How Ransomware Unfolds
With and Without Autonomous Response

Contents

"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, CSO Sun Life

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 RESPOND 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.

In what follows, we explore how ransomware unfolds **with and without Autonomous Response**.

In the first six scenarios, Darktrace was being trialled and so Darktrace RESPOND was not set up in active mode where it can act autonomously. 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 RESPOND *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.

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 RESPOND 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.

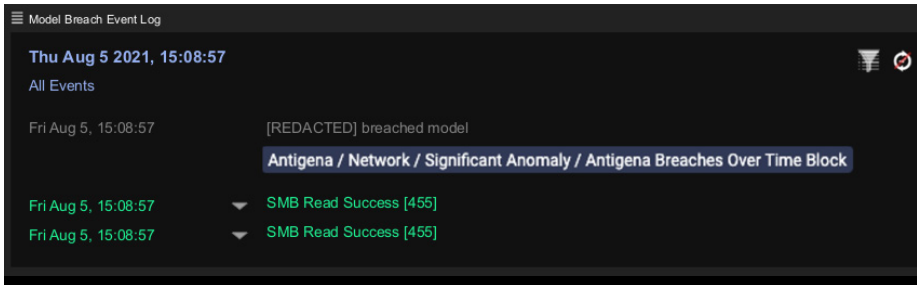

Figure 1: A Darktrace model fires when multiple anomalies are detected over time

> "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."
>
> Leon Shepherd, CIO Ted Baker

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 Darktrace RESPOND would have instantly blocked the C2 traffic on this and various other channels as they emerged.

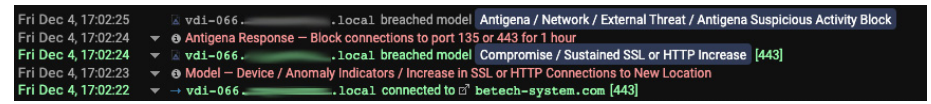

Figure 2: Model breaches and the action Darktrace would have taken to address them

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.

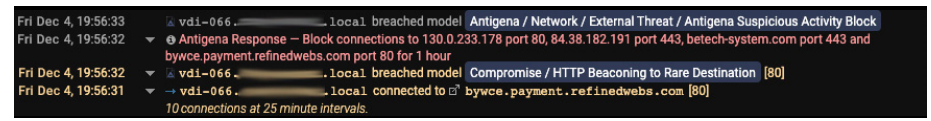

Figure 3: Antigena's potential response escalates

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.

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.

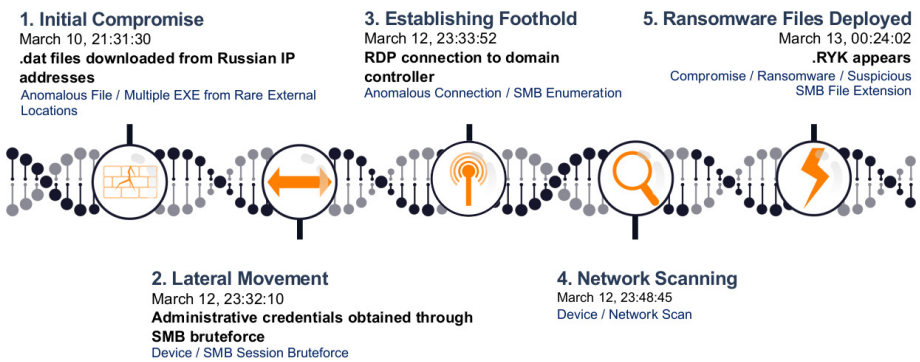

Figure 4: A timeline of the attack

> "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."

Michael Sherwood, Chief Innovation Officer, City of Las Vegas

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.

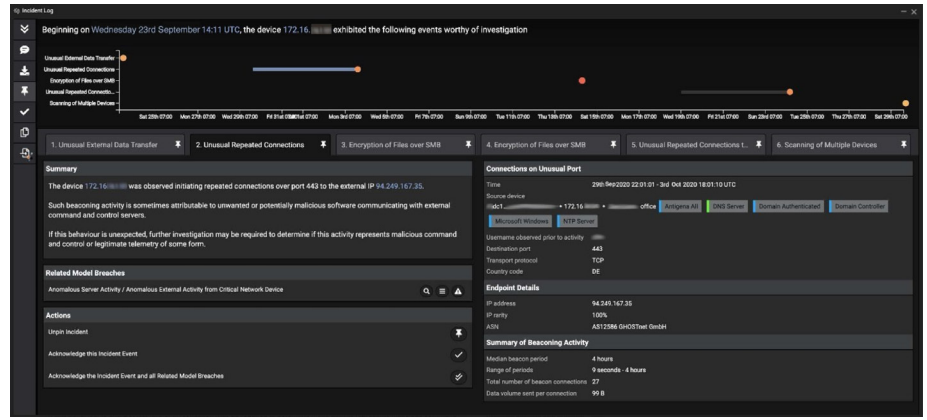

Figure 5: Cyber AI Analyst investigates

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.

Egregor ransomware: Gone but not forgotten

When a logistics company in Europe decided to trail 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 background, 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.

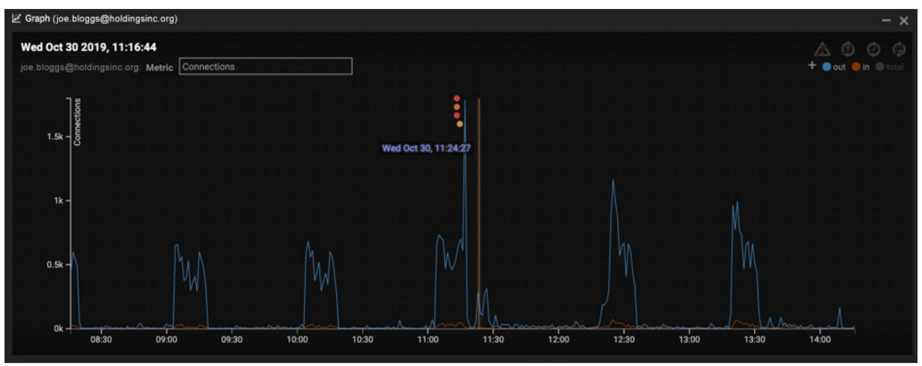

Figure 6: Several Darktrace alerts fire, and a deviation from the regular pattern of life is visible

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.

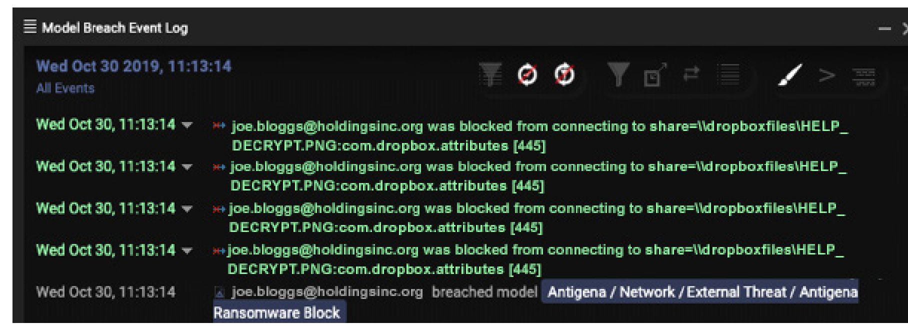

Figure 7: Darktrace stops the infected device from conducting lateral movement & ransom activity

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

David Levin, Head of Corporate Service, Sefalana Group

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.

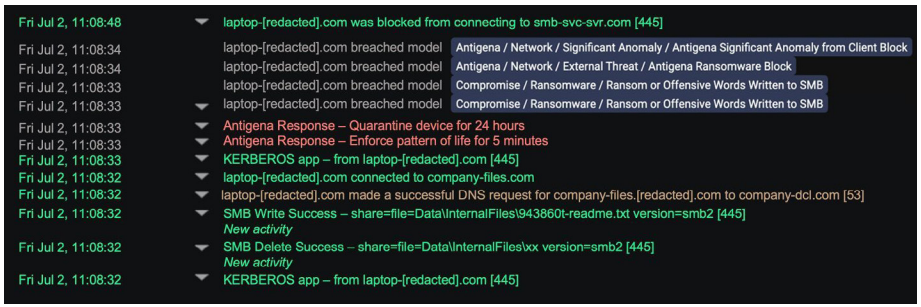

Figure 8: Darktrace detects attempted encryption from the infected device and takes action

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.

> "Crucially, the AI responds intelligently which allows us to continue normal business operations uninterrupted. This is the future of security."
>
> Abhay Raman, CSO Sun Life

Darktrace neutralizes zero-day ransomware

In this example, Darktrace's AI detected a spike in the pattern of regular connections made by a device, as well as suspicious SMB activity and unusual reverse DNS lookups, a tactic often used during reconnaissance.

Further investigation into the SMB activity revealed that hundreds of Dropbox-related files were accessed on SMB shares that the device had not previously accessed. Moreover, several of these files started becoming encrypted, appended with a [HELP_DECRYPT] extension.

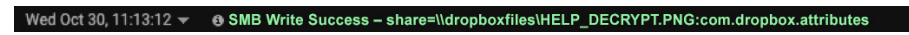

Figure 9: Darktrace detects SMB activity relating to Dropbox files

Fortunately, Darktrace RESPOND 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.

Figure 10: 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.