infinitum IT
Power of integrated Security

MDR Insights

"June"

infinitumitlabs

Content

MDR REPORT

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

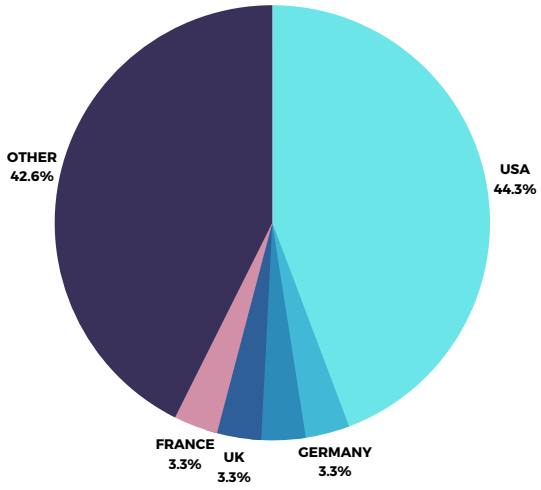
This MDR report provides an analysis of threats and security incidents detected in our company's information systems. The report covers topics such as summary and impact of incidents during the period under review, type and source of threats, status of security measures and recommendations.

Ransomware Groups

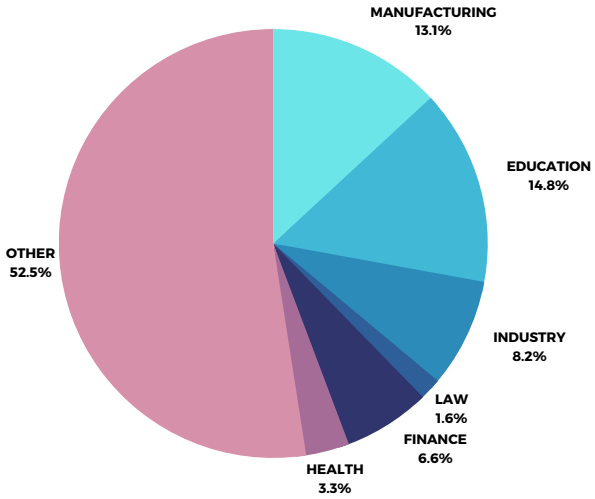
1. LockBit Ransomware Group

Total Number of Attacks: 61

Attack Graph by Country



Attack Graph by Sectors



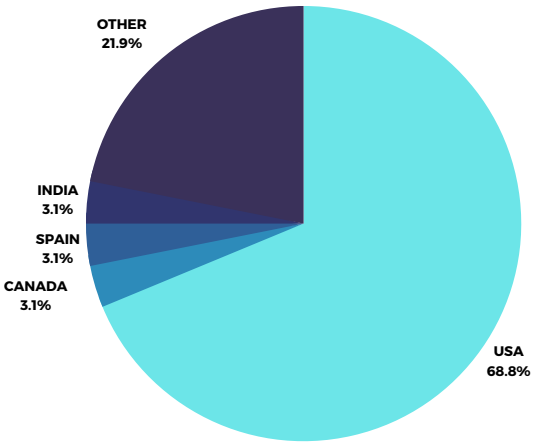
According to the country graph showing the latest wave of cyber attacks, LockBit Ransomware Group has carried out a total of 61 attacks this month. The vast majority of this malicious activity took place in the United States, with 27 attacks occurring. While the US bore the brunt of this attack, several other countries also found themselves targeted, albeit in smaller numbers. Germany, Canada, the United Kingdom and France each suffered two attacks each, emphasising the global reach of LockBit's activities. The fact that a significant number of the attacks, totalling 26, were scattered across various other countries underlines the far-reaching impact and indiscriminate nature of the group's activities. These figures are a stark reminder of the persistent threat posed by ransomware groups and the importance of implementing robust cybersecurity measures on a global scale.

When the data is analysed according to the sector graph of the 61 attacks carried out by the LockBit group in June, it is seen that the Education sector bears the heaviest burden of these malicious activities with 9 incidents. Manufacturing companies were also heavily targeted with 8 attacks, followed by the Industrial sector with 5 breaches. The finance sector also found itself on the target board as the victim of 4 separate attacks. The Healthcare sector faced 2 incidents, albeit a small number, while the Legal sector was subjected to a single attack. Remarkably, a significant number of the 32 attacks were directed at various other sectors, underlining the widespread impact and indiscriminate nature of LockBit Ransomware Group's activities. These figures are a striking reminder of the urgent need for increased cybersecurity measures across multiple sectors to effectively counter such threats.

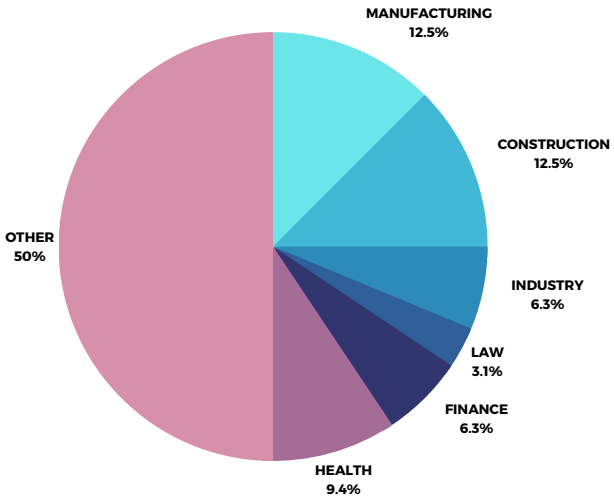
2. ALPHV Ransomware Group

Total Number of Attacks: 32

Attack Graph by Country



Attack Graph by Sectors



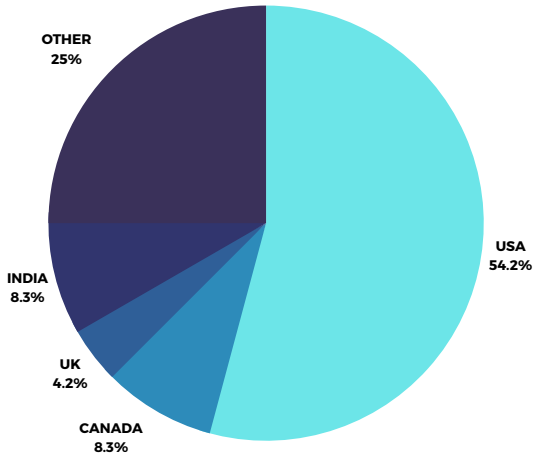
When the attacks belonging to Ransomware Groups for the month of June are analysed, it reveals that the ALPHV Ransomware Group carried out a total of 32 attacks during this month. The United States emerges as the primary target, accounting for a significant majority with 22 reported incidents. While the US faced the brunt of ALPHV's attack, several other countries were also affected, albeit to a lesser degree. Canada, Spain and India each suffered a single attack, emphasising the global reach of the group's operations. In addition, seven attacks were scattered across several other countries, emphasising the widespread nature of ALPHV's activities. These findings underscore the urgent need for robust cybersecurity measures not only in the United States but also in other targeted countries, as cyber threats continue to pose significant challenges on a global scale.

When the sectoral data of the 32 attacks carried out by the ALPHV Ransomware Group in June is analysed, it is revealed that the Manufacturing and Construction sectors, which were subjected to 4 attacks each, bear the heaviest burden of these malicious activities. The Healthcare sector also took a significant hit with 3 breaches. In addition, the Finance and Industry sectors suffered 2 attacks each, while the Legal sector suffered a single breach. Notably, another significant portion of the attacks, comprising 16 attacks, targeted various other sectors, underlining the indiscriminate nature of ALPHV's activities. This data highlights the urgent need for increased cybersecurity measures across many sectors, as organisations need to be vigilant to protect their critical infrastructure and sensitive data against evolving cyber threats.

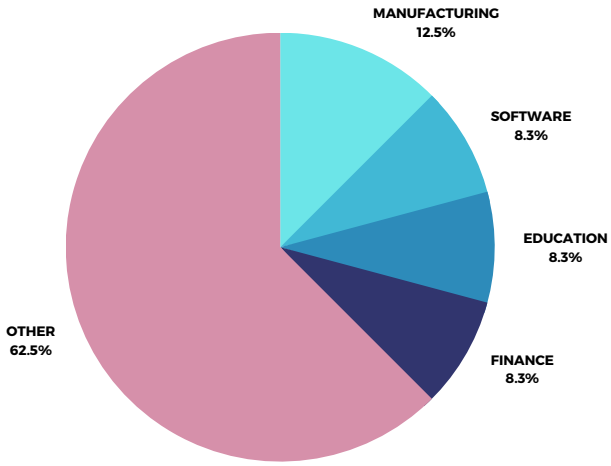
3. AKIRA Ransomware Group

Total Number of Attacks: 24

Attack Graph by Country



Attack Graph by Sectors



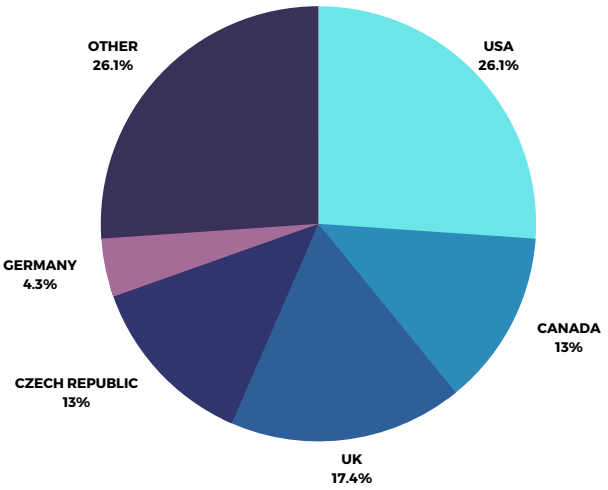
Analysing attacks by Ransomware Groups in June, the Akira Ransomware Group was responsible for a total of 24 attacks during the month. The United States stands out as the primary target, accounting for more than half of the incidents with 13 detected attacks. Canada and India also suffered the effects of Akira's operations with 2 attacks each. The United Kingdom also experienced a single attack. The 6 attacks scattered across various other countries underline the global reach of the Akira Ransomware Group. These findings underline the need for robust cybersecurity measures worldwide, as organisations in multiple countries must remain vigilant and take proactive steps to protect their critical systems and valuable data from such malicious activity.

In June, Akira Ransomware Group organised a total of 24 cyber-attacks, as shown in the sector graph. Analysis of the data reveals that the Manufacturing sector was the most targeted sector with 3 reported incidents. The Software and Education sectors also fell victim to attacks, with 2 attacks each. The Financial sector also suffered 2 breaches. The fact that the majority of attacks, totalling 15 incidents, targeted various other sectors emphasises the indiscriminate nature of Akira's activities. These findings underline the urgent need for robust cybersecurity measures across many sectors, as organisations must remain vigilant and implement effective defence strategies to mitigate the risks posed by ransomware attacks. Protecting critical infrastructure and sensitive information is essential to guard against the growing threats in the digital environment.

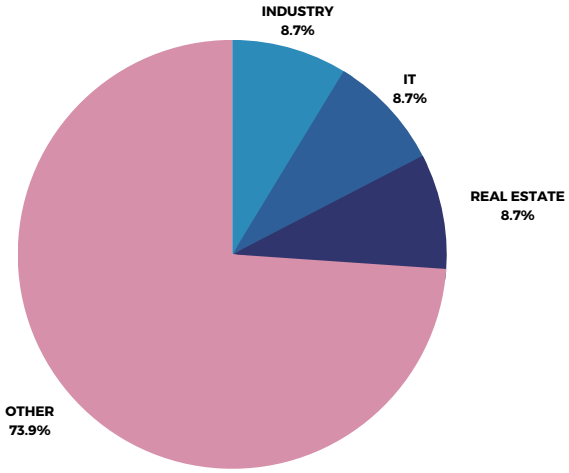
4. PLAY Ransomware Group

Total Number of Attacks: 23

Attack Graph by Country



Attack Graph by Sectors



Based on the country graph depicting the cyberattacks carried out in June, the Play Ransomware Group executed a total of 23 attacks during this period. The United States experienced the highest number of attacks, with 6 incidents reported. The United Kingdom and the Czech Republic were also targeted, facing 4 and 3 attacks, respectively. Canada was not spared, encountering 3 breaches as well. Additionally, a solitary attack occurred in Germany. Moreover, 6 attacks were dispersed across various other countries. This data highlights the global impact of the Play Ransomware Group's activities, underscoring the widespread nature of their operations. These findings emphasize the critical need for organizations worldwide to bolster their cybersecurity measures, as the threat of ransomware attacks continues to pose a significant risk to digital infrastructure and data security. Implementing robust defense mechanisms and maintaining heightened vigilance are imperative in combating such cyber threats effectively.

During the month of June, the Play Ransomware Group executed a total of 23 cyberattacks, as indicated by the sectoral graph. Examining the data, it is evident that no specific sector faced a substantial number of attacks. The Industry, IT, and Real Estate sectors all encountered 2 attacks each, reflecting a distributed impact across various industries. The majority of the attacks, comprising 17 instances, were dispersed among other sectors, underscoring the indiscriminate nature of Play Ransomware Group's operations. These findings emphasize the critical importance of maintaining robust cybersecurity measures across all sectors, as cyber threats continue to pose significant risks to organizations' digital infrastructure and data security. Organizations must remain proactive in implementing comprehensive defense strategies to mitigate the risks associated with ransomware attacks. By prioritizing cybersecurity and fostering a culture of cyber resilience, businesses can enhance their resilience against such threats.

Top Trending CVEs of June 2023

Microsoft SharePoint Server Elevation of Privilege Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-29357	9.8	Critical	Elevation of Privilege

Microsoft Office is receiving an essential update to address a critical vulnerability known as CVE-2023-29357, which has a severity rating of 9.8 according to the CVSS scale. SharePoint, a robust collaboration platform, empowers organizations to seamlessly share, manage, and collaborate on content, knowledge, and applications. The Microsoft Security Response Center (MSRC) has identified a potential security risk where an attacker could exploit spoofed JSON Web Tokens (JWT) to launch a network-based attack that circumvents authentication measures, potentially granting them unauthorized access to administrator privileges.

Mitigations

- Customers who have enabled the AMSI integration feature and use Microsoft Defender across their SharePoint Server farm(s) are protected from this vulnerability.

Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-29363	9.8	Critical	Remote Code Execution
CVE-2023-32014	9.8	Critical	Remote Code Execution
CVE-2023-32015	9.8	Critical	Remote Code Execution

CVE-2023-29363, CVE-2023-32014, and CVE-2023-32015 are critical Remote Code Execution (RCE) vulnerabilities discovered in Windows operating systems, each assigned a CVSSv3 score of 9.8. These vulnerabilities are specifically associated with the implementation of Pragmatic General Multicast (PGM), an experimental multicast protocol, within the Windows Message Queuing Service component. Exploitation of these vulnerabilities can occur when a remote, unauthenticated attacker sends a malicious file to a vulnerable target. Microsoft's recommended mitigation guidance highlights that systems with enabled Message Queuing Services are susceptible to these vulnerabilities.

Mitigations

- The Windows message queuing service, which is a Windows component, needs to be enabled for a system to be exploitable by this vulnerability. This feature can be added via the Control Panel.

You can check to see if there is a service running named Message Queuing and TCP port 1801 is listening on the machine.

.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-24897	7.8	Critical	Remote Code Execution

An issue has been identified in .NET, .NET Framework, and Visual Studio, which represents a security vulnerability. Exploiting this flaw necessitates the attacker's ability to persuade the victim into opening a specifically crafted malicious file, typically obtained from a website.

Although Microsoft is unaware of any instances of public disclosure or active exploitation, and deems the likelihood of exploitation to be low, the extensive list of patches—dating back to .NET Framework 3.5 on Windows 10 1607—indicates that this vulnerability has persisted for several years. Interestingly, Microsoft does not specify the file type associated with this vulnerability. However, the presence of the Arbitrary Code Execution (ACE) descriptor suggests that the attacker's location is denoted as "remote," as opposed to the nature of the attack itself, as it necessitates local user interaction.

Mitigations

- Microsoft has not identified any mitigating factors for this vulnerability.

Windows Hyper-V Denial of Service Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-32013	6.5	Critical	Denial of Service

CVE-2023-32013 is a highly significant security vulnerability that impacts Windows Hyper-V, a virtualization platform developed by Microsoft. This vulnerability has been categorized as 'Critical' with a CVSS score of 6.5. Hyper-V plays a vital role in enabling administrators to efficiently manage multiple operating systems on a single physical server.

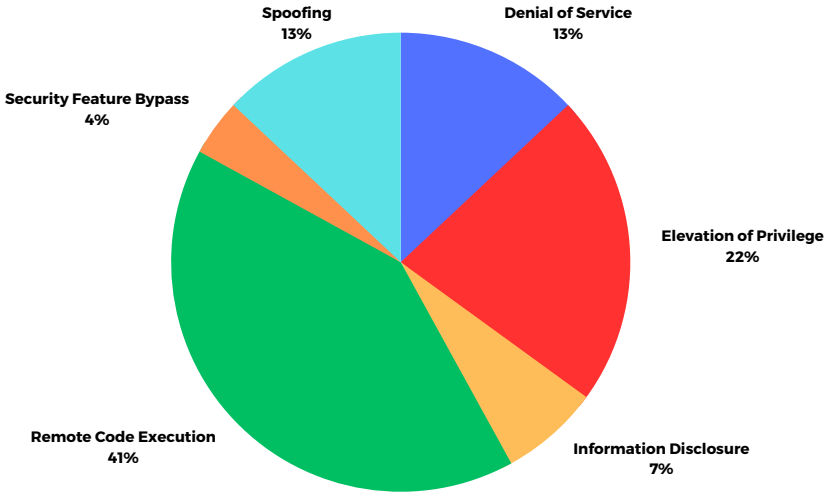
Microsoft has provided insights into the nature of this vulnerability, stating that successful exploitation necessitates the attacker to meticulously prepare the target environment in order to enhance the reliability of the exploit. While the CVSS score may appear relatively lower, the 'Critical' rating is attributed to the exceptional importance of Hyper-V within virtualization infrastructures, as well as the potential ease of network-based access for attackers.

It is crucial to address and mitigate this vulnerability promptly, considering the central role Hyper-V serves in the seamless operation of virtualized environments. By taking appropriate measures to secure systems running Hyper-V, organizations can safeguard against potential exploits and uphold the integrity of their virtualization infrastructure.

Mitigations

- Microsoft has not identified any mitigating factors for this vulnerability.

June 2023 Risk Analysis



The June risk analysis report presents a valuable resource for evaluating the potential security risks faced by an organization or system. The accompanying graph, displaying numerical percentages, offers a comprehensive overview of various security threats. Analyzing the data, we observe that Remote Code Execution emerged as the most prominent threat, constituting a significant 41% of the risks identified. This alarming figure underscores the critical importance of protecting against unauthorized execution of code, which can potentially lead to system compromise and data breaches. It serves as a stark reminder of the need for robust security measures to prevent malicious actors from exploiting vulnerabilities and gaining unauthorized access to sensitive information.

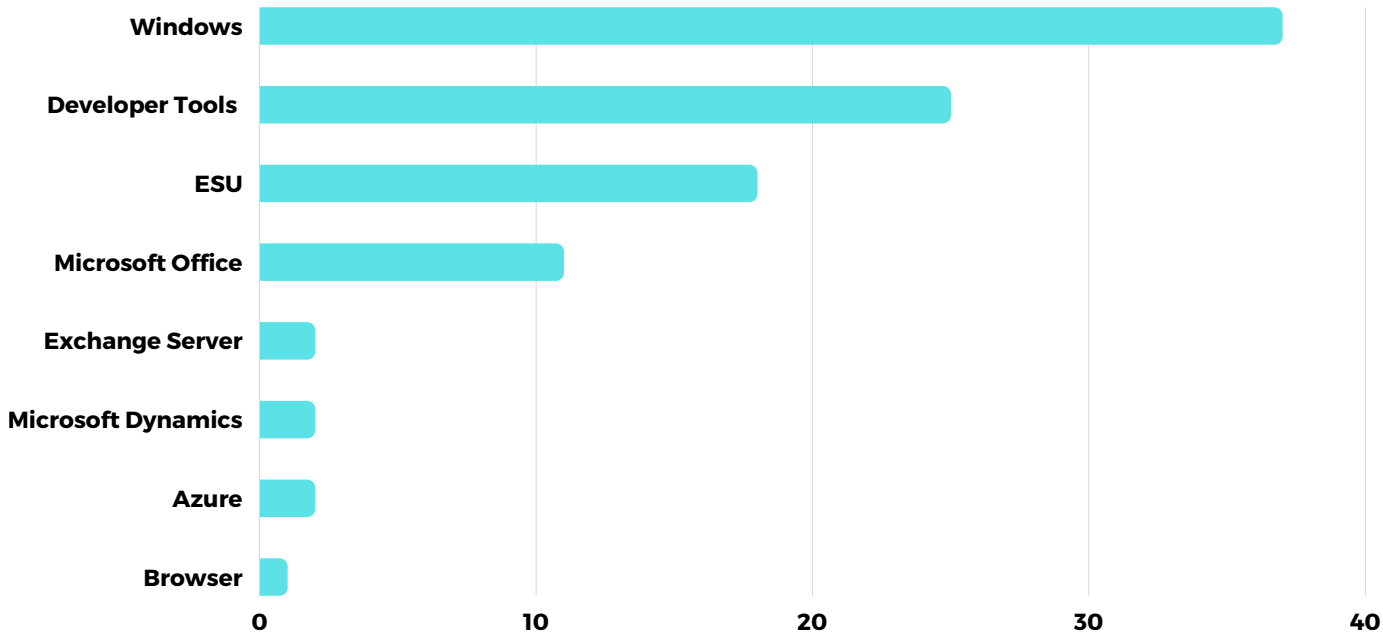
Elevation of Privilege accounted for 22% of the identified security threats. This threat category highlights the risk of unauthorized escalation of user privileges, which can result in unauthorized access to sensitive data or system resources. It emphasizes the need for effective access controls, authentication mechanisms, and regular security updates to prevent potential privilege misuse. Organizations must prioritize stringent access management protocols and continuously monitor user privileges to mitigate the risks associated with this threat.

Denial of Service and Spoofing each accounted for 13% of the identified security threats. Denial of Service attacks can disrupt or render a system unavailable by overwhelming it with a flood of requests, impacting the availability and functionality of critical services. Spoofing, on the other hand, involves masquerading as a trusted entity to deceive users or systems. Both threats underline the significance of implementing robust network defenses, traffic monitoring, and authentication mechanisms to thwart potential attacks and protect the integrity of systems and data.

Information Disclosure and Security Feature Bypass, constituting 7% and 4% respectively, highlight the importance of safeguarding sensitive information and ensuring the proper functioning of security features. Organizations must prioritize the implementation of data encryption, secure communication protocols, and comprehensive security testing to minimize the risks associated with these threats.

By leveraging the insights provided by the June risk analysis, organizations can better understand the prevalent security threats and prioritize the allocation of resources and implementation of security controls accordingly. This comprehensive approach will enable them to mitigate potential risks, protect their assets, and maintain the integrity and availability of critical systems and data.

Patches by Product Family, June 2023

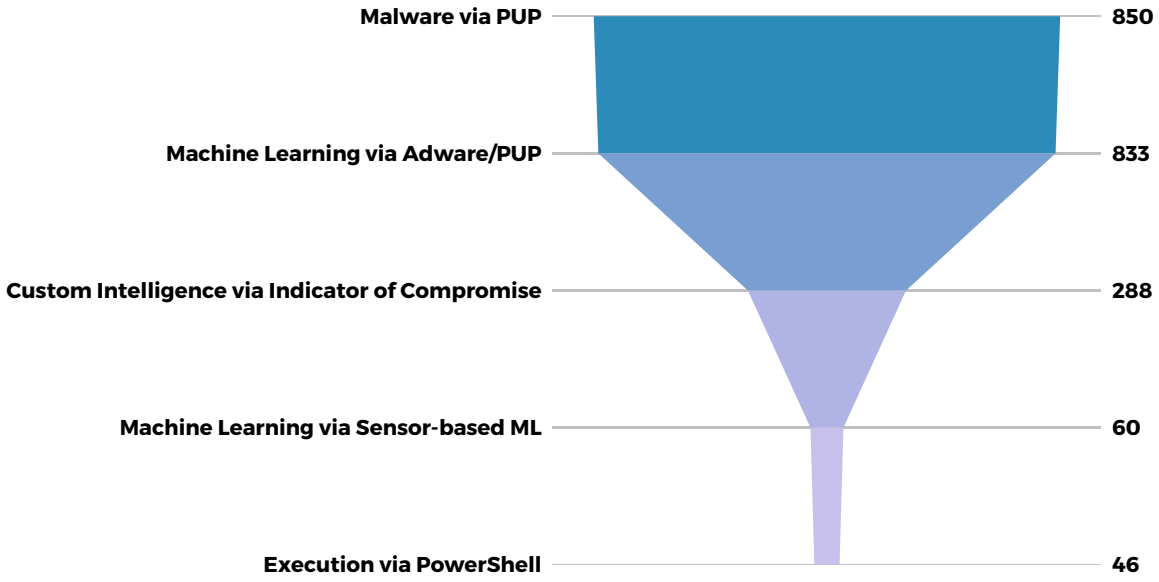


The data from the June risk analysis report provides valuable insights into the rates of patches applied to address various security threats. The analysis reveals that a significant focus was placed on patching vulnerabilities in Windows, highlighting its importance in maintaining system security. Developer Tools also received considerable attention, reflecting the significance of securing the software development environment. Moreover, efforts were made to address security vulnerabilities in Extended Security Updates (ESU) for legacy or unsupported Windows systems. Additionally, patches were dedicated to addressing vulnerabilities in Microsoft Office, Exchange Server, Microsoft Dynamics, Azure, and web browsers. These patching efforts demonstrate the commitment to mitigating potential risks and ensuring the security and integrity of critical systems and applications.

The June risk analysis report provides valuable insights into the rates of patches applied to address various security threats. The data reveals that a significant focus was placed on patching vulnerabilities in Windows, with 37 patches dedicated to ensuring the security and integrity of this widely used operating system. Developer Tools received 25 patches, highlighting the importance of securing the software development environment. Extended Security Updates (ESU) accounted for 18 patches, emphasizing the commitment to protect legacy or unsupported Windows systems. Microsoft Office and Exchange Server both received 11 and 2 patches respectively, underscoring the efforts to address vulnerabilities in these critical software applications. Additionally, Microsoft Dynamics, Azure, and web browsers were not overlooked, with 2, 2, and 1 patches respectively allocated to these platforms. These patching efforts demonstrate a comprehensive approach to mitigating security risks and safeguarding organizations' systems and data.

The Most Common TTPs

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



The graph presents an analysis of the most prevalent TTPs identified within our clients' networks, as derived from the monthly MDR report. Leading the list is malware, which was detected 850 times. Malware encompasses a wide range of malicious software designed to infiltrate systems, compromise security, and facilitate unauthorized activities. Following closely is the category of Potentially Unwanted Programs (PUPs), identified 833 times, often associated with Adware. PUPs are software programs that possess legitimate functionality but are frequently unwanted due to their intrusive behavior or potential security risks.

Machine Learning emerges as another prominent TTP, observed 833 times in connection with Adware/PUP. This indicates the growing adoption of machine learning techniques within the cybersecurity domain, specifically for the purpose of detecting and mitigating threats associated with Adware/PUP.

Custom Intelligence, observed 288 times, plays a critical role in identifying potential security threats. This TTP involves leveraging custom intelligence sources and indicators of compromise (IoCs) to enhance the accuracy and effectiveness of threat detection capabilities.

Additionally, Sensor-based Machine Learning was recorded 60 times, emphasizing the use of sensor data and machine learning algorithms to enhance threat detection and response capabilities. By incorporating sensor-based machine learning, organizations can derive deeper insights from data and identify patterns indicative of security incidents.

Finally, the Execution of PowerShell was identified 46 times, highlighting the utilization of PowerShell, a powerful scripting language and framework primarily used in Windows environments. This TTP signifies the execution of commands or scripts through PowerShell, which can be leveraged for both legitimate and malicious purposes.

The analysis of these prevalent TTPs provides valuable insights into the current threat landscape, enabling organizations to develop proactive cybersecurity strategies and bolster their defenses against emerging threats.

Common Types Attack Vectors

Risk Severity

Critical **High** **Medium**

Buffer Manipulation

An attacker manipulates the interaction between an application and a buffer in an effort to access or modify data they should not have permission to access. Buffer attacks are distinguished by the fact that the buffer space itself is the target of the attack, rather than any code responsible for interpreting the buffer's content.

Overflow Buffers

Buffer overflow attacks aim to exploit inadequate or absent bounds checking in buffer operations, usually triggered by input injected by an adversary. As a result, the adversary gains the ability to write beyond the boundaries of allocated buffer areas in memory, leading to a program crash or potentially allowing the redirection of execution according to the adversary's intention.

Exploiting Trust in Client

Data integrity and client/server communication channel authentication issues are used in this type of attack. It exploits the server's tacit assumption that the client is who they claim to be, and that is more important. The server, which believes it is only speaking to a trustworthy client, is the target of this type of assault when the attacker speaks directly to it. This kind of assault might take many different shapes.

Password Spraying

In a Password Spraying attack, an adversary tries a short list (for example, 3-5) of typical or expected passwords against a known list of user accounts in an attempt to obtain valid credentials. Before moving on to the next password on the list, the adversary tries a specific password for each user account. This strategy helps the adversary escape detection by preventing sudden or frequent account lockouts.

Code Injection

To insert new code into the target's running code, an adversary takes advantage of a flaw in input validation. The difference between this and code inclusion is that the former entails the addition or replacement of a reference to a code file, which is then imported by the target and used as part of the code of some program.

SQL Injection

This attack takes advantage of target software that builds SQL statements from user input. When the target software creates SQL statements based on the input, the attacker designs the input strings so that the resulting SQL statement executes operations that are not what the application intended. The failure of the program to properly validate input leads to SQL Injection.

Excavation

In an effort to get information that could be used for bad intentions, an adversary actively probes the target.

Directory Indexing

A target responds to a request from an adversary by listing or indexing the contents of a directory as output. Since many programs are set up to offer a list of the directory's contents when such a request is received, one typical technique for triggering directory contents as output is to construct a request having a path that terminates in a directory name rather than a file name. An adversary can use this to explore the directory tree on a target as well as learn the names of files.

XML Routing Detour Attacks

An attacker takes control of an intermediary system that processes XML material and forces it to change and/or reroute how the content is processed. Attacks that use XML Routing Detours are of the Adversary in the Middle variety. In order to process the XML message, the attacker compromises or inserts a middle system.

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

Meduza Stealer: The Possible Resurgence of the Infamous Aurora Stealer

A new malware variant called "Meduza Stealer" has emerged, potentially marking the return of the notorious Aurora Stealer. While details from the article are not included, it suggests that Meduza Stealer could be a successor or evolution of the previously identified Aurora Stealer malware. The exact features, capabilities, and potential impact of Meduza Stealer are not discussed. Users should remain vigilant and ensure their systems are protected with up-to-date security measures to mitigate the risk of such malware threats.

RedEnergy Stealer: A Potential Ransomware Threat on the Horizon

A new ransomware threat called "RedEnergy Stealer" has been identified, indicating a potential evolution of the RedEnergy malware. The specifics of this threat are not mentioned in the abstract. RedEnergy Stealer may possess ransomware capabilities, but further details about its functionality, attack vectors, and impact are not provided. It is crucial for users to prioritize robust security measures, including regularly updating their systems and employing reliable backup solutions, to defend against emerging ransomware threats like RedEnergy Stealer.

New EarlyRat Malware Associated with North Korean Andariel Hacking Group

A new malware named "EarlyRat" has been identified, potentially linked to a North Korean hacking group known as Andariel. EarlyRat is a backdoor malware that infiltrates computers to perform espionage activities, including stealing data and remote control. It is believed to have been used by Andariel starting in 2021. The malware spreads through email attachments and spam campaigns.

Microsoft Investigates Outlook.com Bug Affecting Email Search Functionality

An Outlook.com bug is currently under investigation by Microsoft due to its impact on email search functionality. The bug is causing issues with the search feature within Outlook.com, making it difficult for users to locate specific emails or search for relevant content. Microsoft is actively looking into the matter to identify the cause of the problem and develop a solution to restore full email search functionality. Users of Outlook.com are advised to stay updated on any official announcements or updates from Microsoft regarding this issue.

infinitum IT
Power of integrated Security

MDR Insights

"June"

infinitumitlabs