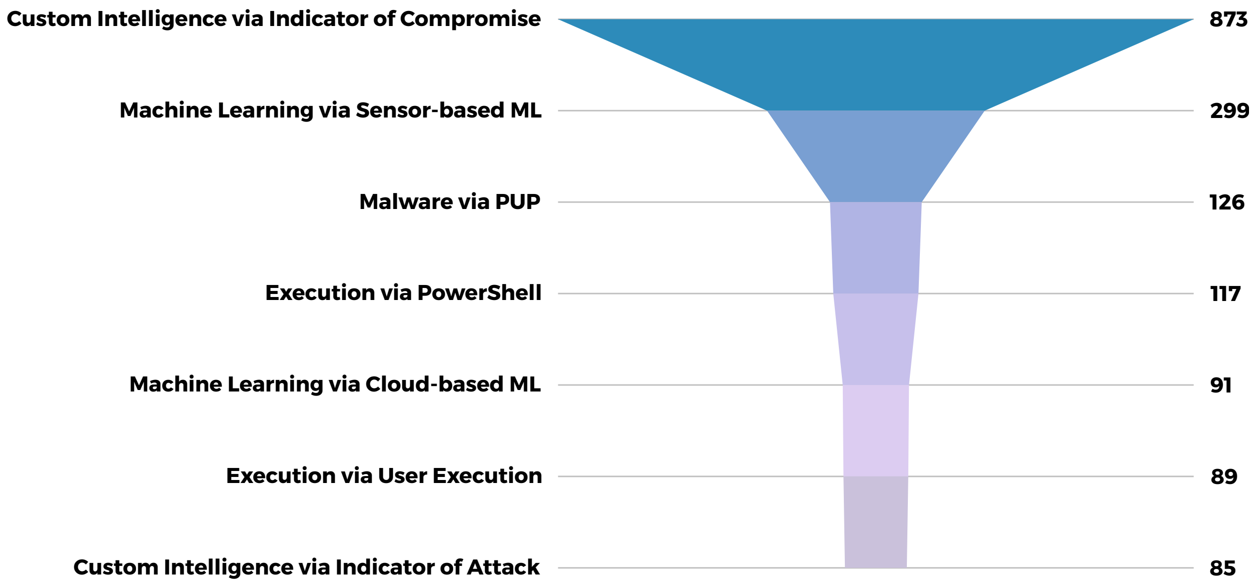
Microsoft Office, a commonly targeted productivity suite, received 5 patches, demonstrating Microsoft's ongoing efforts to protect its users from potential attacks. Interestingly, System Center, a platform for managing IT infrastructure, received 2 patches, suggesting a focus on enhancing the security of IT environments.

Other product families, including Microsoft Dynamics, Azure, and ESU, also received patches, contributing to the total of 17. This diverse distribution indicates Microsoft's dedication to addressing security vulnerabilities across a broad spectrum of products and services.

Overall, the updated data reaffirms Microsoft's unwavering commitment to security. Organizations should remain vigilant and prioritize timely updates for all their Microsoft products, regardless of their perceived popularity, to maintain a robust cybersecurity posture and mitigate potential threats.

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:

Custom Intelligence via Indicator of Compromise: 873

This category represents instances where our custom intelligence, based on indicators of compromise, detected and responded to potential security threats. The high count suggests a significant focus on threat intelligence.

Machine Learning via Sensor-based ML: 299

Sensor-based Machine Learning played a crucial role, with 299 instances of threat detection. This reflects the effectiveness of our machine learning algorithms deployed in the client environments.

Malware via PUP (Potentially Unwanted Program): 126

Detection of malware through Potentially Unwanted Programs indicates vigilance against unwanted and potentially harmful software, with 126 instances identified.

Execution via PowerShell: 117

Instances of execution via PowerShell represent potential security risks associated with this powerful scripting tool. The count of 117 suggests a focus on monitoring and mitigating PowerShell-related threats.

Machine Learning via Cloud-based ML: 91

Our Cloud-based Machine Learning systems contributed to threat detection, with 91 instances. This reflects the importance of cloud-based intelligence in identifying and responding to emerging threats.

Execution via User Execution: 89

Detection of execution via user actions indicates a focus on identifying threats that involve user interaction. The count of 89 suggests attention to potential risks initiated by user actions.

Custom Intelligence via Indicator of Attack: 85

Instances of custom intelligence based on indicators of attack further emphasize our commitment to proactively identifying and mitigating potential cybersecurity threats. The count of 85 reflects a targeted approach to threat detection.

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

Cross Site Tracing

Cross Site Tracing (XST) allows a malicious actor to pilfer the user's session cookie and potentially acquire other authentication credentials found in the HTTP request header. This occurs during the communication between the victim's browser and the web server of the target system.

Reflection Injection

An attacker provides a value to the target application, utilized by reflection methods to identify a class, method, or field. In Java, reflection libraries enable inspecting, loading, and invoking classes by name. If the adversary controls the input, including class/method/field names or method parameters, they can manipulate the application to invoke incorrect methods, access random fields, or load malicious classes they created. This may result in the application exposing sensitive data, producing inaccurate results, or allowing the adversary to take control.

Signing Malicious Code

The attacker obtains code signing credentials from a production environment and uses them to sign malicious content with the developer's key. Developers often use signing keys to sign code, and when users or applications verify the signatures, they trust that the code is from the key owner and hasn't been altered. By extracting signing credentials, the attacker can sign their own code, leading users or verification tools to believe it's from the legitimate developer. This allows the adversary to execute arbitrary code on the victim's computer, distinct from CAPEC-673 as the adversary is performing the code signing

DNS Cache Poisoning

A DNS server translates domain names (e.g., www.example.com) into IP addresses for internet communication. An adversary manipulates a public DNS cache, causing specific names to resolve to incorrect addresses they control. As a result, client applications relying on the targeted cache are directed to an address different from the legitimate one. This can be exploited by adversaries to guide clients to malicious sites, installing malware or participating in Pharming attacks.

Physically Hacking Hardware

An adversary takes advantage of access control vulnerabilities to gain entry to the currently installed hardware. Subsequently, they proceed to make alterations or covertly replace a hardware component, compromising the system's integrity with the intention of executing an attack.

DLL Side-Loading

An attacker implants a malicious version of a Dynamic-Link Library (DLL) in the Windows Side-by-Side (WinSxS) directory, deceiving the operating system into loading the malicious DLL instead of a legitimate one. Programs typically indicate DLL locations through WinSxS manifests or DLL redirection. If not specified, Windows searches predefined directories, making applications susceptible to side-loading if DLL requirements are improperly defined or WinSxS manifests lack explicit DLL characteristics.

Protocol Manipulation

An adversary manipulates a communication protocol to execute an attack, potentially enabling impersonation, disclosure of sensitive information, session outcome control, or other malicious activities. This form of attack focuses on exploiting faulty assumptions in protocol implementation, incorrect protocol implementations, or vulnerabilities inherent in the protocol.

Evercookie

An attacker deploys an exceptionally persistent cookie that remains on the user's device even after attempted removal. This cookie is stored in over ten locations, and when the victim clears the cookie cache using conventional browser methods, the operation eliminates the cookie from some locations but not all. Malicious code then reproduces the cookie from the remaining locations, persisting across various storage points. Notably, failure to delete the cookie in just one location leads to its resurrection everywhere. The evercookie is designed to endure across different browsers by leveraging shared stores, such as Local Shared Objects.

SoundSquatting

An attacker registers a domain name that phonetically resembles a trusted domain but is spelled differently. A SoundSquatting attack capitalizes on user confusion between the two words, redirecting Internet traffic to destinations controlled by the adversary. SoundSquatting doesn't necessitate an attack on the trusted domain or intricate reverse engineering

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

New WailingCrab Malware Loader Spread Through Cargo-themed Emails

IBM X-Force researchers examined sophisticated malware called WailingCrab, which spreads via cargo-themed emails and distributes the Ursnif trojan. Developed by the TA544 threat actor, the malware establishes C2 communication using the MQTT protocol by secretly storing its components on popular platforms such as Discord. The attacks start via emails with PDF attachments and are designed to download and run the installer hosted on Discord via URLs containing JavaScript files. Recent versions receive shellcode-based payloads via C2 directly over the MQTT protocol.

New Variant of Agent Tesla Malware Utilizes ZPAQ Compression Technique in Email Attacks

A new version of Agent Tesla malware uses the ZPAQ compression format to carry out email attacks. Attacks usually include a ZPAQ file attachment that looks like a PDF document. When the file is opened, a bloated .NET application appears and artificially increases its size to bypass security measures. The malware uses common file extensions to disguise traffic and infects the endpoint using a legitimate code protection software called .NET Reactor. Command and control communication takes place over Telegram. This development shows that threat actors are attempting to distribute malware using unusual file formats, so users should be cautious and keep their systems up to date.

SecuriDropper: New Android Dropper Service Bypassing Google's Defenses

Security researchers have identified SecuriDropper, a new dropper service for Android that distributes malware by circumventing Google's latest security measures. SecuriDropper, which aims to bypass the security measures introduced by Android 13, manages to bypass restrictions such as Limited Settings to prevent sideloaded apps from obtaining permissions without being detected. Dropper disguises itself as a harmless app, using names like "com.appd.instll.load" for Google and Google Chrome. SecuriDropper implements a different installation procedure using a new Android API and facilitates the installation of the malicious payload by making victims click the "Reload" button within the app. Such dropper services are emerging as effective tools used by cybercriminals to circumvent Android security and distribute malware.

SideCopy Exploits WinRAR Vulnerability in Attacks

The SideCopy threat actor, associated with Pakistan, has been conducting attacks against Indian government agencies with remote access trojans exploiting the WinRAR vulnerability. SideCopy, known as the Transparent Tribe (APT36) subgroup, has been active since at least 2019 and has been acting aggressively against India. In May, SideCopy participated in a phishing campaign using headers directed at the Defence Research and Development Organisation of India (DRDO). In attacks targeting Linux and Windows, malware such as Ares RAT was distributed using a Golang-based ELF binary. While SideCopy continues to target Indian defence organisations using zero-day vulnerability, APT36 is trying to expand its Linux plot and contributing to the spread of Ares, a Python RAT.

infinitum IT
Power of integrated Security

MDR Insights

“November”

f | in
infinitumitlabs