DARKTRACE

2021 Ransomware Threat Report

A New Era of Threat

Following several high-profile and disruptive campaigns, governments around the world now consider ransomware a risk to national security. In the US, the Department of Justice has ranked ransomware on par with terrorism, while the UK's GCHQ has ranked it as the primary threat facing businesses and citizens.

Security teams in both the private and public sector are being forced to rethink their strategies for dealing with ransomware, as existing defenses repeatedly prove inadequate. The signature-based defenses that organizations rely on are too slow, static, and siloed to meaningful stop fast-moving, sophisticated threats.

As new attack techniques continue to emerge, organizations are being caught off guard. The speed and scale of attack campaigns mean that human teams alone cannot react in time. Self-Learning AI technology that understands the business is becoming critical in empowering defenders to fight back in the face of this increasingly hostile threat landscape.

This threat report explores emerging trends in attacker techniques and includes seven real-world ransomware attacks discovered and stopped by Darktrace's AI in customer environments.

> "The world evolves and the risks change ... I would say that the risk that we keep our eyes on the most now is cyber-risk"
>
> Jerome Powell, Chairman, Federal Reserve

Business are expected to experience a ransomware attack every 11 seconds in 2021, up from 40 seconds in 2016

Capitalizing on Remote Working Conditions

New working practices have exacerbated the ransomware risk facing organizations, with hybrid working making mission-critical infrastructure accessible remotely – resulting in sensitive data spread across a myriad of environments. Cyber-criminals have been quick to capitalize on this, with a rise in RDP exploitation – either as a result of accidental exposure or brute-forcing.

But by far the most common method of entry for ransomware is email. Attacks are moving away from 'pray-and-spray' techniques to increasingly tailored and targeted campaigns which leverage the latest news cycles and trends to get victims to engage with phishing campaigns and click malicious links – resulting in a download of ransomware.

"We're confident that Darktrace is able to evolve with our organization during this time of uncertainty"

CISO, Better.com

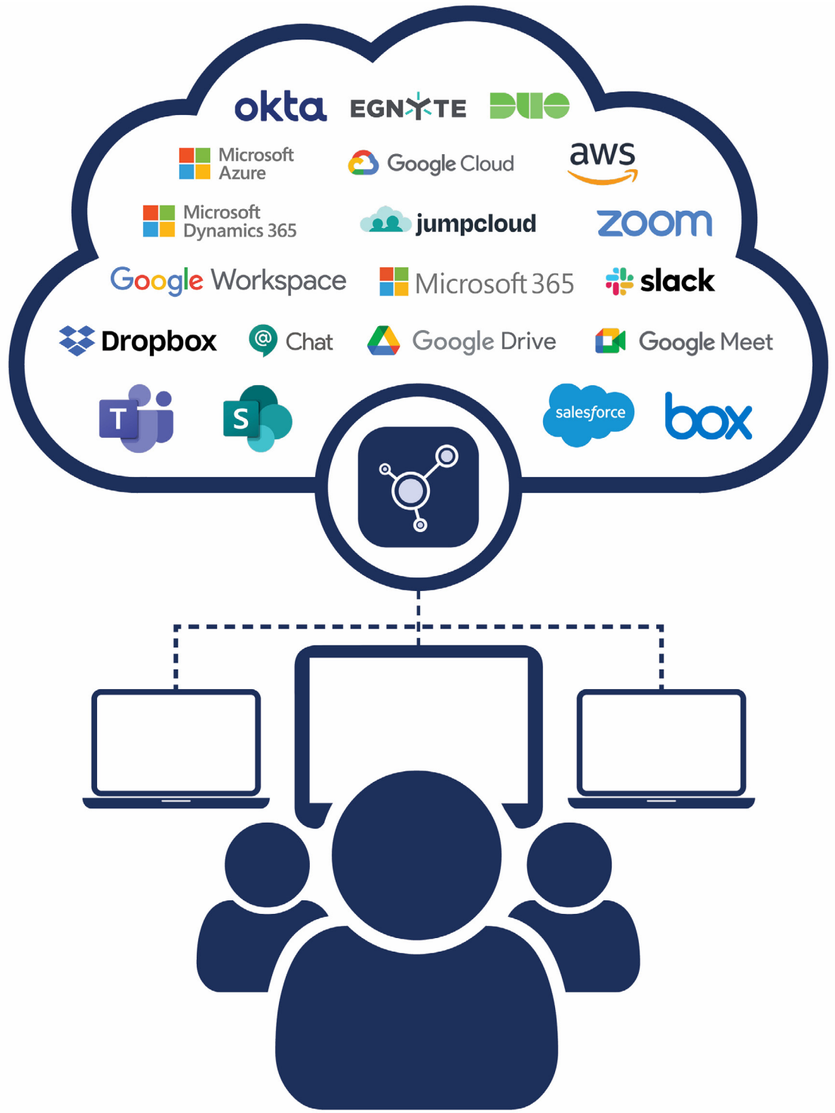


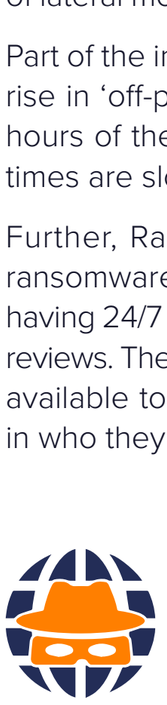
Figure 1: Darktrace protects users wherever they operate and wherever data lives

Increasing Professionalism of Threat Actors

Attackers are acutely aware of the defensive tools they are trying to evade and know better than anyone the limitations of the legacy, siloed approach that the majority of organizations still rely on. And in every area they are innovating, developing new techniques to bypass these – such as creating fileless malware and new methods of lateral movement. The result is millions in profits for threat actors.

Part of the increasingly revenue-driven model of cyber-crime is the rise in 'off-peak' attacks, with ransomware detonating in the early hours of the morning or on the weekend, when human response times are slow.

Further, Ransomware-as-a-Service – a sinister trend in which ransomware is sold or leased to affiliates – is booming, with many having 24/7 customer helpdesks, 'ethics' codes, and even third-party reviews. The result is machine-speed, highly-advanced malware being available to low-skilled mercenaries, who are often less selective in who they target.



Global cyber-crime costs will reach $10.5 trillion by 2025

Cybersecurity Ventures

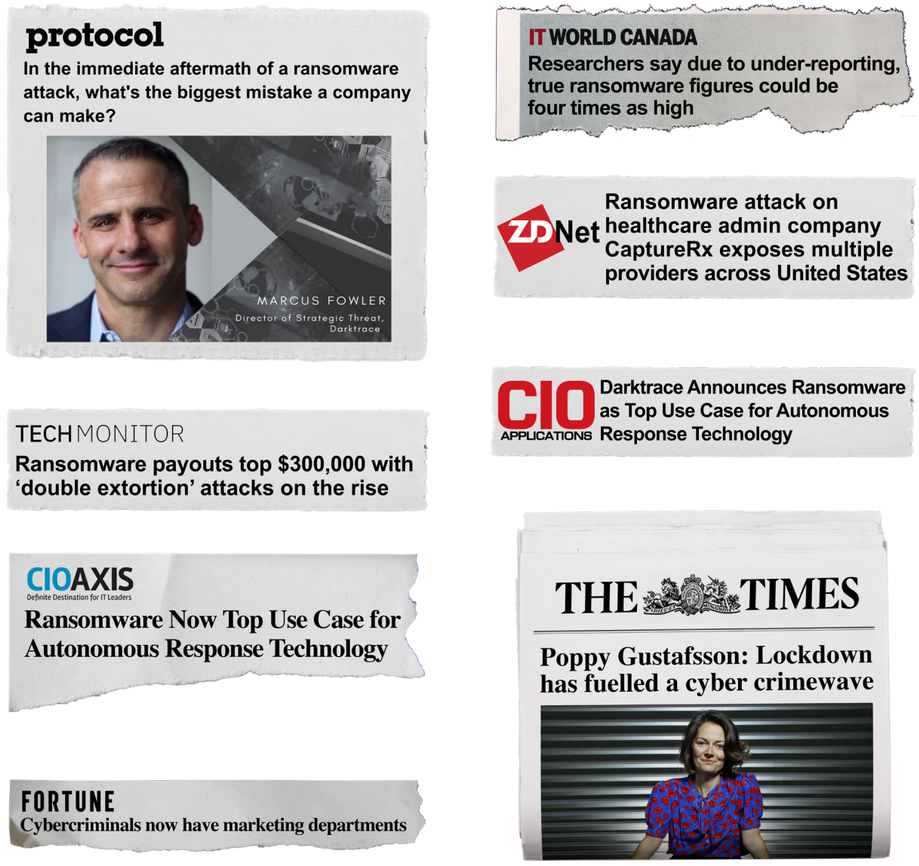


Figure 2: Cyber-attacks are increasingly front page news, with ransomware dominating the headlines

Double Extortion Ransomware

An uptick in double extortion campaigns – where data is first exfiltrated and then encrypted – has provided attackers with further leverage should an organization refuse to pay up. Release of sensitive data results in reputational damage, compliance fines, and competitive disadvantage. But while many hope payment puts an end to the issue, most end up both out of pocket and without their data and systems restored as promised.

Before the rise of double extortion campaigns, business resilience meant data backups in the case of encryption. Now, it means keeping things moving when operations and systems are being held hostage.

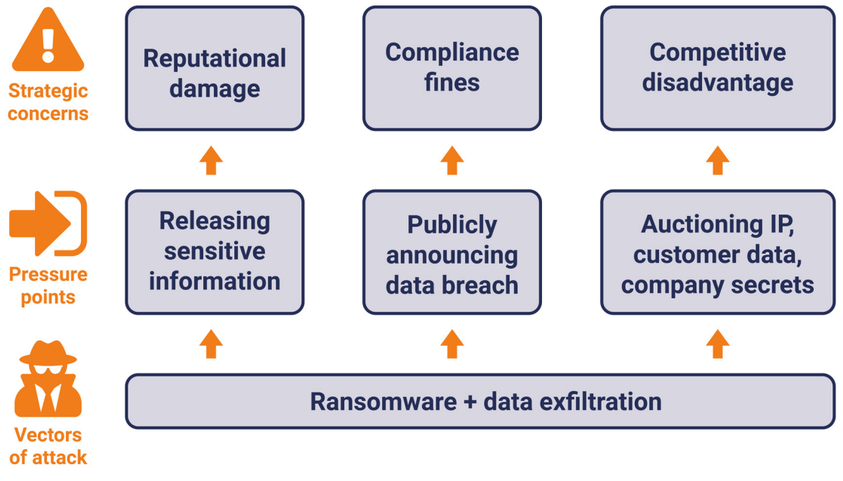


Figure 3: Varieties of double extortion ransomware

> "Ransomware is growing month on month and most are now employing a tactic known as 'double extortion'. In effect, victim organisations are now being held to ransom not only on availability but also on confidentiality"
>
> Ransomware: A Perfect Storm, RUSI

> "Darktrace's AI technology catches the threats other tools miss and has enabled us to take our cyber resilience to the next level"
>
> Director of Technology and Security, NHLPA

Offensive AI: Supercharged Ransomware

The challenge of stopping ransomware is only getting harder as AI-powered attacks emerge in the wild. In a report published by MIT Tech Review, offensive AI is expected to increase the scale, speed, and sophistication of cyber-threats, augmenting every stage of the cyber kill chain.

Deep-learning analytics will enable AI to increase the personalization of attacks, leading to greater accuracy and a higher success rate. At the same time, cyber-criminals will be better able to predict the layout and defensive strategy of victims' digital infrastructure and data.

Today, cyber security is no longer a human-scale problem: it is a machine-on-machine fight. It is critical that organizations adopt defensive AI to protect against this next generation of automated ransomware.

Autonomous Response technology is fundamental to thwarting in-progress ransomware – no matter how novel or sophisticated. Self-Learning AI understands how and when to respond to contain malicious activity in a targeted and proportionate manner, while sustaining normal business operations.

of executives have already begun to prepare for AI-powered cyber-attacks

MIT Tech Review Report

"Darktrace's autonomous cyber response is necessary not only because humans alone cannot keep up with today's threat climate, but also because self-driving AI attacks are approaching"

Michael Ioannou, CIO, Elias Neocleous

Historical Tools vs Novel Threats

The traditional approach to defense comes in many forms, from firewalls and antivirus tools, to email gateways and preventative controls. While these can identify basic threats via simple detection mechanisms, their reliance on pre-defined rules, signatures, and playbooks makes them unable to stop novel and signatureless strains of ransomware.

By definition, a system designed to identify future ransomware campaigns based on the hallmarks of previously encountered attacks is fundamentally incapable of catching new and emerging threats.

Furthermore, cyber security has evolved in silos: email, cloud, network, industrial, and endpoint security have all developed independently. But, with unpredictable employee behavior cutting across a wide range of services and infrastructure, isolated point solutions lack the visibility and context needed to determine malicious from benign, with ransomware able to spread between environments without security tools connecting the dots.

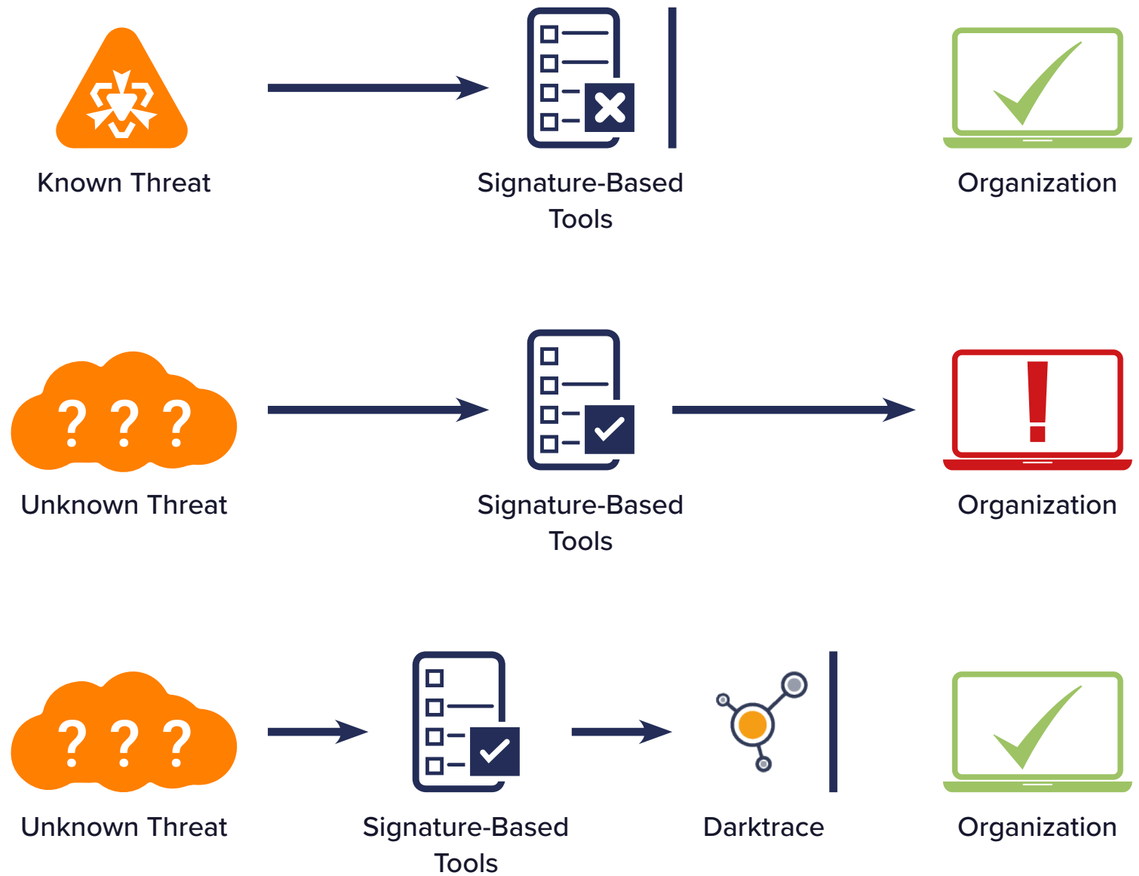


Figure 4: Darktrace's evolving understanding of 'self' allows it to interrupt novel and unknown threats that other tools miss

Automated vs Autonomous Response

Given the speed, scale, and sophistication of modern ransomware, human teams alone are no longer capable of staying ahead of attackers. Organizations need a technology that can not only detect ransomware but contain it – without a human 'on call' to authorize an action.

This has led to automated response solutions, such as SOARs, email gateways, and 'next-gen' IPS. While these respond to known threats, they are bound by historical attack data and pre-defined rules.

As a result, their response mechanisms are mechanical, inflexible, and heavy-handed, favoring a one-size-fits-all approach. All too often, this translates to a choice between encrypted systems or drastic shutdowns when ransomware hits.

Rather than risk facing this difficult dilemma, thousands of organizations are turning to Self-Learning AI that delivers a targeted, proportionate response – stopping ongoing cyber-attacks while allowing business operations to continue as normal.

The technology works by forming a dynamic and evolving understanding of the normal 'patterns of life' for every user and device in an organization, and all the connections between them. This enables the AI to identify the subtlest signals of never-before-seen ransomware in real time, before surgically enforcing 'normal'.

> "We have confidence in Darktrace's AI-enabled Autonomous Response, which has a greater capacity for action and response than a human team"
>
> **CIO, Delfingen**

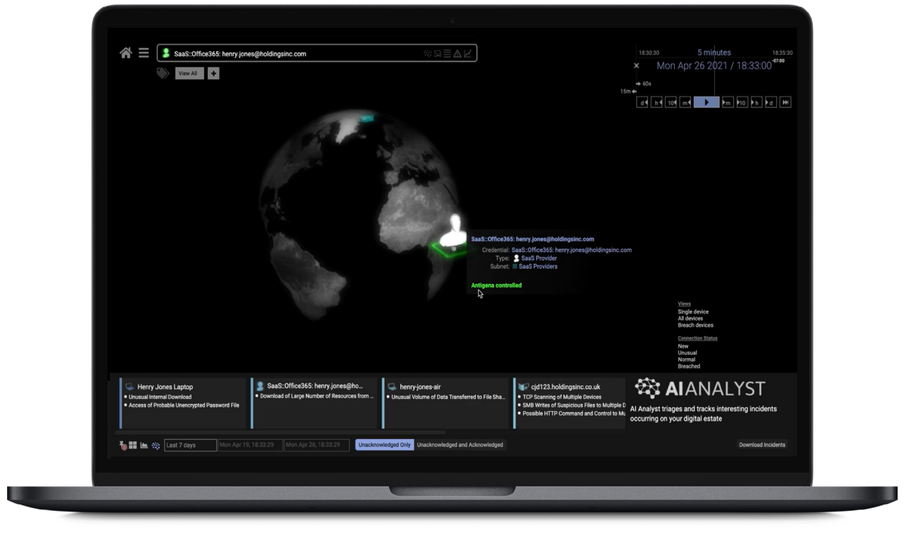


Figure 5: Darktrace Antigena takes surgical and proportionate action to stop threats while maintaining normal business operations

Self-Learning AI

While traditional solutions pre-define ‘bad’ or ‘benign’, Self-Learning AI develops an evolving understanding of your organization to identify and stop the targeted attacks that inevitably get inside. This allows the technology to stop both known and unknown strains of ransomware that static security tools are blind to.

Augmenting the Human With AI-Powered Investigations

When an incident occurs, understanding the origin and nature of the threat is critical. For every security event detect by Self-Learning AI, Cyber AI Analyst, Darktrace’s AI investigation technology, automatically launches an investigation: triaging, interpreting, and reporting on the full scope of security incidents.

Using deep learning, Cyber AI Analyst contextualizes security events, adapts to novel techniques, and translates its findings into a digestible security narrative that can be actioned in minutes - reducing time to triage by up to 92%. It currently investigates over 1.4 million security incidents per week.

> “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”
>
> CIO, Las Vegas

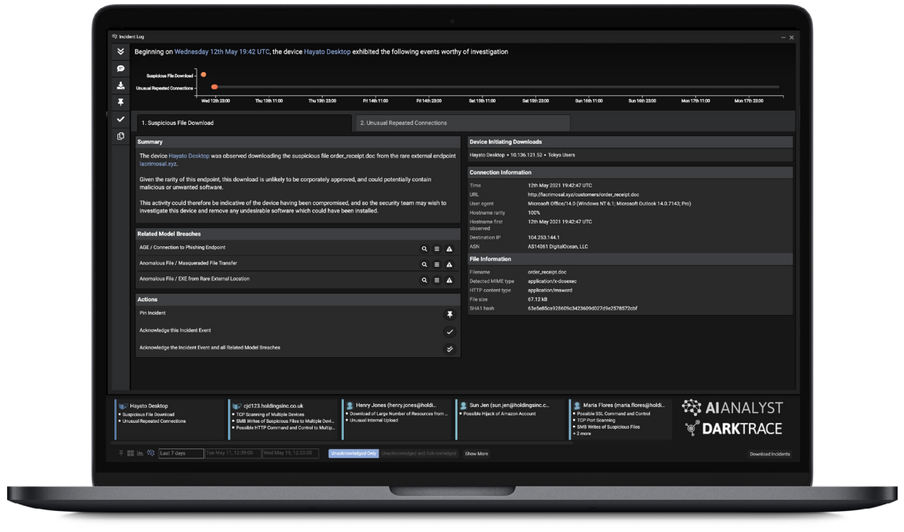


Figure 6: Cyber AI Analyst auto-generates Incident Reports that put teams in a position to take action

Preventing Business Disruption When Ransomware Strikes

Darktrace's Autonomous Response technology, Darktrace Antigena, operates as an AI decision-making framework that acts in seconds to surgically neutralize both novel and signatureless ransomware in real time, enabling organizations to create self-defending businesses.

Darktrace Antigena calculates the best action to take to autonomously contain in-progress ransomware at machine speed. Unlike traditional tools, the Self-Learning AI dynamically reacts on the fly to thwart unusual behavior as it emerges and unfolds – across email, cloud, SaaS, the traditional network, endpoints, IoT, and OT.

Autonomous Response works by enforcing the normal 'patterns of life' for compromised users and devices. Only the malicious activity is interrupted, with employees and systems free to perform their roles as usual.

Such capabilities are only possible through a continually evolving understanding of what 'normal' looks like for each part of the digital ecosystem.

Darktrace Antigena's highly proportionate and targeted response ensures that ransomware is stopped in its tracks - but not at the cost of downtime and business operations.

Key Takeaways: Darktrace Antigena

- Takes action to stop unpredictable and fast-moving ransomware
- Surgical and proportionate response which prevents business disruption
- Operative across the entire digital ecosystem
- 24/7 protection – even on the weekend and at night

Figure 7: Darktrace Antigena stops ransomware at machine-speed

Around-the-Clock Protection

Autonomous Response technology is used by thousands of organizations globally to stop ransomware seconds after it emerges, no matter where it arises. Providing 24/7 autonomous defense, Darktrace Antigena safeguards critical data and systems when teams are overwhelmed, unprepared, or simply unavailable – at night, on the weekends, and on holiday.

By learning 'on the job', Darktrace Antigena helps organizations build cyber resilience over time – understanding better and better how infrastructure, devices, and users normally behave, while surgically neutralizing malicious outliers in real time.

Around the world, Darktrace Antigena neutralizes a threat every second – buying back critical time and freeing employees to prioritize strategic tasks.

> "The comfort that you get from having 24/7 active defenses is like nothing else. Darktrace can really save your skin when you're being attacked from all sides"
>
> Head of IT Operations, PPS Insurance

Figure 8: Autonomous Response neutralizes threats wherever and whenever they occur - without the need for human input

Stopping Ransomware at the Source

Ransomware is often the last stage in the kill chain, with the majority of cases delivered via email. But, due to email gateways' reliance on pre-defined rules and signatures, subtle attacks often slip through.

Darktrace for Email neutralizes targeted spear phishing campaigns and impersonation attacks that other tools miss. By understanding 'normal' for every user and correspondent, Darktrace is the only technology that truly understands the human behind email communications.

This enables the AI to intelligently determine whether a given email meaningfully deviates from the normal interactions between sender, recipient, and the wider organization. Darktrace for Email then stops the threat at the source - autonomously locking links, converting attachments to harmless file types, and holding emails back.

This is vital in the case of ransomware, as Autonomous Response stops the threat before it reaches patient zero: before ransomware can be downloaded, before it can spread laterally, and before encryption even begins.

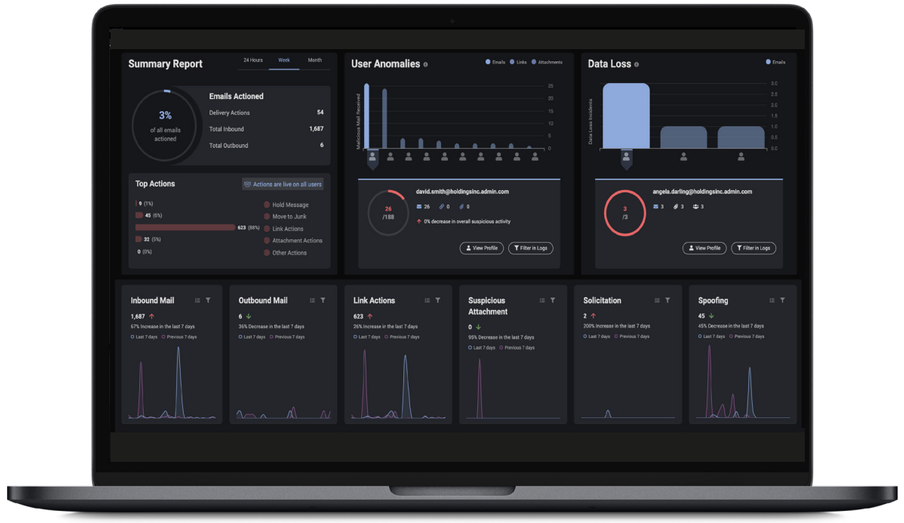


Figure 9: Darktrace for Email stops ransomware before it reaches the inbox due to its understanding of the human behind the email address

"We rely on Darktrace AI to fight back against email attacks with complete autonomy and lightning speed - before damage is done"

CIO, McLaren Group

Threat Finds: A Proportionate, AI-Native Response in Action

Autonomously Neutralizing Zero-Day Ransomware

Darktrace Antigena autonomously stopped a zero-day ransomware attack targeting an electronics manufacturer. Despite the fact that this strain of ransomware was not associated with any publicly known IoCs, Self-Learning AI thwarted the attack in seconds, with only 4 files being successfully encrypted.

A device was infected with ransomware after an employee clicked on a link in a phishing email. The device was first observed by Darktrace as making an unusually large number of connections, writing multiple SMB files, and transferring data internally to a server it did not usually communicate with.

Hundreds of Dropbox-related files were then accessed on SMB shares, with several of these files becoming encrypted, appended with a [HELP_DECRYPT] extension.

Fortunately, Autonomous Response kicked in a second later. It enforced the device's usual 'pattern of life', immediately stopping the encryption before the damage was done – saving the manufacturer from operational downtime, missed orders, and millions in customer fines.

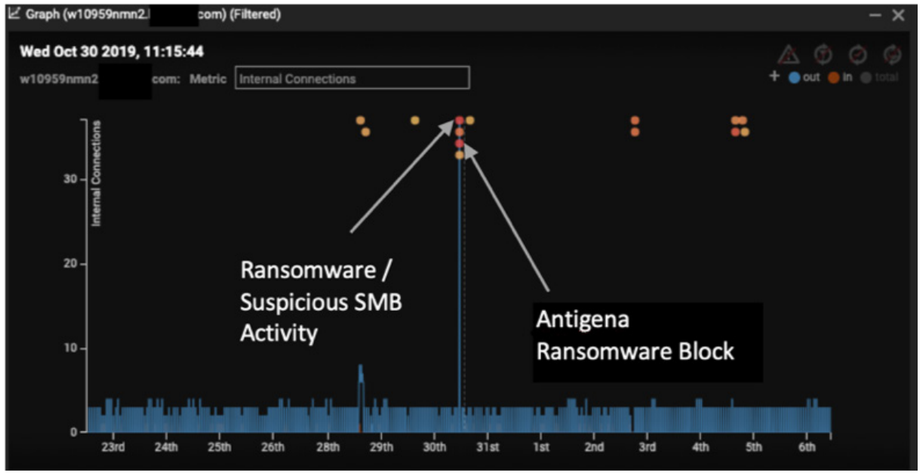


Figure 10: Four model breaches observed and a dotted line representing Darktrace Antigena's actions

"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, Ted Baker

Catching WastedLocker Before Detonation

Darktrace autonomously detected and investigated a WastedLocker intrusion at a US agricultural organization. Autonomous Response was not configured to take action in this case, but we can see how it would have reacted to stop the attack before encryption, escalating its response as the threat progressed.

The initial infection took place when an employee was deceived into downloading a fake browser update. A virtual desktop device then started making HTTP and HTTPS connections to external destinations.

Darktrace Antigena suggested instantly blocking the C2 traffic on port 443 and parallel internal scanning on port 135.

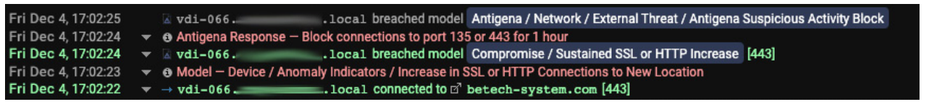


Figure 11: The Threat Visualizer reveals the action Darktrace Antigena would have taken

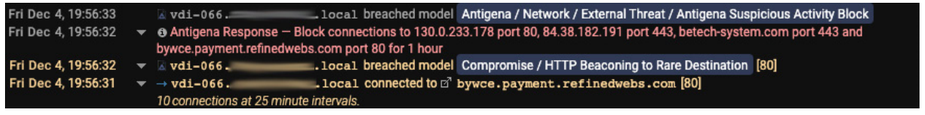


Figure 12: How Darktrace Antigena would have escalated its response

But without Darktrace Antigena in Active Mode, the attack proceeded, with the cyber-criminal using 'living off the land' techniques to authenticate against a Domain Controller. Soon after, a transfer of suspicious .csproj files was detected and at least four other devices began exhibiting similar command and control (C2) communications, encrypted with legitimate certificates.

Thanks to Darktrace's real-time detections – and Cyber AI Analyst investigating and reporting on the incident – the security team was able to contain the attack, taking the infected devices offline.

This attack used many notable Tools, Techniques, and Procedures (TTPs) to bypass signature-based tools, as well as using 'living off the land' techniques. It is plausible that without Darktrace in place, the ransomware would have been successful in encrypting files, preventing business operations at a critical time, and possibly inflicting huge financial and reputational losses.

> "Darktrace is fundamentally transforming how we defend our systems"
>
> Information Systems Manager, Layton Construction

Stopping Automated Extortion Before Encryption

Darktrace detected and responded to an extortion campaign that occurred on a Friday night. While the team was away, Self-Learning AI stopped the threat before a single file or system had been encrypted, all without the need for human input, allowing the team to enjoy their weekend.

The attack began when an employee accessed their personal emails from a corporate smartphone and was tricked into downloading a malicious file containing ransomware. Seconds later, the device began connecting to an external server on the Tor network and SMB encryption activities began.

Within just nine seconds, Darktrace had detected the threat and had raised a prioritized alert. As the behavior persisted over the next few seconds, the AI revised its judgment on the severity of the threat.

Self-Learning AI independently stopped the attack, interrupting all attempts to write encrypted files to network shares – meaning that the organization's sensitive data was kept safe even when humans were not on call.

Figure 13: Self-Learning AI identifies a ransomware attack, taking action at machine speed to neutralize the threat

> "I sleep a lot better at night knowing I have AI tools running"
>
> CIO, Penn Highlands Healthcare

Ransomware-as-a-Service: How AI Fought Back Against Eking Ransomware

At a governmental organization in APAC, Darktrace detected and investigated a case of Eking ransomware. This attack was likely an example of Ransomware-as-a-Service, a growing concern for security teams globally. With autonomous detection and investigation, the security team was able to stop the threat from advancing – and causing damage.

An internal server was infected with Eking ransomware via an attack vector outside of Darktrace's visibility – likely via email where Self-Learning AI was not deployed. The first activity the AI observed was the infected device engaging in internal reconnaissance activity. This included SMB enumeration, extensive scanning over 10 commonly exploited ports, and indicators of Nmap.

Four and a half hours after scanning concluded, the infected server began encrypting files on a second server – all of which took place late at night local time. The device transitioned from making just a few internal connections per day to making thousands in less than an hour. Darktrace not only detected this but immediately began investigating the threat.

Figure 14: A graph of connections and unusual activity demonstrating how significant of a deviation this activity was from normal device behaviour

Had Darktrace Antigena been deployed, it would have taken action at the first stage of the attack, as the initial scanning took place, and prevented the malware from ever reaching the encryption stage.

But as it was, the security team was still able to act faster than they otherwise would have and limit the damage the next morning, thanks to Cyber AI Analyst's actionable insights.

Preventing Ransomware Before Patient Zero

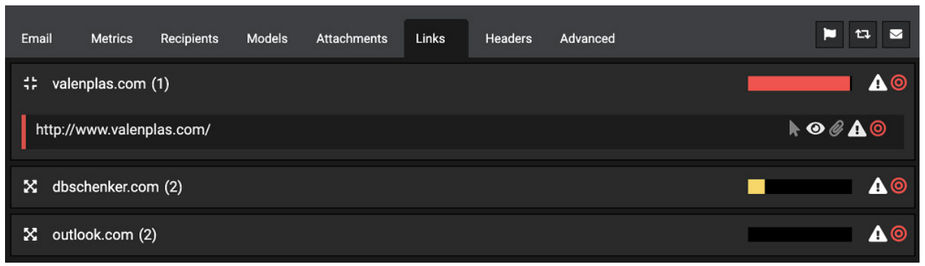


Figure 15: The suspicious link in question

Darktrace detected and stopped one cyber-criminal using ISO files to inflict malware on a food distributor in Spain. This method of attack bypassed the traditional email security tools in place, but Darktrace for Email's dynamic understanding of users' normal 'patterns of life' ensured the attack was recognized and stopped at its earliest stages.

Since the attack was stopped before patient zero, it is difficult to know exactly how the threat would have played out. However, subsequent analysis into the macro-enabled file suggests that this was the first stage of a ransomware attack.

The emails were a clever and well-executed spoof of a legitimate email address of a supplier. However, Self-Learning AI recognized that the sender had never been seen in any prior correspondence across the business. Darktrace surfaced a file titled URGENTE_PO_120620.iso, suggesting the attacker was attempting to inject a sense of urgency to solicit the victim into downloading the file.

Darktrace's Self-Learning AI also recognized that the file extension .iso was highly anomalous for the group, user, and the organization as a whole. Even more suspiciously, the size of the attachment was incredibly small (just 485.4 kB). These findings, in conjunction with the New Contact and Wide Distribution tags of the email, caused Darktrace for Email to hold the email back from every recipient's inbox.

This meant that the attack was stopped before it had even begun, all without the security team needing to do anything.

> "For us, Autonomous Response technology combats the most sophisticated ransomware attacks out there and it does that within seconds of the threat emerging"
>
> Abhay Raman, Chief Security Officer, Sun Life

Thwarting Double Extortion Ransomware at an Energy Company

At an energy company in Canada, Darktrace detected and investigated every stage of a fast-moving and stealthy double extortion ransomware campaign. As a result, the team was able to action a quick response.

Darktrace identified an internal server engaging in unusual network scanning and attempted lateral movement using the Remote Desktop Protocol. Compromised admin credentials were used to spread rapidly from the server to another internal device, 'serverps'.

The device 'serverps' initiated an outbound connection to TeamViewer, before connecting to an internal file server, downloading 1.95 TB of data, and uploading this to pcloud[.]com. This took place during work hours to blend in with regular admin activity. Following the completion of the data exfiltration, the device 'serverps' finally began encrypting files on 12 devices.

As with the majority of ransomware incidents, the encryption happened outside of office hours – overnight in local time – to minimize the chance of the security team responding quickly. But with Darktrace investigating the threat, the team was able to action a quick response the next day to keep operations running.

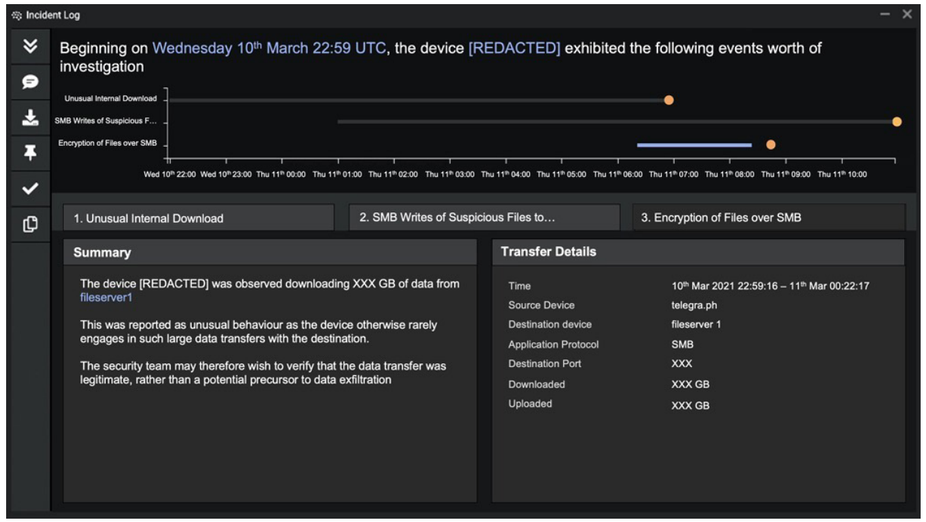


Figure 16: Cyber AI Analyst incident for a compromised device, detailing an unusual internal download

How AI Would Have Stopped LockBit Ransomware Encrypting Over 300,000 Files

During a trial with a retail company, Darktrace detected a LockBit ransomware campaign.

Unlike most ransomware attacks where a threat actor spends days or weeks inside a system before detonation, LockBit only requires the presence of a human for a number of hours, after which it propagates through a system and infects other hosts on its own. Crucially, the malware performs reconnaissance and continues to spread during the encryption phase. This allows it to cause maximum damage faster than other manual approaches.

The attack started when a cyber-criminal gained access to a single privileged credential. With the use of this credential, the device was able to spread and encrypt files within hours of the initial infection.

Shortly afterwards, the first of many WMI commands (ExecMethod) to multiple internal destinations was performed by an internal IP address over DCE-RPC. Within three minutes, the device had started to write executable files over SMB to hidden shares on multiple destinations.

In less than two hours, the ExecMethod command was delivered to a critical device – the 'encryption host' – shortly followed by an executable file write (eck3.exe) to its hidden c$ share. A recovery file – 'Restore-My-Files.txt' – was identified by Darktrace as being targeted one second after the first encryption event. 8,998 recovery files were written, one to each encrypted folder.

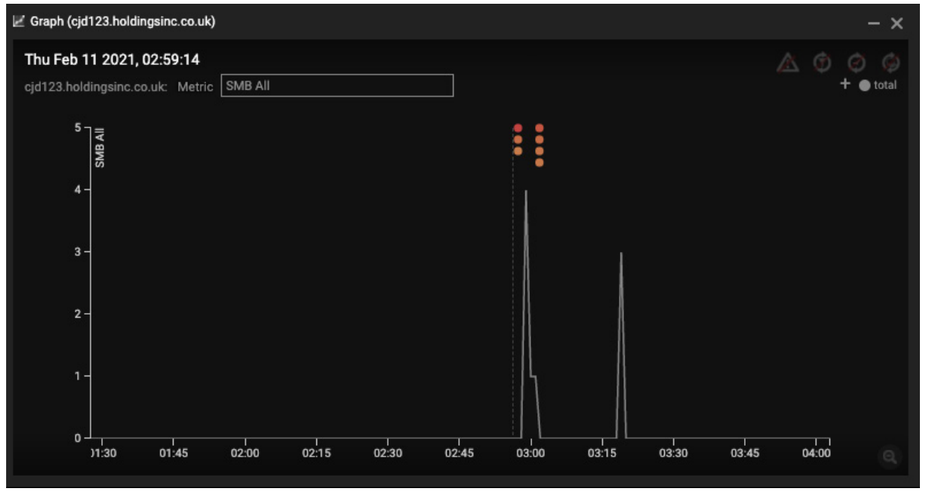


Figure 17: An example of Darktrace's Threat Visualizer showcasing anomalous SMB connections, with model breaches represented by dots

If enabled, Darktrace Antigena would have surgically blocked the initial WMI operations and SMB drive writes that triggered the attack while allowing the critical network devices to continue standard operations. Even if the foothold had been established, Self-Learning AI would have enforced the 'pattern of life' of the encryption host, preventing the cascade of encryption over SMB.

As it was, over 300,000 files were encrypted and appended with the .lockbit extension - even though Darktrace detected the threat before encryption began.

About Darktrace

Darktrace (DARK:L) a global leader in cyber security AI, delivers world-class technology that protects over 5,000 customers worldwide from advanced threats, including ransomware and cloud and SaaS attacks. The company's fundamentally different approach applies Self-Learning AI to enable machines to understand the business in order to autonomously defend it. Headquartered in Cambridge, UK, the company has 1,500 employees and over 30 offices worldwide. Darktrace was named one of TIME magazine's 'Most Influential Companies' for 2021.

For More Information

- Visit darktrace.com
- Book a demo
- Visit our YouTube channel
- Follow us on Twitter
- Follow us on LinkedIn