DARKTRACE

THREAT LANDSCAPE SERIES:

Neutralizing Ransomware

CONTENTS

A New Era of Ransomware

New ransomware strains are emerging to leverage fileless malware and data exfiltration tactics, while opportunistic attackers are using any change in circumstances to launch more effective campaigns.

It is increasingly common knowledge that conventional security tools, which detect only known cyber-threats using rules and signatures, are blind to evolving strains of ransomware for which such signatures do not exist.

Security teams cannot keep up with these threats using traditional controls alone, especially when they are understaffed or out of office. Thankfully, new techniques to ransomware prevention, detection, and response are emerging.

Not All AI is Created Equal

Hundreds of security vendors have emerged in recent years claiming to use 'AI' to combat ransomware.

However, AI is not a homogenous entity, nor is it the silver bullet to solving your ransomware problems. Critically, it is the specific type and application of AI that will determine a technology's ability to stop ransomware before damage is done.

The historical approach to spotting a cyber-attack involves some combination of rules and signatures to spot the presence of a threat based on previously recognized attacks. AI is often used simply to automate and improve this method, but no matter how quickly these rules and signatures are updated to keep up with attacker innovation and new attack techniques, this approach will always be ill-equipped to deal with attacker TTPs that have never been seen before.

Grounded in unsupervised machine learning and deep learning techniques, Darktrace's Cyber AI learns normal 'patterns of life' for every user and technology in the organization in order to recognize the subtle deviations that point to an emerging threat.

This evolving knowledge of 'normal' for your business allows the system to identify and connect abnormal activity that points to a cyber-threat – including never-before-seen ransomware that evades all other defensive strategies.

Response Must Be Machine Speed, Targeted, and Non-Disruptive

By learning your business from the ground up, Darktrace's AI is able to detect the subtle signs of a ransomware attack in its earliest stages. But detection is only half the battle. In today's threat landscape, security teams need autonomous response to contain attacks that detonate at night, on weekends or over holidays.

Darktrace uses its evolving understanding of 'self' for everyone and everything in the business to make split-second decisions and take targeted action, interrupting ongoing attacks without impacting normal business operations.

This means Darktrace AI can interrupt an emerging ransomware attack at machine speed and with surgical precision, even if the threat is highly targeted and entirely unknown.

It autonomously responds with intelligent, proportionate action – from severing a connection to enforcing the normal 'pattern of life' for a specific device.

Rather than applying a binary block (e.g. completely quarantining the device) as legacy tools would, Darktrace acts surgically to stop the attack, ensuring all normal business operations can continue.

This is true autonomous response. The technology can also integrate with your existing security investments to enhance your entire security stack, feeding AI-powered insights and actions to firewalls, SIEMs, and other tools.

How Ransomware Unfolds With and Without Autonomous Response

In what follows, we explore how ransomware unfolds with and without autonomous response.

In the first six scenarios Darktrace was being trialled, and so was not set up in an active mode where it can act autonomously to respond to potential threats. We can see the actions the technology would have taken in active mode, but in these cases, the attack was either allowed to continue, or it was stopped only due to timely human intervention.

In cases where the security team was not monitoring Darktrace, the ransomware attack proceeded to the latter stages and the victim organization incurred the significant costs and disruption associated with data exfiltration and encryption.

The latter two scenarios demonstrate what happens when Darktrace is configured in 'active mode' and can autonomously respond to an emerging attack. We can see in these real-world examples that the technology takes targeted action to contain ransomware in its early stages.

By learning your business from the ground up, Darktrace's AI is able to detect the subtle signs of a ransomware attack in its earliest stages. But detection is only half the battle. In today's threat landscape, security teams need autonomous response to contain attacks that detonate at night, on weekends or over holidays.

Darktrace uses its evolving understanding of 'self' for everyone and everything in the business to make split-second decisions and take targeted action, interrupting ongoing attacks without impacting normal business operations.

> For us, Autonomous Response technology combats the most sophisticated ransomware attacks out there and it does that within seconds of the threat emerging.

CSO
/ Financial Services

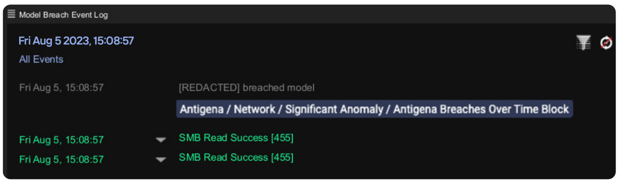
Without Autonomous Response

The early signs of ransomware: A blitz game

At a Canadian defense contractor, an attacker gained access to a server by obtaining an administrator's credentials, and began to spread laterally using WMI commands. However, the unusual and suspicious chain of events was immediately detected by Darktrace's AI, and in active mode autonomous response would have interrupted the attack immediately.

In this case, the attack progressed, and Darktrace's AI detected all 5 attack stages which followed over the next 48 hours, including C2 and further lateral movement. When the attacker deployed ransomware, the few devices on which Darktrace was active were insulated from the attack, while unprotected devices ultimately fell victim to encryption.

With a full deployment of autonomous response, this attack would have ended at the initial login.



```
Model Breach Event Log

Fri Aug 5 2023, 15:08:57
All Events

Fri Aug 5, 15:08:57           [REDACTED] breached model
                              Antigena / Network / Significant Anomaly / Antigena Breaches Over Time Block

Fri Aug 5, 15:08:57      ▾    SMB Read Success [455]
Fri Aug 5, 15:08:57      ▾    SMB Read Success [455]
```

Figure 1: A Darktrace model fires when multiple anomalies are detected over time

Recycling ransomware: The return of Ryuk

Self-Learning AI detected and alerted on Ryuk ransomware when it struck a real estate company trialling Darktrace.

The initial compromise surfaced when unusual .dat files were seen being downloaded onto a device, followed by unusual connectivity between the compromised and target devices indicating lateral movement and bruteforce RDP attempts.

Darktrace successfully detected and alerted on this ransomware attack at multiple stages. With autonomous response activated, the attack would have been quickly neutralized and prevented from advancing to its next stages, saving this company's valuable data. Without it, this company suffered widespread data encryption.

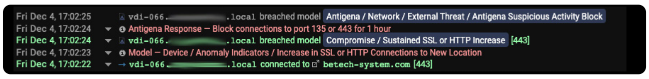
> Ransomware can spread across your network rapidly, so you need tools that can prevent that from occurring. AI can autonomously take control and provide split-second reactions, which is very useful for preventing damage.

CIO
/ Local Government

How AI stopped a WastedLocker intrusion

At an agricultural organization in the US, Darktrace detected a WastedLocker ransomware attack after an employee was deceived into downloading a fake browser update.

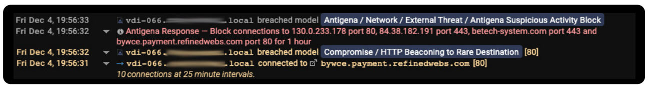
Darktrace immediately detected a series of unusual HTTP connections from one of the 5,000 devices it was monitoring in this trial. We can see how it would have instantly blocked the C2 traffic on this and various other channels as they emerged.



```
Fri Dec 4, 17:02:25        vdi-066.[redacted].local breached model Antigena / Network / External Threat / Antigena Suspicious Activity Block
Fri Dec 4, 17:02:24   ▾    Antigena Response — Block connections to port 135 or 443 for 1 hour
Fri Dec 4, 17:02:24   ▾    vdi-066.[redacted].local breached model Compromise / Sustained SSL or HTTP Increase [443]
Fri Dec 4, 17:02:23   ▾    Model — Device / Anomaly Indicators / Increase in SSL or HTTP Connections to New Location
Fri Dec 4, 17:02:22   ▾    → vdi-066.[redacted].local connected to betech-system.com [443]
```

Figure 2: Model breaches and the action Darktrace would have taken to address them

As the attacker switched tactics and attempted further beaconing, Darktrace escalated its response. At no point did it suggest interfering with activity not related to the attack.



```
Fri Dec 4, 19:56:33        vdi-066.[redacted].local breached model Antigena / Network / External Threat / Antigena Suspicious Activity Block
Fri Dec 4, 19:56:32   ▾    Antigena Response — Block connections to 130.0.233.178 port 80, 84.38.182.191 port 443, betech-system.com port 443 and
                           bywce.payment.refinedwebs.com port 80 for 1 hour
Fri Dec 4, 19:56:32   ▾    vdi-066.[redacted].local breached model Compromise / HTTP Beaconing to Rare Destination [80]
Fri Dec 4, 19:56:31   ▾    → vdi-066.[redacted].local connected to bywce.payment.refinedwebs.com [80]
                           10 connections at 25 minute intervals.
```

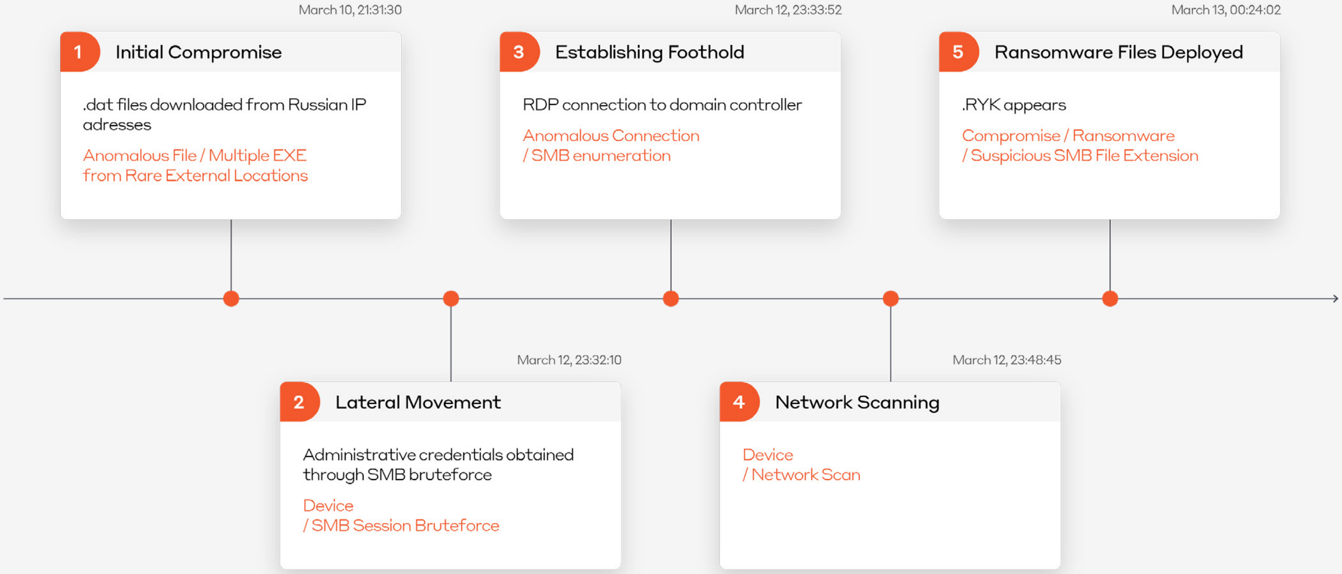
Figure 3: Darktrace's potential response escalates

Fortunately, the security team reacted to Darktrace's alerts in time and, with Cyber AI Analyst automatically generating a concise and actionable incident summary, they were able to stop the attack before serious damage was done.

This fast reaction time was crucial in deterring an extremely costly and damaging security incident. Relying on human reponse alone is a dangerous game: had the team not been on high alert, and without Darktrace's high-confidence detections, the attack would have progressed into the encryption stages.

> The ransomware that we are up against today moves too quickly for humans to contend with alone – the way we stay ahead is by having Darktrace AI fight back precisely and proportionately on our behalf.

CIO
/ Retail


March 10, 21:31:30

1 Initial Compromise

.dat files downloaded from Russian IP adresses

Anomalous File / Multiple EXE from Rare External Locations

March 12, 23:32:10

2 Lateral Movement

Administrative credentials obtained through SMB bruteforce

Device / SMB Session Bruteforce

March 12, 23:33:52

3 Establishing Foothold

RDP connection to domain controller

Anomalous Connection / SMB enumeration

March 12, 23:48:45

4 Network Scanning

Device / Network Scan

March 13, 00:24:02

5 Ransomware Files Deployed

.RYK appears

Compromise / Ransomware / Suspicious SMB File Extension

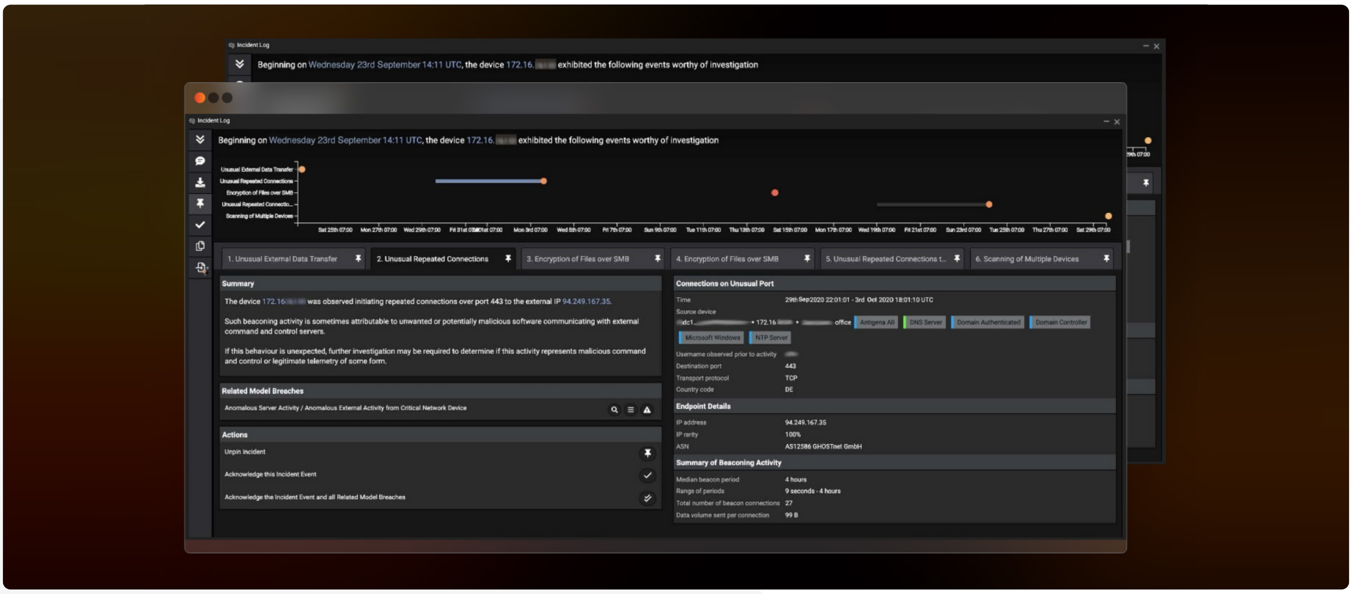
Figure 4: A timeline of the attack

Cyber AI Analyst investigates Sodinokibi (REvil) ransomware

After the credentials of a retail organization's IT team member were used to compromise a domain controller, Darktrace's AI detected the attacker writing suspicious files and then deleting batch scripts and log files in the root directory to clear their tracks.

The domain controller then made connections to several rare external endpoints, and Darktrace witnessed a 28MB upload that was likely exfiltration of initial reconnaissance data.

Over the course of two weeks, Darktrace witnessed an SQL server engaging in a network scan, unusual internal RDP connections using administrative credentials, and data uploads to multiple cloud storage endpoints. PsExec was used to deploy the ransomware, resulting in file encryption. Despite clear findings presented by Cyber AI Analyst across 15 incident reports, Darktrace was in trial mode and nobody was monitoring the technology. In the absence of autonomous response, the Sodinokibi ransomware attack was allowed to succeed, while Darktrace would have stopped it in its early stages.



Incident Log
Unusual External Data Transfer
Unusual Repeated Connections
Encryption of Files over SMB
Unusual Repeated Connectio...
Scanning of Multiple Devices
Sat 25th 07:00
Mon 27th 07:00
Wed 29th 07:00
Fri 31st 07:00
Sat 1st 07:00
Mon 3rd 07:00
Wed 5th 07:00
Fri 7th 07:00
Sun 9th 07:00
Tue 11th 07:00
Thu 13th 07:00
Sat 15th 07:00
Mon 17th 07:00
Wed 19th 07:00
Fri 21st 07:00
Sun 23rd 07:00
Tue 25th 07:00
Thu 27th 07:00
Sat 29th 07:00
1. Unusual External Data Transfer
2. Unusual Repeated Connections
3. Encryption of Files over SMB
4. Encryption of Files over SMB
5. Unusual Repeated Connections t...
6. Scanning of Multiple Devices

Beginning on Wednesday 23rd September 14:11 UTC, the device 172.16.[redacted] exhibited the following events worthy of investigation

Beginning on Wednesday 23rd September 14:11 UTC, the device 172.16.[redacted] exhibited the following events worthy of investigation

Summary

The device 172.16[redacted] was observed initiating repeated connections over port 443 to the external IP 94.249.167.35.

Such beaconing activity is sometimes attributable to unwanted or potentially malicious software communicating with external command and control servers.

If this behaviour is unexpected, further investigation may be required to determine if this activity represents malicious command and control or legitimate telemetry of some form.

Related Model Breaches

Anomalous Server Activity / Anomalous External Activity from Critical Network Device

Actions

Unpin Incident

Acknowledge this Incident Event

Acknowledge the Incident Event and all Related Model Breaches

Connections on Unusual Port

Time	29th Sep2020 22:01:01 - 3rd Oct 2020 18:01:10 UTC
Source device	[redacted]dc1.[redacted] • 172.16[redacted] • [redacted] office Antigena All DNS Server Domain Authenticated Domain Controller Microsoft Windows NTP Server
Username observed prior to activity	[redacted]
Destination port	443
Transport protocol	TCP
Country code	DE

Endpoint Details

IP address	94.249.167.35
IP rarity	100%
ASN	AS12586 GHOSTnet GmbH

Summary of Beaconing Activity

Median beacon period	4 hours
Range of periods	9 seconds - 4 hours
Total number of beacon connections	27
Data volume sent per connection	99 B

Figure 5: Cyber AI Analyst investigates

Egregor ransomware: Gone but not forgotten

When a logistics company in Europe decided to trial Darktrace, the AI quickly discovered pre-existing botnet malware that would result in an Egregor ransomware attack.

Darktrace detected unusual use of HTTPS for lateral movement and reconnaissance, as well as the disguising of endpoints as doppelgangers of legitimate sites. Darktrace revealed every stage of this attack, which triggered 40 individual model breaches, while Cyber AI Analyst investigated in the back-ground, connecting the dots and forming a cohesive security narrative.

With nobody monitoring Darktrace and without autonomous response, however, this company suffered data exfiltration and encryption.

Having seen what autonomous response could have done to stop this attack before it launched, the organization quickly began implementing Darktrace technology at its full capability across their digital estate.

> I don't think we could live without Darktrace's Autonomous Response

Head of Corporate Service
/ Food Retailer

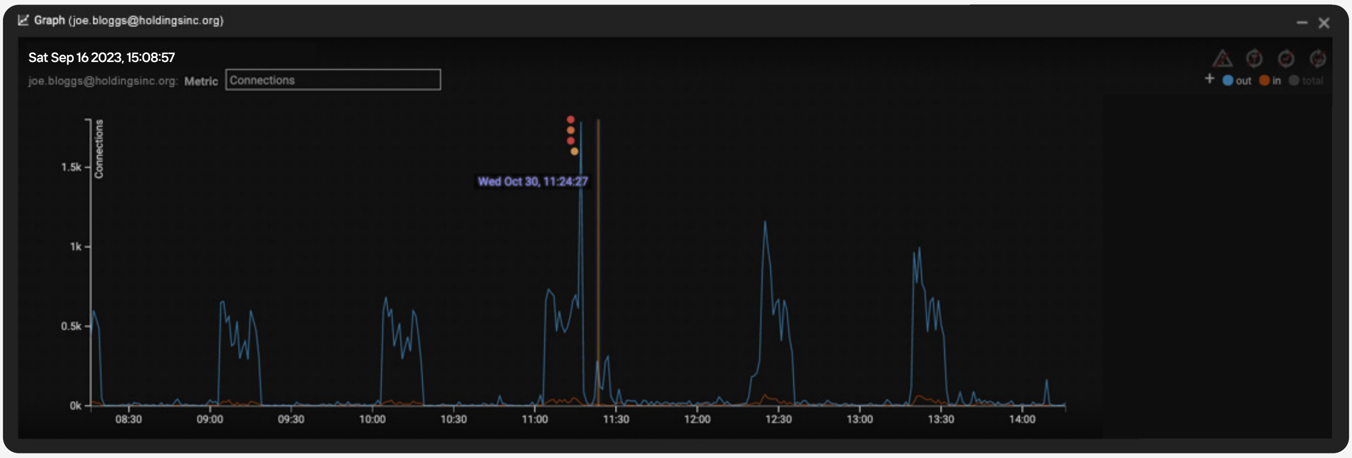
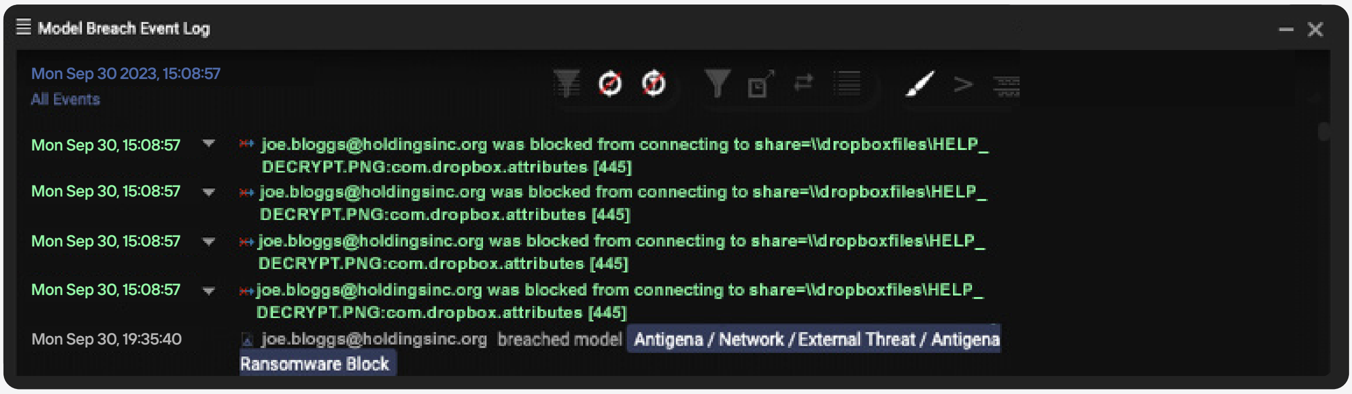


Figure 6: Several Darktrace alerts fire, and a deviation from the regular pattern of life is visible

Double extortion ransomware

The speed with which ransomware can spread was highlighted in this incident at a Canadian energy company, where encryption began just over 12 hours after initial reconnaissance. Every stage of the attack was detected and alerted on by Darktrace, including network scanning, RDP movement and malicious TeamViewer connections.

These activities, along with a subsequent 1.95TB data download and the initiation of encryption, largely occurred out of hours, but were identified as evidence of an attack by Darktrace. With autonomous response, this attack would have ended in the initial reconnaissance and lateral movement stages.



```
Mon Sep 30, 15:08:57   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Mon Sep 30, 15:08:57   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Mon Sep 30, 15:08:57   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Mon Sep 30, 15:08:57   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Mon Sep 30, 19:35:40   joe.bloggs@holdingsinc.org breached model Antigena / Network / External Threat / Antigena
                       Ransomware Block
```

Figure 7: Darktrace stops the infected device from conducting lateral movement & ransom activity

With Autonomous Response

Minimizing the REvil impact delivered via Kaseya servers

As the USA prepared for a holiday weekend ahead of the Fourth of July, the ransomware group REvil leveraged a vulnerability in Kaseya software to attack over 1,500 companies.

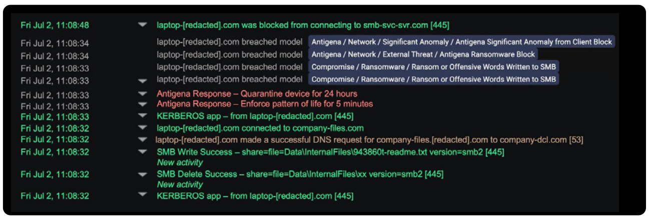
One company with autonomous response deployed was protected from this attack when Darktrace's AI detected unusual SMB traffic, and enforced the laptop's 'pattern of life', preventing it from further unusual connections.

> Crucially, the AI responds intelligently which allows us to continue normal business operations uninterrupted. This is the future of security.

CSO

/ Financial Services

Subsequent attempts made by the infected device to connect to other devices were halted, preventing the attack from spreading. The network's files were saved from encryption only because these actions were taken immediately and kept pace with the machine-speed of the attack **– thanks to autonomous response.**



```
Fri Jul 2, 11:08:48   laptop-[redacted].com was blocked from connecting to smb-svc-svr.com [445]
Fri Jul 2, 11:08:34   laptop-[redacted].com breached model  Antigena / Network / Significant Anomaly / Antigena Significant Anomaly from Client Block
Fri Jul 2, 11:08:34   laptop-[redacted].com breached model  Antigena / Network / External Threat / Antigena Ransomware Block
Fri Jul 2, 11:08:33   laptop-[redacted].com breached model  Compromise / Ransomware / Ransom or Offensive Words Written to SMB
Fri Jul 2, 11:08:33   laptop-[redacted].com breached model  Compromise / Ransomware / Ransom or Offensive Words Written to SMB
Fri Jul 2, 11:08:33   Antigena Response – Quarantine device for 24 hours
Fri Jul 2, 11:08:33   Antigena Response – Enforce pattern of life for 5 minutes
Fri Jul 2, 11:08:33   KERBEROS app – from laptop-[redacted].com [445]
Fri Jul 2, 11:08:32   laptop-[redacted].com connected to company-files.com
Fri Jul 2, 11:08:32   laptop-[redacted].com made a successful DNS request for company-files.[redacted].com to company-dcl.com [53]
Fri Jul 2, 11:08:32   SMB Write Success – share=file=Data\InternalFiles\943860t-readme.txt version=smb2 [445]
                      New activity
Fri Jul 2, 11:08:32   SMB Delete Success – share=file=Data\InternalFiles\xx version=smb2 [445]
                      New activity
Fri Jul 2, 11:08:32   KERBEROS app – from laptop-[redacted].com [445]
```

Figure 8: Darktrace detects attempted encryption from the infected device and takes action

Darktrace neutralizes zero-day ransomware

At an agricultural organization in the US, Darktrace detected a WastedLocker ransomware attack after an employee was deceived into downloading a fake browser update.

Darktrace immediately detected a series of unusual HTTP connections from one of the 5,000 devices it was monitoring in this trial. We can see how Darktrace would have instantly blocked the C2 traffic on this and various other channels as they emerged.

```
Wed Oct 30, 11:13:12 - SMB Write Success - share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes
```

Fortunately, Darktrace was in Active Mode, and kicked in a second later, enforcing the usual pattern of life by blocking anomalous connections for five minutes, immediately stopping the encryption. By the time Darktrace's AI took action, only four of these files were successfully encrypted.

```
Wed Oct 30, 11:13:13 - Darktrace Response - Quarantince device for 24 hours
```

Figure 9: Darktrace responds 1 second after ransomware was detected

Darktrace then took a second action to stop the ransomware from spreading to other devices.

The combination of various anomalous activities was sufficient evidence for autonomous response to neutralize the threat: patient zero was quarantined for 24 hours, unable to connect to the server or any other device on the network.

Darktrace therefore not only stopped the encryption activity in its tracks, but also prevented the attackers from moving laterally across the network unimpeded – either by scanning, using harvested admin credentials, or performing internal reconnaissance.

Darktrace/Email: Stop Ransomware at the Source

Many ransomware attacks originate via email platforms, proving that traditional email gateways and legacy detection approaches relying on rules and signatures are not strong enough to catch advanced ransomware every time.

What's more, these traditional solutions are limited in scope and fail to connect email activity to related malicious actions throughout the digital infrastructure.

With the power of Cyber AI, Darktrace/Email builds a deep understanding of the unique human behind the email address. The technology adapts to your dynamic workforce in order to recognize the nuanced shifts in behavior that indicate a ransomware campaign.

It then responds autonomously and proportionately to stop the threat at machine speed and protect your organization from exposure – whether that means holding back the email entirely, locking a link, or converting attachments to a harmless file type.

Should ransomware make it past the inbox and enter the network, Darktrace/Email is uniquely able to work with Darktrace/Network to trace the origin of the attack and prevent lateral spread.

Darktrace/OT: Protecting Operational Systems from Ransomware

The EKANS ransomware attack in 2020 was the first known ransomware to target ICS-specific machinery, showing the importance of leveraging security tools that can continuously adapt to OT environments and defend these systems against even zero-day attacks.

Many ransomware campaigns also target industrial environments through vulnerabilities in IT infrastructure. Indirect compromise poses an additional threat, as OT systems may become collateral damage during IT-focused attacks.

Given the potential harm to critical infrastructure, the need for a security technology that can correlate patterns across disparate infrastructure is increasingly urgent.

Darktrace/OT learns normal 'patterns of life' for radically different technologies and deployment types, from decades-old PLCs, to distributed sensors and industrial IoT, to highlight unusual activity that may be indicative of ransomware or other cyber-threats.

With its unified view, Cyber AI understands the connection between malicious activity in IT systems and behaviour in OT systems – making it capable of stopping threats that move between what have traditionally been security siloes.

Darktrace offers a free trial for:

Darktrace/Network

Darktrace/Email

Darktrace/OT

Contact your Darktrace representative or get in touch via **https://darktrace.com/contact** today.

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. Breakthrough innovations from its R&D Centers have resulted in over 145 patent applications filed. Darktrace employs over 2,200 people around the world and protects c.8,800 organizations globally from advanced cyber-threats.

Scan to
LEARN MORE

DARKTRACE
Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010
Latin America: +55 11 97242 2011

info@darktrace.com

darktrace.com