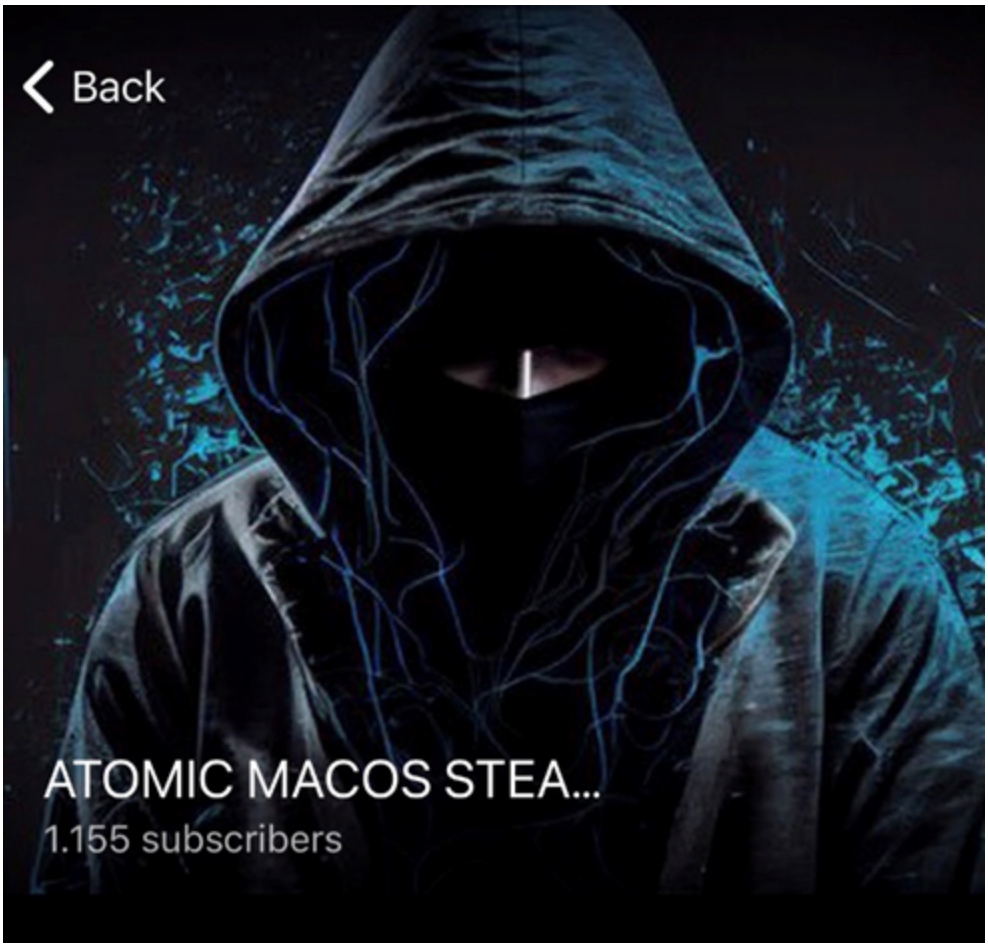
Silent Echoes: The Hidden Dialogue among Malware Entities — Spotlight on AMOS InfoStealer

denshiyurei.medium.com/silent-echoes-the-hidden-dialogue-among-malware-entities-spotlight-on-amos-infostealer-6d7cd70e3219

Denshi Yūrei May 14, 2023



Denshi Yūrei

--

On April 26th, Cyble, a threat intelligence provider, released an article discussing a new infostealer called AMOS, which targets Mac devices. Intrigued by their findings, I conducted a personal investigation and gathered more information about AMOS infostealer. Initially, I planned to conduct a technical analysis of the stealer and its infrastructure. However, delving deeper into AMOS, I decided to shift the main focus and present the analysis of the threat actors behind the stealer instead. As you go with me on this journey, I hope you don’t get lost in my thought process. Let’s go.

I started my investigation by locating the Telegram channel where the stealer was advertised. The first Telegram channel was created on April 9th and has 366 subscribers. However, on April 29th, the admin of the channel declared that they were leaving the project, transferring ownership to the user **@ping3r** and a new coder, adding that he leaves it up to the users to decide how to view it — as a selling point or circumstance. Later the same day, the second channel related to AMOS was created, which currently has 1155 subscribers and where the contact person is referenced as **@ez360x** (I presume this is a new coder).Additionally, a support group was created, which currently has only 15 members. Interestingly, when I saw the new channel, what struck me first was the channel's avatar (see Figure 1). I couldn't get over the feeling that I had seen this avatar somewhere before. I did some searching, and voila — I found it.

Maybe XORacle?

The profile image is similar to the avatar of the malware development team — **XORacle**, which offers malware development services on one of the most popular Russian-speaking forums (see Figure 2). **XORacle** mentions in their advertisement that they have expertise in developing various types of malware, including RATs, Stealers, Clippers, and Loaders, using Rust and Go programming languages (AMOS was written in Go). They also offer malware development services for macOS. Coincidence or not, at this point I can only speculate about the potential relation of XORacle to AMOS.

Possible connection to WhiteSnake stealer

Going back to Telegram, I browsed through the AMOS support group and noticed that out of fifteen members, one of them was named **@WhiteSnake** (see Figure 3).WhiteSnake is a stealer that emerged on the market in February 2023, targeting Windows and Linux operating system users. The user @WhiteSnake was an admin of the Telegram channel advertising WhiteSnake stealer.

Further, WhiteSnake is present on the Russian-speaking forum. While browsing through it, I noticed that WhiteSnake asked a user to message them privately in response to their question about the development of a macOS stealer (see Figure 4). Furthermore, on March 17th, our user posted an interesting statement, citing — "*Here lives Uzbek*"(see Figure 5), which suggests that the user may be originally from Uzbekistan (remember this detail!).

Figure 5. WhiteSnake's profile on Russian-speaking web forum.
As I continued investigating, the next step was to check whether the stealer was advertised elsewhere on Telegram. Lucky me — it was. Although in my earlier examination (two weeks ago), I identified at least seven instances of AMOS advertisements on the various channels, I noticed that earlier advertisements were removed from most channels except for one. Accident or not, it was still there. It was necessary since the earlier advertisements contained

a critical element — mentioning of another person associated with a channel — a user removed later from all the posts on the channel — **@line_liner** (see Figure 6).Could **@line_liner** be the primary coder of AMOS? Well, yes.

So, right now we have three profiles of interest:**@ping3r, @line_liner and @ez360x.** Let's look into each and every one of them individually to see what we can find.

User 1: ping3r (Role — AMOS owner)

The first user of interest is **@ping3r**, who is the present owner of the AMOS stealer. After conducting some research, I found out that **@ping3r** is the owner of the private forum COOKIE.PRO, which has been active since 2018. To join the forum, interested parties must pay a fee ranging from $150 for users to $250 for sellers. The website also has a Telegram group with 3,633 members, where **@ping3r** is referred to as the admin(see Figure 8). Additionally, **@ping3r** serves as an escrow on the forum COOKIE.PRO. The forum advertises several familiar infostealers, including WhiteSnake and Titan.

Figure 7. Atomic macOS advertisement on the COOKIE.PRO website
Figure 8. Screenshot of COOCKIE.PRO Telegram group.

User 2: line_liner (Role — AMOS developer)

The next person of interest is **@line_liner**, who I believe was an admin of the first channel and a coder behind AMOS, and the mentioning of who was erased after the ownership of the stealer was transferred to another person. When I checked the Telegram of **@line_liner**, I noticed an interesting detail in their profile picture: a traditional Uzbek hat called Tubeteika (see Figure 9). This makes me think there might be a connection between **@line_liner** and the WhiteSnake developer. What if they are the same person? Intriguing, right?

User 3: ez360x (Role — new coder)

Lastly, **@ez360x**, new coder. Unfortunately, I found nothing about this user, but he seems to be a "no less popular coder". Could it be previously mentioned XORacle? At this point, I can only guess.

Was it Titan after all?

As I delved deeper into the investigation for this article, I uncovered some additional interesting information which contradicts or supports my previous statements. On May 11th, a Telegram channel called Abbadon posted that on March 18th, the developer of Titan Stealer ceased working on it and sold it to Aurora (another info-stealer). Additionally, it was mentioned that Aurora, who now owns Titan Stealer, focused entirely on operating Titan, ceasing all Aurora operations as of May 1st. Furthermore, according to the information in the

channel — the original developer of Titan started working on developing Atomic macOS Stealer (AMOS), which was later sold to a user named **@ping3r** (see Figure 11). Abbadon shared a screenshot of forwarded messages from **@ping3r** indicating the purchase of AMOS from Titan (see Figure 10).

Conclusion

Although Abaddon's post, in a way, disproves my initial belief that WhiteSnake is the one who developed AMOS, there is no solid evidence to state that they are not. What if WhiteSnake and Titan are the same people, after all? I don't know it, but working on this investigation and having the AMOS as a case study shows the tight interconnectedness between the users behind the development of malicious software. There is a high chance that the same person or team (like XORacle) might be behind several malicious software that we know under different names. I won't be surprised if they operate under the name of a legitimate software company with an office, regular working hours and a coffee machine standing in the corner. I hope you enjoyed being on this journey with me. See you!