infinitum IT
Power of integrated Security

# MDR Insights

## "August"


infinitumitlabs

# Content

# MDR REPORT

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

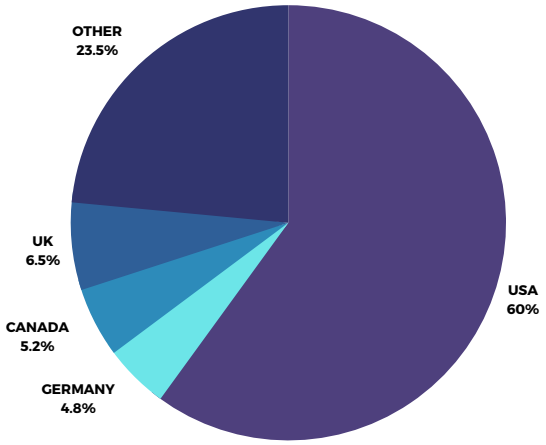
This MDR report provides an analysis of threats and security incidents detected in our company's information systems. The report covers topics such as summary and impact of incidents during the period under review, type and source of threats, status of security measures and recommendations.

# Ransomware Groups

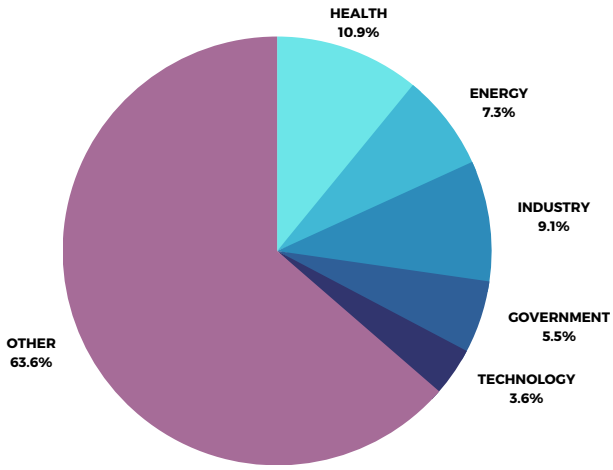
## 1. CL0P Ransomware Group

### Total Number of Attacks: 34

### Attack Graph by Country




### Attack Graph by Sectors



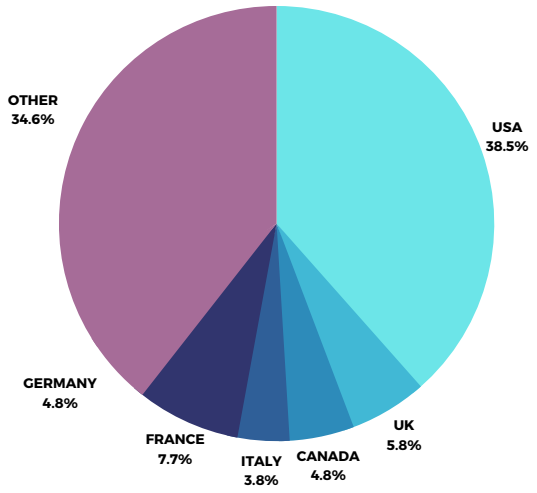

In the ever-evolving cyber-threat landscape, the Clop ransomware group has once again emerged as a harbinger of concerns. This transformation, appears to have Clop move away from traditional methods and promote torrents as a distribution channel for stolen data. Such a shift not only demonstrates their ability to adapt, but also has important ramifications for victims and cybersecurity officials alike. Moreover, Clop's recent actions highlight its expanding global reach, with a focus on targeting developed countries including the US, UK, FRANCE and CANADA. These attacks are not only financially motivated, but also have the potential to create widespread disruptions in key industries and affect economies and national security.

Known for their targeted extortion tactics, the Clop ransomware gang has chosen to leverage torrents as a tool to expose the data they stole in their MOVEit attacks. This change in strategy began on June 14, 2023, as the group gradually began blackmailing their victims. They took a step-by-step approach, incrementally adding victims' names to Tor-based data leak sites and ultimately making the stolen files public. In addition, the concentration of Clop's attacks on developed countries underscores their interest in countries with significant economic and political influence, and signals an increase in their operations globally.

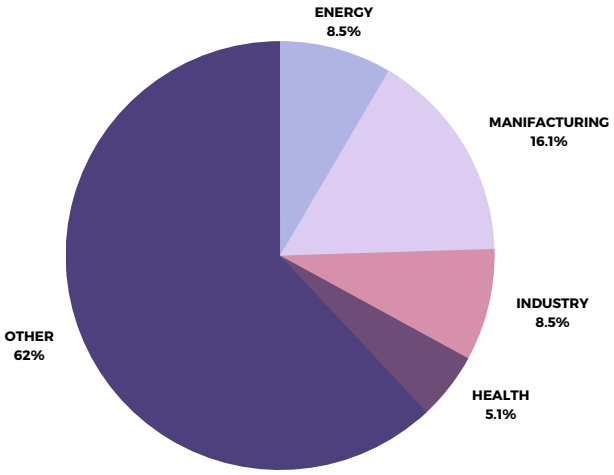
# 2. LockBit Ransomware Group

## Total Number of Attacks: 45

### 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 the healthcare sector is particularly alarming, as it highlights their willingness to exploit vulnerabilities that could have severe consequences for individuals and healthcare systems. Given the increasing frequency of cyberattacks in the healthcare sector, immediate actions are essential to protect sensitive patient information and ensure the uninterrupted delivery of critical medical services.

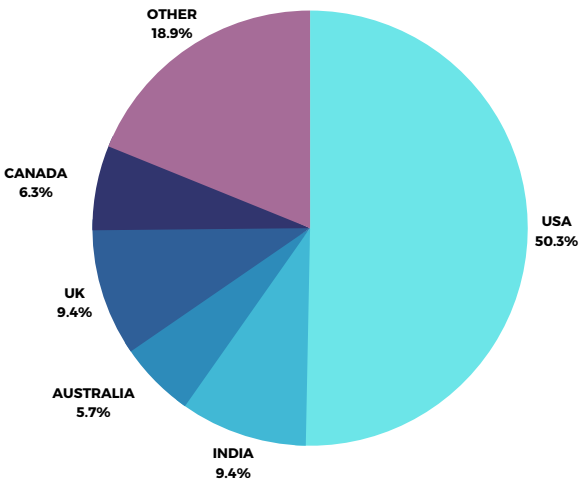
Furthermore, the group's diverse range of attacks on sectors such as energy, industry, government, technology, and construction underscores their broad scope, targeting key infrastructure, economic stability, and national security. The high number of attacks categorized as "OTHER" raises concerns about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

The concentration of LockBit attacks on countries like the USA, UK, France, and Canada highlights the group's interest in targeting developed nations with significant economic and political influence. These attacks not only result in financial losses but also disrupt crucial sectors, causing a ripple effect on the global stage. Additionally, LockBit's willingness to explore vulnerabilities in other countries 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.

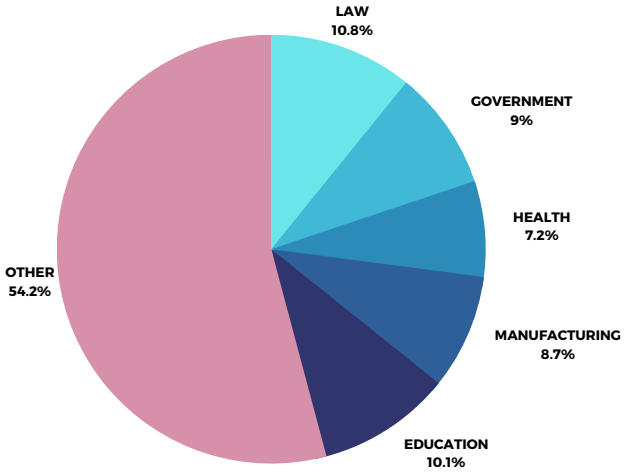
# 3. BianLian Ransomware Group

## Total Number of Attacks: 37

### Attack Graph by Country




### Attack Graph by Sectors




BianLian is a threat group known for its sophisticated and multi-stage attack methodology. They typically gain initial access to target systems through spearphishing emails containing malicious attachments or compromised website links. Once inside, they establish a persistent foothold by communicating with a command and control (C2) server and downloading additional tools to escalate privileges.

Their tactics include using compromised RDP credentials, custom Go-written backdoors, and remote management software for persistence and control. They also employ defense evasion techniques using PowerShell and Windows Command Shell to disable antivirus tools. Discovery is a key part of their strategy, involving various tools to learn about the victim's environment and gather information.

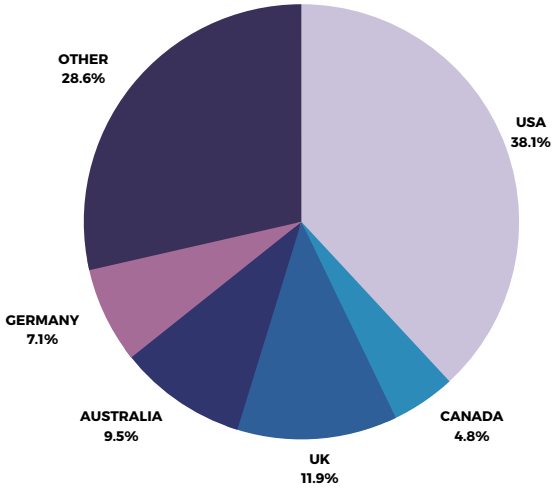
Credential access is crucial for lateral movement, which they achieve by finding unsecured credentials, harvesting from LSASS memory, and attempting to access Active Directory databases. Persistence and lateral movement are facilitated through tools like PsExec and RDP with valid accounts.

BianLian deploys ransomware to encrypt victim data and demands a ransom payment. They primarily target sectors with sensitive data and financial capacity, including financial institutions, government, professional services, manufacturing, media and entertainment, healthcare, education, and law. Geographically, their operations are global, with a higher concentration of attacks reported in North America and Europe, possibly indicating a focus on regions with high economic value.

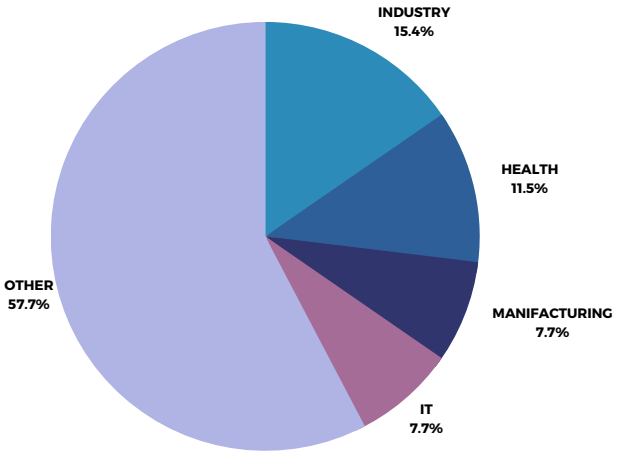
# 4. 8BASE Ransomware Group

## Total Number of Attacks: 35

### Attack Graph by Country




### Attack Graph by Sectors




The numerical graphical data on the 8BASE Ransomware Group sheds light on their targeting patterns and geographical reach, indicating a significant and concerning cyber threat. The sectoral attack data reveals that the group has a wide range of interests, with the construction, health, energy, and industry sectors all experiencing three to four attacks each. This suggests that 8BASE is indiscriminate in its choice of targets, aiming to disrupt critical infrastructure and services across various industries. The sizeable number of attacks labeled as "OTHER" further underscores the group's versatility, implying that they may be exploring unconventional targets or expanding their scope beyond traditional sectors.

When examining the country-by-country data, the USA emerges as the primary target, facing 14 attacks. The USA's prominence as a global economic and technological hub makes it an attractive target for cybercriminals seeking financial gain or aiming to create widespread chaos. Canada, the UK, and the UAE have also experienced attacks, with each country facing two to three incidents. The presence of countries like France, with one attack, highlights the group's willingness to cast a wide net in their activities. Additionally, the significant number of attacks categorized under "OTHER" countries suggests that 8BASE is actively pursuing victims in lesser-known regions, potentially exploiting weaker cybersecurity defenses in those areas.

# Top Trending CVEs of August 2023

## .NET Kestrel Resource Consumption Vulnerability

| CVE | CVSS Score | Severity | Type |
|---|---|---|---|
| CVE-2023-38180 | 9.8 | Critical | Uncontrolled Resource Consumption |

CVE-2023-38180 is a resource consumption vulnerability in .NET's Kestrel component. This vulnerability could allow an attacker to gain unauthorized access to the target system or cause a service disruption. This vulnerability exploits an error in .NET's Kestrel component. Kestrel is a web server used to host web applications. Kestrel can dynamically generate code in response to client requests. An attacker could send a specially crafted request that causes Kestrel to use excessive resources. This could slow down or even crash the target system. Additionally, an attacker could send a specially crafted request that causes Kestrel to execute unauthorized code. This could allow the attacker to gain access to the target system and steal sensitive data or damage the system.

## Mitigations

A patch is available for CVE-2023-38180. To apply this patch, you need to download and install the Windows updates from Microsoft's website. In addition to this:

- Run Kestrel behind a web server or WAF. This will prevent Kestrel from being directly exposed to the internet.
- Limit Kestrel's permissions. Ensure that Kestrel only has the necessary permissions.
- Increase Kestrel's request size limits. By limiting the size of the requests that Kestrel must process, you can reduce the impact of a DoS attack.

# Microsoft Exchange Server Remote Code Execution Vulnerability

| CVE | CVSS Score | Severity | Type |
|---|---|---|---|
| CVE-2023-35385 | 7.8 | High | Remote Code Execution |

CVE-2023-35385 is a remote code execution vulnerability in Microsoft Exchange Server. This vulnerability allows an attacker to execute arbitrary code on the target system by sending a specially crafted message. This vulnerability exploits a flaw in the way Microsoft Exchange Server handles SMTP (Simple Mail Transfer Protocol) messages. SMTP is a protocol used to send and receive email.

An attacker can exploit this vulnerability by sending a specially crafted message that contains malicious code. When the target system receives the message, it will execute the malicious code, which could give the attacker control of the system.
The malicious code could be used to steal sensitive data, install malware, or disrupt the operation of the system.

## Mitigations

A patch is available for CVE-2023-35385. To apply this patch, you need to download and install the Windows updates from Microsoft's website. Additionally:

- Update Microsoft Exchange Server to the latest version. This update will fix this vulnerability.
- Use Microsoft Exchange Server only with trusted users. Only allow trusted users to access Exchange Server.
- Use Microsoft Exchange Server only on a secure network. Only use Exchange Server over a secure network.
- Run Microsoft Exchange Server behind a firewall. This will help to prevent attackers from directly accessing Exchange Server.
- Run Microsoft Exchange Server over a VPN. This will make it even more difficult for attackers to access Exchange Server.

# Microsoft Teams Remote Code Execution and File Download Vulnerabilities

| CVE | CVSS Score | Severity | Type |
|---|---|---|---|
| CVE-2023-29330 | 8.9 | Critical | Remote Code Execution |
| CVE-2023-29328 | 8.9 | Critical | Remote Code Execution |

CVE-2023-29328 and CVE-2023-29330 are two security vulnerabilities in Microsoft Teams. These vulnerabilities allow attackers to join a Microsoft Teams meeting unauthorizedly and execute code in that meeting.

The attack can be carried out by an attacker sending a specially crafted Microsoft Teams invitation. When users receive this invitation and click on it, the code that the attacker executes is run on the target system.

## Mitigations

A patch is available for CVE-2023-29328 and CVE-2023-29330. To apply this patch, you need to download and install the Teams updates from Microsoft's website.

If the patch is not applicable, you can help protect Teams by taking the following measures:

- Update Microsoft Teams to the latest version. This update will fix this vulnerability.
- Use Microsoft Teams only with trusted users. Only allow trusted users to access Teams.
- Use Microsoft Teams only on a secure network. Only use Teams over a secure network.
- Run Microsoft Teams behind a firewall. This will help to prevent attackers from directly accessing Teams.
- Run Microsoft Teams over a VPN. This will make it even more difficult for attackers to access Teams.

# Juniper JunOS SRX / EX Remote Code Execution Vulnerability

| CVE | CVSS Score | Severity | Type |
|---|---|---|---|
| CVE-2023-36845 | 8.8 | High | Remote Code Execution |
| CVE-2023-36846 | 8.8 | High | Remote Code Execution |

CVE-2023-36845 is a PHP external variable modification vulnerability in J-Web, a web-based management interface for Juniper Networks Junos OS on EX Series and SRX Series devices. An unauthenticated, network-based attacker can exploit this vulnerability to modify certain PHP environment variables, which could lead to partial loss of integrity, allowing an attacker to chain to other vulnerabilities.

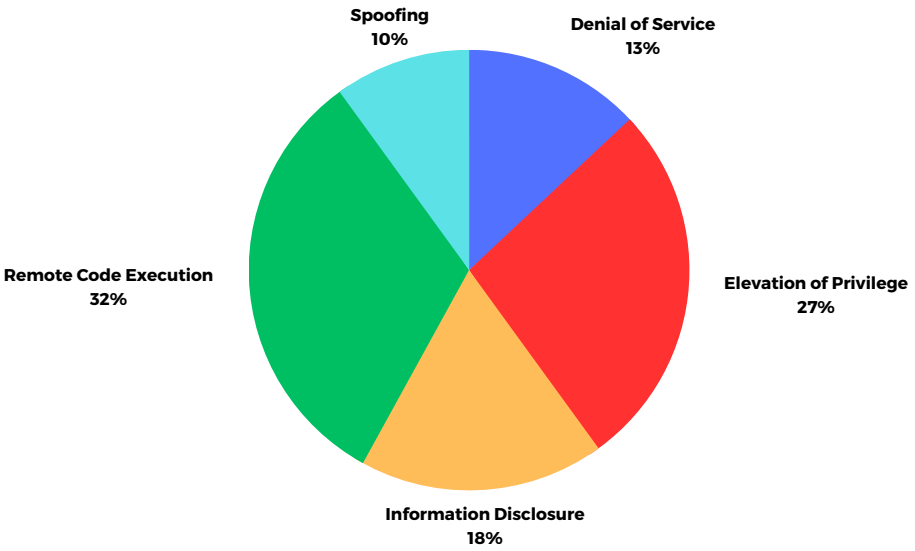
CVE-2023-36846 is a missing authentication for critical function vulnerability in J-Web. An unauthenticated, network-based attacker can exploit this vulnerability to upload arbitrary files to the file system, which could lead to a loss of integrity for a certain part of the file system.

## 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.

- Use J-Web only with trusted systems. Make sure you only have access to J-Web from systems that you trust and that you do not believe will attempt to exploit these vulnerabilities.
- Only users with the necessary permissions should be able to access J-Web. Make sure that users who have access to J-Web only have the necessary permissions. This will prevent attackers from gaining unauthorized access to the J-Web application.
- Keep J-Web up to date. Juniper Networks regularly releases security updates for Junos OS. Installing these updates will help to close vulnerabilities and protect your system.
- Run J-Web behind a firewall. This will help to prevent attackers from directly accessing the J-Web application.

# August 2023 Risk Analysis




Based on the numerical graphical data from our August risk analysis, we can extract valuable insights into the prevailing cyber threats that require our immediate attention. This data provides a comprehensive view of the various attack vectors and techniques that potential adversaries may employ during this specific period.
One particularly concerning development is the significant increase in Remote Code Execution (RCE) vulnerabilities when compared to the previous month. RCE attacks now account for 32% of the identified risks, marking a notable uptick. RCE poses a severe threat as it enables malicious actors to remotely execute code on vulnerable systems, potentially leading to unauthorized access, data breaches, or even the complete compromise of critical infrastructure. Therefore, organizations must remain vigilant in monitoring and promptly patching potential vulnerabilities that could be exploited for RCE attacks.

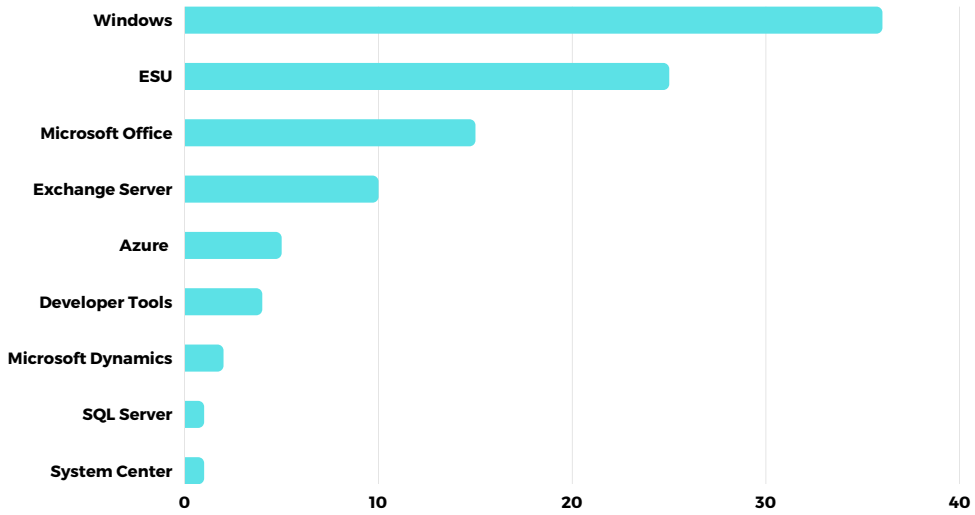
Elevation of Privilege (EoP) stands out as another substantial risk, representing 27% of the analyzed threats. EoP attacks involve adversaries attempting to escalate their privileges within a system, gaining access to resources and capabilities they should not have. To mitigate the impact of EoP attacks, organizations must rigorously implement robust access controls and adhere to the principle of least privilege.

On the other hand, Denial of Service (DoS) attacks, accounting for 13% of the identified risks, continue to be a prominent concern. DoS attacks aim to overwhelm a system, network, or application with an excessive amount of traffic, causing it to become unresponsive or unavailable to legitimate users. Effectively countering DoS attacks requires meticulous network capacity planning, traffic filtering, and the use of distributed denial-of-service (DDoS) protection mechanisms.

Information Disclosure, making up 18% of the identified risks, signifies the exposure of sensitive data to unauthorized parties. Whether due to unsecured configurations, weak authentication, or other vulnerabilities, such incidents can lead to severe consequences, including regulatory non-compliance, reputation damage, and financial losses. Organizations should prioritize data protection through encryption, access controls, and regular security assessments.

Spoofing attacks, accounting for 10% of the identified risks, involve malicious actors attempting to disguise their identity or forge data packets to deceive systems or users. Implementing robust authentication mechanisms, such as multi-factor authentication, can help mitigate the risks associated with Spoofing attacks.

# Patches by Product Family, August 2023




The data on the product families that received the most patches in August provides valuable insights into the focus of Microsoft's security updates during this period. Windows, as the flagship operating system, understandably received the highest number of patches, with a significant count of 36. This emphasizes the continuous effort to address potential vulnerabilities and ensure the security and stability of the operating system. While Windows takes the lead, it is interesting to note that some other product families also required attention.

Extended Security Updates (ESU), which provide additional support for older versions of Windows, accounted for 25 patches. This highlights the commitment to ensuring the security of legacy systems, recognizing that some organizations may still rely on older Windows versions.

Exchange Server, a critical email server product, received 10 patches. This reflects the attention given to securing this product, which is often targeted by attackers.

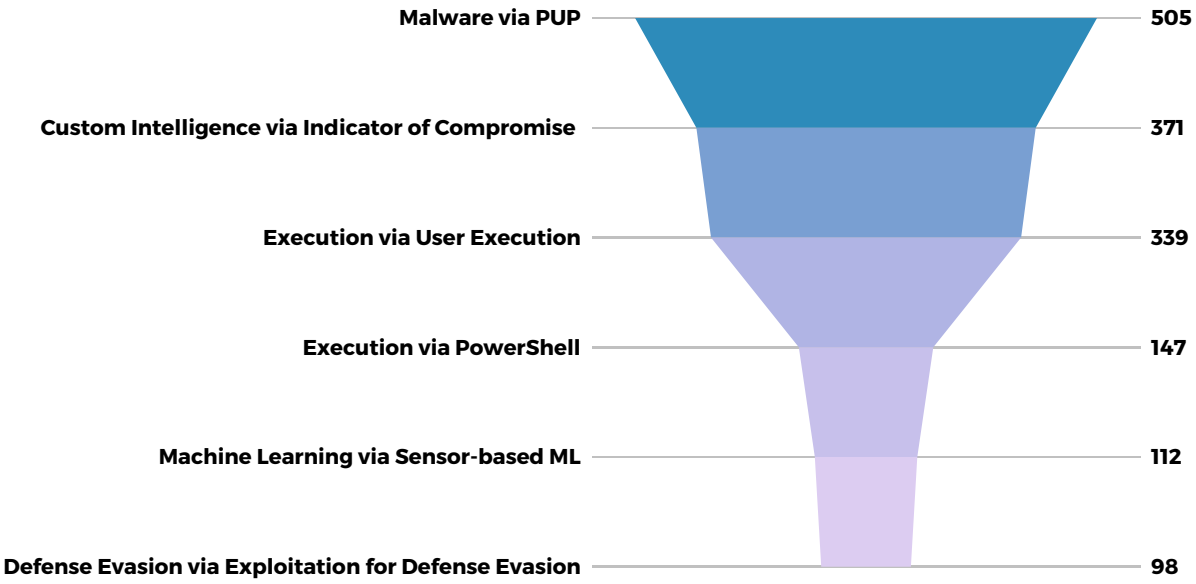
Azure, a rapidly growing cloud computing platform, received 5 patches. As cloud services become increasingly integral to modern business operations, ensuring the security of these platforms is paramount to maintain trust and protect sensitive data.

The other product families received a total of 9 patches. This includes Developer Tools, which are used to create and develop software, and Others, which includes a variety of other products such as Microsoft Dynamics, SQL Server 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.




Our monthly analysis of the data acquired from our customers' cybersecurity systems reveals several significant insights into the prevalent Tactics, Techniques, and Procedures (TTPs) used by cyber attackers.

Malware Detection via Potentially Unwanted Programs (PUP): During this reporting period, we discovered and mitigated 505 instances of potential malware threats through the identification of Potentially Unwanted Programs (PUPs). These PUPs could include software that users might unknowingly install, often carrying security risks.

Custom Intelligence Detection via Indicator of Compromise (IoC): Our monitoring efforts led us to detect 371 cases where we identified and addressed threats using custom intelligence. These threats were pinpointed based on specific indicators of compromise (IoCs), helping us respond proactively to potential security breaches.

Execution Detection via User Execution: We detected 339 instances where we caught suspicious activities related to code execution that initiated through user interactions. This highlights our ability to intercept and prevent unauthorized or malicious code executions driven by user actions.

Execution Detection via PowerShell: Our vigilant monitoring spotted 147 instances where attackers attempted to execute actions using PowerShell, a scripting language with significant capabilities. Detecting these instances is critical, as adversaries often exploit PowerShell for their malicious activities.

Machine Learning Detection via Sensor-based ML: Leveraging sensor-based machine learning techniques, we identified 112 instances of possible threats. This underscores our success in applying machine learning algorithms to learn from the environment and identify abnormal patterns indicating potential cyber threats.

Defense Evasion via Exploitation for Defense Evasion: Our systems alerted us about 98 instances involving attempted exploitation aimed at evading our defense mechanisms. Adversaries frequently resort to exploiting vulnerabilities to bypass security measures. Detecting such attempts is vital for preventing possible breaches.

This analysis highlights the critical need for a multi-layered and proactive cybersecurity approach. Identifying and addressing the most prevalent TTPs will allow us to strengthen our customers' defense against evolving threats effectively. By continually monitoring and analyzing emerging trends, we can stay ahead of cybercriminals and safeguard our customers' digital assets and sensitive information. Collaboration with our customers and sharing these insights with the broader cybersecurity community will further contribute to collective resilience against cyber threats.

# Common Types Attack Vectors

## Risk Severity

**Critical** **High** **Medium**

### Path Traversal

An adversary exploits inadequate input validation of a target using path manipulation techniques to gain unauthorized access to data. A common form of this attack involves inputting a path to a desired file along with dot-dot-slash characters. This causes the file access API or function to navigate beyond the intended directory structure and into the root file system. By altering the provided path information, the attacker manipulates the access function or API to retrieve the desired file. Such attacks may either entail the attacker furnishing a complete path to the targeted file or utilizing control characters (e.g. path separators (/ or ) and/or dots (.)) to access specific directories or files.

### File Content Injection

A threat actor contaminates files by incorporating a harmful payload (directed at the file systems reachable by the targeted software). These files could potentially traverse regular pathways like email attachments, as well as common web-based materials such as PDFs and multimedia files. The threat actor capitalizes on established weaknesses or processing procedures within the targeted processes. This is aimed at exploiting the host's reliance on executing external content, even encompassing executable binary files.

### XQuery Injection

This exploit leverages XQuery for probing and assaulting server systems, analogous to how SQL Injection enables attackers to manipulate SQL calls to relational databases. XQuery Injection capitalizes on inadequately validated data, which is supplied to XQuery commands to navigate and execute actions within the scope of XQuery routines. XQuery injection serves to list elements within the target environment, infuse commands into the local host, or initiate queries to distant files and data sources.

### URL Encoding

This exploit focuses on URL encoding. A threat actor can exploit the various methods of URL encoding to manipulate the interpretation of the URL.

### OS Command

In this form of attack, an attacker inserts operating system commands into pre-existing application functions. Applications that construct command strings using untrusted input are at risk. Exploiting OS command injection within an application, adversaries can escalate privileges, execute unrestricted commands, and potentially breach the underlying operating system.

### WSDL Scanning

This attack aims at the WSDL interface of a web service. Attackers scan the WSDL to uncover details about how the service works and potential weaknesses. This helps them plan more serious attacks like injecting harmful content or commands. WSDL files provide info about service ports and bindings. Attackers can exploit this by sending malicious data to the service, causing disruptions or unauthorized access. They might also try to guess private methods using the WSDL details.

### Privilege Abuse

A threat actor can capitalize on aspects of the target that are meant for privileged users or administrators, but are accessible by lower-privileged accounts. Proper control of access to sensitive information and functions is crucial to restrict access to only authorized users.

### Flash Parameter

A threat actor exploits inadequate data validation to insert harmful global parameters into a Flash file that's incorporated into an HTML document. Flash files can use data from users to set up the Flash content and interact with the hosting HTML document.

### Fuzzing

In this attack method, the adversary employs fuzzing to pinpoint vulnerabilities within the system. Fuzzing is a technique for testing software security and functionality, involving the input of randomly generated data to trigger system failures. Fuzzing treats the system as a black box, devoid of prior assumptions, and aims to expose implicit assumptions regarding user input. It allows attackers to quickly identify such assumptions even without intricate knowledge of the system's internals. These exposed assumptions can then be exploited by manipulating user input to achieve the attacker's objectives.

# 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

## Raccoon Stealer Malware Makes a Comeback with New Version

Raccoon Stealer, which has been in existence since 2019, is a type of malicious software sold through a monthly subscription of $200 USD. This software, used with the intention of stealing information, has gained popularity among hackers. Developers announced the latest version, 2.3.0, by posting a notice on hackers' forums. This software is capable of stealing data from over 60 applications, including login credentials, credit card information, browsing history, personal identification data, and even cryptocurrency wallets. However, due to the arrest of its lead author Mark Sokolovsky in the Netherlands in 2022 and the dismantling of its infrastructure by the FBI, the software went through a period of uncertainty.

## New Remote Access Trojan (RAT) via Telegram and Discord: QwixxRAT

A new remote access trojan (RAT) named QwixxRAT is being sold by threat actors through Telegram and Discord platforms. It is priced at 150 rubles for weekly access and 500 rubles for a lifetime license. The malware targets Windows machines and secretly collects sensitive data, sending it to the attacker's Telegram bot for unauthorized access. QwixxRAT captures web browser history, bookmarks, cookies, credit card info, keystrokes, screenshots, files with specific extensions, and data from applications like Steam and Telegram. The RAT employs anti-analysis techniques to evade detection, including sleep functions for delays during execution and checks to determine if it's in a virtual environment. It also terminates if it detects tools like taskmgr, processhacker, netstat, netmon, tcpview, and wireshark, used for monitoring.

## The Threat Actors Target Microsoft SQL Servers to Distribute FreeWorld Ransomware

Threat actors target insecure Microsoft SQL (MS SQL) servers and carry out attacks using a ransomware type called FreeWorld. Researchers have determined that these attacks are conducted using various tools and methods. The attacks begin by brute-forcing the MS SQL server, then proceed to scan the database, execute shell commands, and conduct reconnaissance using the xp_cmdshell configuration option. Additionally, at the end of the attack, the preferred ransomware payload appears to be a new variant of the Mimic ransomware called 'FreeWorld.'

infinitum IT
Power of integrated Security

# MDR Insights

## "August"


infinitumitlabs