DARKTRACE

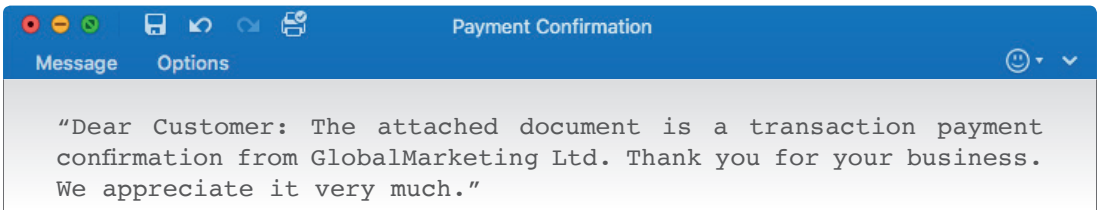
CASE STUDY

Ransomware Case Study – Catholic Charities of Santa Clara

Catholic Charities of Santa Clara County

"Dear Customer…"

On the morning of March 1st 2016, the receptionist at Catholic Charities of Santa Clara County's (CCSCC) headquarters in Santa Clara received an innocent-looking email, which read:



The receptionist was familiar with receiving and processing invoices, so opened the attachment to view the file. Seconds after, a series of threatening events unfolded.

Without realizing it, the compressed file that she had opened connected her computer with a server in Ukraine. It then downloaded powerful, malicious ransomware code, which began to rapidly encrypt files on her device.

Anomaly Detected

A few weeks before the attack, CCSCC's Director of IT, Will Bailey, had been looking to bolster the charity's cyber defense capability with new, innovative technology, in order to be able to face today's sophisticated cyber-attacks.

He had recently started a trial of Darktrace's Enterprise Immune System – a self-learning technology inspired by the human immune system and powered by machine learning and mathematics developed by specialists from the University of Cambridge. Darktrace works by learning a network's 'pattern of life' by modeling the behaviors of each user, device and the network as a whole. Based on this dynamic and adaptive understanding of 'self', Darktrace is capable of real-time threat detection, automatically detecting any behavior or activity that deviates from the norm.

At the time of the attack, Darktrace's technology had been monitoring CCSCC's network for a few weeks and already had a well-established understanding of the company's normal behavior and everyday activity.

> "Darktrace's Enterprise Immune System can detect threats that no other security tool would ever find. The machine learning technology is totally unique."
>
> Will Bailey, Director of IT, CCSCC

Ransomware

Ransomware attacks are becoming increasingly common. The viruses encrypt files and extort companies by charging exorbitant amounts for decryption, since only the criminal hacker responsible holds the key to unlocking them.

These cyber-criminals often demand payments of up to $10,000 in bitcoin, a virtual currency which is hard to trace. In 2016, from January to the end of March, the FBI received reports of more than $209 million in losses due to ransomware attacks.

In some cases, the motive is not financial but purely to destroy data and disrupt business. Even if a ransom is paid, there is no guarantee that the criminals will decrypt the locked files.

Therefore, as the connection was made between the receptionist's computer and the server in Ukraine, Darktrace immediately flagged the activity as 'anomalous', given its specific understanding of CCSCC's environment and the receptionist's individual 'pattern of life'. An alert was generated in real time.

> "The technology delivers a core cyber defense that is specific to our network."
>
> Will Bailey, Director of IT, CCSCC

Defending in Real Time

Fortunately, once detected, a member of the charity's IT security team was able to respond straight away, disconnect the targeted device from the network and prevent any further encryption or financial cost. Will Bailey praised Darktrace for the critical role it played handling this incident: *"if Darktrace's technology hadn't detected the ransomware attack, who knows what could have happened?"*

"The machine learning technology is totally unique. It delivers a core cyber defense that is specific to our network. As we use the Enterprise Immune System and drill down into the anomalies it presents to us, we can tighten parameters, modify the criteria for anomalous activity, verify behaviors which actually are legitimate and, in general, implement best practices," added Will Bailey.

The charity went on to permanently deploy the Enterprise Immune System as its core threat detection tool and now relies on Darktrace's self-learning to continually monitor its network for all potential threats, whether ransomware, hackers, insider attacks or any other type of unpredictable threat.

Contact Us

US: +1 (917) 363 0822
Europe: +44 (0) 1223 350 653

Email: info@darktrace.com

www.darktrace.com