DARKTRACE

Global Threat Report 2017

Selected Case Studies

Introduction

Cyber security has risen to the consciousness of not only nation states, but of business leaders and company boards. High-profile hacks against corporations, many of which are household names, only serve to remind us that no one is invulnerable to cyber-attacks.

Despite investment in traditional security tools, the reality is that 'threats' or attackers can, and do, infiltrate networks and are often undetected by traditional security controls. Across Darktrace's global customer base, which spans all industry sectors, some pertinent trends emerge.

Firstly, we are seeing new areas of vulnerability arise as modern companies embrace the 'Internet of Things'. The proliferation of new connected objects multiplies the inroads to critical networks and data, yet organizations often have remarkably poor visibility of these hidden outposts of their networks.

Secondly, the threat posed by insider-related activity is expanding. These incidents are not necessarily malicious; however, the increasing digitization of everyday work processes means that legitimate network users can expose data and systems to significant vulnerabilities.

Finally, the automation of malware production means that attackers can generate and propagate malicious software at lightning speed, outpacing the efforts of human security teams to identify and block new variants of threats.

Darktrace finds anomalies that bypass other security tools. Across our customer base, Darktrace has detected a wide range of cyber-threats, using a probabilistic approach that takes into account multiple weak indicators to form a compelling picture of overall threat.

This report contains the accounts of nine, real-world case studies, which describe threatening activities and attacks that have taken place within organizations where Darktrace's Enterprise Immune System is installed. In each case study, sophisticated methods, advanced technologies, or unusual strategies have been employed, making the threats undetectable by traditional methods, such as heuristic analysis or rule-based solutions.

Each case study recounts a unique circumstance in which abnormal behaviors have been identified by Darktrace while the threat situation was still 'live' and developing. No rules and signatures, or prior knowledge of the network or threat landscape have been used.

Darktrace's ability to detect these emerging risks – critically, at an early stage of their development or life cycle – can be attributed to the fundamentally different approach it employs, using proprietary machine learning and AI algorithms developed by world-class specialists from the University of Cambridge. It allows for the unbiased, self-learning detection of threats, which takes into account the full range of network activities. By building a comprehensive understanding of 'self', Darktrace is able to detect all types of potential threat, including previously unknown attacks.

Machine learning is changing the paradigm for thousands of organizations who rely on Darktrace's self-learning 'immune system' defense to understand, detect, and respond on their behalves – allowing them to catch up and mitigate threats.

1. Autonomous Response Against Ransomware

Industry: Financial services

Point of Entry: Malicious Word document in disguised email

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

At a global financial services company, an employee circumvented corporate policy to check her personal webmail on a company laptop. The employee opened what she believed to be a Word document, but was actually a malicious ZIP file containing a ransomware payload. The device contacted a rare external domain and began downloading a suspicious EXE file.

Darktrace's Enterprise Immune System recognized this activity as highly anomalous. The platform uses advanced machine learning to learn the unique 'pattern of life' for every user and device. When the executable began to encrypt SMB file shares, this represented a deviation from the device's normal 'pattern of life'. At this stage, Darktrace determined the threat was serious enough to require an immediate response.

Anomalous activity detected:

- HTTP requests to two rare external domains
- Download of an executable file from the anomalous domain
- Rapid encryption of SMB shares, representing a significant deviation from its normal 'pattern of life'

Darktrace Antigena fights back:

The security team was not on site to take action to remediate the situation. Darktrace Antigena took autonomous response and interrupted all attempts to write encrypted files to network shares. In so doing, Antigena neutralized the threat 33 seconds after the malicious activity began.

Ransomware attacks like these are increasingly common, and as new and more insidious strains emerge on the dark web every day, ransomware will inevitably bypass even the most sophisticated perimeter defenses.

Moreover, ransomware is capable of encrypting an entire network in a matter of minutes. Human security teams cannot keep up with such fast-moving attacks, and autonomous response has become vital in today's threat landscape.

2. IoT Devices Co-opted Into Denial-of-service Attack

Industry: Architecture

Point of Entry: Smart drawing pad

Apparent Objective: Denial-of-service attack

Smart devices are often purchased and introduced into corporate networks by employees without the involvement of the IT or security team, opening an easy route into the network for attackers to exploit.

Designers at an architectural firm were using smart drawing pads to enable them to quickly send schematics and drawings to clients and other staff members.

Unbeknown to the firm, the devices were connected to the office Wi-Fi without having changed the default login credentials. As such, the devices were widely accessible via a range of channels. Any external attacker could access them by using the default login credentials that came with the design pad software.

Anomalous activity detected:

- Anomalous spikes in external communications
- Highly unusual volumes of data being sent outside the network
- Communications from a series of globally distributed external hosts that these devices had never communicated with before

Darktrace's AI algorithms learned the unique 'pattern of life' for these devices and the network as a whole. The devices regularly connected to legitimate hosts outside the network, but after several weeks, Darktrace detected a sudden spike in activity.

Indeed, an attacker scanning the internet identified the vunerable smart drawing pads and exploited them to send vast volumes of data to many websites around the world owned by entertainment companies, design companies, and government bodies.

This was identified as a denial-of-service attack. The pads were responding to a specific type of request for information commonly used to disable the target's systems by flooding it with superfluous traffic.

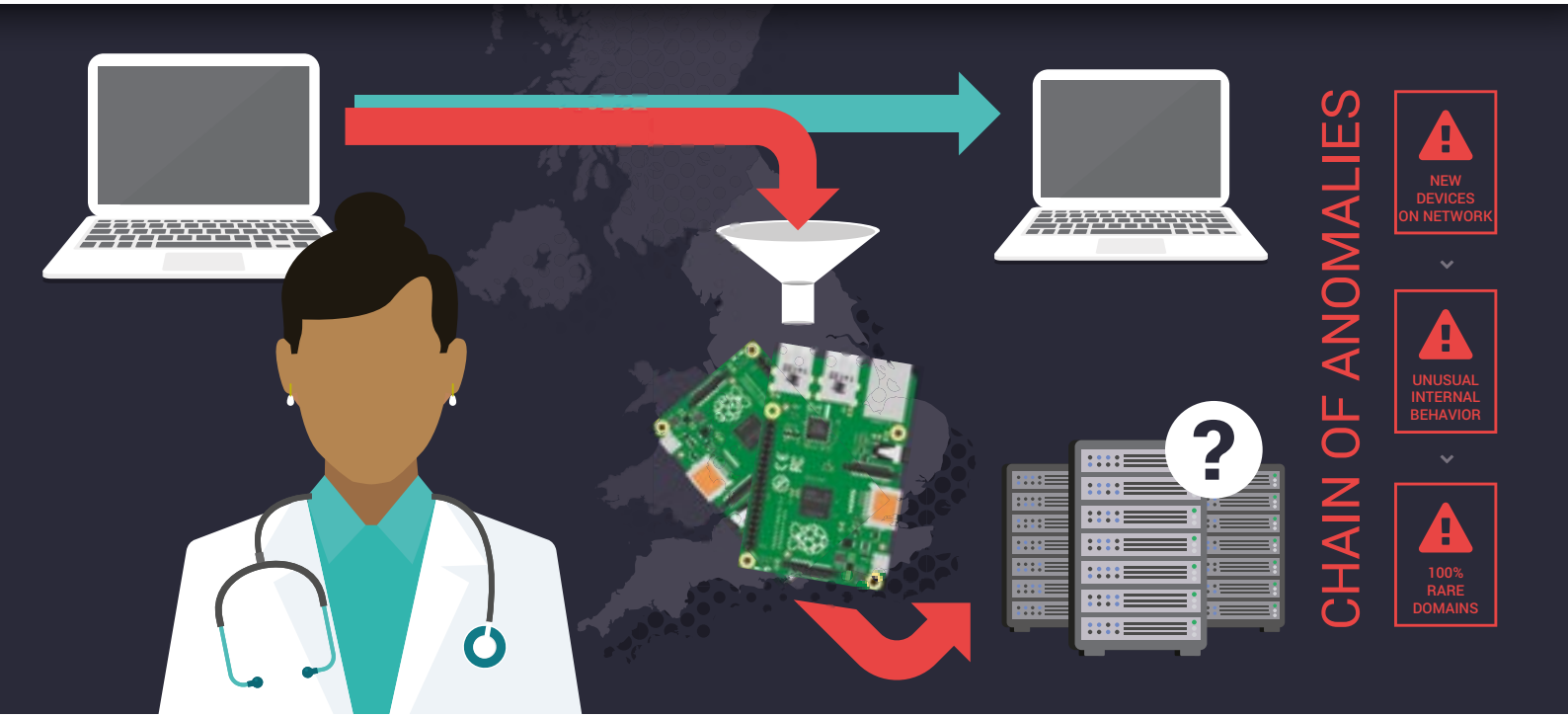
Involvement in the attack could have legal implications for the firm had their infrastructure been responsible for damaging another network. Darktrace detected the anomalous activity from the drawing pads as soon as it began. By providing in-depth details on the nature of the compromise as well as the underlying vulnerability, the firm's security team was able to address the situation and minimize risk of future incidents.

3. Malicious Insider Harvests Data

Industry: Healthcare

Point of Entry: Insider threat

Apparent Objective: Harvest usernames and passwords, and profile network defenses



Insiders have the means and opportunity to inflict disproportionate damage, but the indicators of these threats are often incredibly subtle. At a large healthcare provider, two devices began exhibiting signs of highly anomalous activity. Not only was the activity unusual, but the devices themselves had never been observed on the network before. Their behavior represented a significant deviation from the organization's 'pattern of life'.

Shortly after joining the network, the devices started acting like gateways. They funneled internal traffic to pre-determined destinations. The MAC addresses of these devices identified them as Raspberry Pis, small, inexpensive, high-performance computers the size of a credit card that are easy to smuggle into a network.

Anomalous activity detected:

- New devices with MAC addresses entered the network
- Communications redirected from internal computers to alternative destinations

The Raspberry Pi computers were communicating with a suspicious external website that was made to look like it belonged to the company. However, the websites were actually hosted on alternative servers. The redirected users were being presented with a fake login page and 'security survey' where they were required to enter their usernames and passwords.

This was a brazen attempt to harvest user credentials. In addition, the perpetrator was likely using the devices to profile the network's defenses in order to launch a more targeted attack in the future.

Darktrace identified the threat in real time, meaning no users fell victim to this malicious phishing attack. The Raspberry Pis quickly disappeared from the network.

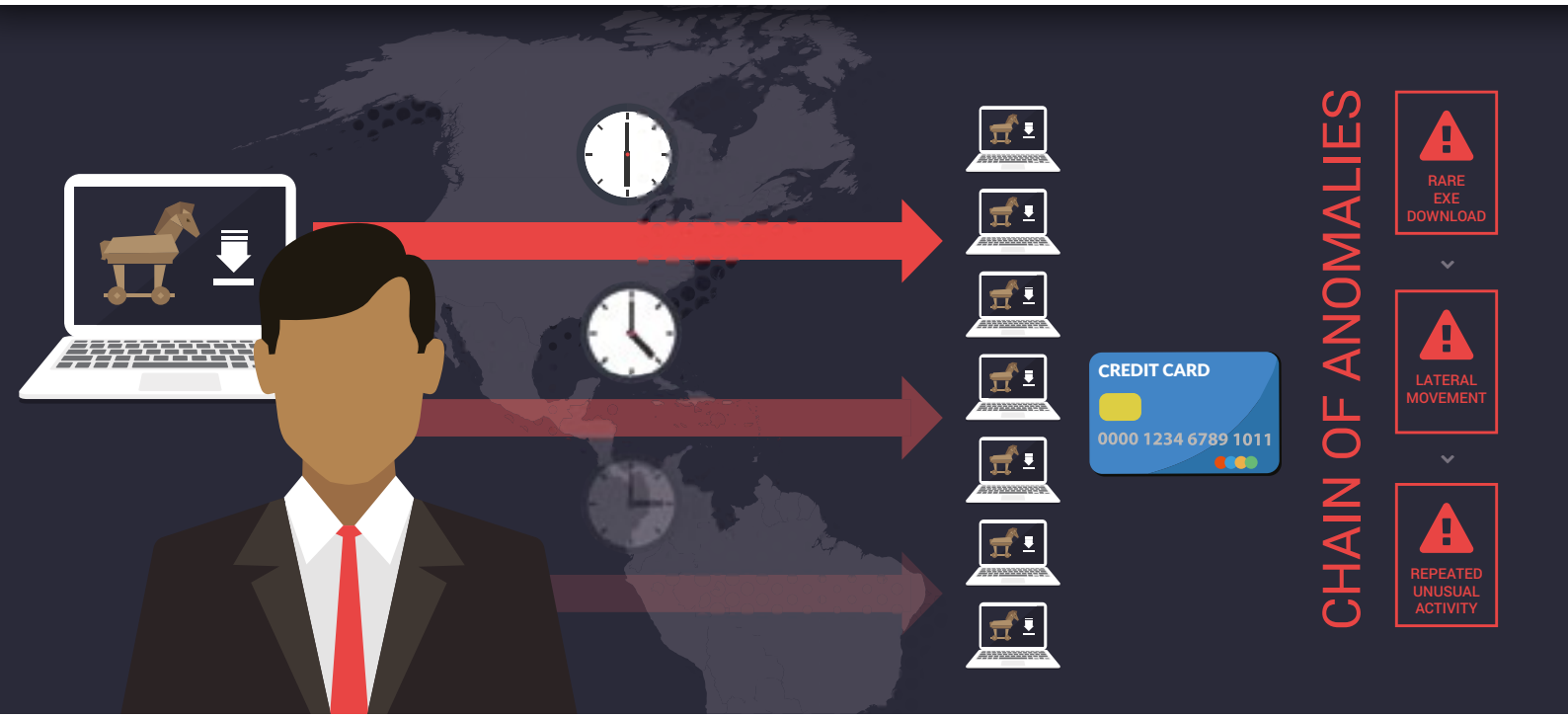
This threat shows how Darktrace's Enterprise Immune System is capable of detecting even the most subtle deviations from normal, whether they represent a sophisticated external attacker or a trusted insider. Human observers and traditional security tools frequently miss these threats, but Darktrace's powerful AI algorithms identify them at the earliest possible stages, before they can do damage.

4. Widespread Infection, Aggressive Banking Trojan

Industry: Government

Point of Entry: Malicious advertisement

Apparent Objective: Extract login credentials and transfer funds into foreign account



Darktrace's AI algorithms detected a series of anomalies on the network of a local government in the United States. A large number of devices were reaching out to unusual servers and websites across the world. The connections occurred at regular intervals, activity that is indicative of the actions of automated software. Further investigation revealed that the sites had algorithmically generated names that were specifically designed to avoid the corporate firewall.

Darktrace was able to trace these communications back to a single company computer that visited a website and clicked on a malicious advertisement and inadvertently downloaded malware.

Anomalous activity detected:

- Download of anomalous executable file
- Multiple unusual connections to other devices, indicating the malware was attempting to spread

The file contained a highly aggressive banking Trojan designed to automatically steal online banking credentials and transfer funds into the attacker's account. The Trojan bypassed the company's perimeter defenses and went unnoticed by their security team. In a matter of hours, the Trojan had infected over 200 computers.

This type of malware tends to have few discernible effects on the infected devices, so victims may not know they have been targeted until transfers have already been made. Moreover, attackers constantly revise the malware's code and migrate their command and control centers around the world.

5. Former Employee Credentials Compromised

Industry: Hospitality

Point of Entry: Malicious insider

Apparent Objective: Steal sensitive company data using old credentials

At a major hotel chain in Asia, Darktrace detected a sudden spike in anomalous activity. External servers were attempting thousands of remote-desktop connections by guessing default usernames and passwords. Darktrace's Enterprise Immune System identified the activity as an anomalous deviation from the network's 'pattern of life' and further investigation revealed that these connection attempts used a specific pattern, indicative of an automated attack. Darktrace identified that some of these remote-desktop connections were using a known set of credentials.

Anomalous activity detected:

- Connection attempts on port 3389 from an external-facing server
- A series of anomalous remote-desktop protocol connections between company devices
- An anomalous volume of SMB read requests

The external server was being accessed from outside the network with an internal user account. The server then made remote-desktop connections between other company computers before arriving at the hotel property management system, from where a large volume of data was downloaded.

A comparable volume of data attempted to leave the network, going to the external device that initiated the original remote-desktop connection. These connections were deemed highly suspicious since they represented an extreme deviation from the devices' normal 'pattern of life'.

Darktrace Antigena fights back:

The company management reported that the user account in question belonged to a former employee who had only recently left the company. It is possible that he had sold his access credentials before they could be disabled, or he could have been attempting to retrieve the data himself before selling to a competitor.

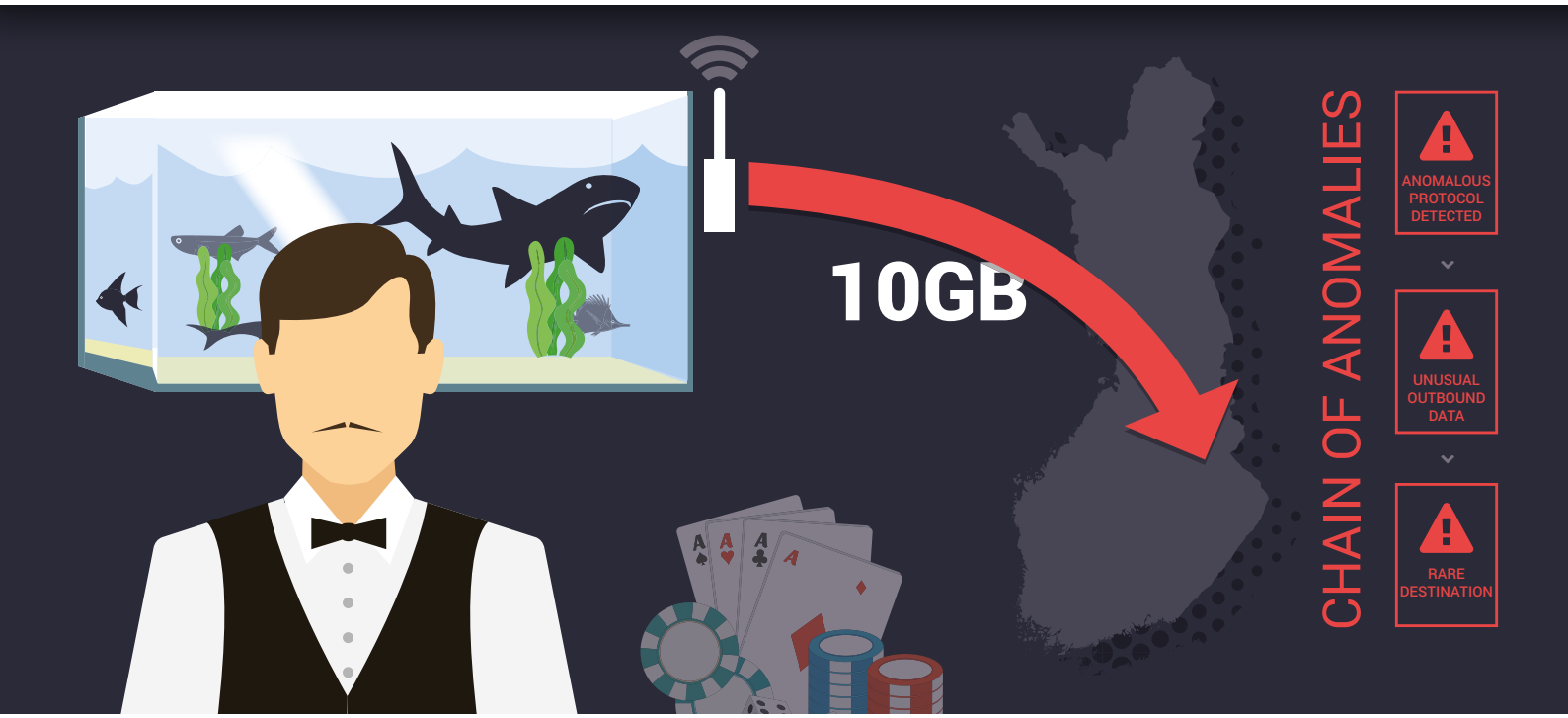
By leveraging unsupervised machine learning, Darktrace Antigena was able to detect and take autonomous action in real time, preventing the attempted data exfiltration before the information left the network, and buying the security team precious time to intervene.

6. Compromised Connected Fish Tank

Industry: Gaming and entertainment

Point of Entry: Connected fish tank

Apparent Objective: Take control of an IoT device to steal valuable information



Technological innovations keep businesses dynamic and profitable, their employees productive and creative, and their premises exciting and modern. A North American casino recently installed a high-tech fish tank as a new attraction, with advanced sensors that automatically regulate temperature, salinity, and feeding schedules.

To ensure these communications remained separate from the commercial network, the casino configured the tank to use an individual VPN to isolate the tank's data. However, as soon as Darktrace was installed, it identified anomalous data transfers from the fish tank to a rare external destination.

Anomalous activity detected:

- Transfer of 10GB outside the network
- No other company device had communicated with this external location
- No other company device was sending a comparable amount of outbound data
- Communications took place on a protocol normally associated with audio and video

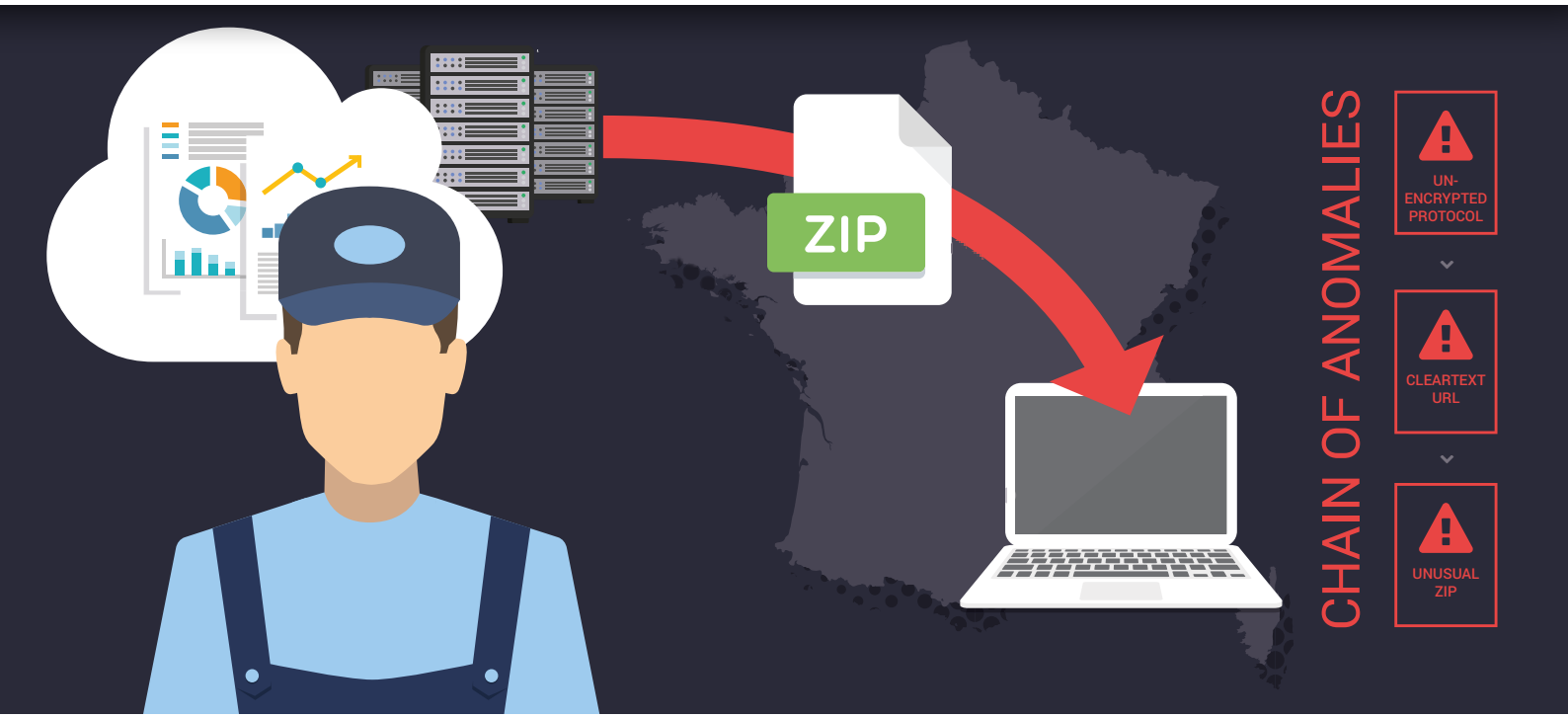
The tank's communication patterns included sporadic communications with company devices, but that activity was in line with similarly configured IoT devices. The external data transfers, however, were deemed highly unusual by Darktrace's AI algorithms.

The data was being transferred to a device in Finland where an attacker had managed to gain control over the tank. This was a clear case of data exfiltration, but far more subtle than typical attempts at data theft.

By targeting an unconventional device that had recently been introduced into the network, the attack managed to evade the casino's traditional security tools. Darktrace's Enterprise Immune System detected the threat because the technology does not make assumptions about where threats will arise. It detected a subtle anomaly that indicated a much larger threat, and it aided the casino in remediating the vulnerability. The incident demonstrates the need to have complete visibility of every user and device – including internet-connected fish tanks.

7. Data Storage Threatens Intellectual Property

Industry: Manufacturing
Point of Entry: Third-party vendor
Apparent Objective: Data exfiltration



At a major European manufacturer, the security team decided to use a cloud server to store their intellectual property. The server was protected with a username and password, but the files on the server were available without further access restrictions and – crucially – without encryption. Any user or malicious actor with the appropriate address could access the files without logging in.

By intercepting network communications, an external attacker could have discovered this address with minimal effort. Likewise, a malicious insider would have faced almost no barriers if they wanted to download the contents and sell them to a competitor.

Darktrace detected this vulnerability when an internal device downloaded a ZIP file from an anomalous server. Ordinarily, this activity indicates unauthorized content entering the network. In this case, the anomaly revealed a critical security vulnerability in the company's cloud server.

Anomalous activity detected:

- Retrieval of an anomalous ZIP file from an external folder
- Server deemed to be 100% rare for the network

This incident demonstrates the value of Darktrace's Enterprise Immune System for anomaly detection. The vulnerability would have been nearly impossible to define with rules or known threat signatures as the inherent risk in this storage system was not obvious. The Enterprise Immune System identified the activity as anomalous and indicative of a larger pattern of abnormality.

Upon further investigation, the ZIP file was found to contain sensitive intellectual property including product specifications, market analysis, and sales projections. The loss or leakage of such information could have placed the entire product line at risk.

By reporting this risk as soon as it was detected, the company prevented the loss of critical intellectual property. Darktrace assisted the security team in revising their data storage practices in order to better protect their product information in the future.

8. Internal Data Theft From the Cloud

Industry: Retail

Point of Entry: Third-party cloud service

Apparent Objective: Download customer database and sell for profit

A retail company based in the United Kingdom decided to restructure its IT department. In so doing, they had to let a number of employees go. One of the affected employees – an IT manager – downloaded contact details and credit card numbers from the customer database. Darktrace detected data transfers to a home server via that company's regular data transfer service. The employee was likely intending to sell the information for a substantial profit.

The database was held on a third-party cloud service in order to enable flexible working and reduce hardware costs. The retailer's business model was based heavily on the usage of cloud synchronization, storage, and file transfer services. However, this IT manager demonstrated how cloud services can be exploited for insider data exfiltration.

Anomalous activity detected:

- Unusual download from the customer database
- Connection to file transfer service that the device had never previously accessed
- Anomalously large external uploads
- Downloaded data from the customer database deemed rare for the device

The company's marketing department frequently used this cloud service, but it was highly unusual for an IT manager to send data externally through the cloud. Darktrace was able to make this distinction because the Enterprise Immune System continually learns normal activity for every user and device in the network, and compares behavior between devices to identify similarities.

Darktrace's technology detected this slight deviation from the normal 'pattern of life', enabling the platform to identify this threatening and subtle behavior even though the cloud service was regularly used for legitimate purposes.

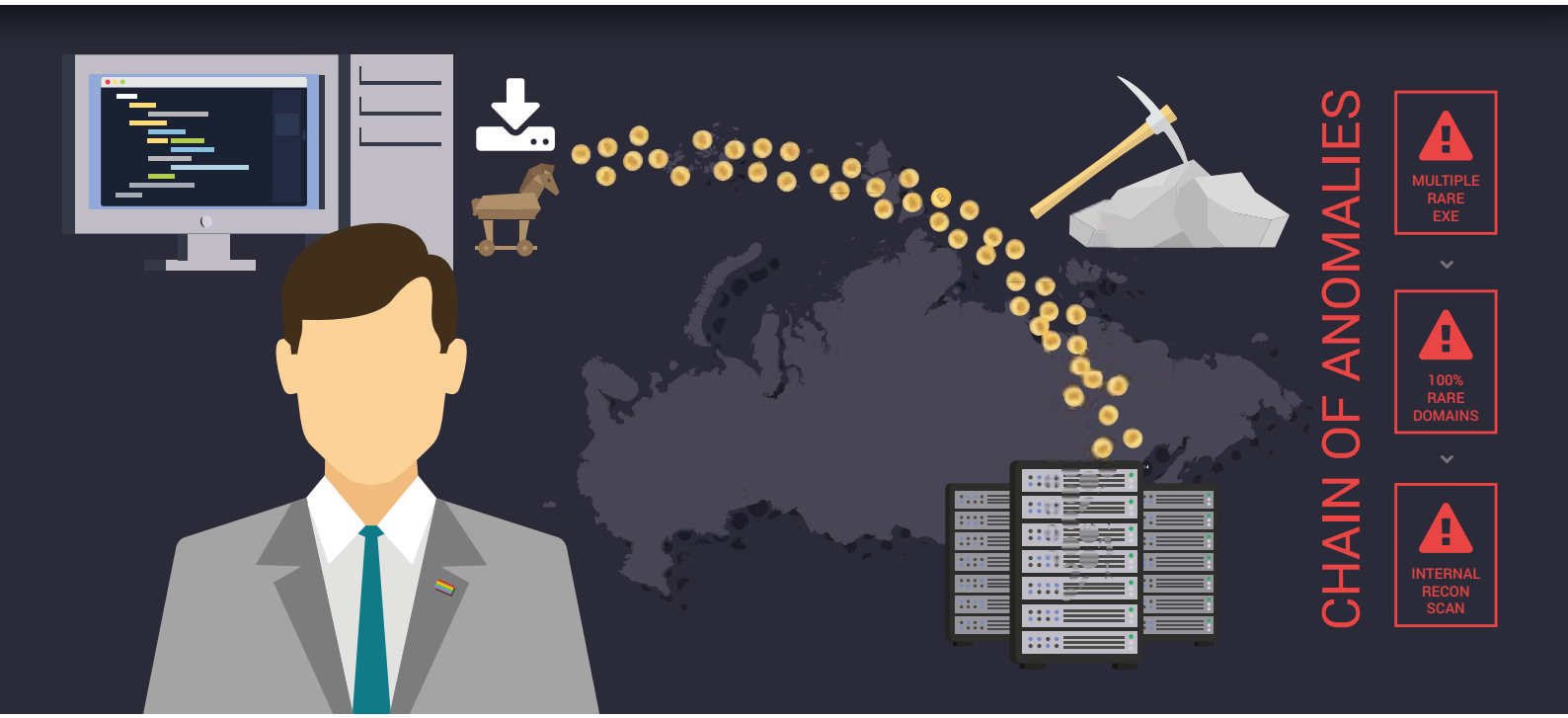
Darktrace detected these anomalies in real time and provided the company with detailed information on the precise nature of the compromise. The employee was reprimanded, their credentials were revoked, and the company quickly retrieved and secured the customer data.

9. Advanced Bitcoin Mining Operation

Industry: Insurance

Point of Entry: Company server

Apparent Objective: Use corporate network to mine bitcoin for profit



Darktrace detected a device at a US insurance company making HTTP connections to a collection of rare servers in Russia. This activity was followed by hundreds of anomalous downloads, the majority of which entered the network through the company's firewall and installed on the device.

Immediately after these downloads, the device began beaconing to suspicious external websites while simultaneously connecting to command and control infrastructure associated with banking Trojans. The device proceeded to scan the network for lateral movement opportunities. Upon inspection, it became clear that the external websites were bitcoin mining pools, and a foreign cyber attacker was attempting to leverage the corporate network to surreptitiously launch an extensive bitcoin mining operation.

Anomalous activity detected:

- Connections to two Russian servers that were 100% rare for the network
- 335 executable downloads containing bitcoin mining malware and polymorphic malware
- Beaconing to anomalous websites

The sheer number and variety of malicious executable files that the device requested ensured that at least some of them would enter the network. The initial payload instructed the device to return to the same external site and request hundreds more files. The infection then attempted to spread through the network and create a botnet of bitcoin mining zombie devices.

Darktrace Antigena fights back:

Darktrace detected each of these anomalies in real time and gained a detailed understanding of this highly advanced and evolving operation. By taking autonomous action to interrupt the communications and alert the security team of the threat, they were able to isolate the infected device before a botnet could be established. Ultimately, the time that the infected device spent mining bitcoin may have enriched the attacker by 0.00000629 bitcoins.

About Darktrace

Darktrace is the world's leading machine learning company for cyber security. Created by mathematicians from the University of Cambridge, the Enterprise Immune System uses AI algorithms to automatically detect and take action against cyber-threats within all types of networks, including physical, cloud and virtualized networks, as well as IoT and industrial control systems. A self-configuring platform, Darktrace requires no prior set-up, identifying advanced threats in real time, including zero-days, insiders and stealthy, silent attackers. Headquartered in San Francisco and Cambridge, UK, Darktrace has 24 offices worldwide.

Contact Us

North America: +1 415 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
info@darktrace.com
darktrace.com
@darktrace