DARKTRACE

2021 Cyber-Threat Landscape

Five Key Trends: From Ransomware to Slow and Stealthy APTs

The New Era of Cyber-Threat

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

The cyber-threat landscape is constantly changing, but with attackers ramping up the scale and sophistication of their campaigns faster than ever, it is now clear that security tools reliant on rules and signatures are fundamentally incapable of protecting organizations from today's threats. To put this into context, it is worth looking at how the cyber security industry has evolved.

Retrospective	Siloed	Outpaced
Legacy tools react to attacks and only detect techniques that have been seen before	Security solutions for email, cloud, network, endpoint, and OT have developed independently	The industry has a history of relying on humans to respond to machine-speed threats

Figure 1: The traditional limitations of the cyber security industry

Attackers are acutely aware of the defensive tools they are trying to evade and know better than anyone the limitations of the legacy, siloed approach that the majority of organizations still rely on. And in every area attackers have innovated, developing new techniques to bypass these systems and achieve their goals.

In recent years, cyber-criminals have begun updating their attack infrastructure with greater ferocity, knowing that novel attacks evade the historical deny lists relied on by email gateways, anti-virus tools, and traditional endpoint solutions.

Further, they have broadened the scope of their attacks, targeting different areas of the digital enterprise – from email and SaaS environments, to cloud infrastructure, the Internet of Things (IoT), and Industrial Control Systems (ICS).

And in late 2020, the World Economic Forum warned that the "first generation of AI-enabled offensive tools is emerging", which will increase the speed, scale, sophistication, and stealth of cyber-criminal campaigns.

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

These developments, in addition to several, recent, high-profile and immensely costly attacks, have further strengthened the case for the use of AI in cyber security. The threat drivers are forever changing, and a reliance on traditional, legacy-based solutions is no longer adequate. According to a recent Forrester survey of Fortune 500 companies, 83% of respondents believe AI augmentation of their security teams is necessary for cyber defense.

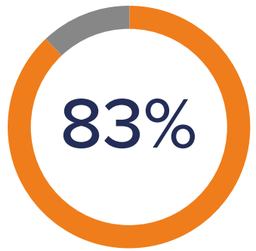
By building an evolving understanding of what 'normal' looks across the entire digital business, Self-Learning AI detects the subtle indicators of attack that evade traditional tools. It then surgically responds at machine speed – disrupting the full range of cyber-threats, regardless of whether they have been seen before.

Now relied upon by thousands of organizations, Autonomous Self-Learning AI is no longer considered a nice to have but a necessity in protecting diverse and ever-changing digital ecosystems from a new era of cyber-threats.

Darktrace Discoveries: Five Key Trends

In what follows, we uncover five threats observed across Darktrace's customer base of over 5,000 organizations. These threat vectors were selected based on how frequently the attacks were seen, their likelihood of success, and the extent of the damage in the case of a successful attack.

Each trend is analyzed in detail by looking at a real-world threat discovered by AI in a customer environment. In every case, the threat in question slipped under the radar of the traditional security tools in place. By uncovering how Self-Learning AI was able to detect and remediate the threat based off a series of subtle anomalies, the advantages of a self-learning, autonomous approach to cyber security is exemplified.



of cyber security professionals believe AI augmentation of their security teams is necessary for cyber defense

Forrester

Stealthy and Subtle APTs

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

Advanced Persistent Threats (APTs) are driven by highly sophisticated threat actors and are often supported by nation-states. They no longer only affect large, multinational organizations and government institutions but now target a wider range of private enterprises.

These campaigns will typically lay low inside systems for weeks or months, leveraging commonly used tools and protocols in a technique known as 'living off the land'. Attackers may subtly exfiltrate sensitive data over a long period, often attempting to blend into regular digital activity by operating during busy times. As the attackers gather intel and build an understanding of the organization, preparations are made for the moment of detonation: the encryption of devices and a ransom note demanding payment for their safe return.

Ransomware will cost businesses over $20 billion in 2021

Cybersecurity Ventures, 2021

Darktrace Cyber AI Analyst detected APT41 two weeks before public attribution

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

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

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.

Self-Learning AI not only detected this zero-day attack campaign but with Cyber AI Analyst, Darktrace's AI investigation technology, automatically analyzed linked security events and generated an Incident Report that immediately put the security team in a position to take action.

Cyber AI Analyst reported on six incidents in total over the eight-day period. Each Cyber AI Analyst Incident Report included a detailed timeline and summary of the incident in a concise format that took 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

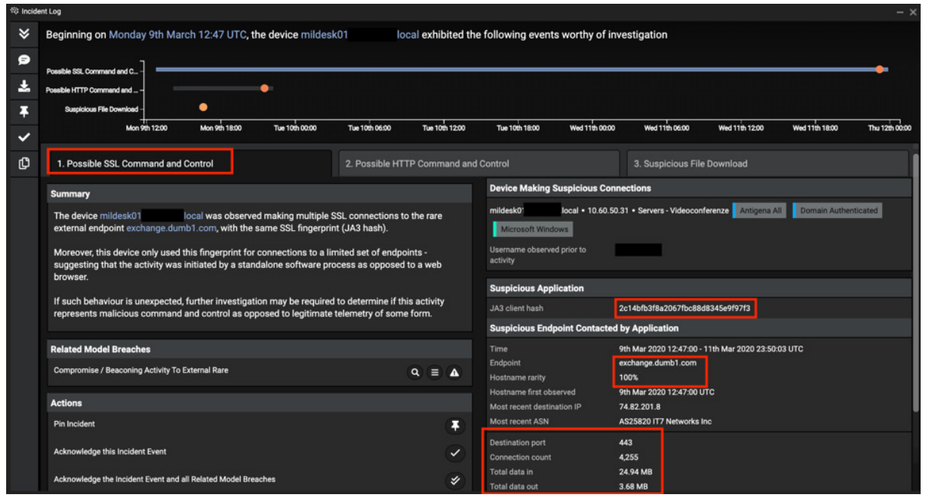


Figure 2: SSL C3 detection by Cyber AI Analyst

The Relentless Rise of Ransomware

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

Ransomware continues to be top of the agenda for security teams globally. Novel attacks are constantly emerging, leveraging fileless malware and new methods of lateral movement. Darktrace has recently seen a sharp increase in attacks detonating in the early hours of the morning or on the weekend, when human response times are slow.

Further, an uptick of double extortion ransomware – where the data is first exfiltrated and then encrypted – provides attackers with greater leverage should an organization refuse to pay the ransom.

In response to the sweeping wave of ransomware attacks targeting public and private institutions, representatives from the FBI as well as the US Department of Justice have declared ransomware a "national security threat".

Educational institutions and hospitals have been particularly targeted in recent months, but no organization is invulnerable. Darktrace detected a 20% year-on-year increase in ransomware incidents across its customer base over the course of 2020. Its Self-Learning AI technology has uncovered a number of infamous attack campaigns in customer environments, including Maze, WastedLocker, Sodinokibi, Eking, Dharma, and LockBit.

But it is not always the well-known attacks that are the most concerning. Zero-day attacks that have never been seen before in the wild clearly indicate the problem of the legacy approach. By definition, a system designed to identify future threats based on the hallmarks of previously encountered attacks is fundamentally incapable of catching novel threats or zero-day exploits.

Industrial Ransomware

Ransomware against industrial environments is on the rise, with a reported 500% increase since 2018. As cyber-physical systems and IT networks continue to converge, Darktrace has observed an increase in the number of cyber-attacks initially targeting IT before pivoting to OT. This was seen with the EKANS ransomware attack that included ICS protocols in its kill list, as well as the attack on the Colonial Pipeline in May 2021 that caused an immediate shut down of operations.

Multiple factors compound the risk ransomware poses to industrial environments. Since the outbreak of COVID-19, many organizations have relied upon remote management tools to allow operators to control ICS and OT environments without having to enter physical premises. Darktrace has already seen common remote management tools used in ransomware specifically targeting critical infrastructure.

More than 4,000 ransomware attacks happen daily

FBI

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

Threat Find: Darktrace Antigena Autonomously Neutralizes Zero-Day Ransomware

Darktrace Antigena, Darktrace's Autonomous Response technology, stopped a zero-day ransomware attack targeting an electronics manufacturer. The Self-Learning AI identified a device, 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, which generated a series of high-confidence alerts.

The device was observed making an unexpectedly large number of connections, writing multiple 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.

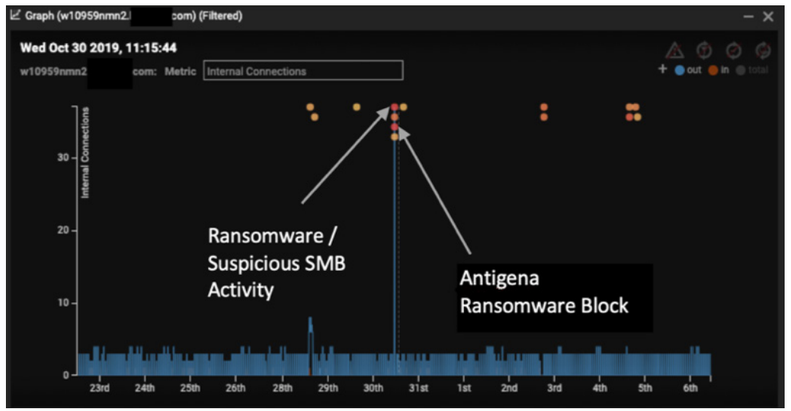


Figure 4: Four model breaches observed on October 30th and a dotted line representing Darktrace Antigena's actions

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, Darktrace 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 deny-listed command and 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 Self-Learning 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.

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

Threat Find: Ransomware Targets Electric Utilities Supplier

In an attack against a North American equipment supplier for electrical utilities this year, Darktrace's Industrial Immune System demonstrated its ability to protect critical infrastructure against double extortion ransomware.

The attacker leveraged 'living off the land' techniques to blend into the organization's normal business activity, using a compromised admin credential and a corporately approved remote management tool in attempts to remain undetected. This specific strain of ransomware successfully evaded detection by anti-virus tools by using a unique file extension when encrypting files.

These forms of signatureless ransomware easily slip past legacy approaches to security that rely on rules, signatures, threat feeds, 'knowledge packs', and lists of documented Common Vulnerabilities and Exposures (CVEs), and so can only detect previously documented threats.

But with real-time detections helping to facilitate an early response, Darktrace prevented the ransomware from spreading further on to the factory floor, minimizing operational disruption.

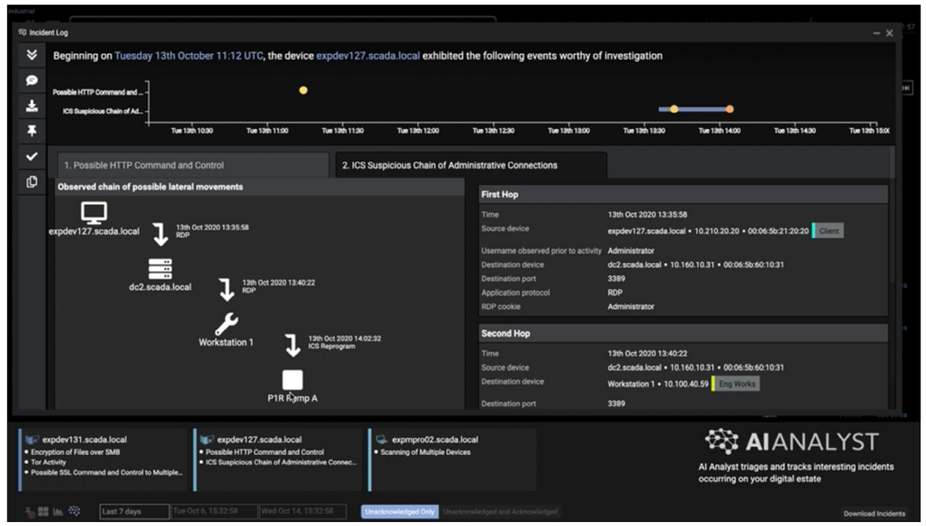


Figure 5: An example of Darktrace's Cyber AI Analyst detecting anomalous encryption and a suspicious chain of ICS administrative connections

Increasing Number of Novel Attacks

- A New Era of Threat
- Stealthy & Subtle APTs
- Rise of Ransomware
- Zero-Days
- Cloud-Based Attacks
- Emergence of Offensive AI
- Self-Learning AI Defense

Attackers understand the legacy approach of the cyber security tools they are trying to evade better than anyone. In response, they are updating their attack infrastructure (which may consist of email domains, IP addresses, strains of malware) and constantly innovating and experimenting with new techniques.

The resulting attacks, often referred to as 'unknown unknowns', lack any indicators of compromise collated in the deny lists used by traditional tools and are becoming increasingly common.

Conventional security tools that detect only known cyber-threats using rules and signatures are blind to new and evolving strains of malware for which such signatures do not exist.

"Anticipating and pre-empting every security risk is practically impossible in the face of 'unknown unknowns' and insider threat"

Information Services Manager, Lockyer Valley Regional Council

"The Enterprise Immune System identifies all kinds of novel threats, including polymorphic malware, stealthy insiders, and highly sophisticated social engineering attacks, without the need for rules or signatures"

IT Director and Data Protection Officer, OpinionWay

Threat Find: Hafnium Attack Detected by Self-Learning AI Three Months Before Signatures Made Available

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

In early December 2020, Self-Learning AI autonomously detected and investigated a sophisticated cyber-attack that targeted a customer's Exchange server. On March 2nd, 2021, Microsoft disclosed an ongoing campaign by the Hafnium threat actor group leveraging Exchange server zero-days.

Based on similarities in techniques, tools, and procedures (TTPs) observed, Darktrace assessed with high confidence that the attack in December was the work of the Hafnium group.

Darktrace observed no signs of compromise or change in behavior from the internet-facing Exchange server affected - no prior internal admin connections, no broadscale brute-force attempts, no account takeovers, and no malware copied to the server via internal channels – when it began to scan the internal network.

This sudden change in behavior on an administrative level points to a complete takeover of the Exchange server, rather than the compromise of a single Outlook Web Application account. To conduct a network scan from an Exchange server, a highly privileged, operating SYSTEM-level account is required.

Less than an hour after the internal network scan, the compromised Exchange server was observed writing further web shells to other Exchange servers via internal SMB. The file path and file name of the actual .aspx web shell bear very close resemblance to the Hafnium campaign details published by Microsoft and others in March 2021.

Over the period of one week, the Hafnium intrusion was in the top five incidents highlighted by Cyber AI Analyst. Even a small or resource-stretched security team, with only a few minutes available per week to review the highest-severity incidents, could have seen and inspected this threat.

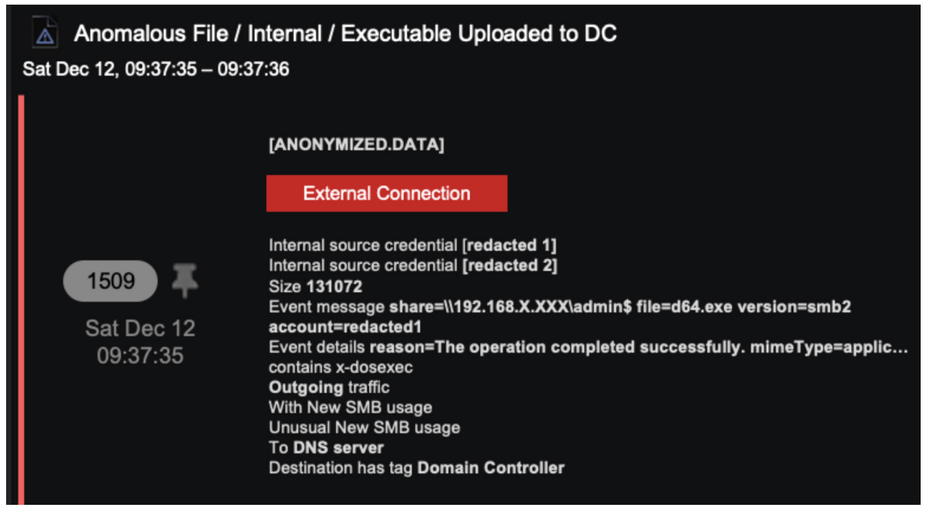


Figure 6: Darktrace alert on unusual activity

Cloud-Based Attacks Targeting The Dynamic Workforce

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

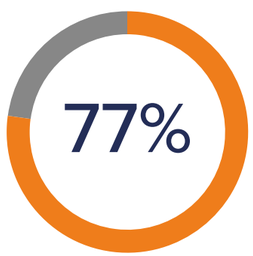
Emergence of Offensive AI

Self-Learning AI Defense

The sudden and widescale 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. The unprecedented speed and scale of these changes has further brought to the fore the inability of legacy solutions – hard-coded with set rules and playbooks based on previous attacks – to adapt to a new normal.

Unsurprisingly, cyber-criminals have been 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. In this climate, pandemic-related phishing emails and social engineering attacks have been common threat vectors.



of cyber security professionals view phishing as the most significant new threat vector concerning remote workers

Cybersecurity Insiders:
2021 Remote Working Risks

Supercharged Phishing Attacks

More than ever before, cyber-criminals are exploiting the latest news cycles and trends to lure recipients into engaging with phishing emails. This was particularly clear during the outbreak of the pandemic where Darktrace saw a surge in 'fearware' emails purporting to offer crucial information at a time of uncertainty.

As attackers continue to update their campaigns, leveraging new, topical subject lines and novel strains of malware, security tools trained to look for 'known bads' based on past attacks need to be constantly updated and fine-tuned, creating a burden for the IT teams they were designed to help.

Furthermore, as part of a wider trend in rising supply chain attacks over the past 12 months, Darktrace has seen an increasing number of Vendor Email Compromise attacks, which involves an account takeover of a trusted supplier or partner, followed by targeted, convincing emails being sent – often fraudulent invoices or malware hidden behind attachments disguised as RFPs or similar documents. Traditional security tools are powerless to stop such attacks: since the malicious emails come from trusted partners and suppliers, they slip through the gateway.

The industry has therefore seen an increasing demand for autonomous email security that uses AI to continually assess 'normal' for every email user and all the relationships between them in order to detect unusual, threatening activity, regardless of whether the attack has been seen before in the wild.

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

Targeting Identities, Not Devices: SaaS Account Takeover

The onset of the pandemic prompted an explosion in usage of SaaS applications such as 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 has 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 fed directly back to the attacker who can log in to the legitimate account and wreak havoc.

Darktrace frequently catches attackers masquerading as WeTransfer, Microsoft Teams, and ShareFile. In each case, these attacks slip through gateway tools but are detected by Self-Learning AI, which then prevents them from reaching the inbox.

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

Cybersecurity Insiders:
2020 Insider Threat Report

"Darktrace's self-learning AI has given me 100% visibility across the cloud, my SaaS providers, my Office 365 services, within my data center, and also on-premises"

Senior Security & Infrastructure Architect,
Retail (IT Central Station Peer Review)

IT Central Station
Unbiased reviews from the tech community

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

Threat Find: Vendor Email Compromise

At one of the world's largest beverage suppliers, which has a sprawling global supply chain and many trusted partners, Darktrace neutralized an inbound email attack after one of their third parties was compromised.

Shortly after some legitimate email communication, a wave of malicious emails were sent from their account to multiple contacts in the organization.

In the emails, there was a link directing the user to a legitimate file storage site ('canva.com') which was being used to host a malicious payload. This tactic is commonly used by cyber-criminals to bypass legacy security gateways because traditional gateways fail to defend against malicious file storage links using reputation checks, since the domains themselves are legitimate.

However, Self-Learning AI detected that this email did not belong and identified the email as 100% anomalous due to slight changes in the behavior of the sender when compared with their previous history.

The figure below shows three of the malicious emails and the scores assigned to them by Darktrace's machine learning. The top email is the supplier emailing the company legitimately, to warn of the compromised account. Despite arriving shortly after the malicious emails, the email was given only a 31% threat score, with no actions suggested. This proves just how valuable Self-Learning AI is, not only in stopping the bad emails but also in accurately identifying benign emails, ensuring it does not interfere with legitimate communication.

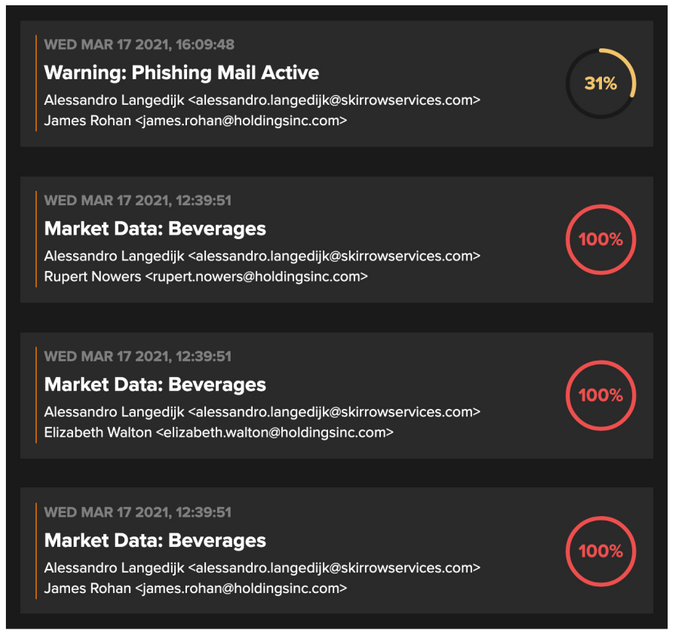


Figure 7: Darktrace clearly distinguishes the benign communication from harmful emails

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

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 Darktrace for 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]. As they came from legitimate and familiar accounts, these emails were all considered non-threatening by the gateway.

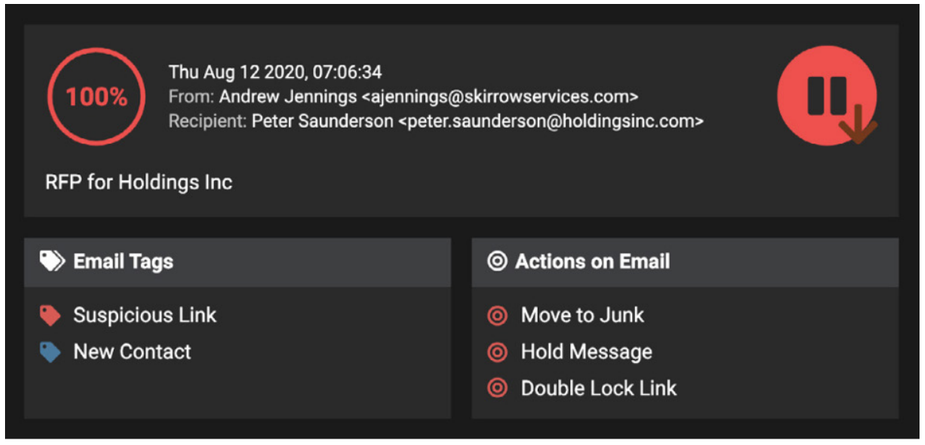


Figure 8: Darktrace monitors the offending email, with the hold icon indicating the action it would have taken in Active Mode. Identities have been anonymized

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 attacker for further account compromise.

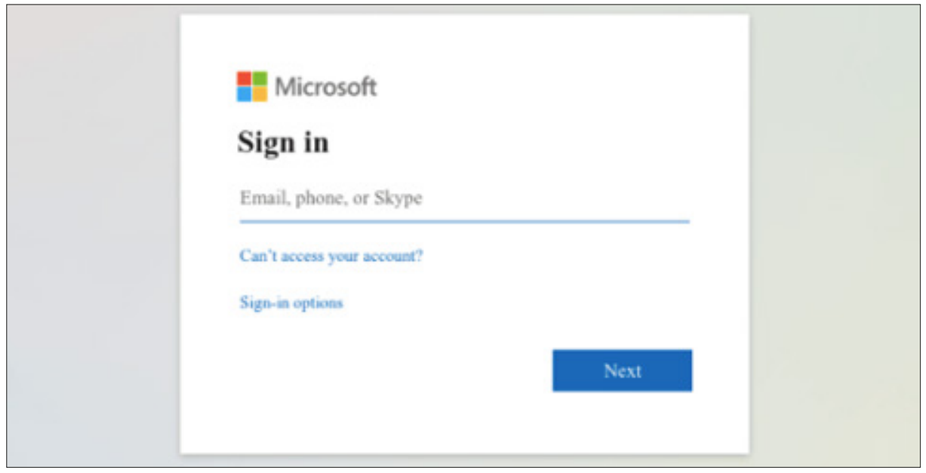


Figure 9: The fake Microsoft login page

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

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 anomalous sharing link being created for a password file.

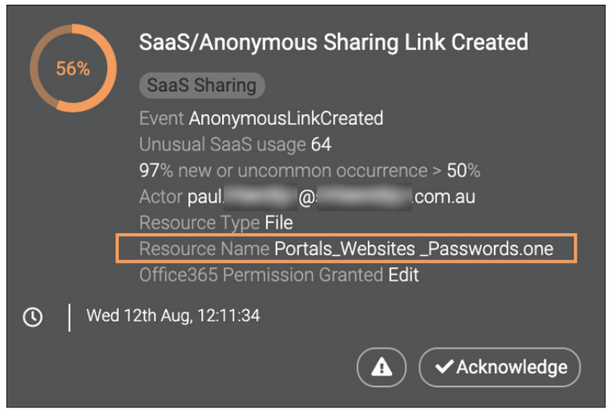


Figure 10: Darktrace reveals the anomalous creation of a link

Self-Learning 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 the sensitive information they could elicit from the email account, they sent out further malicious emails to trusted business associates using the same methodology of the initial compromise. Darktrace for SaaS identified this anomalous behavior, graphically revealing that the attacker sent out over 1,600 tailored emails over the course of 25 minutes.

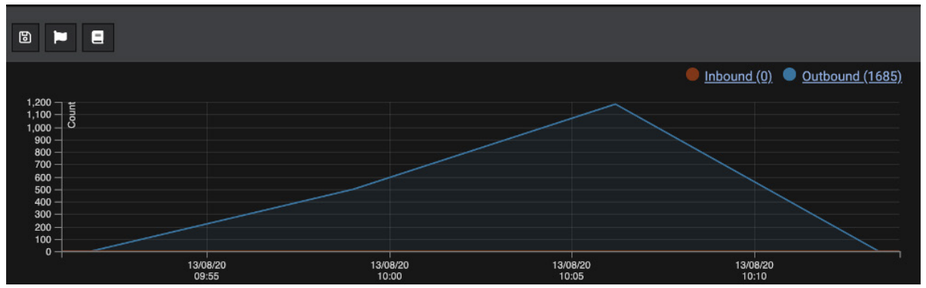


Figure 11: A graphical representation of the burst of emails sent over a 25-minute period

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 Emergence of Offensive AI

A New Era of Threat
Stealthy & Subtle APTs
Rise of Ransomware
Zero-Days
Cloud-Based Attacks
Emergence of Offensive AI
Self-Learning AI Defense

Attackers can leverage AI tools that exist today to make their cyber-attack campaigns more effective at every stage of the kill chain, from more personalized and sophisticated spear phishing, to faster moving ransomware. A recent survey by MIT Tech Review revealed that 97% of cyber security professionals are “concerned” or “very concerned” by AI-powered cyber-attacks, with 98% saying they have already made preparations for this eventuality.

AI will supercharge cyber-criminals on multiple fronts, creating stealthier, faster, and more effective attacks. A contextual understanding of its surroundings will allow malware to more effectively blend in to normal background activity, making post-intrusion detection even more difficult solely using traditional methods.

But in the face of defensive AI, the limitations of AI-powered cyber-attacks become exposed. With full visibility across the entire enterprise, defensive AI understands the entire digital environment of the organization and all its users. Offensive AI, on the other hand, is limited to specific intrusion points and only has visibility across the portion of the digital infrastructure that it has already compromised.

> It will be crucial to use AI as a force multiplier and keep pace with attacker enhancements as they upscale their attack capabilities and efforts
>
> Forrester, The Emergence of Offensive AI

> Offensive AI will enable cyber-criminals to direct targeted attacks at unprecedented speed and scale
>
> MIT Technology Review Insights, Preparing for AI-Enabled Cyberattacks 2021

Self-Learning AI: A Unique Approach

A New Era of Threat

Stealthy & Subtle APTs

Rise of Ransomware

Zero-Days

Cloud-Based Attacks

Emergence of Offensive AI

Self-Learning AI Defense

Darktrace's Self-Learning AI works by building an evolving understanding of your organization from scratch, allowing it to identify subtle outliers indicative of threat in real time.

Whereas other security tools rely on a priori assumptions, pre-programmed responses, or threat intelligence, Self-Learning AI learns the digital DNA of each unique organization, observing how users, devices, and applications typically behave and continuously revising this knowledge in light of new evidence.

Such a deep, granular understanding of what 'normal' looks like across the digital business enables Darktrace to detect subtle, previously unseen patterns and emerging threats that would otherwise go unnoticed.

Self-Learning AI then calculates the best action to take, in the shortest period of time, to effectively respond to the emerging threat, while allowing normal business operations to continue. This capability, called Autonomous Response, decides how to surgically react for itself to stop the in-progress attack - without the need for human input.

To buy back time for security teams, Self-Learning AI additionally carries out automated investigations that reduce time to triage by up to 92%. Combining expert analyst intuition with the speed and scalability of AI, this technology, called Cyber AI Analyst, connects the dots between disparate signs of attack before generating a high-level report about the nature and root cause of the wider security incident.

In today's new era of threat, the limitations of legacy tools are being thrown into the spotlight. The vast majority of serious incidents security teams face tend not to be pre-existing threat vectors but rather novel attacks that evade existing defenses or malicious insiders. To stay on top of the threat trends that follow, organizations need a dynamic security structure that can deal with novelty.

Self-Learning AI that adapts continuously and is able to learn the new normal helps organizations to stay ahead of attacks, protecting workforces and data at a critical time and building cyber resilience.

> "Using machine learning, Darktrace's unique Enterprise Immune System detects zero-day threats and suspicious insider behaviors, without having to define the activity in advance"
>
> CIO, City of Las Vegas

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 5,000 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.

Darktrace © Copyright 2021 Darktrace Holdings Limited. All rights reserved. Darktrace is a registered trademark of Darktrace Holdings Limited. Enterprise Immune System, and Threat Visualizer are unregistered trademarks of Darktrace Holdings Limited. Other trademarks included herein are the property of their respective owners.

For More Information

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