



February 10, 2021 - Anomali Threat Research

Probable Iranian Cyber Actors, Static Kitten, Conducting Cyberespionage Campaign Targeting UAE and Kuwait Government Agencies

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

Manage Preferences

Accept All

Reject All



ScreenConnect Remote Access Tool Utilizing Ministry of Foreign Affairs-Themed EXEs and URLs

Authored by: Gage Mele, Winston Marydasan, and Yury Polozov

Key Findings

- Anomali Threat Research identified a campaign targeting government agencies in the United Arab Emirates (UAE) and likely the broader Middle East.
- We assess with medium confidence that the activity is being conducted by Iran-nexus

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

Overview

Anomali Threat Research has uncovered malicious activity very likely attributed to the Iran-nexus cyberespionage group, Static Kitten (Seedworm, MERCURY, Temp.Zagros, POWERSTATS, NTSTATS, MuddyWater), which is known to target numerous sectors primarily located in the Middle East.^[2] This new campaign, which uses tactics, techniques, and procedures (TTPs) consistent with previous Static Kitten activity, uses ScreenConnect launch parameters designed to target any MOFA with `mfa[.]gov` as part of the custom field. We found samples specifically masquerading as the Kuwaiti government and the UAE National Council respectively, based on references in the malicious samples.

In mid-2020, the UAE and Israel began the process of normalizing relations. Since then, tensions have further escalated in the region, as reported by numerous sources. The targeting of Kuwait could be tied to multiple factors, including Kuwait's MOFA making a public statement that they were willing to lead mediation between Iran and Saudi Arabia.^[3] Furthermore, in October 2020, trade numbers for a peace deal between Israel and UAE included an estimate for the creation of 15,000 jobs and \$2 billion in revenue on each side.^[4] In that same month, Static Kitten reportedly conducted Operation Quicksand, which targeted prominent Israeli organizations and included the use of file-storage service OneHub.^[5]

Details

We identified two lure ZIP files being used by Static Kitten designed to trick users into downloading a purported report on relations between Arab countries and Israel, or a file relating to scholarships. The URLs distributed through these phishing emails direct recipients to the intended file storage location on Onehub, a legitimate service known to be used by Static Kitten for nefarious purposes.^[6] Anomali Threat Research has identified that Static Kitten is continuing to use Onehub to host a file containing ScreenConnect.

The delivery URLs found to be part of this campaign are:

- `ws.onehub[.]com/files/7w1372el`
- `ws.onehub[.]com/files/94otjyvd`

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

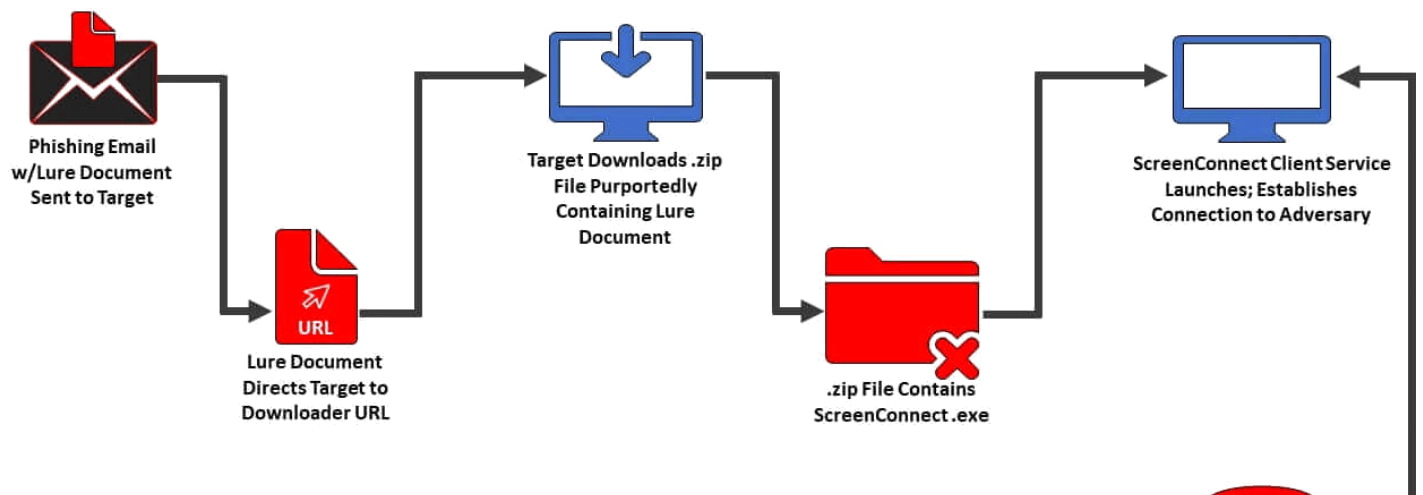
[Cookie Policy](#)

Translated file names

- Analysis and study of the normalization of relations between the Arab countries and Israel
`httpsmod.gov.kw.zip`
- Analysis and study of the normalization of relations between the Arab countries and Israel
`httpsmod.gov.kw.exe`
- Scholarships.zip
- Scholarships.exe
- Project.docx

Static Kitten's objective is to direct users to a downloader URL (`ws.onehub[.]com/files/7w1372el` which downloads a ZIP file) via a phishing email that impersonates an EXE (تحليل ودراسة تطبيع العلاقات الدول العربية واسرائيل `httpsmod[.]gov.kw.exe`). This EXE purports to be a report on Arabic countries and Israel relations but, when executed, actually launches the installation process for ScreenConnect.

A similar second sample uses .docx file that tries to direct users to `ws.onehub[.]com/files/94otjyvd` which downloads a ZIP file called لدراسة .zip. An EXE inside the ZIP of the same name will also begin the ScreenConnect installation process when executed. An overview of the infection chain is shown in Figure 1below.



To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

lure and decoy documents. An example lure is shown in Figure 2 below.



Figure 2 – Static Kitten Lure Document .docx

The .docx file shown in Figure 2 directly refers to government agency recipients while highlighting concerns about recent Iranian actions, the impact of the US elections, and joint studies by government entities on relations between Arabic countries and Israel. The actors reference multiple official agencies, including the General Secretariat of the Cooperation Council for the Arab States of the Gulf and the UAE National Media Council, likely in an effort to add the appearance of legitimacy. A full translation of this document can be viewed in Appendix A. The hyperlink in the .docx file is impersonating the UAE National Media Council, however, the actual link directs to ws.onehub.com/files/7w1372el.

The second file is a ZIP called [الدراسية.zip](#) (see Figure 3). We cannot determine the delivery method for this ZIP, but it is likely similar to the .docx email delivery method of the first download URL. The geopolitical-themed ZIP contains an EXE file with the same name that begins the installation process for ScreenConnect when executed (see Figure 4).

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

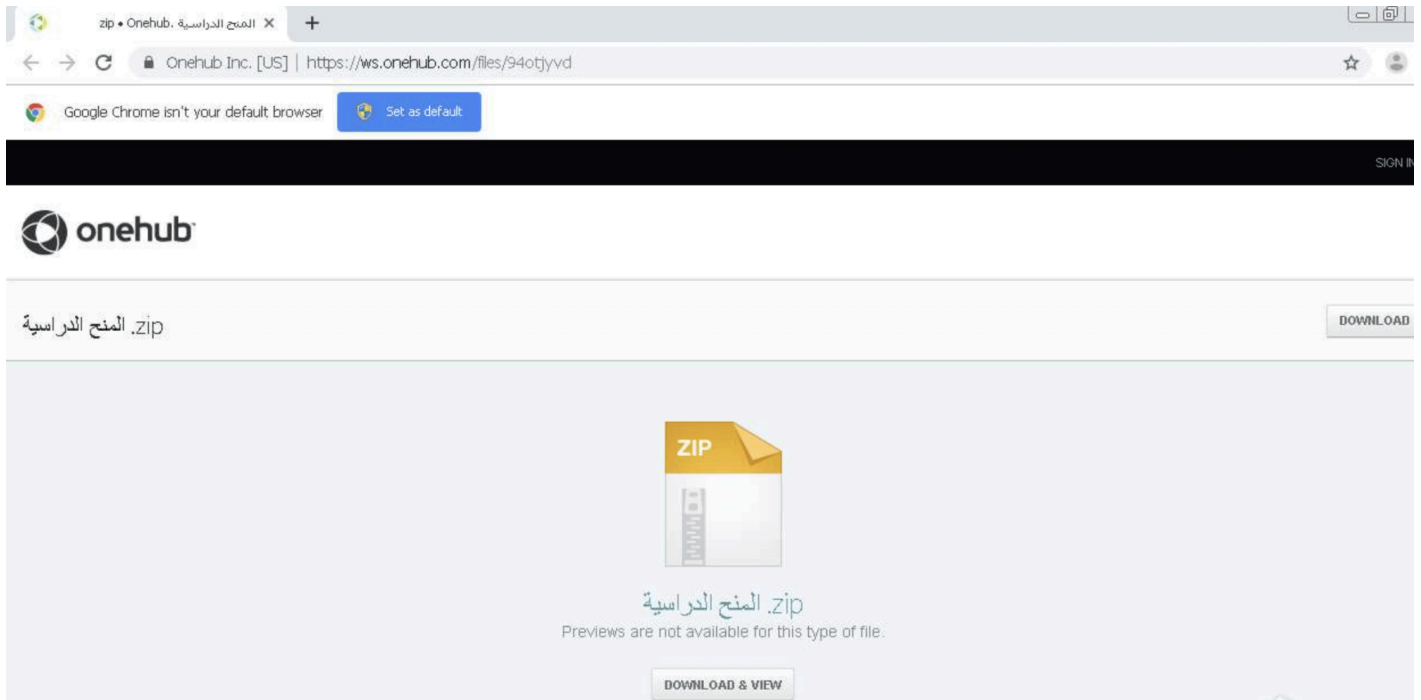


Figure 3 – Download URL ws.onehub.com/files/94otjyvd for Malicious ZIP المنح الدراسية .zip

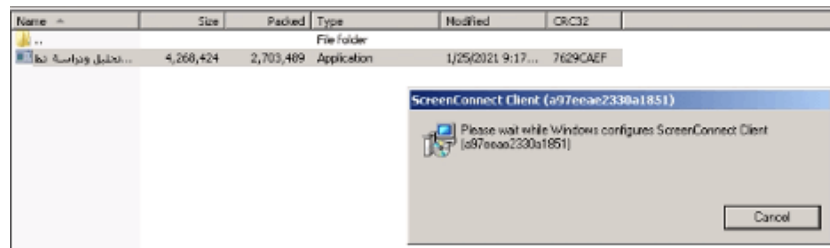


Figure 4 - ScreenConnect Installation

Technical Analysis

ScreenConnect and OneHub Context

Between 2016 and 2020, we have seen ScreenConnect and Onehub used in malicious cyber activity by different, unassociated threat actors. For example, between 2016 and 2019 unknown threat actors

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

Remote desktop management software is a common target and tool used by threat actors because of the wide variety of functionalities they offer. ScreenConnect offers three primary functions that each contain different valuable features for threat actors. ScreenConnect’s capabilities are shown in Table 1 below.

Table 1 - ScreenConnect Capabilities^[9]

Feature	Functions
Remote Support	Remote control and viewing of any internet-connect device.
Unattended Access	Persistent connection allows behind-the-scenes, remote control of any machine or server.
Meetings	Standard screen-sharing meetings with chat and voice communication, record video, and take screenshots.

The cybercriminal group Graceful Spider (TA505, Gold Evergreen, TEMP.Warlock, Hive0065, Chimborazo, FIN11) distributed spearphishing emails impersonating Onehub in 2019 in attempts to trick users into downloading the SDBbot remote access trojan (RAT).[10] Onehub’s file-storage services are also utilized in malspam emails to host various malware, as is common with other file storage locations abused by multiple threat actors.

First Executable

تحليل ودراسة تطبيع العلاقات الدول العربية واسرائيل <https://mod.gov.kw.exe>

When a user tries to double click the executable تحليل ودراسة تطبيع العلاقات الدول العربية واسرائيل <https://mod.gov.kw.exe> (Screenconnect payload), it drops the Microsoft installer file. This begins the installation of the client payload onto victim machines. While the actors attempted to make the installation appear legitimate, closer inspection of the client launch parameters reveals the potential for broader MOFA targeting. The client service launch parameters are:

"C:\Program Files (x86)\ScreenConnect Client

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

Analysis of the authentic launch parameters passed back to the server as part of Screenconnect functionality is shown in Table 2 below.

Table 2 - ScreenConnect Launch Parameters

Launch Parameter	Description
e=Access	Session type: access, meet, support.
y=Guest	ProcessType (Guest or Host).
h=instance-sy9at2-relay.screenconnect.com	URI to reach server's relay service.
p=443	Port on which relay service operates
s=6a1e6739-ad4f-4759-8c69-dfe896b9a817	The GUID to identify the client.
k=BglAAACkAABSU0ExAAgAAAEAAQCVzMmjXhdfu5xyqTHPWDSj9Qjbq%2bQIIQursvinhHWO9UWKiTPrR7quzVCpids4AagFWBCbS6cfow4bTxdtZyrd%2fNQQRVUcQ%2f%2boszJVH6S1JEpmF6ZPruFKyy1yr%2fEuxhNcHAWNf0CQKhhVsK0rXVIRE%2b4%2f4v%2fk%2f7%2bHPg2kwhmBHFZTJVd7xADVdVuYESMiCmu4gx8Akf9aAE2RUz9LjSiCU6LwJtp4AjjMCaGLFSaragsfZ1e%2fD9UEEee8n0J69HLcLoY%2fW8w8RKqQXILC9S3ONSkepA4UHcptKwP5GXogluNbG7UdgiaynRL%2b31oTHOZ32giSoxHDGHc3WphKwDv	The encoded encryption key used to verify the identity.
&t	Is not defined and is the NameCallback Format if the name of

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

These parameters contain predefined properties that can allow an actor to know which target, or from where, has been infected. In this example the infected target is MOFA.

Second Executable

.exe المنح الدراسية

The ScreenConnect launch parameters from `.exe المنح الدراسية` is shown below:

```
"C:\Program Files (x86)\ScreenConnect Client
(03b9d0ec9210f109)\ScreenConnect.ClientService.exe" "?e=Access&y=Guest&h=instance-sy9at2-
relay.screenconnect.com&p=443&s=6a1e6739-ad4f-4759-8c69-
dfe896b9a817&k=BglAAACkAABSU0ExAAgAAAEAAQCVzMmjXhdfu5xyqTHPWDSj9Qjbq%2bQIIQurs
vinhHWO9UWKiTPrrR7quzVCpids4AagFWBCbS6cfow4bTxdTzyrd%2fNQQRVUcQ%2f%2boszJVH6S1
JEpmF6ZPruFKyy1yr%2fEuxhNcHAWNf0CQKhhVsK0rXVIRE%2b4%2f4v%2fk%2f7%2bHPg2kwhmBH
FZTJVd7xADVdVuYESMiCmu4gx8Akf9aAE2RUz9LjSiCU6LwJtp4AjjMCaGLFSaragsfZ1e%2fD9UEEee
8n0J69HLCLoY%2fW8w8RKqQXILC9S3ONSkepA4UHcptKwP5GXogluNbG7UdgiaynRL%2b31oTHOZ3
2giSoxHDGHc3WphKwDv&t=&c=mfa&c=mfa.gov&c=mfa&c=pc&c=&c=&c=&c="
```

The actors again created a custom field parameter, however, this one is kept to a generic MOFA targeting that appears as MFA:

- `&c=mfa&c=mfa.gov`

Conclusion

Utilizing legitimate software for malicious purposes can be an effective way for threat actors to obfuscate their operations. In this latest example, Static Kitten is very likely using features of ScreenConnect to steal sensitive information or download malware for additional cyber operations. As Static Kitten is assessed to be primarily focused on cyberespionage, it is very likely that data-theft is the primary objective behind propagating ScreenConnect to government agency employees.

We will continue monitoring this group for additional malicious activity and provide details when appropriate.

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

Endnotes

- [1] ClearSky Cyber Security, "Operation Quicksand: Muddywater's Offensive Attack Against Israeli Organizations," ClearSky, accessed February 8, 2021, published October 2020, <https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf>, 3.
- [2] MuddyWater," MITRE, accessed February 8, 2021 <https://attack.mitre.org/groups/G0069/>.
- [3] "Kuwait willing to mediate between Iran and Saudi," Middle East Monitor, accessed February 8, 2021, published February 4, 2021, <https://www.middleeastmonitor.com/20210204-kuwait-willing-to-mediate-between-iran-and-saudi/>.
- [4] Attila Shumelby, "Intelligence Minister Eli Cohen: Netanyahu secretly visited other countries besides the Emirates," Ynet, accessed February 8, 2021, published, September 9, 2020, <https://www.ynet.co.il/news/article/S1v00IFsXP>; Jonathan Josephs, "Israel-UAE peace deal 'big' for trade in Middle East," BBC News, accessed February 8, 2021, published October 16, 2020, <https://www.bbc.com/news/business-54574022>.
- [5] ClearSky Cyber Security, "Operation Quicksand: Muddywater's Offensive Attack Against Israeli Organizations," ClearSky, 23.
- [6] Ibid.
- [7] "Wipro Intruders Targeted Other Major IT Firms," KrebsOnSecurity, accessed February 8, 2021, published April 18, 2019, <https://krebsonsecurity.com/2019/04/wipro-intruders-targeted-other-major-it-firms/#more-47453>.
- [8] Ibid.
- [8] Alon Groisman, "Connectwise Control Abused Again to Deliver Zeppelin Ransomware," Morphisec Blog, accessed February 8, 2021, published December 18, 2019, <https://blog.morphisec.com/connectwise-control-abused-again-to-deliver-zeppelin-ransomware>.
- [9] "CAUSE AND EFFECT: SODINOKIBI RANSOMWARE ANALYSIS," Tetra Defense, accessed February 8, 2021, <https://www.tetradefense.com/incident-response-services/cause-and-effect-sodinokibi-ransomware-analysis/>.

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

Docx

31a35e3b87a7f81449d6f3e195dc0660b5dae4ac5b7cd9a65a449526e8fb7535

EXE

3e4e179a7a6718eedf36608bd7130b62a5a464ac301a211c3c8e37c7e4b0b32b
5bfb635c43eb73f25f4e75961a715b96fa764bbe096086fc1e037a7869c7878b

IP

149.202.216.53

URL

<https://ws.onehub.com/files/94otjyvvd>
<https://ws.onehub.com/files/7w1372el>
instance-sy9at2-relay.screenconnect.com
instance-uwct38-relay.screenconnect.com

ZIP

b2f429efdb1801892ec8a2bcdd00a44d6ee31df04721482a1927fc6df554cdcf
77505dcec5d67cc0f6eb841f50da7e7c41a69419d50dc6ce17fffc48387452e1

Appendix A

Gentlemen / employees of government agencies

Happy New Year

After a kind greeting ,,,

In view of the situation in the region, especially after the US elections, and concerns about Iran's actions, joint studies have been conducted between the National Media Council and the General Secretariat of the Cooperation Council for the Arab States of the Gulf on counting the political, security and economic consequences of the normalization of relations between Arab countries and Israel. Consequently, the draft studies on negotiations on the normalization of relations between Arab countries and Israel were presented by experts of the member states of the General Secretariat of the Cooperation Council for the Arab States of the Gulf, and in this regard, the National Media Council seeks to conduct a comprehensive survey by the member states.

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

Get the Latest Anomali Updates and Cybersecurity News – Straight To Your Inbox

Become a subscriber to the Anomali Newsletter

Receive a monthly summary of our latest threat intelligence content, research, news, events, and more.

SUBSCRIBE TODAY

Explore more topics

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

<u>ANOMALI SECURITY OPERATIONS PLATFORM</u> >	<u>COMPLIANCE</u> >
<u>CYBER THREAT INTELLIGENCE</u> >	<u>ISAC</u> >
<u>MALWARE</u> >	<u>MODERN HONEY NETWORK</u> >
<u>RESEARCH</u> >	<u>SIEM</u> >
<u>SOAR</u> >	<u>STAXX</u> >
<u>SPLUNK</u> >	<u>THREAT INTELLIGENCE PLATFORM</u> >
<u>THREATSTREAM</u> >	<u>UEBA</u> >

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[+44 8000 148096](tel:+448000148096) (International Toll-Free).



Platform and Products

[Anomali Platform](#)

[Anomali Copilot](#)

[Anomali Security Analytics](#)

[Anomali ThreatStream](#)

Marketplace

[Anomali Marketplace](#)

[Threat Intelligence Feeds](#)

[Threat Analysis Tools and Enrichments](#)

[Security System Partners](#)

[Marketplace for Partners](#)

Partners

[Partners Overview](#)

[Join the Technology Partner Program](#)

[Anomali SDKs](#)

[Threat Intel Sharing](#)

[Partner Portal Login](#)

Resources

[Resource Library](#)

[Blog](#)

[Events](#)

[Support](#)

[Glossary](#)

Company

[About Us](#)

[Leadership](#)

[Careers](#)

[Press Room](#)

[Contact Us](#)

[Get the App](#)

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Privacy Policy](#) [Terms of Use](#) [Cookies Policy](#) [Security](#)

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)