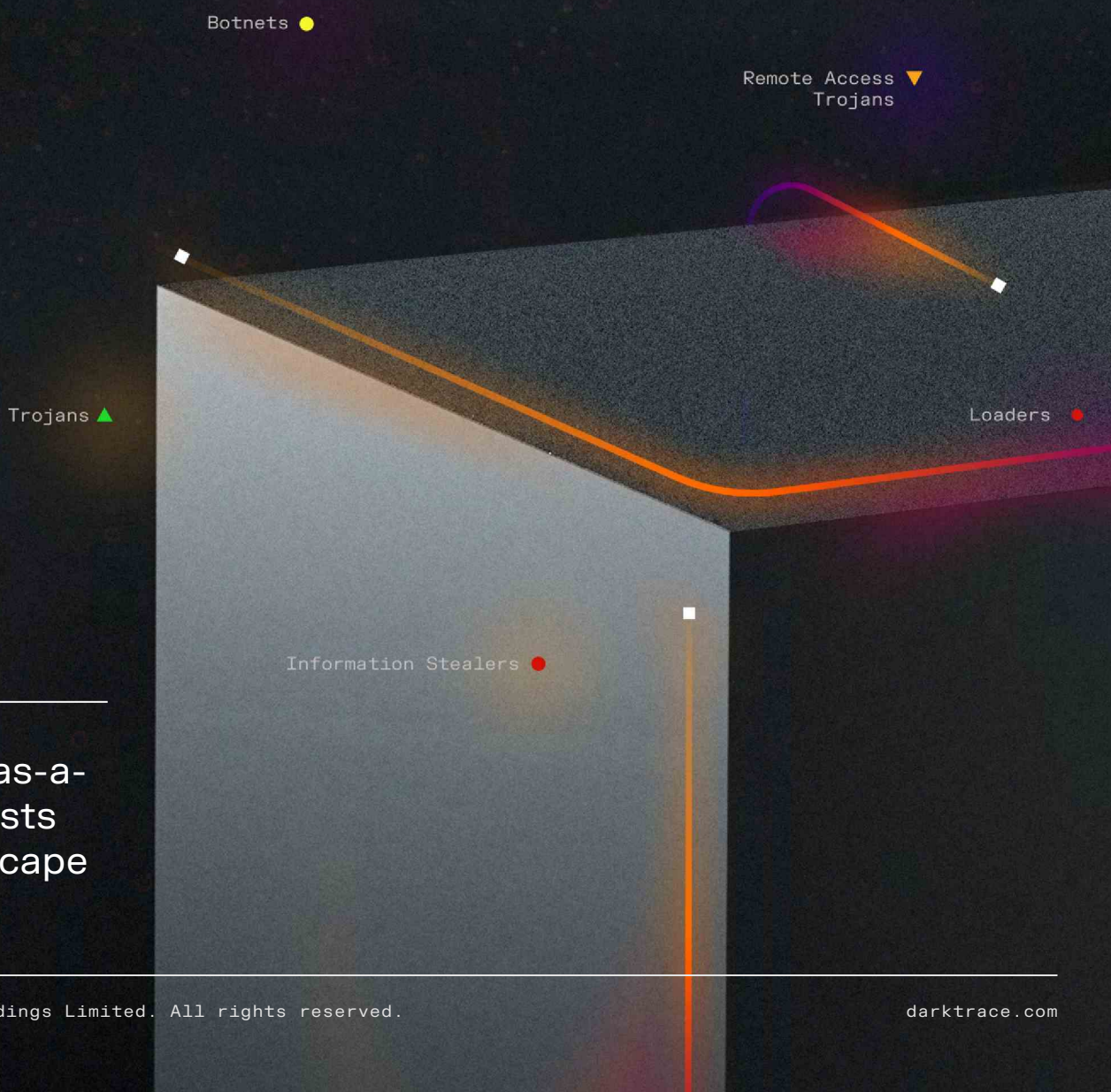
DARKTRACE

First 6: Half-Year Threat Report 2024



Cybercrime-as-a-Service Persists as the Landscape Evolves.

Foreword

Welcome to Darktrace's First 6: Half-Year Threat Report 2024.

At Darktrace, we approach threat intelligence with a unique perspective. Unlike traditional security vendors that rely on established patterns from past incidents, our strategy is rooted in the belief that identifying behavioral anomalies is crucial for identifying both known and novel threats.

Darktrace's AI-driven technology excels at detecting malicious activities that may appear harmless in other environments and could evade traditional security tools that focus solely on specific rules and signatures. By emphasizing behavioral analysis and leveraging multiple AI applications, Darktrace is able to identify and neutralize threats that are yet to be publicly disclosed or attributed. Through hindsight analysis, we have highlighted numerous threats, including zero day, N day and other novel attacks, showcasing their evolving nature and Darktrace's ability to identify them.

For our customers, the primary benefit is the timely detection and containment of emerging threats through Darktrace detection and Autonomous Response capabilities. For our analysts and researchers, these incidents mark the beginning of a deeper investigation, aiming to connect mitigated threats to wider trends from across the threat landscape.

Our findings and insights are regularly shared via our Inside the SOC blog series, providing detailed analysis into specific incidents or campaigns that have been observed across the Darktrace fleet.

We value your feedback and invite you to reach out to us as threatintelligence@darktrace.com with any thoughts or questions.

Thank You

A huge thank you to the following members of the Darktrace Analyst team and other colleagues across the business who contributed the insights for this report:

Joel Davidson, Emma Foulger, Justin Frank, Maria Geronikolou, Steven Haworth, Paul Jennings, Nathaniel Jones, Freek Klein, Qing Hong Kwa, Min Kim, Emily Megan Lim, Sam Lister, Alexandra Marsden, Joanna Ng, Nahisha Nobregas, Diego Noguera Rico, Adam Potter, Alexandra Sentenac, Steven Sosa, Zoe Tilsiter, Ryan Traill, Justin Torres, Brittany Woodsmall.

Executive Summary

Advanced TTPs, Subscription-Based Attack Models, and the Resurgence of Historical Threats

The sophistication of cyber threats has escalated dramatically, with malicious actors' deploying advanced tactics, techniques, and procedures (TTPs) to exploit vulnerabilities and evade detection. Subscription-based tools such as Malware-as-a-Service (MaaS) and Ransomware-as-a-Service (RaaS) have also lowered the barrier-to-entry for less experienced attackers, making it easier to carry out complex, multistage attacks.

Moreover, many historically identified threats are resurging. Attackers are utilizing new techniques, such as leveraging popular, legitimate third-party services in their operations, to bypass conventional security methods. As threat actors continue to evolve their techniques and tactics, it's imperative for organizations to have their finger on the pulse of the most prevalent threats persisting today. Darktrace's First 6: Half-Year Threat Report 2024 aims to highlight the latest attack trends and key threats observed by the Darktrace Threat Research team.

By focusing on anomalies and behavioral analysis coupled with mapping mitigated cases to publicly attributed threats, this report provides rich contextual insights on a wide array of threats, including novel threats that have taken new shape. By reading this report, we hope organizations will be able to better understand the current threat landscape and improve their security posture so they can better defend against these persistent threats.

Key Insights

/ **Malware-as-a-Service continues to pose significant risk for organizations:** Many of the prevalent threats observed by Darktrace were heavily utilizing MaaS tools. These include the continued and repeated presences of multiple malware families from years prior, such as Amadey and Raspberry Robin. This highlights that while MaaS strains often adapt their TTPs from one campaign to the next, many strains remain unchanged yet continue to achieve success. This suggests that some security teams and organizations are still falling short in defending their environments.

/ **Double extortion methods are now prevalent amongst ransomware strains:** As ransomware continues to be a top security concern for organizations, Darktrace's Threat Research team has identified three predominant ransomware strains impacting customers: Akira, Lockbit, and Black Basta. All three have been observed using double extortion methods, with Akira attempting to exfiltrate data within 12 hours of the initial file encryption.

/ **Edge infrastructure compromise is a top security concern:** As part of the top three threats observed by Darktrace's Security Operation Center (SOC), malicious actors are executing mass-exploitation of vulnerabilities in edge infrastructure devices. The most widely exploited edge infrastructure devices observed were those related to Ivanti Connect Secure, JetBrains TeamCity, FortiClient Enterprise Management Server, and Palo Alto Networks PAN-OS.

/ **Email phishing shows no signs of slowing down:** Between December 21, 2023, and July 5, 2024, Darktrace / EMAIL detected 17.8 million phishing emails across the fleet, with 62% of these phishing emails successfully bypassing Domain-based Message Authentication, Reporting, and Conformance (DMARC) verification checks.

Methodology

Threat Research Methodology

Darktrace's Threat Research team conducts research across customer deployments to identify which threats are affecting customers, identify key Indicators of Compromise (IoC) within those threats, and contextualize them with additional information to provide customers with relevant threat intelligence.

This research is based on Darktrace's anomaly detection and revolves around analysis and contextualization of detection information performed by the Threat Research team. Any threats detected were promptly brought to the attention of the relevant customer security teams and, in cases when Darktrace's Autonomous Response technology was enabled, they were swiftly mitigated, preventing them from escalating.

Darktrace analysis assessed a broad variety of threats between the reporting period of January 1 and June 30, 2024. Many of these threats were identified as campaign-like activity targeting multiple customers. Although some of these threats were identified as emerging or novel, 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.

Insights from the Darktrace SOC Methodology

The trends outlined in the 'Insights from the Darktrace Security Operations Center (SOC)' section of this report are derived from analysis of high-fidelity inputs observed through Darktrace's Managed Threat Detection and Security Operations Support services, involving both pattern analysis and assessment of data significance between January 1 and June 30, 2024.

Email Trends Methodology

The statistics highlighted in the 'Email Trends' section are derived from analysis of monitored Darktrace / EMAIL model data for all customer deployments hosted in the cloud December 21, 2023, and July 6, 2024. Around 90% of the global Darktrace customer base's email environments are cloud-based. Darktrace / EMAIL models are 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. Darktrace / EMAIL data is currently collected and processed every 28 days, rather than monthly. Consequently, this analysis includes data from outside the specified reporting period, specifically the last 10 days of December 2023 and the first 5 days of July 2024.

Generative AI Usage Methodology

The statistics in the 'Generative AI Usage' section covers anomalous activity relating to the usage of Generative AI services detected across the global Darktrace customer base between January 1 and June 30, 2024, and were produced using the Compliance opt-in Generative AI module from the Darktrace model data.

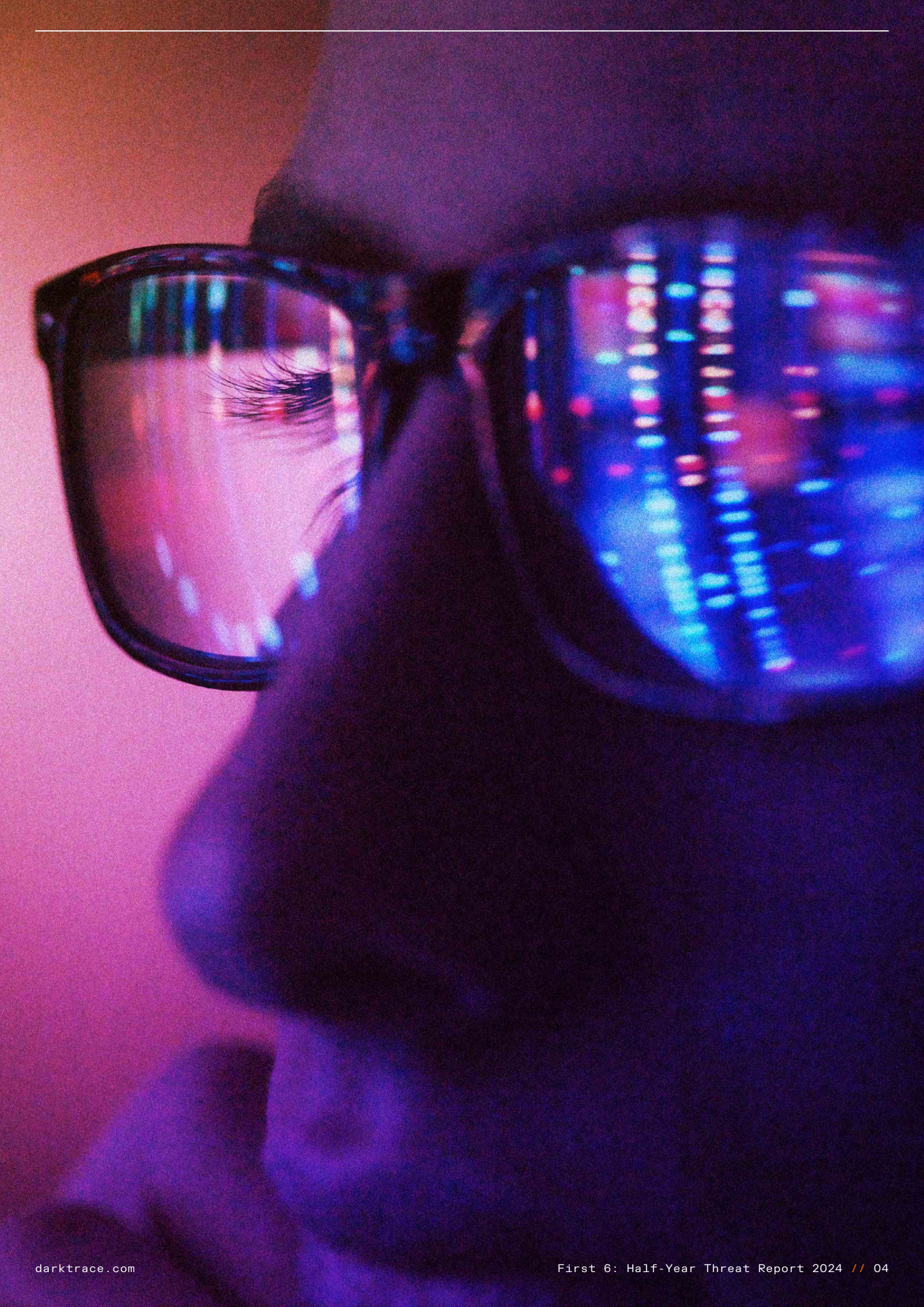
Compliance Generative AI models are primarily based on coverage of key tools utilized throughout multiple industries, highlighted as primary sources for AI adoption. It is, therefore, a realistic probability that Darktrace would not highlight Generative AI usage if unknown hostnames or services are utilized.

Cryptocurrency Mining Activity Methodology

The statistics in the 'Cryptocurrency Mining Activity Breakdown' section refer to the top identified cryptocurrency coins in cryptocurrency mining incidents detected by Darktrace across the global customer base between January 1 and June 30, 2024. The coins being mined were identified by the connection hostname in alerts of the Cryptocurrency Mining Activity model.

In cases where it was unclear, open-source intelligence (OSINT) was leveraged to determine which coin was associated with the hostname. Only the top 95% of hostnames were included in Darktrace's analysis as there were a significant number of low-frequency examples.

The classification "N/A" means the connection hostname could not be mapped to a specific currency due to lack of OSINT evidence, or because multiple currencies could be associated with the same endpoint. The "N/A" category ranked in second place for the most observed currency but has been removed from analysis. It is likely that the overall rankings would change if the coins in the "N/A" category could be identified.



The Continued Prevalence of Malware-as-a-Service

As part of the research, Darktrace identified several key threats that pose significant risk to its customers and organizations worldwide. These threats appear to incorporate various tactics and techniques including MaaS, living-off-the-land, edge infrastructure vulnerability exploitation, and initial access brokers.

Furthermore, previously observed threats have also resurfaced, continuing to affect organizations.

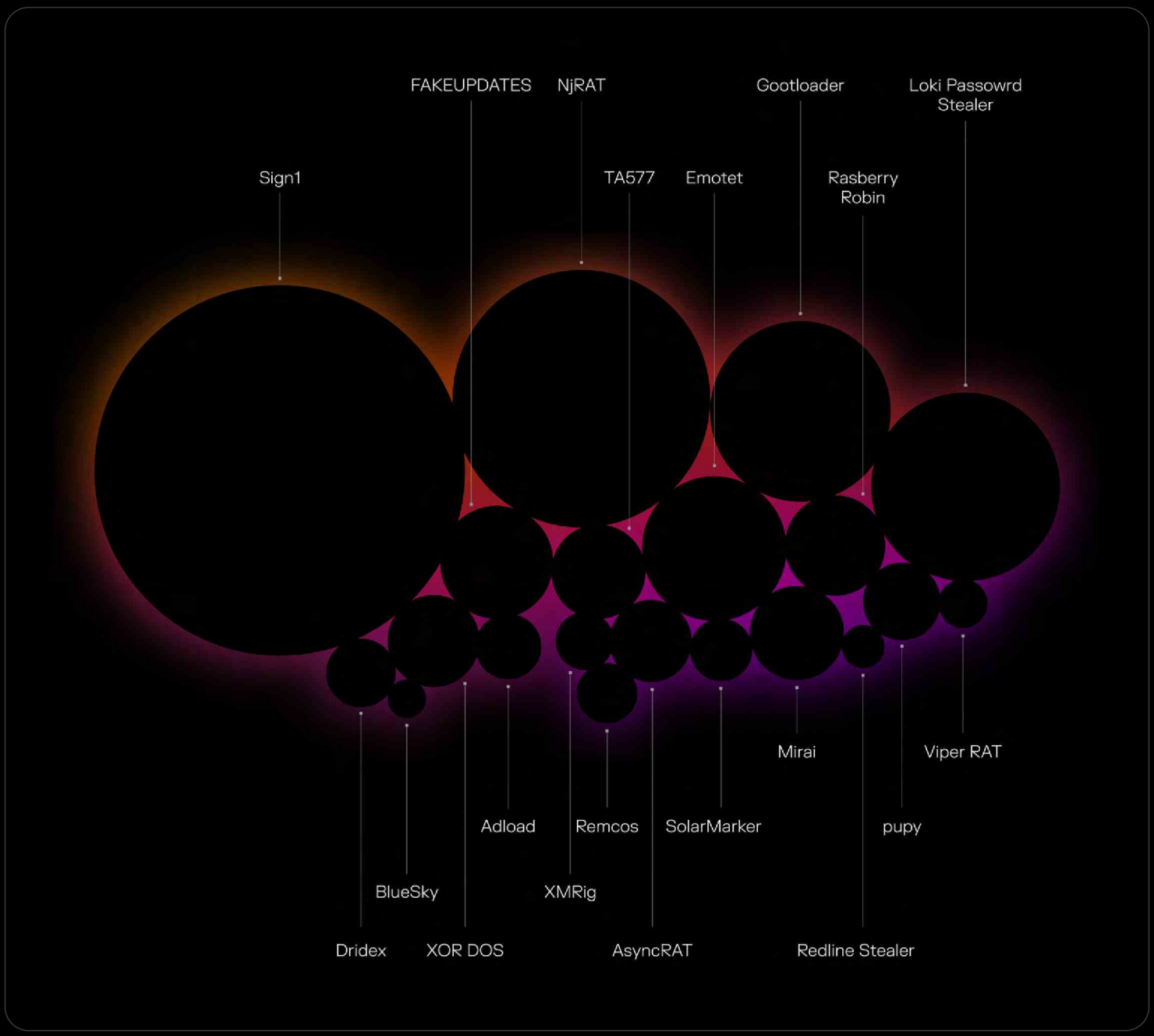


Figure 01: The diagram above represents Darktrace detections containing IoCs associated with particular threats. The size of the bubble displayed relates to the frequency of detections observed across the Darktrace fleet.

When comparing the bubble chart in figure 01 with the previous half year's data, there are several returning threats, notably Mirai, AsyncRAT, Emotet, and NjRAT.

Darktrace also identified that many of the prevalent threats observed targeting its customers were heavily utilizing MaaS tools. Likely owing to the lucrative subscription-based income of MaaS ecosystems as well as the low barrier to entry and high demand, it is unsurprising that MaaS strains remain the most relevant threats for many organizations. By offering pre-packed, plug-and-play malware, the MaaS market has enabled even inexperienced attackers to carry out potentially disruptive attacks regardless of their level of skill or technical ability.

In the past six months, Darktrace's analysis of threats associated with MaaS strains revealed the continued and repeated presence of multiple malware families previously investigated in prior years. Notable examples include the Amadey information stealer [1] and the Raspberry Robin worm.

Despite no major updates to the Amadey information stealer or its TTPs, their persistence indicates an ongoing threat to smaller organizations that are likely under-resourced and outsource portions of this security responsibility and larger organizations where hygiene is poor or have large guest subnets. Although the Amadey information stealer has not displayed significant updates to its TTPs, its persistence remains a considerable threat.

Meanwhile, Darktrace has recently observed Raspberry Robin, which was initially spread through infected USB drives [2], utilizing social engineering and malvertising to infect target networks.

Since March 2024, Darktrace has observed the distribution of Raspberry Robin via obfuscated Windows Script Files (WSFs), which use curl commands to retrieve dynamic-link library (DLL) payloads from a malicious server.

It is anticipated that Malware-as-a-Service will remain a prevalent part of the threat landscape for the foreseeable future.

This persistence highlights the adaptive nature of MaaS strains, which are capable of changing their TTPs from one campaign to the next and bypassing traditional security tools. Therefore, it is crucial for organizations to leverage AI-driven security measures, that can detect anomalous activity in real time without relying on prior knowledge of specific tactics, and counter sophisticated and evolving MaaS threats.

Information-stealing malware strains were the most observed type of malware between January and June 2024, accounting for 29% of early triaged investigations.

The Darktrace Threat Research team further identified that the most significant malware threats to organizations during this time were trojans (15%), remote access trojans (RATs) (12%), botnets (6%), and loaders (6%).

Note: The percentages above represent more than 100%, as customers' data (i.e., the incidents they were observed to experience) may be categorized into more than one threat type based on infections within each category.

Ransomware Remains a Top Security Concern

As ransomware continues to be a top security concern for organizations, the Darktrace Threat Research team has identified three predominant ransomware strains impacting customers: Akira[3], Lockbit[4] and Black Basta[5]. While these ransomware families are not new, they have remained persistent threats in recent years, indicating that these variants are continuing to evolve and adopt new, sophisticated tactics to circumvent security measures.

As organizations harden their digital defences by understanding and pre-empting the TTPs of known ransomware strains, threat actors often incorporate new strategies making them more sophisticated, faster, and harder to defend against. One such strategy noted by Darktrace is the adoption of double extortion methods. Malicious actors will not only encrypt their target's data, but also exfiltrate sensitive files with threat of publication if the ransom is not paid. In the case of Akira in particular, Darktrace observed attackers attempting to exfiltrate data within 12 hours of the initial file encryption, all but confirming that double extortion is a standard part of their playbook.

Both LockBit and Black Basta have been observed using such double extortion tactics, highlighting the lucrative strategy of the RaaS marketplace. RaaS operates not dissimilarly to traditional business franchising by using a strategic model to inform its operations. First, it assesses the overall size and profitability of the business, before determining an appropriate ransom amount to demand based on the quantity and sensitivity of the stolen data. Just like corporate sales, more advanced RaaS operators offer playbooks detailing whom to target, why, and which regulatory bodies to be mindful of. Basic threat actors can then leverage this information to intimidate their targets into paying ransoms, tailored to their geographical location.

RaaS enables ransomware operators to sustain their operations and profitably proliferate their strains. They achieve this by incorporating defense evasion techniques, such as disabling safety prompts when an application runs as an administrator on a user's system [6]. RaaS platforms allow even the least technically skilled actors to deploy ransomware and receive a share of the ransom through an affiliate framework [6] [7]. Darktrace observed significant cyber disruptions and data exfiltration in cases involving both LockBit and Black Basta, confirming likely double extortion intentions.

In the case of Black Basta, Darktrace identified it newly using the remote management tool AnyDesk, which was reportedly being used in their social-engineering campaigns [8]. Interestingly, Black Basta was also noted to be escalating attacks on hospitals and public health organizations, which correlates with the industry for the Black Basta activity observed by Darktrace [9].

To this point, ransomware actors are also seemingly becoming increasingly strategic in their selection of targets with critical infrastructure organizations, particularly the healthcare sector, becoming a primary target for ransomware attacks, likely owing to the fact threat actors know that these targets are more likely to pay a ransom. According to Recorded Future, there were 44 ransomware attacks targeting healthcare organizations in April alone [9], following an attack on US-based Change Healthcare reportedly perpetrated by AlphV/BlackCat, another ransomware group that Darktrace has investigated over the last 12 months [10].

The Emergence of Qilin Ransomware

Following several high-profile compromises at the beginning of 2024, Qilin ransomware has dominated conversations across the security landscape. Notably, this included an attack on the UK-based medical company Synnovis, which severely impacted patient services at multiple National Health Service (NHS) hospitals that utilized Synnovis diagnostic and pathology services [11]. As Qilin is a RaaS operation, the selection of targets reflects the intentions of its affiliates rather than those of the Qilin operators themselves. The TTPs and IoCs identified by Darktrace are therefore associated with the specific affiliates deploying Qilin ransomware for their own purposes, rather than to the Qilin group as a whole. Likewise, the initial vectors of infection may vary from affiliate to affiliate. Previous studies indicate that initial network access was typically gained via spear phishing emails or by leveraging exposed applications and interfaces [12].

During investigations of campaign-like activity associated to Qilin, Darktrace's Threat Research team observed data exfiltration activity via the File Transfer Protocol (FTP) to two IP addresses within the same Autonomous System Number (ASN) associated with Cobalt Strike command-and-control (C2) servers [12].

Darktrace analysts were able to perform a packet capture and analyze the connections to reveal that Qilin affiliates had attempted to exfiltrate sensitive financial, legal and accounting data. Darktrace has also observed actors in Qilin compromises attempting to exfiltrate data to IP addresses associated with the MEGA and AWS cloud storage solutions.

One notable feature of Qilin ransomware observed by Darktrace was its tactic of rebooting infected machines in safe mode, bypassing security tools and making it more difficult for human security teams to react. Actors would then intermittently encrypt a small number of files at a time, rather than in bulk, to evade signature and rule-based detection [12].

You can find the full blog post on Qilin ransomware here:

Qilin ransomware →

Insights from the Darktrace Security Operations Center (SOC)

The Darktrace Security Operations Centers (SOC), located in Cambridge (UK), San Francisco (US), and Singapore, provide 24/7 support to customers through our Managed Threat Detection and Security Operations Support services. As part of delivering SOC services, Darktrace expert cybersecurity analysts investigate a wide range of threats and establish trends observed across the fleet of SOC service customers. These insights have been illustrated in this report so readers can better understand the current threat landscape and support organizations and their security teams in bolstering their overall security posture.

Top Three Threats Observed by Darktrace's SOC

Edge Infrastructure Compromise:

Malicious actors are continuing to execute mass-exploitation of vulnerabilities in edge infrastructure devices to gain entry to organization's networks. Initial compromises of these systems can act as a springboard for malicious actors to conduct further activities, such as tooling, network reconnaissance, and lateral movement. The most widely exploited edge infrastructure devices observed were those related to Ivanti Connect Secure, JetBrains TeamCity, FortiClient Enterprise Management Server, and Palo Alto Networks PAN-OS.

Living Off Trusted Sites:

Darktrace's SOC observed an increase in attackers' leveraging popular, legitimate third-party services in their operations to evade detection. Malicious actors have been hosting payloads on reputable platforms such as Dropbox[13] and AWS, and exfiltrating data to equally trusted platforms like OneDrive. Using well-regarded services enables these threat actors to blend seamlessly into legitimate network traffic, significantly reducing the likelihood of detection by security tools. By leveraging trusted platforms, they can effectively evade suspicion and bypass conventional security measures that might otherwise identify or block malicious activity.

Covert C2 Mechanisms:

Darktrace observed a spike in cases of malicious actors' concealing their C2 infrastructure using remote monitoring and management (RMM), tunneling, and proxy tools/services. In many tracked cases, communication with compromised hosts was conducted via RMM services such as AnyDesk as well as via tunnelling services such as Cloudflare Tunnel (i.e., Cloudflared). In many instances, malicious actors transformed compromised hosts into C2 proxies via tools such as SystemBC, Ngioweb, and Mylobot. The increased utilization of covert C2 methods heightens their anonymity, making it harder for defenders to trace activities.

Monthly Breakdown of the Threats Observed by the SOC

The following table identifies what Darktrace's SOC considered to be the five most salient or noteworthy threats observed each month across the first six months of 2024.

January	February	March	April	May	June
Exploitation of vulnerabilities in Ivanti systems	Phishing via Dropbox's transfer service	Use of tunneling services such as Cloudflare Tunnel	Session cookie abuse to gain access to M365 accounts	Usage of eM Client in M365 compromises	VPN Exploitation
Data exfiltration with WinSCP and Rclone	Brute-forcing activity	Microsoft Teams-based phishing	Exploitation of vulnerabilities in FortiClient Enterprise Management Server (EMS) and Palo Alto Networks PAN-OS	Proxy botnet activity	Adversary-in-the-Middle (AiTM) phishing
Phishing via Microsoft's Customer Voice service	Exploitation of vulnerabilities in Ivanti systems	Exploitation of vulnerabilities in JetBrains TeamCity servers	Usage of RMM tools such as AnyDesk, Atera, and DWService	Insider threats	VPS Exploitation
Amadey info-stealer infections	Usage of RMM tools such as AnyDesk	SSH-based C2 activity	Usage of proxy tools such as Stowaway, SystemBC, and ProxyScrape	Data exfiltration to trusted file storage platforms	Detonation of ransomware strains such as Medusa and Akira
Usage of RMM tools such as AnyDesk and ConnectWise Control	Detonation of ransomware strains such as LockBit, Akira, and 8Base	Detonation of ransomware strains such as Akira and Phobos	Usage of PowerShell for ingress tool transfer	Addition of new MFA methods to compromised accounts	XMRig Crypto-mining

Exploitation of Critical Vulnerabilities is on the Rise

Darktrace has identified a significant rise in the exploitation of critical vulnerabilities by threat actors' aiming to gain initial access to target networks. This indicates that attacks are increasingly leveraging existing organizational infrastructure to gain access to target networks, rather than adding a new device.

Between January and June, in 40% of cases investigated by the Threat Research team, attackers were observed exploiting Common Vulnerabilities and Exposures (CVEs).

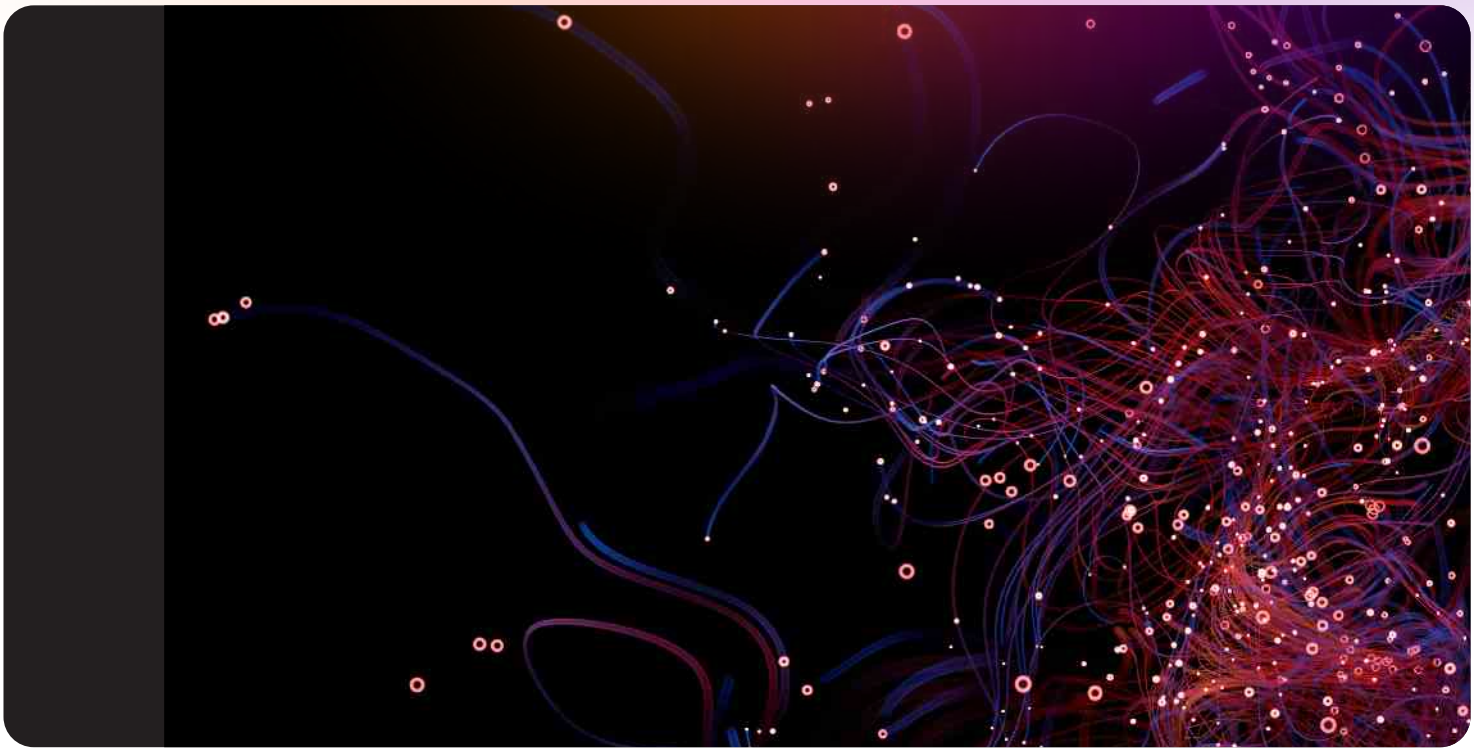
Ivanti Connect Secure and Ivanti Policy Secure

Following the disclosure of two critical vulnerabilities in Ivanti Connect Secure and Policy Secure (CVE-2023-46805 and CVE-2024-21887) in early January 2024, Darktrace detected post-exploit activities across several customer networks [14].

The exploitation of CVE-2023-46805 would enable attackers to bypass authentication controls and access restricted resources, while CVE-2024-21887 enables authenticated administrators to execute arbitrary commands on vulnerable appliances.

If exploited at once, these vulnerabilities would permit unauthenticated attackers to execute several commands on their targeted gateways.

Darktrace identified a variety of post-exploitation activity related to these CVEs, including C2 communication, data exfiltration, and the delivery of a Monero cryptocurrency miner. Given the widespread exploitation of these CVEs, it is likely that multiple threat actors or groups have targeted vulnerable devices in the wild. Darktrace identified a unified cluster activity suggesting that instances observed across the customer base may have been part of a specific coordinated campaign.



Palo Alto Networks PAN-OS

Darktrace's Threat Research team investigated post-exploitation activity of the CVE-2024-3400 affecting GlobalProtect within Palo Alto Networks (PAN-OS) firewalls across multiple customer environments in early 2024 [15]. Darktrace was able to identify a range of malicious activities both before and after the public disclosure of the CVE.

Darktrace detected probable Palo Alto Networks perimeter devices across the fleet carrying out a range of suspicious activities. This included DNS requests for, or TCP connections to, Out-of-band Application Security Testing (OAST) domains, likely signifying successful exploitation validation of the PAN-OS CVE. This was typically followed by HTTP GET and POST requests to rare endpoints on non-standard ports, often using a new user agent. Observed HTTP GET requests frequently returned malicious tooling like Sliver C2 [16] and Cobalt Strike.

Darktrace further identified HTTP POST requests to rare endpoints, many of which featured the URI /upload/ indicating the potential exfiltration of server configuration data such as password hashes and user accounts. Some affected devices were also observed establishing SSH connections with rare external IP addresses, indicating the establishing of C2 communication between affected devices and the attacker's infrastructure.

While it was not directly visible on all affected networks, Darktrace's investigation yielded evidence of multi-functional attacks, with additional payloads being dropped and attempts at further post-exploitation activity. Specifically, some downloaded files observed by Darktrace have been linked to known cryptocurrency mining strains by OSINT sources.

Timely updates and patches for network systems and edge infrastructure can help to address security flaws, reducing the attack surface for malicious actors. Effective patch management not only protects an organization's network and sensitive data but also ensures compliance with Data Loss Prevention (DLP) regulation, making it essential for maintaining both security and integrity. However, in cases where organizations were affected by undisclosed or newly discovered vulnerabilities, Darktrace was able to detect post-exploitation activity as soon as it emerged, in some cases before the CVE was publicly disclosed.

Email Trends

Building on the insights from the 2023 End of Year Threat Report, an analysis of malicious emails detected by Darktrace / EMAIL in 2024 underscores the implication that email threats are increasingly capable of circumventing conventional email security tools. Notably, 62% of the 17.8 million phishing emails identified by Darktrace successfully bypassed Domain-based Message Authentication, Reporting, and Conformance (DMARC) verification checks.

Between December 21, 2023, and July 5, 2024, Darktrace / EMAIL detected 17.8 million phishing emails across the fleet.

At least

1.5 million
- multistage payload emails were identified

4%
- of these emails utilized newly created domains

550,000
- malicious QR codes were detected within these emails

27%
- of these emails contained over 1,000 characters (around 200 words)

39%
- of these emails were identified as spear phishing attempts

33%
- of these emails were identified utilizing novel social engineering techniques

56%
- of these emails passed through all existing security layers

62%
- of these emails successfully passed DMARC authentication

Darktrace's Cyber AI Research Centre found that multistage payload attacks increased by an average of 59% across Darktrace customers between May and July 2023 [17]. These attacks typically include malicious emails attempting to elicit recipients to follow a series of steps, such as clicking a link or scanning a QR code, before delivering a payload or attempting to harvest credentials.

Analysis of Darktrace's email data further supports this trend, with over one million multistage payload emails having been identified. Moreover, Darktrace detected 550,000 malicious QR codes that, when scanned, would direct recipients to a malicious endpoint where attackers can infect a device with malware or steal a user's login credentials. While most traditional email security measures are not able to scan for QR codes, Darktrace / EMAIL is not only able to detect them but also identify their destination, blocking any emails found to lead to suspicious endpoints [18].

Darktrace's analysis of malicious emails has also revealed evidence of threat actors becoming increasingly targeted with their phishing attacks, with almost 40% of phishing emails identified as spear phishing attempts.

More interestingly still, in May and June alone, Darktrace identified 540,000 brand impersonation attempts (malicious email actors attempting to masquerade as trusted and reputable organizations to deceive recipients) and a further 240,000 emails attempting to impersonate a VIP at an organization.

This trend towards impersonation and deception under the guise of a trusted company, or even a company executive, suggests threat actors are curating more bespoke and targeted email campaigns intended to target select organizations, or even individuals, more efficiently than traditional mass phishing attacks.

Generative AI Usage

While the use of Generative AI services is generally seen as a compliance issue for security teams and defenders, it can also represent a significant data leakage concern. For example, OpenAI does not use API data to train its models but rather user input from the standard versions of ChatGPT and DALL.E [19]. This has the potential to expose sensitive information used as input to any user of the same Generative AI service.

With a greater variety of Generative AI products comes an increased risk of leakage due to the different services having different data usage policies [20]. This risk, and others, could potentially be mitigated through regulation. Given that Generative AI is relatively new technology, the full extent of these risks is still relatively unknown; understanding the prevalence of this new technology and how users interact with it will be important in identifying potential security holes in the future.

Between January 1 and June 30, 2024, around half of Darktrace customers were observed accessing Generative AI services.

During the same period, OpenAI was the most observed Generative AI service across Darktrace customers. 58% of all Anomalous Upload to Generative AI incidents involved OpenAI, making it the most used Generative AI service for data transfers.

Microsoft Co-pilot, Hugging Face, Otter AI, and Codium also featured amongst the most used Generative AI services for anomalous data transfers in this period.

Between January 1 and June 30, 2024, 53% of all regular connections to Generative AI services involved OpenAI, making it the most consistently used Generative AI service by Darktrace customers.

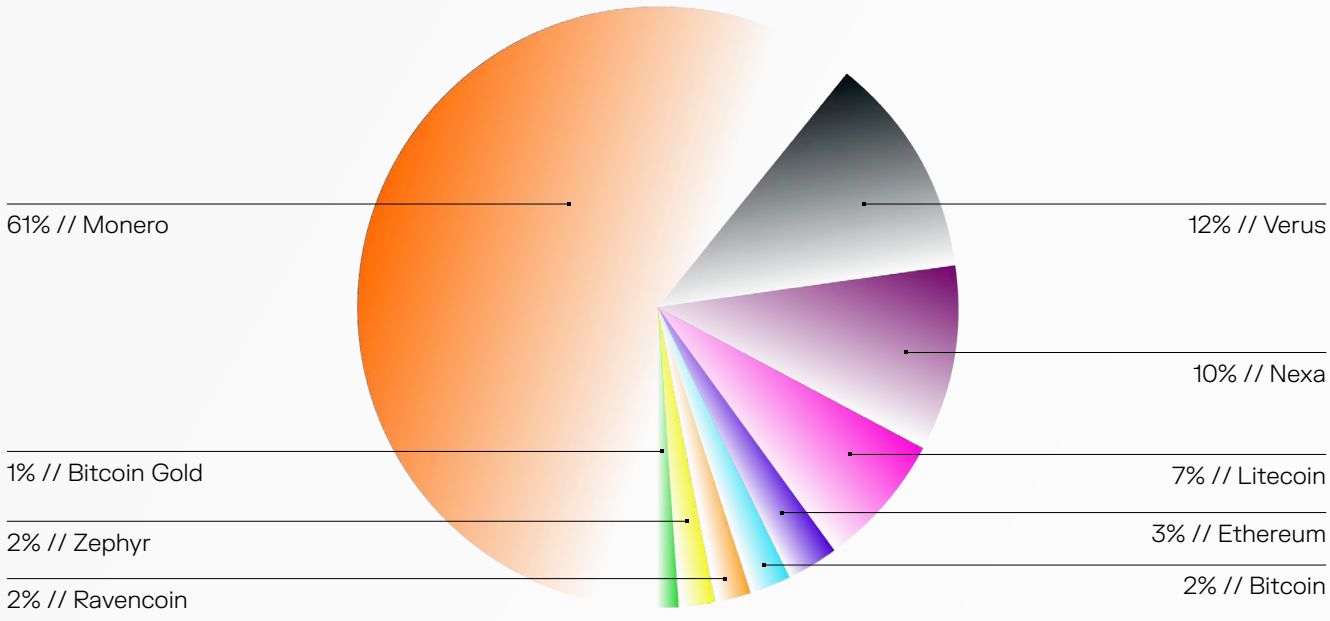
Microsoft Co-Pilot, Codium, Tab Nine, Otter AI, HuggingFace, Bing, Anthropic and StableDiffusion also featured amongst the most consistently used Generative AI services by users on Darktrace customers' networks.

Cryptocurrency Mining Activity Breakdown

The most identified coin being mined in cryptocurrency mining incidents observed by Darktrace between January 1 and June 30, 2024, was Monero, accounting for 61% of the observed coins.

While Monero is not ranked amongst the most popular or widely used cryptocurrencies [21], it remains the top choice for 'cryptojackers' likely due to its untraceable nature and lack of transaction history, offering attackers great anonymity compared to other currencies.

The most identified coins in cryptocurrency incidents observed by Darktrace in this period included:



Closing Comments

The threat landscape continues to evolve, but new threats often build upon old foundations rather than replacing them. While we have observed the emergence of new malware families, many attacks are carried out by the usual suspects that we have seen over the last few years, still utilizing familiar techniques and malware variants. This indicates that cyber threats persist due to the abundance of exploitable vulnerabilities.

The number of active cyber groups is at an all-time high.

Some groups specialize in specific technologies, such as VPNs, firewalls, or file transfer products, and are able to quickly exploit the latest patches thanks to their understanding of the underlying components. Security teams should therefore regularly assess the necessity of routinely compromised devices as part of their risk management efforts.

Ransomware continues to be the most impactful threat to Darktrace customers. With the growth of the RaaS marketplace, which offers a variety of customizable strains that can be adapted from one campaign to the next, even attackers with minimal technical prowess can launch sophisticated ransomware attacks.

Threat actors are increasingly using a combination of custom intrusion tools and publicly available tools throughout the attack life cycle. Beyond exploiting the latest vulnerabilities, Darktrace has observed a growing trend in attackers' leveraging popular, legitimate third-party services in their operations to evade detection and employing cover C2 methods to maintain anonymity, complicating efforts to trace their activities.

As threat actor activities rise, it is crucial for security teams to adhere to best practices to ensure robust preparation and resilience in the event of a cyber incident.

Therefore, Darktrace's Threat Research team recommends:

/ Staying up to date with the evolving threat landscape

/ Understanding the business impact of losing critical data

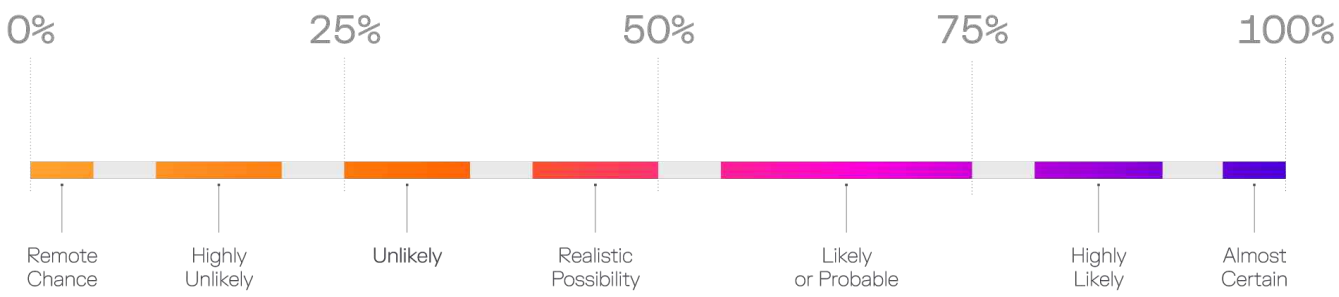
/ Identifying exposed assets

/ Assessing internal and external readiness

/ Reviewing and testing incident response plans

/ Implementing Zero Trust policies and principles

Appendices



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

Sign1	AsyncRAT
NjRAT	pupy
Loki Password Stealer (PWS)	Dridex
Gootloader	MacOS/Adload
Emotet	SolarMarker
FAKEUPDATES	Remcos
Raspberry Robin	xmrig
Mirai	Viper RAT
TA577	RedLine Stealer
XOR DDoS	BlueSky

References:

1. Darktrace Inside the SOC Blog: Understanding Amadey Info-Stealer
   https://darktrace.com/blog/amadey-info-stealer-exploiting-n-day-vulnerabilities
2. Darktrace Inside the SOC Blog: Darktrace Investigates Raspberry Robin
   https://darktrace.com/blog/the-early-bird-catches-the-worm-darktraces-hunt-for-raspberry-robin
3. Darktrace Inside the SOC Blog: How Darktrace Stopped Akira
   https://darktrace.com/blog/akira-ransomware-how-darktrace-foiled-another-novel-ransomware-attack
4. Darktrace Inside the SOC Blog: Lockbit Ransomware Analysis
   https://darktrace.com/blog/lockbit-ransomware-analysis-rapid-detonation-using-a-single-compromised-credential
5. Darktrace Inside the SOC Blog: Black Basta
   https://darktrace.com/blog/black-basta-old-dogs-with-new-tricks
6. CISA: LockBit Advisory
   https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
7. CISA: Black Basta Advisory
   https://www.cisa.gov/news-events/alerts/2024/05/10/cisa-and-partners-release-advisory-black-basta-ransomware
8. Rapid 7: Ongoing Social Engineering Campaign Linked to Black Basta Ransomware Operators
   https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators/
9. Wired: Medical-Targeted Ransomware Is Breaking Records
   https://www.wired.com/story/change-healthcare-22-million-payment-ransomware-spike/
10. Darktrace Inside the SOC Blog: Protecting Against AlphV/BlackCat
    https://darktrace.com/blog/no-bad-luck-for-darktrace-combatting-alphv-blackcat-ransomware
11. BBC: NHS confirms patient data stolen in cyber attack
    https://www.bbc.co.uk/news/articles/c9777v4m8zdo
12. Darktrace Inside the SOC Blog: A Busy Agenda
    https://darktrace.com/blog/a-busy-agenda-darktraces-detection-of-qilin-ransomware-as-a-service-operator
13. Darktrace Inside the SOC Blog: Legitimate Services, Malicious Intent
    https://darktrace.com/blog/legitimate-services-malicious-intentions-getting-the-drop-on-phishing-attacks-abusing-dropbox
14. Darktrace Inside the SOC Blog: Post-Exploitation Activities of Ivanti CS/PS Appliances
    https://darktrace.com/blog/the-unknown-unknowns-post-exploitation-activities-of-ivanti-cs-ps-appliances
15. Darktrace Inside the SOC Blog: Post-Exploitation Activities on PAN-OS Devices
    https://darktrace.com/blog/post-exploitation-activities-on-pan-os-devices-a-network-based-analysis
16. Darktrace Inside the SOC Blog: Sliver C2
    https://darktrace.com/blog/sliver-c2-how-darktrace-provided-a-sliver-of-hope-in-the-face-of-an-emerging-c2-framework
17. Darktrace Blog: Defending Against Personalized Cyber Attacks
    https://darktrace.com/blog/attacks-are-getting-personal
18. Darktrace Blog: Phishing with QR Codes
    https://darktrace.com/blog/phishing-with-qr-codes-how-darktrace-detected-and-blocked-the-bait
19. OpenAI: Enterprise Privacy
    https://openai.com/enterprise-privacy/
20. EWeek: AI Privacy Issues
    https://www.eweek.com/artificial-intelligence/ai-privacy-issues/
21. Forbes: Top 10 Cryptocurrencies for July 2024
    https://www.forbes.com/uk/advisor/investing/cryptocurrency/top-10-cryptocurrencies-july-2024/

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

darktrace.com // info@darktrace.com