infinitum IT
Power of integrated Security

MDR Insights

"September"

infinitumitlabs

Content

MDR REPORT

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

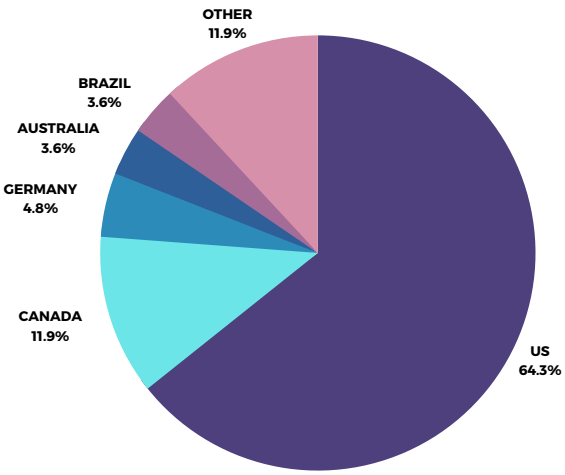
This MDR report provides an analysis of threats and security incidents detected in our company's information systems. The report covers topics such as summary and impact of incidents during the period under review, type and source of threats, status of security measures and recommendations.

Ransomware Groups

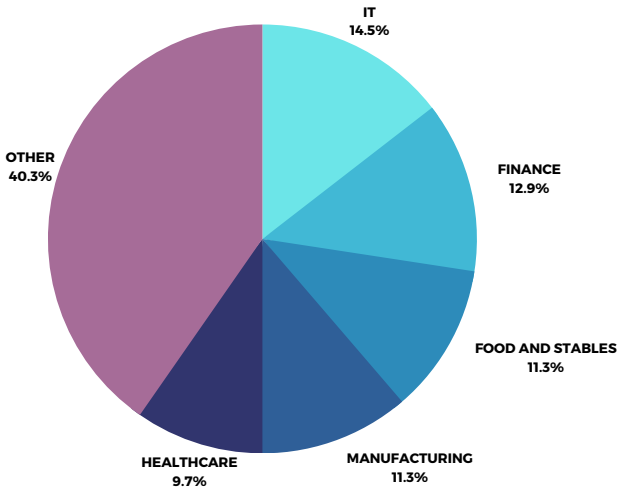
1. Royal Ransomware Group

Total Number of Attacks: 90

Attack Graph by Country



Attack Graph by Sectors



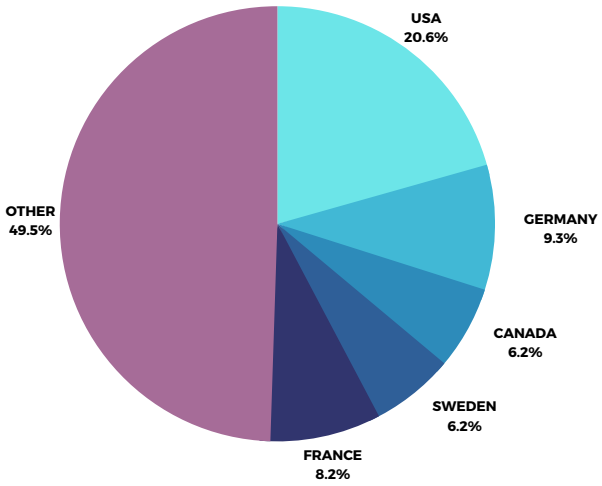
Originally known as Zeon in January 2022, the Royal ransomware group rebranded itself as "Royal" in September 2022. Since then, they have been targeting a wide range of industries, including Manufacturing, Healthcare, Food, and Education. While the majority of their victims have been based in the United States, the Royal Ransomware Group has shown no hesitation in targeting countries worldwide, including Europe and Latin America.

This group exhibits a combination of both old and new hacking techniques. They employ callback phishing to entice victims into unwittingly installing remote desktop malware, enabling threat actors to infiltrate the victim's system with relative ease. This indicates that the individuals behind the Royal Ransomware Group possess a high level of expertise and experience.

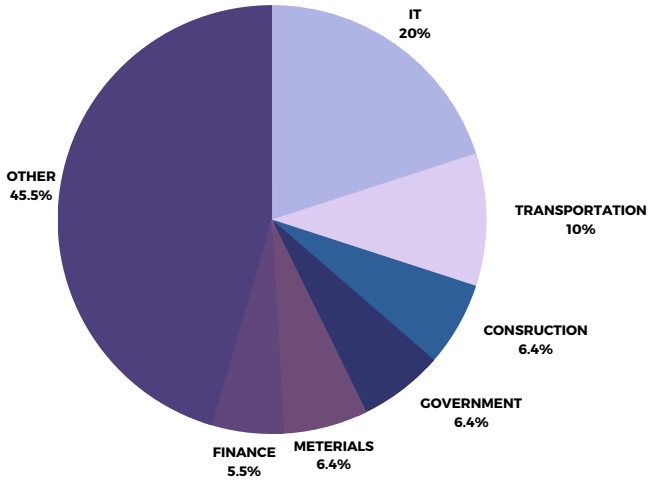
2. Play Ransomware Group

Total Number of Attacks: 110

Attack Graph by Country



Attack Graph by Sectors



Operating under the name "Play," this hacker collective has gained notoriety for its campaigns of ransomware extortion against both corporate entities and governmental institutions. The emergence of the Play group occurred in 2022, and since then, their attacks have spread across various countries, including the United States, Brazil, Argentina, Germany, Belgium, and Switzerland.

Security analysts have strongly suggested potential ties between the Play group and Russia, as the encryption methodologies employed bear striking similarities to those employed by other ransomware groups with known Russian affiliations, such as Hive and Nokoyawa.

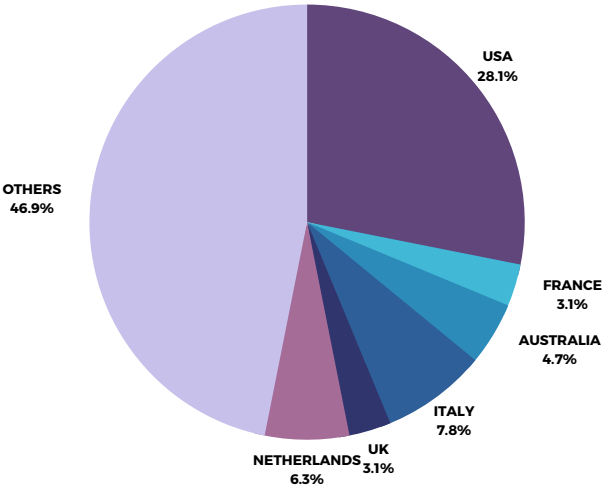
The Play Ransomware group follows a systematic approach to infiltrate their targets. They begin by exploiting known vulnerabilities, particularly the FortiOS vulnerabilities CVE-2018-13379 and CVE-2020-12812, along with exposed RDP (Remote Desktop Protocol) servers. Once initial access is secured, they deploy 'lolbins' binaries, a tactic frequently employed by ransomware groups, as part of their malicious activities.

To propagate their malware within the victim's internal network, Play utilizes Group Policy Objects and executes scheduled tasks, PsExec, or wmic commands. Upon achieving complete control over the internal network, they proceed to encrypt files, appending the '.play' extension to their compromised data. This systematic and well-coordinated approach underscores the sophistication and operational capabilities of the Play Ransomware group.

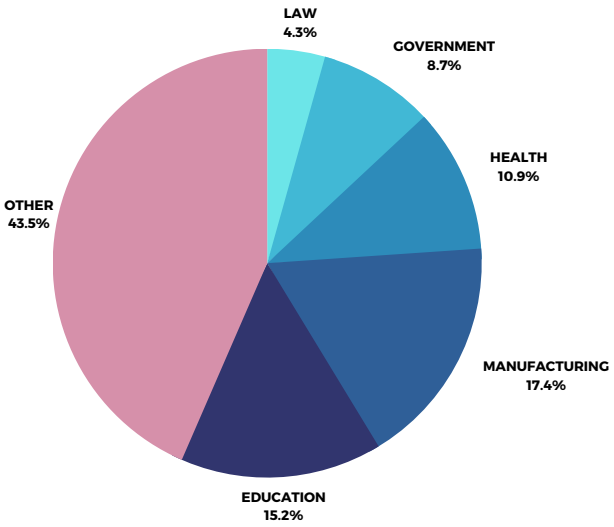
3. ALPHV Ransomware Group

Total Number of Attacks: 47

Attack Graph by Country



Attack Graph by Sectors



First observed in 2021, BlackCat ransomware, also known as AlphaVM, AlphaV, or ALPHV, has quickly gained notoriety as a groundbreaking addition to the ransomware landscape. What sets BlackCat apart from others is that it is the first major professional ransomware family written in the Rust programming language. This unique feature allows cybercriminals to adapt the malware to a variety of operating systems, including Windows and Linux, making it a versatile threat to a wide range of corporate environments.

The Rust programming language provides cybercriminals with a powerful tool to customize malware, and BlackCat exploits this ability to its fullest. In addition to encrypting data and demanding ransom, BlackCat poses an additional threat by disclosing leaked data and threatening victims with Distributed Denial of Service (DDoS) attacks against the victim's infrastructure to force them to pay the ransom.

BlackCat's activities sent shockwaves across many industries. Since its emergence, the healthcare industry, financial institutions, energy companies and government agencies have fallen victim to these insidious attacks. These sectors, which contain sensitive data and provide critical services, have been priority targets.

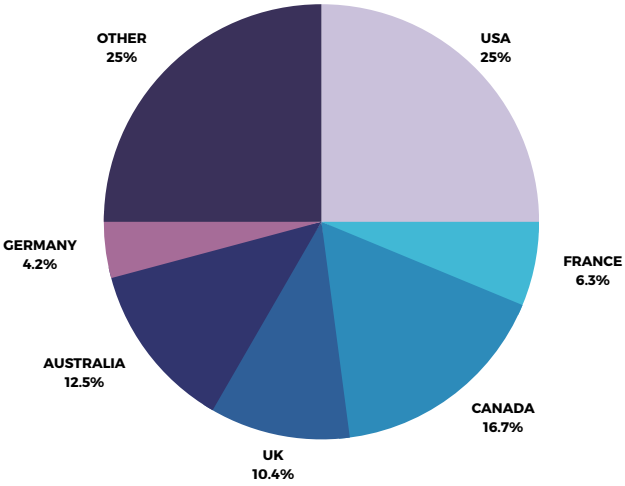
As a testament to its relentless evolution, BlackCat has released the latest updated version known as "Sphynx". This release showcases a more complex execution process compared to previous versions and highlights the group's commitment to staying ahead of security measures
The threat posed by BlackCat (ALPHV) is a persistent and evolving problem for organizations worldwide. While there has been an increase in the group's activities since August 2023, sectors are increasingly exposed to attacks.

As a result, it is crucial for organizations to be aware of the tactics, techniques and procedures (TTPs) used by the BlackCat(ALPHV) group. Implementing strong cybersecurity measures, sharing threat intelligence, and promoting international cooperation are essential steps in countering this evolving threat.

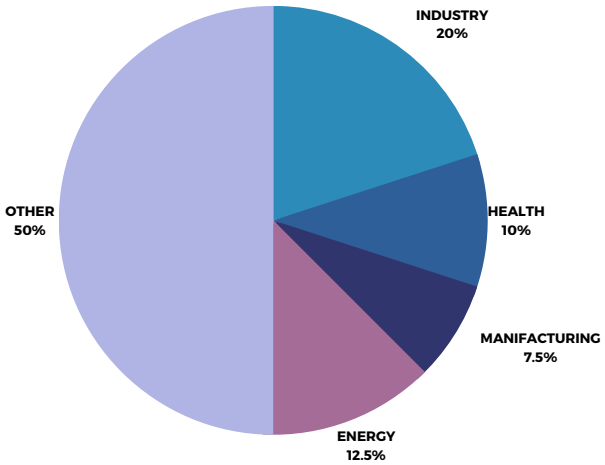
4. LockBit Ransomware Group

Total Number of Attacks: 55

Attack Graph by Country



Attack Graph by Sectors



The activities of the LockBit Ransomware Group paint a concerning picture of the current cybersecurity landscape. Their focus on targeting critical sectors is particularly alarming, as it highlights their willingness to exploit vulnerabilities that could have severe consequences for organizations and individuals alike. Given the rising frequency of cyberattacks across various sectors, immediate action is imperative to safeguard sensitive data and ensure the uninterrupted functioning of essential services.

Moreover, the group's diversified range of attacks on industries such as finance, manufacturing, government, technology, and infrastructure underscores their broad scope, posing threats to economic stability and national security. The high number of attacks categorized as "OTHER" raises concerns about potential unexpected and unconventional targets. This emphasizes the urgent need for comprehensive cybersecurity strategies across all sectors to effectively mitigate risks.

The concentration of LockBit attacks on different regions globally highlights the group's interest in pursuing a wide-ranging strategy. These attacks not only result in financial losses but also disrupt crucial sectors, causing a ripple effect on a global scale. Additionally, LockBit's willingness to explore vulnerabilities in various regions poses a challenge for international efforts to combat their activities effectively. This underscores the importance of global cooperation and cybersecurity measures to counter the evolving threat landscape posed by ransomware groups like LockBit.

Top Trending CVEs of September 2023

Windows TCP/IP Information Disclosure Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-38160	5.5	Medium	Information Disclosure
CVE-2023-38146	8.8	High	Remote Code Execution
CVE-2023-41764	5.5	Medium	Remote Code Execution

CVE-2023-38160 is a buffer overflow vulnerability in the Linux kernel's **tcp_sendmsg()** function. This vulnerability can be exploited by an attacker to execute arbitrary code on the victim's system. The vulnerability is caused by an integer overflow in the **tcp_sendmsg()** function. This overflow can be triggered by an attacker sending a specially crafted TCP packet to the victim's system. The overflow can cause the kernel to write data beyond the bounds of the allocated buffer. This can overwrite other data in memory, including code. If the attacker is able to control the data that is overwritten, they can execute arbitrary code on the victim's system.

Mitigations

A patch is available for CVE-2023-38160, CVE-2023-38146 and CVE-2023-41764 . To apply this patch, you need to download and install the updates. In addition to this:

- Upgrade to a patched version of the Linux kernel. The vulnerability has been patched in Linux kernel versions 6.1.2 and later.
- Disable TCP segmentation offloading (TSO). TSO can increase the risk of exploitation of this vulnerability. To disable TSO, run the following command:

  echo 0 | sudo tee /sys/kernel/net/ipv4/tcp_tso

- Use a firewall to block incoming TCP packets with suspicious flags. An attacker may try to exploit this vulnerability by sending TCP packets with SYN and ACK flags set. A firewall can be used to block these packets.
- Monitor system logs for suspicious activity. If the vulnerability is exploited, it may generate suspicious log entries. Monitor system logs for signs of compromise.

Android System Remote Code Execution Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-20951	9.8	Critical	Remote Code Execution

CVE-2023-20951 is a remote code execution vulnerability in the Linux kernel's **gatt_process_prep_write_rsp()** function. This function is used to handle GATT prepare write responses from Bluetooth devices. The vulnerability is caused by an out-of-bounds write in the **gatt_process_prep_write_rsp()** function. This out-of-bounds write can be triggered by an attacker sending a specially crafted GATT prepare write response to the victim's device. The out-of-bounds write can cause the kernel to write data beyond the bounds of the allocated buffer. This can overwrite other data in memory, including code. If the attacker is able to control the data that is overwritten, they can execute arbitrary code on the victim's device.

Mitigations

A patch is available for CVE-2023-20951. To apply this patch, you need to download and install the updates. Additionally:

- Upgrade to a patched version of the Linux kernel. The vulnerability has been patched in Linux kernel versions 6.1.2 and later.
- Disable Bluetooth on devices that do not need it. If a device does not need to use Bluetooth, it should be disabled to reduce the risk of exploitation.
- Use a firewall to block incoming Bluetooth connections from untrusted devices. A firewall can be used to block incoming Bluetooth connections from untrusted devices, which can reduce the risk of exploitation.
- Monitor system logs for suspicious activity. If the vulnerability is exploited, it may generate suspicious log entries. Monitor system logs for signs of compromise.

Android System Remote Code Execution Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-20954	9.8	Critical	Remote Code Execution

CVE-2023-20954 is a remote code execution vulnerability in the Linux kernel's **SDP_AddAttribute** function. This function is used to add attributes to SDP records.

The vulnerability is caused by an out-of-bounds write in the **SDP_AddAttribute** function. This out-of-bounds write can be triggered by an attacker sending a specially crafted SDP request to the victim's device.

The out-of-bounds write can cause the kernel to write data beyond the bounds of the allocated buffer. This can overwrite other data in memory, including code. If the attacker is able to control the data that is overwritten, they can execute arbitrary code on the victim's device.

Mitigations

A patch is available for CVE-2023-20954. To apply this patch, you need to download and install the Teams updates from Microsoft's website.

- Upgrade to a patched version of the Linux kernel. The vulnerability has been patched in Linux kernel versions 6.1.2 and later.
- Disable SDP on devices that do not need it. If a device does not need to use SDP, it should be disabled to reduce the risk of exploitation.
- Use a firewall to block incoming SDP requests from untrusted devices. A firewall can be used to block incoming SDP requests from untrusted devices, which can reduce the risk of exploitation.
- Monitor system logs for suspicious activity. If the vulnerability is exploited, it may generate suspicious log entries. Monitor system logs for signs of compromise.

WebP/libwebp Remote Code Execution Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-4863	8.8	High	Remote Code Execution

CVE-2023-4863 is a critical vulnerability in the libwebp library, which is used to encode and decode images in the WebP format. The vulnerability is a buffer overflow that can be exploited to execute arbitrary code on a victim's system.

The vulnerability can be exploited by a remote attacker by tricking a victim into opening a specially crafted WebP image file. The image file can be embedded in a web page, email attachment, or other document. Once the victim opens the image file, the vulnerability can be exploited to execute arbitrary code on the victim's system without any user interaction.

The vulnerability affects all versions of libwebp prior to 1.3.2. It is also known to be actively exploited in the wild.

Mitigations

A patch is available for CVE-2023-36845 and CVE-2023-36846. To apply this patch, you need to download and install the updates. In addition to these:

- The best way to mitigate CVE-2023-4863 is to apply the kernel patch that was released by the Linux kernel developers. This patch fixes the race condition that is the cause of the vulnerability.
- Disabling swap can help to mitigate the impact of CVE-2023-4863. This is because the vulnerability requires the attacker to be able to allocate memory from swap. Disabling swap will make it more difficult for the attacker to exploit the vulnerability.
- Using a non-default kernel command line can also help to mitigate the impact of CVE-2023-4863. This is because the vulnerability can be exploited by an attacker who has access to the kernel command line.
- Follow these mitigations:

1. Set the **CONFIG_SECCOMP** kernel configuration option to y. This option enables the kernel's seccomp filter, which can help to prevent the attacker from executing arbitrary code.
2. Set the **CONFIG_SECCOMP_FILTER** kernel configuration option to y. This option enables the kernel's extended seccomp filter, which provides more granular control over the allowed system calls.
3. Set the **CONFIG_SECCOMP_FILTER_ALLOW_SYSCALL** kernel configuration option to n. This option disables the kernel's default allowlist of system calls, which can help to prevent the attacker from exploiting the vulnerability.

ImageIO Remote Code Execution Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-41064	7.8	High	Remote Code Execution

CVE-2023-41064 is a buffer overflow vulnerability in the ImageIO framework, which allows applications to read and write most image file formats. The vulnerability can be triggered with a maliciously crafted image and can lead to arbitrary code execution.

This vulnerability was exploited in a zero-day attack against iPhones in September 2023. The exploit was capable of compromising iPhones running the latest version of iOS (16.6) without any interaction from the victim.

The vulnerability has been patched in iOS 16.6.1 and iPadOS 16.6. Users of affected devices should update to the latest version of the operating system as soon as possible.

Mitigations

A patch is available for CVE-2023-36845 and CVE-2023-36846. To apply this patch, you need to download and install the Junos OS updates from the Juniper Networks website.

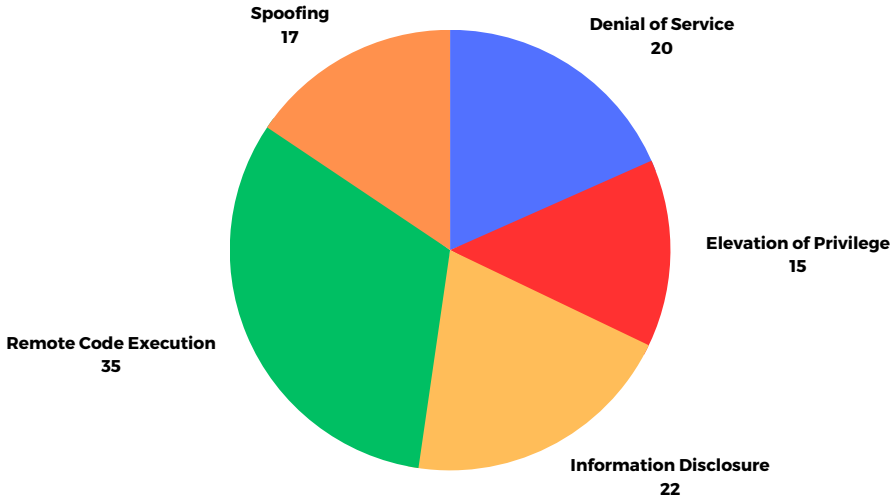
- The best way to mitigate CVE-2023-41064 is to apply the software update that was released by the software vendor. This update fixes the buffer overflow vulnerability that is the cause of the vulnerability.
- Disabling webp support can help to mitigate the impact of CVE-2023-41064. This is because the vulnerability can only be exploited by an attacker who can send a malicious webp image to the victim.
- Using a web filter can also help to mitigate the impact of CVE-2023-41064. This is because a web filter can be used to block malicious webp images from being downloaded.
- Follow these mitigations:

1. On macOS, set the NSAppTransportSecurity value to allowArbitraryLoads to NO. This will prevent the system from loading webp images from untrusted sources.

2. On iOS, set the AllowArbitraryLoads value to NO in the Info.plist file. This will prevent the app from loading webp images from untrusted sources.

3. On Android, set the allowArbitraryLoads value to false in the AndroidManifest.xml file. This will prevent the app from loading webp images from untrusted sources.

September 2023 Risk Analysis



Drawing upon the numerical data derived from our September 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.

One notable development is the substantial increase in Remote Code Execution (RCE) vulnerabilities compared to the previous month. RCE attacks now account for a significant 35% 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.

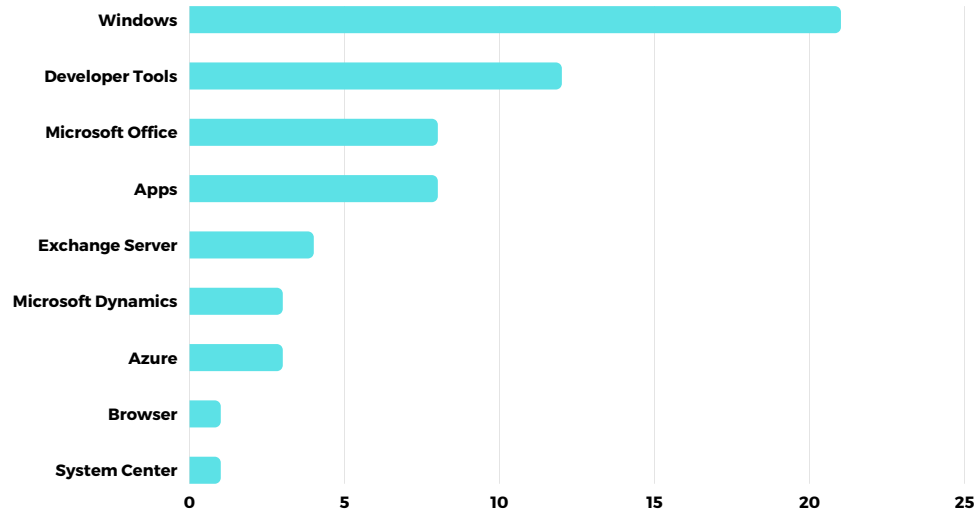
Meanwhile, Denial of Service (DoS) attacks, contributing to 20% of the identified risks, continue to pose a substantial threat. DoS attacks aim to overwhelm a system, network, or application with an excessive volume of traffic, rendering it unresponsive or inaccessible to legitimate users. Effectively 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 22% 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 17% 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 September 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, September 2023



The distribution of Microsoft security updates in September provides valuable insights into the focus of the company's security efforts during this period. Windows, as the flagship operating system, understandably received the highest number of patches, with a count of 21. This emphasizes the continuous effort to address potential vulnerabilities and ensure the security and stability of the operating system.

Developer Tools, which are used to create and develop software, received 12 patches. This highlights the importance of securing the tools that developers rely on to build the software that we use every day.

Apps, which includes a variety of products such as Microsoft Edge, Microsoft Teams, and Windows Defender, received 8 patches. This reflects the attention given to securing the applications that we use on a daily basis.

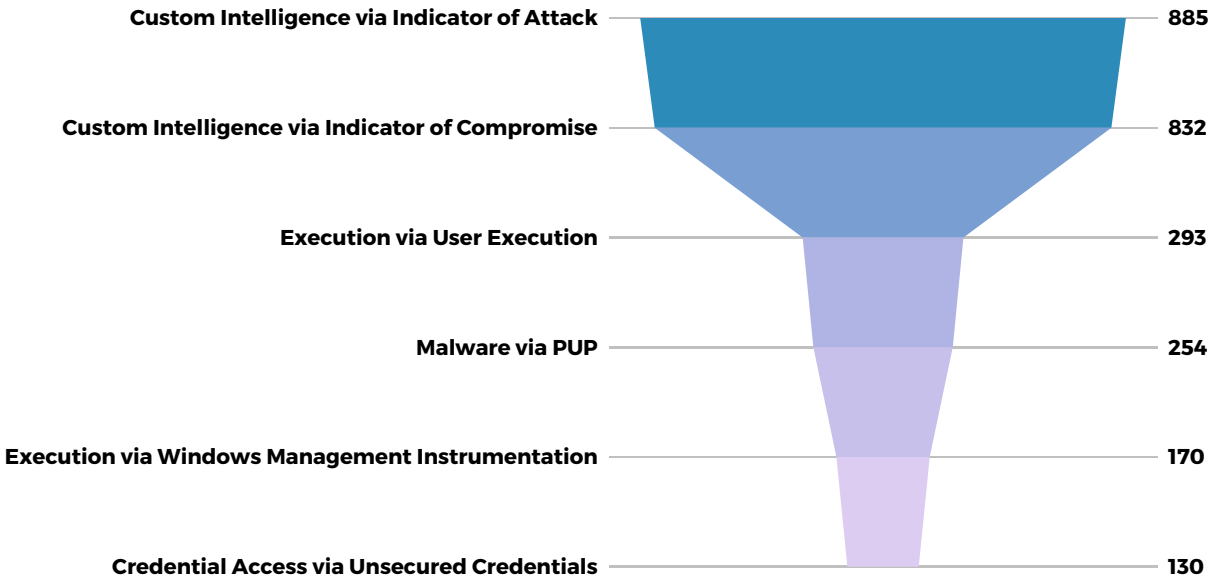
Microsoft Office, a critical productivity suite, received 8 patches. This emphasizes the commitment to ensuring the security of this product, which is often targeted by attackers.

The other product families received a total of 13 patches. This includes Exchange Server, a communication software produced by Microsoft , and Others, which includes a variety of other products such as Microsoft Dynamics, Azure and System Center.

Overall, this data highlights Microsoft's ongoing commitment to addressing security vulnerabilities across various product families. It also emphasizes the importance of regular updates and the proactive approach taken to enhance the security of both widely used and niche products. Organizations that rely on Microsoft technologies should take note of these patch distributions and prioritize timely updates to bolster their cybersecurity posture and protect against 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 our Monthly MDR Report, we analyze cybersecurity data from our clients' systems. This data reveals various types of cyber threats and the number of times they've been detected:

Custom Intelligence via Indicator of Attack (IoA): We found 885 instances where our systems detected unusual activities that could indicate targeted attacks. These activities are based on specific signs of potential threats.

Custom Intelligence via Indicator of Compromise (IoC): In 832 cases, we identified potential signs that our clients' systems might have been breached or compromised. This information helps us react promptly to potential security incidents.

Execution via User Execution: We noticed 293 instances where actions initiated by users led to the execution of potentially risky processes or programs. This could signal attempts to compromise the system.

Malware via Potentially Unwanted Programs (PUP): Our systems detected 254 cases where malware was associated with Potentially Unwanted Programs (PUPs). These are often unwanted or potentially harmful software.

Execution via Windows Management Instrumentation (WMI): There were 170 instances where execution took place through Windows Management Instrumentation, which can be used by attackers to run commands on Windows systems.

Credential Access via Unsecured Credentials: In 130 cases, we identified unauthorized access to credentials due to inadequate security measures. Compromised credentials can be a significant security risk.

These insights help us provide a clear picture of potential threats and vulnerabilities in our clients' environments, allowing us to take proactive measures to enhance their cybersecurity defenses.

Common Types Attack Vectors

Risk Severity

Critical **High** **Medium**

Action Spoofing

An adversary has the ability to obscure one action as another, effectively deceiving a user into initiating a different action than what they intended. For instance, a user may be led to believe that clicking a button will trigger a query submission, but in reality, it initiates a software download. Adversaries can execute this form of attack using either social manipulation tactics, like convincing a victim to perform the action, exploiting a user's inherent trust or tendencies, or employing technical means such as clickjacking. In the case of clickjacking, users perceive one interface, but they are unwittingly interacting with a concealed, second interface

DNS Rebinding

An adversary provides content hosted on a server whose IP address is initially looked up using a DNS server under the adversary's control. Once a web browser or a similar client establishes the first connection, the adversary alters the IP address associated with their server's name. They redirect it to an internal address within the target organization, which is not publicly accessible. This manipulation allows the adversary to have the web browser access the internal address on their behalf.

Leveraging/Manipulating Configuration File Search Paths

This attack pattern involves an adversary inserting a malicious resource into a program's standard path. As a result, when a known command is executed, the system inadvertently runs the malicious component instead. The adversary can achieve this by either altering the program's search path, such as the PATH variable or classpath, or by manipulating resources along the path to point to their malicious components. Applications like J2EE and other component-based systems, which rely on numerous dependencies to function, can have extensive lists of components to execute. If the attacker gains control over one of these libraries or references, they can bypass the application's security controls.

Server Side Include (SSI) Injection

An attacker can utilize Server Side Include (SSI) Injection to transmit code to a web application, which is then executed by the web server. This technique allows the attacker to achieve outcomes akin to Cross-Site Scripting, specifically, executing arbitrary code and revealing information. However, SSI directives are not as potent as a full-fledged scripting language, resulting in more limited capabilities. Nevertheless, the attacker can conveniently gain unauthorized access to sensitive files, such as password files, and execute commands in the system's shell.

LDAP Injection

An attacker exploits or constructs LDAP queries to compromise the security of a target. Certain applications use user inputs to generate LDAP queries processed by an LDAP server. For instance, during authentication, a user might input their username, which is then incorporated into an LDAP query. An attacker could exploit this input to inject extra commands into the LDAP query, potentially revealing sensitive data. For example, inserting '*' into the query might retrieve information about all system users. This attack resembles an SQL injection, as it manipulates a query to gain more information or influence the query's result.

Credential Stuffing

An adversary attempts well-known username and password pairs across various systems, applications, or services in an effort to obtain unauthorized access. Credential Stuffing attacks exploit the common practice of users using the same username and password combination across multiple systems, applications, and services.

Exploiting Incorrectly Configured Access Control Security Levels

An attacker capitalizes on a vulnerability in the configuration of access controls, successfully circumventing the intended safeguards and gaining unauthorized access to a system or network. It's essential to apply access controls to protect sensitive functions. However, configuring access control systems, except for the simplest cases, can be quite intricate, leaving room for errors. If an attacker discovers incorrectly configured access security settings, they may exploit this vulnerability in a cyberattack.

Inducing Account Lockout

An attacker exploits a security feature within a system, designed to thwart potential attacks, in order to carry out a denial of service attack against a legitimate system user. Many systems, for instance, incorporate a password throttling mechanism that locks an account after a certain number of incorrect login attempts. An attacker can manipulate this throttling mechanism to lock a legitimate user out of their own account. Essentially, the attacker is capitalizing on the very security measure put in place to counteract attacks.

Manipulating Opaque Client-based Data Tokens

In situations where an application stores critical data on the client-side within tokens (such as cookies, URLs, or data files), there exists the potential for manipulation of that data. If either client or server-side application components interpret this data as authentication tokens or valuable information (such as item pricing or wallet details), even subtly altering that data might prove advantageous for an attacker. In this scenario, the attacker disrupts the assumption that client-side tokens have been effectively safeguarded against tampering, whether through encryption or obfuscation.

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

ZenRAT Malware Targets Windows Users Using Fake Password Manager Software

The malicious software called ZenRAT targets Windows users using fake Bitwarden password manager installations. Users of other operating systems are directed to a harmless web page. ZenRAT is a remote access Trojan (RAT) with data theft capabilities. This software spreads through fake Bitwarden websites and offers users a malicious .NET application within fake installation packages. Users of non-Windows systems are redirected to a deceptive website. ZenRAT steals computer information and sends it to threat actors. To combat such threats, it is important to download software from reliable sources and carefully verify websites. This information comes at a time when a similar threat, Lumma Stealer, was also discovered.

"Iran-Based APT Group OilRig Utilizes New Malware "Menorah" for Covert Operations"

Iran-backed group OilRig is conducting a spear-phishing campaign using a new malware called Menorah. Menorah is designed for cyber espionage, with various capabilities like machine identification and file manipulation. While the exact targets are unknown, at least one organization in Saudi Arabia has been affected. This attack is based on an evolving phishing campaign distributing a new SideTwist malware variant. OilRig's ongoing efforts to enhance their malware are evident. Menorah, in its latest attack, creates a scheduled task for persistence and drops an executable file while waiting for further instructions. However, the command and control server is currently inactive. APT34 is expected to continue using customized routines and social engineering for infiltration and cyber espionage.

Google Addresses Security Vulnerability Exploited in Targeted Attacks

Google Releases Update for Zero-Day Exploited in Attacks - Google has addressed CVE-2023-5217, a critical security vulnerability found in the VP8 compression format within the libvpx video codec library. This zero-day flaw, discovered by Clément Lecigne of Google's Threat Analysis Group on September 25, 2023, was actively used in targeted attacks by a commercial spyware vendor. This discovery brings the total number of fixed zero-days in Google Chrome this year to five. Users are urged to update to Chrome version 117.0.5938.132 on Windows, macOS, and Linux to enhance security. Chromium-based browser users should also apply patches once available.

CVE-2023-2033 (CVSS score: 8.8) - Type confusion in V8.
CVE-2023-2136 (CVSS score: 9.6) - Integer overflow in Skia.
CVE-2023-3079 (CVSS score: 8.8) - Type confusion in V8.
CVE-2023-4863 (CVSS score: 8.8) - Heap buffer overflow in WebP.

infinitum IT
Power of integrated Security

MDR Insights

"September"

infinitumitlabs