Blog / Network / September 13, 2023

How Darktrace Stopped Akira Ransomware

Learn how Darktrace is uniquely placed to identify and contain the novel Akira ransomware strain, first observed in March 2023.

Got any questions? I'm happy to help.

Introduction to Akira Ransomware

In the face of a seemingly never-ending production line of novel ransomware strains, security teams across the threat landscape are continuing to see a myriad of new variants and groups targeting their networks. Naturally, new strains and threat groups present unique challenges to organizations. The use of previously unseen tactics, techniques, and procedures (TTPs) means that threat actors can often completely bypass traditional rule and signature-based security solutions, thus rendering an organization's digital environment vulnerable to attack.

What is Akira Ransomware?

One such example of a novel ransomware family is Akira, which was first observed in the wild in March 2023. Much like many other strains, Akira is known to target corporate networks worldwide, encrypting sensitive files and demanding huge sums of money to retrieve the data and stop it from being posted online [1].

Inside the SOC

Darktrace cyber analysts are world-class experts in threat intelligence, threat hunting and incident response, and provide 24/7 SOC support to thousands of Darktrace customers around the globe. *Inside the SOC* is exclusively authored by these experts, providing analysis of cyber incidents and threat trends, based on real-world experience in the field.

Written by
Manoel Kadja
Cyber Analyst

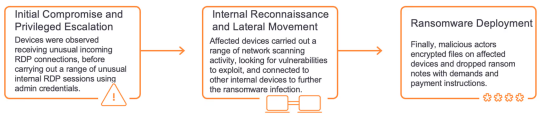
Key characteristics of Akira Ransomware

- **Targeted Attacks**: Focuses on specific industries and organizations, often targeting those with valuable data.
- **Double Extortion Tactics**: Employs double extortion by encrypting data and threatening to release it publicly if the ransom is not paid.
- **Advanced Encryption**: Utilizes sophisticated encryption algorithms to ensure that data recovery is impossible without the decryption key.
- **Custom Ransom Notes**: Delivers personalized ransom notes tailored to the victim, often containing detailed instructions and specific payment demands.
- **Stealth Techniques**: Uses advanced evasion techniques to avoid detection by security tools and to remain undetected for extended periods.
- **Fast Encryption Process**: Known for its rapid encryption process, minimizing the time window for detection and response by the victim.
- **Frequent Updates**: Regularly updates its malware to bypass the latest security defenses and to improve its effectiveness.
- **Professional Communication**: Maintains professional and often polite communication with victims to facilitate ransom

payments and decryption.

Darktrace AI capabilities detect Akira Ransomware

In late May 2023, Darktrace observed multiple instances of Akira ransomware affecting networks across its customer base. Thanks to its anomaly-based approach to threat detection, Darktrace successfully identified the novel ransomware attacks and provided full visibility over the cyber kill chain, from the initial compromise to the eventual file encryptions and ransom notes. In cases where Darktrace was enabled in autonomous response mode, these attacks were mitigated the early stages of the attack, thus minimizing any disruption or damage to customer networks.



Initial access and privileged escalation

Methods used by Akira ransomware for privileged escalation

The Akira ransomware group typically uses spear-phishing

typically uses spear phishing campaigns containing malicious downloads or links as their primary initial access vector; however, they have also been known to use Remote Desktop Protocol (RDP) brute-force attacks to access target networks [2].

While Darktrace did observe the early access activities that are detailed below, it is very likely that the actual initial intrusion happened prior to this, through targeted phishing attacks that fell outside of Darktrace's purview. The first indicators of compromise (IoCs) that Darktrace observed on customer networks affected by Darktrace were typically unusual RDP sessions, and the use of compromised administrative credentials.

Darktrace detection of initial access and priviledged escalation

On one Darktrace customer's network (customer A), Darktrace identified a highly privileged credential being used for the first time on an internal server on May 21, 2023. Around a week later, this server was observed establishing RDP connections with multiple internal destination devices via port 3389. Further investigation carried out by the customer revealed that this credential had indeed been compromised. On May 30, Darktrace detected another device scanning internal devices and

repeatedly failing to authenticate via Kerberos.

As the customer had integrated Darktrace with Microsoft Defender, their security team received additional cyber threat intelligence from Microsoft which, coupled with the anomaly alerts provided by Darktrace, helped to further contextualize these anomalous events. One specific detail gleaned from this integration was that the anomalous scanning activity and failed authentication attempts were carried out using the compromised administrative credentials mentioned earlier.

By integrating Microsoft Defender with Darktrace, customers can efficiently close security gaps across their digital infrastructure. While Darktrace understands customer environments and provides valuable network-level insights, by integrating with Microsoft Defender, customers can further enrich these insights with endpoint-specific information and activity.

In another customer's network (customer B), Darktrace detected a device, later observed writing a ransom note, receiving an unusual RDP connection from another internal device. The RDP cookie used during this activity was an administrative RDP cookie that appeared to have been

compromised. This device was also observed making multiple connections to the domain, api.playanext[.]com, and using the user agent , AnyDesk/7.1.11, indicating the use of the AnyDesk remote desktop service.

Although this external domain does not appear directly related to Akira ransomware, open-source intelligence (OSINT) found associations with multiple malicious files, and it appeared to be associated with the AnyDesk user agent, AnyDesk/6.0.1 [3]. The connections to this endpoint likely represented the malicious use of AnyDesk to remotely control the customer's device, rather than Akira command-and-control (C2) infrastructure or payloads. Alternatively, it could be indicative of a spoofing attempt in which the threat actor is attempting to masquerade as legitimate remote desktop service to remain undetected by security tools.

Around the same time, Darktrace observed many devices on customer B's network making anomalous internal RDP connections and authenticating via Kerberos, NTLM, or SMB using the same administrative credential. These devices were later confirmed to be affected by Akira Ransomware.

Figure 1 shows how Darktrace

detected one of those internal devices failing to login via SMB multiple times with a certain credential (indication of a possible SMB/NTLM brute force), before successfully accessing other internal devices via SMB, NTLM and RDP using the likely compromised administrative credential mentioned earlier.

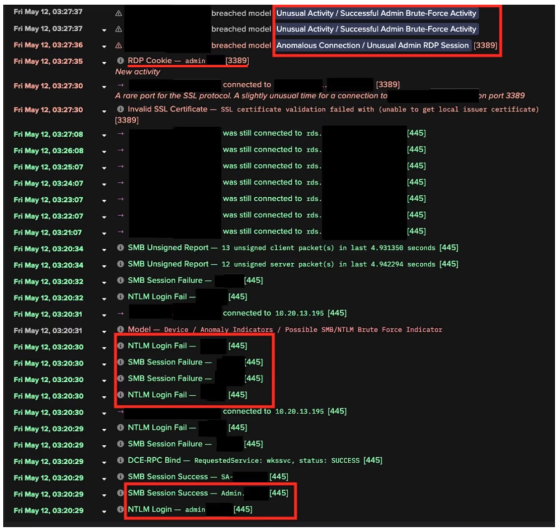


Figure 1: Model Breach Event Log indicating unusual SMB, NTLM and RDP activity with different credentials detected which led to the Darktrace model breaches, "Unusual Admin RDP Session" and "Successful Admin Brute-Force Activity".

Darktrace models observed for initial access and privilege escalation:

- Device / Anomalous RDP Followed By Multiple Model Breaches
- Anomalous Connection / Unusual Admin RDP Session
- New Admin Credentials on Server
- Possible SMB/NTLM Brute Force Indicator
- Unusual Activity / Successful

Admin Brute-Force Activity

Internal Reconnaissance and Lateral Movement

The next step Darktrace observed during Akira Ransomware attacks across the customer was internal reconnaissance and lateral movement.

How Akira Ransomware conducts internal reconnaissance

In another customer's environment (customer C), after authenticating via NTLM using a compromised credential, a domain controller was observed accessing a large amount of SMB shares it had never previously accessed. Darktrace understood that this SMB activity represented a deviation in the device's expected behavior and recognized that it could be indicative of SMB enumeration. Darktrace observed the device making at least 196 connections to 34 unique internal IPs via port 445. SMB actions read, write, and delete were observed during those connections. This domain controller was also one of many devices on the customer's network that was received incoming connections from an external endpoint over port 3389 using the RDP protocol, indicating that the devices were likely being remotely controlled from outside the network. While there were no

direct OSINT links with this endpoint and Akira ransomware, the domain controller in question was later confirmed to be compromised and played a key role in this phase of the attack.

Moreover, this represents the second IoC that Darktrace observed that had no obvious connection to Akira, likely indicating that Akira actors are establishing entirely new infrastructure to carry out their attacks, or even utilizing newly compromised legitimate infrastructure. As Darktrace adopts an anomaly-based approach to threat detection, it can recognize suspicious activity indicative of an emerging ransomware attack based on its unusualness, rather than having to rely on previously observed IoCs and lists of 'known-bads'.

Darktrace further observed a flurry of activity related to lateral movement around this time, primarily via SMB writes of suspicious files to other internal destinations. One particular device on customer C's network was detected transferring multiple executable (.exe) and script files to other internal devices via SMB.

Darktrace recognized that these transfers represented a deviation from the device's normal SMB activity and may have indicated threat actors were attempting to compromise additional devices via

.

the transfer of malicious software.

Figure 2: Advanced Search results showing 20 files associated with suspicious SMB write activity, amongst them executable files and dynamic link libraries (DLLs).

Darktrace DETECT models observed for internal reconnaissance and lateral movement:

- Device / RDP Scan
- Anomalous Connection / SMB Enumeration
- Anomalous Connection / Possible Share Enumeration Activity
- Scanning of Multiple Devices (Cyber AI Analyst Incident)
- Device / Possible SMB/NTLM Reconnaissance
- Compliance / Incoming Remote Desktop
- Compliance / Outgoing NTLM Request from DC
- Unusual Activity / Internal Data Transfer
- Security Integration / Lateral Movement and Integration Detection
- Device / Anomalous SMB Followed By Multiple Model Breaches

Ransomware

deployment

In the final phase of Akira ransomware attacks detected on Darktrace customer networks, Darktrace identified the file extension ".akira" being added after encryption to a variety of files on the affected network shares, as well as a ransom note titled "akira_readme.txt" being dropped on affected devices.

On customer A's network, after nearly 9,000 login failures and 2,000 internal connection attempts indicative of scanning activity, one device was detected transferring suspicious files over SMB to other internal devices. The device was then observed connecting to another internal device via SMB and continuing suspicious file activity, such as appending files on network shares with the ".akira" extension, and performing suspicious writes to SMB shares on other internal devices.

Darktrace's autonomous threat investigator, Cyber AI Analyst™, was able to analyze the multiple events related to this encryption activity and collate them into one AI Analyst incident, presenting a detailed and comprehensive summary of the entire incident within 10 minutes of Darktrace's initial detection. Rather than simply viewing individual breaches as standalone activity, AI Analyst can identify the individual

steps of an ongoing attack to provide complete visibility over emerging compromises and their kill chains. Not only does this bolster the network's defenses, but the autonomous investigations carried out by AI Analyst also help to save the security team's time and resources in triaging and monitoring ongoing incidents.

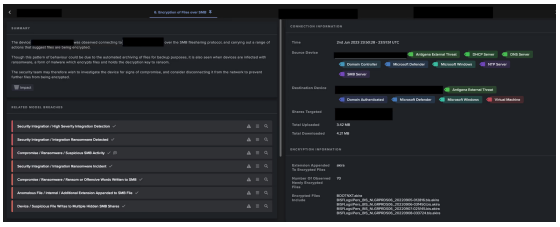


Figure 3: Darktrace Cyber AI Analyst incident correlated multiple model breaches together to show Akira ransomware encryption activity.

In addition to analyzing and compiling Darktrace model breaches, AI Analyst also leveraged the host-level insights provided by Microsoft Defender to enrich its investigation into the encryption event. By using the Security Integration model breaches, AI Analyst can retrieve timestamp and device details from a Defender alert and further investigate any unusual activity surrounding the alert to present a full picture of the suspicious activity.

In customer B's environment, following the unusual RDP sessions and rare external connections using the AnyDesk user agent, an affected device was later observed writing around 2,000 files named "akira_readme.txt" to multiple

internal SMB shares. This represented the malicious actor dropping ransom notes, containing the demands and extortion attempts of the actors.

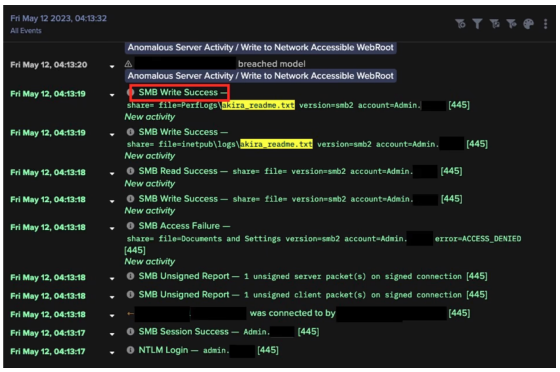


Figure 4: Model Breach Event Log indicating the ransom note detected on May 12, 2023, which led to the Darktrace DETECT model breach, Anomalous Server Activity / Write to Network Accessible WebRoot.

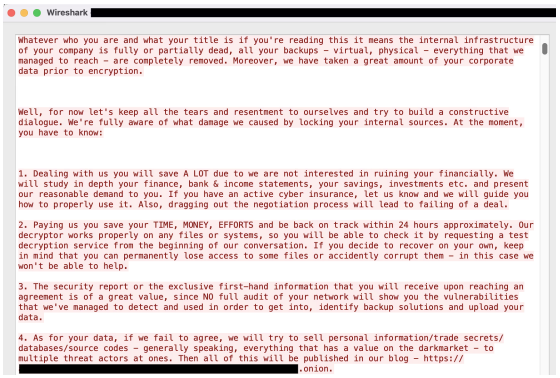


Figure 5: Packet Capture (PCAP) demonstrating the Akira ransom note captured from the connection details seen in Figure 4.

As a result of this ongoing activity, an Enhanced Monitoring model breach, a high-fidelity detection model type that detects activities that are more likely to be indicative of compromise, was escalated to Darktrace's Security Operations Center (SOC) who, in turn were able to further investigate and triage this ransomware activity. Customers who have subscribed to Darktrace's Proactive Threat Notification (PTN) service would receive an alert from

the SOC team, advising urgent follow up action.

Darktrace detection models observed during ransomware deployment:

- Security Integration / Integration Ransomware Incident
- Security Integration / High Severity Integration Detection
- Security Integration / Integration Ransomware Detected
- Device / Suspicious File Writes to Multiple Hidden SMB Shares
- Compliance / SMB Drive Write
- Compromise / Ransomware / Suspicious SMB Activity (Proactive Threat Notification Alerted by the Darktrace SOC)
- Anomalous File / Internal / Additional Extension Appended to SMB File
- Anomalous File / Internal / Unusual SMB Script Write
- Compromise / Ransomware / Ransom or Offensive Words Written to SMB
- Anomalous Server Activity / Write to Network Accessible WebRoot
- Anomalous Server Activity / Write to Network Accessible WebRoot

Darktrace autonomous

autonomous response neutralizes Akira Ransomware

When Darktrace is configured in autonomous response mode, it is able to follow up successful threat identifications with instant autonomous actions that stop malicious actors in their tracks and prevent them from achieving their end goals.

In the examples of Darktrace customers affected by Akira Ransomware outlined above, only customer A had autonomous response mode enabled during their ransomware attack. The autonomous response capability of Darktrace helped the customer to minimize disruption to the business through multiple targeted actions on devices affected by ransomware.

One action carried out by Darktrace's Autonomous Respose was to block all on-going traffic from affected devices. In doing so, Darktrace effectively shuts down communications between devices affected by Akira and the malicious infrastructure used by threat actors, preventing the spread of data on the client network or threat actor payloads.

Another crucial response action applied on this customer's network was combat Akira was to "Enforce a Pattern of Life" on affected devices. This action is designed to prevent devices from performing any activity that would constitute a deviation from their expected behavior, while allowing them to continue their 'usual' business operations without causing any disruption.

While the initial intrusion of the attack on customer A's network likely fell outside of the scope of Darktrace's visibility, Darktrace was able to minimize the disruption caused by Akira, containing the ransomware and allowing the customer to further investigate and remediate.

Darktrace Autonomous Response model breaches:

- Antigena / Network / External Threat / Antigena Ransomware Block
- Antigena / Network / External Threat / Antigena Suspicious Activity Block
- Antigena / Network / Significant Anomaly / Antigena Enhanced Monitoring from Server Block
- Antigena / Network / External Threat / Antigena Suspicious Activity Block
- Antigena / Network / External Threat / Antigena File then New

Outbound Block

- Antigena / Network / Insider Threat / Antigena Unusual Privileged User Activities Block
- Antigena / Network / Significant Anomaly / Antigena Breaches Over Time Block
- Antigena / Network / Significant Anomaly / Antigena Significant Anomaly from Client Block
- Antigena / Network /Insider Threat /Antigena SMB Enumeration Block

Conclusion

The impact of cyber attacks

Novel ransomware strains like Akira Ransomware present a significant challenge to security teams across the globe due to the constant evolution of attack methods and tactics, making it huge a challenge for security teams to stay up to date with the most current threat intelligence.

Therefore, it is paramount for organizations to adopt a technology designed around an intelligent decision maker able to identify unusual activity that could be indicative of a ransomware attack without depending solely on rules, signatures, or statistic lists of malicious IoCs.

Importance of AI-powered cybersecurity solutions

Darktrace identified Akira ransomware at every stage of the attack's kill chain on multiple customer networks, even when threat actors were utilizing seemingly legitimate services (or spoofed versions of them) to carry out malicious activity. While this may have gone unnoticed by traditional security tools, Darktrace's anomaly-based detection enabled it to recognize malicious activity for what it was. When enabled in autonomous response mode, Darktrace is able to follow up initial detections with machine-speed preventative actions to stop the spread of ransomware and minimize the damage caused to customer networks.

There is no silver bullet to defend against novel cyber-attacks, however Darktrace's anomaly-based approach to threat detection and autonomous response capabilities are uniquely placed to detect and respond to cyber disruption without latency.

Credit to: Manoel Kadja, Cyber Analyst, Nahisha Nobregas, SOC Analyst.

Appendices

IOC - Type - Description/ Confidence

202.175.136[.]197 - External destination IP -Incoming RDP Connection

api.playanext[.]com - External hostname - Possible RDP Host

.akira - File Extension - Akira Ransomware Extension

akira_readme.txt - Text File - Akira Ransom Note

AnyDesk/7.1.11 - User Agent - AnyDesk User Agent

MITRE ATT&CK Mapping

Tactic & Technique

DISCOVERY

T1083 - File and Directory Discovery

T1046 - Network Service Scanning

T1135 - Network Share Discovery

RECONNAISSANCE

T1595.002 - Vulnerability Scanning

CREDENTIAL ACCESS, COLLECTION

T1557.001 - LLMNR/NBT-NS Poisoning and SMB Relay

DEFENSE EVASION, LATERAL MOVEMENT

T1550.002 - Pass the Hash

DEFENSE EVASION, PERSISTENCE, PRIVILEGE ESCALATION, INITIAL ACCESS

T1078 - Valid Accounts

DEFENSE EVASION

T1006 - Direct Volume Access

LATERAL MOVEMENT

T1563.002 - RDP Hijacking

T1021.001 - Remote Desktop Protocol

T1080 - Taint Shared Content

T1021.002 - SMB/Windows Admin Shares

INITIAL ACCESS

T1190 - Exploit Public-Facing Application

T1199 - Trusted Relationship

PERSISTENCE, INITIAL ACCESS

T1133 - External Remote Services

PERSISTENCE

T1505.003 - Web Shell

IMPACT

T1486 - Data Encrypted for Impact

References

[1] https://www.bleepingcomputer.com/news/security/meet-akira-a-new-ransomware-operation-targeting-the-enterprise/

[2] https://www.civilsdaily.com/news/cert-in-warns-against-akira-ransomware/#:~:text=Spread%20Methods%3A%20Akira%20ransomware%20is,Desktop%20connections%20to%20infiltrate%20systems

[3] https://hybrid-analysis.com/sample/0ee9baef94c80647eed30fa463447f000ec1f50a49eecfb71df277a2ca1fe4db?environmentId=100

Newsletter

Enjoying the blog?

Sign up to receive the latest news and insights from the Darktrace newsletter – delivered directly to your inbox

Business Email Address*

First Name

Last Name

Submit

Darktrace is committed to protecting and respecting your privacy.

We use the information you provide to send you information about

Trending blogs

1 Securing Generative AI: Managing Risk in Amazon Bedrock with Darktrace / CLOUD
Nov 19, 2025

2 The 17% of email threats SEGs miss – and how Darktrace catches them
Dec 4, 2025

3 Darktrace Named as a Leader in 2025 Gartner® Magic Quadrant™ for Email Security Platforms
Dec 3, 2025

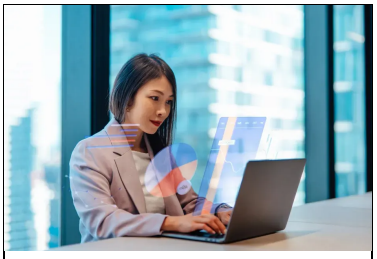
4 From Amazon to Louis Vuitton: How Darktrace Detects Black Friday Phishing Attacks
Nov 27, 2025

5 Pre-CVE Threat Detection: 10 Examples Identifying

Malicious Activity Prior to Public Disclosure of a Vulnerability

Jul 2, 2025

Continue reading

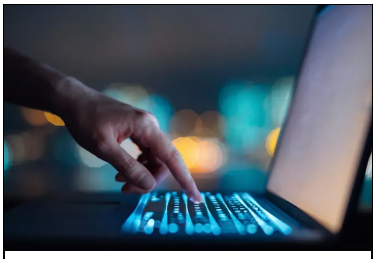


Network • February 5, 2026

AppleScript Abuse: Unpacking a macOS Phishing Campaign

Tara Gould
Malware Research Lead

Read more →



Network • February 3, 2026

Darktrace Malware Analysis: Unpacking SnappyBee

Nathaniel Bill
Malware Research Engineer

Read more →

Network • January 28, 2026

The State of Cybersecurity in the Finance Sector: Six Trends to Watch

Nathaniel Jones
VP, Security & AI Strategy, Field CISO

Read more →

Your data. Our AI.

English

Products

Products Overview

Platform

/ NETWORK

/ EMAIL

/ CLOUD

/ SECURE AI

/ OT

/ IDENTITY

/ ENDPOINT

Platform Add-ons

/ Proactive Exposure Management

/ Attack Surface Management

/ Forensic Acquisition & Investigation

/ Incident Readiness & Recovery

Services

Overview

Company

About us

Contact

News

Leadership

Investors

Careers

SDR Academy

Academy

Federal

Trust Center

Legal

Thoma Bravo Acquisition

Our AI

Cyber AI

AI Research Centre

Resou

All Res

Blog

Custo

Custo Portal

Events

The Inferer

Inside SOC

Glossa

Partne

Partne Overv

Techn Partne

Integra

Partne Portal