Abraham's Ax Likely Linked to Moses Staff

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

Counter Threat Unit Research Team

Both personas are likely operated by the Iranian COBALT SAPLING threat group. Thursday, January 26, 2023 *By: Counter Threat Unit Research Team*
Secureworks® Counter Threat Unit™ (CTU) researchers investigated similarities between the Moses Staff hacktivist group persona that emerged in September 2021 and the Abraham's Ax persona that emerged in November 2022. The analysis revealed several commonalities across the iconography, videography, and leak sites used by the groups, suggesting they are likely operated by the same entity. CTU™ analysis indicates that Abraham's Ax is another hacktivist group persona operated by the Iranian COBALT SAPLING threat group.

Abraham's Ax announced their existence and mission through social media channels such as Twitter posts on November 8, 2022. The group's iconography is reminiscent of Moses Staff (see Figure 1). The Moses Staff logo shows an arm extended from a sleeve holding a staff with a clenched fist. Abraham's Ax shows a clenched fist holding an axe from a different perspective. Both illustrations use a similar style.

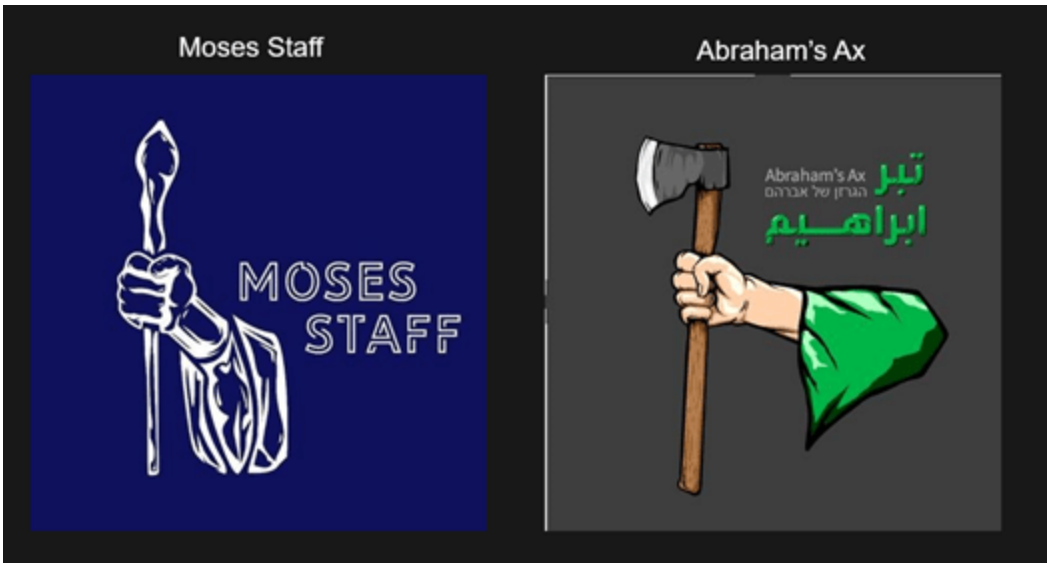

Figure 1. Comparison of Moses Staff and Abraham's Ax logos. (Source: Secureworks)

Abraham's Ax and Moses Staff use a WordPress blog as the basis for their leak sites. Although the overall aesthetics are different, there are clear connections in their operations. 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 sites provide versions

available via Tor websites, although the Abraham's Ax site appeared to be under construction at the time of analysis. Both use domains registered with EgenSajt . se (see Table 1).

Domain	Creation Date
Moses-staff . se	2021-09-09
abrahams-ax . nu	2022-10-14
abrahams-ax . se	2022-11-08

Table 1. Domains registered by Moses Staff and Abraham's Ax.

Although the threat actors registered .nu and .se domains that use the abrahams-ax name, the group appears to use the .nu version in promotional material (see Figure 2). The abrahams-ax . nu domain was registered approximately three weeks before the group emerged publicly.

Figure 2. Screenshot from video segment produced by Abraham's Ax. (Source: Secureworks)

CTU analysis of the hosting infrastructure for the Moses Staff and Abraham's Ax leak sites revealed that at early points in their lifecycles, both sites were hosted in the same subnet, nearly adjacent to each other (see Figure 3). This is highly unlikely to occur by coincidence and strongly indicates that the same entity chose to host the two sites in near contiguous IP address space.

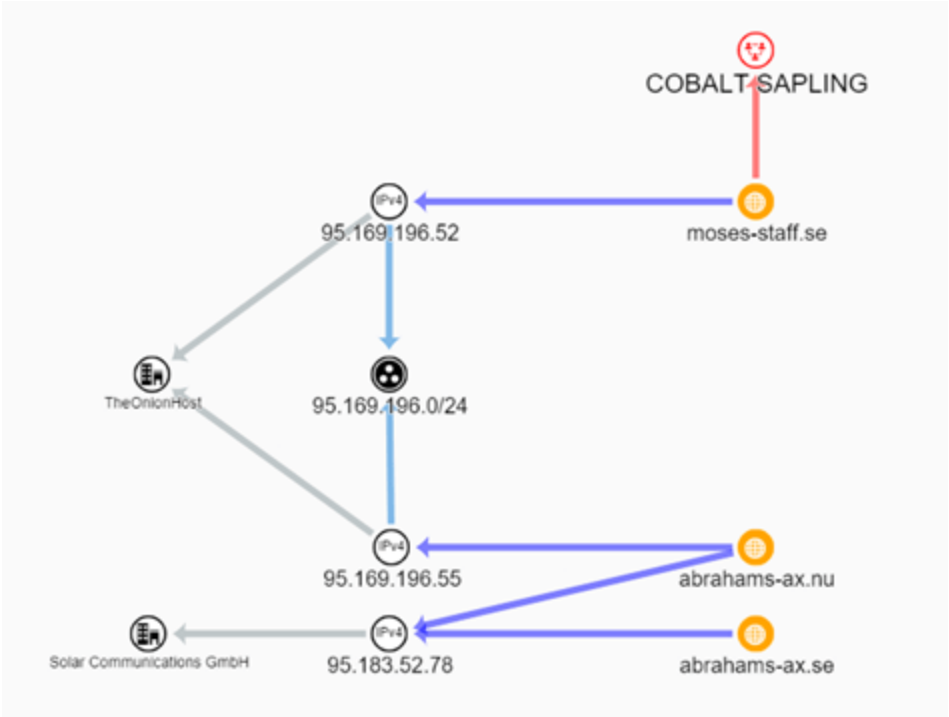

Figure 3. Infrastructure links between Moses Staff and Abraham's Ax. (Source: Secureworks)

Moses Staff 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." Moses Staff posted 16 "activities" to their site as of December 2. 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. Some of the intrusions have been confirmed, although it is likely that Moses Staff embellished the nature and extent of the compromises. The threat actors have reportedly used the custom PyDCrypt loader and DCSrv cryptographic wiper. DCSrv encrypts data using the open-source DiskCryptor library and installs a custom bootloader message. Although the wiper is styled as ransomware, the threat actors do not make a serious attempt to extort a ransom payment. The attacks appear to be politically motivated and focused on disruption and intimidation. The StrifeWater remote access trojan (RAT) (also known as brokerhost.exe) has also been linked to the group based on technical overlaps between intrusions, such as the use of the same customized ASPX web shells. An auxiliary tool named DriveGuard has been deployed alongside StrifeWater to monitor its execution. Malware artifacts indicate that COBALT SAPLING has been operating since at least November 2020 (see Figure 4), even though the Moses Staff persona did not emerge until September 2021.

```
MD5:            a70d6bbf2acb62e257c98cb0450f4fec
SHA-1:          5cacfad2bb7979d7e823a92fb936c5929081e691
SHA-256:        ff15558085d30f38bc6fd915ab3386b59ee5bb655cbccbeb75d021fdd1fde3ac
Path:           C:\Users\win8\Desktop\ishdar_win8\1\x64\Release\brokerhost.pdb
GUID:           6f5b12c0-d6be-48d8-a1b5-e2043909d139
Compile Time:   2020-11-28 20:46:24 UTC
```

Figure 4. Early StrifeWater RAT sample information indicating operations since at least November 2020. (Source: Secureworks)

Like Moses Staff, Abraham's Ax uses a biblical figure as the basis of their persona and includes religious quotes throughout their site. However, Abraham's Ax states they are operating on behalf of the Hezbollah Ummah. Hezbollah is a Lebanese Shia Islamist political party and militant group that is backed by Iran. Ummah refers to a Muslim community. As of this publication, there is no evidence to suggest that Abraham's Ax is linked to Hezbollah. Rather than attacking Israel directly, Abraham's Ax attacks government ministries in Saudi Arabia. They published sample data allegedly stolen from attacks on the Ministry of the Interior, along with a video that purportedly presents intercepted phone conversations between Saudi Arabian government ministers. The group may be attacking Saudi Arabia in response to Saudi Arabia's leadership role in improving relationships between Israel and Arab nations. In June 2022, media reports described secret talks regarding potential air defense collaborations, which Iran perceived as a significant threat to its interests in the region. Progress on normalization of relations between Saudi Arabia and Israel is fragile, and Iran may see these attacks as a way to discourage those efforts.

Moses Staff and Abraham's Ax have both produced and released videos as part of their operations. The videos often depict Hollywood-style hacking involving satellites, CCTV, 3D building models, and fast scrolling through documents allegedly stolen as part of their operations. Some videos depict multiple mobile phones combined with audio playback to suggest that mobile phone calls of senior government officials were intercepted. The video files released by the two groups show clear repetition and evolution of visual themes. The comparison of video screen captures in Figure 5 shows strong similarities between the groups. The Abraham's Ax videos use several of the same stock video elements used by Moses Staff but include additional visual embellishments. One odd addition to the background of Abraham's Ax videos is scrolling text taken from a 2015 news report on former British Prime Minister David Cameron visiting a factory in the UK. This selection appears incongruent with the visual theme and message of the overall campaign.

Figure 5. Similar screenshots from Moses Staff and Abraham's Ax videos. (Source: Secureworks)

The Abraham's Ax persona does not appear to be a direct replacement for Moses Staff. The Moses Staff leak site and Telegram channels remained active following Abraham Ax's emergence. In late November, Moses Staff claimed to have compromised a CCTV system that monitored the site of a terrorist attack in Israel, releasing previously unseen footage of the explosion. Malware and technical indicators from Abraham's Ax operations have not been identified. Assuming that both personas are operated by COBALT SAPLING, it is plausible that the threat actors use the same tools and techniques in their intrusions.

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 2. Note that IP addresses can be reallocated. The domains and IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
moses-staff.se	Domain name	COBALT SAPLING leak site (Moses Staff)
abrahams-ax.nu	Domain name	COBALT SAPLING leak site (Abraham's Ax)
abrahams-ax.se	Domain name	COBALT SAPLING leak site (Abraham's Ax)
95.169.196.52	IP address	Hosted COBALT SAPLING leak site (moses-staff.se)
95.169.196.55	IP address	Hosted COBALT SAPLING leak site (abrahams-ax.nu)

Indicator	Type	Context
ff15558085d30f38bc6fd915ab3386b5 9ee5bb655cbccbeb75d021fdd1fde3ac	SHA256 hash	StrifeWater RAT (agent4.exe)
5cacfad2bb7979d7e823a92fb936c592 9081e691	SHA1 hash	StrifeWater RAT (agent4.exe)
a70d6bbf2acb62e257c98cb0450f4fec	MD5 hash	StrifeWater RAT (agent4.exe)
cafa8038ea7e46860c805da5c8c1aa38 da070fa7d540f4b41d5e7391aa9a8079	SHA256 hash	StrifeWater RAT (calc.exe)
76a35d4087a766e2a5a06da7e25ef76a 8314ec84	SHA1 hash	StrifeWater RAT (calc.exe)
63c4c31965ed08a3207d44e885ebd5e4	MD5 hash	StrifeWater RAT (calc.exe)
1d84159252ed3fc814074312b85f6299 3e0476b27c21eec6cc1cc5c5818467e7	SHA256 hash	StrifeWater RAT (broker.exe)
7a5d75db6106d530d5fdd04332c68cd7 ccec287f	SHA1 hash	StrifeWater RAT (broker.exe)
aba68c4b4482e475e2d4b9bf54761b95	MD5 hash	StrifeWater RAT (broker.exe)

Table 2. Indicators for this threat.

Read more about Iranian threats in the 2022 State of the Threat report. If you need urgent assistance with an incident, contact the Secureworks Incident Response team.

Stay Informed

Get the latest in cybersecurity news, trends, and research

SEND ME UPDATES

Secureworks Taegis™

Security Analytics +
Human Intelligence
Delivers Better
Security Outcomes

About Taegis

Latest Report

Reports

2022 State of the Threat Report