

Disarming the WarmCookie Backdoor: Darktrace's Oven-Ready Solution

 darktrace.com/blog/disarming-the-warmcookie-backdoor-darktraces-oven-ready-solution

26

Jul 2024

WarmCookie is a backdoor malware strain that allows threat actors to gather sensitive system information, facilitating further cyber attacks against their targets. Between April and June 2024, Darktrace's Threat Research team investigated instances of WarmCookie on multiple customer networks, read on to learn more about their findings and the tactics used by this threat.

What is WarmCookie malware?

WarmCookie, also known as BadSpace [2], is a two-stage backdoor tool that provides functionality for threat actors to retrieve victim information and launch additional payloads. The malware is primarily distributed via phishing campaigns according to multiple open-source intelligence (OSINT) providers.

Backdoor malware: A backdoor tool is a piece of software used by attackers to gain and maintain unauthorized access to a system. It bypasses standard authentication and security mechanisms, allowing the attacker to control the system remotely.

Two-stage backdoor malware: This means the backdoor operates in two distinct phases:

1. Initial Stage: The first stage involves the initial infection and establishment of a foothold within the victim's system. This stage is often designed to be small and stealthy to avoid detection.

2. Secondary Stage: Once the initial stage has successfully compromised the system, it retrieves or activates the second stage payload. This stage provides more advanced functionalities for the attacker, such as extensive data exfiltration, deeper system control, or the deployment of additional malicious payloads.

How does WarmCookie malware work?

Reported attack patterns include emails attempting to impersonate recruitment firms such as PageGroup, Michael Page, and Hays. These emails likely represented social engineering tactics, with attackers attempting to manipulate jobseekers into engaging with the emails and following malicious links embedded within [3].

This backdoor tool also adopts stealth and evasion tactics to avoid the detection of traditional security tools. Reported evasion tactics included custom string decryption algorithms, as well as dynamic API loading to prevent researchers from analyzing and identifying the core functionalities of WarmCookie [1].

Before this backdoor makes an outbound network request, it is known to capture details from the target machine, which can be used for fingerprinting and identification [1], this includes:

- Computer name
- Username
- DNS domain of the machine
- Volume serial number

WarmCookie samples investigated by external researchers were observed communicating over HTTP to a hardcoded IP address using a combination of RC4 and Base64 to protect its network traffic [1]. Ultimately, threat actors could use this backdoor to deploy further malicious payloads on targeted networks, such as ransomware.

Darktrace Coverage of WarmCookie

Between April and June 2024, Darktrace's Threat Research team investigated suspicious activity across multiple customer networks indicating that threat actors were utilizing the WarmCookie backdoor tool. Observed cases across customer environments all included the download of unusual executable (.exe) files and suspicious outbound connectivity.

Affected devices were all observed making external HTTP requests to the German-based external IP, 185.49.69[.]41, and the URI, /data/2849d40ade47af8edfd4e08352dd2cc8.

The first investigated instance occurred between April 23 and April 24, when Darktrace detected a series of unusual file download and outbound connectivity on a customer network, indicating successful WarmCookie exploitation. As mentioned by Elastic labs, "The PowerShell script abuses the Background Intelligent Transfer Service (BITS) to download WarmCookie and run the DLL with the Start export" [1].

Less than a minute later, the same device was observed making HTTP requests to the rare external IP address: 185.49.69[.]41, which had never previously been observed on the network, for the URI /data/b834116823f01aeceed215e592dfcba7. The device then proceeded to download masqueraded executable file from this endpoint. Darktrace recognized that these connections to an unknown endpoint, coupled with the download of a masqueraded file, likely represented malicious activity.

Following this download, the device began beaconing back to the same IP, 185.49.69[.]41, with a large number of external connections observed over port 80. This beaconing related behavior could further indicate malicious software communicating with command-and-control (C2) servers.

Darktrace's model alert coverage included the following details:

[Model Alert: Device / Unusual BITS Activity]

- Associated device type: desktop
- Time of alert: 2024-04-23T14:10:23 UTC
- ASN: AS28753 Leaseweb Deutschland GmbH
- User agent: Microsoft BITS/7.8

[Model Alert: Anomalous File / EXE from Rare External Location]

[Model Alert: Anomalous File / Masqueraded File Transfer]

- Associated device type: desktop
- Time of alert: 2024-04-23T14:11:18 UTC
- Destination IP: 185.49.69[.]41
- Destination port: 80
- Protocol: TCP
- Application protocol: HTTP
- ASN: AS28753 Leaseweb Deutschland GmbH
- User agent: Mozilla / 4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705)
- Event details: File: http[:]//185.49.69[.]41/data/b834116823f01aeceed215e592dfcba7, total seen size: 144384B, direction: Incoming
- SHA1 file hash: 4ddf0d9c750bfeaebdacc14152319e21305443ff
- MD5 file hash: b09beb0b584deee198ecd66976e96237

[Model Alert: Compromise / Beaconing Activity To External Rare]

- Associated device type: desktop

- Time of alert: 2024-04-23T14:15:24 UTC
- Destination IP: 185.49.69[.]41
- Destination port: 80
- Protocol: TCP
- Application protocol: HTTP
- ASN: AS28753 Leaseweb Deutschland GmbH
- User agent: Mozilla / 4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;.NET CLR 1.0.3705)

Between May 7 and June 4, Darktrace identified a wide range of suspicious external connectivity on another customer's environment. Darktrace's Threat Research team further investigated this activity and assessed it was likely indicative of WarmCookie exploitation on customer devices.

Similar to the initial use case, BITS activity was observed on affected devices, which is utilized to download WarmCookie [1]. This initial behavior was observed with the device after triggering the model: Device / Unusual BITS Activity on May 7.

Just moments later, the same device was observed making HTTP requests to the aforementioned German IP address, 185.49.69[.]41 using the same URI /data/2849d40ade47af8edfd4e08352dd2cc8, before downloading a suspicious executable file.

Just like the first use case, this device followed up this suspicious download with a series of beaconing connections to 185.49.69[.]41, again with a large number of connections via port 80.

Similar outgoing connections to 185.49.69[.]41 and model alerts were observed on additional devices during the same timeframe, indicating that numerous customer devices had been compromised.

Darktrace's model alert coverage included the following details:

[Model Alert: Device / Unusual BITS Activity]

- Associated device type: desktop
- Time of alert: 2024-05-07T09:03:23 UTC
- ASN: AS28753 Leaseweb Deutschland GmbH

- User agent: Microsoft BITS/7.8

[Model Alert: Anomalous File / EXE from Rare External Location]

[Model Alert: Anomalous File / Masqueraded File Transfer]

- Associated device type: desktop

- Time of alert: 2024-05-07T09:03:35 UTC

- Destination IP: 185.49.69[.]41

- Protocol: TCP

- ASN: AS28753 Leaseweb Deutschland GmbH

- Event details: File: [http://185.49.69\[.\]41/data/2849d40ade47af8edfd4e08352dd2cc8](http://185.49.69[.]41/data/2849d40ade47af8edfd4e08352dd2cc8), total seen size: 72704B, direction: Incoming

- SHA1 file hash: 5b0a35c574ee40c4bccb9b0b942f9a9084216816

- MD5 file hash: aa9a73083184e1309431b3c7a3e44427

[Model Alert: Anomalous Connection / New User Agent to IP Without Hostname]

- Associated device type: desktop

- Time of alert: 2024-05-07T09:04:14 UTC

- Destination IP: 185.49.69[.]41

- Application protocol: HTTP

- URI: /data/2849d40ade47af8edfd4e08352dd2cc8

- User agent: Microsoft BITS/7.8

[Model Alert: Compromise / HTTP Beaconing to New Endpoint]

- Associated device type: desktop

- Time of alert: 2024-05-07T09:08:47 UTC

- Destination IP: 185.49.69[.]41

- Protocol: TCP

- Application protocol: HTTP

- ASN: AS28753 Leaseweb Deutschland GmbH
- URI: /
- User agent: Mozilla / 4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;.NET CLR 1.0.3705) \

SUSPICIOUS APPLICATION	
User Agent	Mozilla / 4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;.NET CLR 1.0.3705)
SUSPICIOUS ENDPOINTS CONTACTED BY APPLICATION	
Time	7th May 2024 09:04:04 - 09:09:24 UTC
Hostname	185.49.69.41 ⓘ
Hostname Rarity	100%
Hostname First Observed	7th May 2024 09:03:09 UTC
Most Recent Destination IP	185.49.69.41 ⓘ
Most Recent ASN	AS28753 Leaseweb Deutschland GmbH
ASN	AS28753 Leaseweb Deutschland GmbH
Total Connections	68
URI	/
Port	80
HTTP Methods	GET, POST
Status Codes	200, 400

Figure 1: Cyber AI Analyst Coverage Details around the external destination, '185.49.69[.]41'.

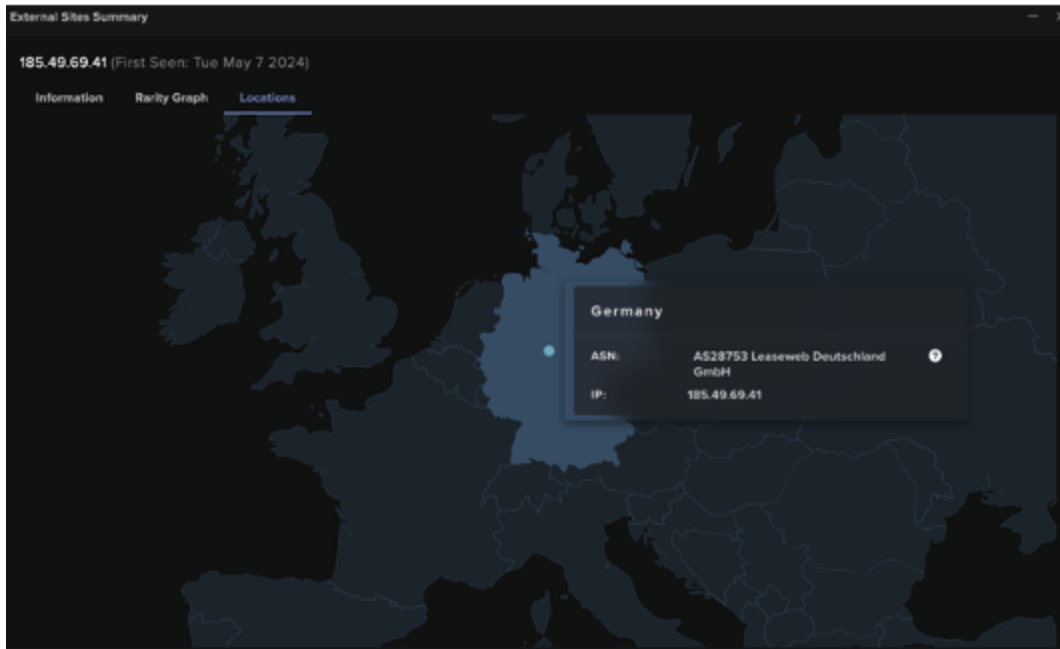


Figure 2: External Sites Summary verifying the geographical location of the external IP, 185.49.69[.]41'.

Fortunately, this particular customer was subscribed to Darktrace's Proactive Threat Notification (PTN) service and the Darktrace Security Operation Center (SOC) promptly investigated the activity and alerted the customer. This allowed their security team to address the activity and begin their own remediation process.

In this instance, Darktrace's Autonomous Response capability was configured in Human Confirmation mode, meaning any mitigative actions required manual application by the customer's security team.

Despite this, Darktrace recommended two actions to contain the activity: blocking connections to the suspicious IP address 185.49.69[.]41 and any IP addresses ending with '69[.]41', as well as the 'Enforce Pattern of Life' action. By enforcing a pattern of life, Darktrace can restrict a device (or devices) to its learned behavior, allowing it to continue regular business activities uninterrupted while blocking any deviations from expected activity.

Network Actions									
Platform Actions									
Settings									
Clear Pending Actions Clear Active Actions									
Pending Actions Active Actions Cleared Actions Expired Actions									
Device	IP	Action	History	Start / Expiration	Type	Model	Actions	Current Status	
	No IP	Block connections to 185.49.69.41 and *.69.41	View History	Tue May 7 2024, 09:04:02 +00:00 Fri May 10 2024, 11:04:02 +00:00	Network	Antigena / Network / Significant Anomaly / Antigena Enhanced Monitoring from Client Block	Reactivate Copy MDR data	No Message	
	No IP	Enforce pattern of life	View History	Tue May 7 2024, 13:13:38 +00:00 Tue May 7 2024, 13:41:38 +00:00	Network	Antigena / Network / Significant Anomaly / Antigena Significant Anomaly from Client Block	Reactivate Copy MDR data	No Message	

Figure 3: Actions suggested by Darktrace to contain the emerging activity, including blocking connections to the suspicious endpoint and restricting the device to its 'pattern of life'.

Conclusion

Backdoor tools like WarmCookie enable threat actors to gather and leverage information from target systems to deploy additional malicious payloads, escalating their cyber attacks. Given that WarmCookie's primary distribution method seems to be through phishing campaigns masquerading as trusted recruitments firms, it has the potential to affect a large number of organizations.

In the face of such threats, Darktrace's behavioral analysis provides organizations with full visibility over anomalous activity on their digital estates, regardless of whether the threat bypasses by human security teams or email security tools. While threat actors seemingly managed to evade customers' native email security and gain access to their networks in these cases, Darktrace identified the suspicious behavior associated with WarmCookie and swiftly notified customer security teams.

Had Darktrace's Autonomous Response capability been fully enabled in these cases, it could have blocked any suspicious connections and subsequent activity in real-time, without the need of human intervention, effectively containing the attacks in the first instance.

Credit to Justin Torres, Cyber Security Analyst and Dylan Hinz, Senior Cyber Security Analyst

Appendices

Darktrace Model Detections

- Anomalous File / EXE from Rare External Location
- Anomalous File / Masqueraded File Transfer
- Compromise / Beacon to Young Endpoint
- Compromise / Beaconsing Activity To External Rare
- Compromise / HTTP Beaconsing to New Endpoint
- Compromise / HTTP Beaconsing to Rare Destination
- Compromise / High Volume of Connections with Beacon Score
- Compromise / Large Number of Suspicious Successful Connections
- Compromise / Quick and Regular Windows HTTP Beaconsing
- Compromise / SSL or HTTP Beacon
- Compromise / Slow Beaconsing Activity To External Rare

- Compromise / Sustained SSL or HTTP Increase
- Compromise / Sustained TCP Beacons Activity To Rare Endpoint
- Anomalous Connection / Multiple Failed Connections to Rare Endpoint
- Anomalous Connection / New User Agent to IP Without Hostname
- Compromise / Sustained SSL or HTTP Increase

AI Analyst Incident Coverage:

- Unusual Repeated Connections
- Possible SSL Command and Control to Multiple Endpoints
- Possible HTTP Command and Control
- Suspicious File Download

Darktrace RESPOND Model Detections:

- Antigena / Network / External Threat / Antigena Suspicious File Block
- Antigena / Network / External Threat / Antigena Suspicious File Pattern of Life Block

List of IoCs

IoC - Type - Description + Confidence

185.49.69[.]41 – IP Address – WarmCookie C2 Endpoint

/data/2849d40ade47af8edfd4e08352dd2cc8 – URI – Likely WarmCookie URI

/data/b834116823f01aeceed215e592dfcba7 – URI – Likely WarmCookie URI

4ddf0d9c750bfeaebdacc14152319e21305443ff - SHA1 Hash – Possible Malicious File

5b0a35c574ee40c4bccb9b0b942f9a9084216816 - SHA1 Hash – Possible Malicious File

MITRE ATT&CK Mapping

(Technique Name) – (Tactic) – (ID) – (Sub-Technique of)

Drive-by Compromise - INITIAL ACCESS - T1189

Ingress Tool Transfer - COMMAND AND CONTROL - T1105

Malware - RESOURCE DEVELOPMENT - T1588.001 - T1588

Lateral Tool Transfer - LATERAL MOVEMENT - T1570

Web Protocols - COMMAND AND CONTROL - T1071.001 - T1071

Web Services - RESOURCE DEVELOPMENT - T1583.006 - T1583

Browser Extensions - PERSISTENCE - T1176

Application Layer Protocol - COMMAND AND CONTROL - T1071

Fallback Channels - COMMAND AND CONTROL - T1008

Multi-Stage Channels - COMMAND AND CONTROL - T1104

Non-Standard Port - COMMAND AND CONTROL - T1571

One-Way Communication - COMMAND AND CONTROL - T1102.003 - T1102

Encrypted Channel - COMMAND AND CONTROL - T1573

External Proxy - COMMAND AND CONTROL - T1090.002 - T1090

Non-Application Layer Protocol - COMMAND AND CONTROL - T1095

References

[1] <https://www.elastic.co/security-labs/dipping-into-danger>

[2] <https://www.gdatasoftware.com/blog/2024/06/37947-badspace-backdoor>

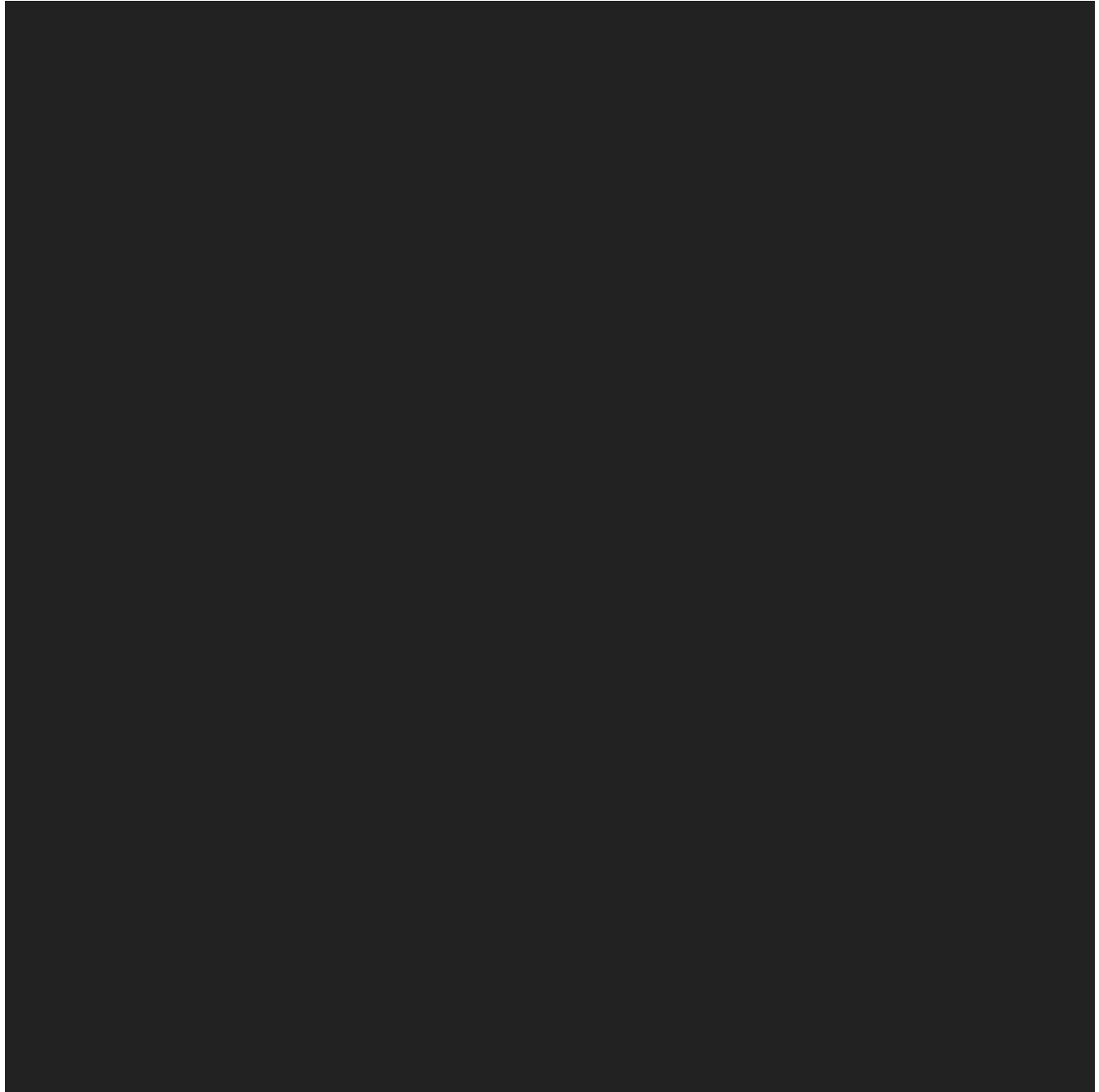
[3] <https://thehackernews.com/2024/06/new-phishing-campaign-deploys.html>

Like this and want more?

Receive the latest blog in your inbox

Thank you! Your submission has been received!

Oops! Something went wrong while submitting the form.



Newsletter

Stay ahead of threats with the Darktrace blog newsletter

Get the latest insights from the cybersecurity landscape, including threat trends, incident analysis, and the latest Darktrace product developments – delivered directly to your inbox, monthly.

Darktrace is committed to protecting and respecting your privacy, and we'll only use your personal information to administer your account and to provide the products and services you requested from us. From time to time, we would like to contact you about our products

and services, as well as other content that may be of interest to you. If you consent to us contacting you for this purpose, please tick below to say how you would like us to contact you:

By clicking submit below, you consent to allow Darktrace to store and process the personal information submitted above to provide you the content requested.

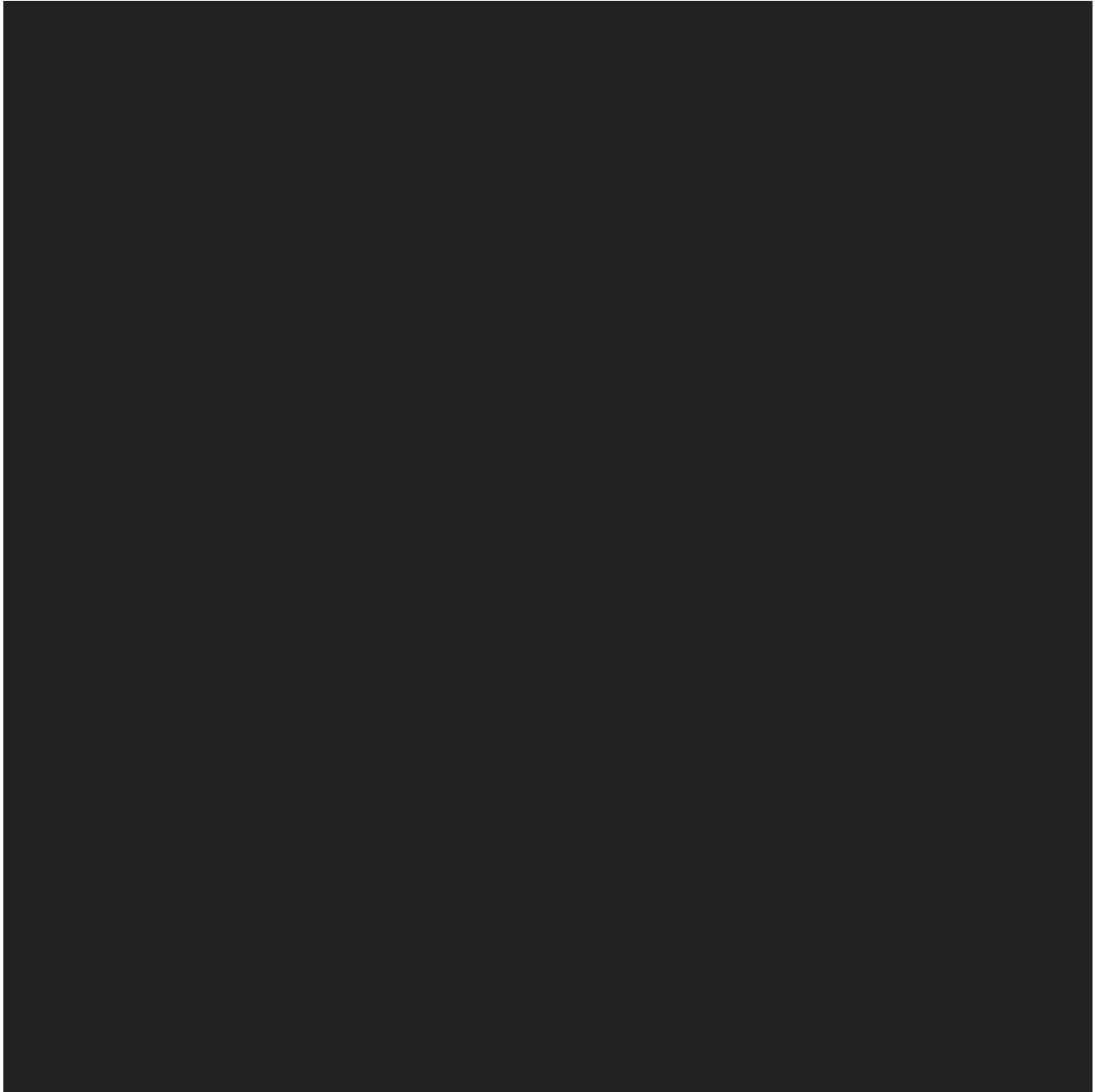
Thanks, your request has been received

A member of our team will be in touch with you shortly.

Oops! Something went wrong while submitting the form.

More in this series

No items found.



Blog

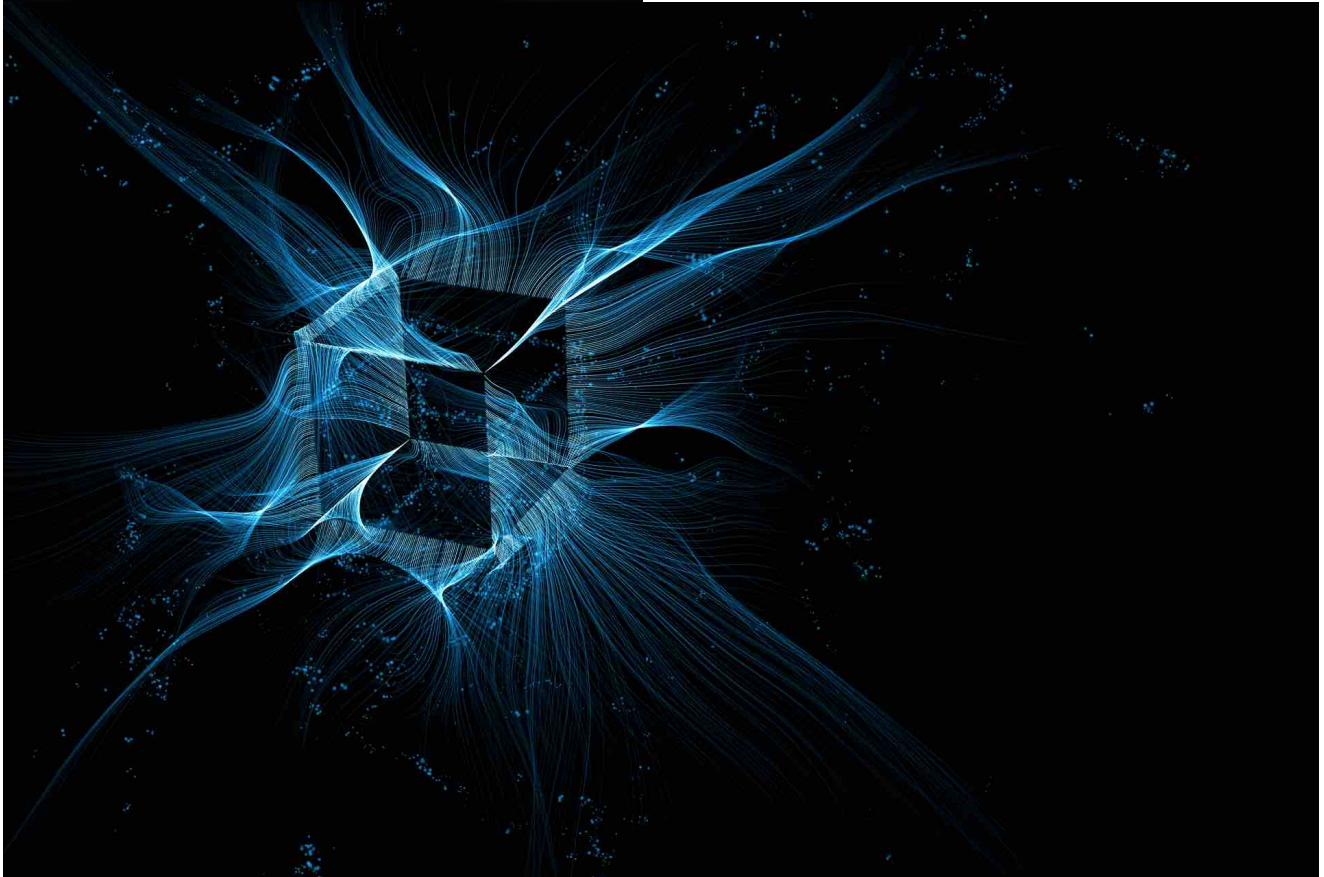
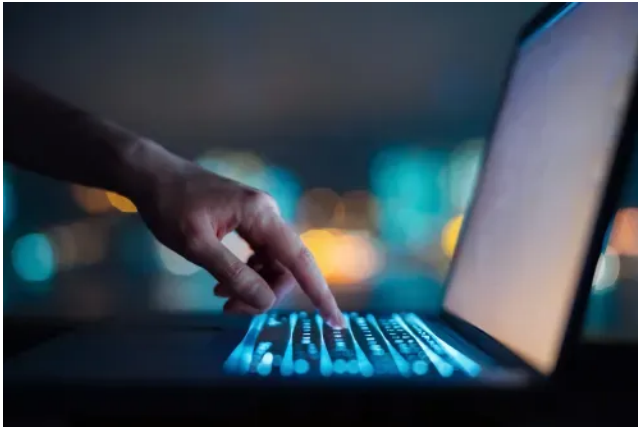
/

January 2, 2025

/

Inside the SOC

A Snake in the Net: Defending Against AiTM Phishing Threats and Mamba 2FA





What are Adversary-in-the-Middle (AiTM) phishing kits?

Phishing-as-a-Service (PhaaS) platforms have significantly lowered the barriers to entry for cybercriminals, enabling a new wave of sophisticated phishing attacks. Among the most concerning developments in this landscape is the emergence of **Adversary-in-the-Middle (AiTM) phishing kits**, which enhance traditional phishing tactics by allowing attackers to intercept and manipulate communications in real-time. The PhaaS marketplace offers a wide variety of innovative capabilities, with basic services starting around USD 120 and more advanced services costing around USD 250 monthly [1].

These AiTM kits are designed to create convincing decoy pages that mimic legitimate login interfaces, often pre-filling user information to increase credibility. By acting as a man-in-the-middle, attackers can harvest sensitive data such as usernames, passwords, and even multi-factor authentication (MFA) tokens without raising immediate suspicion. This capability not only makes AiTM attacks more effective but also poses a significant challenge for cybersecurity defenses [2].

Mamba 2FA is one such example of a PhaaS strain with AiTM capabilities that has emerged as a significant threat to users of Microsoft 365 and other enterprise systems. Discovered in May 2024, Mamba 2FA employs advanced AiTM tactics to bypass MFA, making it particularly dangerous for organizations relying on these security measures.

What is Mamba 2FA?

Phishing Mechanism

Mamba 2FA employs highly convincing phishing pages that closely mimic legitimate Microsoft services like OneDrive and SharePoint. These phishing URLs are crafted with a specific structure, incorporating Base64-encoded parameters. This technique allows attackers to tailor the phishing experience to the targeted organization, making the deception more effective. If an invalid parameter is detected, users are redirected to a benign error page, which helps evade automated detection systems [5].

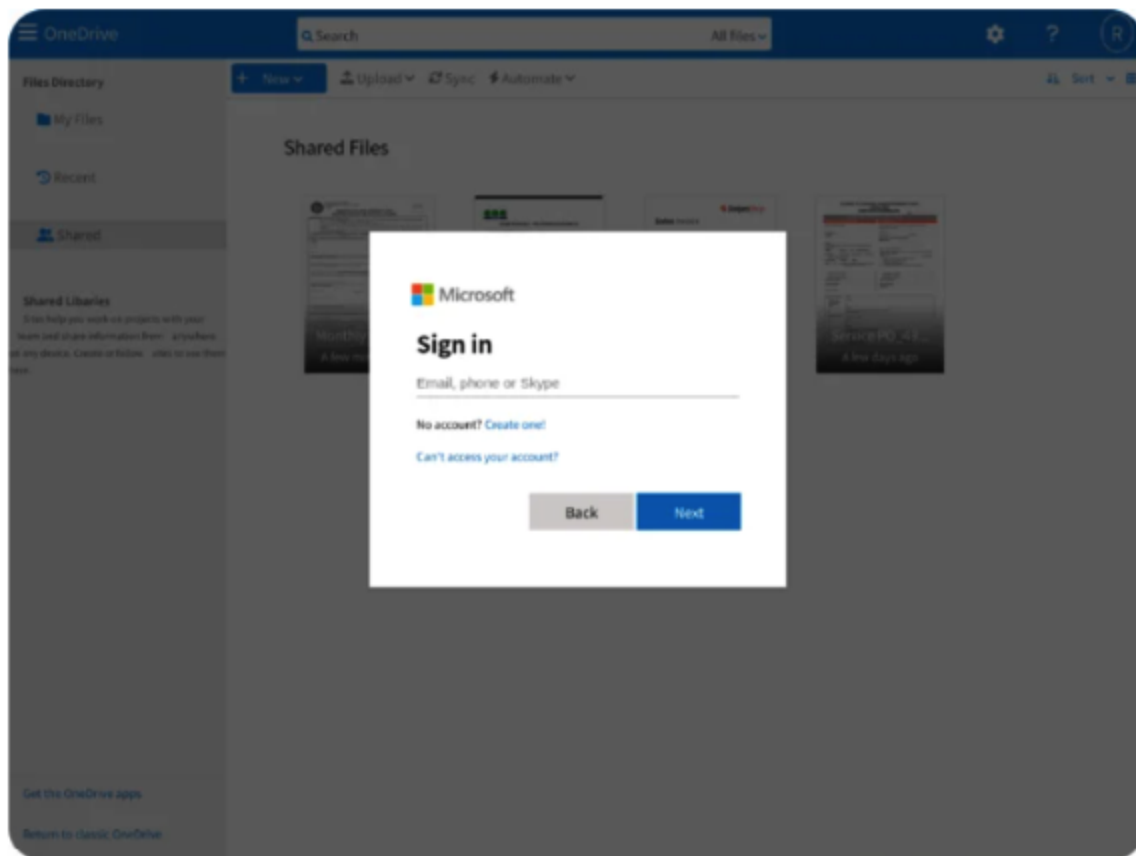


Figure 1: Phishing page mimicking the Microsoft OneDrive service.

Real-Time Communication

A standout feature of Mamba 2FA is its use of the Socket.IO JavaScript library. This library facilitates real-time communication between the phishing page and the attackers' backend servers. As users input sensitive information, such as usernames, passwords, and MFA tokens on the phishing site, this data is immediately relayed to the attackers, enabling swift unauthorized access [5].

Multi-Factor Authentication Bypass

Mamba 2FA specifically targets MFA methods that are not resistant to phishing, such as one-time passwords (OTPs) and push notifications. When a user enters their MFA token, it is captured in real-time by the attackers, who can then use it to access the victim's account immediately. This capability significantly undermines traditional security measures that rely on MFA for account protection.

Infrastructure and Distribution

The platform's infrastructure consists of two main components: link domains and relay servers. Link domains handle initial phishing attempts, while relay servers are responsible for stealing credentials and completing login processes on behalf of the attacker. The relay servers are designed to mask their IP addresses by using proxy services, making it more difficult for security systems to block them [3].

Evasion Techniques

To evade detection by security tools, Mamba 2FA employs several strategies:

- **Sandbox Detection:** The platform can detect if it is being analyzed in a sandbox environment and will redirect users to harmless pages like Google's 404 error page.
- **Dynamic URL Generation:** The URLs used in phishing attempts are frequently rotated and often short-lived to avoid being blacklisted by security solutions.
- **HTML Attachments:** Phishing emails often include HTML attachments that appear benign but contain hidden JavaScript that redirects users to the phishing page [5].

Darktrace's Coverage of Mamba 2FA

Starting in July 2024, the Darktrace Threat Research team detected a sudden rise in Microsoft 365 customer accounts logging in from unusual external sources. These accounts were accessed from an anomalous endpoint, **2607:5500:3000:fea[::]2**, and exhibited unusual behaviors upon logging into Software-as-a-Service (SaaS) accounts. This activity strongly correlates with a phishing campaign using **Mamba 2FA**, first documented in late June 2024 and tracked as Mamba 2FA by Sekoia [2][3].

Darktrace / IDENTITY was able to identify the initial stages of the Mamba 2FA campaign by correlating subtle anomalies, such as unusual SaaS login locations. Using AI based on peer group analysis, it detected unusual behavior associated with these attacks. By leveraging Autonomous Response actions, Darktrace was able to neutralize these threats in every instance of the campaign detected.

On July 23, a SaaS user was observed logging in from a rare ASN and IP address, 2607:5500:3000:fea::2, originating from the US and successfully passed through MFA authentication.

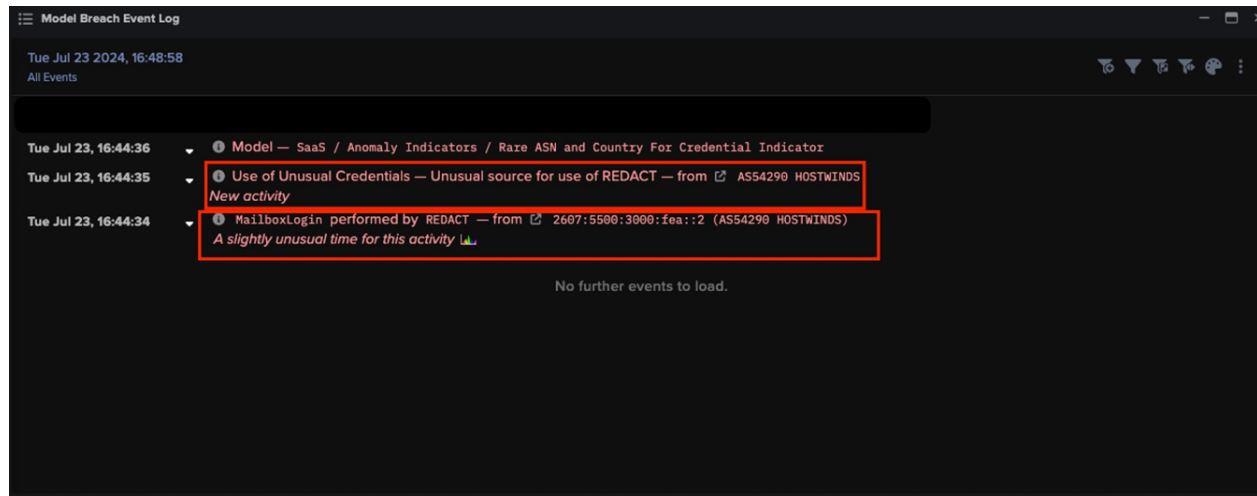


Figure 2: Model Alert Event Log showing Darktrace's detection of a SaaS user mailbox logging in from an unusual source it correlates with Mamba 2FA relay server.

Almost an hour later, the SaaS user was observed logging in from another suspicious IP address, 45.133.172[.]86, linked to ASN AS174 COGENT-174. This IP, originating from the UK, successfully passed through MFA validation.

Following this unusual access, the SaaS user was notably observed reading emails and files that could contain sensitive payment and contract information. This behavior suggests that the attacker may have been leveraging contextual information about the target to craft further malicious phishing emails or fraudulent invoices. Subsequently, the user was detected creating a new mailbox rule titled 'fdsdf'. This rule was configured to redirect emails from a specific domain to the 'Deleted Items' folder and automatically mark them as read.

Implications of Unusual Email Rules

Such unusual email rule configurations are a common tactic employed by attackers. They often use these rules to automatically forward emails containing sensitive keywords—such as "invoice", "payment", or "confidential"—to an external address. Additionally, these rules help conceal malicious activities, keeping them hidden from the target and allowing the attacker to operate undetected.

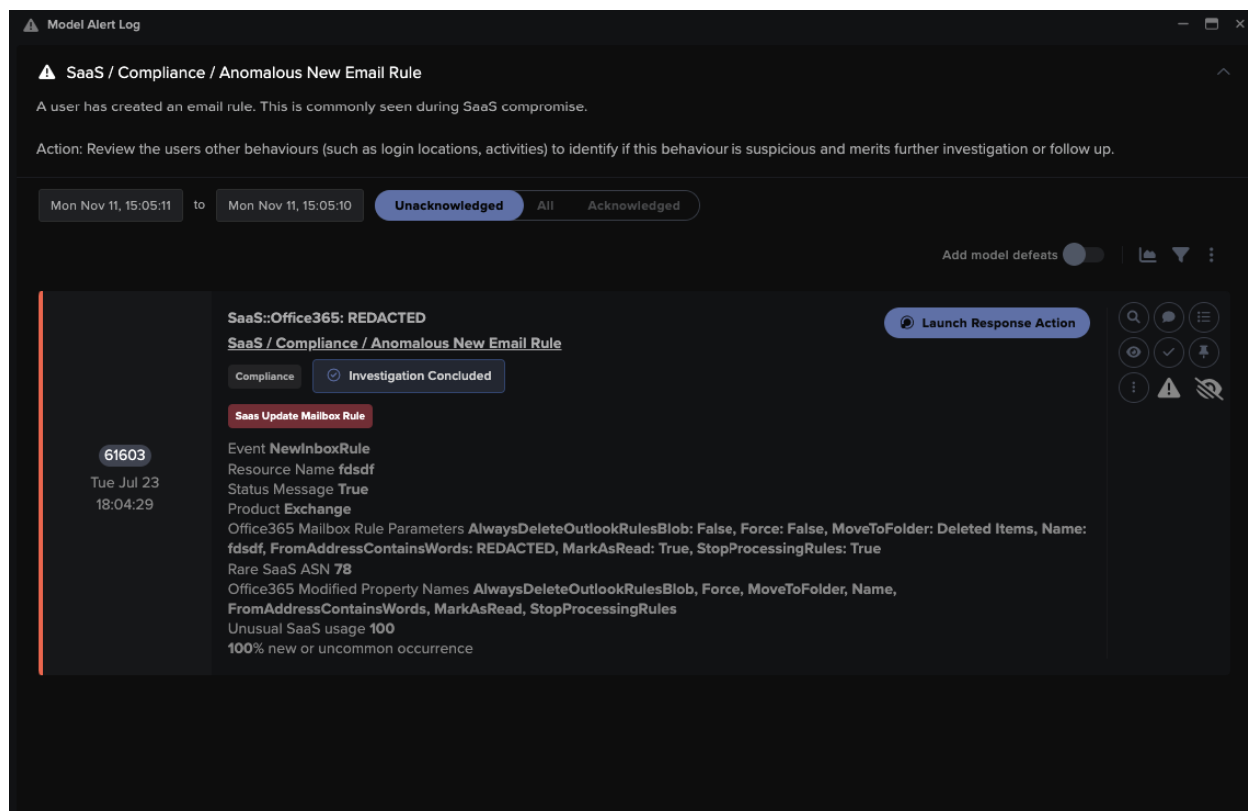


Figure 3: The model alert “SaaS / Compliance / Anomalous New Email Rule,” pertaining to the unusual email rule created by the SaaS user named ‘fdsdf’.

Blocking the action

A few minutes later, the SaaS user from the unusual IP address 45.133.172[.]86 was observed attempting to send an email with the subject “RE: Payments.” Subsequently, Darktrace detected the user engaging in activities that could potentially establish persistence in the compromised account, such as registering a new authenticator app. Recognizing this sequence of anomalous behaviors, Darktrace implemented an Autonomous Response inhibitor, disabling the SaaS user for two hours. This action effectively contained potential malicious activities, such as the distribution of phishing emails and fraudulent invoices, and gave the customer’s security team the necessary time to conduct a thorough investigation and implement appropriate security measures.

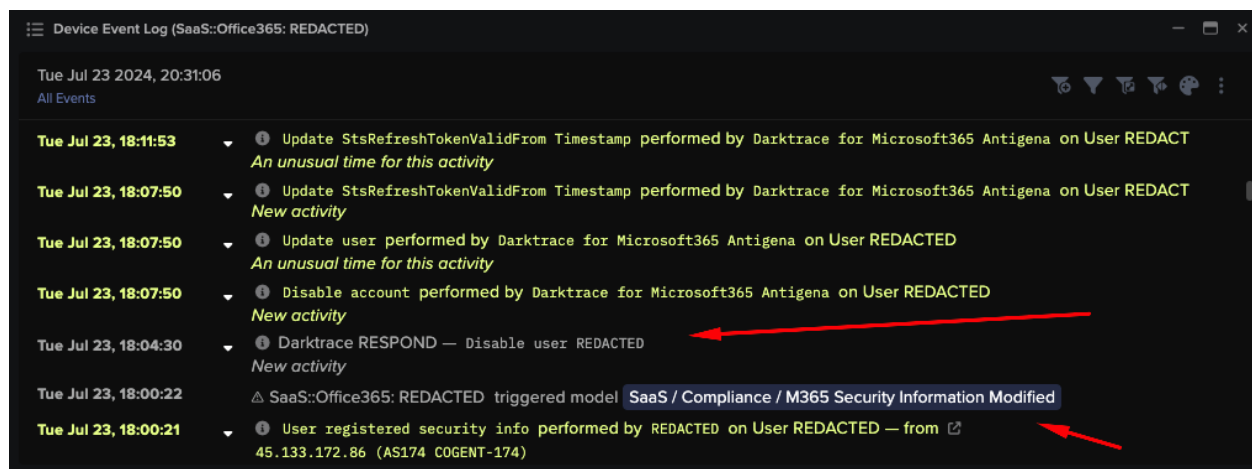


Figure 4: Device Event Log displaying Darktrace's Autonomous Response taking action by blocking the SaaS account.

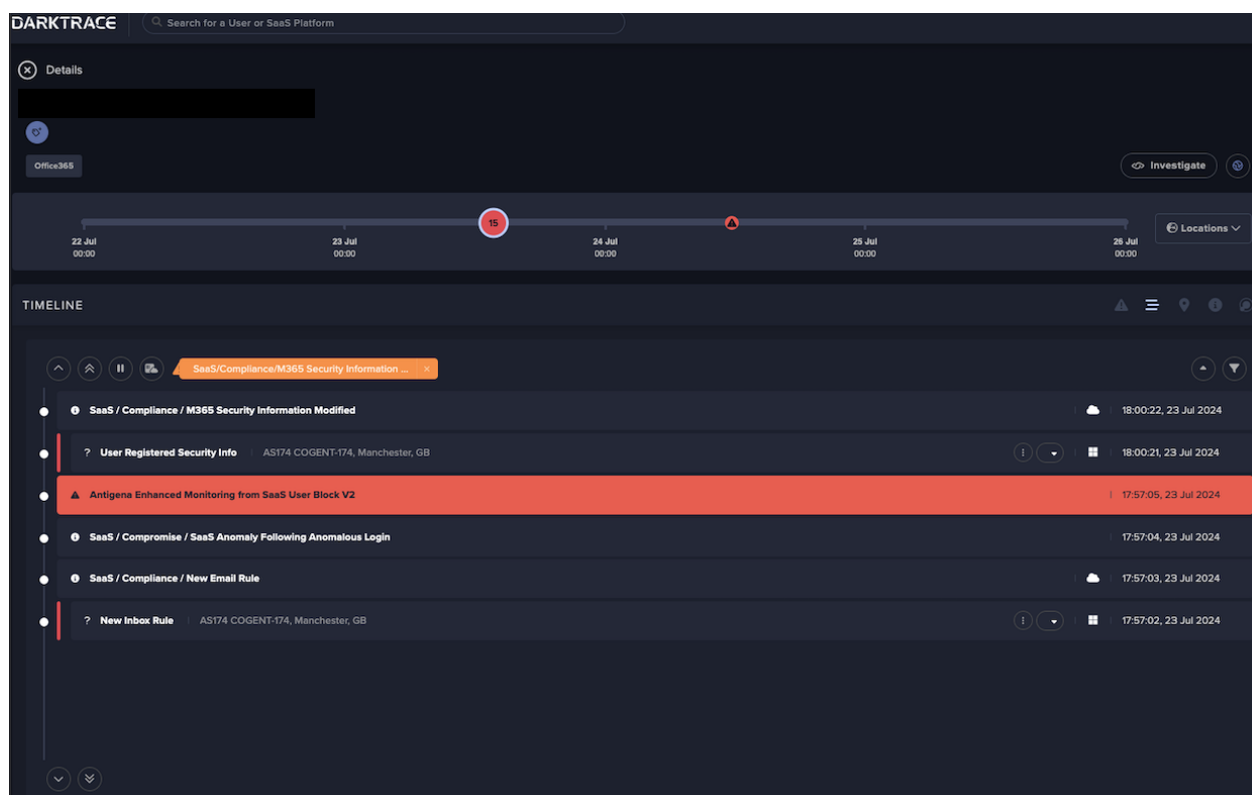


Figure 5: Darktrace / IDENTITY highlighting the 16 model alerts that triggered during the observed compromise.

In another example from mid-July, similar activities related to the campaign were observed on another customer network. A SaaS user was initially detected logging in from the unusual external endpoint 2607:5500:3000:fea[::]2.

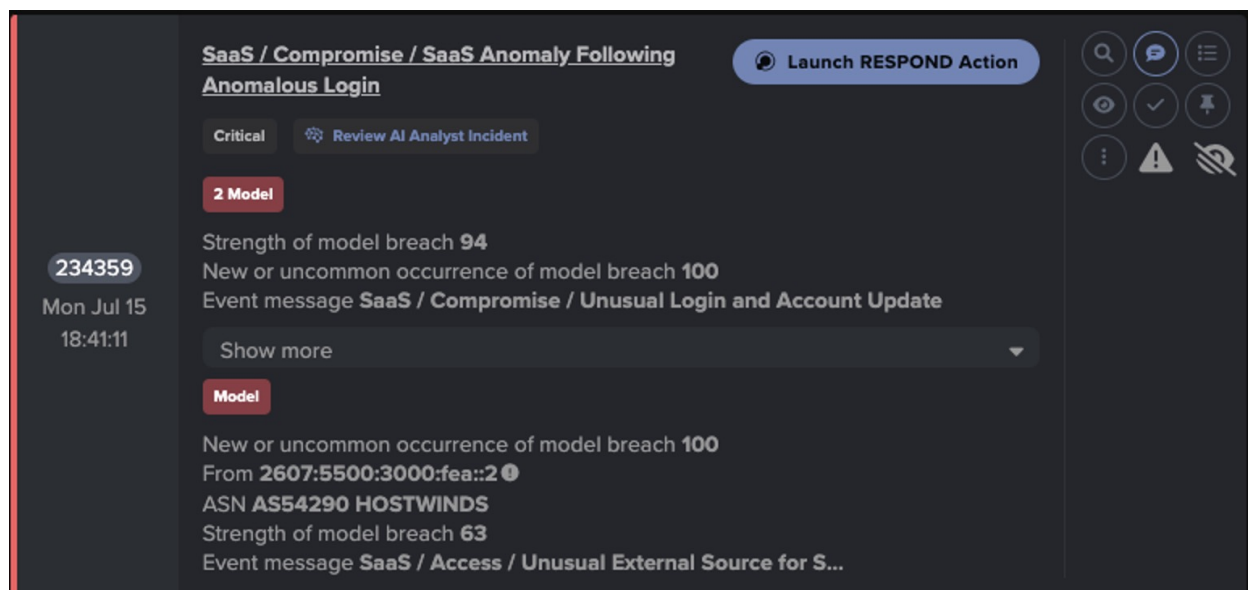


Figure 6: The SaaS / Compromise / SaaS Anomaly Following Anomalous Login model alert was triggered by an unusual login from a suspicious IP address linked to Mamba 2FA.

A few minutes later, in the same manner as demonstrated in the previous case, the actor was observed logging in from another rare endpoint, 102.68.111[.]240. However, this time it was from a source IP located in Lagos, Nigeria, which no other user on the network had been observed connecting from. Once logged in, the SaaS user updated the settings to "User registered Authenticator App with Notification and Code," a possible attempt to maintain persistence in the SaaS account.

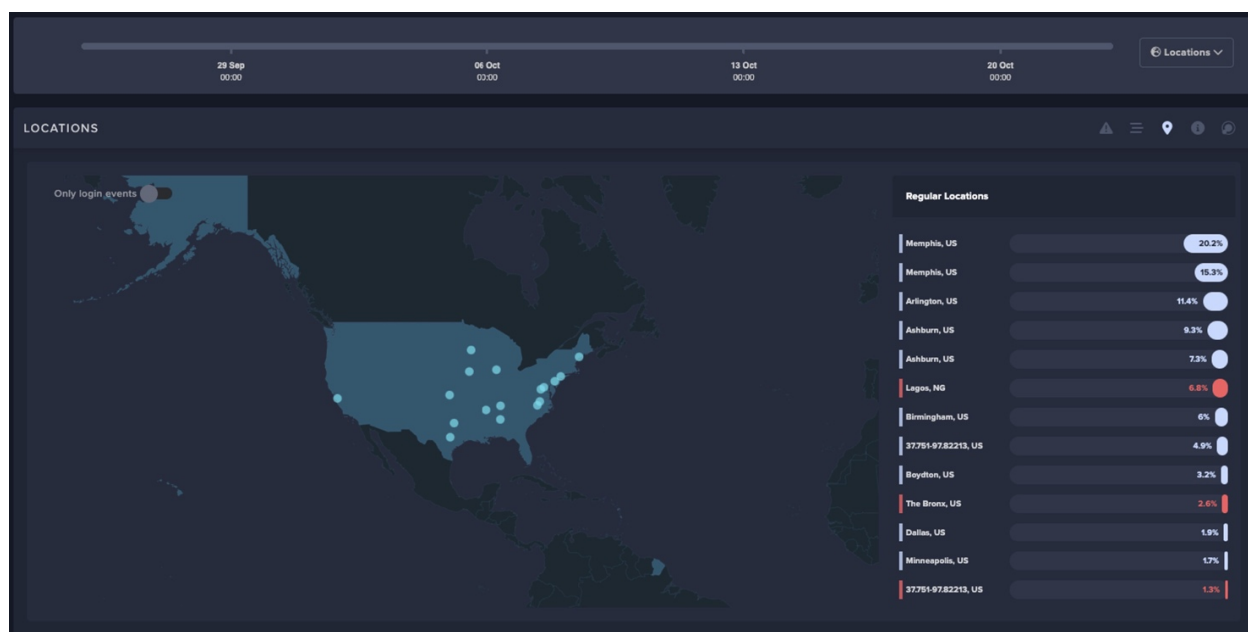


Figure 7: Darktrace / IDENTITY highlighted the regular locations for the SaaS user. The rarity scores associated with the Mamba 2FA IP location and another IP located in Nigeria were classified as having very low regularity scores for this user.

Based on unusual patterns of user behavior, a Cyber AI Analyst Incident was also generated, detailing all potential account hijacking activities. Darktrace also applied an Autonomous Response action, disabling the user for over five hours. This swift action was crucial in preventing further unauthorized access, potential data breaches and further implications.

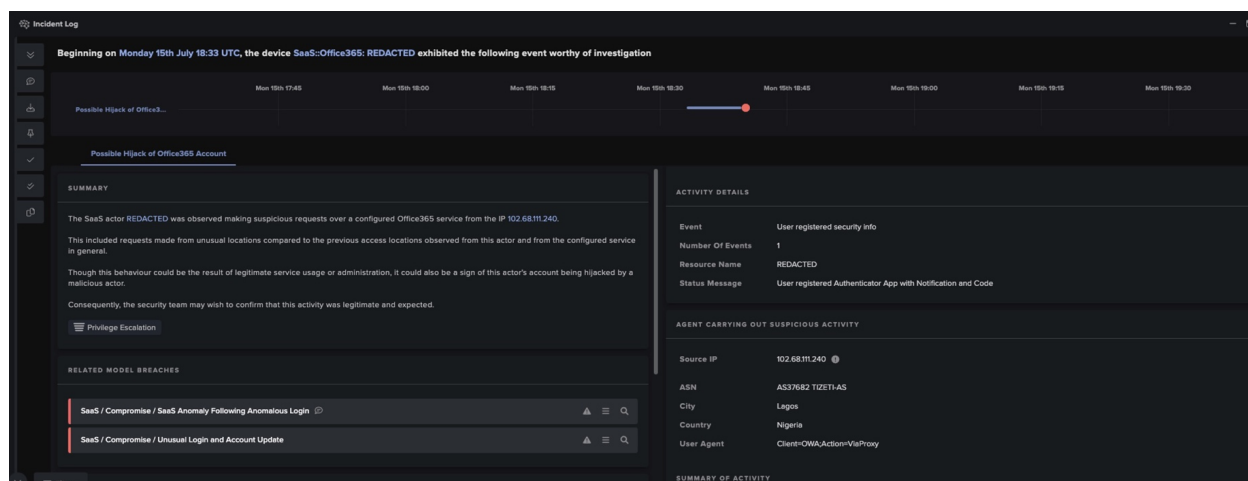


Figure 8: Cyber AI Analyst Incident detailing the unusual activities related to the SaaS account hijacking.

Since the customer had subscribed to Darktrace Security Operations Centre (SOC) services, Darktrace analysts conducted an additional human investigation confirming the account compromise.

How Darktrace Combats Phishing Threats

The initial entry point for Mamba 2FA account compromises primarily involves phishing campaigns using HTML attachments and deceptive links. These phishing attempts are designed to mimic legitimate Microsoft services, such as OneDrive and SharePoint, making them appear authentic to unsuspecting users. Darktrace / EMAIL leverages multiple capabilities to analyze email content for known indicators of phishing. This includes looking for suspicious URLs, unusual attachments (like HTML files with embedded JavaScript), and signs of social engineering tactics commonly used in phishing campaigns like Mamba 2FA. With these capabilities, Darktrace successfully detected Mamba 2FA phishing emails in networks where this tool is integrated into the security layers, consequently preventing further implications and account hijacks of their users.

Mamba 2FA URL Structure and Domain Names

The URL structure used in Mamba 2FA phishing attempts is specifically designed to facilitate the capture of user credentials and MFA tokens while evading detection. These phishing URLs typically follow a pattern that incorporates Base64-encoded parameters, which play a crucial role in the operation of the phishing kit.

The URLs associated with Mamba 2FA phishing pages generally follow this structure [6]:

https://{domain}/{m,n,o}/?{Base64 string}

Below are some potential Mamba 2FA phishing emails, with the Base64 strings already decoded, that were classified as certain threats by Darktrace / EMAIL. This classification was based on identifying multiple suspicious characteristics, such as HTML attachments containing JavaScript code, emails from senders with no previous association with the recipients, analysis of redirect links, among others. These emails were autonomously blocked from being delivered to users' inboxes.

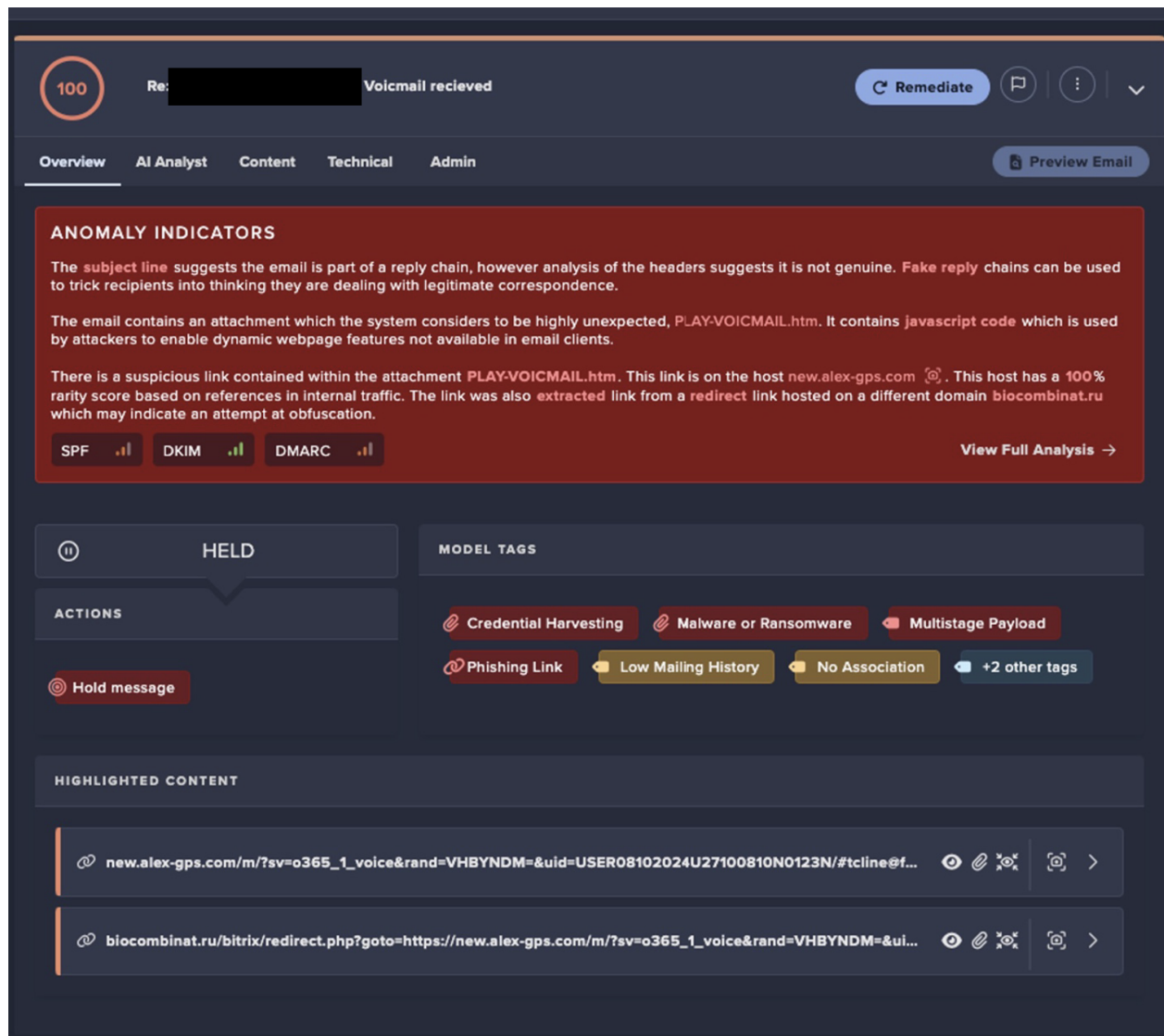


Figure 9: Darktrace / EMAIL highlighted a possible phishing email from Mamba 2FA, which was classified as a 100% anomaly.

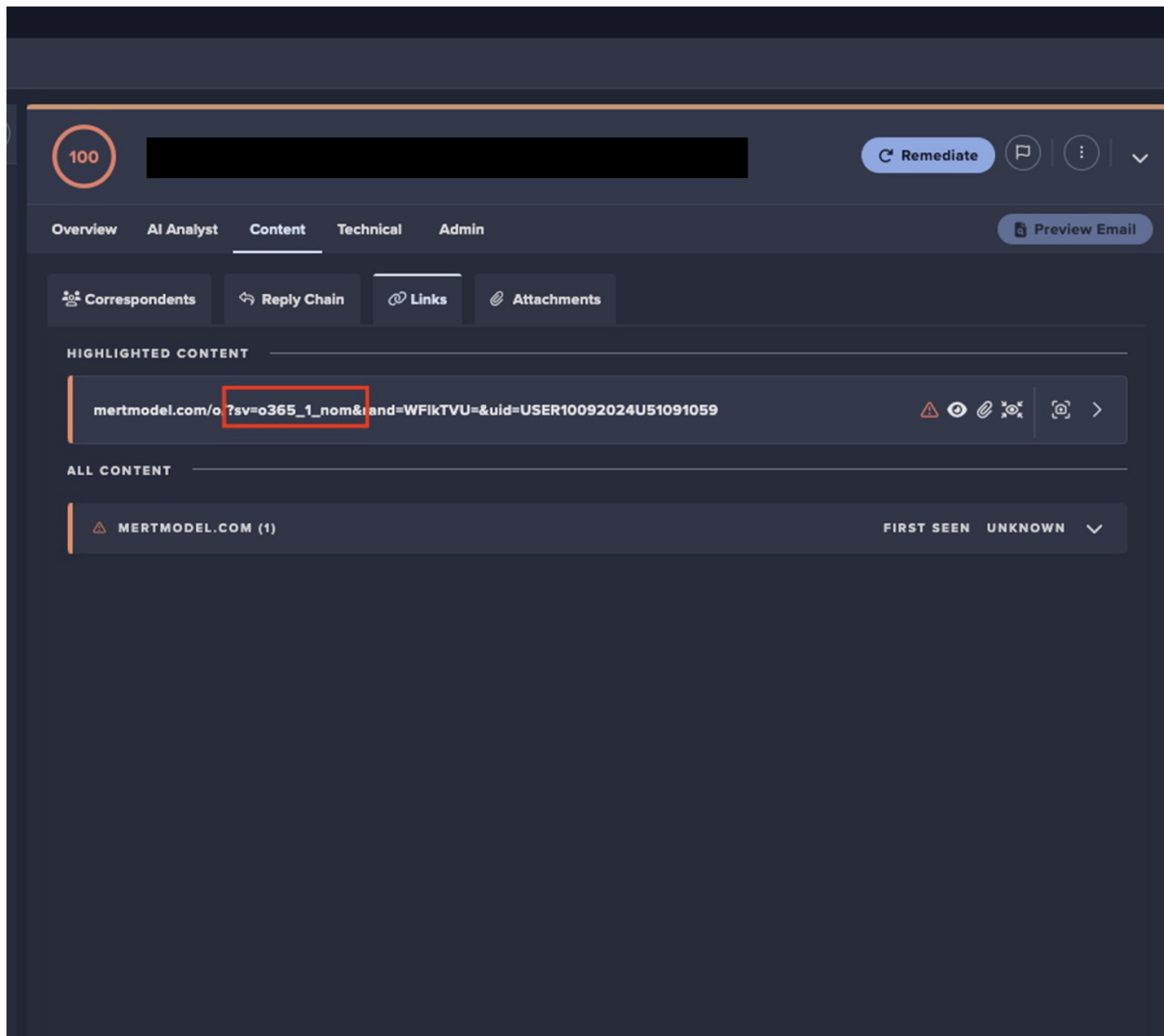


Figure 10: Darktrace / EMAIL highlighted a URL that resembles the characteristics associated with Mamba 2FA.

Conclusion

The rise of PhaaS platforms and the advent of AiTM phishing kits represent a concerning evolution in cyber threats, pushing the boundaries of traditional phishing tactics and exposing significant vulnerabilities in current cybersecurity defenses. The ability of these attacks to effortlessly bypass traditional security measures like MFA underscores the need for more sophisticated, adaptive strategies to combat these evolving threats.

By identifying and responding to anomalous activities within Microsoft 365 accounts, Darktrace not only highlights the importance of comprehensive monitoring but also sets a new standard for proactive threat detection. Furthermore, the autonomous threat response capabilities and the exceptional proficiency of Darktrace / EMAIL in intercepting and neutralizing sophisticated phishing attacks illustrate a robust defense mechanism that can effectively safeguard users and maintain the integrity of digital ecosystems.

Appendices

Darktrace Model Detections

- SaaS / Access / M365 High Risk Level Login
- SaaS / Access / Unusual External Source for SaaS Credential Use
- SaaS / Compromise / Login From Rare Endpoint While User Is Active
- SaaS / Compliance / M365 Security Information Modified
- SaaS / Compromise / Unusual Login and New Email Rule
- SaaS / Email Nexus / Suspicious Internal Exchange Activity
- SaaS / Compliance / Anomalous New Email Rule
- SaaS / Email Nexus / Possible Outbound Email Spam
- SaaS / Compromise / Unusual Login and Account Update
- SaaS / Compromise / SaaS Anomaly Following Anomalous Login
- SaaS / Compliance / M365 Security Information Modified
- SaaS / Compromise / Login From Rare Endpoint While User Is Active
- SaaS / Compromise / Unusual Login, Sent Mail, Deleted Sent
- SaaS / Unusual Activity / Multiple Unusual SaaS Activities
- SaaS / Email Nexus / Unusual Login Location Following Link to File Storage
- SaaS / Unusual Activity / Multiple Unusual External Sources For SaaS Credential
- IaaS / Compliance / Uncommon Azure External User Invite
- SaaS / Compliance / M365 External User Added to Group
- SaaS / Access / M365 High Risk Level Login
- SaaS / Compliance / M365 Security Information Modified
- SaaS / Unusual Activity / Unusual MFA Auth and SaaS Activity
- SaaS / Compromise / Unusual Login and Account Update

Cyber AI Analyst Incidents:

- Possible Hijack of Office365 Account
- Possible Hijack of AzureActiveDirectory Account
- Possible Unsecured Office365 Resource

List of Indicators of Compromise (IoCs)

IoC	Type	Description + Confidence
-----	------	--------------------------

2607:5500:3000:fea:::2	IPv6	Possible Mamba 2FA relay server
------------------------	------	---------------------------------

2607:5500:3000:1cab:::2	IPv6	Possible Mamba 2FA relay server
-------------------------	------	---------------------------------

References

1. <https://securityaffairs.com/136953/cyber-crime/caffeine-phishing-platform.html>
2. <https://any.run/cybersecurity-blog/analysis-of-the-phishing-campaign/>
3. <https://www.bleepingcomputer.com/news/security/new-mamba-2fa-bypass-service-targets-microsoft-365-accounts/>
4. <https://cyberinsider.com/microsoft-365-accounts-targeted-by-new-mamba-2fa-aitm-phishing-threat/>
5. <https://blog.sekoia.io/mamba-2fa-a-new-contender-in-the-aitm-phishing-ecosystem/>

MITRE ATT&CK Mapping

Tactic – Technique

DEFENSE EVASION, PERSISTENCE, PRIVILEGE ESCALATION, INITIAL ACCESS - Cloud Accounts

DISCOVERY - Cloud Service Dashboard

RESOURCE DEVELOPMENT - Compromise Accounts

CREDENTIAL ACCESS - Steal Web Session Cookie

PERSISTENCE - Account Manipulation

PERSISTENCE - Outlook Rules

RESOURCE DEVELOPMENT - Email Accounts

INITIAL ACCESS - Phishing

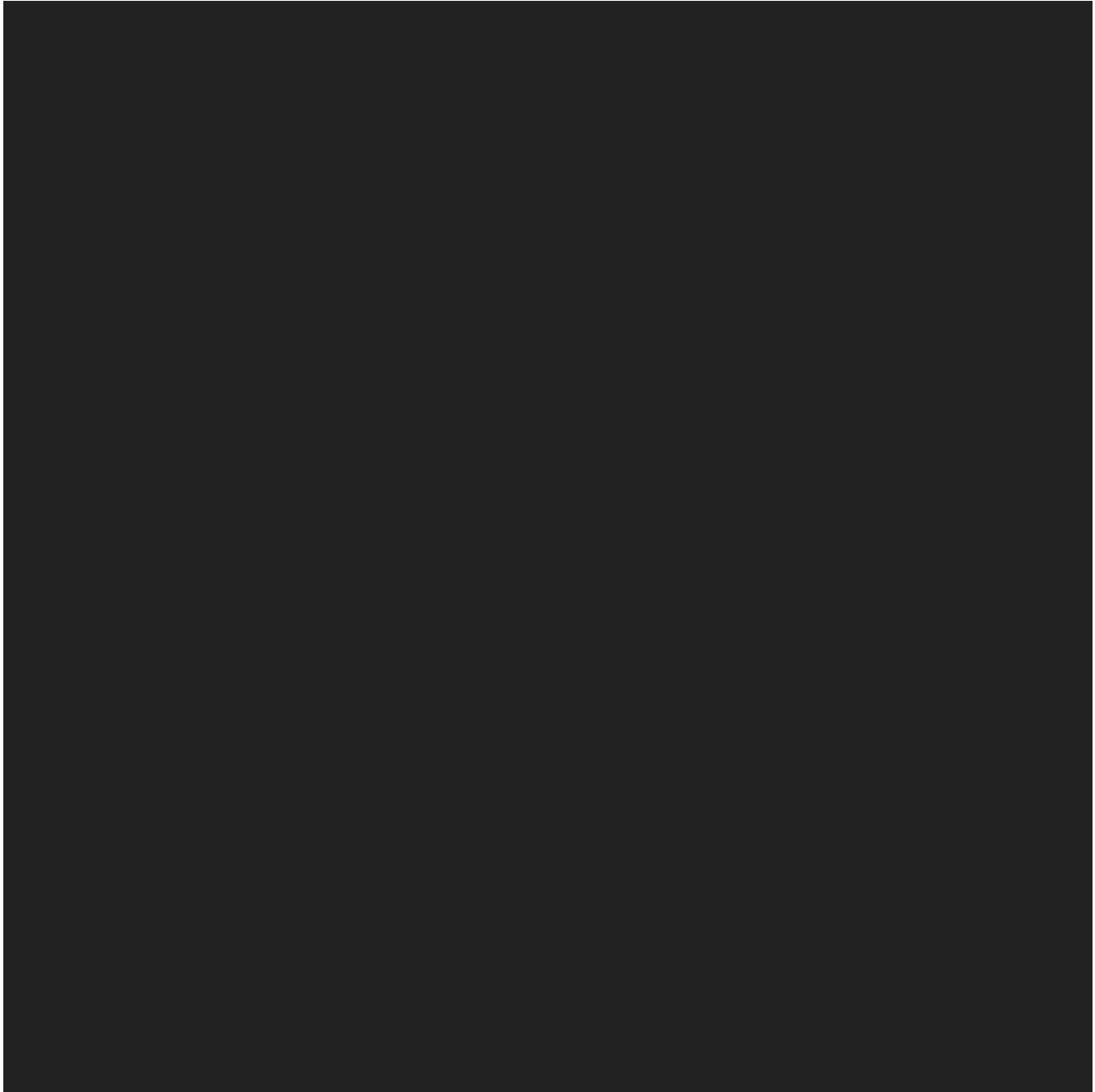
[Continue reading](#)



About the author

Patrick Anjos

Senior Cyber Analyst



Blog

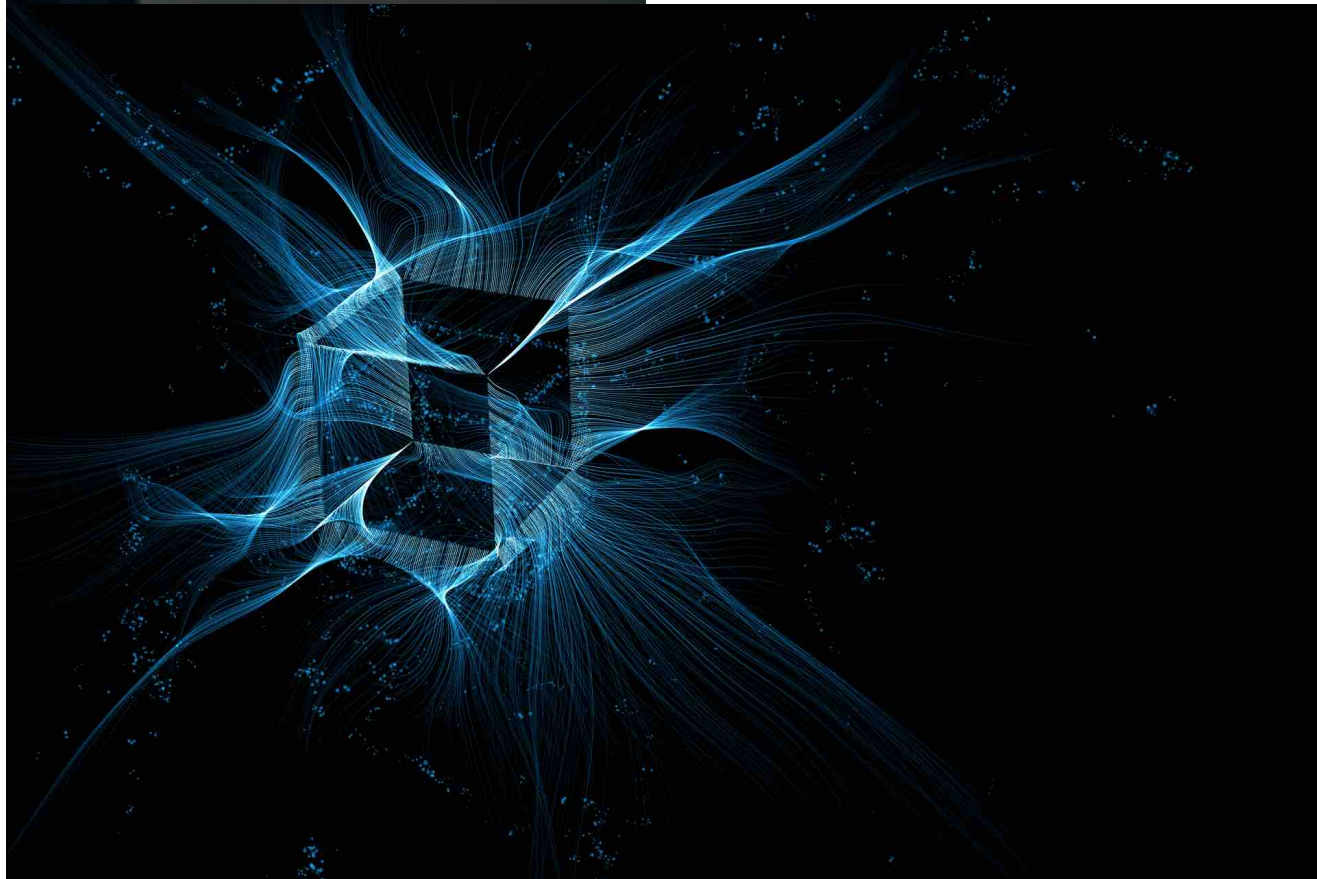
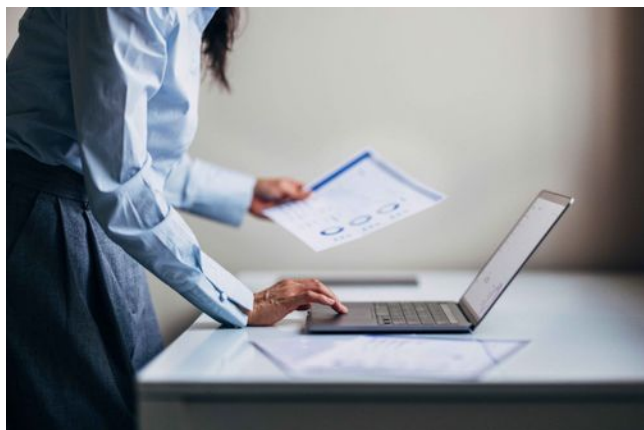
/

December 19, 2024

/

No items found.

Darktrace Recognized in the Gartner® Magic Quadrant™ for Email Security Platforms





Darktrace has been recognized in the first ever Gartner Magic Quadrant for Email Security Platforms (ESP). As a Challenger, we have been recognized based on our *Ability to Execute* and *Completeness of Vision*.

The Gartner Magic Quadrant for Email Security is designed to help organizations evaluate which email security solutions might be the best fit for their needs by providing a visual representation of the market vendors and the strengths and cautions of different vendors. We encourage our customers to read the full report to get the complete picture.

Darktrace / EMAIL has a unique AI approach to identifying threats, including NLP and behavioral analysis, instead of traditional security measures like signatures and sandboxing – providing protection against advanced attacks like Business Email Compromise (BEC) and spear phishing. We believe our AI-first approach delivers high-quality solutions that our customers trust, allowing them to stay ahead of sophisticated threats that other tools miss.

We're proud of Darktrace's rapid growth, geographic scale, and ability to execute effectively in the email security market, which reflect our commitment to delivering high-quality, reliable solutions that meet the evolving needs of our customers.

What do we believe makes Darktrace the fastest growing email security solution on the market?

An AI-first approach to innovation: Catching the threats others miss

As one of the founders of the ICES category, Darktrace has a long history of innovation, backed by over 200 patents. While other email security solutions are only just starting to apply machine learning (ML) techniques to outdated methods like signature analysis, reputation lists, and sandboxing, Darktrace has redefined the approach to email threat detection with its pioneering AI-driven anomaly detection engine.

Traditional ESPs often miss advanced threats because they rely on rules and signatures that focus on payloads and blindly trust known sources. This approach requires constant updates and frequently fails to detect threats like Business Email Compromise and Spear Phishing. In contrast, Darktrace / EMAIL uses advanced anomaly detection to identify the most sophisticated threats by focusing on unusual patterns and behaviors. This innovative approach has consistently delivered superior detection, stopping on average 58% of the threats that other solutions in the security stack miss.¹

But our AI-first approach doesn't stop at the inbox. At Darktrace, we transcend the limitations of traditional email security by leveraging a platform that unifies insights across multiple domains, providing robust protection against multi-domain threats. Our award-winning solutions defend the most popular attack vectors, including email, messaging, network, and identity protection. By combining signals from all domains, we establish unique behavioral profiles for each device and user, significantly enhancing detection precision.

This pioneering approach has led to introducing industry-first advancements like QR code analysis and automated incident investigations, alongside game-changing functionality including:

- **Microsoft Teams security with advanced messaging analysis:** The ability to identify critical early phishing and insider threats across both email and Microsoft Teams messaging.
- **AI analyst narratives for improved end user reporting:** that reduces phishing investigations by 60% by exposing unique narratives that provide the context of each received email and give feedback to each employee as they interact with their mail.²
- **Mailbox Security Assistant:** to perform advanced behavioral browser analysis and stop malicious links within webpages, detecting and remediating 70% more malicious phishing links than traditional tools.³
- **AI based, autonomous data loss prevention:** to immediately secure your organization from misdirected emails, insider threats, and data loss—both classified and unclassified- without any administrative overhead.

Customer trust that fuels exponential growth

With almost 5,000 customers in under 5 years, we've doubled the growth rate of other vendors in the email security market. Our rapid market penetration, fueled by customer satisfaction and pioneering technology, showcases our revolutionary approach and sets new industry standards.

Darktrace's exceptional customer retention is fueled by an unparalleled customer experience, extensive regional support, dedicated account teams, and cutting-edge scalable technology. We pride ourselves on having a global network with local expertise, consisting of 110 worldwide offices which provide local language and technical support to offer multilingual, in-house assistance to our customer base.

Check it out – Darktrace / EMAIL has the highest percentage of 5-star ratings with a 4.8 rating on Gartner® Peer Insights™.⁴

Supporting every stage of your email security journey

Darktrace / EMAIL supports your security maturity journey, from first time security buyers to mature security stacks looking to augment their existing ESPs – by handling advanced threats without extensive tuning. And unlike other solutions that create a siloed and parallel solution, it works harmoniously with native email providers to create a modern email security stack. That's why Darktrace performs well with first-time email security buyers and has strong renewal rates.

Integrating with Microsoft and Google via API, we replace traditional Secure Email Gateways (SEGs) with a modern, comprehensive email security stack. By combining approaches, our solution merges attack-centric analysis, which learns attack patterns and threat intelligence, with a business-centric approach that understands user behavior and inbox activity to deliver a unified stack that defends the entire threat spectrum – leading Darktrace to be recognized as Microsoft Partner of the year UK 2024.

Our user-friendly, self-learning AI solution requires minimal tuning and deployment, making it perfect for customers looking for a highly usable but lightly configurable solution that will accompany them throughout their lifetime as they mature their email security stack in line with the evolving threat landscape.

Learn more

Get complimentary access to the full Gartner® Magic Quadrant™ for Email Security Platforms [here](#).

To learn more about Darktrace / EMAIL or to get a free demo, [check out the product hub](#).

References

¹ From September 1 – December 31 2023, 58% of the phishing emails analyzed by Darktrace / EMAIL had already passed through native spam filtering and email security controls. (Darktrace End of Year Threat Report 2023)

² When customers deployed the Darktrace / EMAIL Outlook Add-in there was a 60% decrease in incorrectly reported phishing emails. Darktrace Internal Research, 2024

³ Once a user reports phishing that contains a link, an automated second level triage engages our link analysis infrastructure expanding the signals analyzed. Darktrace Internal Research, 2024

⁴ Based on 252 reviews as of 19th December 2024

[Continue reading](#)

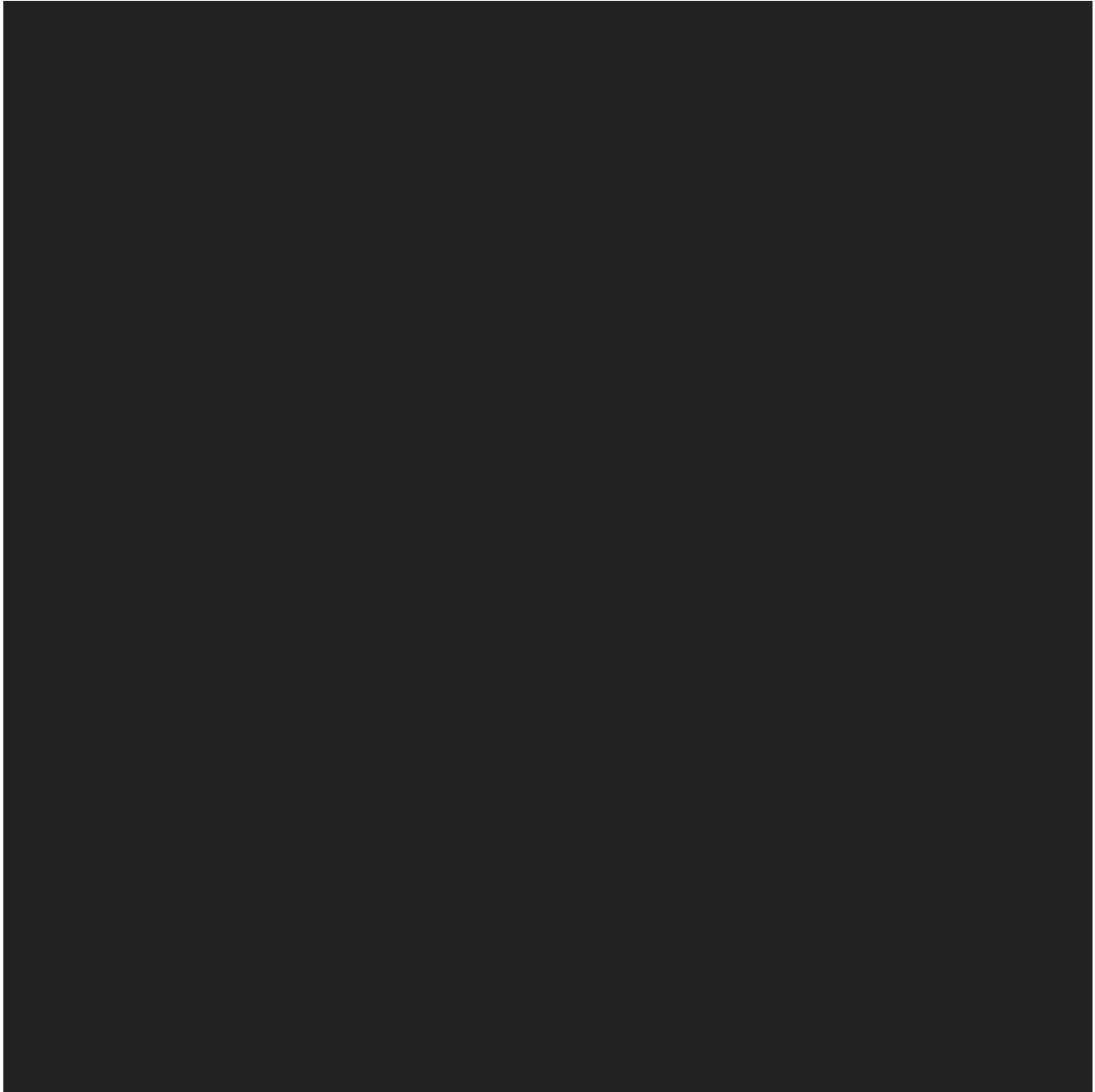


About the author



Carlos Gray

Product Manager



Your data. Our AI.

Elevate your network security with Darktrace AI

[Get a demo](#)

