deepwatch™

2024 annual threat report

ATR

Observations, Metrics, Trends
& Forecast from the Deepwatch
Adversary Tactics & Intelligence Team

Welcome to the **Deepwatch ATI 2024 Annual Threat Report**

INTRODUCTION

For our third year, the Deepwatch Adversary Tactics and Intelligence team presents our Annual Threat Report. Here we provide Deepwatch Observations from 2023, and forecast what organizations can expect in 2024.

With in-depth analysis of our open source intelligence reporting, we share data on nearly 1.5 million security related events detected across our customers' environments, and through response engagements.

For 2023, we cover the most predominant threats, techniques, and trends, as well as our most significant observations. Finally, our 2024 forecast calls for increased cyber resilience

This report sets itself apart with our proprietary data and insights derived from comprehensive detection coverage coupled with human-led expert investigation and confirmation of threats. The data that powers Deepwatch results from thousands of expert investigations across hundreds of thousands of protected systems.

Each of the nearly 1.5 million detected security related events that we responded to have one thing in common: They were not prevented by our customers' expansive security controls—they are the product of our analytics that we use to detect the threats that would otherwise go undetected.

When our Security Content team and detection engineers develop detection analytics, they map them to one or more corresponding MITRE ATT&CK techniques. If the detection uncovers a potential threat, a Deepwatch expert will investigate and, if confirmed, provide detailed information about the activity observed.

Because we know which ATT&CK techniques a detection aims to detect and which detection led us to identify a threat, we can look at this data over time and determine technique prevalence, correlation, and much more.

To ensure effective detection coverage, Deepwatch takes advantage of a defense in depth strategy encompassing various stages of an attack. As a result, technique coverage is not skewed to a specific stage. This contrasts with other providers whose visibility may focus towards the beginning, middle, or later stages of an intrusion due to technology visibility limitations.

This report examines the broader landscape of threats that leverage techniques and other tradecraft. We also track specific threats associating malicious or suspicious activity with a new or existing threat activity cluster, specific malware variants, abuse of legitimate tools, and known threat actors. ATI continually tracks and analyzes threats throughout the year, publishing weekly threat intelligence reports.

In 2024 organizations can expect:

- Information Stealing Malware Will Continue to Become More Sophisticated
- Mass Vulnerability Exploitation and Supply Chain Attacks Will Continue to be a Significant Threat
- Tactics Involving External Remote Services, User Execution, and Application Layer Protocol Will Continue to be Widely Observed
- Prevalence of Ai in Malleable Tool Performance and Defense Evasion
- Abuse of Legitimate Internet Services Will Continue, Likely Escalating in 2024
- Rise of Non-Malware-Based Cyber Attacks in 2024

CONTENT INSIDE

2023 Top Threats

In an ever-evolving cyber threat landscape, understanding the top threats from the previous year is crucial for organizations to bolster their cybersecurity posture. Identifying the top threats provides valuable insights into the methods and motivations of threat actors and serves as a cornerstone for developing robust defense strategies.

This knowledge enables organizations to anticipate potential attacks, prioritize security investments, and effectively tailor their incident response plans.By analyzing these critical aspects, organizations can see the shifts in the cyber threat environment, identify emerging trends, and proactively adapt to the changing tactics of adversaries.

This, in turn, enhances resilience against cyber threats, ensuring the continuity and protection of critical assets, in a landscape marked by sophistication and unpredictability.

MITRE ATT&CK Technique Metrics

Total of All Techniques Observed: **1,343,862**

MITRE ATT&CK TECHNIQUE STATS

Detection Metrics

Total of All Detections: **1,351,145**

DETECTION STATS

Malware and Hacking Tool Metrics

Total Malware Families Reported in OSINT: **207**

MALWARE STATS

Threat Response Metrics

Total Engagements: **45** *(not including benign activity and pentest activity)*

INCIDENT RESPONSE ENGAGEMENT STATS

2023 Observations Quick Look

In 2023, over half of incident response engagements involved suspicious activities and account compromises, signifying a major challenge for organizations. These included unauthorized account access and malicious script executions, often evading standard security measures and leading to fraudulent activities. This underscored the need for improved email security and employee training.

Ransomware remained a significant threat, particularly targeting healthcare organizations, with sophisticated attacks using double extortion tactics. Deepwatch responded to a range of ransomware groups, including ALPHV, Monti, and Blacksuite, highlighting the evolving threat landscape.

The year also saw diverse malware and hacking tool attacks, notably impacting the manufacturing and finance sectors. Deepwatch frequently dealt with threats like Raccoon Stealer, IcedID, and Cobalt Strike, emphasizing the need for continuous vigilance and advanced security measures.

Additionally, the exploitation of critical vulnerabilities in internet-facing systems was prevalent, particularly involving known vulnerabilities. This trend called for a proactive risk management approach, evidenced by numerous system exploitation responses, including ColdFusion Exploitation.

The MITRE ATT&CK framework revealed consistent attack tactics in 2023, including Valid Accounts, User Execution, and Brute Force, indicating a focus on exploiting legitimate credentials and user interaction. The most observed tactics were Application Layer Protocol, Valid Accounts, Brute Force, Create or Modify System Process, and External Remote Services.

Finally, malware and hacking tool families like Cobalt Strike, Mimikatz, and QakBot dominated open-source reports. Known for network infiltration and credential theft, these malware families continued to challenge global cybersecurity, quickly resuming operations even after law enforcement disruptions.

deepwatch

Suspicious Activity and Account Compromise Dominated Incident Response Engagement

Account compromise and various forms of other suspicious activity were a top threat for organizations in 2023. The activity typically involves unauthorized access to user accounts, malicious network traffic, script execution, suspicious network traffic, and brute force activity to carry out fraudulent activities, such as stealing sensitive information or requesting wire transfers. Additionally, these attacks can be challenging to detect and prevent because cybercriminals use compromised accounts to access various data and perform actions, such as sending phishing emails and setting inbox rules. Whereas various suspicious activities may bypass security solutions. As a result, organizational leadership expects their security teams to increase their focus on email security and employee training to mitigate the risk of BEC and EAC in 2024.

> When a threat actor has the keys to the kingdom (valid admin usernames and passwords) they are afforded a level of access and freedom within a network that allows them to bypass standard security measures with ease. These credentials can be used to perform actions with the same authority as legitimate administrators, rendering traditional detection mechanisms ineffective.
>
> Eric Ford, Deepwatch Senior Intelligent Analyst

In Q1, over 50% of threat response engagements resulted from account compromises and suspicious activities, including social engineering attacks on IT help desks, abnormal O365 access with unauthorized inbox rule creations, RDP brute force attacks, and the execution of malicious scripts and applications.

Over 50% of all incident response engagements involved suspicious activity or account compromise, encompassing everything from unauthorized account access and various activities to access a user account to suspicious network traffic and brute force activity.

Deepwatch responded to account compromise and malicious activity for organizations across nine different industries, predominantly in the finance and insurance, manufacturing, and health care and social assistance sectors.

deepwatch

Ransomware Still Continues to Affect Many Industry Sectors

Ransomware continued to be a significant threat in 2023, as cybercriminals continued to use this type of malware to hold organizations' data and systems hostage for financial gain. Despite increased awareness and efforts by businesses and governments to protect against ransomware attacks, the frequency and sophistication of these attacks continued to advance. The use of double extortion techniques, where attackers encrypt data and threaten to release stolen data publicly, added to the pressure on organizations to pay the ransom. Businesses continue to incur significant losses due to ransomware attacks, both from the ransomware payment and operational costs due to disruption of service and restoration.

The majority of ransomware events we responded to involved the use of double extortion techniques, where threat actors not only encrypt data but also, threaten to release stolen data publicly, adding to the pressure on organizations to pay the ransom.

Health Care and Social Assistance organizations were the leading targets for ransomware incidents observed and responded to by Deepwatch.

Deepwatch responded to incidents involving ALPHV, Monti, and Blacksuite Ransomware threat groups. Several incidents involved the exfiltration of data.

deepwatch

Malware

In 2023, Deepwatch observed various malware families during incident response engagements, highlighting the evolving nature of cyber threats. Various malware families have different purposes, from dropping additional malware and data theft to establishing command and control to enrolling the infected device in a botnet. Our team detected and responded to various malware infections, such as Raccoon Stealer, IcedID, Cobalt Strike, ngrok usage, and malicious script executions in customer environments. This diverse range of threats underscores the need for continuous vigilance and advanced security measures in the ever-changing landscape of cyber threats.

Almost 15% of all incident response engagements involved a malware infection, not including ransomware.

Nearly all infections impacted the manufacturing and finance and insurance sectors.

64 Cyber Intel Briefs published in the last year involved malware.

deepwatch

Exploitation of Critical Vulnerabilities for Internet-Facing Systems

In 2023, active exploitation of software vulnerabilities was a common trend observed in the threat landscape. We observed this trend across various industries and organizations, significantly impacting incident response efforts. Many organizations responded to multiple instances of active exploitation, often involving known vulnerabilities and publicly available exploit code. Despite the efforts of security teams to patch and secure systems, the speed and sophistication of attackers made it challenging to prevent or quickly remediate these types of incidents. Looking forward, organizations should take additional steps to be more vigilant and proactive in their approach to risk management to mitigate the impact posed by active exploitation.

50% of Deepwatch threat response engagements
resulted from coldfusion exploitation.

10% of all incident response engagements
involved significant system exploitation.

9 customer advisories
involved vulnerabilities being actively exploited against internet-facing systems.

deepwatch

Top ATT&CK Techniques and Detections Observed in 2023

In 2023, the cybersecurity landscape was dominated by a consistent pattern of attack tactics and threat detections.

They underscore a persistent focus of threat actors on exploiting system vulnerabilities and leveraging legitimate credentials for unauthorized access.

This trend suggests that threat actors are increasingly bypassing conventional security measures, emphasizing the need for robust identity and access management. Trends demand continuous monitoring of system processes and network activities.

The top detections, particularly the recurring instances of Suspicious Activity and Increasing Risk Score observed in the majority of months, highlight the critical importance of proactive threat detection and risk assessment strategies.

The frequent occurrence of Internal Network Service Discovery and Increased Activity by New Threat Object detections further indicates that adversaries constantly evolve their methods,. It demands a dynamic and adaptive security posture that can quickly respond to emerging threats and anomalies within the network infratstructure.

Top 5 MITRE ATT&CK Tactics Observed in 2023

- T1071: Application Layer Protocol
- T1078: Valid Accounts
- T1110: Brute Force
- T1543: Create or Modify System Process
- T1133: External Remote Services

The following MITRE ATT&CK tactics placed in the Top 10 of observed tactics in every month of 2023

- T1078: Valid Accounts
- T1204: User Execution
- T1046: Network Service Scanning
- T1543: Create or Modify System Process
- T1110: Brute Force
- T1071: Application Layer Protocol i

Top 5 Detections Observed in 2023

External Authentication from Non-Excluded Country: The objective of this detection rule is to detect suspicious authentications to resources by monitoring the country information that the user's are logging in from. If the user is logging in from a Country that is not expected, then it will alert.

Suspicious Activity: This detection rule's objective is to detect when many distinct anomalies are observed for a single user or system over a 7 day time period.

Increasing Risk Score: This detection rule is intended to detect when the risk score for a single user or system rapidly increases in a 24 hour time period.

Increased Activity by New Threat Object: This detection rule is intended to detect when a new threat object (i.e., a known malicious domain, IP address, etc.) is observed across multiple risk objects or detection/anomaly searches in a 7 day time period.

Internal Network Service Discovery: This rule is designed to detect an internal host sending unsolicited packets to many destinations over a single port to map the network or discover live hosts to exploit.

Top Detections Observed in the Majority of Months in 2023

- Suspicious Activity
  10 months
- Increasing Risk Score
  10 months
- Internal Network Service Discovery
  7 months
- Increased Activity by New Threat Object
  7 months

Cobalt Strike, MimiKatz, and Qakbot Among the Most Reported Malware

In 2023, open-source reporting was dominated by a triad of formidable malware families: Cobalt Strike, Mimikatz, and QakBot. These families not only persisted as significant threats ,but also topped the list of the most reported malware in hundreds of open-source reports gathered from various vendors throughout the year.

Cobalt Strike, originally a legitimate penetration testing tool, was frequently exploited by attackers for its advanced network infiltration and reconnaissance capabilities.

Mimikatz, on the other hand, gained notoriety for its effectiveness in harvesting credentials from Windows systems, making it a go-to tool for threat actors seeking unauthorized access.

QakBot, a multifaceted and evolving banking trojan, continued to cause disruptions with capabilities including credential theft and network propagation.

While law enforcement action in August 2023 disrupted QakBot operations, it was not long before they resumed operations in December.

The prevalence of these three malware families in 2023 underscores their adaptability, sophistication, and the continuous challenge they pose to cybersecurity defenses worldwide.

Cobalt Strike consistently ranked as the most reported malware family in almost every month of 2023.

MimiKatz consistently ranked in the top 10 most reported malware families, making the top 10 in 9 of the 12 months of 2023.

QakBot was consistently ranked in the top 10 most reported malware families, and topped the list in two of the 12 months.

Recommendations

Perimeter (Internet Edge)

Organizations should implement a perimeter discovery and attack surface monitoring solution, like Deepwatch's Threat Signal, to identify internet-exposed systems and the threats targeting these systems. Deepwatch's Threat Signal adopts an 'outside-in' perspective, evaluating an organization's externally accessible presence from the perspective of an attacker to pinpoint risky systems and services.

Regularly scan systems for vulnerabilities and patch systems as soon as possible. Prioritization should be placed on those systems that are internet-exposed with a focus on known exploited vulnerabilities like those featured in CISA's **Known Exploited Vulnerabilities Catalog.**

Assets on the public internet expose exploitable services, such as RDP. Where these services must be exposed, appropriate compensating controls should be implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols should be disabled on internet-facing assets.

Integrating a secure email gateway as part of the organizational technology stack can significantly reduce the risk of phishing emails arriving in the end-user's inboxes.

Prevent users from launching embedded files in Microsoft OneNote files, like .hta, .bat, .com, .cmd, .exe, .js, .jse, ps1, .scr, .vbs, and .wsf, through Group Policy settings by using the "Embedded Files Blocked Extensions" template available from Microsoft **here.**

> The KEV catalog sends a clear message to all organizations to prioritize remediation efforts on the subset of vulnerabilities that are causing immediate harm based on adversary activity. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.
>
> -CISA

Recommendations

Accounts

Integrating **phishing-resistant multi-factor authentication** (MFA) as part of the organizational policy can significantly reduce the risk of a cybercriminal gaining control of valid credentials for additional tactics such as initial access, lateral movement, and collecting information. Organizations can also use phishing-resistant MFA to restrict access to cloud resources and APIs.

An enforced organization-wide policy and process that requires changing default passwords for all hardware, software, and firmware before being deployed on any network. Organizations have a system-enforced policy requiring a minimum password length of 15 or more characters for all password-protected IT assets, and all OT assets are technically possible.

No user accounts have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g. for business email, web browsing, etc.)—Disable remote PowerShell execution for non-administrative users where possible.

Recommendations

Network & Host

Determine if certain websites or attachment types (such as Telegram, Discord, .lnk, and .iso.) are necessary for business operations and block access if security analysts cannot monitor the activity well or if it poses a significant risk.

Prevent users from opening scripts, like .hta, .jse, .js, .vbs, and .wsf, through Group Policy settings and prevent the execution of script interpreters (MSHTA.exe and WSCRIPT.exe) through Group Policy or Application Control.

A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.

Employ an anti-virus or EDR solution that can automatically quarantine suspicious files.

Security applications that look for behavior used during exploitation can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring.

Recommendations

Disaster Recovery

Customers are highly encouraged to establish an incident response plan and frequently test it. These plans should include the calculation for the amount of time it would take to restore from backups and the overall cost. Customers should restore data from backups when testing their plans.

Customers with encrypted off-site backups should ensure that the digital decryption key or the applications needed to restore are not stored on a local file-sharing network and access is tightly controlled.

2024 Forecast Quick Look

Heading into 2024, the threat landscape is expected to rapidly evolve with sophisticated threats that demand proactive and dynamic responses.

Information-stealing malware will likely become more advanced, capitalizing on compromised credentials and expanding the cybercriminal toolbox beyond traditional malware.

Organizations will also witness a surge in mass vulnerability exploitation and supply chain attacks, with cybercriminals exploiting software-as-a-service vulnerabilities. They reveal the critical need for organizations tovalidate their suppliers' cybersecurity practices.

Furthermore, predictive analysis indicates a continued reliance on tactics like External Remote Services, User Execution, and Application Layer Protocol, as per the MITRE ATT&CK framework, signaling persistent and sophisticated attack vectors.

The integration of Artificial Intelligence in malware development will add a new dimension to threat capabilities, enhancing evasion techniques and adaptability.

The abuse of legitimate internet services is expected to escalate, with platforms like GitHub and Telegram being increasingly leveraged for malicious purposes.

Finally, organizations may see more malware and tool-less attacks as threat actors leverage compromised credentials to access networks and employ various techniques to avoid files. As the threat landscape evolves, these trends underscore the urgent need for robust and adaptable cybersecurity strategies in 2024.

Information Stealing Malware Will Continue to Become More Sophisticated

As cybercriminals look for new ways to access sensitive information for financial gain, information-stealing malware will continue enhancing their capabilities, increasing in sophistication in 2024. As long as organizations allow users to store credentials in their browsers and policies are not established to invalidate sessions after they have ended, cybercriminals will continue to use infostealers to compromise accounts.

In addition, as more businesses and individuals work remotely and use devices to access sensitive internet-facing systems, the attack surface increases, giving cybercriminals more attack vectors. As a result, we can expect to see a continued increase in the development and use of information-stealing malware as a means for cybercriminals to steal sensitive information and sell it on cybercriminal marketplaces.

A significant development at the end of 2023 saw various infostealers incorporate an exploit that allowed cybercriminals to restore expired Google cookies, even after users reset their passwords.

With infostealers now able to restore expired Google cookies, we expect the continuous enhancement of infostealers to incorporate additional exploitation techniques and vulnerabilities. Many are expected to become all-purpose data stealers, targeting other data types beyond passwords stored in browsers.

The rise in infostealing malware in 2023 will see an increase in stolen credentials being sold on cybercriminal marketplaces. This trend will likely result in gaps between initial infostealer infection and follow-on post-infection activity.

Mass Vulnerability Exploitation and Supply Chain Attacks Will Continue to be a Significant Threat

2023 saw cybercriminals exploiting vulnerabilities to target hundreds of organizations. Significant events included mass exploitation of vulnerabilities in Fortra GoAnywhere, Progress MOVEit Transfer, and Citrix, as well as the supply chain attacks against 3CX, JetBrains, and Okta.

As more organizations use software-as-a-service to streamline critical processes, the attack surface for cybercriminals continues to expand. As more sensitive information is stored and processed online, the incentives for attackers to find and exploit vulnerabilities in these software systems will only continue to grow. Many organizations do not validate the cybersecurity of their suppliers, making them attractive targets for cybercriminals. This highlights the need for organizations to vet the cybersecurity practices of their suppliers, before acquiring any software solution.

Over the past year, the trend of exploiting vulnerabilities in software supply chains indicates that cybercriminals will likely continue to exploit these vulnerabilities in 2024.

Cybercriminals can effortlessly identify vulnerable systems for exploitation, allowing them to quickly develop exploit code or weaponize publicly available proof-of-concept code.

Organizations are forced to rely on the security practices of their suppliers to ensure their data is safe. This is compounded by organizations' lack of knowledge of their full attack surface and the race against cybercriminals in identifying vulnerable systems and must first ensure the patches do not “break” current production systems giving the upper hand to cybercriminals.

Techniques Involving External Remote Services, User Execution, and Application Layer Protocol Will Continue to be Widely Observed

Our predictive analysis, leveraging advanced modeling techniques on historical cybersecurity data, provides a forecast for the upcoming year that is crucial for shaping cybersecurity strategies. **We focused on the three most observed MITRE ATT&CK techniques - 'External Remote Services,' 'User Execution,' and 'Application Layer Protocol.'**

The model anticipates a fluctuating yet consistently high occurrence for External Remote Services. Adversaries initially leverage external-facing remote services to access and/or persist within a network. This suggests threat actors' sustained reliance on this tactic, necessitating continued vigilance and enhanced defensive measures in network security and access control protocols. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. Often, remote service gateways manage connections and credential authentication for these services.

User Execution is forecasted to maintain a relatively stable presence. This stability implies continued reliance on users to interact with files and highlights the importance of ongoing user education and behavioral analysis as key defense strategies. Adversaries rely on user interaction for the execution of malicious code. User interaction may include installing applications, opening email attachments, or granting higher document permissions. Adversaries may embed malicious code or visual basic code into files such as Microsoft Word and Excel documents or software installers. Execution of this code requires that the user enable scripting or write access within the document. Embedded code may not always be noticeable to the user, especially in cases of trojanized software.

The Application Layer Protocol technique is expected to increase slightly in use. This uptrend underscores a growing sophistication in attack methods targeting application layers, emphasizing the need for robust application security and real-time monitoring systems. Adversaries communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally, such as those between a proxy or pivot node and other nodes, commonly used protocols are SMB, SSH, or RDP.

These forecasts underscore the importance of adaptive and proactive cybersecurity strategies. While the consistency in some techniques reflects persistent threat vectors, the variations highlight the evolving nature of cyber threats. Organizations should prioritize resource allocation towards these identified areas, ensuring their defense mechanisms are robust and agile enough to respond to these projected trends.

Prevalence of AI in Malleable Tool Performance and Defense Evasion

The rapid advancement of AI's technical skills along with its increased availability to the general public has provided an easy way to leverage its capabilities without a high level of technical proficiency. While very few real-world examples of AI being used by adversaries have been noted, given AI's ease of use and available nature, its usage in malicious operations is expected to increase in 2024. One example of how threat actors can use AI is to enumerate various obfuscation variances of the same command/objective. While specific prompts requesting obfuscation routes for a command may be denied for violating content policies, bypassing these restrictions is not difficult.

Taking one command a malware sample needs to run and using AI to create a list of various obfuscated versions as backup paired with logic error handling is a simple example of how malicious developers and threat actors could use AI to add redundancy and flexibility to malicious code with minimal time investment. While partially automated, this still involves manual/static inclusion of the generated variants of the original command. Beyond using AI to enumerate commands, the idea of connecting an AI tool to a Command and Control (C2) panel and programming prompts based on status updates from infected endpoints reporting to the C2 server is not far-fetched given current AI tools' compatibility with API's and automated input. Doing so would allow a C2 server to dynamically create alternate commands/routes that would be returned to the infected client if a specific action is detected or blocked by Endpoint Detection & Response (EDR) or Antivirus solutions.

This type of dynamic adaptation enabled by AI would not only allow individual compromised hosts to adapt to defensive measures, but it could also allow the entire fleet of compromised machines to receive AI-generated code that has adapted since the original malware deployment to evade global updates to defensive measures such as CrowdStrike and Windows Defender.

Malware polymorphism is not a new concept, and malleable profiles and modularity of components have been around for decades. Still, the presence and availability of AI presents an opportunity to integrate these features with a lower skill level and time commitment.

For defenders, malicious code with access to the command and control server may act more like a human operator with complex problem-solving skills and more persistent and diverse actions at the procedural level. This represents a significant departure from a blocked malware action as "not being a problem". Malware with AI-based augmentation is significantly less likely to try an action, be blocked, and run out of error-handling mechanisms to achieve the objective. This persistence and adaptation, typically seen more with "hands-on keyboard" activity by human operators, will become increasingly available to automated malware strains. As the chances of evading defenses increase, defenders must pay more attention to alerts in a shorter time frame.

Abuse of Legitimate Internet Services Will Continue, Likely Escalating in 2024

As we advance into 2024, the cyber threat landscape is expected to see a marked increase in the abuse of legitimate internet services (LIS) by threat actors. This trend, observed extensively in recent years, points towards a strategic shift in cybercriminal activities. The ability to leverage platforms like GitHub, Telegram, and Discord provides a veil of legitimacy, making detection and defense increasingly complex for cybersecurity professionals. These services, designed for efficiency and ease of use, inadvertently offer a fertile ground for malicious activities, blending criminal actions within the bounds of normal network traffic.

GitHub's services have been extensively exploited by cybercriminals and advanced persistent threats (APTs) for various malicious purposes, such as payload delivery, dead drop resolving, exfiltration, and full command-and-control operations.

Discord has also been significantly abused, especially for payload delivery and C2 (Command and Control) communications, as evidenced in the WhisperGate attacks against Ukraine. Its simple exfiltration capabilities make it attractive to infostealers, contributing to its high abuse rate alongside Telegram.

Slack, while not as commonly abused as Telegram or Discord, has been utilized by APT groups such as APT29 for malicious purposes, indicating a growing trend among threat actors to exploit a diverse range of messaging services for their operations.

Rise of Non-Malware-Based Cyber Attacks in 2024

The rapid advancement of AI's technical skills along with its increased availability to the general public has provided an easy way to leverage its capabilities without a high level of technical proficiency. While very few real-world examples of AI being used by adversaries have been noted, given AI's ease of use and available nature, its usage in malicious operations is expected to increase in 2024. One example of how threat actors can use AI is to enumerate various obfuscation variances of the same command/objective. While specific prompts requesting obfuscation routes for a command may be denied for violating content policies, bypassing these restrictions is not difficult.

Taking one command a malware sample needs to run and using AI to create a list of various obfuscated versions as backup paired with logic error handling is a simple example of how malicious developers and threat actors could use AI to add redundancy and flexibility to malicious code with minimal time investment. While partially automated, this still involves manual/static inclusion of the generated variants of the original command. Beyond using AI to enumerate commands, the idea of connecting an AI tool to a Command and Control (C2) panel and programming prompts based on status updates from infected endpoints reporting to the C2 server is not far-fetched given current AI tools' compatibility with API's and automated input. Doing so would allow a C2 server to dynamically create alternate commands/routes that would be returned to the infected client if a specific action is detected or blocked by Endpoint Detection & Response (EDR) or Antivirus solutions.

This type of dynamic adaptation enabled by AI would not only allow individual compromised hosts to adapt to defensive measures, but it could also allow the entire fleet of compromised machines to receive AI-generated code that has adapted since the original malware deployment to evade global updates to defensive measures such as CrowdStrike and Windows Defender.

Malware polymorphism is not a new concept, and malleable profiles and modularity of components have been around for decades. Still, the presence and availability of AI presents an opportunity to integrate these features with a lower skill level and time commitment.

For defenders, malicious code with access to the command and control server may act more like a human operator with complex problem-solving skills and more persistent and diverse actions at the procedural level. This represents a significant departure from a blocked malware action as "not being a problem". Malware with AI-based augmentation is significantly less likely to try an action, be blocked, and run out of error-handling mechanisms to achieve the objective. This persistence and adaptation, typically seen more with "hands-on keyboard" activity by human operators, will become increasingly available to automated malware strains. As the chances of evading defenses increase, defenders must pay more attention to alerts in a shorter time frame.

Deepwatch Threat Intelligence Process

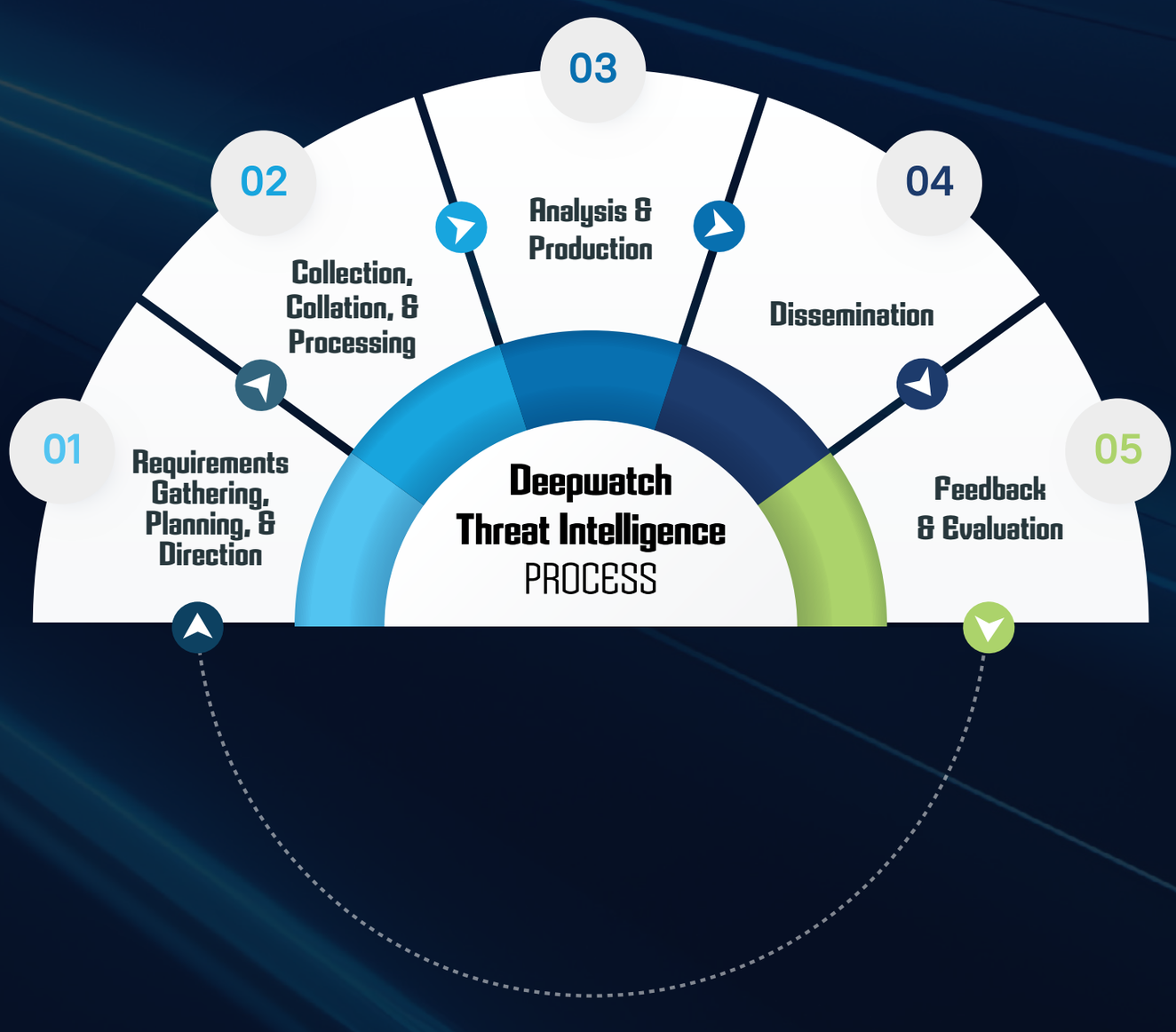
Requirements Gathering, Planning, & Direction. The ATI team mission is to provide intelligence that drives effective business decisions. We derive requirements from a combination of shifts in the cybersecurity landscape and customers' business needs.

Collection, Collation, & Processing. ATI collects data through various methods, including open-source and internal intelligence. Collected data is ingested into a centralized system for analysis where it can be collated and processed for analysis.

Analysis & Production. Threat Intelligence Analysts examine and evaluate all the information collected, add context as needed, and integrate it into a complete finished intelligence product. These products include assessments of events and estimates about the developing threat landscape.

Dissemination. Relevant intelligence is disseminated both to Deepwatch internally and to our customer base through various mechanisms: including but not limited to weekly Cyber Intelligence Briefings, alerting, and time-sensitive Advisory Reports.

Feedback & Evaluation. Feedback and evaluations is a continuous process that occurs at all stages of the intelligence lifecycle and after we have completed the analysis and disseminated the final product. This process is essential to ensure that produced intelligence effectively provides cybersecurity operational value and drives strategic business decisions.



MITRE ATT&CK Technique Stats

TECHNIQUE STATS

MITRE_TECHNIQUE_ID	DESCRIPTION	TOTAL	TACTICS
T1071	Application Layer Protocol	136039	Command and Control: TA0011
T1078	Valid Accounts	119783	
T1110	Brute Force	91382	
T1543	Create or Modify System Process	82400	
T1133	External Remote Services	82302	
T1204	User Execution	81843	
T1046	Network Service Scanning	76115	
T1595	Active Scanning	65302	
T1190	Exploit Public-Facing Application	46065	
T1562	Impair Defenses	45313	

TECHNIQUE STATS BY MONTH

MONTH	ID	DESCRIPTION	TOTAL
January	T1110	Brute Force	9901
January	T1543	Create or Modify System Process	8348
January	T1078	Valid Accounts	7922
January	T1046	Network Service Scanning	7504
January	T1204	User Execution	6880
January	T1595	Active Scanning	6806
January	T1133	External Remote Services	5752
January	T1071	Application Layer Protocol	5732
January	T1190	Exploit Public-Facing Application	4334
January	T1048	Exfiltration Over Alternative Protocol	4083

MITRE ATT&CK Technique Stats

TECHNIQUE STATS BY MONTH

MONTH	ID	DESCRIPTION	TOTAL
February	T1078	Valid Accounts	14130
February	T1071	Application Layer Protocol	13639
February	T1110	Brute Force	11631
February	T1133	External Remote Services	11325
February	T1204	User Execution	10565
February	T1543	Create or Modify System Process	9265
February	T1046	Network Service Scanning	7864
February	T1105	Ingress Tool Transfer	6069
February	T1595	Active Scanning	5606
February	T1190	Exploit Public-Facing Application	4200
March	T1133	External Remote Services	13946
March	T1595	Active Scanning	12388
March	T1543	Create or Modify System Process	10818
March	T1110	Brute Force	9743
March	T1204	User Execution	9563
March	T1071	Application Layer Protocol	8806
March	T1078	Valid Accounts	7862
March	T1046	Network Service Scanning	4396
March	T1190	Exploit Public-Facing Application	3893
March	T1003	OS Credential Dumping	3510
April	T1595	Active Scanning	9714
April	T1078	Valid Accounts	9637
April	T1046	Network Service Scanning	8926
April	T1110	Brute Force	8392

MITRE ATT&CK Technique Stats

TECHNIQUE STATS BY MONTH

MONTH	ID	DESCRIPTION	TOTAL
April	T1071	Application Layer Protocol	7969
April	T1190	Exploit Public-Facing Application	5860
April	T1204	User Execution	5674
April	T1543	Create or Modify System Process	5567
April	T1133	External Remote Services	4694
April	T1016	System Network Configuration Discovery	4260
May	T1071	Application Layer Protocol	16738
May	T1110	Brute Force	8192
May	T1078	Valid Accounts	7153
May	T1204	User Execution	6790
May	T1059	Command and Scripting Interpreter	5790
May	T1021	Remote Services	5614
May	T1543	Create or Modify System Process	5441
May	T1595	Active Scanning	5271
May	T1046	Network Service Scanning	5269
May	T1105	Ingress Tool Transfer	4823
June	T1071	Application Layer Protocol	16910
June	T1543	Create or Modify System Process	7707
June	T1110	Brute Force	7381
June	T1046	Network Service Scanning	7265
June	T1059	Command and Scripting Interpreter	6160
June	T1204	User Execution	5837
June	T1078	Valid Accounts	4654
June	T1595	Active Scanning	4385

MITRE ATT&CK Technique Stats

TECHNIQUE STATS BY MONTH

MONTH	ID	DESCRIPTION	TOTAL
June	T1133	External Remote Services	4292
June	T1190	Exploit Public-Facing Application	4167
July	T1071	Application Layer Protocol	19471
July	T1078	Valid Accounts	7475
July	T1046	Network Service Scanning	6549
July	T1110	Brute Force	6218
July	T1133	External Remote Services	5472
July	T1204	User Execution	5336
July	T1543	Create or Modify System Process	5295
July	T1087	Account Discovery	4763
July	T1190	Exploit Public-Facing Application	4710
July	T1090	Proxy	4646
August	T1078	Valid Accounts	29075
August	T1133	External Remote Services	22902
August	T1071	Application Layer Protocol	11451
August	T1543	Create or Modify System Process	7647
August	T1204	User Execution	7265
August	T1046	Network Service Scanning	7028
August	T1595	Active Scanning	6794
August	T1110	Brute Force	6618
August	T1562	Impair Defenses	4853
August	T1039	Data from Network Shared Drive	4788
September	T1071	Application Layer Protocol	17252
September	T1562	Impair Defenses	7704

MITRE ATT&CK Technique Stats

TECHNIQUE STATS BY MONTH

MONTH	ID	DESCRIPTION	TOTAL
September	T1204	User Execution	7611
September	T1078	Valid Accounts	7065
September	T1046	Network Service Scanning	6982
September	T1543	Create or Modify System Process	6959
September	T1110	Brute Force	6085
September	T1578	Modify Cloud Compute Infrastructure	6031
September	T1584	Compromise Infrastructure	5752
September	T1595	Active Scanning	4167
October	T1071	Application Layer Protocol	10161
October	T1204	User Execution	8033
October	T1078	Valid Accounts	7227
October	T1046	Network Service Scanning	6252
October	T1543	Create or Modify System Process	5848
October	T1110	Brute Force	4970
October	T1505	Server Software Component	3865
October	T1562	Impair Defenses	3656
October	T1133	External Remote Services	3512
October	T1595	Active Scanning	3136
November	T1078	Valid Accounts	10168
November	T1110	Brute Force	7305
November	T1562	Impair Defenses	6623
November	T1543	Create or Modify System Process	6321
November	T1046	Network Service Scanning	5152
November	T1204	User Execution	4811

MITRE ATT&CK Technique Stats

TECHNIQUE STATS BY MONTH

MONTH	ID	DESCRIPTION	TOTAL
November	T1071	Application Layer Protocol	4678
November	T1003	OS Credential Dumping	4666
November	T1578	Modify Cloud Compute Infrastructure	4616
November	T1584	Compromise Infrastructure	4549
December	T1078	Valid Accounts	7415
December	T1110	Brute Force	4946
December	T1098	Account Manipulation	3727
December	T1204	User Execution	3478
December	T1071	Application Layer Protocol	3232
December	T1543	Create or Modify System Process	3184
December	T1003	OS Credential Dumping	3124
December	T1222	File and Directory Permissions Modification	3025
December	T1046	Network Service Scanning	2928
December	T1546	Event Triggered Execution	2160

MITRE ATT&CK Technique Stats

TECHNIQUE BY MONTH

DESCRIPTION NAME	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.	Aug.	Sept.	Oct.	Nov.	Dec.	GRAND TOTAL
Valid Accounts	1	1	1	1	1	1	1	1	1	1	1	1	12
User Execution	1	1	1	1	1	1	1	1	1	1	1	1	12
Network Service Scanning	1	1	1	1	1	1	1	1	1	1	1	1	12
Create or Modify System Process	1	1	1	1	1	1	1	1	1	1	1	1	12
Brute Force	1	1	1	1	1	1	1	1	1	1	1	1	12
Application Layer Protocol	1	1	1	1	1	1	1	1	1	1	1	1	12
Active Scanning	1	1	1	1	1	1		1	1	1			9
External Remote Services	1	1	1	1		1	1	1		1			8
Exploit Public-Facing Application	1	1	1	1		1	1						6
Impair Defenses								1	1	1	1		4
OS Credential Dumping			1								1	1	3
Modify Cloud Compute Infrastructure									1		1		2
Ingress Tool Transfer		1			1								2
Compromise Infrastructure									1		1		2
Command and Scripting Interpreter					1	1							2
System Network Configuration Discovery				1									1
Server Software Component										1			1
Remote Services					1								1
Proxy							1						1
File and Directory Permissions Modification												1	1
Exfiltration Over Alternative Protocol	1												1
Event Triggered Execution												1	1
Data from Network Shared Drive								1					1
Account Manipulation												1	1
Account Discovery							1						1

Detection Stats

TOP 10 DETECTIONS

DETECTION ID	DETECTION NAME	TOTAL
dwa_auta_00044	External Authentication from Non-Excluded Country	42899
dwa_cora_00001	Suspicious Activity	42263
dwa_infa_00040	Missing Critical Sourcetype	40701
dwa_cora_00002	Increasing Risk Score	37995
dwa_cora_00004	Increased Activity by New Threat Object	31868
dwa_neta_00001	Internal Network Service Discovery	30087
dwa_inta_00025	Network - Emerging Threat Detected	24580
dwa_infa_00027	Significant spike or drop in log activity	22818
dwa_enda_00025	Crowdstrike Event Detected	21950
dwa_cora_00003	Multiple Tactics Observed	20321

DETECTIONS BY MONTH

DETECTION NAME	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.	Aug.	Sept.	Oct.	Nov.	Dec.	TOTAL
Suspicious Activity	1	1	1	1	1	1	1	1	1	1			10
Increasing Risk Score	1	1	1	1	1	1	1	1	1	1			10
Missing Critical Sourcetype		1	1	1	1	1	1	1		1			8
Internal Network Service Discovery	1	1						1	1	1	1	1	7
Increased Activity by New Threat Object	1	1	1	1	1	1	1						7
Network - Emerging Threat Detected				1	1	1	1	1	1				6
Crowdstrike Event Detected	1	1	1							1	1	1	6
Significant spike or drop in log activity	1		1							1	1		4
External Authentication from Non-Excluded Country	1	1	1					1					4
Threat Intel - Outbound IP Match					1	1					1		3

Detection Stats

DETECTIONS BY MONTH

DETECTION NAME	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.	Aug.	Sept.	Oct.	Nov.	Dec.	TOTAL
Web Emerging Threat Detected										1	1		2
Suspicious Process Execution On Host (Linux/Unix)						1						1	2
Successful Login From Ip Displaying Brute Force Behavior - External	1	1											2
Sentinelone Event Detected	1											1	2
Powershell With Download Cradles					1	1							2
Outbound Tor Traffic						1	1						2
Multiple Tactics Observed			1					1					2
Executable File Downloaded From Root Directory		1			1								2
Executable File Downloaded Followed By High Risk Traffic									1	1			2
Encrypted Powershell Command Detected								1			1		2
Dns - Emerging Threat Detected		1					1						2
Access To Windows Network Share From Unusual Source Ip								1				1	2
Windows C2 Multi-Stage Behavior										1			1
Webshell Execution With Command Line Keywords								1					1
Waf Multiple Drops Followed By Allowed Traffic				1									1
User Added To Privileged O365 Group												1	1
Unauthorized P2p Application	1												1
Threat Intel - Outbound Domain Match									1				1
Suspicious Port Scanning Activity				1									1
Suspicious Lsass Activity												1	1
Successful Login After Password Spray Activity											1		1
Successful Login After Password Guessing Activity												1	1
Sophos Alert Detected							1						1

Detection Stats

DETECTIONS BY MONTH

DETECTION NAME	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.	Aug.	Sept.	Oct.	Nov.	Dec.	TOTAL
SentinelOne Incomplete Quarantine Event						1							1
Potential Malicious DNS Zone Transfer				1									1
POST Exfiltration to Hardcoded IP Address									1				1
Network Sniffing Tool					1								1
Multiple Suspicious Powershell Executions									1				1
MS 365 Defender Incident												1	1
Missing Critical Asset										1			1
Local Host Enumeration							1						1
Lateral Movement over SMB to Admin Shares					1								1
Intsights - Inbound Domain Match			1										1
Graph Security Alert									1				1
Geographically Improbable Access				1									1
Crowdstrike Event Detected Clone			1										1
Critical IDS Alert Detected and not Blocked - Clone							1						1
Critical IDS Alert Detected and not Blocked				1									1
AWS Configuration Change Clone									1				1
AWS Configuration Change											1		1
Application Shimming												1	1
Anonymous NTLM Connection											1		1
Anomalous PowerShell Script with Risky COM Object											1		1
GRAND TOTAL	10	10	10	10	10	10	10	10	10	10	10	10	120

Detection Stats

TOP 10 DETECTIONS BY MONTH

MONTH	DETECTION ID	DETECTION NAME	TOTAL
January	dwa_auta_00044	External Authentication from Non-Excluded Country	4175
January	dwa_cora_00002	Increasing Risk Score	3549
January	dwa_cora_00001	Suspicious Activity	3470
January	dwa_neta_00001	Internal Network Service Discovery	2553
January	dwa_cora_00004	Increased Activity by New Threat Object	2447
January	dwa_auta_00043	Successful Login from IP displaying Brute Force behavior - External	2073
January	dwa_enda_00075	SentinelOne Event Detected	1844
January	dwa_infa_00027	Significant spike or drop in log activity	1799
January	dwa_neta_00017	Unauthorized P2P Application	1660
January	dwa_enda_00025	Crowdstrike Event Detected	1626
February	dwa_auta_00044	External Authentication from Non-Excluded Country	9373
February	dwa_inta_00026	DNS - Emerging Threat Detected	7588
February	dwa_cora_00001	Suspicious Activity	4467
February	dwa_neta_00001	Internal Network Service Discovery	4019
February	dwa_cora_00004	Increased Activity by New Threat Object	4000
February	dwa_cora_00002	Increasing Risk Score	3813
February	dwa_auta_00043	Successful Login from IP displaying Brute Force behavior - External	3797
February	dwa_enda_00025	Crowdstrike Event Detected	2386
February	dwa_weba_00009	Executable File Downloaded from root Directory	2251
February	dwa_infa_00040	Missing Critical Sourcetype	2019
March	dwa_inta_00034	Intsights - Inbound Domain Match	7642
March	dwa_cora_00004	Increased Activity by New Threat Object	4382
March	dwa_cora_00001	Suspicious Activity	4138
March	dwa_infa_00040	Missing Critical Sourcetype	3333

Detection Stats

TOP 10 DETECTIONS BY MONTH

MONTH	DETECTION ID	DETECTION NAME	TOTAL
March	dwa_enda_00025	Crowdstrike Event Detected Clone	3036
March	dwa_auta_00044	External Authentication from Non-Excluded Country	2949
March	dwa_enda_00025	Crowdstrike Event Detected	2886
March	dwa_cora_00002	Increasing Risk Score	2834
March	dwa_infa_00027	Significant spike or drop in log activity	2399
March	dwa_cora_00003	Multiple Tactics Observed	2236
April	dwa_cora_00001	Suspicious Activity	4936
April	dwa_neta_00008	Suspicious Port Scanning Activity	4313
April	dwa_infa_00040	Missing Critical Sourcetype	4191
April	dwa_dnsa_00011	Potential Malicious DNS Zone Transfer	3947
April	dwa_cora_00004	Increased Activity by New Threat Object	3831
April	dwl_auta_00044	Geographically Improbable Access	3706
April	dwa_idsa_00009	Critical IDS Alert Detected and not Blocked	3365
April	dwa_cora_00002	Increasing Risk Score	3094
April	dwl_idsa_00036	WAF Multiple Drops Followed by Allowed Traffic	2790
April	dwa_inta_00025	Network - Emerging Threat Detected	2483
May	dwa_infa_00040	Missing Critical Sourcetype	6787
May	dwa_enda_00027	Powershell with Download Cradles	5030
May	dwa_inta_00025	Network - Emerging Threat Detected	4597
May	dwa_cora_00004	Increased Activity by New Threat Object	4576
May	dwa_cora_00002	Increasing Risk Score	4472
May	dwa_cora_00001	Suspicious Activity	4374
May	dwa_inta_00044	Threat Intel - Outbound IP Match	3361
May	dwa_enda_00052	Network Sniffing Tool	3279

Detection Stats

TOP 10 DETECTIONS BY MONTH

MONTH	DETECTION ID	DETECTION NAME	TOTAL
May	dwa_enda_00035	Lateral Movement over SMB to Admin Shares	3128
May	dwa_weba_00009	Executable File Downloaded from root Directory	2646
June	dwa_infa_00040	Missing Critical Sourcetype	8099
June	dwa_inta_00044	Threat Intel - Outbound IP Match	6370
June	dwa_enda_00027	Powershell with Download Cradles	5985
June	dwa_cora_00001	Suspicious Activity	4759
June	dwa_cora_00004	Increased Activity by New Threat Object	4413
June	dwa_cora_00002	Increasing Risk Score	4402
June	dwa_inta_00025	Network - Emerging Threat Detected	3966
June	dwl_enda_00077	SentinelOne Incomplete Quarantine Event	2906
June	dwa_enda_00080	Suspicious Process Execution on Host (Linux/Unix)	2773
June	dwa_neta_00011	Outbound TOR Traffic	2751
July	dwa_idsa_00009	Critical IDS Alert Detected and not Blocked - Clone	10378
July	dwa_infa_00040	Missing Critical Sourcetype	7253
July	dwa_inta_00026	DNS - Emerging Threat Detected	4908
July	dwa_cora_00001	Suspicious Activity	4427
July	dwa_enda_00011	Local Host Enumeration	3965
July	dwa_cora_00002	Increasing Risk Score	3750
July	dwa_inta_00025	Network - Emerging Threat Detected	3675
July	dwa_neta_00011	Outbound TOR Traffic	3222
July	dwa_cora_00004	Increased Activity by New Threat Object	2977
July	dwl_mala_00050	Sophos Alert Detected	2849
August	dwa_auta_00044	External Authentication from Non-Excluded Country	20627
August	dwl_enda_00073	Encrypted powershell command detected	7869

Detection Stats

TOP 10 DETECTIONS BY MONTH

MONTH	DETECTION ID	DETECTION NAME	TOTAL
August	dwa_auda_00077	Access to Windows Network Share from Unusual Source IP	5436
August	dwa_cora_00001	Suspicious Activity	5031
August	dwa_cora_00002	Increasing Risk Score	3810
August	dwa_inta_00025	Network - Emerging Threat Detected	3323
August	dwa_cora_00003	Multiple Tactics Observed	2939
August	dwa_infa_00040	Missing Critical Sourcetype	2927
August	dwa_enda_00034	Webshell Execution with Command Line Keywords	2536
August	dwa_neta_00001	Internal Network Service Discovery	2232
September	dwa_auda_00052	AWS Configuration Change Clone	5038
September	dwa_inta_00046	Threat Intel - Outbound Domain Match	4995
September	dwa_cora_00001	Suspicious Activity	3645
September	dwa_cora_00002	Increasing Risk Score	3474
September	dwl_idsa_00015	Graph Security Alert	3263
September	dwa_neta_00001	Internal Network Service Discovery	2868
September	dwa_weba_00011	POST Exfiltration to Hardcoded IP Address	2466
September	dwa_weba_00022	Executable File Downloaded Followed by High Risk Traffic	2139
September	dwa_inta_00025	Network - Emerging Threat Detected	2101
September	dwl_auda_10000	Multiple Suspicious Powershell Executions	2019
October	dwa_cora_00002	Increasing Risk Score	3848
October	dwa_weba_00022	Executable File Downloaded Followed by High Risk Traffic	2646
October	dwa_neta_00001	Internal Network Service Discovery	2152
October	dwa_cora_00001	Suspicious Activity	2150
October	dwa_inta_00043	Web Emerging Threat Detected	2073
October	dwa_enda_00086	Windows C2 Multi-Stage Behavior	1925

Detection Stats

TOP 10 DETECTIONS BY MONTH

MONTH	DETECTION ID	DETECTION NAME	TOTAL
October	dwa_infa_00027	Significant spike or drop in log activity	1855
October	dwa_infa_00040	Missing Critical Sourcetype	1687
October	dwa_enda_00025	Crowdstrike Event Detected	1580
October	dwa_infa_00041	Missing Critical Asset	1441
November	dwa_auta_00064	Successful Login after Password Spray Activity	4639
November	dwa_auda_00052	AWS Configuration Change	4519
November	dwa_neta_00001	Internal Network Service Discovery	3823
November	dwa_inta_00043	Web Emerging Threat Detected	3093
November	dwa_enda_00025	Crowdstrike Event Detected	2521
November	dwa_enda_00095	Anomalous PowerShell Script with Risky COM Object	2236
November	dwa_infa_00027	Significant spike or drop in log activity	1887
November	dwl_enda_00073	Encrypted powershell command detected	1644
November	dwa_inta_00044	Threat Intel - Outbound IP Match	1575
November	dwa_auta_00056	Anonymous NTLM Connection	1562
December	dwa_enda_00080	Suspicious Process Execution on Host (Linux/Unix)	4247
December	dwa_enda_00075	SentinelOne Event Detected	2793
December	dwa_enda_00088	Suspicious LSASS Activity	2189
December	dwa_neta_00001	Internal Network Service Discovery	1849
December	dwa_auda_00077	Access to Windows Network Share from Unusual Source IP	1835
December	dwa_auta_00020	Successful Login after Password Guessing Activity	1663
December	dwa_auda_00035	User Added to Privileged O365 Group	1530
December	dwa_enda_00063	Application Shimming	1405
December	dwa_enda_00025	Crowdstrike Event Detected	1387
December	dwa_enda_00105	MS 365 Defender Incident	1145

Malware and Hacking Tool Stats

ALL MALWARE FAMILIES OBSERVED IN 2023 THROUGH OSINT REPORTING

Agent Racoon	CLOUDBURST	GoTitan	Matanbuchus
Agent Tesla	Cobalt Strike	Gozi	MATIEX
AHK Bot	CollectionRAT	GraceWire	Maui
Akira ransomware	Creal	GraphicalProton	MBR Killer
ALPHV ransomware	CrossLock ransomware	GuLoader	Meduza
Amadey bot	Cylance ransomware	H0lyGh0st	Merdoor
AppleSeed	DarkBit ransomware	Havoc	Metasploit
AresLoader	Darkcloud Stealer	HelloKitty ransomware	Meterpreter
AsyncRAT	DarkGate	HemiGate	Millenium RAT
AuKill	DarkMe	HiatusRAT	Mimikatz
Ave Maria	DCRAT	HOOKSHOT	MINODO
AvosLocker ransomware	Ddostf	HrServ web shell	Mirai
BabLock ransomware	DEPTHCHARGE	IcedID	Money Message ransomware
BabyShark	Diceloader	IconDown	More_Eggs
Bandit Stealer	Emotet	ICONIC Stealer	MortalKombat ransomware
Batloader	Evilginx2	IFSB	MuddyC2Go
BellaCiao	EvilProxy	IZ1H9	MyDoom
BendyBear	FakeDead	Jaguar Tooth	NetSupport RAT
BianLian ransomware	Flagpro	JSSLoader	NetWire RAT
Bifrose	FlawedGrace	KEYPLUG	NineRAT
Bitrat	FONELAUNCH	Kinsing	Ninja
BlackBasta ransomware	ForestTiger	Knight ransomware	Nitrogen
BlackByte ransomware	FORMBOOK	LambLoad	Noberus ransomware
BlackDog 2023 ransomware	FOXGLOVE	Laplas Clipper	Nokoyawa ransomware
Brute Ratel	FOXTROT	LIDSHOT	Nova
BTSDoor	FrontShell	LockBit ransomware	Ntospy
Bumblebee	FULLHOUSE.DOORED	LOKIBOT	OriginBotnet
BunnyLoader	Gh0st RAT	Lorenz	Persian loader
CatB ransomware	GhostCringe	LuaDream	Persian RAT
Cerber ransomware	GlobeImposter ransomware	LummaC2	PhonyC2
Chae$	GootBot	M2RAT	PikaBot
China Chopper	GootLoader	MalasLocker ransomware	PLANKWALK
CL0P ransomware	Gopuram	Mallox ransomware	PLEAD

Malware and Hacking Tool Stats

ALL MALWARE FAMILIES OBSERVED IN 2023 THROUGH OSINT REPORTING

PlugX	Rhysida ransomware	SpiderSpring	Truebot
PrCtrl Rat	RomCom 3.0	SpiderStack	TZW ransomware
PupyRAT	ROOTSAW	SprySOCKS	Ursnif
Qakbot	Rorschach ransomware	Stormkitty	VectorStealer
qBit stealer	Royal ransomware	STRATOFEAR	Vice Society ransomware
Quantum ransomware	Samurai	StripedFly	VIDAR stealer
QuasarRAT	Scarab ransomware	STRRAT	W3LL
QuiteRAT	Screenshotter	SugarGh0st RAT	WasabiSeed
Raccoon stealer	SectopRAT	SystemBC	WaterBear
Raspberry Robin	SIDESHOW	TIEDYE	WhisperGate
RDStealer	SKIPJACK	Titan Stealer	WhiteSnake Stealer
Read The Manual Locker	Skuld	TOITOIN	WSO-NG web shell
ReconShark	Sliver	TOUCHKEY	XMRig
RedLine Clipper	SMOKELOADER	TOUCHMOVE	XWorm
RedLine Stealer	Snake	TOUCHSHIFT	Zapoa
ReGeorg	Snatch ransomware	TOUCHSHOT	Zeon ransomware
Remcos	Socks5Systemz	Trap Stealer	Zingdoor
ReShell	Sordeal	TrickGate	ZXShell
Rhadamanthys Stealer	SpiderPig	TrillClient	

Top 10 Malware Families Observed In 2023 Through OSINT Reporting

MALWARE FAMILY	
Cobalt Strike	LockBit ransomware
Mimikatz	ALPHV ransomware
Qakbot	AsyncRAT
RedLine stealer	Mirai
IcedID	Emotet

Malware and Hacking Tool Stats

TOP 10 MALWARE FAMILIES OBSERVED IN JANUARY 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Cobalt Strike
2. IceID
3. Gootloader
4. Ursnif
5. Qakbot
6. Meterpreter
7. Vidar
8. Mimikatz
9. Rhadamanthys Stealer
10. XMRig coinminer

TOP 10 MALWARE FAMILIES OBSERVED IN FEBRUARY 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Qakbot
2. Cobalt Strike
3. AsyncRAT
4. Quasar RAT
5. RedLine Stealer
6. IcedID
7. XMRig coinminer
8. Xworm
9. NetWire RAT
10. Gootloader

TOP 10 MALWARE FAMILIES OBSERVED IN MARCH 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Qakbot
2. AsyncRAT
3. PlugX
4. BlackLotus
5. RedLine Stealer
6. Mimikatz
7. Ave Maria
8. Emotet
9. MyDoom
10. LockBit ransomware

TOP 10 MALWARE FAMILIES OBSERVED IN APRIL 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Cobalt Strike
2. ALPHV ransomware
3. Qakbot
4. LockBit ransomware
5. Emotet
6. Mirai
7. Mimikatz
8. Maui
9. IcedID
10. XMRig coinminer

Malware and Hacking Tool Stats

TOP 10 MALWARE FAMILIES OBSERVED IN MAY 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Cobalt Strike
2. LokiBot
3. NetWire RAT
4. BlackByte ransomware
5. Rhysida ransomware
6. MalasLocker ransomware
7. 8Base ransomware
8. Babuk ransomware
9. LockBit ransomware
10. Diceloader

TOP 10 MALWARE FAMILIES OBSERVED IN JUNE 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Cobalt Strike
2. Mirai
3. Mimikatz
4. Qakbot
5. TrueBot
6. RedLine Stealer
7. ReGeorg
8. WhisperGate
9. ReconShark
10. Meterpreter

TOP 10 MALWARE FAMILIES OBSERVED IN JULY 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Cobalt Strike
2. ALPHV ransomware
3. Metasploit
4. Mimikatz
5. LockBit ransomware
6. GuLoader
7. Emotet
8. Meterpreter
9. IcedID
10. Bumblebee

TOP 10 MALWARE FAMILIES OBSERVED IN AUGUST 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Cobalt Strike
2. LummaC2
3. Nitrogen
4. AsyncRAT
5. Metasploit
6. LockBit ransomware
7. CL0P ransomware
8. BlackByte ransomware
9. BianLian ransomware
10. Qakbot

Malware and Hacking Tool Stats

TOP 10 MALWARE FAMILIES OBSERVED IN SEPTEMBER 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Cobalt Strike
2. RedLine Stealer
3. Metasploit
4. Mimikatz
5. Nokoyawa ransomware
6. Akira ransomware
7. LummaC2
8. Whirlpool
9. IcedID
10. SKIPJACK

TOP 10 MALWARE FAMILIES OBSERVED IN OCTOBER 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Cobalt Strike
2. Mimikatz
3. LummaC2
4. DarkGate
5. IcedID
6. AvosLocker ransomware
7. ALPHV ransomware
8. RedLine Stealer
9. Rhysida ransomware
10. Qakbot

TOP 10 MALWARE FAMILIES OBSERVED IN NOVEMEBER 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Cobalt Strike
2. AsyncRAT
3. ALPHV ransomware
4. Rhysida ransomware
5. Mimikatz
6. Agent Tesla
7. Remcos
8. SystemBC
9. DarkGate
10. RedLine Stealer

TOP 10 MALWARE FAMILIES OBSERVED IN DECEMBER 2023 THROUGH OSINT REPORTING

MALWARE FAMILY
1. Cobalt Strike
2. Mimikatz
3. LockBit ransomware
4. Qakbot
5. DarkGate
6. AsyncRAT
7. Babuk ransomware
8. LokiBot
9. Nokoyawa ransomware
10. AppleSeed

Threat Response Metrics

TOP ENGAGEMENT TYPE

ENGAGEMENT TYPE	NUMBER	PERCENTAGE
Suspicious Activity	12	27%
Account Compromise	11	25%
Ransomware Incident	7	16%
Malware Infection	6	13%
Vulnerability Exploitation	4	9%
Phishing	2	4%
Supply Chain	1	2%
Insider Threat	1	2%

ENGAGEMENTS BY INDUSTRY

INDUSTRY	TOTAL	PERCENTAGE
Finance and Insurance	14	31%
Manufacturing	10	22%
Health Care and Social Assistance	8	18%
Professional, Scientific, and Technical Services	4	9%
Arts, Entertainment, and Recreation	2	4%
Utilities	1	2%
Wholesale Trade	1	2%
Transportation and Warehousing	1	2%
Information	1	2%
Educational Services	1	2%
Accommodation and Food Services	1	2%
Other Services	1	2%

Threat Response Metrics

TOP ENGAGEMENT TYPE

Suspicious Activity by Industry	NUMBER
Manufacturing	3
Health Care and Social Assistance	2
Finance and Insurance	2
Utilities	1
Professional, Scientific, and Technical Services	1
Educational Services	1
Arts, Entertainment, and Recreation	1
Accommodation and Food Services	1

Account Compromise by Industry	NUMBER
Finance and Insurance	4
Professional, Scientific, and Technical Services	2
Manufacturing	2
Health Care and Social Assistance	2
Information	1

Ransomware Incident by Industry	NUMBER
Health Care and Social Assistance	4
Transportation and Warehousing	1
Manufacturing	1
Arts, Entertainment, and Recreation	1

Malware Infection by Industry	NUMBER
Manufacturing	3
Finance and Insurance	2
Wholesale Trade	1

Vulnerability Exploitation by Industry	NUMBER
Finance and Insurance	3
Professional, Scientific, and Technical Services	1

ENGAGEMENTS BY MONTH

MONTH	NUMBER	PERCENTAGE
November	11	24%
February	6	13%
March	6	13%
January	5	11%
October	5	11%
April	3	7%
June	3	7%
July	3	7%
May	2	4%
August	1	2%
September	0	0%
December	0	0%

deepwatch™

Deepwatch® is the leading managed security platform for the cyber resilient enterprise.

The Deepwatch Managed Security Platform and security experts provide enterprises with 24x7x365 cyber resilience, rapid detections, high fidelity alerts, reduced false positives, and automated actions. We operate as an extension of cybersecurity teams by delivering unrivaled security expertise, unparalleled visibility across your attack surface, precision response to threats, and the best return on your security investments. The Deepwatch Managed Security Platform is trusted by many of the world's leading brands to improve their security posture, cyber resilience, and peace of mind.

Deepwatch

Learn more: **www.deepwatch.com**

Follow us:

Blog | **LinkedIn** | **Facebook**

Ready to bolster your defenses?

Speak with a **Deepwatch Security Expert**