DARKTRACE

WHITE PAPER

First 6: Half-Year Threat Report

Darktrace Analysis

CONTENTS

Darktrace analysis has assessed a broad variety of threats during the first 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 identified, known tooling. All of the insights provided by Darktrace analysis are centered on the detections and specific data made available through our AI applications and anomaly investigations.

Toby Lewis,
Global Head of Threat Analysis

Foreward

Firstly, let me welcome you to our first six-month Threat Report. Whilst we've been pulling together insights such as these for some time, this is the first time we've pulled it together in one place such that you can see some of the same trending information upon which we base a lot of our own assesments.

Threat Intelligence works a little differently at Darktrace than most traditional security houses. The core of our detection methods is not patterned playbooks based on previous attacks but rather a clear understanding that behavioral anomalies will always yield valuable results for security teams looking to identify both known and unknown threats. Malicious activity that could look benign in any other organization and may be bypassed by tools looking only for specific use cases is detected and responded to through Darktrace's unique AI-driven approach.

Because of Darktrace's focus on anomalies and behavioral analysis, combined with our unparalleled combination of several AI applications, Darktrace's Cyber AI Loop™ often detects and mitigates threats which have yet to be publicly attributed. Hindsight analysis with additional cyber security context allows us to highlight that many of threats, including Zero Days, N Days, and various other novel and identified threats, have taken new shape.

For our customers, the primary focus and outcome is that an unwanted threat has been detected (by Darktrace DETECT™) and contained, often using our autonomous Darktrace RESPOND™ capability. For our analysts, this is where the exploration begins, looking to map those mitigated cases over to some of the more publicly attributed threats which the Threat Intelligence community is working to combat.

At a micro level, we present many of our findings on individual cases or campaigns through our Inside the SOC blog series. At a macro level, we have the ability to present you some of the trending and observations in this report. As a new product for us, we'd be grateful for any feedback you can provide - please reach out to us at threatintelligence@darktrace.com.

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 Darktrace's anomaly detection and revolves around analysis and contextualization of detection information per- formed by the Threat Research team.

In this first 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) remain extremely prominent in the cyber threat land- scape and are the most consistently identified threat affecting the Darktrace customer fleet. Darktrace assesses MaaS and RaaS as the most likely threats to affect the majority of organizations and will continue to be the most relevant threat for most organizations throughout the rest of 2023 and likely 2024.

MaaS and RaaS threats come in a variety of forms, with many of them including tailorable or bespoke elements which can be altered campaign to campaign. Darktrace assesses with moderate to high confidence that this trend of tailorable or combined threats will continue to dominate the cyber threat ecosystem, as more malware developers combine code, use open-source repositories, and possibly even learning from Threat Intelligence that reverse engineers other strains.

Darktrace has analyzed campaign-like activity affecting the fleet and identified the following threats as the most observed according to case volume. Many of these threats, such as CobaltStrike and Mirai, are observed alongside malware offerings including QakBot malware and Hive ransomware.[1] [2]

> Malware-as-a-Service strains are the most observed threats affecting Darktrace customers, consistent with their prevalence in the wider cyber threat landscape.

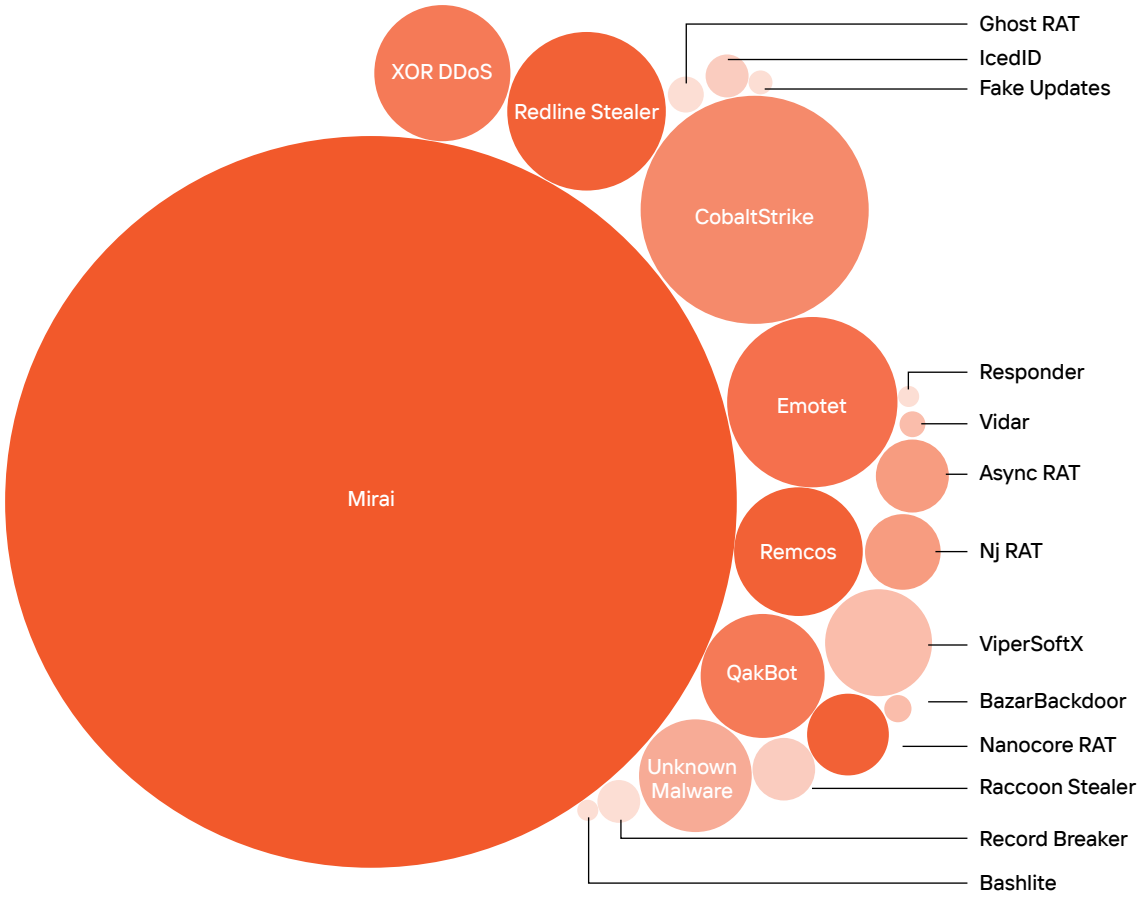

Figure 1: Most observed threats by volume as investigated by the Darktrace Threat Research team, with relative size representative of the proportional scale of observation by Darktrace. A full list of threats can be found in the Appendices.

Darktrace's analysis of threat indicators and Threat Intelligence, including threats with limited evidence of impact to the Darktrace fleet, suggests that many malware strains, specifically in the MaaS ecosystem, are utilizing cross-functional components from other strains as part of their evolution and customization.

This 'Frankenstein' approach is evidenced by analysis of several malware strains currently observed both in the cyber threat landscape and within Darktrace's insights. Threat actors are likely to make use of one or more readily available tools in their deployment of even novel strains of ransomware, the most infamous example of this being Cobalt Strike.

Cobalt Strike started as a paid penetration testing product which includes functionality such as command execution, key logging, file transfer, privilege escalation, port scanning, and lateral movement.[3] Cobalt Strike has become synonymous with malware as multiple malware families, such as Bumblebee, QakBot, and Royal, utilize Cobalt Strike as part of their payloads.[4] [5] Cobalt Strike is a representative example of similar utilization of external tools by threat actors to create and deliver multi-facetted malware and ransomware, especially in "as-a-Service" offerings.

Darktrace's Threat Research team assesses this 'Frankenstein' approach will very likely increase, as use of open-source code such as leaked Conti and Babuk code and the growth of the MaaS marketplace continues across the threat landscape.

Signposts: Key signals to indicate 'Frankenstein' approach to malware and ransomware is increasing:

- Reverse engineering reveals portions of new malware strains which have code adopted from open-source leaks or already identified threats that have been sold on the MaaS market
- IoCs become less and less mutually exclusive between malware strains as compromised infrastructure is used by multiple threat actors through access brokers or the "as-a-Service" market

Interesting Threat Finds: First Half of 2023

Hive Ransomware-as-a-Service

Hive ransomware is a relatively new strain that was first observed in the wild in June 2021. It is known to target a variety of industries including healthcare, energy providers, and retailers, and has reportedly attacked over 1,500 organizations, collecting more than USD 100m in ransom payments[6].

Hive is distributed via a RaaS model where its developers update and maintain the code, in return for a percentage of the eventual ransom payment, while users (or affiliates) are given the tools to carry out attacks using a highly sophisticated and complex malware they would otherwise be unable to use. Hive uses typical tactics, techniques and procedures (TTPs) associated with ransomware, though they do vary depending on the Hive affiliate carrying out the attack.

Owing to the highly customizable nature of RaaS, the tactics and methods employed by Hive actors are expected to differ on a case-by-case basis. Nonetheless in the majority of Hive ransomware incidents identified on Darktrace customer environments, Darktrace DETECT observed the following general attack stages and features. This is possibly indicative of the attacks originating from the same threat actor(s) or from a widely sold batch with a particular configuration to a variety of actors.

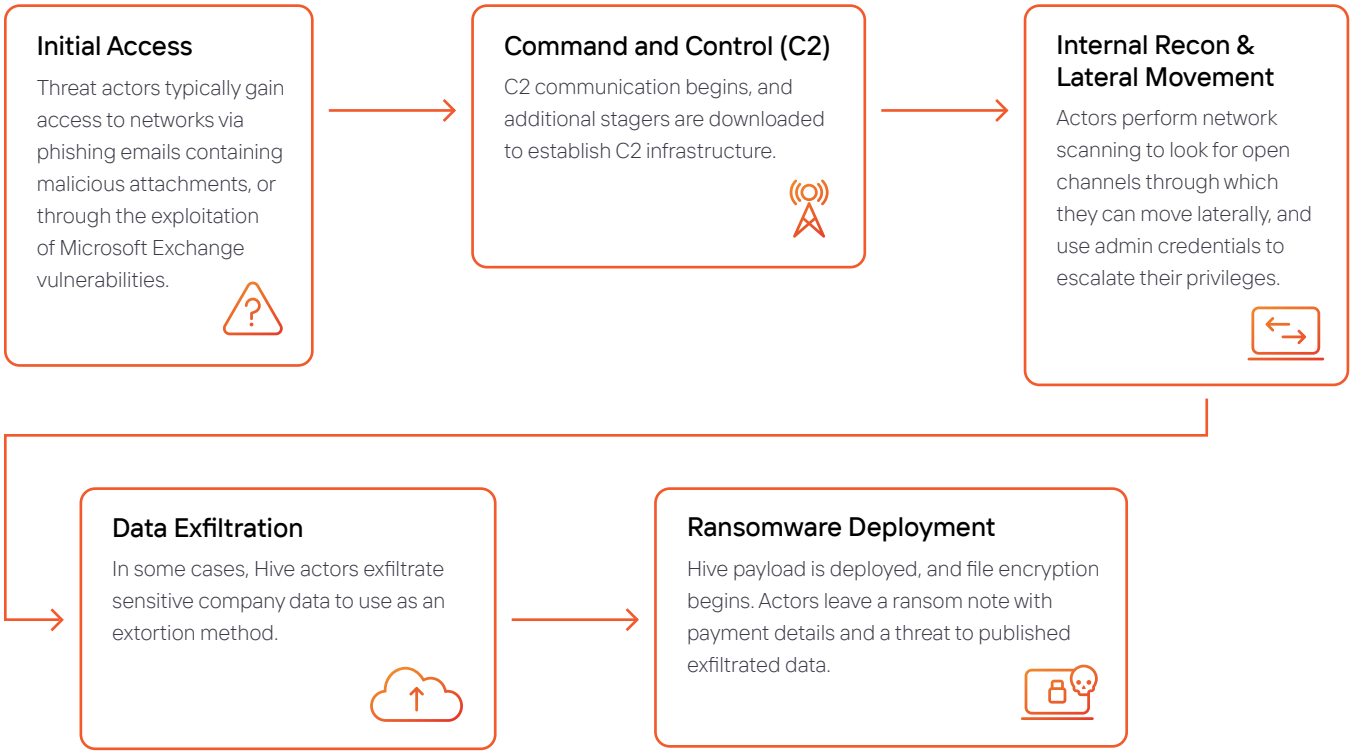

Figure 2: A typical attack progression of Hive ransomware attacks observed by Darktrace.

In some cases of Hive, a few key tools are used in Hive's download of stagers and privilege escalation, namely CobaltStrike and Mimikatz. CobaltStrike command and control servers are used to download additional stagers after the execution of malicious PowerShell code. Mimikatz is used at the next phase to move laterally as part of a 'pass-the-hash' attack leveraging System permissions to create a new system administrator and dump additional credentials.

Hive is just one of many RaaS offerings currently on the market, and this market is only expected to grow in usage and diversity of presentations. Ransomware strains like Hive are very likely to go from newly seen in the wild to either partially or fully sold on MaaS and RaaS marketplaces given the demand and potential profit.

PlugX Malware

In early 2023, Darktrace's Threat Research team identified multiple cases of PlugX malware affecting the customer base. PlugX is a Chinese Remote Access Tool (RAT) which has been identified in use since at least 2008. It is known for its modularity and plug-in-style approach to malware development.

The RAT has reportedly been used by Chinese APT groups like Mustang Panda and has featured in multiple high-profile attacks over the years, such as the targeting of governmental officials in several countries in Europe, the Middle East, and South America in late 2022 [7].

Traditionally, DLL-side loading is used to load a malicious PlugX payload via a trusted software application. PlugX has been distributed in a variety of ways including via malicious files on USB devices, exploiting vulnerabilities in remote software, and within malicious email attachments. Late last year it was reported by researchers that PlugX had been delivered via spear phishing campaigns [8].

According to Darktrace researchers, the PlugX malware utilized fixed user agents, namely "Mozilla/5.0 (Windows NT 10.0;Win62;x64)AppleWebKit/537.36" for HTTP connections. Darktrace DETECT observed multiple connections per affected client to identified PlugX command and control (C2) infrastructure, primarily via ports 80, 110, 443, and 5938.

In one case detected by Darktrace, additional connections to a suspicious domain (clipper[.]guru) were observed suggesting the possible presence of Laplas Clipper malware [9], either as part of the PlugX compromise or concurrently.

PlugX is a RAT that can be used to remotely control affected devices. It has a range of modules that provide various capabilities including rebooting systems, keylogging, managing system processes, and file upload and download. In addition, the newest variant of the PlugX malware has been reported to continuously monitor for new USB devices to infect, allowing it to spread further. It has also been observed creating a directory containing a collection of stolen documents, likely in preparation for exfiltration via its C2 channels.

PlugX malware is a tool most associated with espionage, but which now appears to be deployed more broadly against a less discerning target list, likely either for informational or financial gain. It is a realistic possibility that this pattern of behaviour indicates the threat actors developing PlugX are selling access to the tool. The evolution of previously espionage-centric malware into commonly used attack tooling will very likely continue as the demand for malware continues to increase in the MaaS and RaaS marketplaces.

SOC Trends

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

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.

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 clients.

The Darktrace SOC has observed ransomware, malicious use of existing tooling, and business email compromise as the most significant trends across the customer base in the first half of 2023.

Ransomware

Techniques observed include living off the land, exploitation of internet-facing infrastructure, Ngrok, MEGA, WinSCP to conduct C2 and data exfiltration, and initial access via account credentials or internet-facing infrastructure.

Strains observed include Play, BlackByte, LockBit, Cuba, Akira, ALPHV, Elbie, and Black Basta.

Malicious Use of Existing Tools

Techniques observed included dynamic DNS for C2, such as Duck DNS, MFA-based persistence by registering authentication to compromised accounts, SmbExec for lateral movement, and Nmap and Netscan for internal reconnaissance and lateral movement.

Business Email Compromise

Techniques observed include Paypal abuse for phishing, sophisticated phishing via multiple links, file storage endpoints, and RSS feeds, brand impersonation, and inbox rule creations following account compromise to obfuscate malicious activity.

The Darktrace SOC reported the most prevalent trends identified through investigations of customer environments in the first six months of 2023 as ransomware, malicious use of existing tools, and business email compromise. The most common strains of the ransomware observed included Play, BlackByte, LockBit, Cuba, Akira, ALPHV, Elbie, and Black Basta. Another key trend identified was compromise via the exploitation of vulnerabilities in edge infrastructure, such as exploitation of the PaperCut vulnerability (CVE-2023–27350) and Microsoft Exchange server vulnerabilities.

Monthly Trends: First Half of 2023

January	February	March	April	May	June
Fake software websites / "cracked" software	Paypal abuse for phishing	Application registration: [Azure] new applications on compromised credentials	PaperCut vulnerability exploitation	QakBot initiated via PowerShell HTTP GET requests to external endpoints with target URIs often followed by CobaltStrike and ransomware activity	Cloud account hijacks abusing stolen credentials or session cookies to gain entry
Info-stealing malware such as Raccoon and Vidar	Denial of Service (DoS)	MFA persistence via registering applications on compromised accounts	Exchange server compromise	Cryptomining	Brand impersonation
Dynamic DNS such as Duck DNS and No IP	QakBot and QakNote	Sophisticated phishing including multiple links, file storage, and RSS feeds	QakBot	Nmap for internal reconnaissance or lateral movement	Netscan for reconnaissance prior to ransomware
Laplas Clipper malware	WinSCP for data exfiltration	Internet-facing server compromise such as RDP and Exchange	SmbExec for lateral movement	Ransomware with initial access via compromised account credentials or internet-facing infrastructure	File Transfer Protocol-based data exfiltration (FreeFileSync)
Ransomware with living off the land TTPs	Ransomware via internet-facing infrastructure and utilising AnyDesk	Ransomware via internet-facing infrastructure including utilisation of CobaltStrike	Ransomware using Ngrok, MEGA, and WinSCP to conduct C2 and data exfiltration	Inbox rule creations as part of account compromise and business email compromise	Ransomware such as LockBit, ALPHV, Akira, and Elbie.

AI Insights and Incident Statistics

Methodology: The following statistics cover anomalous activity detected across the global Darktrace customer base from January 1, 2023 to June 30, 2023, using modelling data from Enhanced Monitoring models and Cyber AI Analyst™ data. The data from Darktrace modelling 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 modelling data points. The data does not take into account the proportion of customers in sectors or customer growth, as per industry standard. MITRE tactics and techniques have been included as they are mapped to both Darktrace modelling and pattern analysis in Enhanced Monitoring models and AI Analyst data, respectively.

AI Analyst Statistics

The following statistics cover anomalous activity detected across the global Darktrace customer base between January 1 and June 9, 2023, and were produced using Cyber AI Analyst data and takes 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 modelling 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 modelled within DETECT. Cyber AI Analyst investigations are designed to produce reports on the most interesting and high-priority activity observed by Darktrace within a client environment.

The most observed patterns of activities identified by Cyber AI Analyst between January and June 2023 were Beaconing.

Beaconing is indicative of Command and Control activity as per the MITRE attack tactics categorization. The other most observed AI Analyst patterns of activity during the same period included:

- Scanning (Discovery and Reconnaissance MITRE attack tactic)
- HTTP Agent (Command and Control MITRE attack tactic)
- SaaS Hijack (Privilege Escalation MITRE attack tactic)
- Lateral Movement (Lateral Movement MITRE attack tactic)

The most observed MITRE tactic across Cyber AI Analyst investigations between January and June 2023 was Lateral Movement.

The other most observed MITRE tactics included:

- Command and Control
- Credential Access
- Compliance
- Discovery and Reconnaissance

Cyber AI Analyst observed more patterns of activities from customers in the Manufacturing sector than any other sector between January and June 2023.

The other sectors with the most observed activity included::

- Information and Communication
- Financial and Insurance
- Human Health and Social Work
- Education

Incident Statistics

The following statistics cover anomalous activity detected across the global Darktrace customer base between January 1 and June 9, 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 modelling within DETECT.

During the first six months of 2023, the most observed probable cyber incidents were Multiple Lateral Movement breaches.

Within the wider behavioral modelling across the Darktrace fleet DETECT product suite, the most observed probable cyber incidents between January and June 2023 were Multiple Lateral Movement breaches. As per the MITRE attack tactics categorization, this is indicative of Lateral Movement. The other most observed probable cyber incidents during the first six months of 2023 were Suspicious Network Scanning, Crypto Currency Mining, Unusual External Data Transfer, and SaaS Login from Rare Location Following Suspicious Login Attempts.

During the first six months of 2023, the proportion of SaaS-related incidents compared with all observed probable cyber incidents remained consistent across Darktrace's global customer base.

In the past six months, Darktrace observed that SaaS Enhanced Monitoring model breaches accounted for more than 25% of Enhanced Monitoring model breaches, and 25% of the global probable cyber incidents observed.

Observations and Predictions

"As-a-Service" Markets Create Demand for Bespoke Malware and Widens Threat Actor Talent Pool

Over the last year, the threat landscape has seen a drastic increase in both the variance and customizability of malware as the Malware- and Ransomware-as-a-Service markets continue to increase. Previous years would have seen household names such as Conti or Lockbit as the focal point of malware and ransomware development, making attribution simpler and the development speeds markedly slower for new variants. Previously, the landscape was almost certainly more dependent on vulnerability release than malware and ransomware development, with household name threat actors very likely focused on causing significant damage and entry vectors, rather than on producing a wide variety of samples.

With this recent increase in the variance and bespoke nature of malware and ransomware strains, security teams have more to be aware of than ever before, which can make for sleepless nights. Staying on top of the evolving threat landscape is a more and more monumental task. Whether its keeping up with the development of hundreds if not thousands of new strains of malware, completely novel adaptations of leaked source code, such as Babuk or Conti, or "plug and play" tailoring of malware or ransomware with other existing tooling such as Cobalt Strike or loader variants, the race to stay ahead is becoming a futile task.

Similarly, the threat actor pool is demonstrably widening and with it, motivations for attacks, which are always a murky pool, are becoming increasingly difficult to identify. With the rapid growth of the "as-a-Service" marketplaces for malware, ransomware, and even now phishing campaigns, there is a class of threat actor which heretofore has been excluded from cybercrime due to necessary skills. The cybercrime skill gap is almost certainly shrinking to the point that even the most novice individual can deploy bespoke malware with the help of customer service support and step by step instructions, giving organizations more to worry about than the big label ransomware gangs and nation-states alone.

This democratization of malware and ransomware through the "as-a-Service" markets creates challenges for defenders, as cyber criminals can now order bespoke malware, ransomware, or phishing kits, purchase credentials through initial access brokers, and could require little to no technical prowess or social engineering. For defenders who have prepared their strategies for more mainstream malware and ransomware, or who have based playbooks on specific threats or scenarios involving financial or political motivation, this could create large gaps in their security posture.

Interconnectivity of Technology "By Design" and the Challenges It Creates for Defenders

At the same time as the market for malware and ransomware has a demand and supply increase, technologies are continuing to evolve and change which could present additional issues for defenders. Previously, technologies were accepted to work for specific purposes and within specific areas of a business. For example, accountancy software was not required to work with developer production environments. These could naturally, by design, exist separately with few complaints.

With the continuing push for Cloud integration and virtualization, more and more businesses are demanding integration by design for their technologies, both within the cyber security space and normal business operations. Across industries, greater volumes of technologies and software are being designed specifically to integrate with other technologies to create a "one-stop shop", evidenced by key integrations like Microsoft's product suites and Cloud, AWS and Google programmatic workspaces, and other large providers. More and more technology is being intentionally integrated into either email or virtual data storage to increase efficiency and ease of work.

With these massive technological changes, so comes cyber risk increases. This interconnectivity of technology by design creates previously unavailable pathways between services and devices which can be exploited by threat actors. With the standardization of multi-factor authentication (MFA) across most organizations as a baseline of security, single sign-on access creates a potential portal of mass access for threat actors if they can simply gain a credential or, in some cases, perform successful business email compromise.

So, What's Next?

Cascading Supply Chain Attacks

The interconnectivity of technology is critical for business scaling and innovation but can create serious cyber security drawbacks, such as cascading supply chain attacks. The 3CX supply chain attack reported earlier this year was diagnosed as a cascading supply chain attack following additional research by incident responders [10] [11]. The researchers found that the 3CX supply chain attack was caused by a separate supply chain attack to X_Trader, a platform for real-time and historical trading markets. The X_Trader website was reportedly compromised by North Korean hackers which led to the 3CX supply chain attack after a 3CX employee downloaded an affected version of the X_Trader software. Although this specific incident may not have occurred by design, it is possible that threat actors will aim to affect multiple technology platforms through cascading supply chain attacks in future. Similarly, due to the increasing variety of technologies incorporated into organizations' supply chains, it is likely cascading supply chain attacks will become more frequent.

With a widening pool of supply chains enabled by interconnective and adaptable technology, there will likely be a continuation of cascading supply chain attacks, whether by design or due to accidental spread of tainted technology.

Cloud-Focused Identity Targeting

The "simply logging in" hack has become extremely prevalent with the increasing push from organizations toward Cloud infrastructure incorporation and remote working. Previous data pools which would have been only stored on-premises are now accessible via common working tools, like SharePoint, which make a threat actor gaining the ability to "simply log in" a potential disaster, not only from a data loss perspective but also access to intellectual property or even further credentials to escalate privileges. The targeting of SaaS and applications as a primary attack vector has seen a steady increase in the global cyber threat landscape over the past five years owing to the increasing reliance on Cloud infrastructure.

As organizations are still largely reliant on passwords to access SaaS and applications, and MFA, though growing in popularity, is seen as an additional exploitable vector, it is very likely Cloud-focused identity targeting will continue to be a significant attack vector.

Appendices

Figure 4: 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
- Cobalt Strike
- Emotet
- RedLine Stealer
- XOR DDoS
- Remcos
- QakBot
- Unknown malware
- ViperSoftX
- Nanocore RAT
- NjRAT
- AsyncRAT
- Raccoon
- IcedID
- RecordBreaker
- Ghost RAT
- BazarBackdoor
- Vidar
- FAKEUPDATES
- Bashlite
- Responder

Darktrace Analysis: Inside the SOC Blogs

References

1. Darktrace Analyst Blog: Qakbot Resurgence
https://darktrace.com/blog/qakbot-resurgence-evolving-along-with-the-emerging-threat-landscape
2. Darktrace Analyst Blog: Hive Ransomware-as-a-Service
https://darktrace.com/blog/tracking-the-hive-darktraces-detection-of-a-hive-ransomware-as-service
3. Malpedia description: Cobalt Strike
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike
4. Darktrace Analyst Blog: BumbleBee Malware
https://darktrace.com/blog/from-bumblebee-to-cobalt-strike-steps-of-a-bumblebee-intrusion
5. Microsoft Threat Intelligence: Royal Ransomware Payloads
https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/
6. Darktrace Analyst Blog: Hive Ransomware-as-a-Service
https://darktrace.com/blog/tracking-the-hive-darktraces-detection-of-a-hive-ransomware-as-service
7. ComputerWeekly Report: PlugX Malware
https://www.computerweekly.com/news/252524710/Chinese-APT-using-PlugX-malware-on-espionage-targets
8. Bleeping Computer: PlugX Malware via USB
https://www.bleepingcomputer.com/news/security/plugx-malware-hides-on-usb-devices-to-infect-new-windows-hosts/
9. Darktrace Analyst Blog: Laplas Clipper Malware
https://darktrace.com/blog/laplas-clipper-defending-against-crypto-currency-thieves-with-detect-respond
10. TechCrunch Blog: 3CX Compound Supply Chain Attack
https://techcrunch.com/2023/04/20/3cx-supply-chain-xtrader-mandiant
11. Darktrace Analyst Blog: 3CX Cascading Supply Chain Attack
https://darktrace.com/blog/3cx-supply-chain-compromise-how-darktrace-uncovered-a-smooth-operator

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 in over 145 patent applications filed. Darktrace employs over 2,200 people around the world and protects c.8,800 organizations globally from advanced cyber-threats.

Scan to LEARN MORE