DARKTRACE

WHITE PAPER

Darktrace Discoveries 2018

Real-World Threats Identified by Cyber AI

Introduction

Cyber-attacks in 2018 are increasingly moving at machine-speeds, encrypting or compromising machines within seconds. Strained security teams simply cannot keep pace, and struggle to respond fast enough. As attackers learn to move at unprecedented speeds, we have also seen AI become a fundamental ally against them with the emergence of autonomous response technology which stops threats in real time and more effectively than any human can.

The speed at which AI can intelligently respond to an emerging threat has proven to be a game changer. Crucially, AI buys back time for security teams during an attack, the debilitating impact of which increases with every passing second. As we move into an era of machines fighting machines, autonomous response will be vital in averting a headline-grabbing crisis.

The quiet threat lurking within also remains a unique challenge. Insiders, especially those with privileged access, can cause crippling damage to an organization. From a systems administrator eager to use corporate infrastructure for crypto-mining, to the non-malicious worker who unknowingly downloads malware from a phishing email, insider threat is notoriously difficult to detect.

Today's attacker also has the advantage of the entire digital infrastructure at their disposal. Networks no longer have clearly defined borders. New computing models provided by the cloud, the explosion of IoT, and the convergence of IT and OT networks are blurring the lines and introducing new security blind spots, making it impossible to secure every entry point. Security teams are turning to AI for the answer, capable of detecting and responding to threats wherever they emerge.

Powered by artificial intelligence, Darktrace finds and autonomously responds to never-before-seen threats that have bypassed the perimeter to find their way into an organization's systems. Inspired by the immune system, the technology learns a 'pattern of life' for every user and device. From this ever-evolving understanding of normal, the Enterprise Immune System identifies deviations indicative of a threat. Darktrace Antigena can then take targeted autonomous action within seconds to neutralize an emerging threat before it is too late.

As we move into a new age of cyber warfare, it's a call to arms for both attackers and defenders. By embracing world-leading cyber AI, organizations are for the first time regaining the advantage over today's ever-changing adversary – and winning.

1. Internet-Connected Locker Attempts Data Exfiltration

Industry: Media & Entertainment

Point of Entry: Internet-connected locker at amusement park

Apparent Objective: Exfiltrate sensitive, personal information

At an amusement park in North America, an advanced attacker targeted an IoT device – a physical locker designed to store personal belongings – to gain access to sensitive customer data. As part of its default setting, the 'smart' locker regularly established contact with the supplier's third-party online platform. The threat-actor identified the source of this automated process, and hijacked it to compromise the locker.

Once infiltrated, the locker started to move over a gigabyte of unencrypted data across the network to a rare external site. The connections, which could have included identifying details or sensitive credentials, had the potential to be transmitted over the internet entirely unprotected – giving the attackers ability to intercept the connections and use the information to breach the company's network defenses.

Making the attack particularly sophisticated and difficult to detect, the locker was sending data out in a slow but consistent manner. Without Darktrace's AI-powered threat detection, the malicious activity could have remained hidden for months or even years.

Darktrace Antigena Fights Back

Due to the severity of the threat, Darktrace determined that an autonomous response was required. Within seconds, Darktrace Antigena took action by intelligently blocking all outgoing connections from the compromised locker. In doing so, it gave ample time for the security team to remove the smart locker from the internet without impacting normal business processes.

Darktrace's AI is uniquely able to identify the subtlest indicators of 'low and slow' attacks and intuitively blocks the attack within seconds, regardless of where it originates on the network. In this case, autonomous response was critical in mitigating the risk for the amusement park, before any sensitive company or consumer data could be exfiltrated.

2. Cloud Environment Compromised

Industry: Financial Services

Point of Entry: Third-party cloud

Apparent Objective: Gain access through an exposed cloud environment to exfiltrate data

Organizations are increasingly migrating to new computing architectures to optimize efficiency and reduce costs, but the move to cloud and SaaS environments fundamentally shifts the security paradigm. Strained security teams grapple with defending their data in these new environments where they have limited control and visibility, and where their on-premise security tools are often not applicable.

A leading financial services company deployed a third-party cloud environment to host a number of critical servers on virtual appliances. While configuring the cloud deployment, it mistakenly left an important server open to the internet when it was meant to be isolated behind the firewall. Soon after, the exposed server fell under attack by malicious actors trying to gain access to that device and use it as a route into the cloud and back into the center of the physical network.

Darktrace identified the critical vulnerability before the security team had even realized the misconfiguration. Due to the AI's ability to respond in real time, the organization was able to secure the cloud perimeter before it escalated into a more serious Denial-of-Service attack or before an attacker could successfully gain access to the core infrastructure to exfiltrate data.

Darktrace AI is effective across all major cloud and SaaS applications to identify never-before-seen threats, while providing unprecedented visibility across previously obscure parts of the digital infrastructure

3. Intellectual Property Targeted by Advanced Malware

Industry: Medical Manufacturing

Point of Entry: Malicious Word document in disguised email

Apparent Objective: Encrypt crucial system files and spread to subsequent victims

At a European medical manufacturing firm, an administrative assistant received an email regarding payments with an invoice attached. Believing the attachment to be authentic, she clicked on it and unwittingly downloaded a fast-acting malware that had bypassed all other security controls.

The sophisticated malware was specifically targeting the organization's intellectual property, which included highly confidential medical formulas. If these assets were compromised, the firm would be exposed to significant risk to their competitiveness and reputation.

Once the malware was downloaded on to the administrative assistant's computer, the device rapidly began connecting to a rare external destination while trying to move laterally to other areas of the corporate network. Within two seconds, Darktrace AI identified the emerging foreign presence.

Darktrace Antigena Fights Back

Darktrace Antigena instantly neutralized the infected device by restricting its activity to fall within its normal 'pattern of life'. This action prevented the spread of the malware, buying back time for the organization to take the infected device off the network. Critically, the autonomous response was surgical and proportionate, helping avert a crisis but without disrupting business operations.

When catching a threat, time is working against the security team. As demonstrated in this incident, Darktrace AI technology is capable of responding to an emerging threat in seconds -- preventing it from escalating with potentially-devastating consequences.

4. Compromised Equipment on Assembly Line

Industry: Food Manufacturing

Point of Entry: Connected manufacturing devices

Apparent Objective: Take control of industrial IoT to infiltrate organization

The rapid rise of the industrial Internet of Things is dramatically increasing both the complexity of OT networks and the challenge of securing them. While increasing efficiencies for organizations, the convergence of IT and OT systems expand the attack surface significantly.

An unknown attacker targeted several industrial IoT devices on the assembly line at a leading food manufacturer in an attempt to gain a foothold into the corporate IT infrastructure. The devices included baggers, slicers, and blenders which were making connections to external destinations and attempting to move within the network.

These devices did not have approval from the security team to be connected to the core IT infrastructure. By correlating these factors in real time, Darktrace AI detected the anomalous behavior and determined the activity to be a significant risk to the integrity of both the corporate network and the organization's assembly line.

With Darktrace's artificial intelligence, the entire infrastructure was visualized and protected, including industrial IoT and ICS. The security team was able to take the compromised devices off the network, preventing the food provider's manufacturing infrastructure from any harm and before the attacker could gain access to the core IT infrastructure.

Further, because the outbound connections slipped through their perimeter defenses, the security team was also alerted to several additional problems with their firewall that they were then able to remediate.

As industrial networks go online and become more interconnected, Darktrace AI is uniquely able to identify cyber-threats and latent vulnerabilities across OT and IT environments, preventing damage to any critical infrastructure.

5. Insider Runs Widespread Bitcoin Operation

Industry: E-Commerce

Point of Entry: Insider threat

Apparent Objective: Use company hardware to profit from rising crypto-currency values

It can be easy to overlook the risk that employees pose – individuals with access to sensitive data and systems, but whose digital activities are often difficult to oversee. Privileged access users in particular have the potential to inflict an enormous amount of damage – but are notoriously difficult to spot.

At a Fortune 500 e-commerce company, a disgruntled systems administrator decided to hijack power sources from the company's infrastructure for his own monetary gain. Over several months, the employee co-opted the user credentials of eleven other users and service accounts to stealthily take over multiple machines for the purpose of crypto-mining.

On installation, Darktrace identified over 140 devices that had been using their computing processing power to mine cryptocurrency for the 30 days prior. One of the expropriated devices had connected to the rare external crypto-mining destination over 170 times in just one week.

Darktrace's ability to learn a 'pattern of life' for every user and device enabled the organization to not only identify and stop the activity, but also trace the malicious activity back to a single insider: the systems administrator.

As the value of cryptocurrencies soar to new heights, the incentive for insiders and external attackers alike to exploit company infrastructure for their own profit has significantly risen. Insider threat is supercharged by new monetization mechanisms and the premium attackers are willing to pay to access internal systems.

6. Compromised Parking Payment Kiosk

Industry: Transportation

Point of Entry: Internet-connected parking payment kiosk

Apparent Objective: Take control of IoT device as a foothold into the network

The explosion of the Internet of Things has created a dynamic business environment, increasing both profit and productivity for organizations. But the introduction of these devices has created a significant challenge for CISOs and their security teams who now need to protect devices they might not even know are connected to the network.

A transportation center in the United States installed several high-tech payment kiosks in the parking lots to help process payments and alert to maintenance issues in real time. To ensure the security of the corporate network, the organization configured the devices to ensure that they never connected to the corporate IT network.

However, one of the payment kiosks began making connections to suspicious websites containing adult content. For a duration of 5 hours, the kiosk continued to visit and connect to the rare external location. Beyond the anomalous activity exhibited, the payment kiosk's presence on the corporate network was a critical, latent vulnerability.

Fortunately, Darktrace AI was able to identify and remediate the vulnerability before it could be exploited for a far more sinister purpose. Darktrace's AI meets the challenge of securing IoT devices by establishing visibility of all devices across the entire business, including rogue devices and unconventional IT.

While the motives of the attacker behind the compromise might never be known, the incident exemplifies again the vulnerabilities of IoT devices and the need for visibility and protection of an increasingly diverse digital infrastructure.

7. Darktrace Prevents Encryption of 5,000 Documents

Industry: Financial Services

Point of Entry: Malicious attachment sent via phishing email

Apparent Objective: Encrypt crucial files and extort payment for decryption key

Despite many high-profile cases and a large amount of public information, ransomware remains one of the most serious cyber-threats. As new strains emerge every day, CISOs cannot afford to become complacent. Compounding the challenge, new GDPR regulations have made the need for total visibility and control over sensitive information even more pressing.

On the network of a leading technology and media investment company in Asia, an investment associate inadvertently downloaded a ransomware file designed to look like an authentic email. The infected device connected to the GandCrab ransomware infrastructure and instantly started to encrypt almost 5,000 internal documents, adding a file extension containing a ransom note demanding payment in order to unlock them.

Darktrace Antigena Fights Back

The moment the device downloaded the executable, Darktrace identified the ongoing threat as a widespread and sophisticated ransomware attack. Darktrace Antigena blocked all outgoing communications from the infected device, stopping the infection in its tracks and preventing subsequent data loss.

Had Darktrace's AI not reacted within seconds, a crippling amount of highly sensitive financial information could have been encrypted. Due to the swift autonomous response against the machine-speed attack, the organization was spared tremendous financial losses and reputational damage.

8. 68 Computers Infected with WannaMine Malware

Industry: Technology

Point of Entry: Malicious attachment via a phishing email

Apparent Objective: Infect multiple devices with WannaMine malware to profit from Monero coins

A sophisticated attacker targeted a European IT services company with a piece of malware that was designed to set up crypto-mining pools. On entering the network, the malware spread to infect 68 separate desktop computers and hijacked their processing power to mine for Monero coins.

Each device was using the same set of login details and the same user agent for the Monero mining pool, confirming that the mining activity was the result of malware proliferating across the network. All 68 devices were observed beaconing to the same command and control destination on a daily basis. In fact, the initial source device had attempted to connect to the rare external location over 668,000 times before laterally spreading the worm to other computers on the network.

Darktrace Antigena Fights Back

Within moments of deploying, Darktrace instantly recognized this behavior as a significant deviation from its uninfected peers on the network. Because the malware was rapidly spreading through the network, Darktrace Antigena autonomously restricted all infected devices to a group 'pattern of life'.

The malicious behavior was blocked, while normal behavior was allowed to continue. Because Darktrace Antigena fought back within seconds, the security team was able to gain back the time advantage and respond to the infection before any company data or hardware was lost or damaged.

9. Novel Malware Infiltrates Leading European Bank

Industry: Financial Services

Point of Entry: Desktop server

Apparent Objective: Exfiltrate sensitive company information

More and more sophisticated forms of malware are constantly being developed, leaving blacklists and signature-based solutions behind the curve. Novel attacks, the 'unknown unknowns', are challenging to identify – now more than ever.

A pernicious and previously unknown malware took hold within the infrastructure of a multinational bank when a device was infected via a malicious email attachment. The malware, called 'Squirtdanger' had only been identified in open source intelligence just days prior, and a rule or signature to detect the threat had yet to be created.

Squirtdanger has a wealth of functionality – including the ability to take screenshots, modify system processes, download files and directory information, and steal browser passwords.

Once infected, the device began communicating with Squirtdanger's online infrastructure. It subsequently downloaded payloads, installing a program that persists via an automated process set to run at regular intervals, maintaining contact with malicious servers. Simultaneously, multiple anomalous internal events were observed around the time of the infection, including large volumes of login failures and new usage of administrative credentials.

Crucially, the malware was observed attempting to spread to other machines on the network by forcing access to other devices and reaching restricted resources by guessing passwords and hijacking high-privilege user accounts.

Because Darktrace's AI technology does not rely on prior assumptions of 'known bad', it is able to identify never-before-seen threats as they emerge. The speed at which Darktrace detected this malware prevented the infection from spreading across the organization – defending the integrity of the bank's highly sensitive customer information.

About Darktrace

Darktrace is the world's leading AI company for cyber defense. With thousands of customers worldwide, the Enterprise Immune System is relied on to detect and fight back against cyber-attacks in real time. The self-learning AI protects the cloud, SaaS, corporate networks, IoT and industrial systems against cyber-threats and vulnerabilities, from insider threats and ransomware, to stealthy and silent attacks. Darktrace has over 800 employees and 40 offices worldwide. It is headquartered in San Francisco, and Cambridge, UK.

Contact Us

North America: +1 415 229 9100

Latin America: +55 11 97242 2011

Europe: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010

info@darktrace.com

darktrace.com