Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

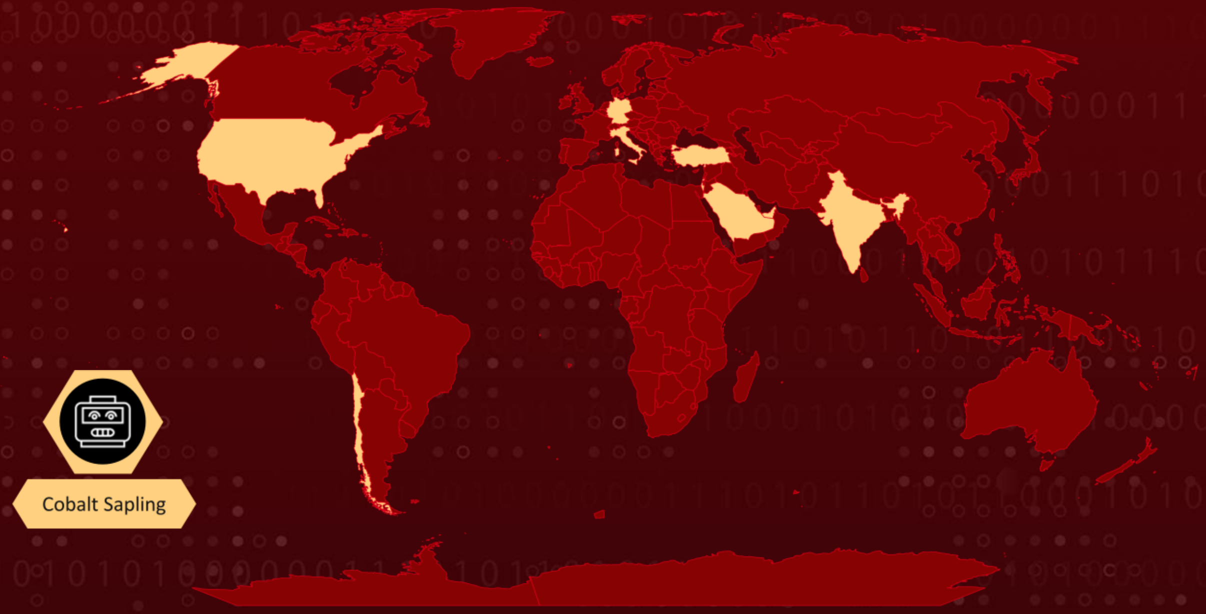
Similarities between hacktivist groups reveal Iranian connection

Date of Publication	Admiralty code	TA Number
January 27, 2023	A1	TA2023049

Summary

First Appearance: September 2021
Actor Name: Cobalt Sapling
Target Countries: Chile, Germany, India, Israel, Italy, Turkey, UAE, USA, Saudi Arabia
Target Sectors: Energy, Financial, Government, Manufacturing, Transportation, Utilities, Defense, Engineering, Legal, Media, Satellite Imagery, Technology

Actor Map



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Actor Details

#1

COBALT SAPLING is a threat actor group that is believed to be Iranian in origin. The group has been found to operate multiple hacktivist group personas, including Moses Staff and Abraham's Ax. Researchers have investigated similarities between the two groups and found several commonalities in their iconography, videography and leak sites, suggesting that they are likely operated by the same entity. The Moses Staff group emerged in September 2021, and the Abraham's Ax group emerged in November 2022.

#2

Both groups use a WordPress blog as the basis for their leak sites, and both sites offer multiple languages. Moses Staff is available in Hebrew and English, while Abraham's Ax is available in Hebrew, Farsi, and English. Both groups use domains registered with EgenSajt.se. The Moses Staff group claims to be anti-Israeli and pro-Palestinian and encourages leak site visitors to take part in "exposing the crimes of the Zionists in occupied Palestine." The group has posted 16 "activities" to their site as of December 2, and the leaked information is predominantly data sets stolen from Israeli companies but also includes compilations of personal information on individuals affiliated with Israel's signals intelligence Unit 8200.

#3

The Abraham's Ax group, on the other hand, claims to be operating on behalf of the Hezbollah Ummah and attacks government ministries in Saudi Arabia.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
Cobalt Sapling (Moses Staff, DEV-0500, Abraham's Ax)	Iran	Chile, Germany, India, Israel, Italy, Turkey, UAE, USA, Saudi Arabia	Energy, Financial, Government, Manufacturing, Transportation, Utilities, Defense, Engineering, Legal, Media, Satellite Imagery, Technology
	MOTIVE		
	Sabotage and destruction		

Recommendations

Security Leaders
Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actor through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0007 Discovery	TA0008 Lateral Movement
TA0011 Command and Control	TA0003 Persistence	TA0005 Defense Evasion	T1087 Account Discovery
T1087.001 Local Account	T1587 Develop Capabilities	T1587.001 Malware	T1190 Exploit Public-Facing Application
T1562 Impair Defenses	T1562.004 Disable or Modify System Firewall	T1105 Ingress Tool Transfer	T1027 Obfuscated Files or Information
T1588 Obtain Capabilities	T1588.002 Tool	T1021 Remote Services	T1021.002 SMB/Windows Admin Shares
T1505 Server Software Component	T1505.003 Web Shell	T1553 Subvert Trust Controls	T1553.002 Code Signing
T1082 System Information Discovery	T1016 System Network Configuration Discovery		

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA1	7a5d75db6106d530d5fdd04332c68cd7ccec287f 76a35d4087a766e2a5a06da7e25ef76a8314ec84 5cacfad2bb7979d7e823a92fb936c5929081e691
SHA256	ff15558085d30f38bc6fd915ab3386b59ee5bb655cbccbeb75d021fdd1fde3ac cafa8038ea7e46860c805da5c8c1aa38da070fa7d540f4b41d5e7391aa9a8079 1d84159252ed3fc814074312b85f62993e0476b27c21eec6cc1cc5c5818467e7
MD5	680ce7d56fc427ee2fbedb5baea59d68 1094aa25e2d637e7f5795edd6c0f60e4 5ffc255557796512798617ae61c4274d 3dde69212234c98b503081d64b9beb52 a44775e7568b790505bbcaadbd61c993 3649c106c6edd7ef47acd46586c74d8e c1bc20a9bbebbbdd19869999b9cec03b a06c125e6da566be67aacf6c4e44005e e776c4e24c00fa3eeba68cde38ae24f3 3dfb7626dbe46136bc19404b63c6d1dc 7be30062c1a2c42a7061dfbfec364588 93c19436e6e5207e2e2bed425107f080 2372c7639e70820f253a098dfcaf5060 aba68c4b4482e475e2d4b9bf54761b95 63c4c31965ed08a3207d44e885ebd5e4 a70d6bbf2acb62e257c98cb0450f4fec
IPV4	95[.]169[.]196[.]52 95[.]169[.]196[.]55
Domains	moses-staff[.]se abrahams-ax[.]nu abrahams-ax[.]se

References

https://www.secureworks.com/research/threat-profiles/cobalt-sapling

https://attack.mitre.org/groups/G1009/

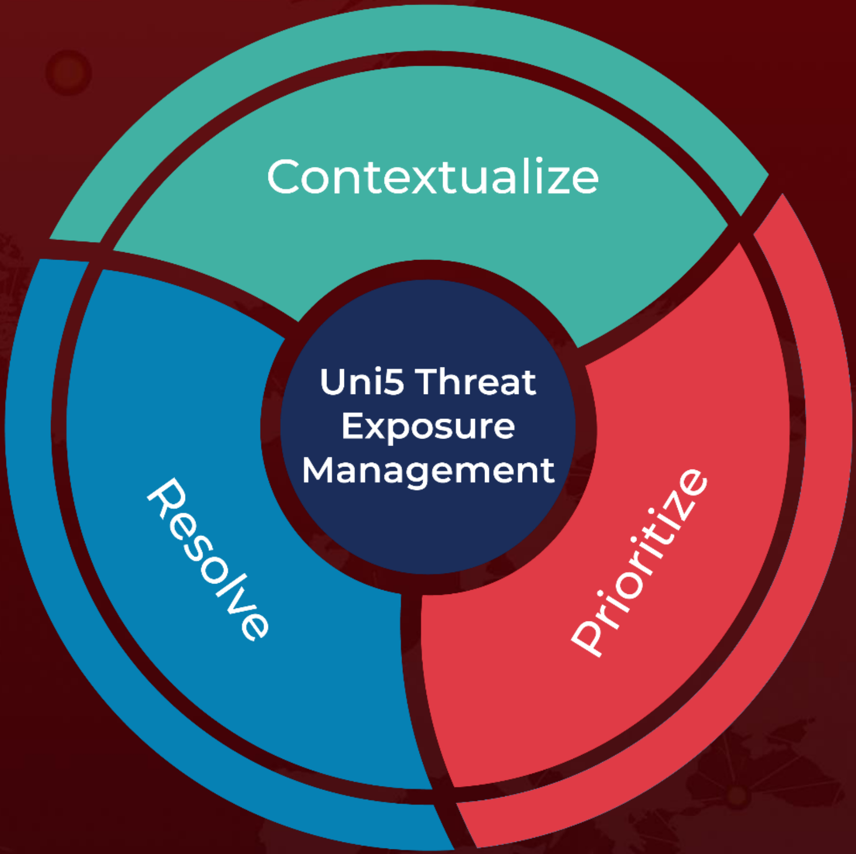
https://www.infosecurity-magazine.com/news/iran-cobalt-sapling-targets-saudi/

https://www.secureworks.com/blog/abrahams-ax-likely-linked-to-moses-staff

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 27, 2023 • 3:00 AM

More at www.hivepro.com