infinitum IT
Power of Integrated Security

MDR Insights

“January”

LO BREWİNG

infinitumitlabs

Content

MDR REPORT

As Infinitum IT MDR team, we are pleased to provide you January 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 ;

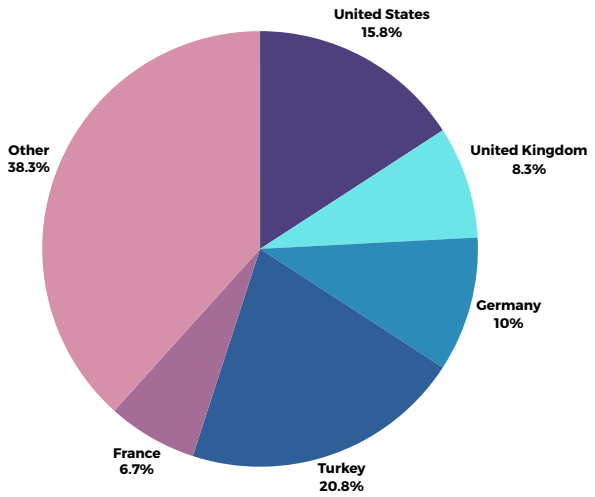
- Data on ransomware groups and graphical representation of their activity this month
- Emerging vulnerabilities
- This month's risk analysis graph
- Graph of product families with the most patches
- Infinitum IT MDR team presents the most common TTPs and their descriptions in our customer environment.
- 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.

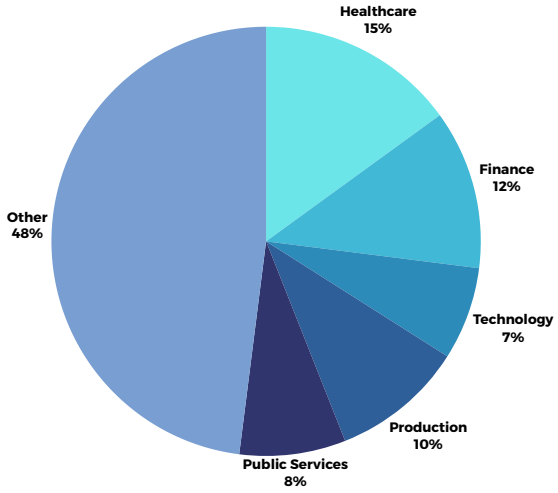
Ransomware Groups

1. Lockbit Ransomware Group

Attack Graph by Country



Attack Graph by Sectors



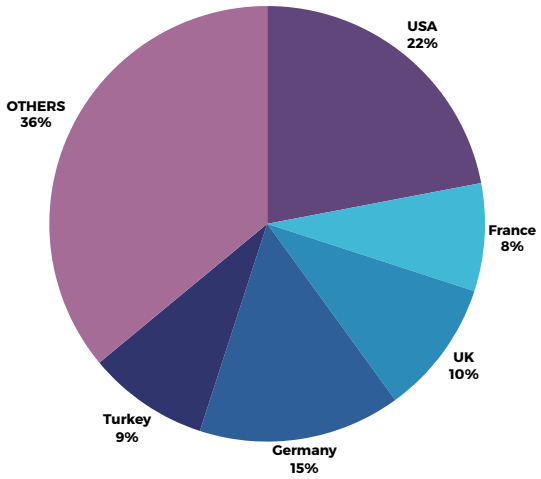
To complicate matters, the term LockBit refers not only to the malware, but also to the group that developed it. LockBit, which first appeared in 2019, is a type of malware designed to be secretly embedded inside organizations. However, unlike other malware, LockBit operates as ransomware instead of stealing data.

Instead of stealing valuable data, LockBit encrypts it, preventing legitimate users from accessing it. A ransom is then demanded from victims to regain access to this data; otherwise, it cannot be accessed again. If they don't pay the ransom, they are threatened with the stolen data being leaked online, which is often referred to as a double extortion. The countdown timer on LockBit's blog on the dark web makes this threat even more dire.

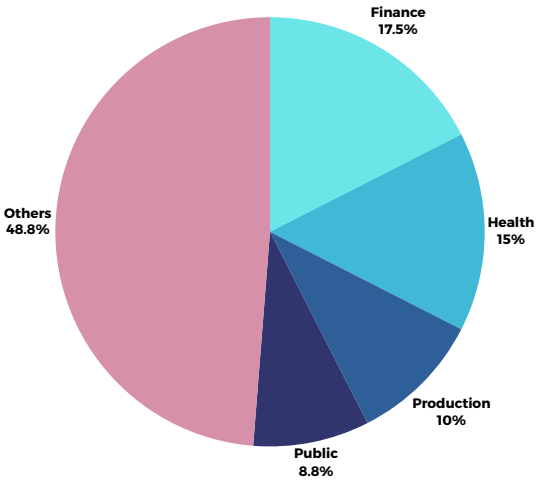
There is a lack of information about the LockBit group and the group does not have a specific political affiliation. Unlike some other cybercrime groups, the LockBit group does not limit the number of members and is highly secretive. This has created a kind of veil of secrecy about the group that is difficult to understand.

2. Play Ransomware Group

Attack Graph by Country



Attack Graph by Sectors



Since its inception, the Play ransomware group has attracted attention by specifically targeting businesses and government organisations in the US, UK, Canada, the Netherlands, Brazil, Argentina, Germany, Belgium and Switzerland. Security experts believe that the Play ransomware group is linked to Russia. The group is also known by the name PlayCrypt and was created by the Balonfly team, which Symantec is monitoring. The ransomware locks victims' files by adding the ".play" extension after encrypting the files.

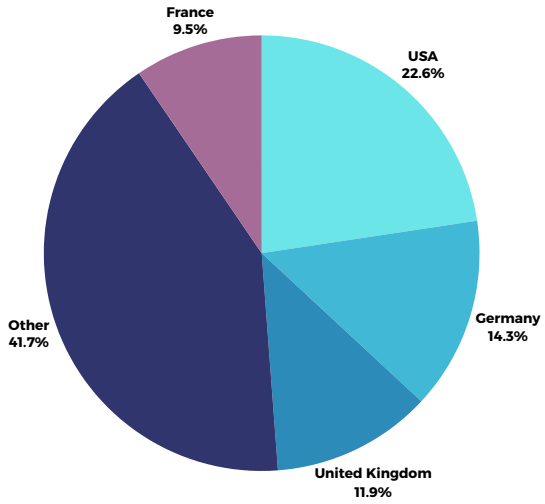
The ransom note contains the word "PLAY" and contact details left by the group responsible for the attack. The group used two new tools specially developed to support their attacks: The first is the Volume Shadow Copy Service (VSS) and the second is Grixbat.

As the Play ransomware group remains active in the ransomware environment, their actions have not been static. In-depth research has unveiled a clear pattern of the group continuously refining their tactics and enhancing their toolkit. This persistence underscores their commitment to perpetuate their presence and expand their influence.

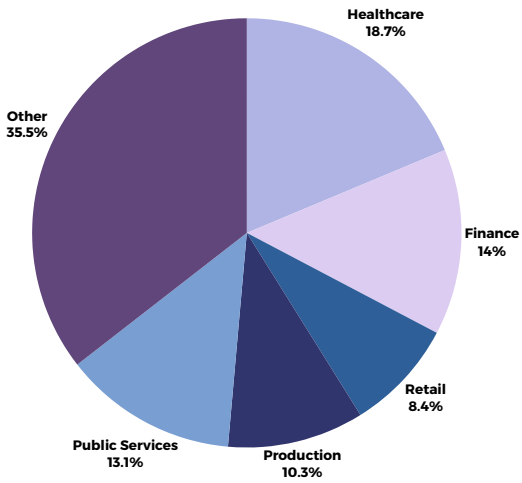
In their quest to achieve these objectives, the Play ransomware group has exhibited an adeptness at leveraging new vulnerabilities and incorporating fresh tools into their attacks. Notably, they have targeted vulnerabilities such as ProxyNotShell, OWASSRF, and Microsoft Exchange Server Remote Code Execution. Furthermore, they have introduced innovative components into their arsenal, including Grixba, a proprietary network scanner and information-stealer, as well as the open-source VSS management tool AlphaVSS.

3. Alphv Ransomware Group

Attack Graph by Country



Attack Graph by Sectors

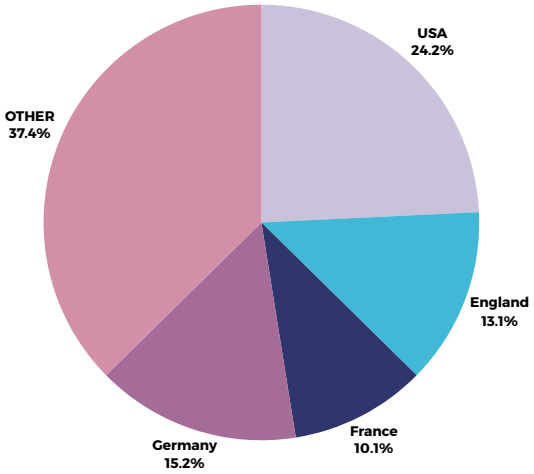


The Alphv ransomware group is a cybercrime group that first emerged in November 2021 and has been described as the first major ransomware family written in the Rust programming language. The group targets organizations all over the world, but with a particular focus on companies in North America, Europe and Asia. Targeted sectors include healthcare, finance, utilities and energy.

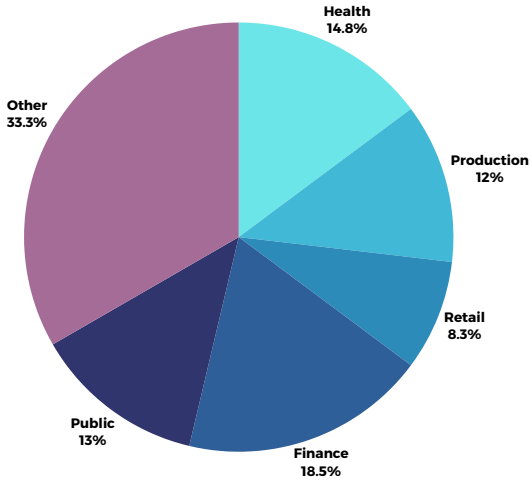
Alphv uses a variety of methods to carry out its attacks. These include malicious email, phishing attacks and security vulnerabilities. After carrying out the attacks, the group demands a ransom from victims to retrieve the encrypted data. Ransom demands are usually in the range of several million dollars.

4. 8BASE Ransomware Group

Attack Graph by Country



Attack Graph by Sectors

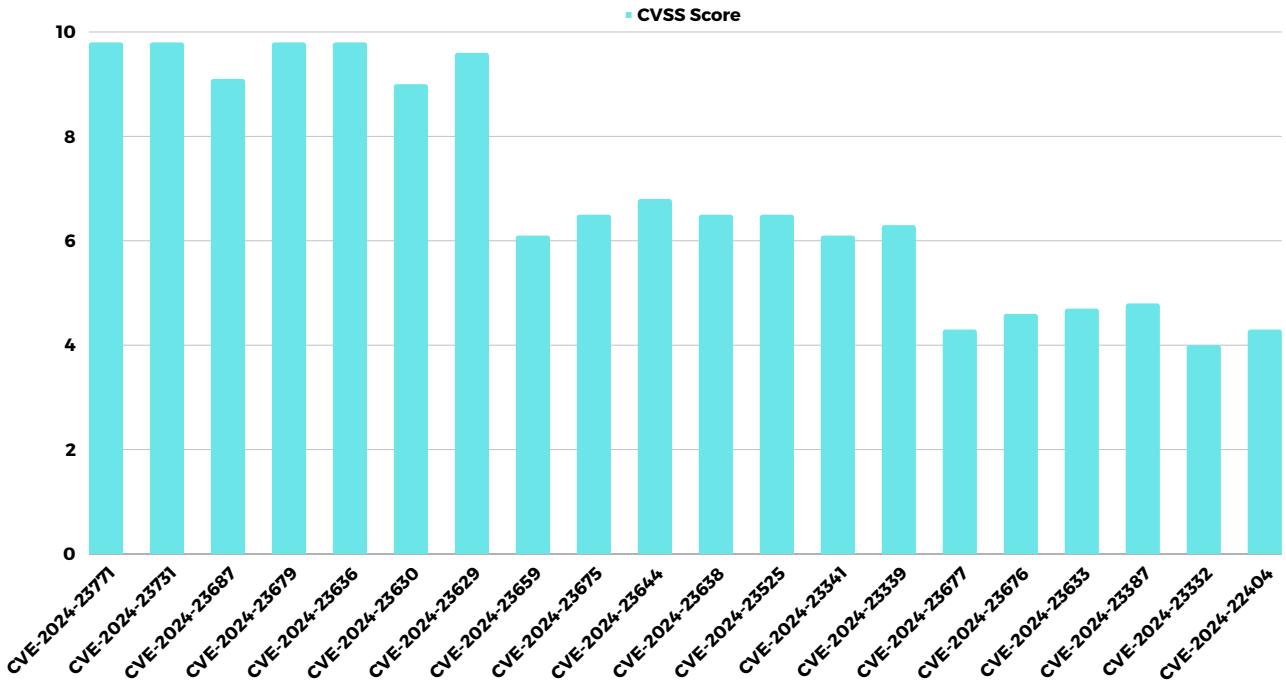


The 8Base ransomware group first showed its face in early 2023. The group transitioned to various ransom models, including a TOR-based victim blogging site in May 2023, but traces of the operation can be traced back to smaller-scale campaigns in 2022. 8Base ransomware has some surface-level similarities with other ransomware families such as Phobos, RansomHouse and Hive, but no official link or relationship has yet been confirmed.

Ransomware campaigns operate across a broad spectrum, targeting a variety of sectors including finance, manufacturing, information technology and healthcare. So far, most of the 8Base campaigns have affected victims in the US and Brazil. While the methods of first access used in the campaigns vary, delivery via phishing email or the use of first access tools (IABs) have been commonly observed.

Furthermore, the ransomware was distributed as data at a later stage in SmokeLoader and similar campaigns. The group's ability to target a wide range of domains through these methods has led cybersecurity experts and organizations to be more vigilant and strengthen their defense strategies.

Top Trending CVEs of January 2023



	CVEs	Published	Description
Critical	CVE-2024-23771	2024-01-22	darkhttpd before 1.15 uses strcmp (which is not constant time) to verify authentication, which makes it easier for remote attackers to bypass authentication via a timing side channel.
	CVE-2024-23731	2024-01-21	The OpenAPI loader in Embedchain before 0.1.57 allows attackers to execute arbitrary code, related to the openapi.py yaml.load function argument.
	CVE-2024-23687	2024-01-19	Hard-coded credentials in FOLIO mod-data-export-spring versions before 1.5.4 and from 2.0.0 to 2.0.2 allows unauthenticated users to access critical APIs, modify user data, modify configurations including single-sign-on, and manipulate fees/fines.
	CVE-2024-23679	2024-01-19	Enonic XP versions less than 7.7.4 are vulnerable to a session fixation issue. An remote and unauthenticated attacker can use prior sessions due to the lack of invalidating session attributes.

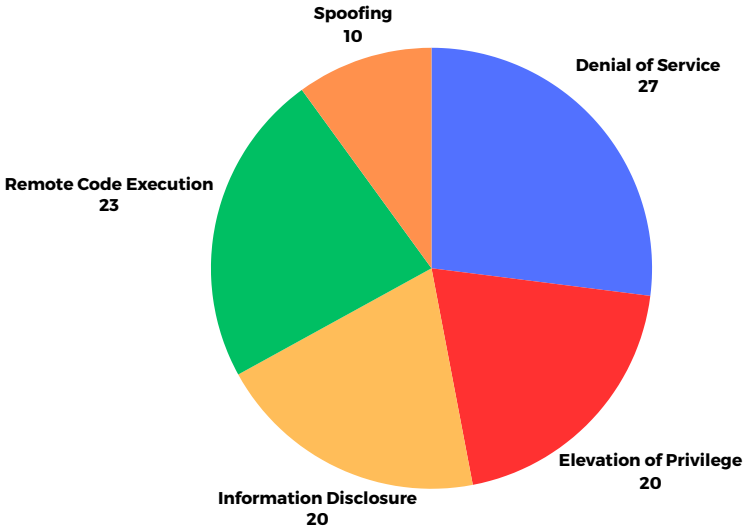
High

CVEs	Published	Description
CVE-2024-23768	2024-01-22	Dremio before 24.3.1 allows path traversal. An authenticated user who has no privileges on certain folders (and the files and datasets in these folders) can access these folders, files, and datasets. To be successful, the user must have access to the source and at least one folder in the source. Affected versions are: 24.0.0 through 24.3.0, 23.0.0 through 23.2.3, and 22.0.0 through 22.2.2. Fixed versions are: 24.3.1 and later, 23.2.4 and later, and 22.2.3 and later.
CVE-2024-23689	2024-01-19	Exposure of sensitive information in exceptions in ClichHouse's clickhouse-r2dbc, com.clickhouse:clickhouse-jdbc, and com.clickhouse:clickhouse-client versions less than 0.4.6 allows unauthorized users to gain access to client certificate passwords via client exception logs. This occurs when 'sslkey' is specified and an exception, such as a ClickHouseException or SQLException, is thrown during database operations; the certificate password is then included in the logged exception message.
CVE-2024-23683	2024-01-19	Artemis Java Test Sandbox versions less than 1.7.6 are vulnerable to a sandbox escape when an attacker crafts a special subclass of InvocationTargetException. An attacker can abuse this issue to execute arbitrary Java when a victim executes the supposedly sandboxed code.
CVE-2024-23682	2024-01-19	Artemis Java Test Sandbox versions less than 1.7.6 are vulnerable to a sandbox escape when an attacker crafts a special subclass of InvocationTargetException. An attacker can abuse this issue to execute arbitrary Java when a victim executes the supposedly sandboxed code.

Medium

CVEs	Published	Description
CVE-2024-23675	2024-01-22	In Splunk Enterprise versions below 9.0.8 and 9.1.3, Splunk app key value store (KV Store) improperly handles permissions for users that use the REST application programming interface (API). This can potentially result in the deletion of KV Store collections.
CVE-2024-23659	2024-01-19	SPIP before 4.1.14 and 4.2.x before 4.2.8 allows XSS via the name of an uploaded file. This is related to javascript/bigup.js and javascript/bigup.utils.js.
CVE-2024-23525	2024-01-18	The Spreadsheet::ParseXLSX package before 0.30 for Perl allows XXE attacks because it neglects to use the no_xxe option of XML::Twig.
CVE-2024-23179	2024-01-12	An issue was discovered in the GlobalBlocking extension in MediaWiki before 1.40.2. For a Special:GlobalBlock?uselang=x-xss URI, i18n-based XSS can occur via the parentheses message. This affects subtitle links in buildSubtitleLinks.

January 2023 Risk Analysis



Drawing upon the numerical data derived from our January risk analysis, we can discern critical trends and emerging threats that demand immediate attention. This data provides a comprehensive perspective on the array of attack vectors and techniques that potential adversaries may exploit during this specific timeframe.

RCE attacks now account for a significant 23% of the identified risks. RCE remains a serious concern as it grants malicious actors the ability to execute code on vulnerable systems remotely, potentially resulting in unauthorized access, data breaches, or even the complete compromise of critical infrastructure. Hence, organizations must maintain vigilant monitoring and swift remediation of potential RCE vulnerabilities.

Elevation of Privilege (EoP) emerges as another significant risk, constituting 20% of the analyzed threats. EoP attacks involve threat actors attempting to escalate their privileges within a system, seeking access to resources and capabilities beyond their authorized level. To mitigate the impact of EoP attacks, organizations should rigorously enforce robust access controls and adhere to the principle of least privilege.

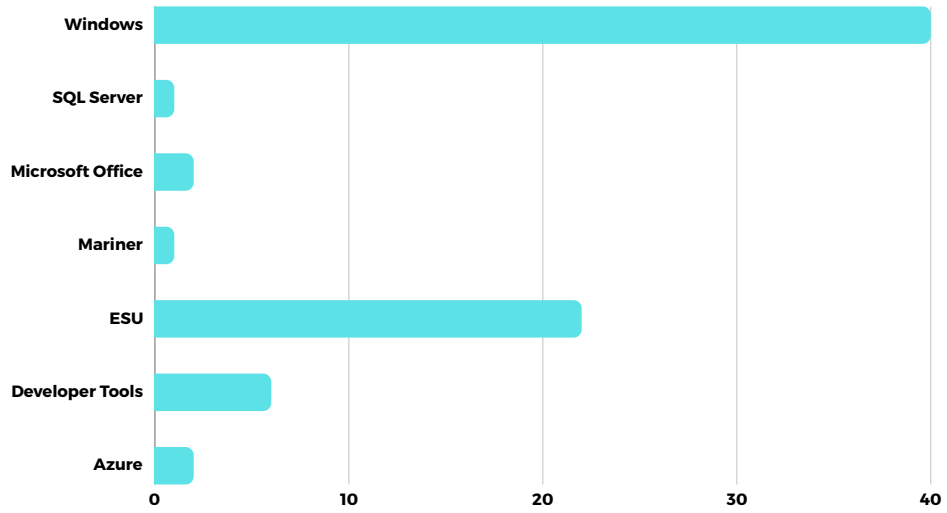
Meanwhile, Denial of Service (DoS) attacks, contributing to 27% of the identified risks, continue to pose a substantial threat. DoS attacks aim to overwhelm a system, network, or application with an excessive volume of traffic, rendering it unresponsive or inaccessible to legitimate users. Effectively countering DoS attacks requires meticulous network capacity planning, traffic filtering, and the deployment of distributed denial-of-service (DDoS) protection mechanisms.

Information Disclosure, making up 20% of the identified risks, signifies the inadvertent or unauthorized exposure of sensitive data to unauthorized entities. Such incidents can result from unsecured configurations, weak authentication, or other vulnerabilities, potentially leading to regulatory non-compliance, reputational damage, and financial losses. Organizations must prioritize data protection through robust encryption, access controls, and regular security assessments.

Lastly, Spoofing attacks, contributing to 10% of the identified risks, encompass malicious actors' attempts to conceal their identities or manipulate data packets to deceive systems or users. Implementing robust authentication mechanisms, such as multi-factor authentication, is crucial in mitigating the risks associated with Spoofing attacks.

Navigating the ever-evolving cybersecurity landscape in January demands vigilance, adaptability, and proactive measures. Staying ahead of emerging threats and vulnerabilities is essential for safeguarding organizational assets and ensuring robust security posture.rawing upon the numerical data derived from our January risk analysis, we can discern critical trends and emerging threats that demand immediate attention. This data provides a comprehensive perspective on the array of attack vectors and techniques that potential adversaries may exploit during this specific timeframe.

Patches by Product Family, January 2023



Critical Vulnerabilities in Kerberos and Microsoft Hyper-V
CVE-2024-20674 is a security feature bypass vulnerability that can allow a remote attacker to intercept a valid Kerberos authentication message from the authentication server and use it to impersonate the authentication server to the victim machine. This relationship can then be leveraged to intercept valid Kerberos authentication sessions and enable the attacker to harvest credentials from the victim to impersonate the victim to other services covered by the Kerberos single sign-on implementation.

According to Microsoft, this vulnerability has an adjacent attack vector, meaning the adversary must first be on the restricted network to intercept these messages. Though Microsoft does not have data to suggest this vulnerability has been exploited in the wild, they have noted that exploitation is very likely after this announcement.

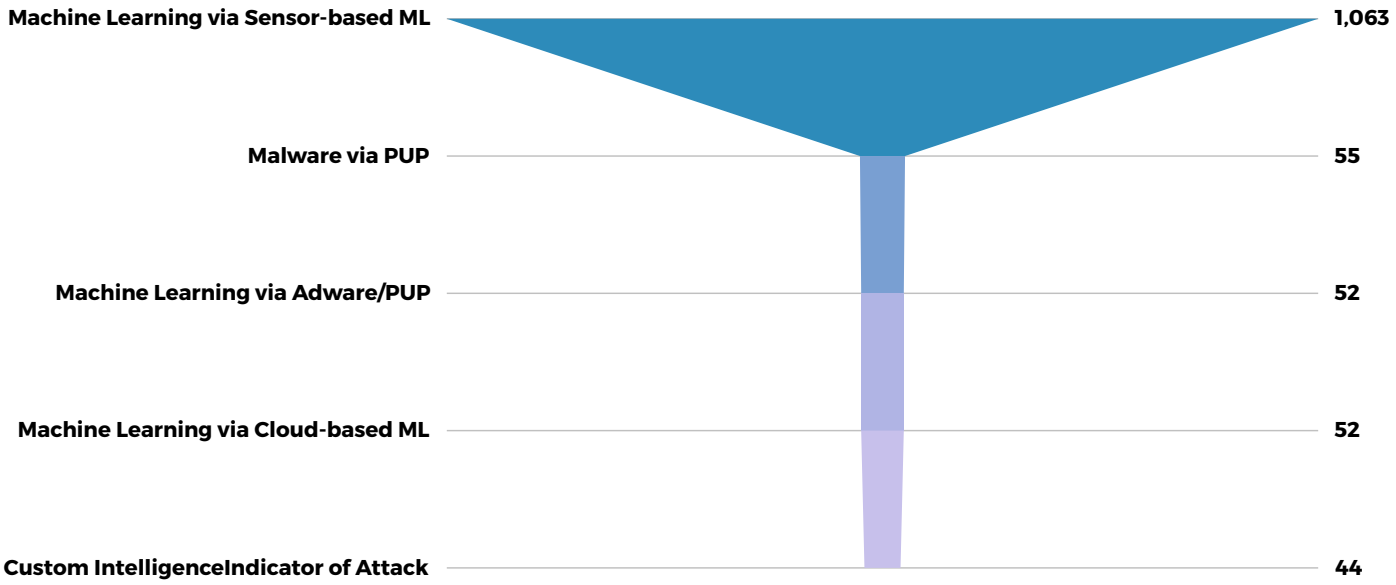
CVE-2024-20700 is a remote code execution vulnerability with high attack complexity present in the Windows Hyper-V subsystem. Little is publicly revealed about this vulnerability. However, given that Hyper-V is the built-in hypervisor for all Windows platforms, this vulnerability should be patched with haste.

Not All Relevant Vulnerabilities Have Patches: Consider Mitigation Strategies
As we have learned with other notable vulnerabilities, such as Log4j, not every highly exploitable vulnerability can be easily patched. As is the case for the ProxyNotShell vulnerabilities, it's critically important to develop a response plan for how to defend your environments when no patching protocol exists.

Regular review of your patching strategy should still be a part of your program, but you should also look more holistically at your organization's methods for cybersecurity and improve your overall security posture.

The Most Common TTPs

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



In this monthly MDR report, we present an analysis of the data obtained from our customers' cybersecurity systems. The graphic includes information on the Detection Counts for various categories:

1. Machine Learning via Sensor-based ML (1063):
This high number, 1063, indicates there have been a substantial number of attacks detected using machine learning models integrated with various sensors. These sensors could be:

Network security tools monitoring traffic for suspicious activity.
Endpoint security software watching for malware behavior on individual devices.
Industrial control system sensors detecting anomalies in operational data.
2. Malware via PUP (55):
This data point shows there have been 55 attacks where Potentially Unwanted Programs (PUPs) were used as a delivery mechanism for malware. PUPs are often seemingly harmless applications that bundle with malware, tricking users into installing both unintentionally.

3. Machine Learning via Adware/PUP (52):
Similar to the previous point, this indicates 52 attacks utilized adware or PUPs alongside machine learning algorithms. This could involve using adware for reconnaissance, spreading malware through ad networks, or employing machine learning embedded within the PUPs for malicious purposes.

4. Machine Learning via Cloud-based ML (52):
Matching the number for Adware/PUP, we see 52 attacks used cloud-based machine learning. This could involve:

Utilizing cloud-based malware detection services.
Attackers training their own models on cloud infrastructure.
Exploiting vulnerabilities in cloud platforms for malicious purposes.
5. Custom Intelligence Indicator of Attack (44):
This lower number suggests there have been 44 attacks detected based on custom indicators of attack (IOAs) developed specifically for specific threats or threat actors. This highlights the importance of threat intelligence and tailored security solutions for addressing unique and emerging threats.

Overall, this data points towards a trend of attackers increasingly using machine learning in their strategies. Integrating sensor-based detection, leveraging seemingly harmless PUPs, and utilizing cloud infrastructure are all concerning tactics. However, the presence of custom IOAs indicates defenders are also adapting and developing targeted countermeasures.

This monthly analysis provides valuable insights into the effectiveness of our cybersecurity measures, showcasing a proactive and multi-faceted approach to safeguarding our clients' environments.

Common Types Attack Vectors

Risk Severity

Critical **High** **Medium**

Subverting Environment Variable Values

The assailant manipulates the environment variables that either directly or indirectly influence the target software. The objective of the attacker is to induce a deviation in the expected behavior of the target software, ultimately favoring the attacker, without disrupting its core functionality.

Overflow Binary Resource File

This type of attack capitalizes on a buffer overflow vulnerability within the processing of binary resources, which can encompass various file types such as MP3 for music or JPEG for images, among others. Perpetrators may exploit these vulnerabilities discreetly, potentially infiltrating a client machine without raising suspicion, such as when a web browser loads what appears to be a harmless JPEG file. This exploitation grants the adversary access to the execution stack, enabling the execution of arbitrary code within the targeted process.

Manipulating Writeable Configuration Files

Typically, these files are manually edited and escape the scrutiny of system administrators. Any capability on the part of attackers to manipulate such files, such as those within a CVS repository, bestows unauthorized access directly to the application, on par with the privileges of authorized users.

Symlink Attack

An attacker strategically places a symbolic link in a way that leads the targeted user or application to access the endpoint of the link, mistakenly believing it is accessing a file with the link's name.

Spear Phishing

An attacker performs a CAPEC-98-specific Phishing attack by targeting a specific user or group, focusing on maximum attention and deception ability. Spear Phishing is a sophisticated Phishing attack targeted at a specific user or group, and the quality of the targeted email is often enhanced by showing that it comes from a familiar or trusted source. If a trusted entity's email account has been compromised, the message is usually digitally signed. The message contains information specific to the target users, making them more likely to follow the URL to the compromised site. Once the user follows the instructions, the attack proceeds as a standard Phishing attack.

Jamming

An attacker employs radio noise or signals to interfere with communications, aiming to disrupt the normal flow. Through deliberately flooding system resources with unauthorized traffic, legitimate traffic from authorized users is denied access.

Interception

An attacker monitors data streams to or from the target for information gathering. This may involve sniffing network or other data streams, such as radio signals, either actively initiating or passively observing communications. The attacker is not the intended recipient of the data and positions themselves to observe explicit channels, like network traffic. Unlike other information gathering methods, this attack does not involve altering or forwarding communication content, distinguishing it from a Adversary-In-the-Middle (CAPEC-94) attack.

Excessive Allocation

The attacker performs an attack that disrupts the target's resources by over-allocation. It is usually centred on memory allocation, but may also affect bandwidth, processing cycles or other resources. The attack aims to overload the target's resources using one or several carefully formatted requests, often exploiting a fault of the target, causing it to allocate more resources than usual.

Sniffing Network Traffic

In this attack scenario, the attacker observes network traffic between nodes in a public or multicast network with the aim of capturing sensitive information at the protocol level. Network sniffing tools can expose details of TCP/IP, DNS, Ethernet, and other low-level network communications. The attacker adopts a passive role, merely observing and analyzing the traffic. While the attacker may influence the content of the observed transaction, they are not the intended recipient of the target information

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

North Korean Hackers Weaponize Research Traps to Propagate RokRAT Backdoor

In November 2023, a North Korea-linked threat actor called ScarCruft launched a campaign targeting experts. According to SentinelOne, ScarCruft uses technical threat research reports to trick cybersecurity professionals. The attack targets a North Korea-related expert, prompting them to open a ZIP archive file containing malicious Windows shortcut files. Researchers found that LNK files are part of the planning and testing processes, suggesting that ScarCruft has effectively adjusted its tactics. ScarCruft's commitment to obtaining strategic intelligence is ongoing, and it continues its efforts to understand how the international community perceives developments in North Korea.

Critical Jenkins Vulnerability Leaves Servers Open to Remote Code Execution Attacks Update Now

A critical vulnerability in Jenkins' open source CI/CD automation software poses a potential risk of remote code execution (RCE) on systems. The vulnerability, identified as CVE-2024-23897, is caused by the ability to read arbitrary files via Jenkins' built-in command-line interface (CLI). This feature, which is enabled by default in older versions of Jenkins, could allow attackers to remotely intervene. Although this vulnerability, discovered by security researcher Yaniv Nizry, has been closed with the latest versions of Jenkins, system administrators should quickly apply this update and turn off CLI access as a workaround. Otherwise, attackers may find the opportunity to carry out a variety of dangerous attacks. Therefore, it is critical that security measures are taken immediately, as it is of utmost importance for Jenkins users to quickly apply security updates.

AllaKore RAT Malware Targeting Mexican Firms with Financial Fraud Scams Exposed

A new phishing campaign targeting Mexican financial institutions contains a modified version of the AllaKore RAT. The campaign, carried out by an unknown Latin America-based threat actor, has been ongoing since at least 2021. The AllaKore RAT is used in attacks aimed at targeting large companies. The attacks cover the retail, agriculture, public sector, manufacturing, transportation, commercial services, capital goods and banking sectors. The campaign starts with a .NET downloader that verifies the geographic location of Mexico and infects the victim's machine with the AllaKore RAT. The RAT is capable of remote control, keystroke logging, screenshotting, uploading/downloading files, but new functions have been added, such as banking fraud and targeting Mexican banks. The threat actor's relationship with Latin America is evident through Mexican Starlink IPs and instructions in Spanish. The actor has consistently attacked Mexican institutions for financial gain, and this activity has been ongoing for over two years.

infinitum IT
Power of Integrated Security

MDR Insights

“January”

infinitumitlabs