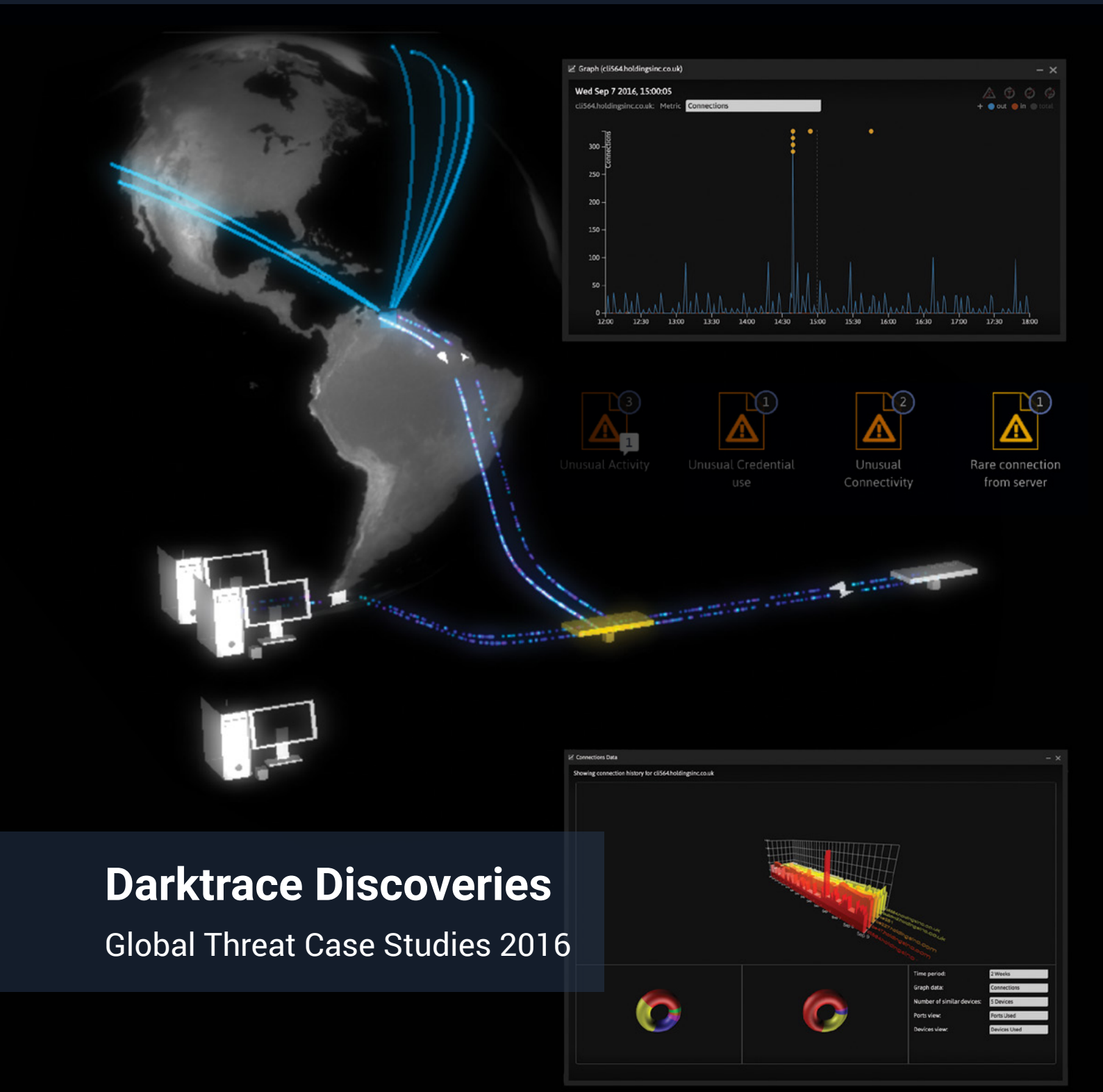
DARKTRACE

THREAT REPORT



Darktrace Discoveries

Global Threat Case Studies 2016

Introduction

Since launching the Enterprise Immune System in 2013, Darktrace has achieved over 1,200 deployments worldwide of the 'immune system' technology and reported 16,000 'serious' early-stage threats. This experience has provided Darktrace with a unique insight into in-progress attacks and novel threat patterns that have been mitigated before the attacker or threat actor has fulfilled their objectives.

While cyber security trends are widely reported in the media, those trends are only built from confirmed breaches. Incident response investigations reveal valuable insights into attacker targets, but often fail to report on longer-term cyber missions and insider-related threats, for the simple reason that these threats are still going unnoticed in too many organizations.

This report contains the accounts of six, real-world case studies, which describe threatening activities and attacks that have taken place in the last 12 months within sites where Darktrace 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 or rule-based solutions.

Human analysis is inherently flawed, as attackers do everything they can to hide amid normal activity, and security analysts can only manually look for obvious deviations. Businesses' reliance on signature-based systems means that they are not catching threats fast enough, if at all – the average time to detect a cyber threat stands at 146 days, according to the Verizon's 2016 Data Breach Investigations Report.

Across Darktrace's global customer base, which spans all industry sectors, some pertinent trends emerge. Firstly, we are seeing new areas of vulnerability emerge 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 atomization of malware production means that attackers can generate and propagate malicious software at lightning speed, fast outpacing the efforts of human security teams to identify and block new variants of threats.

It is all too easy to produce reports on how bad things have got, and how exposed our data and systems have become. Machine learning is changing the paradigm for hundreds of organizations however, who rely on self-learning, 'immune system' defense to understand, detect, and even respond, on their behalves – allowing them to catch up and mitigate threats continually, without being constantly overwhelmed.

This report aims to illuminate the kind of threats that Darktrace is capable of uncovering, using this self-learning, technological approach. 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 even prior knowledge of the network or threat landscape, have been used. Instead, the Enterprise Immune System uses advanced mathematics and machine learning to learn as it goes, quickly understanding what is normal and what is not, and highlighting developing threats in real time – in order for mitigating action to be taken.

1. Compromise of Biometric Control System

Industry: Manufacturing
Point of Entry: Fingerprint scanner
Apparent Objective: Alter biometric access keys

In early February 2016, Darktrace was working with a large manufacturing company with several high priority locations. This company went to great lengths to physically secure their facilities and used fingerprint scanners to restrict access to certain areas. However, an attacker had successfully exploited known software vulnerabilities to gain access to the scanners and the sensitive user information they contained. This breach implied that the attacker was able to transfer fingerprint details to and from the network, and provide unauthorized access to the company's facilities to unwanted and potentially dangerous individuals.

What we found:

- Immediately after being installed, Darktrace detected suspicious Telnet connections to the scanners from an external computer that the company otherwise had no contact with.
- This external server successfully accessed the scanners with default credentials and used root privileges to retrieve CPU information.
- The server then attempted to delete the history file of each device.
- Further investigation revealed that the scanner's availability on Telnet port 23 was recorded on the IP database shodan.io.

Fingerprint scanners are a sophisticated physical access control and their use indicates that the company had gone to considerable lengths to protect their physical assets. The ever-increasing connectivity of modern networks meant that the company could integrate these devices into their IT network. This integration allowed the company to efficiently manage physical access controls – but also introduced a new means of compromising these physical defences through a sophisticated cyber-attack, carried out by a remote third-party. The synergy between physical and network resources meant that remote attackers on their keyboard now had an opportunity to gain physical access to the company's facilities.

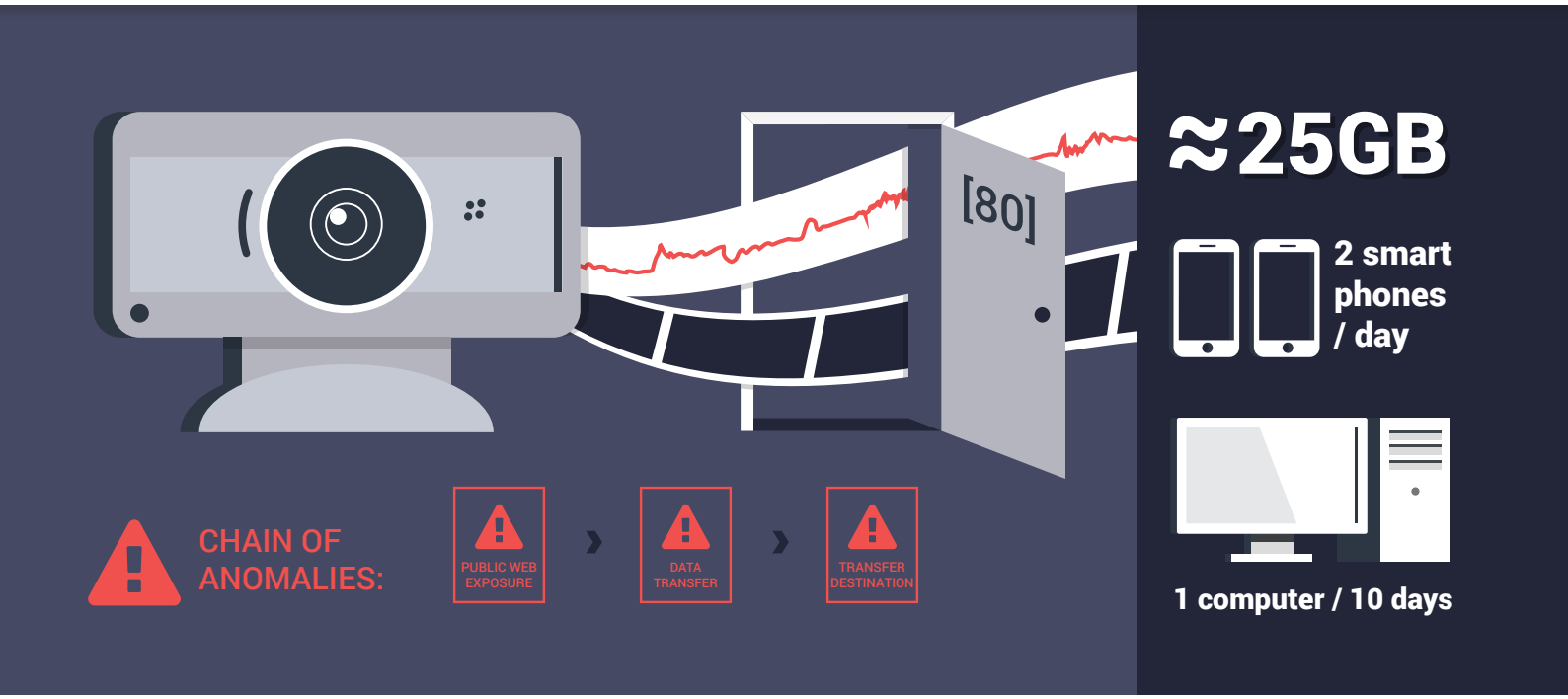
Standard anti-malware solutions would not have been able to detect the subtle and discrete operations that caused the compromise, as they are not linked to any type of attack 'signature' that could be listed in a known database of threats. However, by alerting the security team to anomalous behavioral patterns, Darktrace was able to detect this non-traditional threat and alert the company before the attacker had a chance to cause serious damage.

2. Data Exfiltration from Video Conferencing Device

Industry: Retail

Point of Entry: Video conference camera

Apparent Objective: Transmit mass amounts of data out of host network



Spring 2016 saw considerable international expansion for a foreign sporting company that opened new offices across the world and invested in video conferencing equipment to facilitate day-to-day communication between multinational teams. However, risky configuration of these devices meant that an external attacker was able to take complete control over a conferencing camera and exploit it to exfiltrate significant volumes of data from the network.

Darktrace originally flagged the camera for transmitting much larger quantities of data outside the network compared to similar devices. Unusually, the camera was sending this information via Telnet – a protocol normally restricted for use within the network. Darktrace analysts then discovered that the entire video conferencing system supported unauthenticated remote access, which the attacker had exploited to execute malicious code.

What we found:

- This device was the only internal computer connecting externally via Telnet.
- The anomalously large volumes of information were uploaded to six rare external computers.
- A back-door Trojan had been uploaded to the device before Darktrace was installed.
- External servers that the company otherwise never contacted were connecting to the camera via FTP, Telnet and HTTP.

The anomalous data transfers from the compromised camera were easily detectable through Darktrace's behavioral modeling approach. However, it is the sort of indicator that a signature-based model could easily miss as such activity is not inherently malicious.

The attacker was likely aiming to do one of two things with these large transmissions:

1. To steal corporate information, including highly invasive audio and video feed data.
2. Take remote control of the device to launch a DDoS attack on another network.

Either situation would have been a serious security risk to the company; the same breach would allow the attacker to eliminate the confidentiality and privacy of company activities or to create legal liability for an outsider's criminal activity. Darktrace's prompt network analysis indicated that the situation required immediate action to isolate the affected device and investigate the vulnerabilities that had led to this risk.

3. Malware Connecting to Explicit and Illegal Content

Industry: Security

Point of Entry: Network server

Apparent Objective: Plant incriminating evidence of illegal web activity via malware infection

In the weeks following a Darktrace installation at a security company in the Middle East, the Enterprise Immune System flagged multiple employee desktops accessing unusual websites on servers located all across the world. The websites had random, algorithmically generated names – which suggested that they were not intended or regular traffic and were being masked from signature-based defenses. Investigation by Darktrace revealed that the websites were associated with explicit and illegal content that could pose serious legal risks to the company and its employees.

What we found:

- Seven internal desktops were initiating SSL connections to algorithmically generated hostnames serving self-signed certificates.
- The websites were highly anomalous for the company's network as there had been no previous contact with either the sites or the servers that hosted them since Darktrace was installed.
- The SSL connections were utilizing abnormally strong cipher suites.

Shortly after detecting the activity in the Middle East, Darktrace found similar communications on the website of a major American retailer. The retailer's devices were accessing the same explicit websites, on the same servers – a coincidence that strongly pointed to malware infection rather than deliberate user behavior.

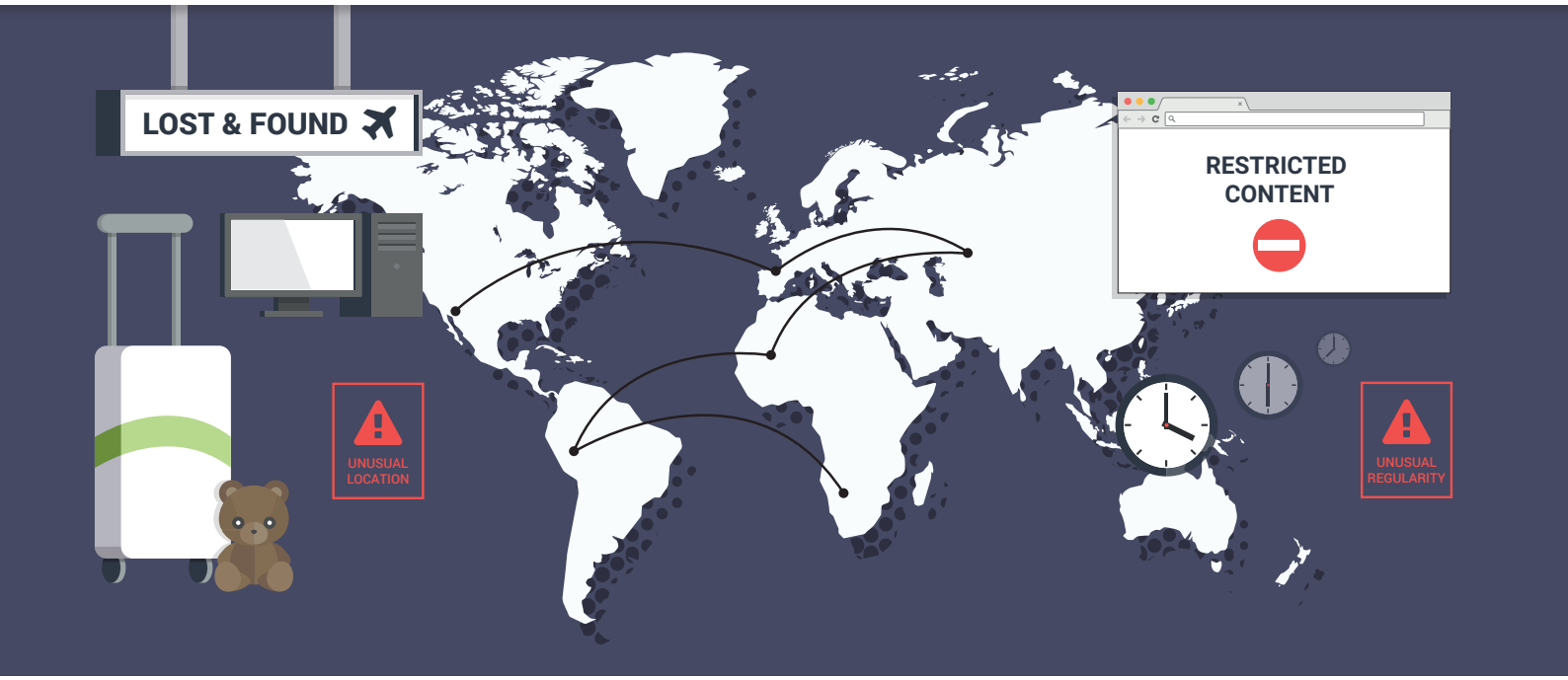
Again, these devices were flagged by Darktrace as their web-browsing behavior was anomalous compared to other computers in the company's American environment. The malware behind this activity was new and sufficiently advanced to avoid detection by both companies' security stacks. If the infection had progressed, multiple internal devices could have been compromised before signature-based defenses were updated to recognize this variant of infection.

4. Boutique Malware Beaconing Through DNS

Industry: Travel

Point of Entry: Lost & Found Department of European Airport

Apparent Objective: Exfiltrate data through boutique malware



In late March 2016, a major European airport was put at risk through a subtle malware infection that avoided detection through signature-based defenses by disguising its communications as DNS requests. Darktrace first detected this activity when a computer in the Lost and Found Department initiated external communications that were highly anomalous compared to previously modeled patterns of activity. The device was regularly contacting American data centers via port 53. This port is assigned to DNS traffic; however, while most DNS requests (including on this network) use UDP, these messages were being transmitted via TCP. As it was the only device communicating outside the network in this way, Darktrace flagged the Lost and Found computer as worthy of further investigation. Analysis soon revealed that the American servers were not DNS servers and were likely being exploited by an attacker as part of its command and control infrastructure.

What we found:

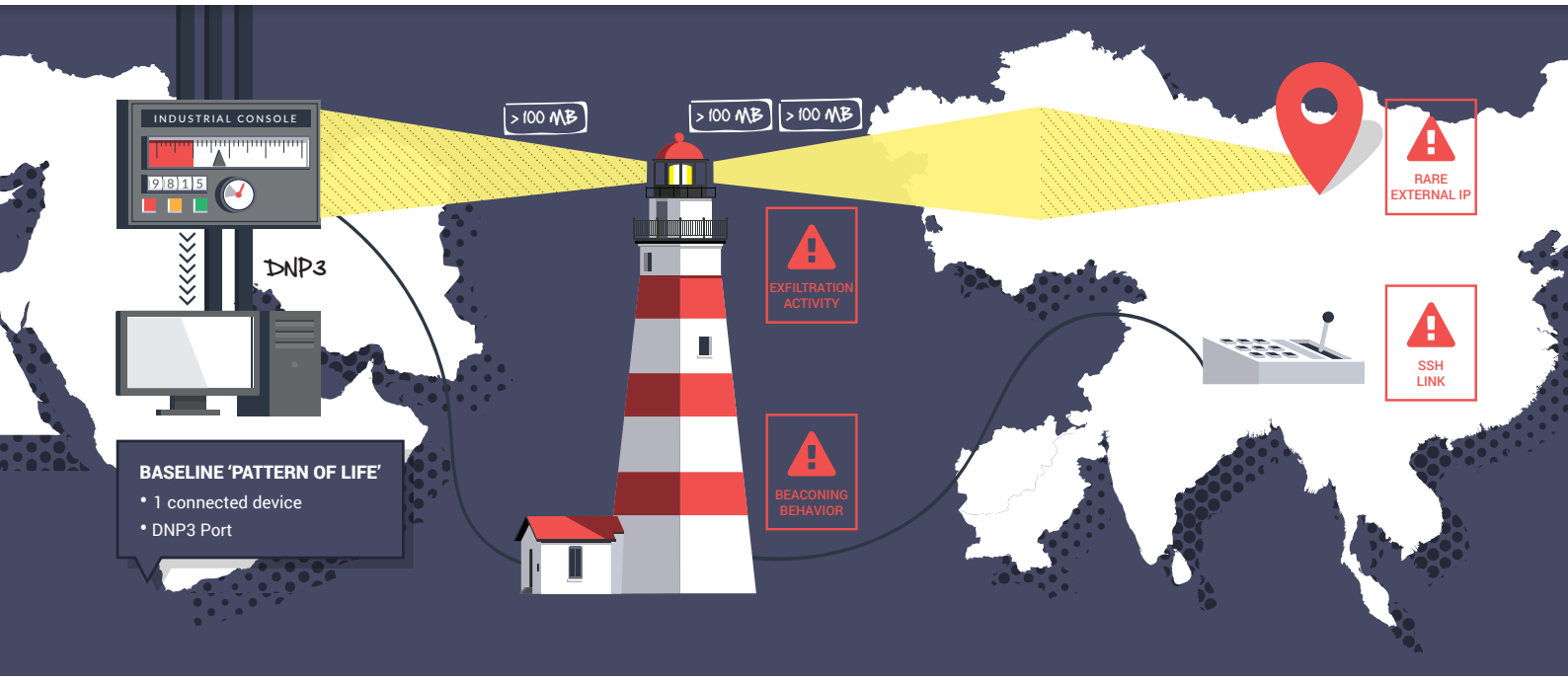
- The external servers were 100% anomalous on the airport's network; meaning that no other internal devices had contacted them since Darktrace was installed.
- The size of each DNS request was anomalously large compared to DNS traffic across the rest of the network.
- Darktrace packet capture revealed that the communications contained encrypted information.

DNS is an essential capability for internet communication and most devices therefore leave port 53 open. As DNS is not a channel normally used to transmit information, many organizations minimize the security resources dedicated to monitoring it – especially in departments that deal more commonly with lost property than critical operational information. However, this means that DNS can be exploited for malicious communications. These are hard to detect with traditional signature-based and perimeter defenses, especially if these are not set-up to specifically monitor DNS traffic.

By noting the anomalous DNS requests at an early stage of the infection life cycle, Darktrace enabled the security team to proceed directly to incident response and immediately stem the exfiltration of data.

5. Data Exfiltration from an Industrial Power Network

Industry: Energy
Point of Entry: SCADA Network
Apparent Objective: Exfiltrate sensitive data and establish remote control link



While working with a SCADA energy network in the Middle East in Fall 2015, Darktrace identified an internal server that was compromised and leaking data to an external attacker. This was first discovered when Darktrace flagged an anomalous SSH connection to the server, which could be traced back to a computer in Asia that had no evident connection with the energy network.

Considering the remote control that SSH facilitates, its use is normally restricted to trusted network administrators and communicating externally via this protocol was therefore highly anomalous behavior compared to activity across the rest of the network. In investigating this unusual connection, Darktrace discovered that the server was also regularly contacting the external server via ICMP, transferring large volumes of information. This was a case of highly concerning data exfiltration and by detecting it in its earliest stages, Darktrace enabled the security team to quickly patch the breach before any critical information left the network.

What we found:

- The server was sending anomalously large volumes of information outside the network compared to its previously modeled behavior.
- No other servers on the network were receiving SSH connections from external computers.
- Communicating via ICMP was anomalous activity for the server as this protocol was otherwise rarely used.
- Darktrace packet capture revealed that the external server had successfully authenticated via SSH after a series of failed SSH connections using access codes listed as factory defaults online.

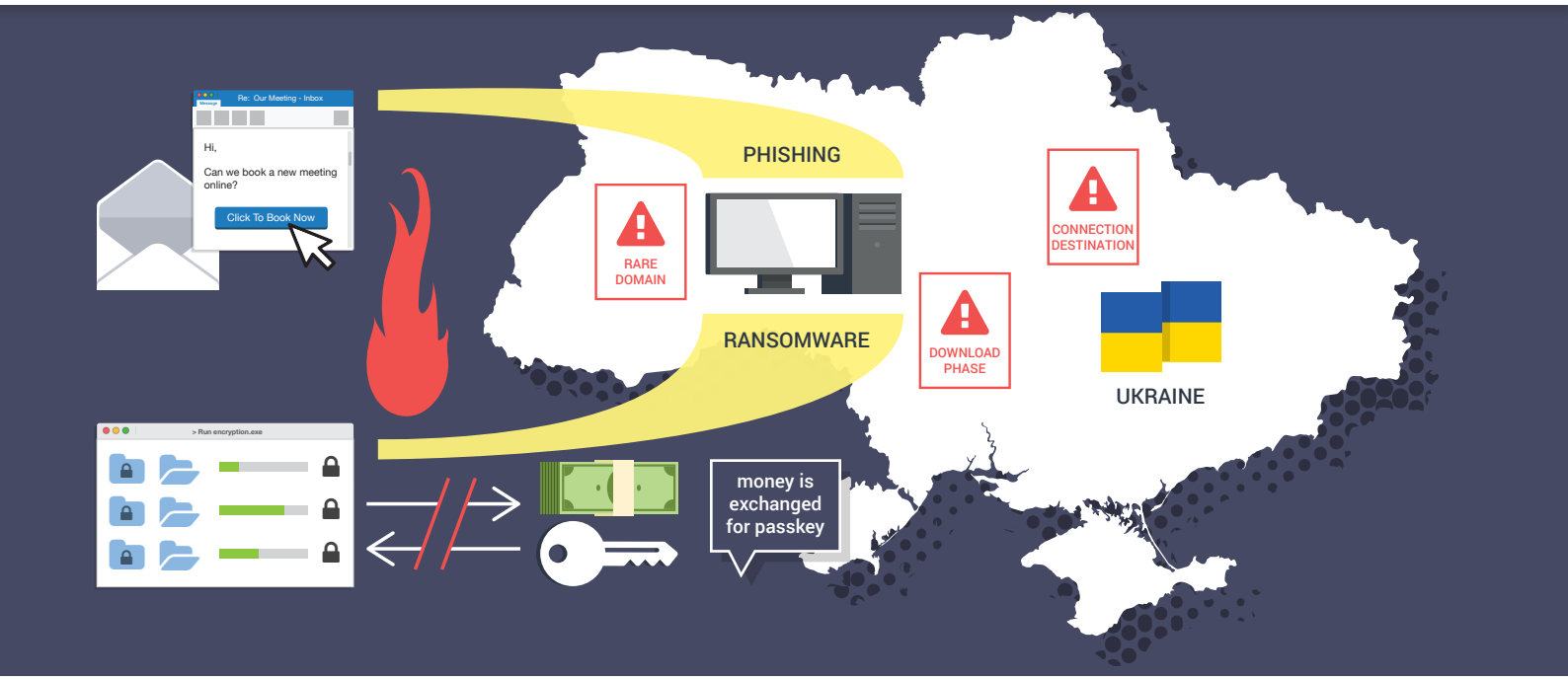
Industrial infrastructure is commonly well-shielded from contact with the public internet. However, the critical nature of such networks means that they are by definition more attractive to the most sophisticated cyber attackers interested in high profile targets. The fast development of the threat landscape means that signature-based defenses are unlikely to detect all sources of such threats. However, through a self-learning approach, Darktrace is able to draw attention to the unusual connections and data transfers that constitute emerging cyber-attacks.

6. Ransomware Attack on Charity

Industry: Non-profit

Point of Entry: Malicious PDF in disguised email

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



In late April 2016, a California-based charity became the target of a malicious ransomware campaign that threatened the functionality of the entire organization. Seen as a 'soft target' with limited security infrastructure, an attacker had researched the charity and forged a fake email disguised to resemble an invoice from a legitimate stationary supplier. The email was addressed and sent to the charity's receptionist.

Even the best-trained employees are vulnerable to this form of socially-engineered attack, and the receptionist had few clues that the email was malicious. After opening the attached pdf, JavaScript within the document connected the receptionist's computer with a server in Ukraine and downloaded malware designed to read and encrypt company files. The ultimate objective of this attack was to encrypt a large volume of crucial files and then demand payment (normally in the form of bitcoins) for the private key to unlock them again.

However, the charity had recently started a 4-week 'Proof of Value' trial ('POV') with Darktrace and the behavior of all devices on the network had been modeled for two weeks by self-learning algorithms. Darktrace therefore flagged the receptionist's computer for anomalous behavior when it contacted the Ukrainian server and downloaded a strange file. The computer then proceeded to make significantly more SMB requests than it ever had in the past. This was the ransomware attempting to read and encrypt shared files.

What we found:

- The Ukrainian server was rare for the charity's network as internal devices rarely contacted computers in that part of the world.
- The file the receptionist's computer retrieved was anomalous as no other company devices had downloaded a similar program since Darktrace was installed.
- The volume of SMB requests from the receptionist's computer was unusual compared to previous communications via this protocol.

Ransomware attacks unfurl more quickly than human security teams can deal with. However, in this case, a Darktrace analyst in New York recognized the computer's behavioral anomalies as a potential ransomware infection and quickly contacted the charity to take the infected computer offline. No significant harm occurred as although the ransomware managed to encrypt local files, the SMB requests were mostly unsuccessful and the malware had not yet spread throughout the network.

Conclusion

Anomaly detection is incredibly challenging, because while threats are getting more and more sophisticated and diverse, networks are simultaneously becoming more complex. The threats described in this report are therefore illustrative of a global trend in sophisticated, diverse and fast-moving attacks, which exploit the increasing digitization of work processes and the proliferation of connected objects.

These examples help to demonstrate the range of different types of threats that organizations today face, and yet which go unnoticed by traditional security tools, which inherently rely on pre-defined notions of what a 'threat' constitutes.

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 that it employs, using proprietary machine learning and probabilistic mathematics developed by world-class specialists from the University of Cambridge. It allows for the unbiased, self-learning detection of threats, which takes into account a range of network activities and combines deviations from a range of norms to form an overall picture of potential threats.

This approach eliminates the desensitization to threat alerts from legacy tools, which tend to flood security teams with false positives, allowing genuine threats to receive immediate attention and response. Machine learning techniques allow real-time screening and detection to be extended across entire information infrastructures, processing all traffic 24/7 – more than could ever be analyzed by a security team, however large. As such, it matches the speed of its adversaries, finding the tiny cracks in the wall that intruders are constantly on the lookout to exploit, as well as the early stages of internally-driven threats or attacks.

With the cyber black market reaching maturation, the barrier to entry for would-be attackers is lower than ever. All industries are now being targeted by non-traditional attacks, particularly by sophisticated software that blends into the background of day-to-day network activity. Artificial intelligence is now being deployed by attackers to emulate legitimate user behaviors, automatically. Cyber warfare has become an arms race.

The good news is that self-learning technologies can keep apace of these evolutions in the attack and threat landscape, because they grow and adapt with your organization. Darktrace's Enterprise Immune System technology rejects the one-size-fits-all methods of legacy tools that can only find what they already know to look for, and rather embraces the uncertainty inherent in today's threat environment.

About Darktrace

Darktrace is a world-leading cyber-threat defense company. Its multi-award-winning Enterprise Immune System technology automatically detects and responds to emerging threats, powered by machine learning and mathematics developed by specialists from the University of Cambridge. Without using rules or signatures, Darktrace models the 'pattern of life' of every device, user and network within an organization, identifying and mitigating cyber-threats before damage is done. Darktrace's self-learning technology has been deployed globally and across all sectors, including energy, retail, telecommunications, manufacturing, financial services and healthcare. The company is headquartered in San Francisco and Cambridge, UK, with over 20 global offices including London, New York, Milan, Mumbai, Paris, Singapore, Sydney, Tokyo and Toronto.

info@darktrace.com US: +1 (415) 243 3940 Europe: +44 (0) 1223 324 114 APAC: +65 6248 4516 www.darktrace.com