Detecting & Fighting Ransomware in Real Time

In 2016 cyber-criminals launched 638 million ransomware attacks. That's a 167-fold increase from the 4 million attack attempts in 2015, with most of the attacks delivered as phishing campaigns capable of by-passing existing defense mechanisms. In the recent global ransomware campaign, Darktrace detected and automatically responded to the WannaCry ransomware due to the highly anomalous way in which the devices were behaving as they attempted to access and encrypt files, and laterally scan for other exposed devices.

Traditional security tools that use rules and signatures to stop cyber-threats at the border fell short in the face of this never-seen-before and fast-spreading malware. Darktrace uses machine learning and AI algorithms to automatically learn about our customers' infrastructures, and then detect and respond to developing threats as they happen.

Modeled after the most powerful biological system, the human immune system, Darktrace finds anomalies that bypass other security tools, capable of detecting threats without reliance on rules, signatures or any prior knowledge. As a part of the Enterprise Immune System, Darktrace Antigena acts like a digital antibody, taking only very targeted action – for example, it can slow down or stop a compromised connection or device, but does not impact normal business operations.

Darktrace Identifies Ransomware Before it Spreads

Darktrace's Enterprise Immune System has been proven to detect and defend against emerging ransomware attacks across every industry. The Enterprise Immune System, using machine learning and AI algorithms, is able to identify a wide range of anomalies pertaining to ransomware, to form a compelling picture of the overall threat level.

Antigena Stops Ransomware in its Tracks

On detecting the ransomware, Darktrace responds in real time by forcibly dropping suspect connections within the internal network and stopping its spread. This entirely autonomous response, generated by Darktrace Antigena, gave security teams the vital time to catch up before the data was lost or encrypted.

For example, Darktrace successfully identified WannaCry malware activity due to the highly anomalous way in which the devices were behaving as they attempted to access and encrypt files, and laterally scan for other exposed devices. Darktrace Antigena took immediate action by sending out a TCP Kill command to block connections to port 445, thus preventing the malware from spreading laterally across the network and infect other devices.

Detection and Autonomous Response

Let's take a look at how Darktrace's machine learning detected and responded to a ransomware attack at a large financial services organization. As with most ransomware, it all started with a phishing email..

1. Darktrace first noticed anomalous behavior when an employee checked his personal webmail on a corporate laptop. The device started making HTTP requests to a rare external domain:

```
Thu Nov 17, 20:20:22 192.168.103.106 connected to webmail.northrock.bm [80]
```

2. The employee opened what he believed to be a Word document, but was actually a malicious .zip file containing a ransomware payload. The device then connected to a second rare external domain. It was not until the next day that OSINT vendors identified the domain as malicious:

```
Thu Nov 17, 20:20:55 192.168.103.106 connected to www.inhabitantap[.]top [80]
```

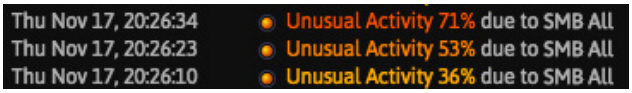
3. Darktrace then observed the device downloading a suspicious .exe file from the anomalous domain:

```
File Transfer (EXE) — FileTransfer::Exe file found with filetype (application/x-dosexec) [80] SHA1:
7099508c86c3b40268a4039afa5aabafb6f36d90
```

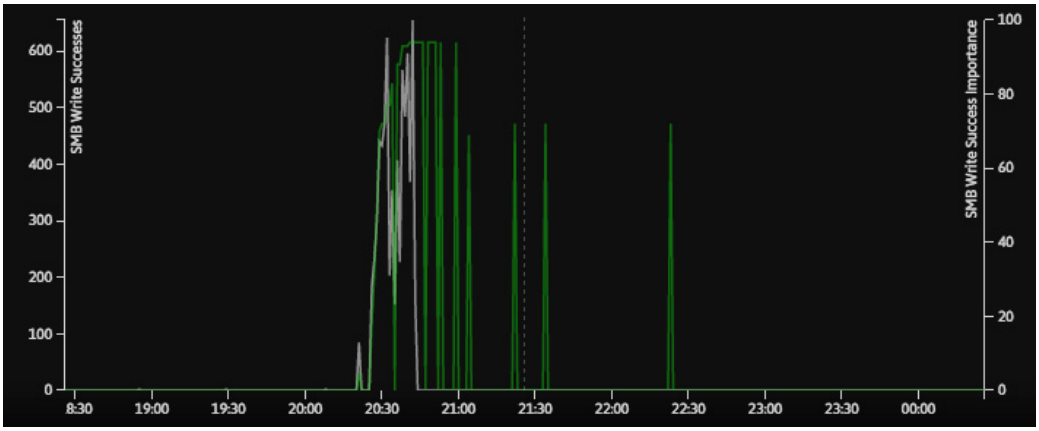
4. At this point, the ransomware executable had already bypassed multiple perimeter security protocols on the device. The ransomware then began to search for available SMB shares. Unlike the encryption of data on individual devices, SMB encryption jeopardizes data across the entire corporate network. Darktrace highlighted this activity as a major deviation from normal:

```
20:26:01
1 SMB Move Success — share= rename_to=[REDACTED].thor file=[REDACTED].xls [445]
An unusual time for this activity
20:26:01
1 SMB Read Success — share= file=[REDACTED].xls [445]
An unusual time for this activity
```

5. Nine seconds after the start of the SMB encryption activities, Darktrace raised an alert signifying that the anomaly required further investigation. As the behavior persisted over the next 24 seconds, Darktrace continually revised its understanding of the deviation as it progressed into a serious threat.



6. At this point, Darktrace's Enterprise Immune System determined that the threat required an immediate response, but the security team had gone home for the weekend and wasn't on site to manually remediate the situation. Antigena stepped in and automatically interrupted all attempts to write encrypted files to network file shares. In so doing, Darktrace neutralized the threat 33 seconds after the malicious activity began.



SMB write successes are observed as the device encrypts files on the network share (shown in gray). The green spikes represent the 'significance' of the activity as understood by Darktrace. This pattern of SMB activity represented a major deviation from the device's normal behavior.