DARKTRACE

2021 Threat Report

Four Key Trends in the Cyber-Threat Landscape

The Security Implications of Remote Working

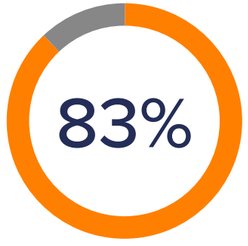
The sudden and wide-scale transformation to remote and hybrid working last year changed the digital landscape overnight, and introduced heightened risks and new challenges. Well-established procedures were quickly rewritten, best practices rethought, and policies stretched to breaking point.

Business transformation is always a security risk. New technology and working practices need new security measures, but normally this risk is managed carefully, and over time. Unsurprisingly, cyber-criminals were quick to capitalize on the unforeseen nature of the changes brought about by COVID-19, exploiting not only the overnight changes in working practices, but also the general sense of fear and uncertainty, with pandemic-related phishing emails and social engineering playing a key part in changes to the cyber-threat landscape.

All this demonstrated the necessity for companies' cyber security strategies to be dynamic and adaptive. Legacy solutions that rely on hard-coded rules and deny lists struggled in a new threat landscape which rendered many of these rules inappropriate or ineffective. These solutions failed to adapt when attackers sought out new vulnerabilities and new routes into the organization, while producing false positives on the legitimate and necessary changes that were occurring in workforce behaviors and technologies.

This threat report looks at four key trends that have been identified by Darktrace based on observations across its global customer base. Every stage of the attack lifecycle is explored, from reconnaissance and initial intrusion, through to the final stage of the kill chain: ransomware and data exfiltration.

The findings presented have been identified by Darktrace's team of world-class cyber analysts, based on their oversight of Darktrace Cyber AI's detections and investigations across over 4,500 organizations worldwide. The report details seven real-world cyber-threats that evades traditional, legacy security tools but were detected and investigated on in real time by Darktrace's AI. In many cases, the threats were neutralized within seconds by Darktrace's Autonomous Response technology, Darktrace Antigena.



of cyber security professionals say that their expanded infrastructure has complexified security challenges.

Forrester

New Opportunities for Attackers

Change brings novelty, and novelty brings opportunity for scammers. The sudden move to remote working forced internal security teams to work at full capacity, racing to roll out essential remote working tools and changes in authentication measures. This provided ample opportunity for spear phishers to impersonate third-parties and clients, drafting up convincing and clickable subject lines exploiting the general sense of uncertainty and commotion that characterized those few weeks.

New risks were exacerbated by the relaxing of security controls in order to facilitate non-standard working practices. Employees taking their work computer home with them found themselves suddenly stripped of protection as they traded the office network for home Wi-Fi, with client devices sitting exposed on potentially unsecured networks amongst potentially compromised machines.

In addition, widescale remote working increased the risk of malicious insiders, as data could now be easily taken from a company device over USB within the privacy of their own home. From a company perspective, employee homes are zero-trust environments: confidential conversations are conducted within range of eavesdroppers and intellectual property is visible on screens and monitors in living rooms around the world.

> "The COVID-19 pandemic accelerated the adoption of collaboration and cloud technologies as the world rapidly scaled up home working... this could heighten the cyber-resilience deficit where cybersecurity capacity is insufficient."
>
> World Economic Forum

Traditional Tools More Easily Bypassed

As organizations around the world began adopting new working patterns at a speed and scale that had never been seen before, one word in particular slipped into the lexicon time and time again. Unprecedented. Legacy security tools, by nature, cannot deal with unprecedented. Confined to playbooks and deny lists put together solely from previous attacks, these tools became increasingly redundant once the digital landscape had changed beyond recognition.

Grappling with these new circumstances, employees and IT teams alike increasingly sought workarounds to get their jobs done and ensure business continuity. Pre-existing use cases and rules that may have been suitable in the past did not apply to new cyber challenges, as organizations realized the need for a more proactive and dynamic approach to detection and response.

Increasing Pressure on the SOC

All of the above changes and risks created a monitoring nightmare for SOCs entering into a period of digital unknown. Data flows and topology changed overnight. New technology and services were deployed in record time. Logging formats changed. SIEM use cases that took 12 months to develop had to be scrapped overnight.

As working practices continue to change in unforeseen ways, companies need to leverage technology that allows them to continue to operate amidst uncertainty without impeding productivity at this critical time. The following case studies showcase how cyber security technology grounded in AI that continually evolves and adapts to change is critical in identifying the latest attack trends.

SaaS Account Takeover

The onset of the pandemic has prompted an explosion in usage of SaaS applications such Microsoft Teams, Zoom, and Webex. From a security perspective, these working practices form a complex patchwork of siloed services that do not benefit from visibility across the rest of the business.

This surge in SaaS usage introduced a heightened risk of compromised credentials and insider threats, especially from malicious administrators with privileged access.

Cyber-criminals often take to the email realm to solicit these credentials directly from employees, posing as the SaaS platforms themselves and sending fake notification emails that lead the user to a fake login page. When an employee enters their credentials, these are then fed directly back to the attacker who can then log in to the legitimate account and wreak havoc.

Darktrace frequently catches attackers masquerading as WeTransfer, Microsoft Teams, and ShareFile in a string of these attacks. In each case, these attacks routinely slip through gateway tools, but were detected by AI, which then prevented them from reaching the inbox.

of organizations are monitoring unusual activity across their cloud and SaaS environments

Cybersecurity Insiders:
2020 Insider Threat Report

"Darktrace provides complete visibility of all cloud infrastructure, allowing us to monitor all activity in our remote locations and across offices."

Director of IT, TRJ Telecom

Threat Find: Phishing Attack Slips Through Gateway and Leads to Microsoft 365 Account Hijack

To gain an insight into how credentials can so easily fall into attackers' hands and how this can set the stage for a string of further attacks, we can look at the case of an Australian logistics company that had installed Antigena Email in passive mode just days before a serious security incident took place.

The company was under sustained attack from a cyber-criminal who had already hijacked the accounts of numerous trusted partners, sending out several tailored emails with the same convention in the subject line – RFP for [compromised company's name] – and all appeared to be credential harvesting. As they came from legitimate and familiar accounts, these emails were all considered non-threatening by the gateway.

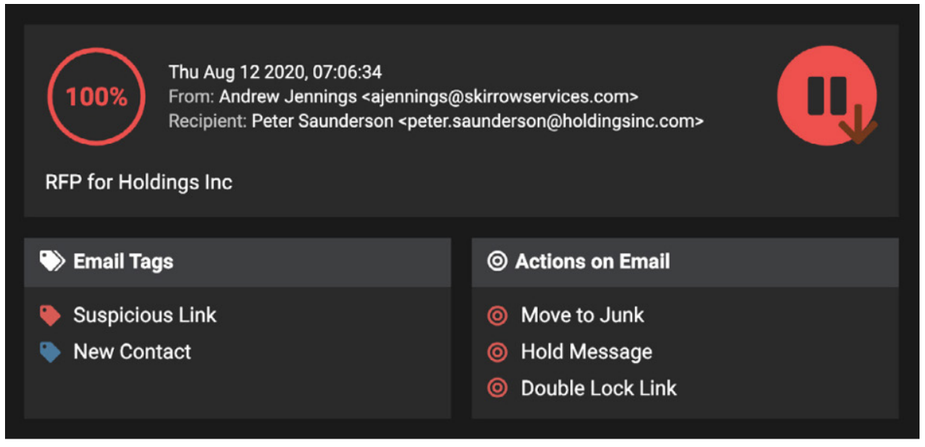


Figure 1: Antigena Email monitors the offending email, with the hold icon indicating the action it would have taken in active mode. Identities have been anonymized

When clicked on, the victim was taken to a fake Microsoft login page for credential harvesting. This was an accurate replica of a genuine login page and sent email and password combinations directly to the attack for further account compromise.

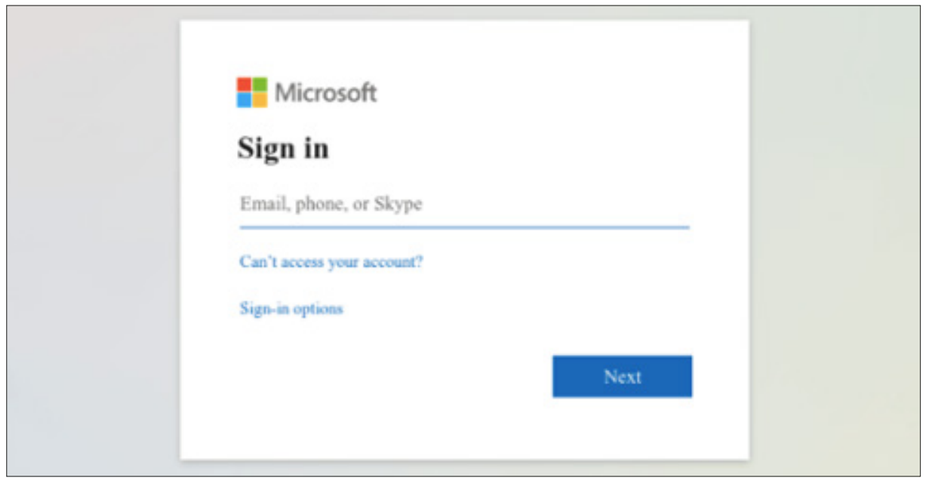


Figure 2: The fake Microsoft login page

A number of employees read the email, including the CEO. However only one person – a general manager – appeared to get their email account hijacked by the attacker. About three hours after opening the malicious email, Darktrace detected an anomalous SaaS login on the account from an IP address not seen across the business before.

Open source analysis of the IP address showed that it was a high fraud risk ISP, which runs anonymizing VPNs and servers – this may have been how the attacker overcame geofencing rules. Shortly afterwards, Darktrace detected an anonymous sharing link being created for a password file.

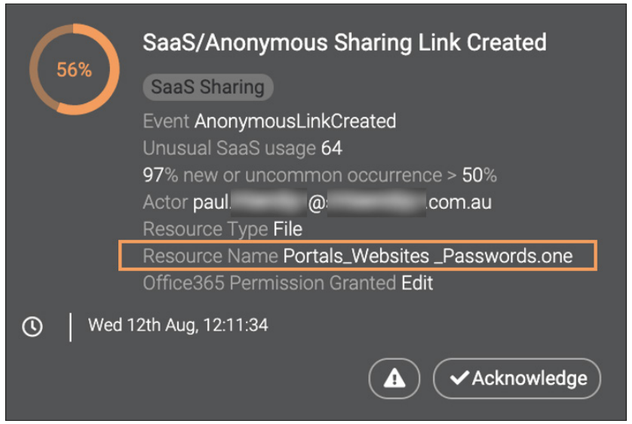


Figure 3: Darktrace's SaaS Module revealing the anomalous creation of a link

Darktrace AI observed the attacker accessing potentially sensitive information, including a file that appeared to hold information about credit card transactions, as well as a document containing passwords.

After the attacker had exhausted all sensitive information they could elicit from the email account, they sent out further malicious emails to trusted business associates using the same methodology that using the same methodology of the initial compromise. Darktrace's SaaS module identified this anomalous behavior, graphically revealing that the attacker sent out over tailored 1600 emails across the course of 25 minutes.

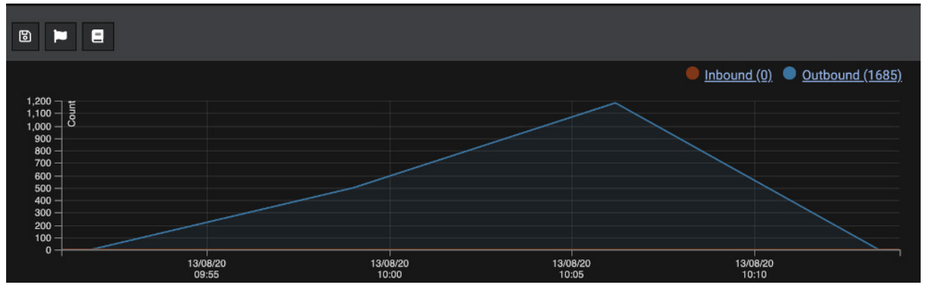


Figure 4: A graphical representation of the burst of emails sent over a 25-minute period

The Managed Security Service Provider (MSSP) running this logistics organization's cloud security was completely unaware of the account takeover. With the modern workforce more dispersed and agile than ever, there is a growing need to protect remote users across SaaS collaboration platforms, while neutralizing email attacks before they reach the inbox.

The Rise of Fearware: Phishing Emails Exploiting Uncertainty

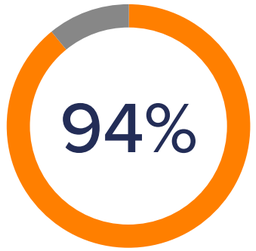
The cyber-criminals behind email attacks are well-researched and highly responsive to human behaviors and emotions, often seeking to evoke a specific reaction by leveraging topical information and current news. It's therefore no surprise that last year Darktrace saw attackers attempting to latch onto COVID-19 in their latest effort to convince users to open their emails and click on seemingly benign links.

Between March and May, Darktrace witnessed a massive surge in spoofing attacks – accounting for 40% of all attacks over the initial lockdown period. 130,000 newly-registered domains relating to COVID were created – with over half of those used for malicious purposes.

By April, 60% of all email attacks were related to COVID or remote working in some way, confirming what we knew already: attackers are inherently opportunistic and continue to leverage the latest trends and news items as fuel for their social engineering attacks.

Email gateways that relied on reputation checks and lists of 'known-bad' IPs, domains, and file hashes to determine an email's threat level unanimously failed to stop these attacks. Freshly purchased domains don't have a reputation and these tools are torn between triggering countless false positives or letting these attacks through by default.

Traditional email security tools resort to 'sandboxing', which creates an isolated environment for testing links and attachments seen in emails. But most advanced threats now employ evasion techniques like an activation time that waits until a certain date before executing. When deployed, the sandboxing attempts see a harmless file, not recognizing the sleeping attack waiting within.



of cyber-attacks start with an email

Threat Find: 'Fearware' Attacks Neutralized by Darktrace's AI

Over the past year, attackers have increasingly played into Fear, Uncertainty, and Doubt (FUD) by leveraging 'Fearware' tactics where they purport to be officials with pertinent information about the current state of events in the world.

Darktrace caught several of these attacks targeting all industries, including this sample of emails neutralized in early March, purportedly from the Center for Disease Control (CDC).

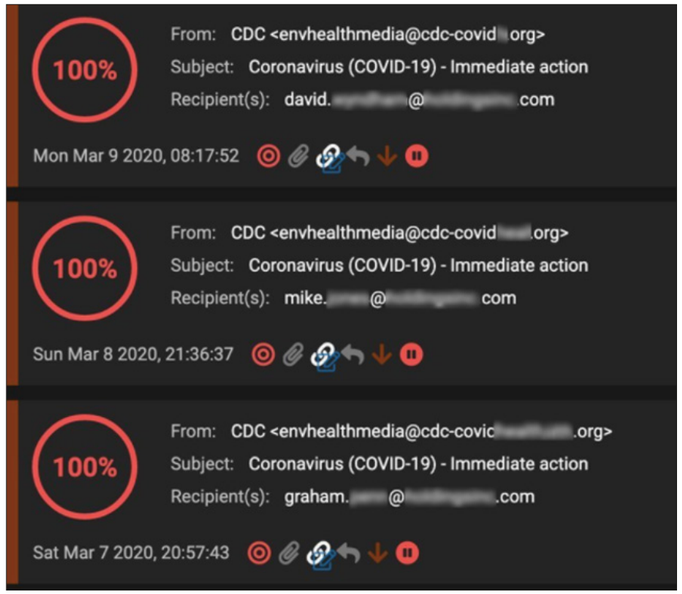


Figure 5: The CDC spoof emails that evaded gateways but were topped by Antigena Email

These emails claimed to offer urgent information on the spread of the pandemic and requested that immediate action would be taken. However, Darktrace detected that these emails contained malicious and highly anomalous links, holding the communication back from the recipients' inboxes and protecting the organizations from harm.

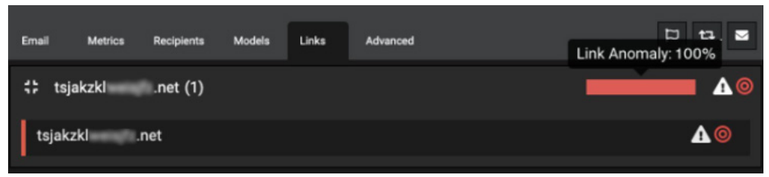


Figure 6: The 100% anomalous link surfaced by Darktrace

As the situation changed over the course of the year, so did attackers' approach to phishing. Cyber-criminals pivoted away from emails offering urgent health-related advice or localized infection data and towards fake emails from well-known institutions sharing forms for COVID relief funds.

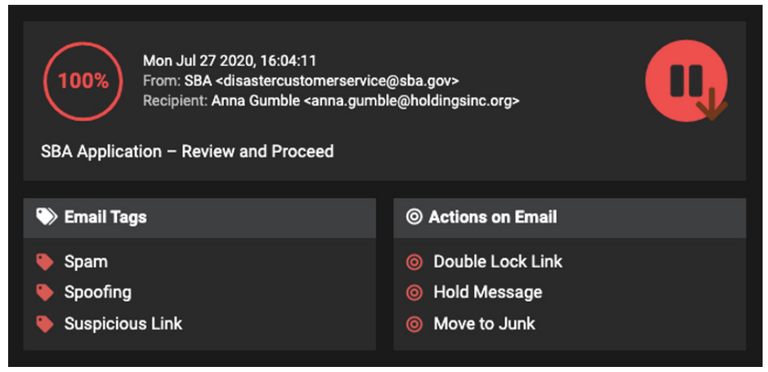


Figure 7: The indicators that led Antigena Email to hold back the phishing attempt

If clicked on, these emails would have led to a fake login page using the logo of SBA and formatted in the same style as legitimate pages from the genuine SBA website. If entered, these credentials would be sent straight into the attacker's hands, enabling them to launch the kind of SaaS account takeover described above.

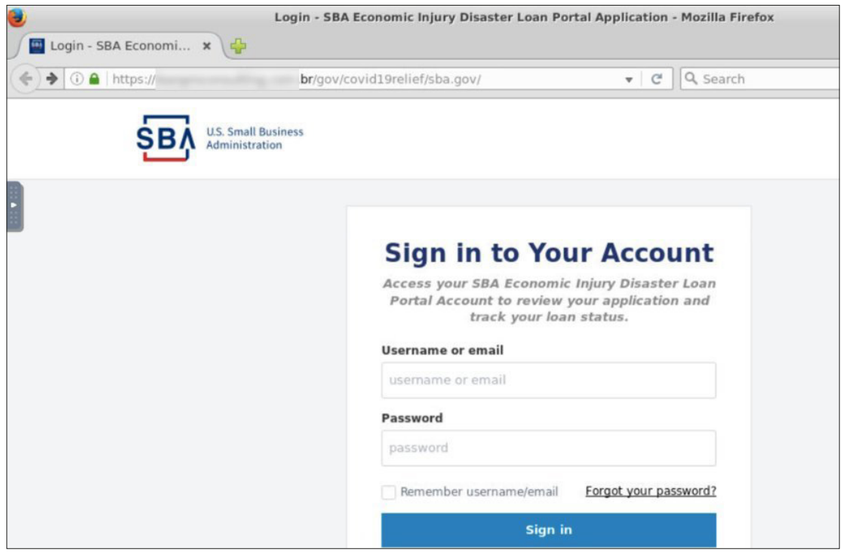


Figure 8: The fake login page

2021 will bring fresh developments and news items which we cannot yet imagine that email attackers will undoubtedly look to capitalize on. Email tools that rely on defining 'bad' with reference only to past attacks will be ineffective against the next wave of phishing emails exploiting new topics, since training data does not yet exist for this type of threat.

"Antigena Email is light years ahead of any other email security system."

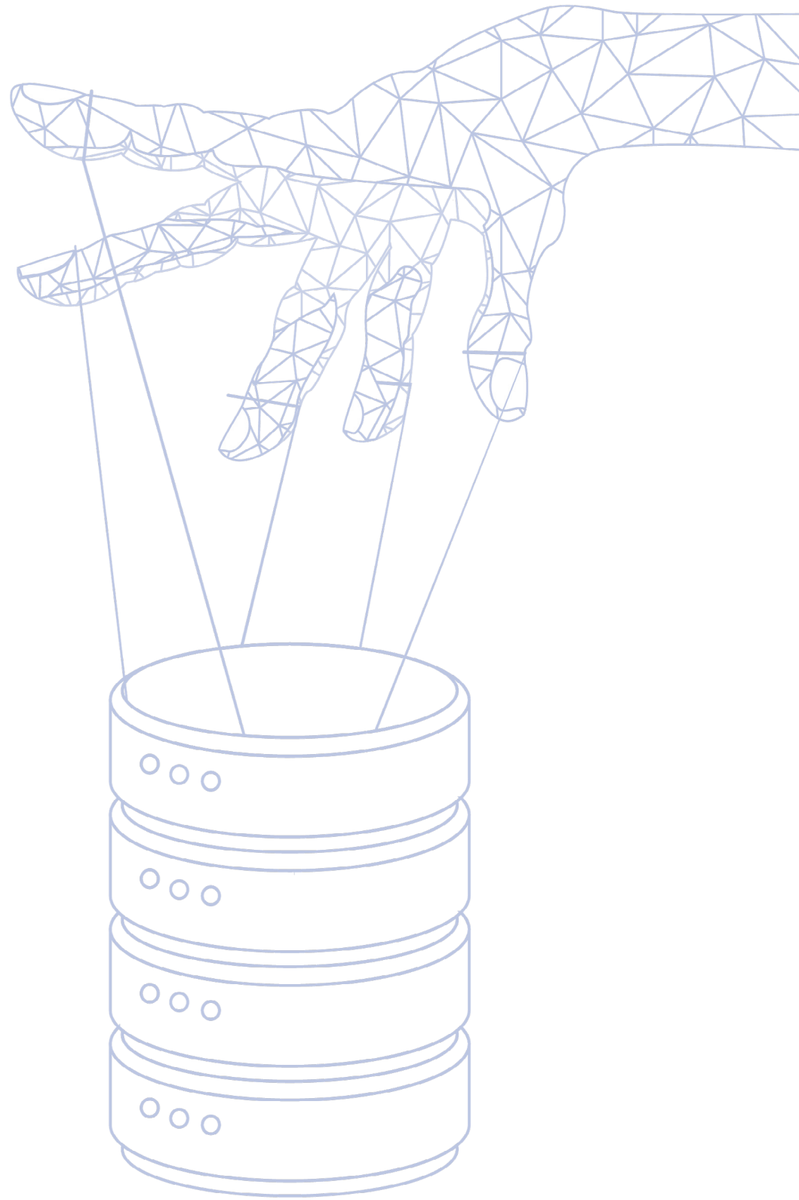
Cyber Security Vice President, Global Conglomerate

"Our experience with Antigena Email has been positive since the day we installed it."

Manager of IT, Entegrus

Resurgence of Server-Side Attacks

The spinning up of new infrastructure in rapid succession has reinvigorated more ‘traditional’ risks. With companies rapidly deploying VPN gateways and expanding their internet-facing perimeter, this rapidly increased attack surface has paved the way for a surge in more ‘traditional’ brute-force and server-side attacks.



Exploiting Internet-Facing Servers

With poorly-secured public-facing systems rushed out in record time, companies prioritized availability – inevitably sacrificing some security in the process. Patching vulnerabilities has been as difficult as ever this year and with IT teams over-stretched and many staff members furloughed or laid off, financially-motivated actors sought to weaponize these weak points in organizations.

A number of vulnerabilities against such internet-facing servers and systems were disclosed this year, such as the Citrix Netscaler security flaw explored below. Darktrace found many instances of vulnerabilities in similar networking and firewall gear throughout the year.

On the attacker’s side, targeting and exploiting internet-facing infrastructure is easier than ever – scanning the internet for vulnerable systems is easy with tools like Shodan or MassScan.

Threat Find: Cyber AI Analyst Investigates APT41 Exploiting A Zero-Day Vulnerability

Darktrace recently detected Chinese threat-actor APT41 exploiting the Zoho ManageEngine zero-day vulnerability CVE-2020-10189 across multiple customers, principally in the legal sector.

Darktrace Cyber AI not only detected this zero-day attack campaign, but Cyber AI Analyst also saved security teams valuable time by investigating disparate security events and generating a report that immediately put them in a position to take action.

Cyber AI Analyst reported on six incidents in total over the eight-day period. Each AI Analyst incident report includes a detailed timeline and summary of the incident in a concise format that takes an average of two minutes to review. This means that, even a non-technical person could have actioned a response to this sophisticated, zero-day incident in less than five minutes.

Darktrace detected these attacks well before any associated signatures had become available. The attacks were not publicly attributed to Chinese threat-actor APT41 until two weeks after these events.

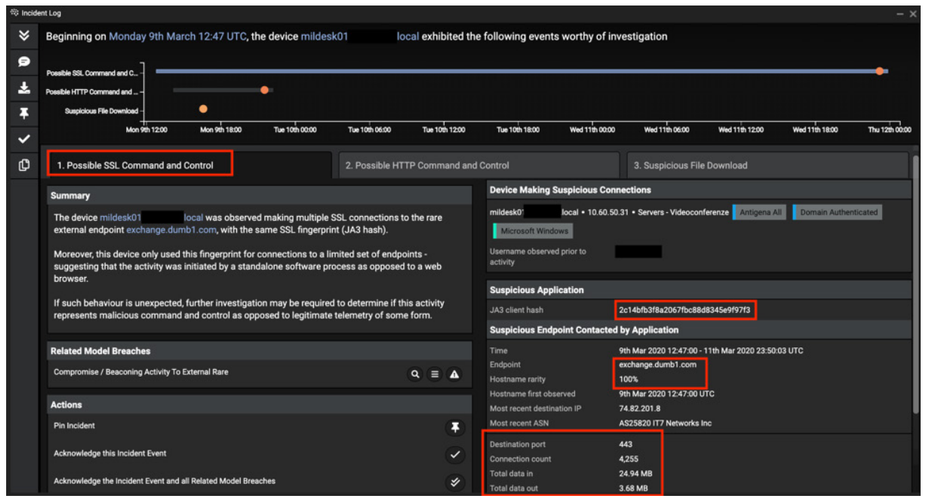


Figure 9: SSL C3 detection by Cyber AI Analyst

Remote Working

SaaS Takeover

Rise of Fearware

Server-Side Attacks

Ransomware

The Immune System

Threat Find: Bitcoin Mining Campaign Leveraging Zero-Day Citrix Netscaler Vulnerabilities

Darktrace's Cyber AI identified at least 80 different customers being targeted through the CVE-2019-19781 vulnerability — affecting the Citrix Application Delivery Controller and Citrix Gateway solution for public cloud. The exploitation of this vulnerability allowed unauthenticated attackers to perform arbitrary code execution. Although patches were rolled out after just a couple of weeks, in that critical window of time, cyber-criminals were quick to weaponize the exploits with crypto-mining payloads.

Darktrace identified and alerted on the following activity:

1. Exploited Citrix Netscaler devices beginning to execute shell commands, receiving HTTP POST requests to URIs vulnerable to directory traversal attacks
2. Code execution being triggered, leading to the download of shell scripts and other malware with the end-goal of running crypto-mining malware
3. Compromised devices downloading an executable file from unusual locations (commonly Ukraine and Russia), containing an ELF:BitCoinMiner Malware

Darktrace Antigena immediately kicked in, eliminating the incoming threat by blocking miner file downloads and activity for 24 hours. This offered security teams ample time to react to this anomalous activity and halt the malware's spread to other devices. Despite this being a zero-day vulnerability, every stage of the attack lifecycle involved behavior that in some way deviated from Darktrace's learned 'pattern of life'.

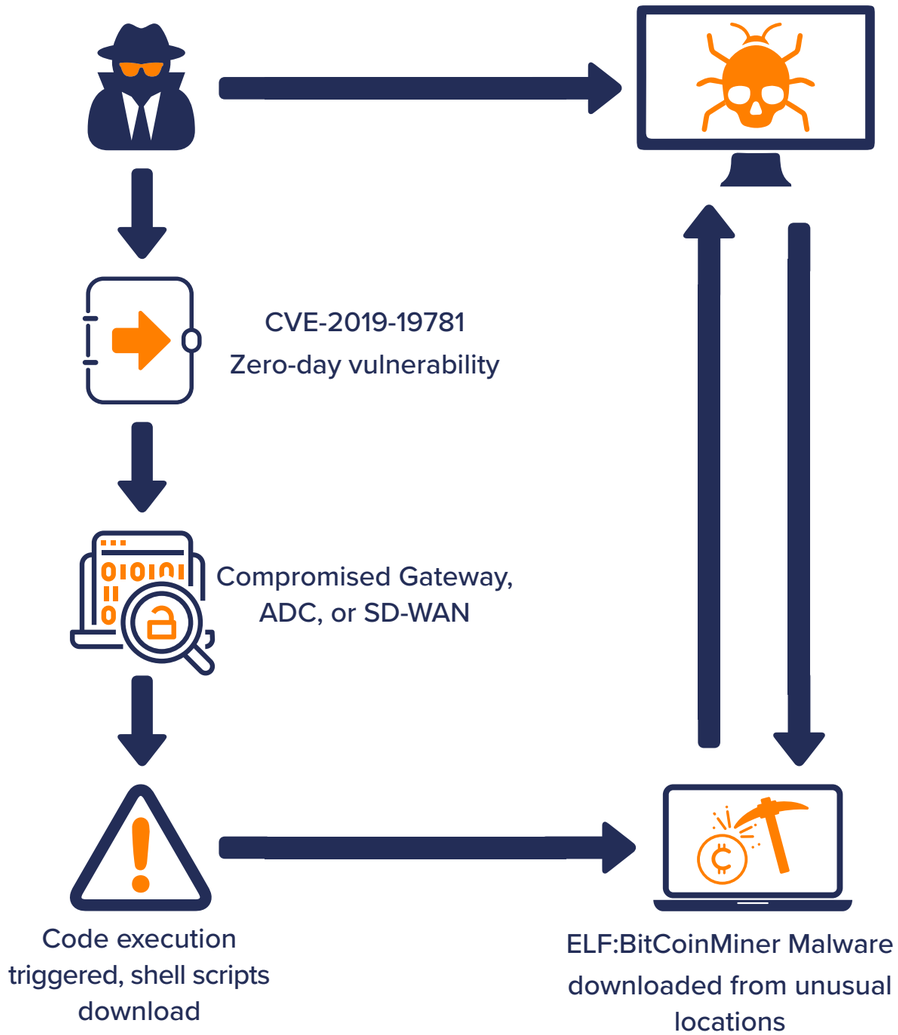


Figure 10: The life cycle of a crypto-mining campaign

Threat Find: Crypto-Mining on a Biometric Scanner

Darktrace detected a crypto-mining campaign that used the processing power of a corporate server to mine cryptocurrency at a manufacturing firm in Asia. This server was in control of biometric door access within the client's office and first downloaded a suspicious executable before beginning to mine for cryptocurrency. This occurred while the firm's physical office was closed, with all employees working remotely due to COVID-19.

Darktrace Cyber AI detected the server downloading a suspicious executable file from a new external IP that had never been seen before across the organization's digital infrastructure.

Cyber AI Analyst launched an automatic investigation into these events, presenting a fully actionable report of the security incident. This incident demonstrates the importance of security tools that not only can detect known IoCs, but emerging and unknown incidents.

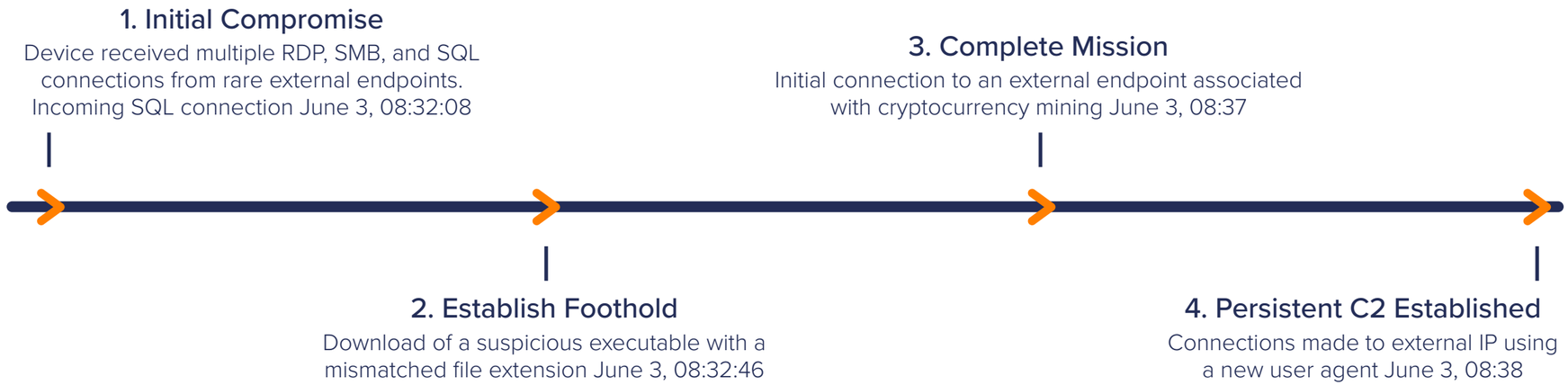
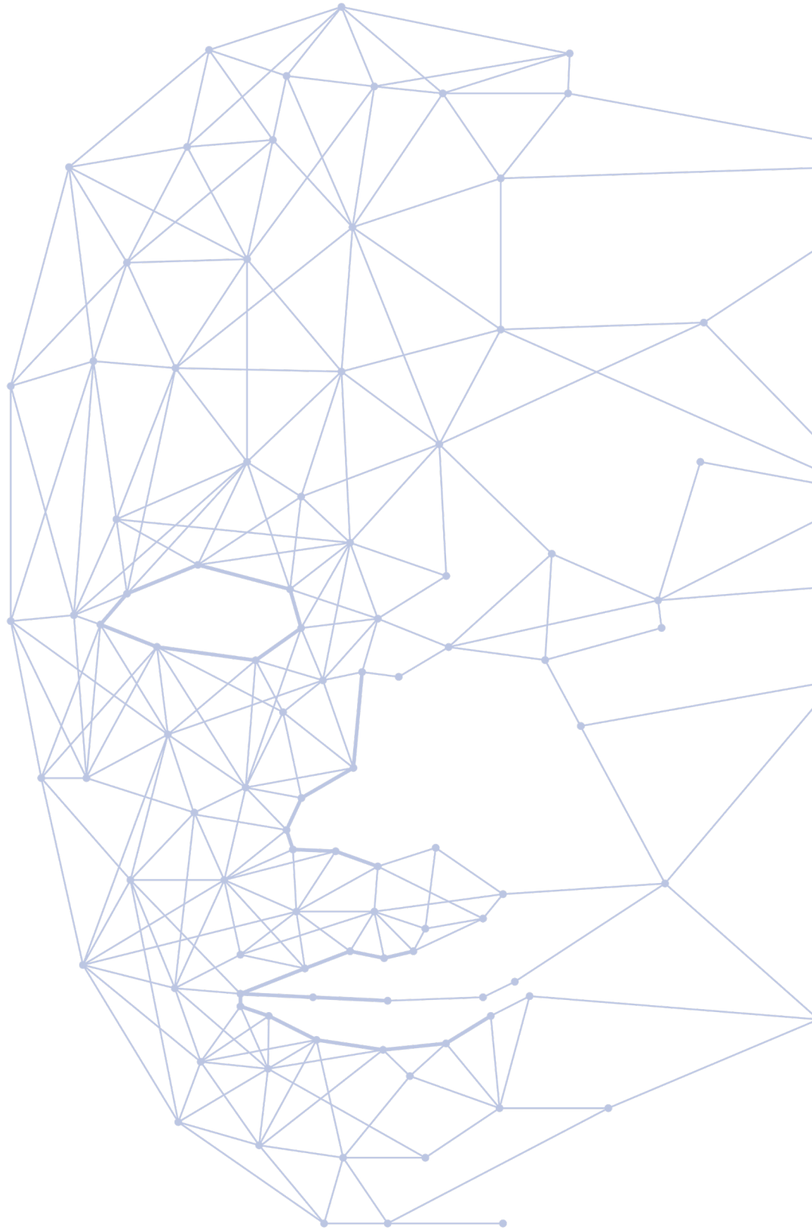


Figure 11: Timeline of crypto-mining attack

Stolen Credentials Over RDP Servers and VPNs

Another server-side threat vector Darktrace has witnessed becoming increasingly common is cases of RDP brute-forcing and stolen credentials being used for initial infiltration. In addition to credential stuffing, credential reusing is also very popular, that is, reusing legitimate credentials from previous data dumps. This has much higher precision and is less noisy than a classic brute-force attack.

- As many as 85% of ransomware attacks use RDP as an entry vector.
- Ensuring that backups are isolated, configurations are hardened, and systems are patched is not enough – real-time detection of every anomalous action is needed.
- A TTP growing in popularity is to buy RDP credentials on marketplaces and skip to initial access.
- This is part of a wider trend of 'living off the land': using legitimate off-the-shelf tools (RDP, abusing SMB1 protocol) to blur detection and attribution by blending in with typical administrator activity.
- Darktrace recommends monitoring internet-facing systems and critical servers closely – keeping track of administrative credentials and carefully considering security when rapidly deploying internet-facing infrastructure.



Threat Find: Dharma Ransomware Detected via RDP Intrusion

Darktrace detected a targeted Dharma ransomware attack exploiting an open RDP connection through internet-facing servers. The RDP credential used in this attack had likely been compromised prior to the attack – either via common brute-force methods, credential stuffing attacks, or phishing.

Cyber AI identified that the RDP server began initiating a large number of anomalous and rare connections to new external destinations located in India, China, and Italy – most likely an attempt to establish C2.

The RDP server then wrote a number of files over SMB, appended with a file extension containing a throwaway email account possibly evoking the current COVID-19 pandemic, 'cov2020@aol[.]com'.It was during the encryption activity that the security team pulled the plug from the compromised RDP server, ending the ransomware activity.

This incident serves as a reminder of how 'legacy' ransomware may morph to resurrect itself and exploit new vulnerabilities in remote working infrastructure. Darktrace detected every stage of the attack without having to depend on threat intelligence or rules and signatures, and the internal security team acted on the malicious activity to prevent further damage.

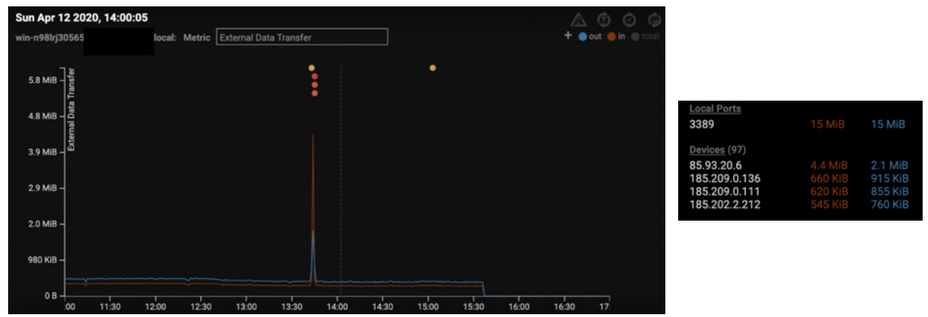


Figure 12: Darktrace detects the anomalous external data transfer

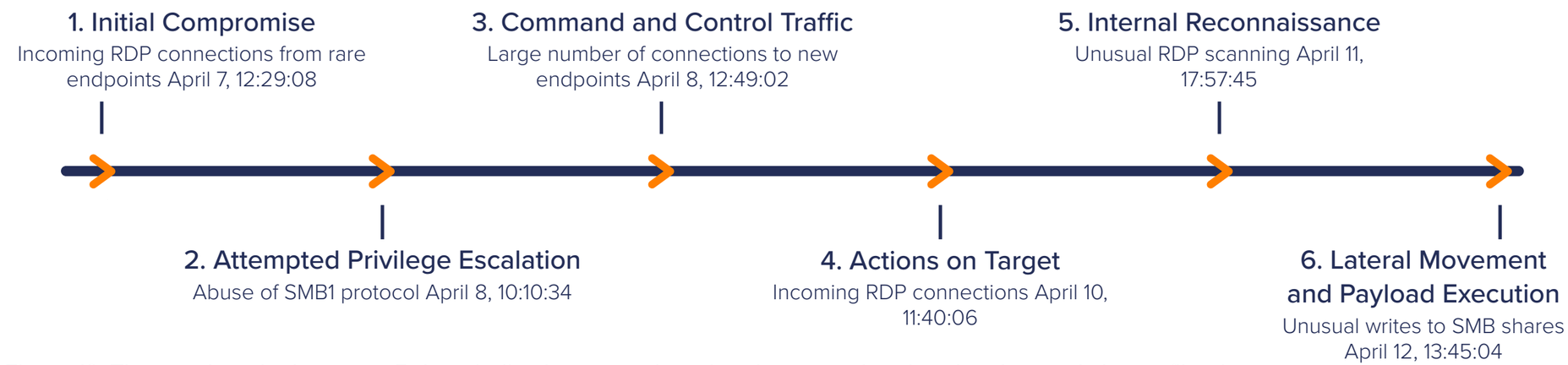


Figure 13: The attack took place over 5 days, indicating a smash-and-grab approach rather than low-and-slow exfiltration

Ransomware

Remote Working
SaaS Takeover
Rise of Fearware
Server-Side Attacks
Ransomware
The Immune System

Ransomware represents just the final stage of a cyber-attack and should not be seen as a separate entity to the preceding trends. It is plausible for an attack to start with a 'Fearware'-style phishing email, for example, and then culminate in the encryption of files.

Darktrace has witnessed a significant rise in 'double threats' that exfiltrate sensitive files before encryption begins. The exfiltrated data can then be used as leverage, with threat-actors threatening to leak them if payment is not met.

Traditional security tools programmed only to detect known cyber-threats using rules and signatures are left blind to tailored and novel ransomware that have never been seen before in the wild. With machine-speed attacks often striking at night or weekends, having Autonomous Response capable of acting without human oversight is critical.

Autonomous Response in Seconds

Unusual admin SMB session: Compromised credentials used to login to server	This anomalous event heightens alert level, but no reinforcing action is taken at this point.
New admin credentials on client: The attacker used multiple new admin credentials on the device	**Antigena action:** Antigena enforces the device's typical 'patterns of life'. New logins are blocked for one hour, while habitual admins are allowed to continue.
Network scan: The attacker scanned the network to identify further victims	**Antigena action:** Antigena stops the device from scanning the network for two hours.
EXE from rare external location: Later-stage payloads downloaded for further infection	**Antigena action:** Antigena blocks downloads from rare locations while allowing the device to continue conducting normal and expected downloads.

Threat Find: Antigena Autonomously Neutralizes Zero-Day Ransomware

Darktrace Antigena stopped a 'zero-day' ransomware attack targeting an electronics manufacturer. Darktrace's Cyber AI identified patient zero deviating significantly from its typical pattern of internal behavior. This was illustrated by a spike in the pattern of regular connections made by patient zero and a series of high-confidence alerts.

The device was observed making an unexpectedly large number of connections, writing a multiple number of SMB files, and transferring this data internally to a server it did not usually communicate with. This spike in internal connections between patient zero and the server was detected immediately by Darktrace.

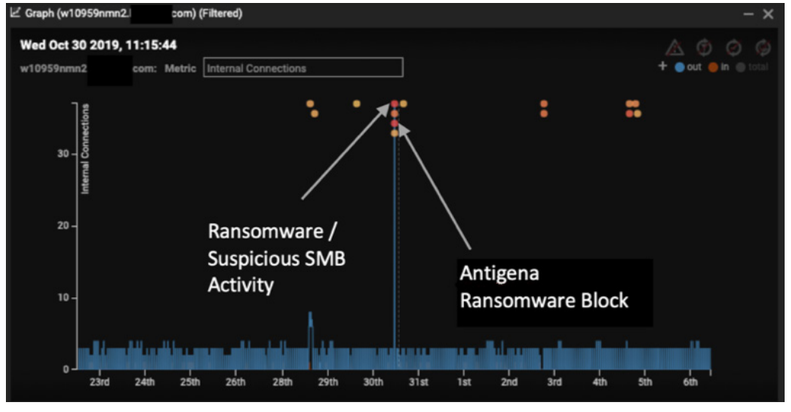


Figure 14: Four model breaches observed on October 30th and a dotted line representing Antigena's actions

Hundreds of Dropbox-related files were accessed on SMB shares that the device had not previously accessed, and several of these files started becoming encrypted, appended with a [HELP_DECRYPT] extension.

Fortunately, Antigena was in Active Mode and kicked in a second later, enforcing the usual pattern of life by quarantining the device for 24 hours, immediately stopping the encryption. By the time Darktrace's AI took action, only four of these files were successfully encrypted.

This strain of ransomware was not associated with any publicly known indicators of compromise such as blacklisted command & control domains or malware file hashes. Darktrace was able to detect this never-before-seen attack based purely on its comprehensive understanding of the normal pattern of life for every device and user within the organization. This stealthy strain of ransomware is unlikely to have been noticed, let alone stopped, by a security team reliant on legacy tools.

The Return-On-Security-Investment (ROSI) is often discussed when it comes to cyber security expenditure and this incident provides a great example of the ROSI manifesting itself – ransomware attacks usually demand hundreds of thousands of dollars. By relying on Cyber AI, the company was able to take back the advantage over an ever-evolving adversary, saving time, money, resources, and – perhaps most critically – the company's reputation.

Darktrace Immune System

Remote Working
SaaS Takeover
Rise of Fearware
Server-Side Attacks
Ransomware
The Immune System

The Darktrace Immune System emerged from a simple yet ground-breaking premise: that cyber security cannot protect from today's threats by relying on pre-existing knowledge of yesterday's attacks. The technology marks a drastic departure from legacy security tools that rely on hard-coded rules and signatures and focuses instead on learning the normal 'pattern of life' for individual businesses and spotting subtle deviations indicative of a threat.

Like the human immune system, the Enterprise Immune System learns 'on the job' from the data and activity that it observes in situ. This means making billions of probability-based calculations in light of new evidence and continuously learning as the business evolves. By learning a sense of 'self' for your entire organization, Darktrace discovers subtle, previously unseen patterns and emerging threats that would otherwise go unnoticed.

Darktrace Antigena, the world's first world's leading Autonomous Response technology, intelligently fights back against threats that deviate from this learned 'pattern of life', taking swift and targeted action to interrupt attacks with precision, even if the threat is targeted or entirely unknown.

With Cyber AI Analyst, Darktrace combines expert analyst intuition with the speed and scalability of AI, carrying out automated investigations that reduce time to triage by up to 92%. Whenever Darktrace's Immune System detects a pattern of suspicious behavior, Cyber AI Analyst launches into an enterprise-wide investigation, stitching together disparate anomalies before generating a high-level report about the nature and root cause of the wider security incident.

The vast majority of serious incidents security teams face this year tend not to be pre-existing threat vectors but rather novel threats that evaded existing defenses. The limitations of legacy tools were thrown into the spotlight in new ways while organizations with a dynamic security structure that could deal with novelty were able to stay on top of the threat trends that follow. AI that adapts continuously and is able to learn the "new normal" is enables organizations to stay ahead of the threat, protecting their workforce and data at a critical time.

Figure 15: Darktrace's Immune System platform

About Darktrace

Darktrace is a leading autonomous cyber security AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 4,700 organizations to protect against threats to the cloud, email, SaaS, traditional networks, IoT devices, endpoints, and industrial systems.

The company has over 1,500 employees and is headquartered in Cambridge, UK. Every second, Darktrace AI fights back against a cyber-threat, before it can cause damage.

For More Information

- Visit darktrace.com
- Book a demo
- Visit our YouTube channel
- Follow us on Twitter
- Follow us on LinkedIn