DARKTRACE

Five Cyber Threat Trends for 2022

with real-world case studies

Five Cyber Threat Trends for 2022

Contents

Trend 1: Technology Supply Chain Attacks 2

Log4Shell attack stopped by Autonomous Response

Trend 2: Account Takeovers 3

Business Email Compromise leads to fraudulent payment request

Trend 3: Out-of-Hours Attacks 4

Autonomous Response stops an REvil July 4th Attack

Trend 4: Lower Barrier to Entry for Cyber Criminals 5

AI neutralizes Hafnium copycat attacks

Trend 5: New Approaches to Ransomware 6

Autonomous Response Stops Advanced Ransomware

Autonomous Response 7

This report consolidates findings from Darktrace's worldwide Cyber Analyst team to present five overarching trends observed in the Darktrace Customer Community in 2021. Significant developments have been identified within each trend to help indicate what organizations should be looking out for in 2022 and beyond.

Key trends explored include the expansion of ransomware tactics beyond encryption, supply chain exploitation, cloud account takeovers and advanced phishing. In each case, a real-world case study highlights how threat actors are innovating to evade traditional security defenses, and shows how these attacks can be stopped by an AI technology which learns its surroundings to stop never-before-seen attacks.

Trend 1: Technology Supply Chain Attacks

Several major incidents in 2021 demonstrated the far-reaching consequences of supply chain attacks, with attackers exploiting vulnerabilities in Kaseya, GitLab and Log4Shell to gain backdoor access into thousands of organizations, including governments, corporations, and critical infrastructure.

The IT and communications sector was identified as the most targeted by cyber-attacks among Darktrace's customer base, with Darktrace's Autonomous Response stopping 150,000 attacks per week in this sector alone. As technology supply chains become more complex, we can expect attackers to continue to target these businesses.

Attackers can embed malicious software throughout supply chains through proprietary source code, developer repositories or open-source libraries. Because these infections are passed on through legitimate channels, such as a regular software updates, from trusted partners, traditional security tools struggle to identify them.

An effective response to supply chain attacks requires technology that can identify subtle deviations in activity that point to an emerging compromise, without relying on pre-defined rules and binary 'block' or 'allow' response mechanisms.

Real-World Case Study:

Log4Shell attack stopped by Autonomous Response

In December 2021, Darktrace's AI discovered an Internet-facing server that had been compromised via the Log4Shell vulnerability. The server connected to anomalous external IP for C2 and malware delivery, using HTTP over port 88 – which was highly unusual for that device, its peer group, and the organization as a whole.

The organization had implemented Darktrace's Autonomous Response technology, meaning the AI could take actions to respond to ongoing cyber-attacks. These responses can be delivered via a variety of mechanisms, including interactions with firewalls and other security tools, or native responses issued by Darktrace.

Antigena interacted with the organization's firewall in this case to block any connections to or from the malicious IP address – 164.52.212[.]196 – over port 88 for 2 hours with the option of escalating the block and duration if the attack appeared to persist.

Figure 1: Antigena responds, blocking connections to the malicious IP address.

This targeted response meant that the server could continue functioning as normal – but all the highly anomalous actions were interrupted in real time.

Trend 2: Account Takeovers

Attackers continue to capitalize on organizations' widespread adoption of cloud applications such as Microsoft Teams, SharePoint and Zoom.

Because data in these applications is hosted in third-party cloud environments, security teams struggle with reduced visibility in this area. Account credentials can be obtained via bruteforcing methods, phishing attacks, exchanges on the Dark Web, or by exploiting password reuse between personal and corporate accounts.

Once armed with the right credentials, attackers are easily able to access, manipulate, and exfiltrate the sensitive corporate data stored on platforms like SharePoint and OneDrive. Meanwhile, a compromised email account may serve as a springboard for further attacks, with threat actors sending malicious outbound messages to trusted colleagues, seeking to expand their foothold.

Real-World Case Study:

Business Email Compromise leads to fraudulent payment request

A convincing spear phishing attack targeted an employee at an academic institution, directing them to a fake Microsoft login page which captured their credentials. Their Microsoft 365 account was then compromised.

The attacker then logged into their account and sent out over 30 emails to the employee's colleagues, repeating the approach and hoping to gain new victims. They also sent a request to the accounts department to pay an overdue invoice for $78,000 – copying a legitimate invoice but changing the bank details. Darktrace's email and SaaS coverage provided a full overview of the attack, and in active mode, Autonomous Response would have intervened at every stage, holding back the original phishing attack and stopping the account takeover.

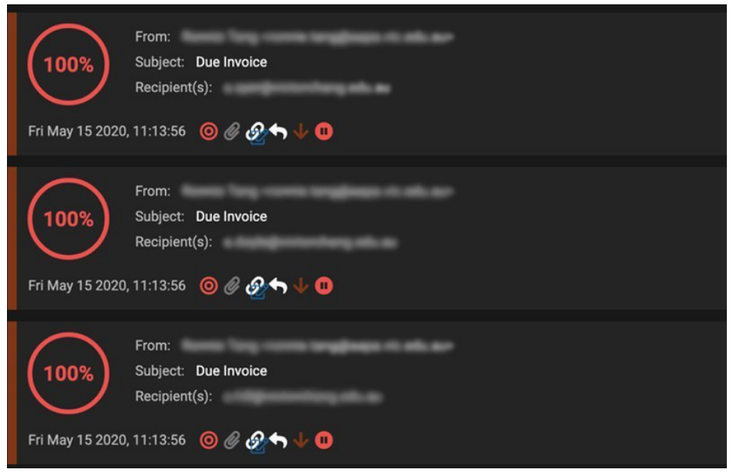

Figure 2: Antigena Email detects anomalous emails from the compromised account. The red hold icon indicates that these were held back from the recipient.

Trend 3: Out-of-Hours Attacks

Darktrace has observed an increase in attacks striking at nights, weekends and holidays, with 76% of ransomware attacks conducted outside of normal business hours.

Meanwhile, the period between initial intrusion and attack execution known as the 'dwell time' has continued to decline, giving security teams very little time to react to fast-moving attacks.

This has led the cyber security industry to turn to automated response solutions that contain cyber-attacks on behalf of human teams. But these automated response solutions can only take action based on prior human input, and can only block activity that has been pre-defined as 'bad'. The action they can take is usually a binary choice, either quarantining a device completely or not taking action at all – often resulting in heavy-handed responses and business disruption.

To keep up with the pace of attacker innovation, a fundamentally different approach is necessary, one that can learn what's normal for a business and enforce the 'pattern of life' of an infected device, contain only the threatening behavior while allowing regular business activity to continue.

Real-World Case Study:

Autonomous Response stops an REvil July 4th Attack

In 2021, as the US prepared for a holiday weekend ahead of July 4th, the ransomware group REvil leveraged a vulnerability in Kaseya software to attack over 1,500 companies. One of these was a company employing Darktrace's Autonomous Response. When a company laptop began to read files on an SMB server, Darktrace detected the behavior as unusual for this device, and Autonomous Response took action.

The ransomware began to take action at 11:08:32, shown by the 'SMB Delete Success' from the infected laptop to an SMB server. Autonomous Response kicked in a second later, quarantining the device for 24 hours given the severity of the attack. The laptop attempted to connect to other internal devices via SMB to continue the encryption activity, but Autonomous Response was able to block it using integrations with native security controls.

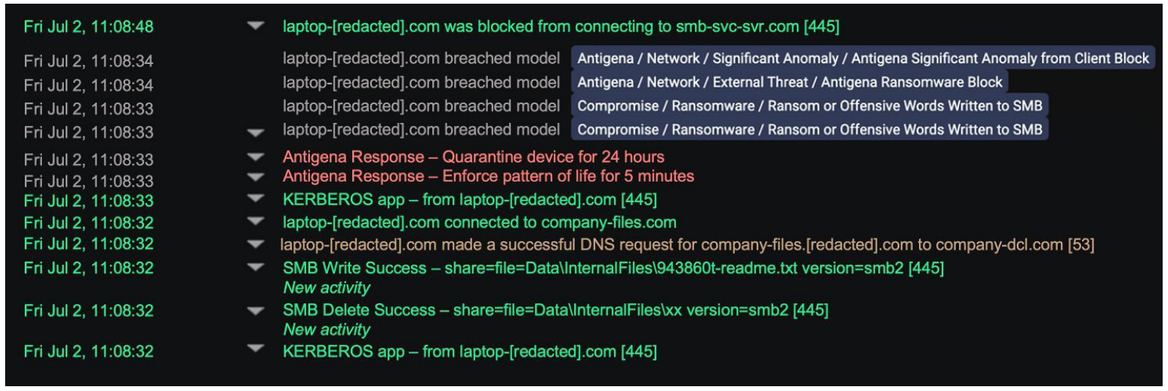

Figure 3: Darktrace detects encryption from the infected device and takes action with Autonomous Response.

Trend 4: Lower Barrier to Entry for Cyber Criminals

The barrier to entry for cyber-crime is at an all-time low. There are now numerous tutorials, affiliate schemes, and Ransomware as a Service (RaaS) models that allow unskilled attackers to access and deploy sophisticated tools and methods. Inexperienced actors can rent ready-to-go software from the Dark Web or obtain it through open-source applications such as Mimikatz and C2 frameworks like Empire, and it only takes a few adjustments to a pre-made malware strain to render it into an effective novel attack.

This will likely translate to a much greater frequency of advanced attacks being launched from a wider base of attackers. Attempts to tackle cyber-crime by targeting individual ransomware groups will become more futile, as complex RaaS ecosystems are developed. The most pernicious malware is no longer reserved for advanced threat actors, and novel threats will become more and more common.

Real-World Case Study:

AI neutralizes Hafnium copycat attacks

In 2021, the advanced cyber espionage group Hafnium used a ProxyLogon vulnerability to target Microsoft Exchange Servers. After being publicly disclosed, however, the vulnerability was rapidly exploited by numerous other threat actors. This new wave of attacks came from amateur attackers for whom Threat Intelligence did not yet exist, and so these 'copycat' intrusions regularly circumvented rule and signature-based security solutions.

For customers with Darktrace's Autonomous Response, however, unknown threat actors can be stopped. In one of the Hafnium-inspired attacks in March 2021, Autonomous Response detected an unusual PowerShell user agent performing potential C2 activity. The AI blocked all outgoing traffic to malicious external endpoints on the relevant ports within seconds of this activity beginning. The precision of this response meant that the threat was contained without disrupting the target organization.

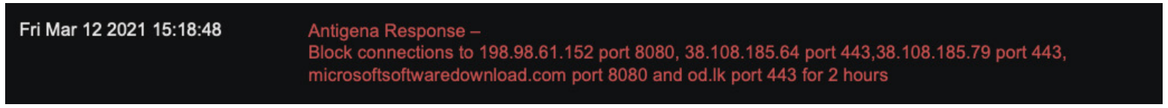

Figure 4: Autonomous Response takes action in one of Darktrace's customer environments, neutralizing a Hafnium copycat attack

Trend 5: New Approaches to Ransomware

Ransomware attacks expand beyond encryption

Data encryption is no longer the sole method of extortion relied on by ransomware attackers. Strategies including data exfiltration, backup encryption and deletion, corporate domain hijacking, and industrial system attacks can all be used to support ransom demands. With each new tool or tactic, these attacks become harder to anticipate and detect.

Smaller businesses make easier targets

Well-known ransomware groups like DarkSide and REvil shut down last year in the wake of high-profile attacks and increased attention from government and law-enforcement agencies. Now, attacks on small and mid-size businesses are rising, as attackers look to avoid gaining similar notoriety.

Small and midsize businesses, which may have limited in-house security expertise and budgets, will need to find smart solutions to combat ransomware, including the deployment of AI that can perform time-consuming tasks autonomously on behalf of security teams.

Fighting Ransomware with Autonomous Response

Ransomware is the top use case for Autonomous Response, which uses its knowledge of an organization's digital environment to spot anomalous activity and rapidly neutralize emerging threats. Autonomous Response interrupts ransomware at every stage of an attack, from the initial intrusion to C2, lateral movement, data exfiltration and encryption. Precise, proportionate actions ensure that attacks are stopped without disrupting the business.

Real-World Case Study:

Autonomous Response Stops Advanced Ransomware

Darktrace was deployed in a pre-infected public sector organization, where it soon detected malicious lateral movement indicative of a Trickbot attack. The malware spread to 280 devices, 160 of which began to download disguised executable files likely containing Ryuk ransomware. Autonomous Response was initially being trialed in active mode, but at this stage, the organization switched it to autonomous mode to help contain the attack.

The AI took action on several compromised devices, blocking anomalous connections to contain the threat, in each case enforcing the normal 'pattern of life' to ensure that the company's work continued uninterrupted. With their C2 communications severed, the attackers were unable to execute Ryuk ransomware and the attack came to an end. This last-minute activation of Autonomous Response likely avoided widespread data exfiltration and encryption.

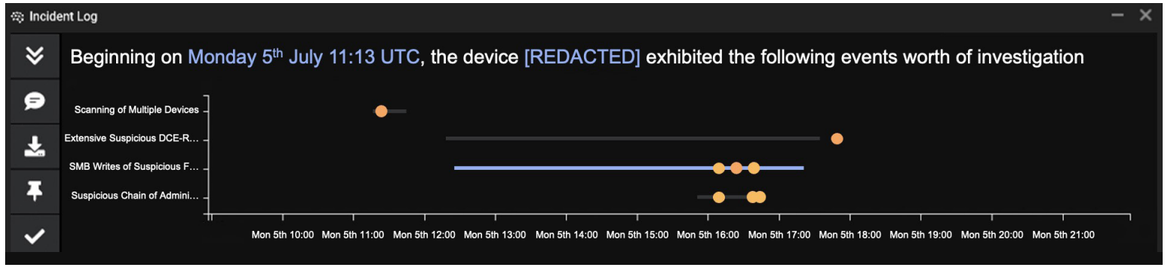

Figure 5: Cyber AI Analyst identifies a device attempting to spread a malicious payload using SMBv1

Autonomous Response

Darktrace's Autonomous Response capability, powered by Self-Learning AI, transforms an organization's ability to defend itself against the full range of cyber-threats, from fast-moving ransomware to stealthy supply chain infections, and beyond. Irrespective of the threat type, Darktrace AI can stitch together anomalous activity that points to an emerging attack, and initiate a timely and targeted response.

Traditional, signature-based security tools rely on historical attack data to predict future threats, but the speed of attacker innovation today has rendered this approach ineffective. Darktrace's Self-Learning AI takes a different approach, learning its unique digital surroundings from the ground up, without any preconceptions about what constitutes a threat. It learns the normal 'pattern of life' of every user and device, and can then spot and stop emerging attacks regardless of whether they have been seen before.

This allows Autonomous Response to contain threats in a targeted and proportionate manner, rather than issuing blanket, pre-programmed responses that risk disrupting business. This technology protects all areas of the digital estate, from cloud and email environments to IoT and endpoints, as well as IT and OT networks.

Organizations in every sector rely on Darktrace to contain the most sophisticated attacks they face each day, and trust its AI to keep them protected them against whatever novel threats the next year will bring.

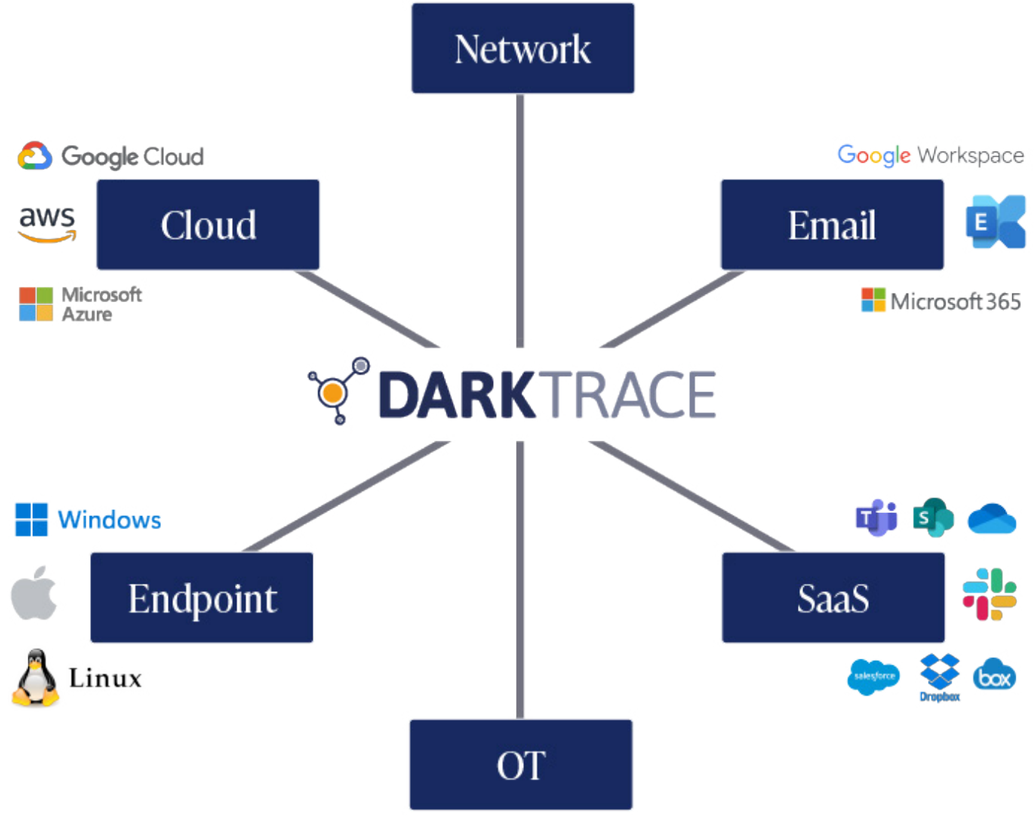

Figure 6: Defends across the enterprise: Autonomous Response can take action across every corner of the digital estate

About Darktrace

Darktrace (DARK:L), a global leader in cyber security AI, delivers world-class technology that protects over 6,500 customers worldwide from advanced threats, including ransomware and cloud and SaaS attacks. Darktrace's fundamentally different approach applies Self-Learning AI to enable machines to understand the business in order to autonomously defend it. Headquartered in Cambridge, UK, the company has 1,700 employees and over 30 offices worldwide. Darktrace was named one of TIME magazine's 'Most Influential Companies' for 2021.

Darktrace © Copyright 2022 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