infinitum IT
Power of Integrated Security

MDR Insights

"October"

infinitumitlabs

Content

Ransomware Groups.....03
Lost Trust Ransomware Group 03
ALPHV Ransomware Group 04
Play Ransomware Group 05
LockBit Ransomware Group 06
Top Trending CVEs of October 2023.....07
Windows TCP/IP Information Disclosure Vulnerability.....07
Android System Remote Code Execution Vulnerability.....08
Android System Remote Code Execution Vulnerability.....09
WebP/libwebp Remote Code Execution Vulnerability.....10
ImageIO Remote Code Execution Vulnerability.....11
October 2023 Risk Analysis.....12
Patches by Product Family, October 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 October 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.

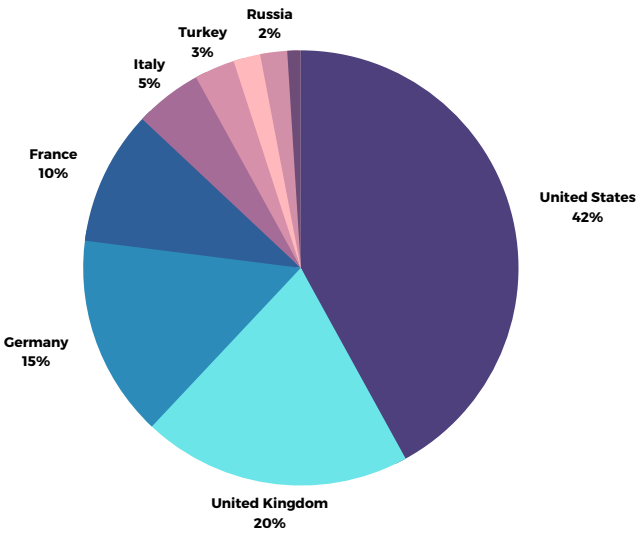
This MDR report provides an analysis of threats and security incidents detected in our company's information systems. The report covers topics such as summary and impact of incidents during the period under review, type and source of threats, status of security measures and recommendations.

Ransomware Groups

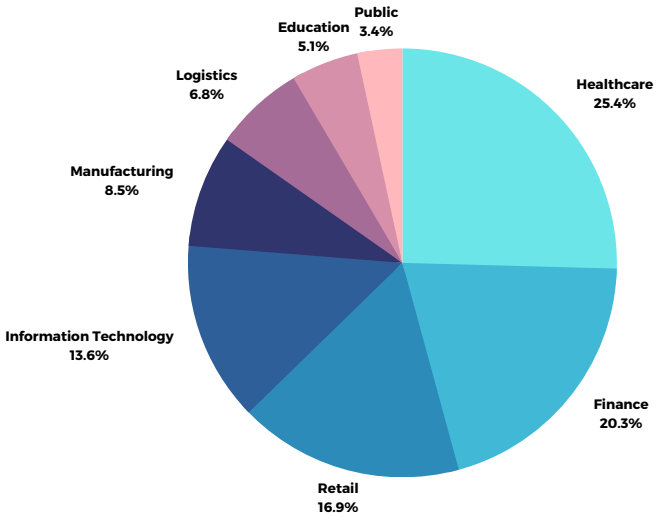
1. Lost Trust Ransomware Group

Total Number of Attacks: 53

Attack Graph by Country



Attack Graph by Sectors



Lost Trust Ransomware group is a ransomware group that emerged in 2023 and rapidly became a global threat. The group infiltrates computers using various methods, encrypts data, and demands a ransom.

In October 2023, the group carried out attacks, with 42% of them targeting the United States, 20% in the United Kingdom, and 15% in Germany. Other targeted countries include France, Italy, Turkey, Spain, Russia, and China.

This Ransomware group primarily targets the healthcare, financial, and retail sectors. These sectors are appealing targets for the group due to their possession of critical and sensitive information.

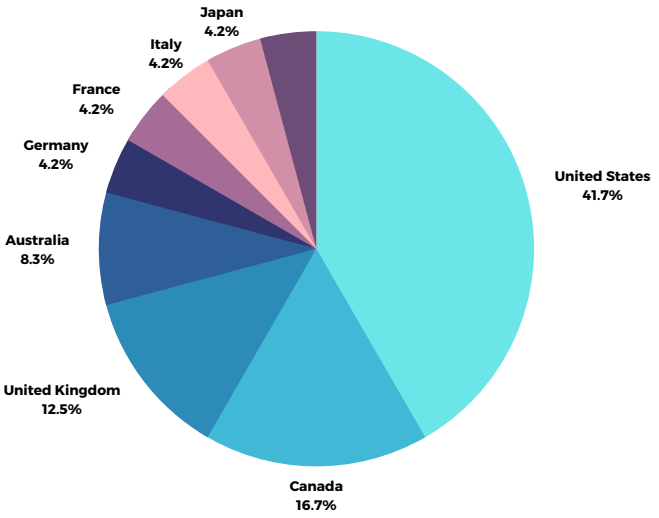
Lost Trust Ransomware employs a variety of methods for their attacks, including malicious software distributed through email, ransomware through websites, and gaining unauthorized access using remote access software.

The group typically demands Bitcoin as ransom from their victims. Failure to pay the ransom may result in the permanent loss of data.

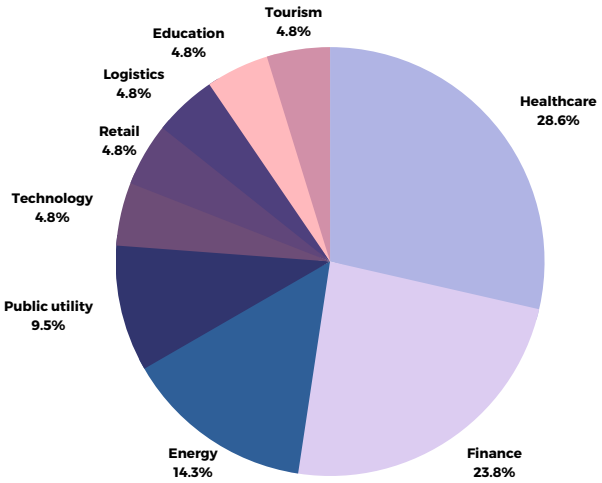
2. ALPHV Ransomware Group

Total Number of Attacks: 120

Attack Graph by Country



Attack Graph by Sectors



In October 2023, the ALPHV Ransomware group, a prolific ransomware threat actor, significantly increased its attacks compared to September. The group primarily targeted the healthcare, financial, and energy sectors.

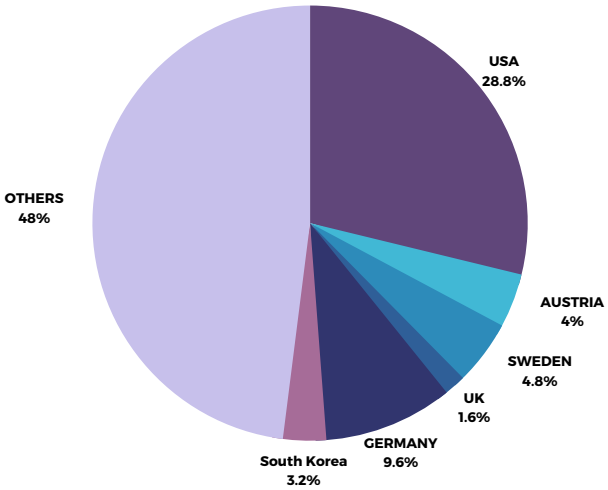
The ALPHV Ransomware group often utilizes a malicious software distribution tool known as ContiLoader to carry out its attacks. Using this tool, the group creates a backdoor into the networks of organizations for data encryption. Subsequently, the group demands ransom payments from these organizations.

The ALPHV Ransomware group has become one of the most active ransomware groups in recent years. The group poses a serious threat due to its advanced attack techniques and high ransom demands.

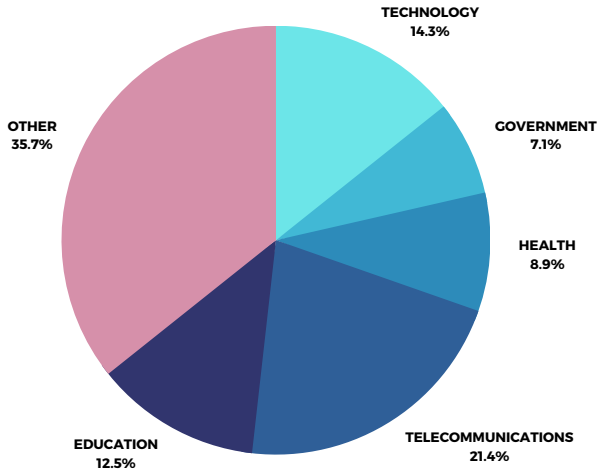
3. Play Ransomware Group

Total Number of Attacks: 28

Attack Graph by Country



Attack Graph by Sectors



The emergence of "Play ransomware" in July 2022 marked a significant and concerning development in the landscape of cyber threats. This ransomware strain, characterized by its unique behavior of appending the ".play" extension to encrypted files and presenting a ransom note with only the word "PLAY" and contact information for the ransomware group, quickly garnered attention. However, what is most alarming is the group's apparent determination to continuously evolve and adapt.

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.

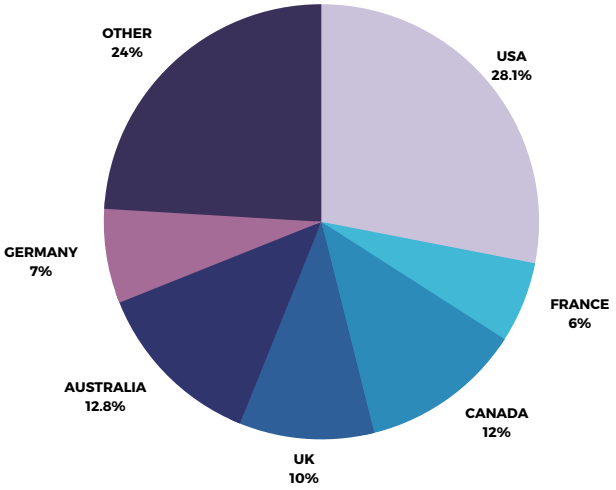
In their quest to achieve these objectives, the Play ransomware group has exhibited an adeptness at leveraging new vulnerabilities and incorporating fresh tools into their attacks. Notably, they have targeted vulnerabilities such as ProxyNotShell, OWASSRF, and Microsoft Exchange Server Remote Code Execution.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

A noticeable escalation in attacks was observed in October, indicating an intensification of the threat posed by the Play ransomware group. Given these developments, it is imperative for organizations to maintain a heightened awareness of the Play ransomware group's dynamic tactics and expanding toolkit. 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.

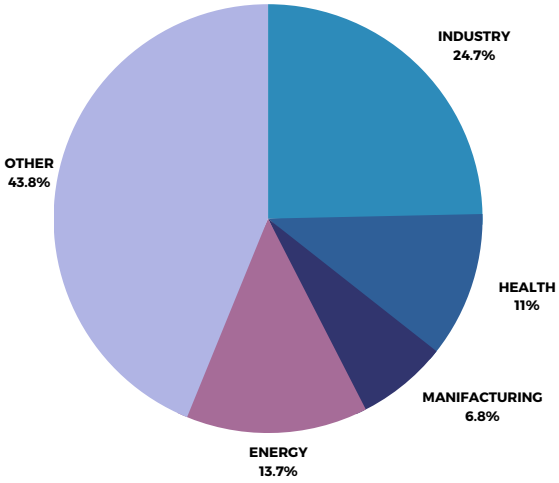
4. LockBit Ransomware Group

Total Number of Attacks: 47

Attack Graph by Country



Attack Graph by Sectors



The activities of the LockBit Ransomware Group increased in October. Their focus on targeting critical sectors is particularly concerning because it reveals their willingness to exploit vulnerabilities that could have serious consequences for both organizations and individuals. Considering the increasing frequency of cyber attacks across various sectors, urgent action is imperative to protect sensitive data and ensure the uninterrupted operation of essential services.

Moreover, the group's diverse attacks on sectors such as finance, manufacturing, government, technology, and infrastructure highlight the broad scope of attacks and pose threats to economic stability and national security. The high number of attacks classified as "OTHER" raises concerns about potential unexpected and unusual targets. This highlights the urgent need for comprehensive cybersecurity strategies across all sectors to effectively mitigate risks.

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

Top Trending CVEs of October 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.

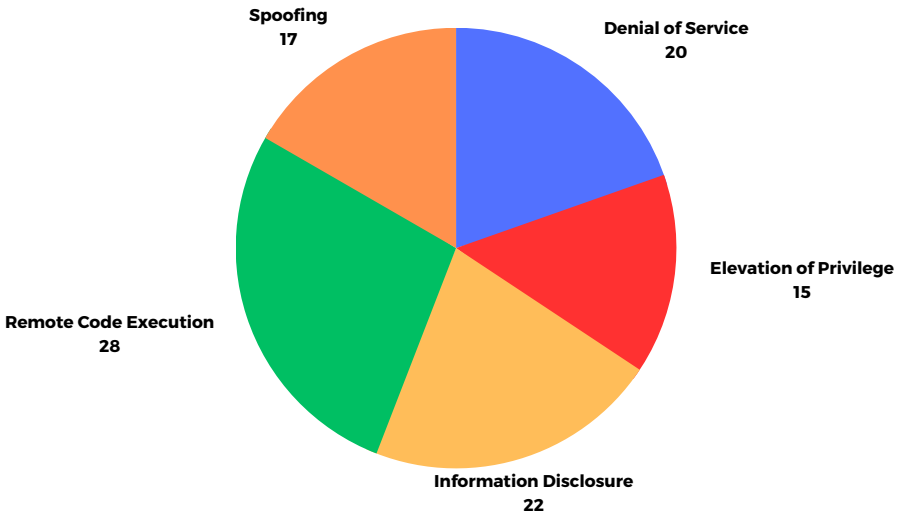
- The best way to mitigate CVE-2023-41064 is to apply the software update that was released by the software vendor. This update fixes the buffer overflow vulnerability that is the cause of the vulnerability.
- Disabling webp support can help to mitigate the impact of CVE-2023-41064. This is because the 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.

October 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 28% 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 17% 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.

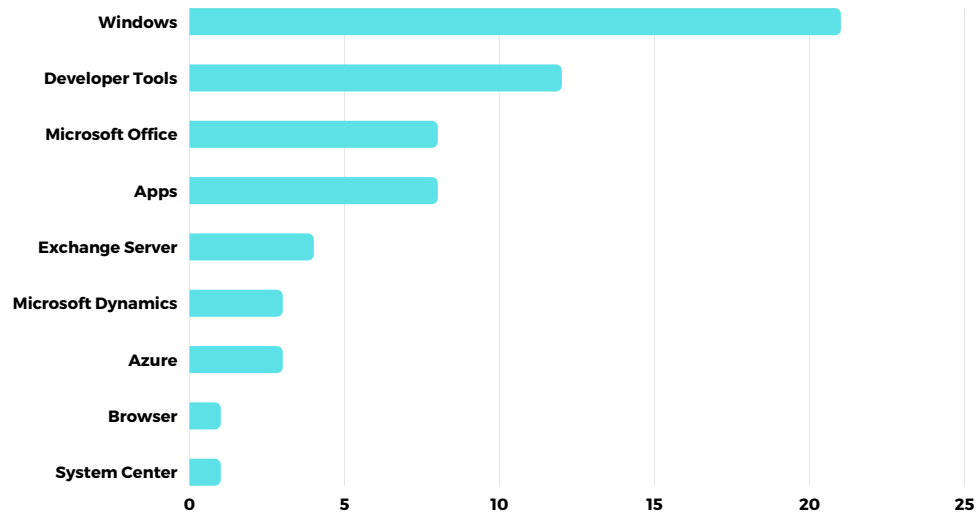
Meanwhile, Denial of Service (DoS) attacks, contributing to 20% of the identified risks, continue to pose a substantial threat. DoS attacks aim to overwhelm a system, network, or application with an excessive volume of traffic, rendering it unresponsive or inaccessible to legitimate users. Effectively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

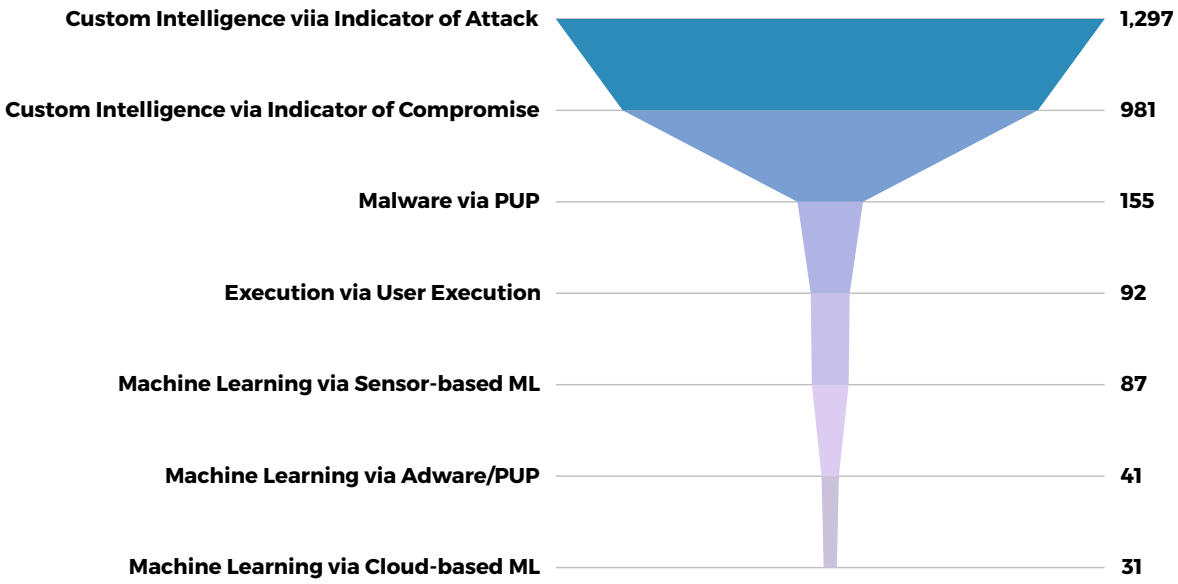
Microsoft Office, a critical productivity suite, received 8 patches. This emphasizes the commitment to ensuring the security of this product, which is often targeted by attackers.

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 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 Attack: 1297 detections
This category indicates that we identified 1297 potential attacks based on custom intelligence sources. These could be advanced threats that require specific attention and response.

Custom Intelligence via Indicator of Compromise: 981 detections
We discovered 981 indicators of compromise, which are often signs of security incidents that need further investigation and remediation.

Malware via PUP: 155 detections
155 instances of malware associated with Potentially Unwanted Programs (PUPs) were identified. These should be addressed promptly to mitigate potential risks.

Execution via User Execution: 92 detections
92 cases of executions initiated by user actions were detected. Understanding the context and nature of these executions is essential for overall system security.

Machine Learning via Sensor-based ML: 87 detections
Our sensor-based Machine Learning algorithms identified 87 potential security threats. Machine Learning can provide valuable insights into emerging risks.

Machine Learning via Adware/PUP: 41 detections
41 detections related to adware and Potentially Unwanted Programs (PUPs) were recorded. These may be causing disruptions and should be addressed.

Machine Learning via Cloud-based ML: 31 detections
Our cloud-based Machine Learning systems identified 31 security threats. Leveraging cloud-based ML can help in identifying threats across various environments.

These findings reflect the continuous monitoring and proactive approach we take to safeguard our customers' environments. It is crucial to further investigate and respond to the identified threats, ultimately enhancing the overall cybersecurity posture.

Common Types Attack Vectors

Risk Severity

Critical **High** **Medium**

Cryptanalysis

Cryptanalysis is the process of identifying and exploiting vulnerabilities in cryptographic algorithms to decipher ciphertext without the secret key. Attackers aim for total key discovery, finding equivalent algorithms, gaining new information about plaintext or ciphertext, and distinguishing encrypted output from random permutations.

Session Hijacking

This attack scenario involves a malicious actor exploiting flaws in an application's session management during the authentication process. The attacker can hijack or manipulate an ongoing session, thereby gaining unauthorized access to the application

Stored XSS

An attacker employs a variant of Cross-site Scripting (XSS) in which a malevolent script is enduringly stored as legitimate input in the data storage of a susceptible web application.

Cache Poisoning

An attacker leverages cache technologies to store specific data that serves their objectives. This type of attack involves placing incorrect or malicious content in a cache, whether it's an application's cache (like a web browser cache) or a public cache (e.g., DNS or ARP cache). Until the cache is refreshed, most applications or clients will treat the compromised cache data as valid, potentially leading to various exploits such as redirecting web browsers to malware-infected sites and producing incorrect calculations based on the erroneous value.

Malicious Software Update

An attacker employs deceptive techniques to induce a user or an automated process to download and install malicious code under the guise of a legitimate update, which appears to originate from a source controlled by the attacker.

Exploitation of Trusted Identifiers

An attacker guesses, acquires, or piggybacks on a trusted identifier (e.g., session ID, resource ID, cookie, etc.) to carry out authorized actions while impersonating an authenticated user or service.

Exponential Data Expansion

An attacker inputs data into a target application, using nested exponential data expansion to generate an unusually large output. Several data format languages permit the creation of macro-like structures to simplify complex structures, but this feature can be misused to place excessive strain on a processor's CPU and memory. Even a few nested expansions can lead to a significant increase in memory usage.

SaaS User Request Forgery

Through a previously installed malicious app, an attacker infiltrates a cloud-based application, exploiting the ongoing trust within an authenticated user's session. This attack occurs after a trusted user logs into a cloud service, deceiving the service into believing it's exclusively interacting with the trusted user. If successful, the actions embedded in the malicious app are executed by the targeted SaaS application at the trusted user's privilege level.

Artificially Inflate File Sizes

An attacker alters the contents of files by appending data to them, often for various purposes. This pattern can lead to a variety of different attacks and outcomes. In cases of devices with limited storage capacity, adding data to a file could potentially lead to a Denial of Service condition.

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

Quasar RAT Utilizes DLL Side Loading Technique

An open-source Trojan horse known as Quasar RAT secretly employs the DLL Side Loading technique to steal data from Windows-based computers. This attack occurs by mimicking trusted files. Quasar RAT has the capability to extract information from target systems and provide remote management. The identity of the attackers is unknown, but it is crucial to exercise caution against such attacks.

Flipper Zero Begins Disturbing Android and Windows Users with Bluetooth Alerts

The Flipper Zero software, known as 'Xtreme,' has introduced a feature that allows for Bluetooth spam attacks targeting Android and Windows devices. These attacks aim to disturb users by sending deceptive advertisement packets to devices. It is important for users to be vigilant and take measures to prevent such attacks.

North Korean Lazarus Group Targets Software Supplier Using Known Vulnerabilities

The Lazarus Group, associated with North Korea, appears to be responsible for a new campaign targeting a software supplier by exploiting known security vulnerabilities. The attacks involved malicious software such as SIGNBT and LPEClient. Lazarus Group used legitimate security software as an intermediary to encrypt web communications using digital certificates. These recent activities included a range of targeted victims until mid-2023. These developments are indicative of Lazarus Group's continuously evolving and expanding tactics and techniques, and the group is still considered an active and versatile threat actor.

Security Alert - PoC Attack Attempts for Citrix and VMware Vulnerabilities Released

VMware has identified a serious security vulnerability in Aria Operations for Logs. Citrix has announced an actively exploited security flaw, CVE-2023-4966, which can have severe consequences, including session hijacking. Three critical remote code execution vulnerabilities were discovered in SolarWinds Access Rights Manager. These developments underscore the need for organizations to keep their security up to date.

infinitum IT
Power of Integrated Security

MDR Insights

"October"

infinitumitlabs