How ransomware unfolds with and without Autonomous Response

Contents

Introduction 1

Without Autonomous Response

The early signs of ransomware: A blitz game 2

How AI stopped a WastedLocker intrusion 2

Cyber AI Analyst investigates Sodinokibi (REvil) ransomware 3

Double extortion ransomware 3

With Autonomous Response

Minimizing the REvil impact delivered via Kaseya servers 4

Antigena neutralizes zero-day ransomware 4

Conclusion 5

Introduction

In an era of fast-moving and ever-changing attacks, with shrinking dwell times and increasingly stretched security teams, detection alone is not enough, and technology which can respond to emerging attacks has become a necessity in stopping cyber disruption.

Darktrace Antigena 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 four scenarios, Darktrace was being trialled and so Darktrace Antigena was not set up in Active Mode where it can act autonomously. In these cases, the attack was either allowed to continue, or it was stopped only due to timely human intervention. The latter two scenarios demonstrate what happens when Antigena is set up to autonomously respond to an emerging attack.

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 Antigena 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.

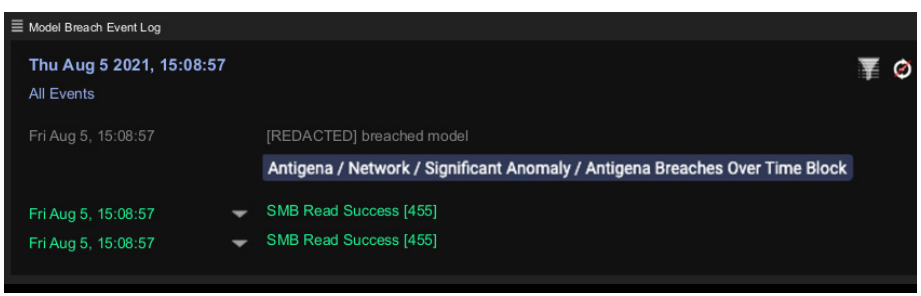

Figure 1: An Antigena model fires when multiple anomalies are detected over time

> "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. We can see how Antigena would have instantly blocked the C2 traffic on this and various other channels as they emerged.

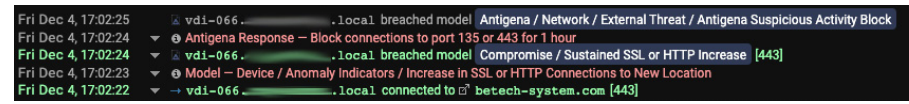

Figure 2: Model breaches and the action Antigena would have taken to address them

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

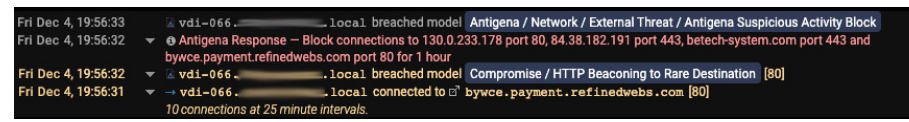

Figure 3: Antigena's potential response escalates

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.

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.

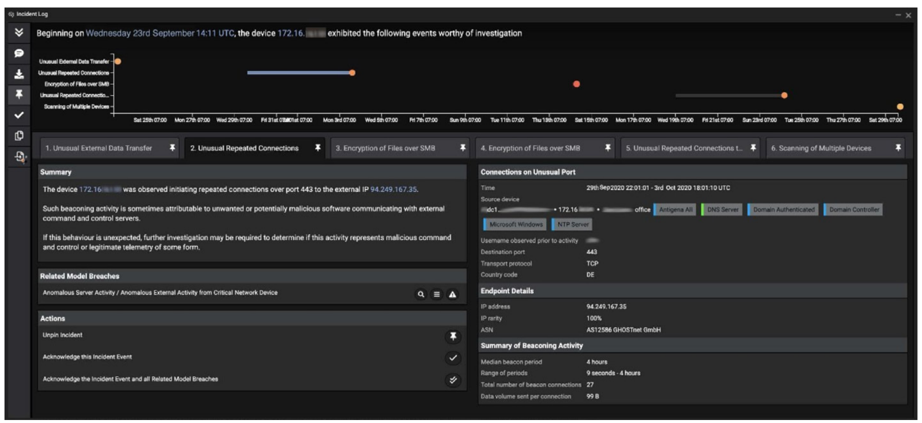

Figure 4: Cyber AI Analyst investigates

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 Antigena would have stopped it in its early stages.

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.

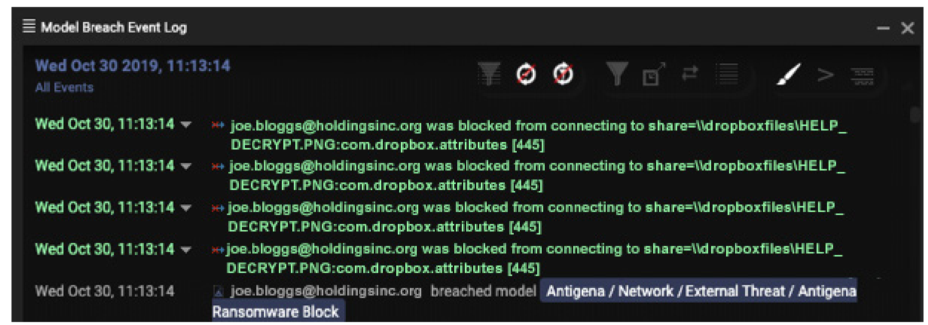

Figure 5: Antigena stops the infected device from conducting lateral movement & ransom activity

> "Autonomous Response combats the most sophisticated ransomware attacks and it does that within seconds of the threat emerging."

Abhay Raman, CSO, Sun Life

With Autonomous Response

Minimizing the REvil impact delivered via Kaseya servers

As the US prepared for a holiday weekend ahead of July 4th, 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.

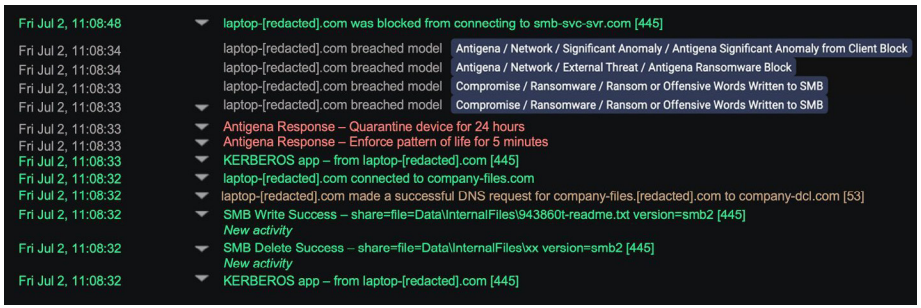

Figure 6: Darktrace detects attempted encryption from the infected device and takes action

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 speed of the attack – thanks to Autonomous Response.

Darktrace Antigena responds to ransomware within 1 second.

Antigena 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.

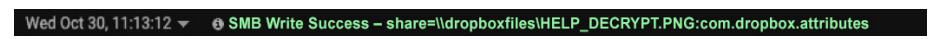

Figure 7: Darktrace detects SMB activity relating to Dropbox files

Fortunately, Antigena 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.

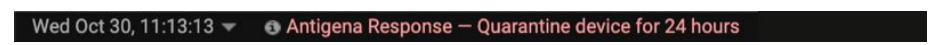

Figure 8: Darktrace Antigena responds 1 second after ransomware was detected

Antigena 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. Antigena 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.

Conclusion

As ransomware becomes quicker and attackers continue to experiment with new techniques, Autonomous Response has become a vital component of the security stack. Its bespoke knowledge of your digital enterprise allows it to respond to emerging attacks with surgical precision, containing the threat without disrupting your business.

The above examples illustrate that even with state-of-the-art detection mechanisms, without a machine-speed and proportionate response mechanism in play, ransomware can still cause significant and costly cyber disruption.

Autonomous Response protects your critical data, wherever it resides – whether in cloud infrastructure and applications, email, the corporate network or on endpoint devices.

About Darktrace

Darktrace (DARK:L), a global leader in cyber security AI, delivers world-class technology that protects over 6,500 customers worldwide from advanced threats, including ransomware and cloud and SaaS attacks. Darktrace'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 1,700 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
info@darktrace.com
Follow us on Twitter