DARKTRACE

Annual Threat Report 2025

Evolving Threats and Emerging Tactics in Cybersecurity

Contents

Foreword

from Darktrace's Threat Research team

It is with great interest and growing concern that we present our findings for the 2025 Annual Darktrace Threat report. At Darktrace, we approach threat intelligence with a non-traditional perspective, rooting in the belief that identifying behavioral anomalies is crucial for identifying both known and emerging threats in the landscape.

While continuing to understand the threat landscape, we also have shifted to a more proactive approach to applying our methodologies across different data elements, threat hunting techniques, and community engagement across the cyber industry. We believe this type of approach will not only improve early warnings to our customers but also provide insight to different critical infrastructure sector issues for the broader community.

As we continue to evolve in an increasingly digital world, there are a few takeaways and observations that we would like to highlight. Attackers are focusing more on evasion via edge device vulnerabilities, Living-off-the-Land (LOTL), while also taking advantage of compromised Software-as-a-Service (SaaS) credentials, highlighting that identity continues to be an expensive problem across the estate and a persistent source of pain across enterprise and business networks.

Throughout 2024, we observed multiple threat trends across Critical National Infrastructure (CNI), with one key observation being the intensified race to identify software vulnerabilities. In 2020 MITRE listed roughly 18,000 vulnerabilities, while the current list for 2024 exceeds 29,000 [1].

There are a few explanations for this increase: the growth in Common Vulnerabilities and Exposures (CVE) Numbering Authorities (CNAs), with greater emphasis on finding vulnerabilities through academic research, maturing "bug bounty" programs, and ongoing research.

While the total number of **vulnerabilities worldwide is around 240,000**, it is important to note that the U.S. Cybersecurity and Infrastructure Agency's (CISA) Known Exploited Vulnerability (KEV) catalog lists just **over 1,200 vulnerabilities as being actively exploited** [2]. While threat actors continue to evade detection as much as ever, understanding a smaller scope of edge network technology allows for repeated reverse engineering and continued exploit findings, enabling zero-day discoveries and initial access [3].

Ransomware groups are evolving their tactics beyond phishing to include interactions with IT teams to elicit information to improve access, SaaS-based attacks, and even studying file-transfer technology for rapid exploitation and double extortion methods. For IT administrators and practitioners, it is crucial to prioritize your vulnerability management program and establish possible attack paths across your estate to prevent unauthorised access. This includes applying best practices across the business and wider IT teams. Impact to CNI is a continued and growing concern with the applications of AI-based capabilities for both offensive and defensive teams [4].

The following sections of our Threat Report discuss these broader concerns at a landscape level and how the Darktrace Threat Research team's findings mirrored a number of these concerns.

A huge thank you

to the Darktrace Analyst team members and colleagues across the wider business for their invaluable insights and contributions to this report:

Adam Potter, Alexandra Sentenac, Anna Gilbertson, Daniela Alvarado, Dylan Hinz, Emma Foulger, Freek Klein, Iris Isac, Justin Frank, Justin Torres, Maria Geronikolou, Min Kim, Nahisha Nobregas, Nathaniel Jones, Nicole Wong, Ryan Traill, Safiy Soel, Sam Lister, Steven Sosa, Vivek Rajan, Weronika Walczak and Zoe Tilsiter.

Methodology and Caveats

This 2025 Annual Darktrace Threat Report is intended for informational purposes only and is based on data, trends, and analysis available at the time of publication. The contents of this report reflect the best understanding of current and emerging threats in the cybersecurity landscape. The information provided is not exhaustive, and the nature of cybersecurity threats can evolve rapidly.

While efforts have been made to ensure the accuracy and reliability of the data and insights presented, Darktrace does not guarantee the completeness or accuracy of the information. Furthermore, Darktrace makes no representations or warranties, either express or implied, regarding the effectiveness, sufficiency, or applicability of the information provided in this report.

The findings and conclusions expressed in this report are those of Darktrace and do not necessarily reflect the views or endorsement of any third parties. Readers are encouraged to conduct their own independent assessments and consult with cybersecurity professionals to address specific security needs. Darktrace is not liable for any direct, indirect, or consequential damages arising from the use of or reliance on the information provided in this report.

Darktrace's Threat Research methodology

Darktrace's Threat Research team conducts extensive research across customer deployments to identify active threats, pinpoint key Indicators of Compromise (IoCs), and provide relevant threat intelligence.

This research leverages Darktrace's anomaly-based detection and involves thorough analysis and contextualization by the Threat Research team. Detected threats are promptly reported to the relevant customer security teams. When a customer has Darktrace's Autonomous Response technology enabled, these threats are swiftly mitigated to prevent escalation.

Between January 1 and December 31, 2024, Darktrace investigated a wide range of cyber threats. Many were identified as campaign-like activities targeting multiple customers. All insights from Darktrace's analysis are based on detections and specific data from our AI-driven applications and anomaly investigations.

'Critical exploited vulnerabilities according to Darktrace' methodology
The 'Most commonly observed exploited vulnerabilities' listed in the 'Critical Exploited Vulnerabilities According to Darktrace' section are based on confirmed exploitation attempts identified across multiple customers using Darktrace / NETWORK. These vulnerabilities, which affected the most Darktrace customers between January 1 and December 31, 2024, are those where we have triaged compromise activities that align with confirmed IoCs, ascertained through our internal threat research and Open-Source Intelligence (OSINT).

'A view from the SOC' methodology
The observations in the 'A View from the SOC' section of this report are based on high-fidelity inputs analyzed through Darktrace's Managed Threat Detection and Security Operations Support services. This analysis, conducted between January 1 and December 31, 2024, involves both pattern analysis and assessment of data significance. These insights are primarily qualitative and reflect our SOC team's evaluation of the most significant cyber threats in 2024.

'Email threats' methodology
The statistics highlighted in the 'Email threats' section are derived from analysis of monitored Darktrace / EMAIL model data for all customer deployments hosted in the cloud between December 21, 2023, and December 18, 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. For the same reason, it does not include December 19 through December 31, 2024, either.

Preface

Darktrace's Threat Research team has observed a significant increase in sophisticated threat actors targeting organizations within designated CNI globally over the past year.

This trend is informed both by the heightened warnings from national intelligence agencies as well as an overall focus of threat analysis on activity identified within customers in these industries. The targeting of CNI entities, and the subsequent operations following access, suggest threat actors may be building strategic pathways to yield geopolitical leverage in the event of conflict. This reality manifests in both the focus and content of Darktrace's threat investigations throughout 2024.

The past year saw multiple high-profile public disclosures of malicious activity within CNI sectors. The Darktrace Threat Research team conducted threat hunting investigations across the customer base driven by information suggesting Advanced Persistent Threats (APTs) infiltrating CNI organizations.

For example, analysts searched for evidence of Salt Typhoon and LiminalPanda activity in response to the public disclosure that these groups were targeting Internet Service Providers (ISPs). Additionally, 2024 saw the emergence of new ICS/OT native malware like Fuxnet and FrostyGoop, as well as the continued prevalence of ransomware groups targeting vulnerable industries like healthcare. The Darktrace Threat Research team also conducted multiple in-depth investigations for specific customers in defense and government services showing indications of compromise. These investigations yielded distinct evidence of sophisticated threat actors operating within the networks of high-profile defense and government customers that could be leveraged in emerging geopolitical conflicts.

The varying methods of attack and long-term orientation of goals by such threat actors will pose unique challenges to CNI organizations. Many instances of CNI compromise have stemmed from the exploitation of internet-facing devices through both zero-day and known exploits.

Even when CVE exploitation was not present, threat actors can and will rely on perimeter devices running external remote services for access. IoCs are also increasingly proving less effective at deterring such attacks. Groups such as VoltTyphoon continue to build vast botnets of Internet of Things (IoT) (KV Botnet) and internet-facing devices by exploiting unpatched systems. Usage of these botnets and operational relay networks will assist in evading detection and attribution, as evidenced in specific cases investigated by the Darktrace team. Generally, APTs targeting CNI sectors are also increasingly relying on LOTL tactics to remain undetected.

Moreover, malicious groups exploiting CNI networks may have differing aims based on their operating context. Some APT groups may not have immediate objectives once persistence is obtained within CNI networks. Potentially state-sponsored actors may take a lay-and-wait approach: opting to sit within networks with minimal activity beyond beaconing only increasing activity when outside strategic conditions change [5].

Alternatively, threat actors targeting CNI organizations may pursue a more aggressive approach by attempting to exfiltrate sensitive data that can support broader strategic goals for sponsor nations. Darktrace observed this pattern of behavior in June-July 2024 when a government agency in the Asia-Pacific (APAC) region was likely exploited by Mustang Panda to exfiltrate sensitive data to cloud storage providers. Similarly, Darktrace research identified evidence of a potential North Korean APT exfiltrating data from a manufacturing organization, likely in response to geopolitical developments. This trend extends even to actors targeting sectors such as healthcare where Darktrace analysts have observed a shift towards favoring data exfiltration over traditional encryption during ransomware events.

Certain threat actors will also leverage malware aimed at causing immediate disruption to suit their goals. This threat is particularly relevant for organizations with Operational Technology (OT) and Industrial Control Systems (ICS) environments, such as customers within the energy sector, as well as traditional targets of ransomware like hospitals and financial institutions.

Darktrace Threat Research analysts noted an uptick in attacks in the energy sector motivated by disruption. The means of disruption observed by Darktrace ranged from an OT specific attack on Canadian energy provider's PLC motor in the SCADA environment at a field substation, to multiple Fog ransomware attacks that successfully led to encryption. APT groups also are increasingly targeting healthcare organizations for non-financial goals. OSINT suggests many of these compromises attempted to inhibit public health services to promote general instability. This trend also became apparent in the evolution of Ransomware-as-a-Service (RaaS) groups are leveraging such services in furtherance of nation-state aims, targeting both healthcare and non-medical organizations via ransomware platforms.

The following sections will further discuss and expand the trends noted here by providing a review of Darktrace's investigation into specific industries and threats. Ultimately, the work Darktrace's Threat Research team has conducted during 2024 highlights the increasing risk advanced cyber actors may pose to CNI organizations in 2025.

Campaign overview

The most significant campaigns observed in 2024 involved the ongoing exploitation of zero-day and n-day vulnerabilities in edge and perimeter network technologies. This widespread exploitation across the threat landscape was consistent with Darktrace's observations throughout the year.

Ivanti Connect Secure (CS) and Ivanti Policy Secure (PS) appliances - CVE-2023-46805 and CVE-2024-21887

- Amongst the observed activities, the following threads were identified as salient: exploit validation activity, exfiltration of system information, delivery of C2 implant from AWS, delivery of JavaScript credential stealer, SimpleHelp usage, and encrypted C2 on port 53.
- For more information, read: Darktrace's Inside the SOC Blog - The Unknown Unknowns: Post-Exploitation Activities of Ivanti CS/PS Appliances.

Palo Alo Network (PAN-OS) Firewall Devices - CVE 2024-3400

- A critical vulnerability in PAN-OS firewall devices was publicly disclosed on April 11, 2024. Due to anomaly-based detection, Darktrace's Threat Research team identified a range of suspicious behavior as early as March 26, related to the exploitation of PAN-OS devices, including C2 connectivity, data exfiltration, and brute-forcing activity.
- For more information, read: Darktrace's Inside the SOC Blog - Post-Exploitation Activities on PAN-OS Devices: A Network-Based Analysis.

Fortinet - FortiManager CVE 2024-47575

- This analysis focuses on the September 2024 exploitation of FortiManager via CVE-2024-47575, along with related malicious activity observed in June and September.
- Campaign Comparison: Both Mandiant and Darktrace sources acknowledge the June exploitation attempts. The Darktrace article expands upon wider industry reporting by revealing a potentially broader campaign occurring earlier.
- For more information, read: Darktrace's Inside the SOC Blog - Post-Exploitation Activities on Fortinet Devices: A Network-Based Analysis.

Operation Lunar Peek: Palo Alto Network firewall devices (CVE 2024-0012 and 2024-9474

- The second campaign observed related to PAN-OS firewall exploitation. Darktrace observed exploit validation and initial payload retrieval, C2 connectivity, among other activities.
- The use of the Sliver C2 platform further differentiates the latest round of PAN-OS compromises, with evidence of Sliver activity in about half of the investigated cases.
- For more information, read: Darktrace's Inside the SOC Blog - Darktrace's view on Operation Lunar Peek: Exploitation of Palo Alto firewall devices (CVE 2024-0012 and 2024-9474).

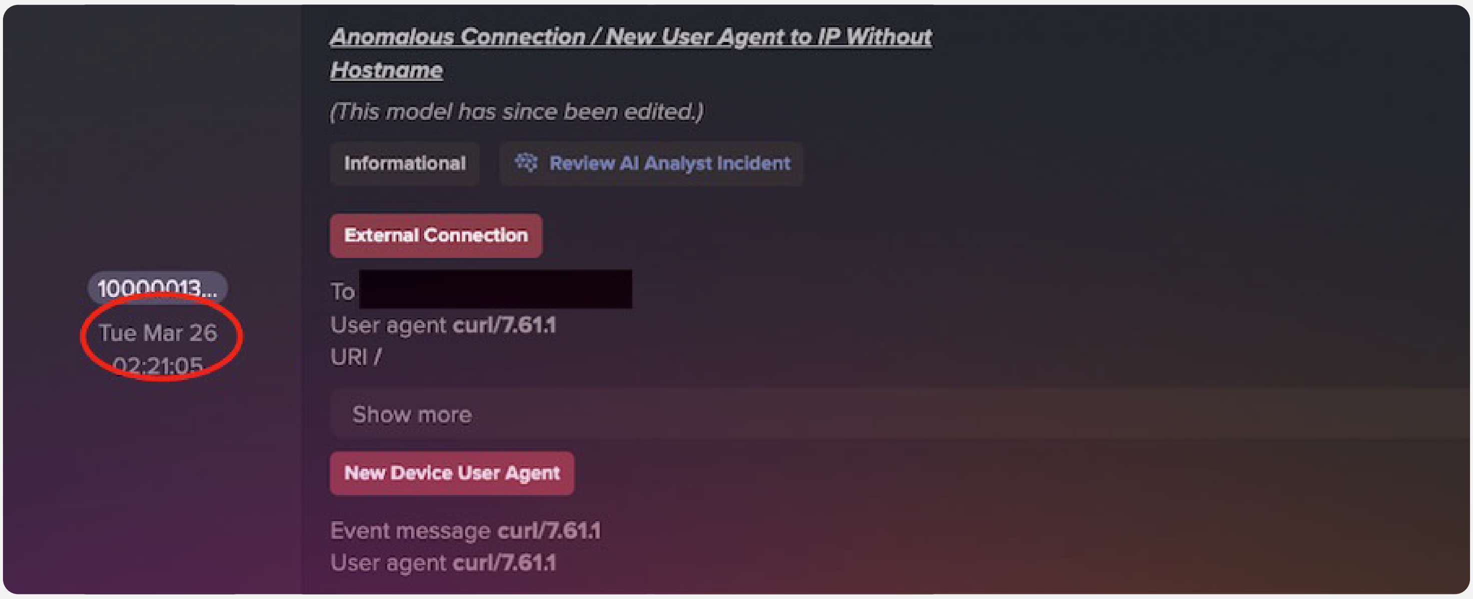
Honorable Mentions: Cleo and Jet Brains

- 2024 vulnerabilities in Cleo's MFT software, namely CVE-2024-50623, and JetBrains TeamCity CVE 2024- 27198.
- Highlights that ransomware groups particularly like to target file transfer applications, such as Cleo, for exfiltration and double extortion due to the significant amount of business information in these appliances. Meanwhile, JetBrains highlights that shortened time-to-exploit has become fairly common for software deeply embedded in an organization's supply chain.
- For more information, read: Darktrace's Inside the SOC Blogs - Race Against Time: Detecting JetBrains' TeamCity Exploitation Activity with Darktrace and Cleo File Transfer Vulnerability: Patch Pitfalls and Darktrace's Detection of Post-Exploitation Activities.

Beyond the specific campaigns observed and documented by Darktrace, the following have become universal use cases demonstrating how attackers continue to achieve success:

- Adversary-in-the-Middle (AiTM) phishing threats like Mamba 2FA
- Remote monitoring and management (RMM) tool usage (Supremo, AnyDesk, UltraVNC, SplashTop, N-able - formerly Solarwinds MSP, SimpleHelp) in ransomware campaigns, including Fog ransomware.
- DNS tunneling in many campaigns, including the cryptomining operation CoinLoader.

PAN-OS exploitation detection



10000013...
Tue Mar 26
02:21:05

Anomalous Connection / New User Agent to IP Without Hostname

(This model has since been edited.)

External Connection

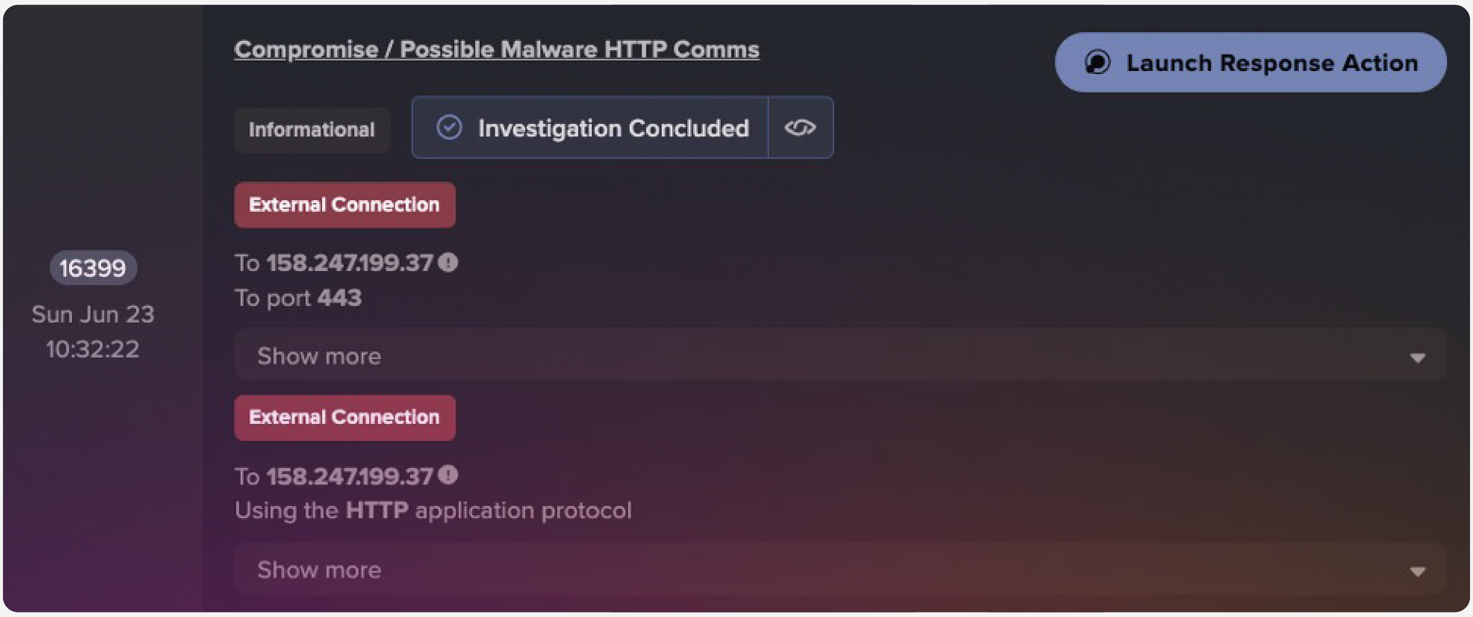
To [redacted]
User agent **curl/7.61.1**
URI /

New Device User Agent

Event message **curl/7.61.1**
User agent **curl/7.61.1**

Figure 01: Model Alert in Darktrace / NETWORK showing the detection of malicious activity associated with the exploitation of PAN-OS prior to the vulnerability's public disclosure.

FortiManager exploitation detection



16399
Sun Jun 23
10:32:22

Compromise / Possible Malware HTTP Comms

External Connection

To **158.247.199.37**
To port **443**

External Connection

To **158.247.199.37**
Using the **HTTP** application protocol

Figure 02: Model Alert in Darktrace / NETWORK showing the detection of malicious connections associated with FortiManager devices in June 2024.

Throughout 2024, Darktrace's Threat Research team sent out notifications to customers detailing campaign activities observed on their deployments. In the first half of the year, **40% of identified campaign activity** involved the exploitation of internet-facing devices.

However, from June to December 2024, information-stealer activity became the most prominent campaign type identified by the Darktrace Threat Research team.

Remote Access Trojans (RATs) also saw a significant increase in the latter half of the year, representing **46% of campaigns identified**, compared to only **12% in the first half**.

Malware-as-a-Service (MaaS) accounted for 57% of campaign activity identified by the Darktrace Threat Research team in the latter half of 2024, up from 40% between January and June.

Ransomware: Persistent threats and emerging strains

While 2024 saw fewer ransomware cases globally compared to the year before, the average payment per ransomware case rose to USD 2.73 million, a USD 1 million increase from 2023 [6].

This rise is unsurprising given the continued adoption of the RaaS model, providing even less experienced threat actors with the tools needed to carry out disruptive attacks, significantly lowering the barrier to entry.

Darktrace's Threat Research team tracked several ransomware threats across the fleet throughout 2024, observing novel strains like Lynx, as well as re-emerging threats such as Akira, RansomHub, Black Basta, Fog, and Qilin (Agenda). Notable trends observed by the team included the frequent use of phishing emails as an attack vector and the use of legitimate tools like AnyDesk, Atera, and Splashtop to mask malicious C2 communication.

LOTL techniques, such as using Windows Management Instrumentation (WMI) and PSEXESVC for lateral movement, are frequently employed, with administrative credentials often used for privilege escalation. Data exfiltration to cloud storage services like MEGA and Rclone is another trend, as these services are commonly used for legitimate purposes.

This section will highlight five ransomware actors that the Darktrace Threat Research team identified as significant threats to organizations in 2024, and which are expected to remain prominent in the threat landscape moving forward.

1. Akira Ransomware

- **Background:** RaaS strain first observed in the wild in 2023, re-emerged in 2024 [7]
- **Affected Customer Countries:** Australia, Canada, South Africa, United Kingdom, United States
- **Observed TTPs:** Double extortion, incoming connections to Remote Desktop Protocol (RDP) servers, leveraging RDP during lateral movement and VMWare usage, encrypting files with ".akira" extension

2. LockBit Ransomware

- **Background:** RaaS group described by the US Department of Justice as "the most active and destructive ransomware group in the world," affecting over 2,500 victims in more than 120 countries and accumulating more than USD 500 million ransom payments [8]. Despite the arrest of its members and developers [9], LockBit has remained a persist threat that Darktrace has continued to observe
- **Affected Customer Countries:** Global impact
- **Observed TTPs:** Abusing NetScan for reconnaissance, exploiting vulnerabilities in VMware ESXi devices

3. Lynx Ransomware

- **Background:** First observed in the wild in 2024 as a successor to INC ransomware. Targets organizations across multiple sectors including real estate, retail, financial, and environmental services [10]
- **Affected Customer Countries:** United Kingdom and United States
- **Observed TTPs:** Phishing emails and malicious payloads as initial access, double extortion, encrypting files with ".LYNX" extension, likely using Restart Manager [10]. If encryption fails, actors attempt to escalate privileges. RDP connections to domain controller using administrator credentials

4. Fog Ransomware

- **Background:** First observed in the wild around April/May 2024 with most of its victims located in the United States and within the education sector. Variants of Fog ransomware exist for both Linux and Windows platforms [11][12][13]
- **Affected Customer Countries:** United States
- **Observed TTPs:** Compromised Virtual Private Network (VPN) credentials, unusual default admin credential usage, SMBv1 lateral movement, anomalous connections to AnyDesk, large volumes of data exfiltration, and '.flocked' or '.flock' extensions

5. RansomHub Ransomware

- **Background:** RaaS group first observed in the wild in February 2024; known to target cloud storage backups and misconfigured Amazon S3 instances. Believed to have absorbed BlackCat/AL-PHV affiliates [14]. Darktrace observed ShadowSyndicate using RansomHub in multiple attacks in late 2024, affecting education manufacturing and social services sectors
- **Affected Customer Countries:** Global impact but avoids targeting entities in Commonwealth of Independent States (CIS), China, North Korea, or Cuba [15]
- **Observed TTPs:** Gains initial access via vulnerabilities in Windows, Linux, ESXI, NAS, and Zerologon (CVE-2020-1472), use of legitimate tools like Atera and Splashtop for C2 and NetScan for reconnaissance [16] [17]. Double extortion tactics

■ Ransomware spotlight:

RansomHub

Organizations and entities face increasing challenges from sophisticated ransomware actors like RansomHub. To better understand and analyze such adversary activities, security analysts and researchers widely use the Diamond Model of Intrusion Analysis, a cybersecurity framework designed for this purpose.

By applying the Diamond Model and combining it with Darktrace's capabilities, Darktrace's Threat Research team enhances its ability to understand the behavior of these persistent adversaries. This approach provides organizations with deeper insights and proactive defense strategies.

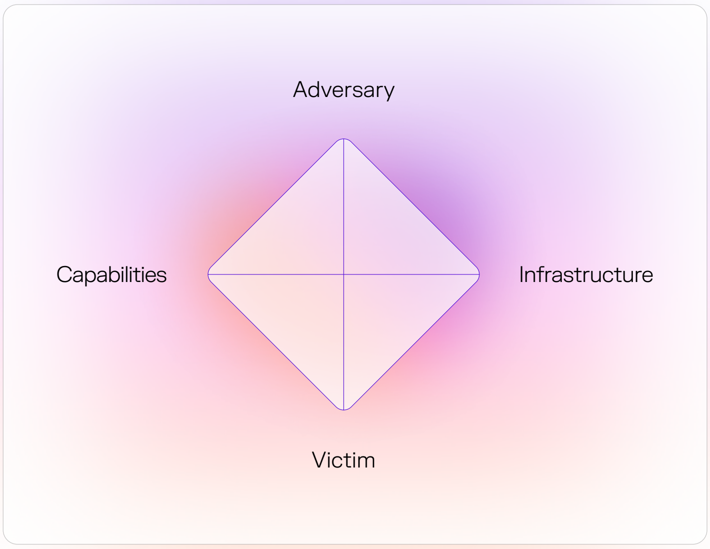


Figure 03: The Diamond Model of Intrusion Analysis

Understanding RansomHub through the Diamond Model

Adversary identification

Despite being a relatively young ransomware group, RansomHub have quickly become known globally due to their aggressive tactics and high-profile attacks. Their approach mirrors that of predecessor groups like LockBit and ALPHV (BlackCat), with reports suggesting that former members of these groups now operate under RansomHub [14].

The group operates under a RaaS model, recruiting affiliates to execute attacks and providing them with the necessary tools, infrastructure, and support.

Like most ransomware actors, they are financially motivated, with their primary goal being to extort victims through double extortion tactics—encrypting critical data and threatening to release sensitive information unless a ransom is paid [15].

Darktrace's Threat Research team investigated several customer networks impacted by RansomHub in 2024. Attacks have continued into early 2025, with Darktrace's Security Operations Center (SOC) team investigating at least three additional cases.

Infrastructure analysis

RansomHub employs HTTPS and DNS-based communication protocols to encrypt the data flow between compromised systems and their C2 servers, complicating efforts for defenders to monitor or intercept these exchanges [17]. Additionally, RansomHub frequently registers numerous domains through anonymized services such as Tor to conceal ownership information, making attribution increasingly challenging [17].

When the group drops their ransom note, it usually only contains information directing the victim to a unique ".onion" URL for payment and communication [17].

For the stolen data, the group employs dedicated servers and cloud storage services to temporarily store the exfiltrated data, using this as leverage in their double extortion tactics by threatening victims with public exposure. Once the victim agrees to make the payment, they must do so using Bitcoin or Monero, as RansomHub only accepts ransom payments exclusively in cryptocurrency [18].

Victim profiling

RansomHub has reportedly attacked around 500 organizations and entities, including high-profile attacks on Mexico's presidential legal counsel [19] and a Scottish housing society [20]. RansomHub specifically targets victims across North America, Europe, and Asia, with a particular focus on government agencies, financial institutions, and healthcare providers, likely due to the critical nature of their data and the potential financial impact [21] [22].

However, other sectors, including information technology, emergency services, food and agriculture, and telecommunications, have also been targeted [23]. Alongside targeting critical infrastructures, the group also targets specific individuals such as C-level executives and IT administrators, aiming to obtain privileged credentials that grant full network access [15].

The group does not attack non-profit organizations and has a rule not to target victims who have already paid. Additionally, RansomHub does not allow their affiliates to target members of the Commonwealth of Independent States (CIS), Cuba, North Korea, and China [15], potentially indicating the group's location or alignment.

Capability analysis

For initial access, RansomHub exploits known vulnerabilities in internet-facing applications and uses phishing and spear-phishing attacks to gain entry, along with credential stuffing and brute-force attacks to exploit weak authentication mechanisms [17]. Once inside, RansomHub uses advanced exploitation techniques, such as leveraging ZeroLogon (CVE-2020-1472) and deploying EDRKillShifter, a tool designed to disable endpoint detection and response (EDR) defenses [16] [24].

They use PowerShell scripts to execute malicious commands and perform network reconnaissance, manipulating existing accounts and re-enabling disabled accounts to escalate privileges. Additionally, RansomHub uses tools such as Mimikatz to extract credentials from compromised systems and exploits vulnerabilities in SMBExec, AnyDesk, and Cobalt Strike to move laterally.

For encryption, the ransomware group typically employs an Elliptic Curve Encryption algorithm called "Curve 25519", which appends unique 6-digit alphanumeric code extensions to encrypted files [17]. For data exfiltration, they have been observed using tools such as BITSAdmin, HTTP POST requests, and WinSCP to transfer stolen data over web services [17].

Darktrace's coverage of RansomHub

Focusing on the attacks observed by Darktrace, in the three cases, the compromised devices were observed triggering multiple C2-related models in Darktrace / NETWORK as they were detected communicating with external C2 infrastructure. Further investigation revealed that the devices were also communicating on unusual TCP ports. These connections were detected based on Darktrace's ability to identify the rarity of the domains in question, as well as the unusualness of the TCP ports used in some of these connections.

As one of these customers was subscribed to Darktrace's Managed Threat Detection service, the SOC team promptly alerted them about the observed activities when the first signs of an emerging compromise were detected on the network.

In this case, Darktrace's SOC analysts informed the customer of a device receiving incoming connections using AnyDesk, performing network scanning, and lateral movement on the network.

Following the first alert, Darktrace's SOC sent multiple additional alerts as the attack propagated rapidly on the network. Throughout the course of the attack, Darktrace also detected affected devices uploading a large amount of data to external endpoints, including legitimate cloud services such as MEGA and Atera. This activity was consistent with threat actors exfiltrating data as part of their double extortion methods.

This malicious activity was detected due to the anomalous nature of the device transferring a large volume of data externally. It is important to note that the rarity of the external domain is not a primary parameter for triggering models related to external data transfer in Darktrace, as legitimate services can be exploited by attackers, as seen with the use of MEGA and Atera in this case.

In contrast, the other two customers were not subscribed to the Managed Threat Detection service and therefore were not notified when the attackers gained access to their respective networks. However, Darktrace's SOC team was still able to support them through the Security Operations Support service, giving the customers direct access to Darktrace's expert analysts. The SOC analysts provided information on how the attack may have started, a list of infected devices, details on how the attack propagated, and a record of the files encrypted with the code extension ".b2202a" by the attackers.

For more information, you can read Darktrace's full investigation into the deployment of RansomHub by the ShadowSyndicate threat actor in late 2024, which features a breakdown of the IoCs and TTPs observed and the associated Darktrace / NETWORK models.

Critical exploited vulnerabilities according to Darktrace

It is increasingly common for threat actors to identify and exploit newly discovered vulnerabilities in widely used services and applications. Attackers often prioritize developing exploits for severe and global CVEs but typically find the most success with known vulnerabilities within the first couple of years after public disclosure.

In some cases, exploit validation occurs within hours of disclosure.

In 2024, the Darktrace Threat Research team identified multiple campaigns where threat actors targeted vulnerabilities in internet-facing systems, as discussed earlier, such as Ivanti CS/PS appliances, Palo Alto firewalls, Fortinet appliances, Cleo software, ScreenConnect servers, and TeamCity on-premises servers. These exploited vulnerabilities were strongly associated with malware such as Spark, WARPWIRE, Spectre RAT and CACTUS ransomware, as well as malicious cryptocurrency activities.

Timely addressing these vulnerabilities reduces their effectiveness, slowing malicious operations and forcing attackers to pursue more costly and time-consuming methods, such as zero-day exploits or software supply chain attacks. While actors develop tools for other vulnerabilities, exploiting critical and publicly known vulnerabilities provides them with impactful, low-cost tools for extended use.

Darktrace's most commonly observed exploited vulnerabilities in 2024

CVE-2024-3400

- **Vulnerable products:** Palo Alto Networks firewall appliances running PAN-OS
- **Type of vulnerability:** Command injection and improper input validation
- **Associated malware:** Spark (backdoor)
- **Activity seen:** Exploit validation activity, retrieval of binaries and shell scripts, data exfiltration via HTTP POST activity, and ongoing C2 communication with rare external endpoint
- Technical details and IoCs

CVE-2023-46805 and CVE-2024-21887

- **Vulnerable products:** Ivanti Connect Secure (CS) and Ivanti Policy Secure (PS)
- **Type of vulnerability:** Authentication bypass via improper authentication and command injection
- **Associated malware:** WARPWIRE, Monero cryptocurrency miner
- **Activity seen:** Usage of Out-of-Band Application Security Testing (OAST) services for exploit validation, exfiltration of system information, delivery of AWS-hosted C2 implants, delivery of JavaScript credential stealers, usage of SimpleHelp (remote support software), usage of SSL-based C2, and the delivery of cryptocurrency miners
- Technical details and IoCs

CVE 2024-23113 and CVE-2024-47575

- **Vulnerable products:** FortiGate and FortiManager
- **Type of vulnerability:** Use of externally controlled format string and missing authentication for critical function
- **Activity seen:** Command execution on host, payload retrieval, and sensitive data exfiltration
- Technical details and IoCs

CVE-2024-0012 and CVE-2024-9474

- **Vulnerable products:** Palo Alto Networks Firewalls and PAN-OS (Web Management Interface)
- **Type of vulnerability:** Authentication bypass via missing authentication for critical function and OS command injection
- **Associated malware:** Spectre RAT
- **Activity seen:** Exploit validation, initial payload retrieval, C2 connectivity potentially featuring further binary downloads, potential reconnaissance and cryptocurrency mining activity
- Technical details and IoCs

CVE-2023-48788

- **Vulnerable products:** FortiClient EMS
- **Type of vulnerability:** SQL Injection
- **Activity seen:** Exploit validation, use of Sliver C2 framework, use of various RMM tools such as Splashtop, Atera, and AnyDesk, internal reconnaissance, privilege escalation, lateral movement, and sensitive data exfiltration
- Technical details and IoCs

CVE-2024-1708 and CVE-2024-1709

- **Vulnerable products:** ConnectWise Screen Connect
- **Type of vulnerability:** Improper limitation of a pathname to a restricted directory (path traversal) and authentication bypass vulnerability
- **Activity seen:** Outbound connections to suspicious endpoints, use of PowerShell, executable file downloads
- Technical details and IoCs

CVE-2024-50623

- **Vulnerable products:** Cleo's Managed File Transfer (MFT) Software
- **Type of vulnerability:** Unrestricted upload of file with dangerous type
- **Activity seen:** Outbound connections to suspicious endpoints, data exfiltration, command execution via PowerShell
- Technical details and IoCs

CVE-2024-27198

- **Vulnerable products:** JetBrains TeamCity
- **Type of vulnerability:** Authentication bypass using an alternate path or channel
- **Associated malware:** Cryptocurrency mining (XMRig)
- **Activity seen:** Use of public proof-of-exploits, malicious file downloads, C2 connectivity, and the delivery of cryptocurrency miners
- Technical details and IoCs

CVE-2023-41266, CVE-2023-41265, and CVE-2023-48365

- **Vulnerable products:** Qlik Sense Enterprise
- **Type of vulnerability:** Path traversal, HTTP request tunnelling
- **Associated malware:** CACTUS Ransomware
- **Activity seen:** Beaconing to suspicious endpoints, malicious executable file download using PowerShell, network scanning and lateral movement over the RDP, SMB and LDAP protocols Qlik, Kerberos brute-force attack, ransomware encryption, and attempted concealment of encrypted files
- Technical details and IoCs

Email threats

Between December 21, 2023, and December 18, 2024, Darktrace / EMAIL detected **30.4 million phishing emails** across the fleet.

The abuse of legitimate services and senders continued to be a significant method for threat actors throughout 2024.

At least

2.7 million

- **multistage payload emails** were identified in these emails

Over

940,000

- **malicious QR codes** were detected within these emails

By leveraging trusted platforms and domains, malicious actors can bypass traditional security measures and increase the likelihood of their phishing attempts being successful.

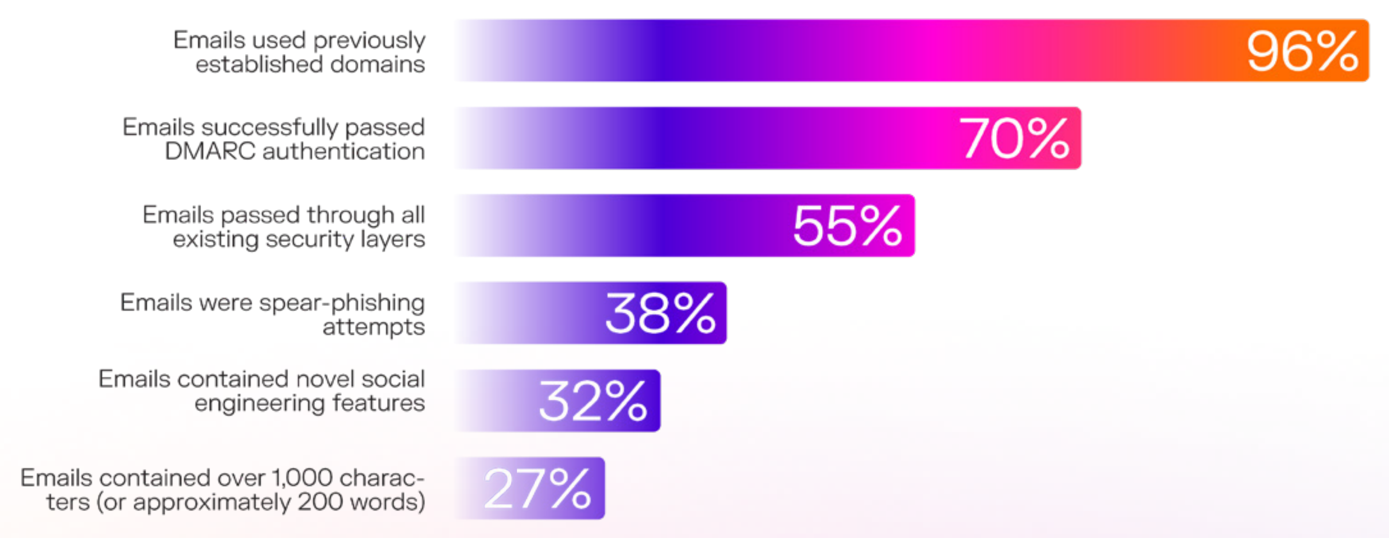
In the final six months of 2024 alone, Darktrace's Threat Research team observed a significant trend in email-based cyber incidents involving the abuse of legitimate domains within sender addresses or payload links.

This trend aligns with the overall patterns observed by Darktrace in phishing emails throughout 2024, where there was a substantial use of legitimately authenticated senders and previously established domains, with **96% of phishing emails** detected by Darktrace / EMAIL utilizing existing domains rather than registering new ones.

Throughout the course of the year, Darktrace observed threat actors exploiting trusted services including Zoom Docs, QuickBooks, HelloSign, Adobe, and Microsoft SharePoint to send phishing emails via legitimate sender addresses. These emails often appear more legitimate, increasing the chances of recipients engaging with them.

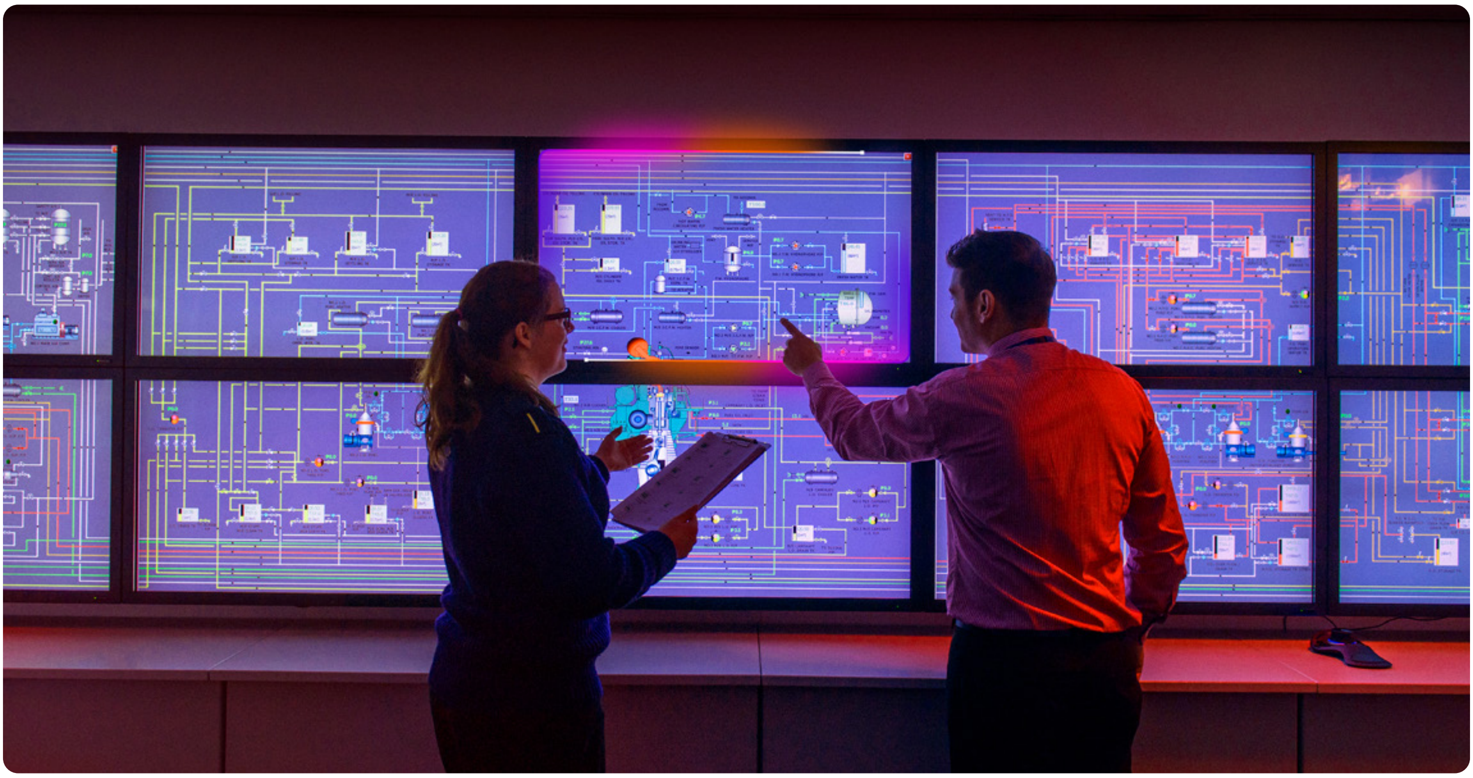
Threat actors were frequently observed using redirects via legitimate services like Google to deliver malicious payloads, effectively evading detection. Additionally, Darktrace noted instances where attackers hijacked email accounts, including Amazon Simple Email Service (SES) accounts, belonging to legitimate third parties, such as business partners and trusted vendors.

This tactic further complicated the detection process for traditional email tools, as the emails originated from trusted recipients with previous correspondence.



■ Exploiting native tools:

LOTL techniques



Throughout 2024, LOTL techniques were ever-present across threats observed by the Darktrace Threat Research team, with numerous incidents featuring attackers exploiting native protocols and services to achieve their objectives while remaining undetected on target networks.

Towards the start of the year, the team investigated a credential theft campaign associated with the TA577 Initial Access Broker (IAB) group. This campaign exploited the SMB protocol and the NTLMv2 challenge/response to steal NTLM authentication hashes. Darktrace identified devices on multiple customer networks attempting to retrieve a text file from attacker-controlled external SMB servers. The servers required SMB session authentication via NTLM, which, once completed, exposed the NTLM hash to the attackers. This encrypted challenge string could then be used in pass-the-hash attacks or brute-forced to obtain the original credential.

During the investigation into the exploitation of the PAN-OS command injection vulnerability (CVE-2024-3400) in April and May, Darktrace's Threat Research team identified multiple devices across customer environments making HTTP requests to rare external endpoints, often using "cURL" or "wget" utilities. These utilities, typically used by developers and system administrators, were seemingly leveraged by attackers to retrieve payloads and exfiltrate sensitive configuration information to attacker-controlled IPs.

Around the same time, the Threat Research team investigated a campaign that used legitimate Windows processes to spread the Raspberry Robin worm. The infections utilized the "cmd.exe" and "msiexec.exe" executables to run malicious files from an external drive and connect to Raspberry Robin C2 servers to download the main malware component.

Finally, Darktrace investigated multiple infections by ShadowPad, a modular malware platform previously associated with nation-state sponsored activity, including APT41 [25]. Anomalous SMB and RDP activity between an infected device and a domain controller led to the domain controller initiating TXT DNS requests for long, encoded subdomains associated with ShadowPad's DNS C2 infrastructure, likely indicating DNS tunneling activity.

Differentiating between legitimate use by administrators and malicious use by attackers is challenging without an established baseline of user behavior. LOTL techniques allow attackers to blend in with normal traffic, making them ideal for espionage and information-gathering campaigns where remaining undetected is crucial. APTs use these techniques to hinder attribution efforts based on malicious signatures and IoCs. However, smaller criminal enterprises also benefit from exploiting native tools, saving time and money by avoiding the need for custom malware development that might be blocked by traditional security tools once IoCs and TTPs are published.

A view from the SOC

The following insights from the Darktrace SOC highlight the most significant cyber threats that organizations faced in 2024 and are expected to persist into 2025 and beyond.

Abuse of remote network access solutions

Remote network access solutions, such as VPN solutions, Virtual Desktop Infrastructure (VDI) solutions, and Microsoft's Remote Desktop Services (RDS), enable organizations to provide users with remote access to their networks. In 2024, Darktrace's SOC observed malicious actors regularly abusing these remote network access solutions, particularly VPNs, to gain entry into organizations' networks. After logging in with stolen credentials to VPN, VDI, and RDS environments, malicious actors conducted widespread network reconnaissance in preparation for the subsequent phases of their attacks.

AiTM phishing

AITM phishing is a popular technique among threat actors as it allows them to bypass Multi-Factor Authentication (MFA) protections on SaaS accounts. This technique was widely observed in the SaaS compromises investigated by Darktrace's SOC in 2024, with the phishing kits Mamba 2FA and Tycoon 2FA being particularly popular among threat actors. After gaining access to users' SaaS accounts through AiTM phishing, threat actors concealed their origins by using VPN services such as HideMyAss (HMA) VPN, Private Internet Access (PIA) VPN, ExpressVPN, and Cloudflare WARP VPN.

Data exfiltration

Data exfiltration remained a common objective for malicious actors in 2024, observed in both extortion and espionage operations. The extortion operations varied, with stealthy data exfiltration techniques used in RansomHub double extortion ransomware attacks, and ransomware-less extortion methods employed in the recent Cleo compromises orchestrated by the Clop extortion gang. In an espionage operation observed by Darktrace's SOC, a state-linked actor used a network of legitimate, compromised sites to smuggle sensitive data out of a target network.

The SOC's Monthly Breakdown

The table below highlights some of the most impactful and noteworthy threats affecting Darktrace customers, tracked by Darktrace's SOC each month in 2024.

January	February	March
Ivanti exploitation	Dropbox abuse	Tunneling tool abuse (Cloudflare Tunnel, Ngrok)
Data exfiltration (MEGA, Put.io)	Brute-force activity	Teams phishing
Microsoft Customer Voice service abuse	Ivanti exploitation	JetBrains TeamCity exploitation
Amadey infostealer	RMM tool usage (AnyDesk)	SSH-based C2
RMM tool usage (AnyDesk, ConnectWise Control)	Ransomware (LockBit, Akira, and 8Base)	Ransomware (Akira, Phobos)

April	May	June
Session cookie abuse	eM Client abuse for mailbox reconnaissance	Initial access through VPN
FortiClient EMS and Palo Alto Pan-OS exploitation	Proxy botnet activity	AiTM phishing
RMM tool usage (AnyDesk, Atera, DWService)	Insider threats	VPS exploitation
Proxy tool usage (Stowaway, SystemBC, ProxyScrape)	Data exfiltration (OneDrive, Vultr)	XMRig crypto-mining
PowerShell usage	MFA manipulation	Ransomware (Medusa, Akira)

July	August	September
DNS tunneling	LDAP reconnaissance	SSH usage
Initial access through VPN	Initial access through VPN	Initial access through VPN and VDI infrastructure
SharePoint abuse	Purple Fox	Cobalt Strike
Mailbox reconnaissance	Payment diversion fraud	Data exfiltration (MEGA)
Ransomware (Medusa, Fog)	Ransomware (LockBit, Akira, Fog)	Ransomware (LockBit, Akira, RansomHub)

October	November	December
Stealthy C2	AiTM phishing	Chrome extension supply chain compromise
Exchange and Fortinet exploitation	Payment diversion fraud	AiTM phishing
LOTL (comsvcs.dll, drsuapi)	Palo Alto Pan-OS exploitation	Cleo exploitation
Data exfiltration (Easyupload.io)	RMM tool usage (Splashtop, Supremo, NetSupport Manager)	RMM tool usage (Supremo, AnyDesk, UltraVNC, SplashTop, N-able, SimpleHelp)
Ransomware (Black Basta, Crytox, RansomHub, Fog)	Ransomware (Play, Brain Cipher)	Ransomware (Lynx, Medusa, RansomHub)

Threats to Operational Technology (OT) and Industrial Control Systems (ICS)

In 2024, Darktrace's Threat Research team investigated numerous OT attacks, more than doubling the number of OT investigations from the previous year.

The team researched new tailored malware for ICS, joint warnings from government agencies, and potential compromises from Darktrace / OT customers. The research highlighted that hacking OT systems is becoming increasingly achievable, a trend likely to continue.

In May 2024, multiple security organizations, including NCSC and CISA, issued a warning about the increasing threat of state-aligned groups against western critical national infrastructure. NCSC stated, "As of early 2024, pro-Russia hacktivists have been observed targeting vulnerable, small-scale industrial control systems in North America and Europe" [26]. The NCSC urged all OT owners and operators to harden their defenses. The "defense in depth" approach provides CNI the greatest protection. Notably, a few months after this warning, two Darktrace customers based in North America experienced OT-related incidents; both occurring between June and late August. Both incidents involved unexpected activity from OT devices linked to national critical infrastructure, with one case later revealing an impact on the customer's physical critical infrastructure.

Suspicious activities on one of the customers during this time included:

- Anomalous RDP use from various devices in the customer's IT network to OT devices including HMIs and a SCADA server.
- Unexpected Nmap scanning and attempted SMBv1 sessions from an HMI device.
- Unusual external DNS requests originating from a SCADA server.

This aligns with NCSC and CISA's [27] warnings on mitigation needed within CNI networks; hardening of HMI remote access, restricting internet access, and restricting internal connections to only allow connections from a required list of IPs.

Alongside investigating incidents experienced by Darktrace OT customers, the Threat Research team explored new threats to OT environments, such as the FrostyGoop ICS Malware, and investigated possibilities of detection within Darktrace.

The malware was first discovered in April 2024 and may have been used in a cyber-attack against Ukrainian energy infrastructure [28]. It was only the ninth ICS-specific malware strain identified, underscoring the rarity of such attacks while also demonstrating the growing capabilities of threat actors in the OT space [28]. External research into FrostyGoop revealed that attackers had potentially gained access to affected networks through an undetermined vulnerability in an externally facing router that was not properly segmented [28].

While there were no signs of FrostyGoop across the Darktrace customer base, the potential exploitation of router vulnerabilities reported by external researchers highlighted the risk posed by edge devices. Predictions across the sector suggest a rise in attacks against edge devices and specifically IoT devices [29]. IoT devices and sensors typically have weaker security, making them prime targets for attackers seeking access to OT networks.

The Threat Research team's investigations into Darktrace / OT customers revealed how common it is for OT networks to be insecure by design. These security gaps include insecure protocols and systems, unsegmented networks, and insufficient asset inventory.

As OT becomes more integrated with IT systems, it presents more opportunities for attackers. OT security is strongest when supported by robust IT security, requiring coordination between IT and OT teams to defend the entire network.

■ Sector spotlight:

Energy

In 2024, Darktrace's Threat Research team focused on producing industry-specific outputs, including for the energy sector. The energy sector is critical, powering every part of the economy, and has undergone vast technological transformation. Such changes have increased the sector's cyber-attack surface and risk.

A 2023 Rockwell Automation report on OT/ICS security incidents found that threat actors are intensely focused on the energy sector, targeting it over three times more than the next most frequently attacked verticals (critical manufacturing and transportation) [30].

Darktrace's research into the energy sector sought to understand the threat landscape for the sector across the United Kingdom and United States, focusing on:

- Which APTs and attack vectors target energy organizations?
- How has technology, including AI, transformed the threat landscape?
- Whether AI has changed the nature of cyber defense within the sector?
- Is this changing threat landscape reflected within policy, and what are the key considerations for businesses and governments?

Key findings

- Technological advancement brings cyber risks. IoT adoption and control automation in non-dispatchable solar and wind sectors increases attack surface and IT/OT convergence makes islanding during cyber incidents more difficult.
- Overdependency on few vendors and systems and a movement towards cloud operations creates further single points of failure, whilst tangled supply chains reduce visibility and management of assets.
- AI-driven attacks have not yet been observed in the energy sector based on our findings.
- The energy sector has long been using AI in sector, although not yet adopted sector-wide due to lack of data quality readiness, data risks, and heavy sector regulation.
- Stakeholders are facing challenges in becoming data-driven to develop in-house AI systems.

Implications

- Businesses must ensure comprehensive asset management across their supply chains, conduct regular risk assessments, and practice response plan scenarios. Efforts should not be siloed; increased collaboration across the sector is essential.
- Enhancing email security is crucial to reduce initial access, and addressing vulnerabilities by enforcing MFA policies and securing internet-facing devices is vital.
- Governments should enhance preparedness and response to nation-state attacks and fund innovation in cyber detection and defense within the energy sector.

Complete findings will be reported in our upcoming white paper dedicated to the state of energy sector.

■ Sector spotlight:

Healthcare

Healthcare has traditionally been perceived as more vulnerable to cyber-attacks due to a historic lack of investment in cybersecurity. However, recent years have seen significant improvements in cyber awareness, defenses, and standards to ensure patient safety. In 2024, governments in countries such as the United Kingdom, United States, and Brazil have pledged significant investment to support further digital transformation, with cybersecurity specifically named as a priority area.

The contrasting healthcare operating models across these three countries, along with different levels of digital transformation and policy expansion, made them ideal examples to leverage Darktrace's internal subject matter expertise.

Darktrace's research into the healthcare sector sought to understand the **threat landscape for the sector across the United Kingdom, United States and Brazil, focusing on:**

- Which APTs and attack vectors target healthcare organizations?
- How has the threat landscape changed since the sector's last major review post-WannaCry ransomware attack in 2017?
- Whether the advancements in AI and increasing adoption of medical IoT devices has transformed the threat landscape?

Key findings

- Ransomware continues to pose a key threat to healthcare, although threat actors have demonstrated a preference for data exfiltration for extortion, rather than encryption
- Business Email Compromise (BEC), cloud account takeovers, and other network intrusions were highly prevalent
- Fraud was a common objective for US threat actors, who used social engineering to access to payroll systems and accounting personnel to re-route banking information. The difference in objectives of BEC attacks in other regions, associated with data collection and second-stage attacks, likely reflects the business-oriented model of healthcare delivery in the US, where the commonplace exchange of payment information in addition to a general culture of helpfulness in healthcare organizations and the operational and financial ramifications of missed payments augment the effectiveness of payment fraud in this region. This demonstrates how organizations must consider operational and systemic risks alongside the current threat landscape
- Access to sensitive data (potentially in preparation for second-stage attacks) was observed in other regions
- Attackers frequently exploited trusted relationships in supply chains, either through direct compromise of a supplier or "typo-squatting" a supplier's domain
- There is no significant difference in the number of cyber-attacks targeting healthcare suppliers compared to those targeting healthcare providers

See the complete findings in our white paper dedicated to the state of AI cybersecurity in the UK, US, and Brazil

■ Darktrace's investigation of the year:

Uncovering state-linked espionage

In October 2024, a likely state-linked espionage operation unfolded within the network of a European customer within the manufacturing industry. The operation was highly targeted and stealthy, with the threat actor likely lying dormant for several weeks or months before initiating the data exfiltration phase of their operation. The exfiltration phase involved the internal distribution of highly masqueraded executable files via SMB and WMI, the targeted collection of the targeted collection of sensitive information from an internal server, and the exfiltration of collected information to a web of legitimate, compromised sites.

The behaviors involved in the operation's data exfiltration phase resulted in many Darktrace Real-Time Detection alerts and Cyber AI Analyst Incident events.

Cyber AI Analyst launched an autonomous investigation into this suspicious activity, weaving together individual events - including C2 connectivity to multiple endpoints, lateral movement, and suspicious SMB writes - into a broader compromise incident rather than viewing them as isolated events.

This ensured that both the customer and analysts could build a complete picture of the attack.

After the incident had concluded, Darktrace's Threat Research team continued their investigation to further their understanding of the threat actor behind the operation. The evidence, some of which cannot be shared publicly, pointed in two conflicting directions: towards actors possibly linked to the People's Republic of China (PRC) and actors possibly linked to the Democratic People's Republic of Korea (DPRK).

The competing DPRK and PRC hypotheses were compared based on the evidence observed in the network of the targeted customer. The ShadowPad intrusion activity observed in the targeted customer's network in the months prior to the data theft activity served as potential evidence in favor of the PRC hypothesis, however, no evidence was found of a clear link between the ShadowPad intrusion activity in July and the data theft activity in October. Furthermore, even if a clear link between such activities had been found, the inference to a PRC-link from the observation of ShadowPad activity would still have only been tentative, given that ShadowPad may, despite lack of public evidence, be used by actors linked to states other than the PRC or non-state actors.

The DPRK-indicating behaviors observed in the targeted customer's network provided stronger evidence in favor of a DPRK-link. Amongst the behaviors observed in the data theft phase of the operation were TTPs, artifacts, and C2 infrastructure resembling TTPs, artifacts, and C2 infrastructure seen in previous DPRK-linked intrusions [31] [32] [33] [34] [35].

Darktrace assesses with medium to high confidence that a nation-state, very likely DPRK, was responsible, based on its applied resources, patience, obfuscation, and evasiveness combined with external reporting, collaboration with the cyber community, and assessing the attacker's motivation and world geopolitical timeline [36]. Such an assessment left question marks over the link between the October exfiltration activity and the July ShadowPad activity but does highlight that attribution is an arduous task. Given that state-linked actors are known to use misdirection techniques to evade attribution [37] [38] [39] [40], the possibility of a false flag operation was explored. To further investigate the incident, Darktrace's Threat Research team also collaborated with a world-leading cyber intelligence firm and a well-known government agency; their expertise provided additional insights, although the definitive attribution remains unresolved.

Recommendations from the Darktrace Threat Research team

Given the constantly evolving nature of the threat landscape and the increasing capabilities of threat actors, as highlighted in this report, Darktrace's Threat Research team recommends the following actions to enhance your cybersecurity posture:

01 **Stay Informed:** Keep up to date with the evolving threat landscape

02 **Risk-Based Approach:** Understand the business impact of losing critical data and adopt a risk-based approach

03 **AI Integration:** Prepare for and understand how AI will be incorporated into different levels of your business

04 **Identify Exposed Assets:** Regularly identify and assess exposed assets

05 **Prioritize Edge Devices:** Focus on edge devices within your vulnerability management processes

06 **Supply Chain Risks:** Assess internal and external readiness and critical attack paths to better understand supply chain risks

07 **Incident Response Plans:** Regularly review and test your incident response plans

08 **Zero Trust Policies:** Implement zero trust policies and principles

09 **Identity Access Management:** Ensure robust identity access management policies and technologies are in place

10 **Early Anomaly Detection:** Investigate lower-level anomalies in the earlier stages of the kill chain before they have a significant impact

By adopting good cyber hygiene, proactively securing your digital estate, and addressing any vulnerabilities before they can be exploited, organizations will be much better equipped to defend their networks against increasingly opportunistic threat actors.

Community interest efforts

Cybersecurity professionals frequently describe threat actor motivations and strategic goals in an abstract sense. However, the operational and tactical realities of these objectives are regularly shaped by events beyond the scope of cybersecurity. Major events in the realms of sports, politics, and culture, among others, provide opportunities for threat actors to operate.

Two such events occurred in 2024: the Paris Summer Olympic Games and the US presidential election.

As a stakeholder in the broader cybersecurity ecosystem, Darktrace recognizes the responsibility to use its knowledge and skills to benefit the wider public. The Darktrace Threat Research team supported projects aimed at promoting these community interests. These projects featured analyst investigations and monitoring efforts to identify potentially malicious activities targeting the participants and operators of both events.

Paris Olympic Games 2024 and the US presidential election

Sporting events such as the Olympics pose unique opportunities for threat actors to launch high-profile attacks. Darktrace's Threat Research team conducted analysis both prior to and during the Olympics to identify potentially malicious activities and threat actor operations. The team identified all potential adversaries with the means and motivation to target the Paris Olympics, including APTs. Similarly, the 2024 US presidential election presented a unique opportunity for both state-sponsored groups and cyber-criminal gangs.

Darktrace's Threat Research team assessed that operations resulting in the release of privileged information, or the loss of election data integrity would support the strategic aims of some adversarial states sponsoring APT groups. Analysts aggregated existing information and prior investigations on APTs likely to attempt disruption of the US election. They also collaborated with national security agencies and Cyber Threat Intelligence (CTI) firms to gather and share any pertinent information.

Going forward, we will continue to engage the community through our Inside the SOC blog and our ongoing collaboration with national agencies like the UK's National Cyber Security Centre. Additionally, we will focus on sector and project-based work.

In 2025, we will release sector-focused reports, starting with healthcare and energy. These reports will reflect Darktrace's Threat Research team's engagement with national agencies, CTI firms, think tanks, governments, and our customers to best understand issues in each specific sector.

The resulting cycle between threat research and community projects will continue to develop Darktrace's expertise and hopefully enable further collaboration with other providers. This model can potentially serve as a template for community partners going forward. Darktrace's Threat Research team will continue to engage stakeholders within both the cyber community and the wider public in 2025 and beyond.

Want to collaborate on a future community project? Get in touch at threatintelligence@darktrace.com we would love to hear from you.

References

01 CVE Metrics: https://www.cve.org/about/Metrics

02 CISA Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

03 Pacific Rim: Neutralizing China-Based Threat: https://news.sophos.com/en-us/2024/10/31/pacific-rim-neutralizing-china-based-threat/

04 Adversarial Misuse of Generative AI: https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai

05 CISA Cybersecurity Advisory AA21-201A: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a

06 Ransomware Statistics: https://www.varonis.com/blog/ransomware-statistics

07 CISA Cybersecurity Advisory AA24-109A: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

08 Two Foreign Nationals Plead Guilty in LockBit Ransomware Group: https://www.justice.gov/opa/pr/two-foreign-nationals-plead-guilty-participating-lockbit-ransomware-group

09 US Charges Dual Russian and Israeli National in LockBit Ransomware Group: https://www.justice.gov/usao-nj/pr/us-charges-dual-russian-and-israeli-national-developer-lockbit-ransomware-group

10 Ransomware Rebrand to Lynx: https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/

11 Arctic Wolf: Fog Ransomware: https://arcticwolf.com/resources/blog/lost-in-the-fog-a-new-ransomware-threat/

12 Darktrace Inside the SOC - Lifting the Fog: https://darktrace.com/blog/lifting-the-fog-darktraces-investigation-into-fog-ransomware

13 SentinelOne - Fog Ransomware: https://www.sentinelone.com/anthology/fog/

14 ESET Threat Report H2 2024: https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h22024.pdf

15 RansomHub Ransomware: https://blackpointcyber.com/resources/threat-profile/ransomhub-ransomware/

16 RansomHub Actors Exploit Zerologon Vulnerability: https://www.darkreading.com/cyberattacks-data-breaches/ransomhub-actors-exploit-zerologon-vuln-in-recent-ransomware-attacks

17 CISA Cybersecurity Advisory AA24-242A: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

18 Meet RansomHub: https://www.s-rminform.com/latest-thinking/meet-ransomhub

19 Mexico President Hacking Attack: https://apnews.com/article/mexico-president-hacking-attack-ransomhub-ransomware-a97fa044850ba05f574f-71d2af3d67c8

20 Russian Gang Hacks Scottish Housing Charity: https://www.thetimes.com/uk/scotland/article/russian-gang-hacks-one-of-scotlands-largest-housing-charities-j7spkmmrv

21 Ransomware Groups: https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/ransomware-groups

22 Ransomware on the Move: BlackBasta, Fog, KillSec, RansomHub: https://www.halcyon.ai/attacks-news/ransomware-on-the-move-blackbasta-fog-killsec-ransomhub

23 RansomHub: https://www.sentinelone.com/anthology/ransomhub/

24 Ransomware Spotlight: RansomHub: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomhub

25 ShadowPad: A Masterpiece of Privately Sold Malware in Chinese Espionage: https://www.sentinelone.com/labs/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/

26 Heightened Threat of State-Aligned Groups: https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups

27 Defending OT Operations Against Pro-Russia Hacktivist Activity: https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity

28 Dragos FrostyGoop ICS Malware Intel Brief: https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_.pdf

29 Top 25 Security Predictions for 2025 (Part 2): https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-25-security-predictions-for-2025-part-2

30 Cyberattacks Against Critical Infrastructure on the Rise: https://www.rockwellautomation.com/en-us/company/news/press-releases/New-Research-Finds-Cyberattacks-Against-Critical-Infrastructure-on-the-Rise-State-affiliated-Groups-Responsible-for-Nearly-60.html

31 Lazarus Luring Employees with Trojanized Coding Challenges: https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/

32 ZINC Attacks Against Security Researchers: https://www.microsoft.com/en-us/security/blog/2021/01/28/zinc-attacks-against-security-researchers/

33 Lazarus Initial Access Tradecraft Using Social Media: https://www.nccgroup.com/es/research-blog/north-korea-s-lazarus-their-initial-access-trade-craft-using-social-media-and-social-engineering/

34 ZINC Weaponizing Open Source Software: https://www.microsoft.com/en-us/security/blog/2022/09/29/zinc-weaponizing-open-source-software/

35 Lazarus Malware: https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html

36 Joint Cyber Security Advisory: https://media.defense.gov/2024/Jul/25/2003510137/-1/-1/1/Joint-CSA-North-Korea-Cyber-Espionage-Advance-Military-Nuclear-Programs.PDF

37 Frequent Freeloader Part I: Secret Blizzard Compromising Storm-0156 Infrastructure: https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

38 Frequent Freeloader Part II: Russian Actor Secret Blizzard Using Tools of Other Groups: https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/

39 ChamelGang Attacking Critical Infrastructure with Ransomware: https://www.sentinelone.com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/

40 State-Backed Hackers Using Ransomware: https://thehackernews.com/2022/06/state-backed-hackers-using-ransomware.html

■ **About Darktrace**

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,400+ employees who protect nearly 10,000 customers globally. To learn more, visit http://www.darktrace.com.

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