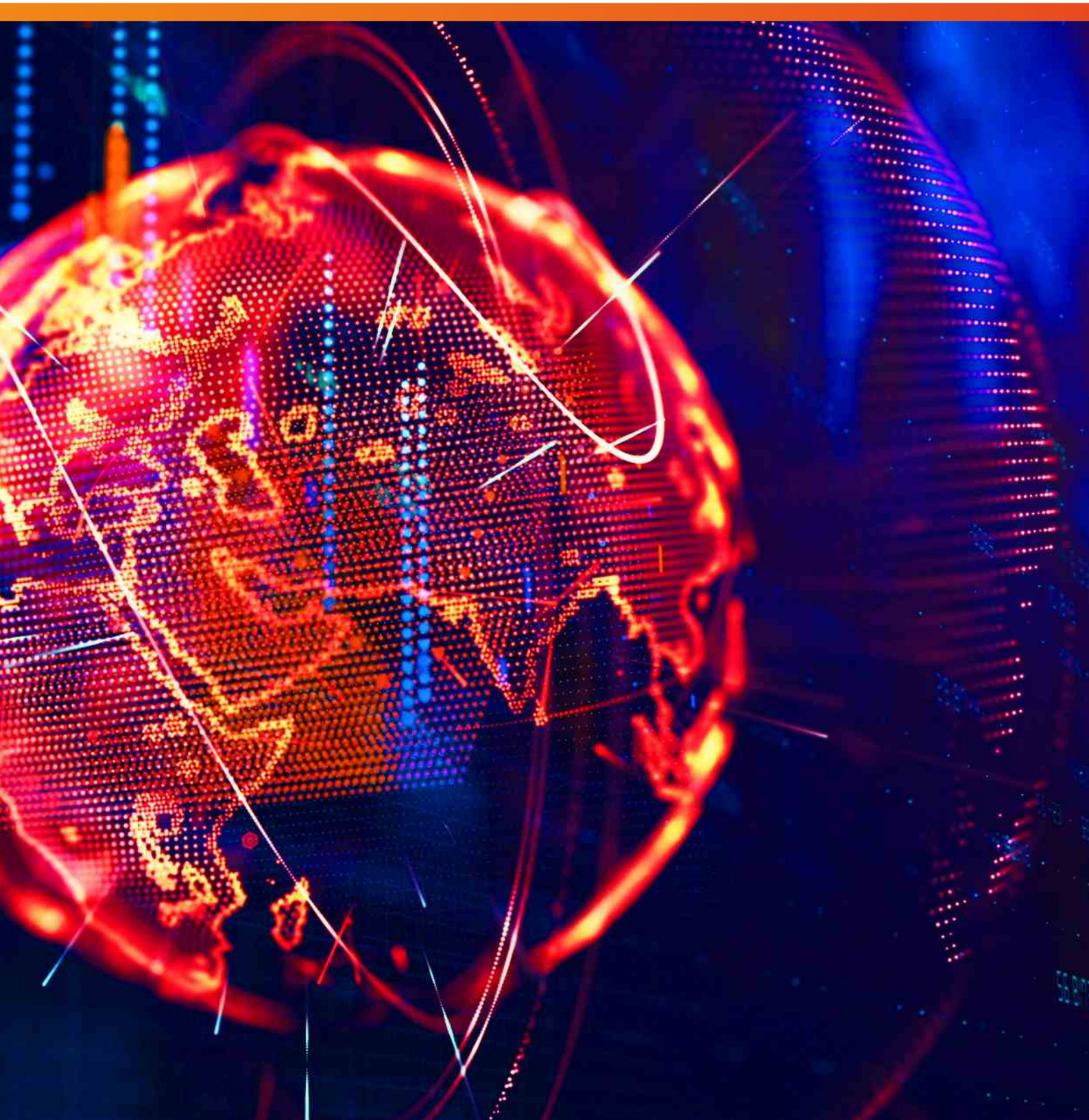
DARKTRACE

ANALYSIS OF THE SECOND HALF OF 2023

End of Year Threat Report



CONTENT

Foreword

In this, our first End of Year Threat Report, we build on the work of our previous First 6: Half-Year Threat Report, sharing the insights we've garnered throughout the latter half of 2023. A combination of Darktrace's anomaly-driven AI and deeper contextual analysis provides us fresh insights and a unique perspective on the threat landscape.

We have observed not only the continuing development and evolution of identified threats in the malware and ransomware spaces, but also changes brought about by innovations in the cyber security landscape and broader technological ecosystem, such as the boom in Generative AI. Amid these challenges, the breadth, scope, and complexity of threats to organizations have grown significantly, reinforcing the importance of employing behavioral analysis, anomaly detection, and AI for cyber security.

As the core focus of our detection methods lies in understanding the patterns of normality for organizations, our threat insights pattern the progressive changes in tactics, techniques, and procedures (TTPs), rather than the more traditional focus on specific threat actors' modus operandi. You will find our End of Year report differs from other actor-focused intelligence, as we chronicle threat characteristics that we believe are most relevant to organizations and defenders, rather than identifying and studying the behaviors of attackers.

My hope is that you find the insights reached by our AI and analysts to be practical, interesting, and relevant for security professionals. Darktrace's AI technology not only keeps ahead of the ever-changing threat landscape but also grants our analysts a unique perspective in cyber security – one we hope to share with you in this, and our future threat reports to come.

If you are interested in more threat finds from Darktrace, understanding our exceptional AI at a more granular level, or simply learning more about our organization, I encourage you to explore the resources on our website, from the analytical technical blogs on Inside the SOC, which explore individual and campaign-focused case studies, to the product-oriented materials on our site's central blog. As these Threat Reports are an evolving and novel product for us, we'd be grateful for any feedback you wish to provide. To do so, please reach out to us at threatintelligence@darktrace.com.

Hanah Darley
Director of Threat Research

Threat Research

Darktrace's Threat Research team conducts fleet research to identify which threats are affecting customers, identify key indicators of compromise (IoC) within those threats and observed impacts in customer environments, and contextualize them with additional information to provide customers with relevant Threat Intelligence. This cross-fleet research is based on the anomaly detection of Darktrace DETECT™ and revolves around analysis and contextualization of detection information performed by the Threat Research team. The threats were promptly brought to the attention of the relevant customer security teams and, in cases when Darktrace RESPOND™ was enabled, they were swiftly mitigated, preventing them from escalating.

Darktrace analysis assessed a broad variety of threats during the second half of 2023. Many of these threats were identified as campaign-like activity targeting multiple customers. Although some of these threats were identified as emerging or novel exploits, the majority were pre-existing, identified tooling. All the insights provided by Darktrace analysis are centered on the detections and specific data made available through our AI applications and anomaly investigations.

In this second half of 2023, the most observed threat type to affect Darktrace customers was Malware-as-a-Service. Both Malware-as-a-Service (MaaS) and Ransomware-as-a-Service (RaaS) represent the majority of malicious tools across the cyber threat landscape and are the most consistently identified threat affecting Darktrace customers.

Darktrace assesses MaaS and RaaS as the most probable threats to continue affecting the majority of organizations throughout 2024. With the repeated subscription-based income and demand market, Darktrace expects the MaaS and RaaS ecosystems to sustain growth in 2024, keeping MaaS and RaaS as the most relevant threats for most organizations.

MaaS and RaaS tools have a variety of capabilities, with many including tailorable or bespoke elements alterable campaign to campaign. In the first half of 2023, Darktrace assessed with moderate to high confidence that tailorable, combined threats, specifically within the MaaS and RaaS ecosystems, would continue to dominate the threat landscape. This trend focused on the interoperability of existing tools, use of combined code, and multi-functional malware.

Throughout the latter of 2023, Darktrace's observations confirmed this trend, highlighting the cross-functional adaptation of many malware strains, such as remote access trojans (RATs) and information-stealing malware, along with existing tools like Cobalt Strike. Darktrace assesses this multi-functional malware evolution is likely to continue into 2024. The use of open-source repositories, leaked code, and multi-facetted tooling is both efficient for malware developers and can increase the difficulty of detection by combining kill chain elements and utilizing overlapping compromised infrastructure.

Malware-as-a-Service infections are the most observed threats affecting Darktrace customers, consistent with their increasing prominence within the cyber threat landscape.

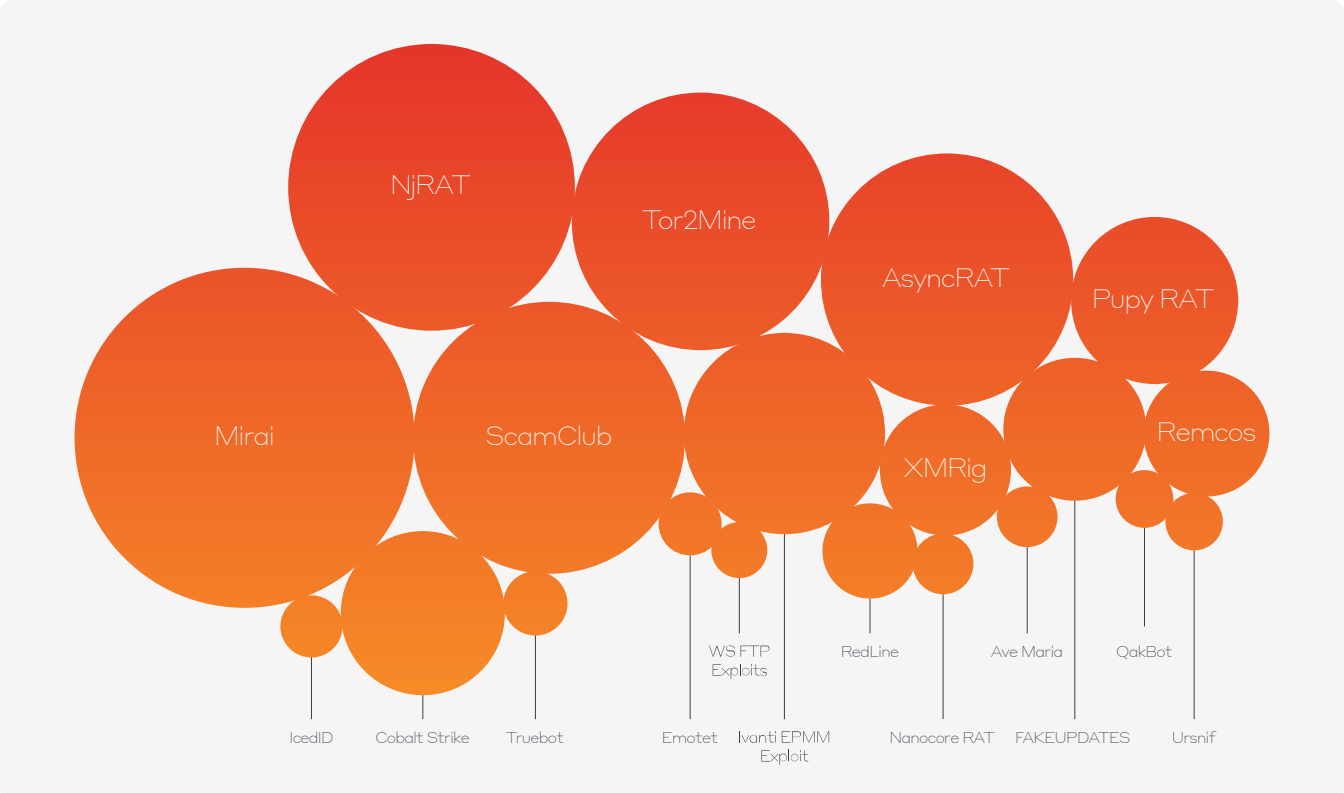
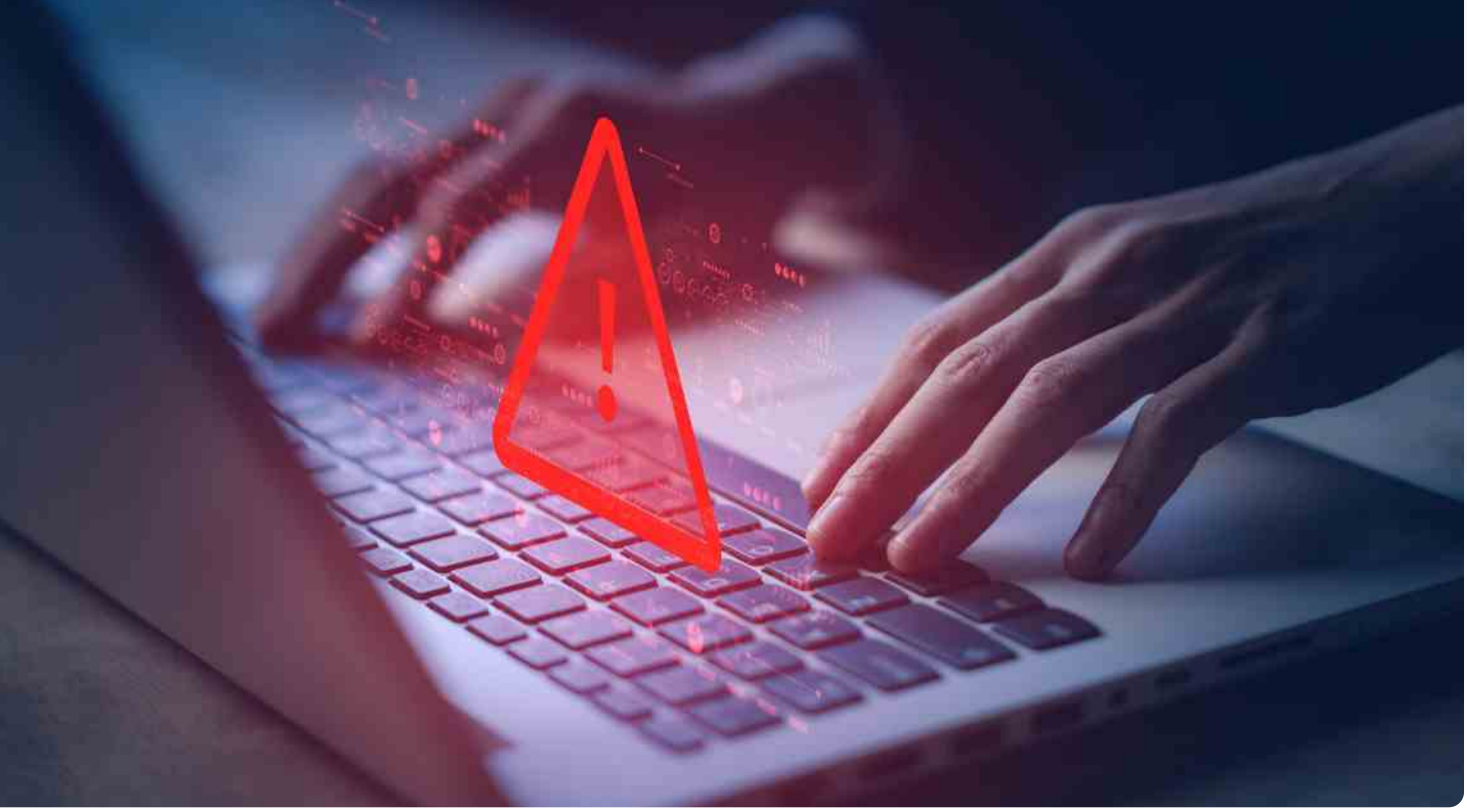


Figure 1: The diagram above represents Darktrace detections containing indicators of compromise that have been associated with particular MaaS and RaaS threats. The size of the bubble displayed relates to the frequency of detections observed across the Darktrace fleet.



The Darktrace Threat Research team performed further investigations into many of the threats that affected the customer base.

Loader malware was the most observed threat category within the MaaS and RaaS offerings Darktrace analyzed in the latter half of 2023, accounting for 77% of all investigated threats.

Cryptominers also featured prominently, representing 52%, followed by botnets (39%), information-stealing malware (36%), and proxy botnets (15%).

Note: The percentages above represent more than 100%, as customers are categorized into more than one threat type based on infections within each category.

Darktrace considers loader malware likely to be a key, prominent threat within the wider landscape in 2024. Initial access malware such as loaders and information stealers will probably remain some of the most relevant threats to most organizations, especially when noted in the context that many are interoperable, tailorable MaaS tools.

One of the components which makes these malicious tools so dangerous to organizations is their ability to harvest data and credentials without exfiltrating files. This combined with the rising value of data in the modern cyber threat marketplace make initial access MaaS tools a significant concern for security teams.

Darktrace often observes these MaaS initial access malware offerings harvesting data which could then be then sold and loading or enabling subsequent infections by second and third-stage payloads, resulting in more damaging malware attacks and even ransomware.

Signposts: Key signals to indicate multi-functional MaaS threats are increasingly evolving:

- Reverse engineering and detection analysis reveal malware strains are progressively developed with a minimum of two functions and are interoperable with a greater number of existing tools
- IoCs are routinely interchanged and shared between malware strains as compromised infrastructure is used by multiple threat actors through access brokers or the "as-a-Service" market

Signposts: Key signals to indicate loader malware remains a prominent threat:

- Detections continue to highlight existing or novel strains of loader malware affecting a large number of organizations
- Loader malware continues to precede additional malware or ransomware infections, where organizations are affected by multi-phase compromises

Interesting Threat Finds

ViperSoftX Information-Stealing Malware

ViperSoftX is a key example of the prevalence of initial access malware within the threat landscape. ViperSoftX malware is an information stealer and RAT malware known to gather privileged information such as cryptocurrency wallet addresses, and password information stored in browsers or password managers. It is commonly distributed via the download of cracked software from suspicious domains, torrent downloads, and key generators from third-party sites.

ViperSoftX was first observed in the wild in 2020 but more recently, new strains were identified in 2022 and 2023 utilizing more sophisticated detection evasion techniques. This included the use of more advanced encryption methods alongside monthly changes to command-and-control servers (C2).

The updates also featured the use of dynamic-link library (DLL) sideloading for execution techniques, and subsequently installing a malicious browser extension upon infection which works as an independent info-stealer named VenomSoftX. VenomSoftX, which is typically disguised as legitimate browser extensions, is then able to collect sensitive data from password managers and cryptowallets. Using this information, VenomSoftX is able to redirect cryptocurrency transactions by intercepting and manipulating API requests between the sender and the intended recipient.

Darktrace detected activity related to the VipersoftX information stealer on the networks of more than 100 customers across its fleet throughout 2023.

ViperSoftX activity detected across the Darktrace fleet included downloads from connections relating to multimedia sites, cracked software sites, and torrent endpoints. These connections likely represented the sources of the initial infections. Subsequently, ViperSoftX begins to run on the affected device, gather configuration information, and perform HTTP GET and POST requests to begin C2 communication to ViperSoftX-associated endpoints, such as to the hostname 'apibilng[.]com' observed in many cases.

Once C2 communication was established, devices were detected retrieving a secondary PowerShell executable. This was observed in many cases when HTTP GET requests were made to algorithmically generated domains (DGA) associated to ViperSoftX endpoints.

New and unusual PowerShell user agents were observed, such as 'Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.2364'. During these connections, there were additional commonalities observed in the URI's. The format for URIs during these connections included the following: /api, /api/, v1/, /v2/, or /v3/. Evidence from open-source intelligence (OSINT) and other Darktrace investigations revealed these URIs were linked to ViperSoftX C2 communication.

Prior to loading the aforementioned secondary PowerShell executable, a digital snapshot of the affected device is taken. This includes information such as computer name, username, operating system, and whether there is a security tool on the device. This leads to a PowerShell file being decrypted and executed. Following HTTP GET requests, various devices investigated also performed HTTP POST requests and beaconing to ViperSoftX endpoints such as 'apibilng[.]com', with varying globally unique identifiers (GUID) found in the URIs.

This activity demonstrated exfiltration of the information previously gathered throughout the attack phases.

Darktrace DETECT recognized the subtle changes in network activity that surrounded these emerging information stealer infections and brought them to the attention of customer security teams, while Darktrace RESPOND was able to quickly intervene and shut down malicious downloads and data exfiltration attempts, minimizing disruption to the business and preventing potentially significant financial losses.

Despite many information stealing malware strains being overlooked as less impactful threats, adaptable initial access malware like ViperSoftX underscores the significant impact and potential damage to organizations by threats which do not require file encryption or advanced exfiltration to steal sensitive data. The ever-increasing value of data and the potential for second and third-stage compromises which often follow the initial reconnaissance of malware highlights the significance of these malware strains within the wider cyber threat ecosystem.

The continued evolution of initial access malware strains like ViperSoftX into multi-functional malicious tools makes adopting anomaly detection critical to staying ahead of constantly advancing threats.

You can find the full technical blog on this threat find here: https://darktrace.com/blog/enemies-on-our-teams-darktrace-stops-darkgate-malware-through-microsoft-teams

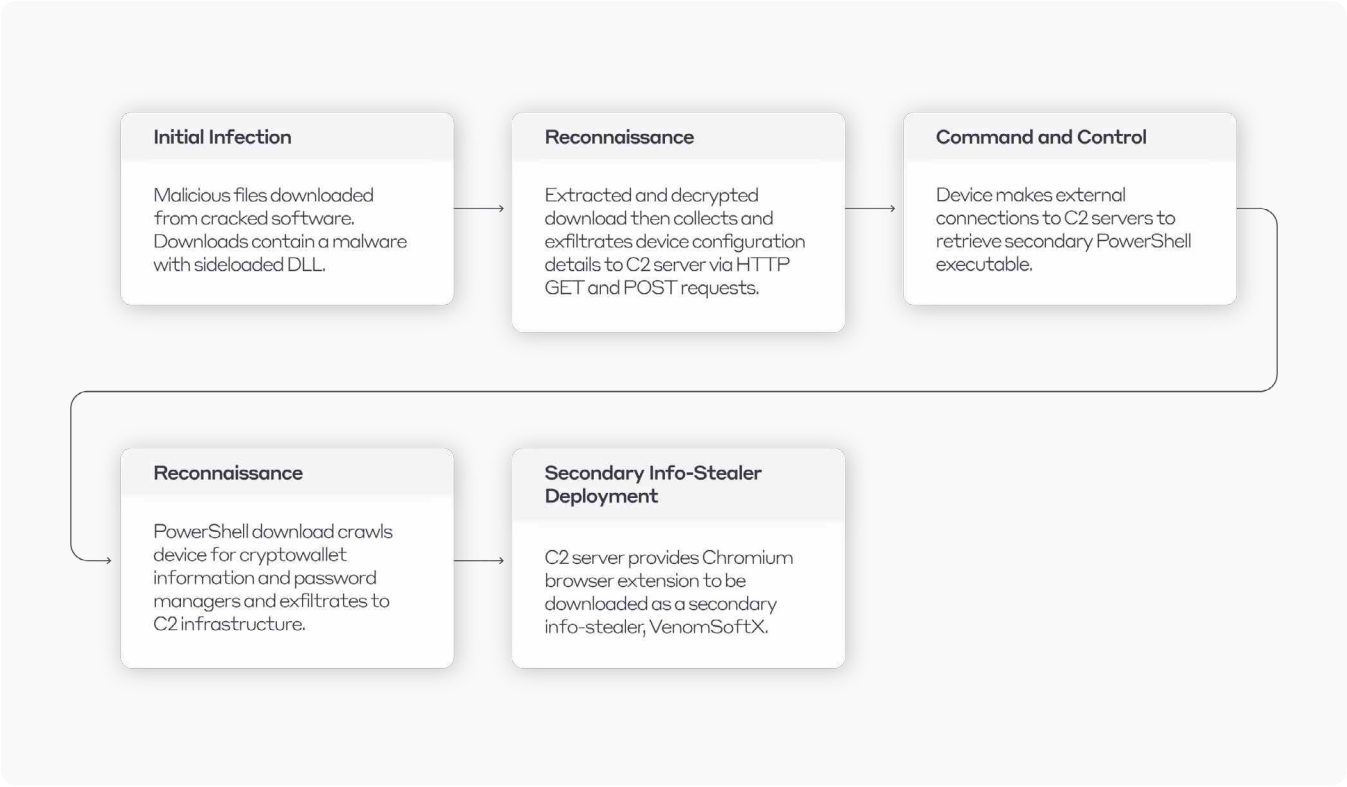


Figure 2: A typical attack progression of ViperSoftX malware observed by Darktrace.

SharePoint Phishing via Microsoft Teams (DarkGate Malware)

Around 83% of Fortune 500 companies rely on Microsoft Office products and services [1], with Microsoft Teams and Microsoft SharePoint in particular emerging as critical platforms to the business operations of the everyday workplace.

Researchers across the threat landscape have begun to observe these legitimate services being leveraged more and more by malicious actors as an initial access method. Microsoft Teams can be exploited to send targeted phishing messages to individuals within an organization, while appearing legitimate and safe. Although the exact contents may vary, the messages frequently use social engineering techniques to curate embedded SharePoint links. The malicious SharePoint links trigger payload delivery from compromised infrastructure.

In September 2023, Darktrace identified the malicious use of SharePoint, almost certainly delivered via Microsoft Teams, to infect a customer's network with the DarkGate malware. DarkGate is a commercial trojan, or commodity loader, known to deploy additional strains of malware on infected networks.

In one case, around 30 devices were observed connecting to a malicious SharePoint destination that had been tailored to include the name of a person, making it appear trustworthy. The organization did not have any employees who went by this name and this SharePoint site had never been seen on the network prior to this activity. The malicious actors likely sent multiple Microsoft Teams messages to deliver these spoofed SharePoint links.

Darktrace subsequently observed 10 of these devices downloading an unusual amount of data from SharePoint before making HTTP GET requests to a confirmed DarkGate malware endpoint using the user agent 'Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)'.

Following these HTTP GET requests, the devices proceeded to download a series of executable files and scripts, including 'Autoit3.exe', a legitimate file that DarkGate malware has been observed using previously, before making hundreds of HTTP POST connections with the target URI '/' to the malicious DarkGate endpoint using the user agent 'Mozilla/4.0 (compatible; Synapse).

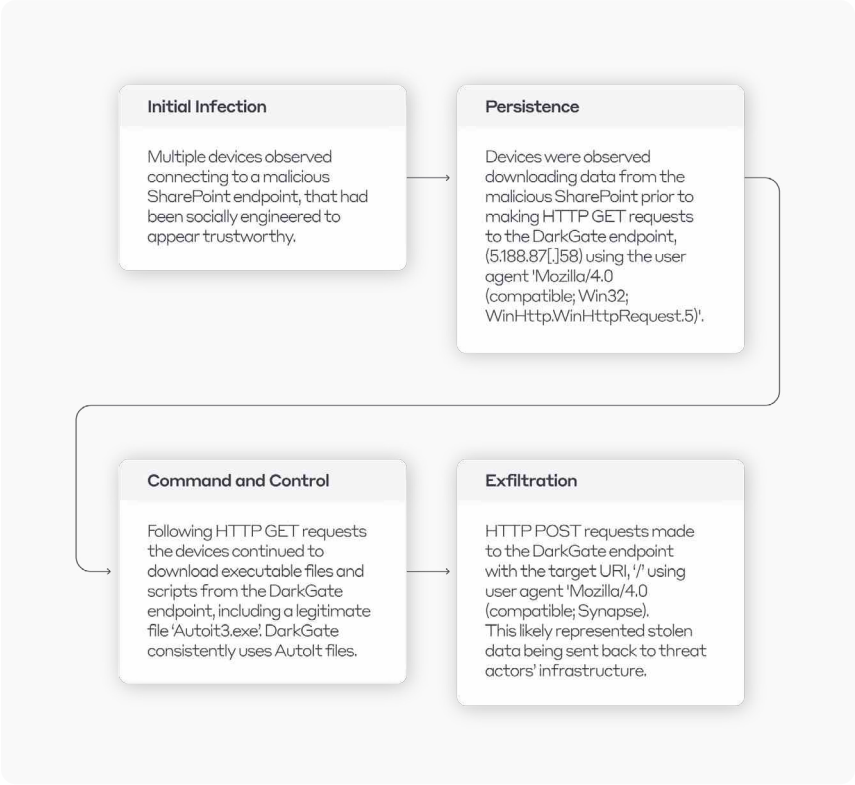


Figure 3: Attack overview of a malicious actor attempting to deploy DarkGate via Microsoft SharePoint and Teams.

The camouflaged nature of this phishing campaign allowed it to convince endpoint users of its legitimacy leading to the download of malicious malware, but also to bypass traditional security tools and even Microsoft's native email security capabilities.

Additional research highlights DarkGate's multi-facetted capabilities beyond loading, to include keylogging, information-stealing capabilities, and privilege escalation.

Fortunately for Darktrace customers, DETECT identified the malicious activity at the earliest possible stage despite its attempts at evasion.

RESPOND, in turn, was able to stop affected devices from communicating externally with suspicious endpoints, thus preventing the download of any additional malicious payloads.

Living off the land techniques corrupting business-critical programs such as Microsoft Teams and SharePoint intensify the already dogged fight to prevent phishing attacks and account compromise.

Combined with the context of the public emergence and evolution of Generative AI tools, the social engineering techniques utilized in phishing attacks could feasibly be written by AI and catered to a higher degree of specificity, making attacks extremely scalable and efficient.

As such, combatting exceptionally sophisticated social engineering requires the use of anomaly detection to differentiate between legitimate and compromised trusted services.

You can find the full technical blog on this threat find here: https://darktrace.com/blog/vipersoftx-how-darktrace-uncovered-a-venomous-intrusion

Darktrace/Email Trends

By learning the normal 'pattern of life' for every correspondent, Darktrace/Email™ is able to understand users and their unique communication patterns. Its Self-Learning AI develops an understanding of the person behind every email communication. This differs from the traditional security solutions, which rely heavily on previously seen malicious emails and known bad senders, meaning they are often prone to miss novel and increasingly sophisticated email threats.

Darktrace/Email can recognize the subtle deviations in expected email activity to determine whether any given email could represent a threat to customer networks. It is then able to make highly accurate decisions to mitigate and neutralize any email attack it faces.

Methodology: *The following email trends are derived from analysis of monitored Darktrace/Email model data for all customer deployments hosted in the cloud between September 1 and December 31, 2023. Around 90% of the global Darktrace customer base's email environments are cloud-based. The statistics presented here were obtained from dedicated Darktrace/Email models created in September 2023 to study email trends. The models were designed to alert for emails that were considered 100% anomalous for a customer's environment and contained "phishing indicators". For the purpose of this report, and indeed Darktrace's analysis of email environments, "phishing indicators" refers to emails that are confirmed as malicious, as opposed to merely unwanted spam emails. There was a total of 28 million spam emails held by Darktrace during this time.*

Darktrace's analysis of TTPs across customer email environments indicates that a significant number of email threats are capable of bypassing or manipulating traditional email security or authentication systems.

While Domain-based Message Authentication (DMARC) is often positioned as a way for organizations to 'solve' their email security problems, 65% of the phishing emails observed by Darktrace successfully bypassed its verification checks, indicating that malicious actors are increasingly improving their stealth and evasion tactics. Likewise, the fact that a significant portion of phishing emails were not detected by major email providers points to possible gaps or vulnerabilities in traditional security measures.*

Threat actors are evidently adapting and innovating their tactics through the use of novel social engineering techniques designed to manipulate recipients into giving up sensitive information like user credentials or bank information, or downloading malicious payloads.

Considering that over a quarter of the observed phishing emails were identified as containing a "significant" amount of text (200 words), threat actors are demonstrably having to innovate and bolster their efforts to craft sophisticated phishing campaigns, potentially leveraging Generative AI tools to automate social engineering activity.

Between September 1 and December 31, 2023, Darktrace/Email detected 10.4 million phishing emails across the customer fleet.

65%
of these emails successfully passed DMARC authentication

58%
of these emails passed through all existing security layers

45%
of these emails were identified as spear phishing attempts

3%
of these emails utilized newly created domains

38%
of these emails were observed utilizing novel social engineering techniques

28%
of these emails contained over 1,000 characters (or around 200 words)

Darktrace/Email detected at least 639,000 malicious QR codes within these emails

* All emails seen by Darktrace/Email have already passed through any existing gateway; emails are then checked by native spam filtering (Microsoft or Google Workspace). In 58% of cases, phishing emails detected by Darktrace/Email passed through this filtering, either because of gaps in detection or because customers have disabled it, trusting Darktrace/Email to handle all decisions.

SOC Trends

The Darktrace Security Operations Centers (SOC), located in Cambridge, San Francisco, and Singapore, provide 24/7 support to customers through our Proactive Threat Notification (PTN) and Ask the Expert (ATE) services.

As part of delivering SOC services, Darktrace expert cyber security analysts investigate a wide range of threats and produce trends observed across the fleet of SOC service customers.

Methodology: *The SOC Trends are derived from analysis of high-fidelity inputs through the SOC PTN and ATE services, involving both pattern analysis and assessment of data significance.*

The Darktrace SOC has observed the following as the most significant trends across its customer base in the second half of 2023:

- alternative initial access methods
- enhanced defense evasion methods
- ransomware deployment

Inbox-based initial access for malware delivery is typically seen as the most common method used by malicious actors.

The latter half of 2023, however, has seen a significant rise in the usage of alternative initial access methods, such as malware delivery via Microsoft Teams and malware delivery via sponsored search engine results.

This rise in alternative initial access methods is likely a result of the continued development and enhancement of traditional email security solutions.

During the latter half of 2023, Darktrace's SOC saw an increase in usage of a variety of defense evasion methods, such as the session cookie abuse to evade multi-factor authentication (MFA), the targeting of ESXi servers for ransomware encryption to evade host-based security measures, and the use of tunnelling services such as Cloudflare Tunnel to hide C2 infrastructure.

Malicious actors' increased usage of these defense evasion methods is a probable result of prominence of endpoint solutions within the security industry.

Ransomware continued to be the most common compromise during the latter half of 2023. Darktrace's SOC observed ransomware actors compromising Internet-facing servers, such as Exchange, Citrix Netscaler, Ivanti Sentry, Remote Desktop Services (RDS) hosts, VPN appliances, and Confluence, in order to gain entry to target networks. Once inside, ransomware actors abused Remote Monitoring and Management (RMM) tools such as Splashtop, Atera, AnyDesk, and Action1, to gain access to target systems.

A variety of ransomware strains were observed, with LockBit, ALPHV (i.e, BlackCat), Play, and Akira being the most common.

Monthly SOC Trends: Second Half of 2023

The top trends identified by the Darktrace SOC are based on activities investigated through Darktrace's Proactive Threat Notification (PTN) and Ask the Expert (ATE) services.

July	August	September	October	November	December
Usage of personal VPN services such as PIA VPN, HideMyAss VPN, and X-VPN in Microsoft 365 account hijackings	FTP-based Data Exfiltration	Exploitation of Ivanti Sentry Vulnerability	PsExec Usage	Session cookie abuse	Invoice Fraud
Laplas Clipper Malware	PsExec Usage	DarkGate Malware	Pikabot Malware	Drive-by downloads	Mailbox Exfiltration
Insider Threats	Compromise of Internet-facing systems, such as Exchange servers, Citrix NetScaler servers, and SQL servers	Cloudflare Tunnel Usage	Compromise of Internet-facing systems, such as VPN appliances and RDS hosts	WinRAR usage for data compression prior to exfiltration	Ransomware Deployment (mainly INC, Akira, and Black Basta) via usage of a variety of native tools and services, such as PsExec and RDP
Remote Access protocols, such as RDP and SSH	Remote Monitoring and Management (RMM) tools, such as AnyDesk	MS Teams-based Malware Delivery	Usage of anonymous file sharing services such as file[.]io	Exploitation of vulnerabilities in Internet-facing services, such as Confluence and Citrix	Usage of Hostkey's virtual private server (VPS) infrastructure
Ransomware (mainly ALPHV and Rhysida) deployment via usage of a variety of tools, such as PsExec, Nmap, AnyDesk, and RustDesk	Cloud account hijackings	Ransomware (mainly LockBit, ALPHV and Play) deployment via usage of a variety of tools, such as AnyDesk, NetScan, and WinSCP	Ransomware (mainly Akira and ALPHV) deployment via usage of a variety of tools, such as Splashtop, Atera, and PsExec	Ransomware deployment (mainly Rhysida, Play, and Akira) via usage of a variety of tools, such as Action1, PsExec, WinRM, and WinRAR	Usage of reconnaissance tools such as Netscan, Advanced IP Scanner, and Nmap

AI Insights and Incident Statistics

Methodology: *The following statistics cover anomalous activity detected across the global Darktrace customer base between July 1 and December 31, 2023, using modeling data from Enhanced Monitoring models and Cyber AI Analyst™ data. The data from Darktrace modeling represented below is comprised of high-fidelity models and pattern analysis; however, the data does not represent confirmed cyber-attacks. The statistics were derived through collection and analysis of these modeling data points. As per industry standard, the data does not take into account the proportion of customers in sector or customer growth. MITRE tactics and techniques have been included as they are mapped to both Darktrace modeling and pattern analysis in Enhanced Monitoring models and AI Analyst data, respectively.*

Cyber AI Analyst Statistics

The following statistics cover anomalous activity detected across the global Darktrace customer base between July 1 and December 31, 2023, and were produced using Cyber AI Analyst data and take into account Enhanced Monitoring models.

Cyber AI Analyst investigates, analyzes, and triages threats seen within customers' Darktrace environments. By learning from the millions of interactions between Darktrace's expert analysts and Darktrace DETECT components, the Cyber AI Analyst combines human expertise with the consistency, speed, and scalability of AI.

Enhanced Monitoring models are correlated with high-fidelity activity associated with indicators of an emerging attack. The Enhanced Monitoring models represent a subset of Darktrace's behavioral modeling within DETECT.

Cyber AI Analyst conducts investigations to identify emerging patterns of activity which are indicative of security incidents; this analysis includes one or more anomalies which are modeled within DETECT. Cyber AI Analyst investigations are designed to produce reports on the most interesting and high-priority activity observed by Darktrace within a customer environment.

The most observed patterns of activities identified by Cyber AI Analyst during the second half of 2023 were related to Beaconing. Beaconing is indicative of Command-and-Control activity as per the MITRE attack tactics categorization.

The subsequent most observed AI Analyst patterns of activity during the second half of 2023 included:

- Software-as-a-Service (SaaS) Hijack (Privilege Escalation MITRE attack tactic)
- SSL C2 (Command and Control MITRE attack tactic)
- HTTP Agent (Command and Control MITRE attack tactic)
- Scanning (Discovery and Reconnaissance MITRE attack tactic)

The most observed MITRE tactic across Cyber AI Analyst investigations between July and December 2023 was Command-and-Control.

The subsequent most observed MITRE tactics included:

- Lateral Movement
- Credential Access
- Compliance
- Privilege and Escalation

Cyber AI Analyst observed more patterns of activities from customers in the EMEA region than any other region between July and December 2023.

The other region with the most observed activity included:

- Americas
- APAC

Incident Statistics

The following statistics cover anomalous activity detected across the global Darktrace customer base between July 1 and December 31, 2023, and were produced using data primarily focused on Enhanced Monitoring breaches.

Enhanced Monitoring models are correlated with high-fidelity activity associated with indicators of an emerging attack. The Enhanced Monitoring models represent a subset of Darktrace's behavioral modeling within DETECT.

During the second half of 2023, the most observed probable cyber incidents were 'Multiple Lateral Movement' related breaches. As per the MITRE attack tactics categorization, this is indicative of Lateral Movement.

The other most observed probable cyber incidents were:

- Suspicious Network Scanning (Discovery & Reconnaissance MITRE attack tactic)
- SaaS Login From Rare Following Suspicious Login Attempt (Credential Access MITRE attack tactic)
- SaaS Unusual Login and New Email Rule (Persistence MITRE attack tactic)
- Unusual External Data Transfer (Exfiltration MITRE attack tactic)

Between July 1 and December 31, 2023, Darktrace observed that SaaS-related Enhanced Monitoring model breaches accounted for 23% of the global probable cyber incidents, remaining consistent with the previous six months.

Between July 1 and December 31, 2023, Darktrace observed more probable cyber incidents from customers within EMEA than any other customer region.

The other customer regions by descending order were:

- Americas
- APAC

Generative AI Statistics

The following statistics cover anomalous activity relating to the usage of Generative AI services detected across the global Darktrace customer base between July 1 and December 31, 2023, and were produced using the Compliance opt-in Generative AI module from the Darktrace model data.

The Compliance Generative AI models are primarily based on coverage of key tools utilized throughout multiple industries, highlighted as primary sources for AI adoption. It is, therefore, a realistic probability that Darktrace would not highlight Generative AI usage if unknown hostnames or services are utilized.

Between July 1 and December 31, 2023, around half of Darktrace customers were observed accessing Generative AI services.

During this period, OpenAI was the most common Generative AI service observed across Darktrace customers. Between July 1 and December 31, 2023, more than half of all Anomalous Upload to Generative AI model breaches observed involved OpenAI, making it the most used Generative AI service for anomalous data transfers in this period

- Microsoft Copilot, Hugging Face, Otter AI and Codium also featured amongst the most used Generative AI services for anomalous data transfer breaches

Between July 1 and December 31, 2023, 72% of all regular connections to Generative AI services via API involved OpenAI, making it the most consistently used Generative AI service by Darktrace customers

- Tab Nine, Microsoft Copilot, Codium, Otter AI, Hugging Face, Bing and StableDiffusion also featured amongst the most used Generative AI services for this breach

Vulnerabilities

Darktrace/Newsroom, a capability of the Darktrace PREVENT/Attack Surface Management (ASM)™ product, continuously monitors OSINT sources for new critical vulnerabilities (CVEs) and assesses each organization's exposure through its in-depth knowledge of their unique external attack surface.

Darktrace quickly assess which assets on customer networks could potentially be affected by emerging CVEs and provides prioritized mitigation advice specific to each organization.

Newsroom finds are published on the PREVENT/ASM dashboard, where it presents a detailed summary of the vulnerability, highlighting the affected software and how many assets run this software on the customer's network.

New CVEs, like Log4J and ProxyLogon, regularly enter the public domain within a short time of discovery, meaning the average time to exploitation is shorter than ever. As such, organizations must be able to identify whether they are susceptible to new vulnerabilities, and promptly understand mitigation techniques.

CVE-2022-42889 is a critical vulnerability in the Apache Commons Text Library which has been compared to Log4Shell, albeit not as widespread. Apache Commons Text performs variable interpolation, allowing properties to be dynamically evaluated and expanded. Affected versions are vulnerable to remote code execution or unintentional exposure to remote servers if untrusted configuration values are used.

CVE-2023-25690 is a critical vulnerability which enables HTTP request smuggling attacks on Apache HTTP Server. If exploited, it could be used by an attacker to bypass access constraints in proxy servers, route undesired URLs to existing origin servers and perform cache poisoning.

Two critical vulnerabilities were observed in Git that would enable attackers to execute arbitrary code after successfully exploiting heap-based buffer overflow weaknesses.

Top five most observed vulnerabilities by Newsroom in the second half of 2023 by number of affected assets:

Text4Shell in Apache Commons Text Library (CVE-2022-42889)
Apache HTTP Server (CVE-2023-25690)
Git (CVE-2022-41903, CVE-2022-23521)
Wordpress Social Login and Register (miniOrange) (CVE-2023-2982)
BIG-IP (CVE-2023-46747)

CVE-2022-41903 would allow an attacker to trigger a heap-based memory corruption during clone or pull operations, resulting in remote code execution, while **CVE-2022-23521** could enable code execution during an archive operation, which is commonly performed by Git forges.

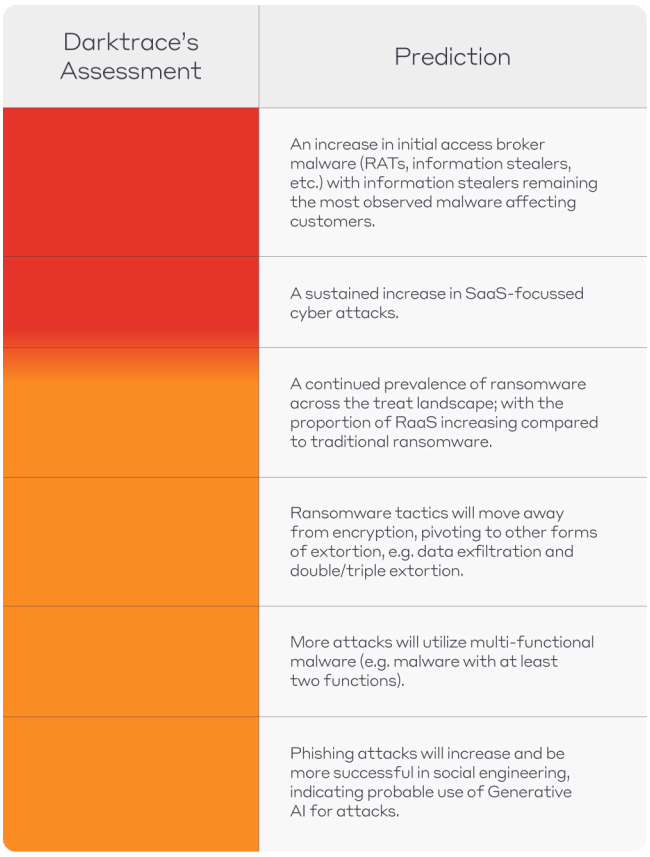
CVE-2023-2982 is an authentication bypass vulnerability disclosed in miniOrange's Social Login and Register plugin for WordPress that could enable a malicious actor to log in as any user, provided that they know the corresponding email address.

CVE-2023-46747 is a critical vulnerability rooted in the configuration of BIG-IP that could result in unauthenticated remote code execution. This vulnerability allows malicious actors to gain unauthorized access to networks through the management port and/or self-IP addresses to execute arbitrary system commands.

Observations and Predictions

After analyzing the observed threats and trends that have affected customers across the Darktrace fleet in the second half of 2023, the Darktrace Threat Research team have made a series of predictions. These assessments highlight the threats that are expected to impact Darktrace customers and the wider threat landscape in 2024.

Methodology: *The Threat Research team utilized structured analytic techniques to analyze their hypotheses and provide evidentiary support.*



Initial Access Broker Malware

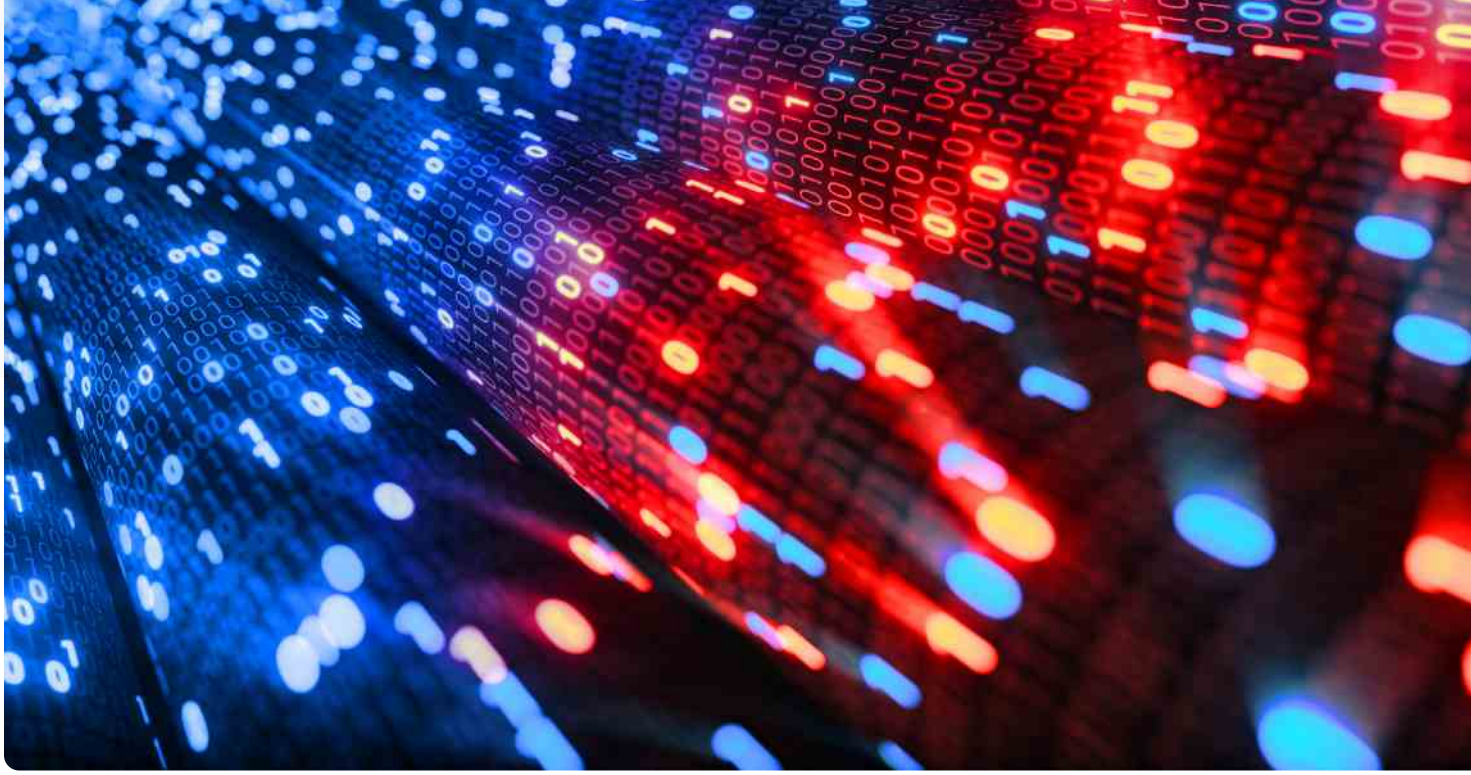
The prevalence of initial access broker malware is expected to continue increasing in 2024, indicating a shift towards more sophisticated intrusion techniques to gain illicit entry to organization networks. Analysis of the latter half of 2023 has indicated the top three initial access broker malwares investigated were information stealers, RATs, and downloaders. These types of malware often serve as a gateway for threat actors to compromise a target network before launching subsequent, and often, more severe attacks.

Would-be cyber criminals are now able purchase and deploy these malware without the need for technical expertise. Information stealers are just one type of initial access broker that Darktrace has consistently observed throughout the course of 2023 and is likely to remain the most relevant threat to customers in 2024. In addition to the ViperSoftX information stealer detailed in this report, in 2023 Darktrace also investigated multiple instances of Lumma Stealer, an information stealer known to primarily target cryptocurrency wallets, browser extensions and two-factor authentication (2FA) before exfiltrating sensitive data from compromised devices to malicious C2 infrastructure. [2] [3] In one particular Lumma Stealer compromise, Darktrace observed malicious connections to endpoints related to commonly marketed MaaS strains, including Laplas Clipper, Raccoon Stealer and Vidar [4] [5] [6], suggesting the developers of information stealers may cross-functionally utilize other compromised infrastructure or possibly collaborate amongst strain developers, highlighting the trend of multi-phase compromises involving multiple varied malware families.

Increase in SaaS Attacks

Given the increasing reliance on SaaS solutions and platforms for business operations, the forecasted uptick in SaaS-centric attacks should come as no surprise. With larger attack surfaces than ever before, attackers are very likely to continue targeting organizations' cloud environments with account takeovers granting unauthorized access to privileged accounts. These account hijacks can be further exploited to perform a variety of nefarious activities, such as data exfiltration or launching phishing campaigns. In one such example detailed in September 2023, Darktrace detected a suspicious chain of SaaS activity on the network of a customer who was about to begin its trial period. Despite having only been installed on the customer's network for a matter of days, Darktrace identified that a legitimate SaaS account, belonging to a privileged user, was behaving anomalously. [7]

Through the detection of unusual login attempts from geographically improbable locations and suspicious administrative changes, Darktrace recognized that the account had been hijacked and was subsequently used to launch an internal spear-phishing campaign. It is paramount for organizations to not only fortify their SaaS environments with security strategies including MFA, regular monitoring of credential usage, and strict access control, but moreover augment SaaS security using anomaly detection.



The Prevalence and Evolution of Ransomware

Without doubt ransomware will continue to dominate conversation across the threat landscape in 2024. However, the Darktrace Threat Research team anticipates this will be accompanied by a notable surge in RaaS attacks, marking a shift away from conventional ransomware. The uptick in RaaS observed in 2023 evidences that ransomware itself is becoming increasingly accessible, lowering the barrier to entry for threat actors.

This surge also demonstrates how lucrative RaaS is for ransomware operators in the current threat landscape, further reinforcing a rise in RaaS.

This development is likely to coincide with a pivot away from traditional encryption-centric ransomware tactics towards more sophisticated and advanced extortion methods. Rather than relying solely on encrypting a target's data for ransom, malicious actors are expected to employ double or even triple extortion strategies, encrypting sensitive data but also threatening to leak or sell stolen data unless their ransom demands are met. One pertinent example of this identified by the Darktrace SOC in 2023 was the Black Basta ransomware strain. [8]

Black Basta is known to utilize double extortion as part of its modus operandi, exfiltrating sensitive data from affected networks and threatening to publish it on the dark web if ransom payments are not made.

Multi-functional Malware Attacks

Whereas malware has traditionally been designed with one specific function as its primary purpose, the emergence and utilization of multi-functional malware is expected to continue throughout 2024. Multi-purpose malware poses an increased threat to security teams due to its adaptability and versatility, allowing threat actors to carry out a number of malicious activities within one attack phase and decreasing dwell time on affected networks.

One recently observed example of this cross-functionality was observed in the Darktrace Threat Research team's investigation into CyberCartel. [9] The investigation discovered around 40 networks potentially affected by CyberCartel, a Latin American threat group that had been active since 2012 and known to leverage MaaS offerings from other malware strains like the Fenix botnet.

In doing so CyberCartel is able to effectively deploy its malware and carry out information-stealing activity while utilizing shared C2 infrastructure, making accurate attribution and assessment of the confidence level for which group was affecting the customer base extremely difficult.

So, What's Next?

Continuous Reliance on Living off the Land

With evolving sophistication of security tools and greater industry adoption of AI techniques, threat actors have focused more and more on living off the land. The exploitation of native programs has steadily increased, both in the voracious research to identify new vulnerabilities and through novel techniques to use legitimate programs for nefarious purposes, such as exploiting business-critical programs like Microsoft Teams.

As evidenced by exploitation of native Windows programs and repeated spoofing of trusted services such as AnyDesk throughout 2023, the increasing cyber hygiene of organizations forces threat actors to exploit the bonds of trust placed upon business normal and business-critical services.

This has the added benefit of increasing dwell time as security teams have to distinguish between friendly and adversarial services that are packaged identically. The extremely high volume of vulnerabilities discovered in 2023 highlights threat actors persistent need to compromise trusted organizational mechanisms and infrastructure to gain a foothold in networks. Although inbox intrusions remain prevalent, the exploitation of edge infrastructure has demonstrably expanded compared to previously endpoint-focused attacks.

Given the prevalence of endpoint evasion techniques and the high proportion of tactics utilizing native programs, threat actors will likely progressively live off the land, even utilizing new techniques or vulnerabilities to do so, rather than relying on unidentified malicious programs which evade traditional detection.

An Increase in Multi-Phase Compromises

With the increasing 'as-a-Service' marketplaces, it is likely that organizations will face more multi-phase compromises, where one strain of malware is observed stealing information and that data is sold to additional threat actors or utilized for second and/or third-stage malware or ransomware.

This trend builds on the concept of initial access brokers but utilizes basic browser scraping and data harvesting to make as much profit throughout the compromise process as possible. This will likely result in security teams observing multiple malicious tools and strains of malware during incident response and/or multi-functional malware, with attack cycles and kill chains morphing into less linear and more abstract chains of activity. This makes it more essential than ever for security teams to apply an anomaly approach to stay ahead of asymmetric threats. A good initial indicator example of this trend observed during 2023 is the prevalence of information-stealing malware and the volume of organizations affected by those strains. Information-stealing malware was consistently observed not only harvesting basic user information but also performing more advanced data compromise, often leading to credential harvest and secondary infections.

With the probable increase of multi-functional malware and the escalating value of data, multi-phase compromises are likely to stretch already scant security resources resulting in longer incident remediation and higher damage attacks. Specific attribution will very likely become more difficult amid the varied threat actor landscape and the concurrent nature of the compromises with non-linear kill chains.

Appendices

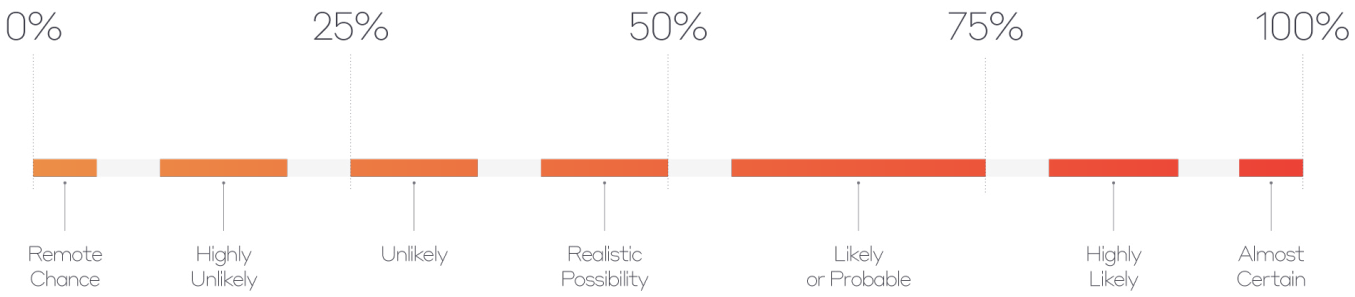


Figure 4: **Probability Yardstick.** The language utilized throughout Darktrace's assessments mirrors the probability yardstick to determine probability and likelihood for analytical tradecraft. Probability Yardstick, reference: https://www.gov.uk/government/news/defence-intelligence-communicating-probability

Threat Research: Most Observed Threats

Mirai	Remcos
NJRAT	RedLine
ScamClub	Truebot
RedLine Stealer	Emotet
Tor2Mine	IcedID
AsyncRAT	Ave Maria
Ivanti EPMM Exploit	Nanocore RAT
Pupy RAT	Qakbot
Cobalt Strike	Ursnif
FAKEUPDATES	WS FTP Exploits
XMRig	

Darktrace Analysis: Inside the SOC Blogs

References

[1] Essential Microsoft Office Statistics in 2024:
https://zipdo.co/statistics/microsoft-office/#:~:text=Microsoft%20Office's%20suite%20of%20software,companies%20use%20Microsoft%20Office%20365

[2] Darktrace Analyst blog: ViperSoftX
https://darktrace.com/blog/vipersoftx-how-darktrace-uncovered-a-venomous-intrusion

[3] Darktrace Analyst blog: The Rise of the Lumma Info-Stealer
https://darktrace.com/blog/the-rise-of-the-lumma-info-stealer

[4] Darktrace Analyst blog: Laplas Clipper
https://darktrace.com/blog/laplas-clipper-defending-against-crypto-currency-thieves-with-detect-respond

[5] Darktrace Analyst blog: Racoon Stealer Part 1
https://darktrace.com/blog/the-last-of-its-kind-analysis-of-a-raccoon-stealer-v1-infection-part-1

[6] Darktrace Analyst blog: Vidar Info-Stealer
https://darktrace.com/blog/vidar-info-stealer-malware-distributed-via-malvertising-on-google

[7] Darktrace Analyst blog: Protecting Prospects
https://darktrace.com/blog/the-rise-of-the-lumma-info-stealer

[8] Darktrace Analyst blog: Black Basta
https://darktrace.com/blog/black-basta-old-dogs-with-new-tricks

[9] Darktrace Analyst blog: Countering the Cartel
https://darktrace.com/blog/countering-the-cartel-darktraces-investigation-into-cybercartel-attacks-targeting-latin-america

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. Breakthrough innovations from its R&D Centers have resulted more than 145 patent applications filed. Darktrace employs 2,200+ people around the world and protects over 9,000 organizations globally from advanced cyber-threats.

Scan to
LEARN MORE

DARKTRACE

Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 4949 7696
info@darktrace.com
darktrace.com