infinitum IT
Power of integrated Security

MDR Insights

"July"

infinitumitlabs

Content

MDR REPORT

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

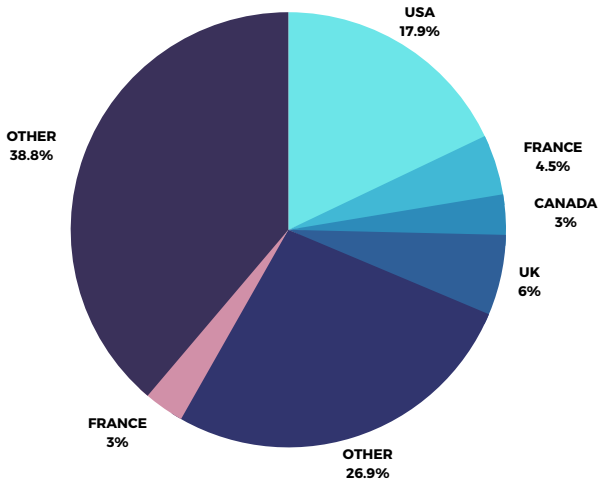
This MDR report provides an analysis of threats and security incidents detected in our company's information systems. The report covers topics such as summary and impact of incidents during the period under review, type and source of threats, status of security measures and recommendations.

Ransomware Groups

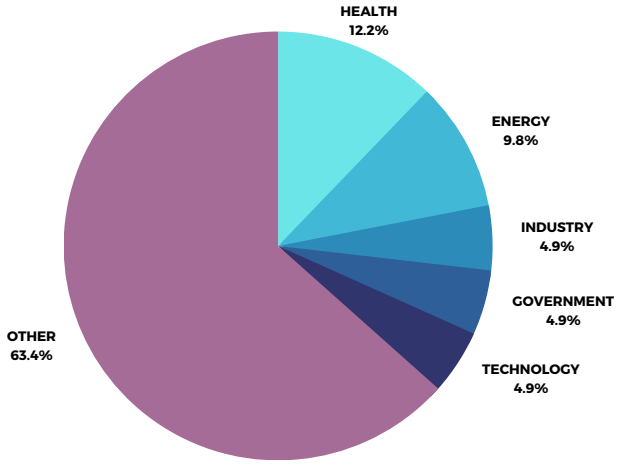
1. LockBit Ransomware Group

Total Number of Attacks: 39

Attack Graph by Country



Attack Graph by Sectors



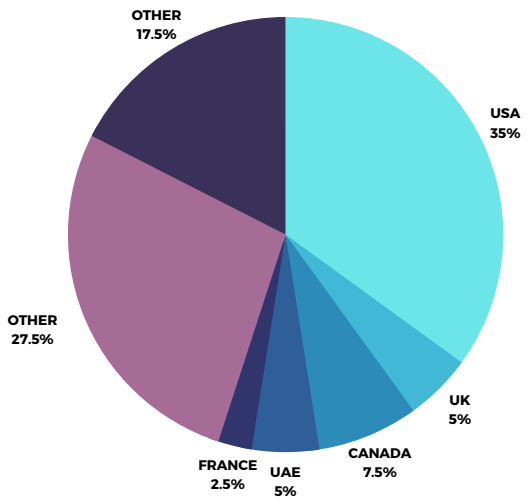
The data on LockBit Ransomware Group's activities presents a distressing picture of the current cybersecurity landscape. The group's preference for targeting the HEALTH sector is especially alarming, as it indicates a willingness to exploit vulnerabilities that could have dire consequences for individuals and healthcare systems. With cyberattacks in the HEALTH sector on the rise, urgent measures are required to safeguard sensitive patient information and ensure the continuity of critical medical services. The group's varied attacks on sectors like ENERGY, INDUSTRY, GOVERNMENT, TECHNOLOGY, and CONSTRUCTION reflect a broad focus on key infrastructure, economic stability, and national security. The "OTHER" category's high number of attacks raises concerns about the potential for unanticipated and unconventional targets, highlighting the need for comprehensive cybersecurity strategies across all industries.

The concentration of attacks on countries like the USA, UK, FRANCE, and CANADA underscores the ransomware group's interest in targeting developed nations with significant economic and political influence. These attacks not only cause financial losses but also create disruptions in crucial sectors, resulting in a ripple effect on the global stage. The data also indicates that LockBit is not confining its operations to well-known targets but is willing to explore vulnerabilities in other countries, making it a challenge for international efforts to combat their activities effectively.

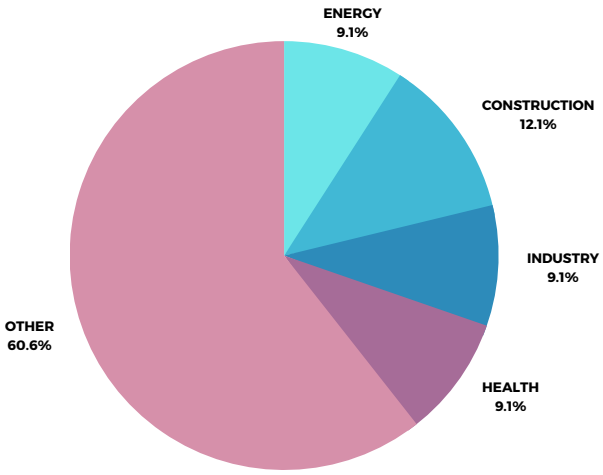
2. 8BASE Ransomware Group

Total Number of Attacks: 33

Attack Graph by Country



Attack Graph by Sectors



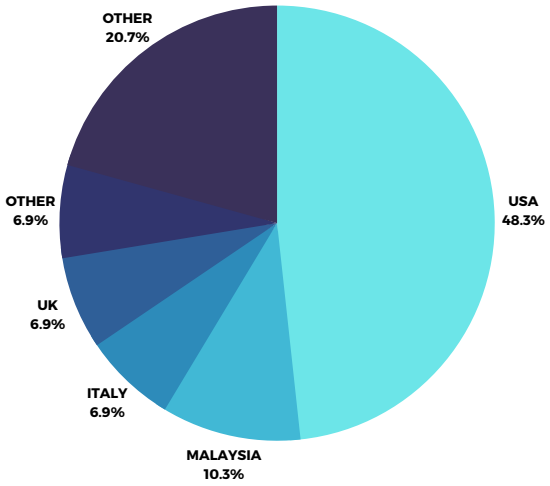
The numerical graphical data on the 8BASE Ransomware Group sheds light on their targeting patterns and geographical reach, indicating a significant and concerning cyber threat. The sectoral attack data reveals that the group has a wide range of interests, with the construction, health, energy, and industry 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.

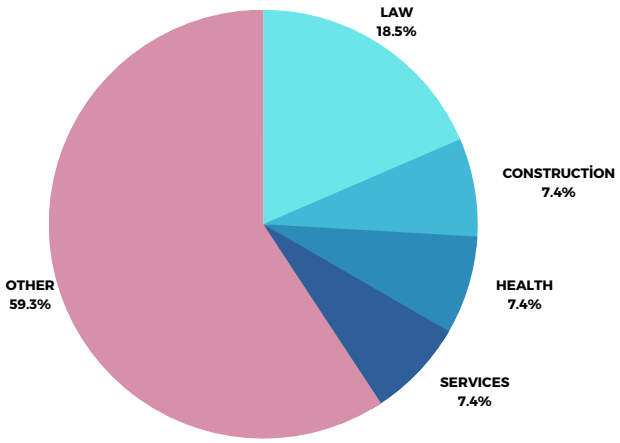
3. ALPHV Ransomware Group

Total Number of Attacks: 27

Attack Graph by Country



Attack Graph by Sectors



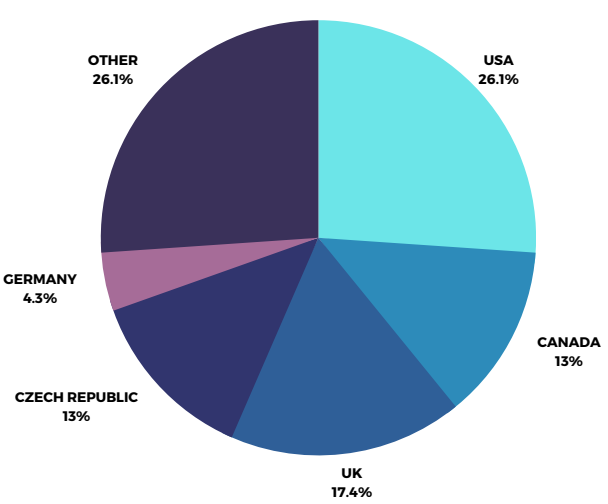
The numerical graphical data on the ALPHV Ransomware Group reveals interesting trends in their targeting strategy, which differs from the previously discussed ransomware groups. The sectoral attack data indicates that the group has a pronounced focus on the legal sector, with five reported attacks. Targeting the legal industry is particularly concerning, as it involves sensitive and confidential information of clients, potentially leading to severe implications for data privacy and legal proceedings. While the construction, health, and services sectors have each experienced two attacks, the majority of their activities are labeled under "OTHER," suggesting a diverse range of targets that are not explicitly specified. This broad targeting approach makes it difficult to predict their next move, posing challenges for cybersecurity experts and organizations in mitigating potential risks.

On the country level, the USA emerges as the primary target, facing 14 attacks. The USA's status as a global economic powerhouse and a hub for various industries makes it an attractive target for ransomware groups seeking lucrative opportunities. Malaysia, the UK, and Italy have also experienced attacks, but their numbers are relatively lower compared to the USA. The presence of "OTHER" countries with 6 attacks suggests that ALPHV is actively expanding its scope globally and exploring vulnerabilities in regions that might have less robust cybersecurity infrastructure.

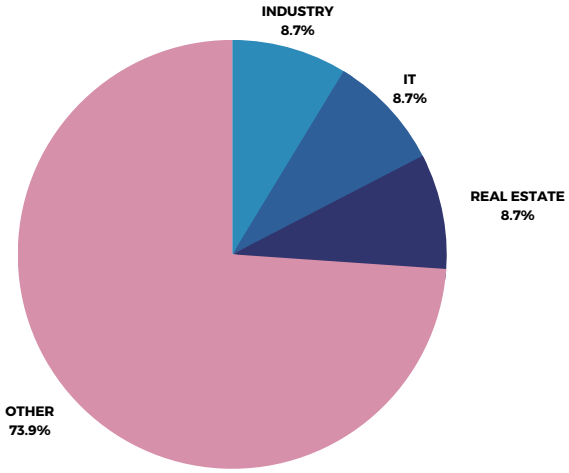
4. NOESCAPE Ransomware Group

Total Number of Attacks: 14

Attack Graph by Country



Attack Graph by Sectors



The numerical graphical data on the NOESCAPE Ransomware Group highlights their selective targeting of specific sectors and countries, signifying a focused and calculated approach in their cyberattacks. The sectoral attack data reveals that the manufacturing sector is the primary target, experiencing three reported attacks. Manufacturing companies often hold valuable intellectual property and trade secrets, making them attractive targets for ransomware groups seeking lucrative payouts or opportunities for industrial espionage. Health and construction sectors have each faced two attacks, while the business sector experienced one attack. The majority of their activities are classified under "OTHER," indicating that NOESCAPE may be exploring vulnerabilities in various sectors beyond the specified categories.

On the country level, the UK emerges as the most targeted, facing three attacks. The UK's strong economy and presence of key industries make it an appealing target for cybercriminals seeking financial gains or aiming to disrupt critical operations. Italy and the USA have also experienced attacks, with two and one incident, respectively. Additionally, Belgium has faced one attack. The presence of "OTHER" countries with seven attacks suggests that NOESCAPE is actively broadening its geographical scope, potentially seeking targets with weaker cybersecurity defenses.

Top Trending CVEs of July 2023

Office and Windows HTML Remote Code Execution Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-36884	8.3	Important	Remote Code Execution

A recently discovered unpatched and Important-rated vulnerability with the identifier CVE-2023-36884 has been disclosed in Microsoft Office and Windows. This vulnerability has a CVSS score of 8.3. In response to this issue, Microsoft has issued guidance on the matter, acknowledging the potential risk posed by this remote code execution vulnerability affecting both Windows and Office products. According to Microsoft's statement, they are actively investigating reports of several remote code execution vulnerabilities that impact their Windows and Office software. Additionally, there have been reports of targeted attacks that aim to exploit these vulnerabilities through specially-crafted Microsoft Office documents.

Mitigations

- In current attack chains, the use of the Block all Office applications from creating child processes Attack Surface Reduction Rule will prevent the vulnerability from being exploited.
- Organizations who cannot take advantage of these protections can set the FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION registry key to avoid exploitation. No OS restart is required, but restarting the applications that have had the registry key added for them is recommended in case the value was already queried and is cached. Please note that while these registry settings would mitigate exploitation of this issue, it could affect regular functionality for certain use cases related to these applications. For this reason, we suggest testing. To disable the mitigation, delete the registry key or set it to "0".
- Add the following application names to this registry key as values of type REG_DWORD with data 1.:
- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION
- Excel.exe
- Graph.exe
- MSAccess.exe
- MSPub.exe
- Powerpnt.exe
- Visio.exe
- WinProj.exe
- WinWord.exe
- Wordpad.exe

Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-35365	9.8	Critical	Remote Code Execution
CVE-2023-35366	9.8	Critical	Remote Code Execution
CVE-2023-35367	9.8	Critical	Remote Code Execution

In addition to the aforementioned unpatched vulnerability, there are eight critical remote code execution (RCE) vulnerabilities that have been successfully patched. Among these, three are associated with the Windows Routing and Remote Access Service (RRAS) and have received a CVSS v3 base score of 9.8. The identified vulnerabilities are CVE-2023-35365, CVE-2023-35366, and CVE-2023-35367. In each case, an attacker has the potential to exploit these vulnerabilities by sending specially-crafted packets to vulnerable assets, resulting in remote code execution.

Fortunately, RRAS is not automatically installed or configured by default, which provides some level of relief. However, for system administrators who have enabled RRAS on their Windows Server installations, it is of utmost importance to prioritize the application of these patches to mitigate potential risks and secure their systems effectively. Swift remediation is crucial to ensuring the protection of critical assets and data from potential exploitation.

Mitigations

- This vulnerability is only exploitable on Windows Servers that have installed and configured the Routing and Remote Access Service (RRAS) role which is not installed and configured by default.

Microsoft Message Queuing Remote Code Execution Vulnerability

CVE	CVSS Score	Severity	Type
CVE-2023-32057	9.8	Critical	Remote Code Execution

CVE-2023-32057 is classified as a Critical vulnerability that impacts Microsoft Message Queuing (MSMQ), with a CVSS score of 9.8. To exploit this vulnerability successfully, an attacker must send a specifically crafted malicious MSMQ packet to a targeted MSMQ server, which could result in remote code execution. It's essential to note that for a system to be vulnerable, the "Message Queuing" service must be enabled.

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.

Windows SmartScreen Security Feature Bypass Vulnerability

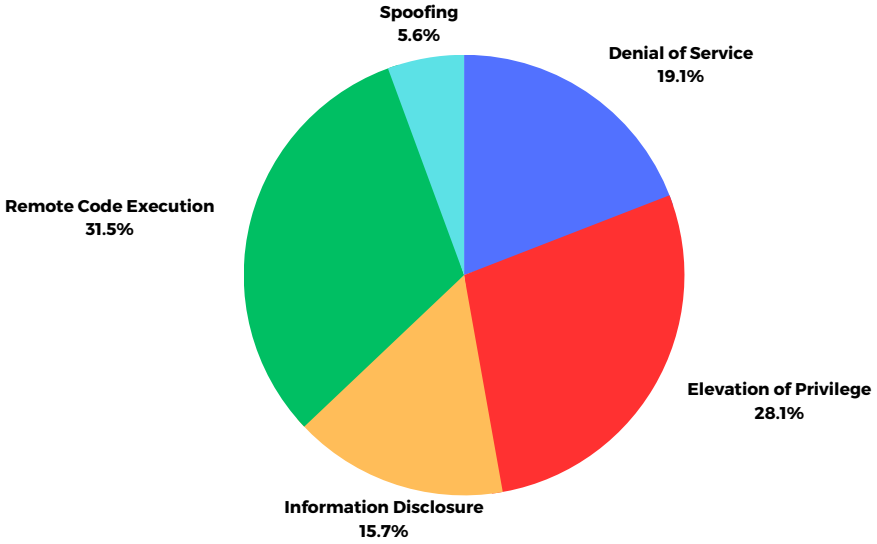
CVE	CVSS Score	Severity	Type
CVE-2023-32049	8.8	Important	Security Feature Bypass

Microsoft has recently addressed the security concern associated with CVE-2023-32049, a security feature bypass vulnerability identified in Microsoft Windows SmartScreen. This vulnerability has been rated as Important, with a CVSS score of 8.8. The vulnerability permits adversaries to bypass the standard Open File Security Warning prompt that typically appears when a user downloads or opens a file from the internet. It is important to note that for this vulnerability to be exploited, user interaction is required.

Mitigations

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

July 2023 Risk Analysis



Based on the numerical graphical data of the risk analysis for July, we can gain valuable insights into the prevalent cyber threats that need attention. This data sheds light on the different attack vectors and techniques that potential adversaries may employ during this period.
One noteworthy observation is the significant increase in the occurrence of Remote Code Execution (RCE) attacks, which account for 28% of the identified risks. RCE is a particularly dangerous threat, as it allows malicious actors to execute code remotely on vulnerable systems, potentially leading to unauthorized access, data breaches, or even complete compromise of critical infrastructure. Organizations must be vigilant in monitoring and patching potential vulnerabilities that could be exploited to execute such attacks.

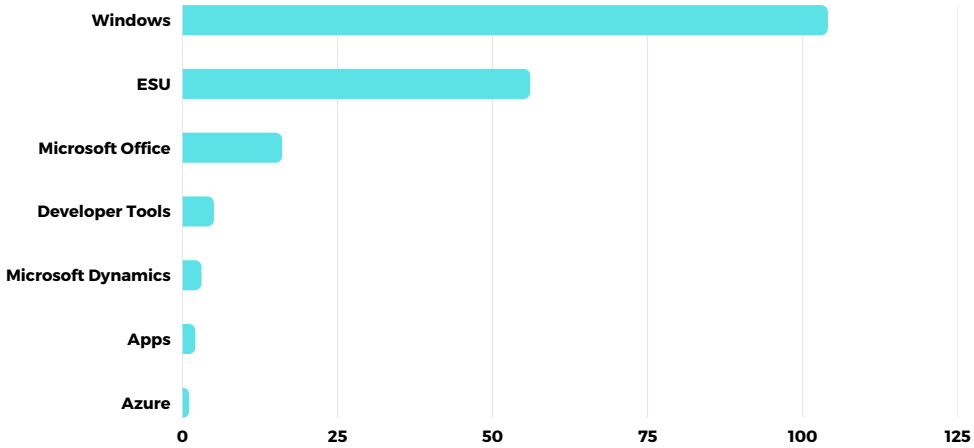
Elevation of Privilege (EoP) stands out as another considerable risk, representing 25% of the analyzed threats. EoP attacks involve adversaries attempting to escalate their privileges within a system, gaining access to resources and capabilities they should not have. Organizations must implement strong access controls and least-privilege principles to mitigate the impact of EoP attacks.

On the other hand, Denial of Service (DoS) attacks, which account for 17% of the identified risks, continue to be a prominent concern. A DoS attack aims to overwhelm a system, network, or application with an excessive amount of traffic, causing it to become unresponsive or unavailable to legitimate users. Mitigating DoS attacks involves robust network capacity planning, traffic filtering, and employing distributed denial-of-service (DDoS) protection mechanisms.

Information Disclosure, accounting for 14% 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.

Lastly, Spoofing attacks, at 5% of the identified risks, demonstrate the attempt by malicious actors 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, July 2023



The data on the product families that received the most patches in July 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 104. 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. Microsoft Office, a widely used suite of productivity applications, received 16 patches, indicating the importance of securing these applications due to their vast user base and potential exposure to various threats.

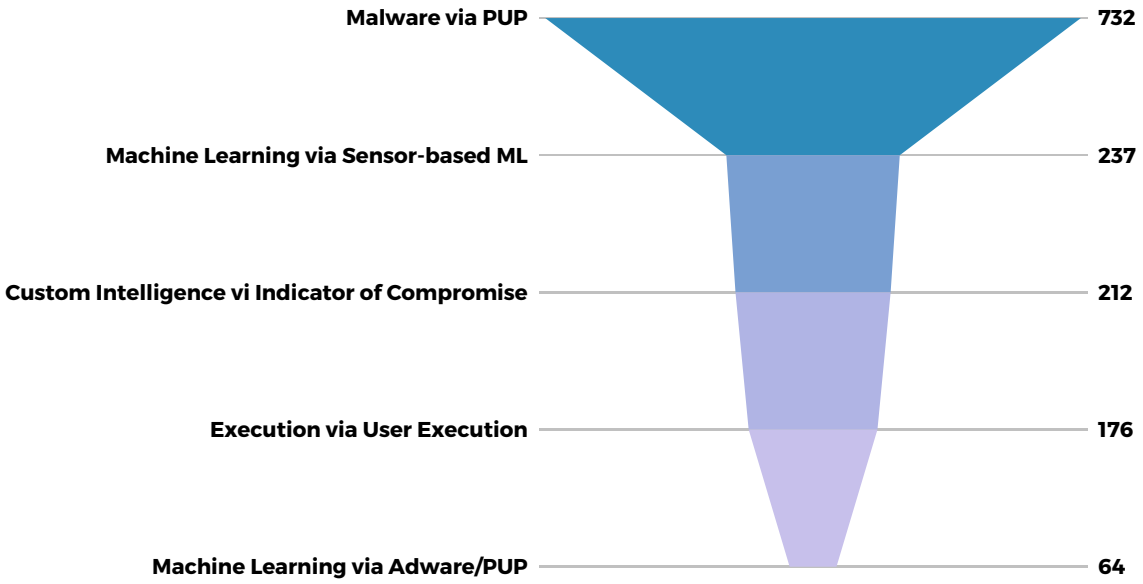
Additionally, Extended Security Updates (ESU), which provide additional support for older versions of Windows, accounted for 56 patches. This highlights the commitment to ensuring the security of legacy systems, recognizing that some organizations may still rely on older Windows versions. System Center and Microsoft Dynamics, with 1 and 3 patches respectively, reflect the attention given to securing critical management and enterprise resource planning (ERP) solutions. These products often handle sensitive data and play crucial roles in business operations, making their security a top priority.

On the other hand, Developer Tools and Apps received 5 and 2 patches, demonstrating the significance of securing the tools and applications used by developers and end-users. Vulnerabilities in these areas can have far-reaching consequences, from compromising the software development process to impacting end-user data and experiences. Lastly, Azure, a rapidly growing cloud computing platform, received 1 patch. 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.

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 and Potentially Unwanted Programs (PUP) are the most widespread threat types, both occurring 732 times. This indicates that traditional malicious software and potentially harmful applications that users might unknowingly install are common attack vectors. Dealing with these threats should remain a top priority in our defense strategies.

Machine Learning techniques, particularly those based on sensor data (Sensor-based ML), exhibit 237 occurrences. This finding highlights the increasing sophistication of cybercriminals in employing artificial intelligence and machine learning algorithms to conduct attacks. Their ability to adapt their strategies and evade traditional security measures requires a proactive and dynamic defense approach.

Custom Intelligence and Indicator of Compromise both show 212 occurrences. This demonstrates that attackers are utilizing tailored intelligence and specific indicators to target victims effectively. As a result, we must continuously enhance our threat intelligence capabilities to identify and respond promptly to emerging threats.

Execution and User Execution, each with 176 occurrences, indicate that cybercriminals frequently rely on tactics that involve executing malicious code or actions by users to infiltrate systems. Educating users about potential risks and implementing stringent execution controls can help mitigate these threats.

The combination of Machine Learning and Adware/PUP at 64 occurrences raises concerns about attackers leveraging machine learning for the distribution of unwanted and potentially harmful programs. Understanding the underlying mechanisms of these attacks is essential for developing effective countermeasures.

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**

Blue Boxing

For decades, attackers have targeted older telephone switches and trunks with a technique known as 'Blue boxing.' By sending a deceptive tone that mimics a supervisor signal, they can reroute or take control of the line. Although the US infrastructure is relatively resilient to such attacks, global connectivity through call centers and outsourcing introduces vulnerabilities. Many international systems, particularly in countries with outdated Telco infrastructure, remain susceptible to Blue boxing due to weak authorization enforcement for administrative functions.

Pharming

In a pharming attack, the target is deceived into inputting sensitive information into seemingly reliable destinations, like an online banking site or a trading platform. The attacker can replicate these trustworthy sites and redirect the victim to their fraudulent site instead of the intended one. Unlike other attacks, pharming does not rely on script injections or the victim clicking on malicious links to accomplish its objective.

Malicious Software Download

An assailant employs deceitful methods to induce a user or an automated process into downloading and installing hazardous code that originates from a source controlled by the attacker. This attack strategy comes in several variations.

HTTP Request Splitting

The flexibility and discrepancies in parsing and interpreting HTTP Request messages by various intermediary HTTP agents (such as load balancer, reverse proxy, web caching proxies, application firewalls, etc.) are exploited by adversaries to divide a single HTTP request into multiple unauthorized and malicious ones directed towards a back-end HTTP agent (e.g., web server). Possible consequences can be explored through CanPrecede relationships.

Kerberoasting

The adversary exploits how service accounts use Kerberos authentication with Service Principal Names (SPNs) to acquire and crack the hashed credentials of a targeted service account, gaining unauthorized privileges. Kerberos authentication relies on a ticketing system to request and grant access to services. The adversary, authenticated as a user, can request Active Directory and obtain a service ticket with portions encrypted via RC4. By extracting and saving the local ticket to disk, they can then brute force the hashed value to reveal the target account credentials.

IP Address Blocking

In this attack scenario, the adversary deliberately discards packets directed to a specific target IP address. The objective is to disrupt access to the service hosted at that particular IP address.

Flooding

The adversary overwhelms a target by rapidly engaging in numerous interactions, exploiting weaknesses in rate limiting or flow control. This type of attack exhausts the target's resources and can lead to denial of service, hindering legitimate user access and potentially causing the target to crash. Unlike resource depletion through leaks or allocations, flooding attacks rely on the volume of requests, with the key factor being the number of requests the adversary can make in a given time period. A higher volume increases the likelihood of success against the target.

Content Spoofing

Content spoofing refers to the act of modifying content to display something different from the original intention, while maintaining the appearance of the legitimate source. Commonly seen in web pages, it can affect various forms of content like emails, file transfers, or other network communication protocols. Spoofing can occur at the source or during transit, and adversaries often try to conceal their modifications. However, in cases like web site defacement, they may not hide their actions. Content spoofing can lead to malware exposure, financial fraud, privacy violations, and other undesired consequences.

Shared Resource Manipulation

An adversary exploits a shared resource, like an application pool or hardware pins, to manipulate behavior. This shared resource is accessed by multiple applications or threads. By co-opting one of the applications or threads, the adversary can manipulate the shared resource. As a result, other applications or threads may trust the compromised resource, leading to invalid trust assumptions, corruption of data, or even crashes and compromises in the sharing applications.

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

Patchwork Group Exploits EyeShell Backdoor to Target Chinese Research Organizations

A hacking group called Patchwork has been targeting universities and research organizations in China using a backdoor named EyeShell. The group is suspected to operate on behalf of India and has been active since at least December 2015, focusing on Pakistan and China with custom implants. Patchwork shares tactical similarities with other Indian-related cyber-espionage groups. Meta previously took down 50 Patchwork-operated accounts on Facebook and Instagram, which were used to collect data from victims in multiple countries. The group used fictitious personas and malicious apps to trick users into clicking on links. Some of their activities have been reported under the name ModifiedElephant, linked to surveillance against human rights activists in India. EyeShell, detected alongside BADNEWS, is a .NET-based backdoor with various capabilities. Another group called Bitter has also been launching phishing attacks in South Asia, targeting aerospace, military, enterprises, government, and universities using the ORPCBackdoor.

Cyberattack on Microsoft Exposes Email Theft from Multiple US Agencies

On July 14, Microsoft announced that a China-based threat actor known as Storm-0558 executed a cyber-attack to steal emails from over 20 U.S. organizations. The attackers exploited a software vulnerability, gaining unauthorized access to Microsoft email accounts. They acquired an inactive MSA consumer signing key and used it to forge authentication tokens, accessing OWA and Outlook.com. The specific method of obtaining the inactive MSA key is under investigation. Microsoft patched the vulnerability after the breach. Storm-0558 successfully exfiltrated email data, including emails, attachments, and conversations from the compromised accounts.

IBM Report: Data Breach Expenses Surge by 15%

IBM's recent report reveals that the cost of data breaches has risen by 15% in the past three years, reaching $4.45 million per breach for affected businesses. Surprisingly, 57% of businesses prefer passing the burden to consumers instead of investing in stronger cybersecurity. This approach leads to consumers facing the consequences of both lax data protection and higher costs. IBM suggests that organizations can enhance data security by investing more in cybersecurity and collaborating with law enforcement, but 37% of breached companies refused to involve authorities. While cybersecurity solutions are readily available, some businesses fail to prioritize it, which could be detrimental to their reputation and customer trust.

infinitum IT
Power of integrated Security

MDR Insights

"July"

infinitumitlabs