CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

June 17, 2024

The Travels of “markopolo”: Self-Proclaimed Meeting Software Vortax Spreads Infostealers, Unveils Expansive Network of Malicious macOS Applications

Vortax, a self-proclaimed virtual meeting software, proliferates infostealer malware at scale in a cross-platform campaign targeting cryptocurrency users on social media.

Further investigation into Vortax revealed a sprawling infostealer operation, attributed to the Atomic macOS Stealer (AMOS) user "markopolo" — previously identified targeting Web3 gaming.

"markopolo" is an agile, adaptable, and versatile threat actor that quickly pivots their scams upon detection, which is likely indicative of a long-term credential harvesting strategy.

Analysis cut-off date: May 15, 2024

Executive Summary

While monitoring data in Recorded Future Malware Intelligence, Insikt Group identified purported virtual meeting software called Vortax that, upon download and installation, delivers three information stealers (“infostealers”) in cross-platform attacks — Rhadamanthys, Stealc, and, most notably, Atomic macOS Stealer (AMOS) — in an extensive campaign aimed at cryptocurrency theft. AMOS typically has a niche client base because of its high barrier to entry, its low success rate, and the lower demand for macOS infostealers in the cybercriminal underground. AMOS is not often observed in the wild, relative to its Windows-based counterparts, which makes observing such extensive activity around AMOS, including diverse scams, targets, and infrastructure in a single campaign, particularly noteworthy. This campaign, operated by the threat actor tracked as “markopolo”, and its wide-ranging implications also likely signal that future AMOS campaigns will employ similar tactics to spread — resulting in a long-term increase in the volume of AMOS victims.

While macOS stealers are generally less popular than their Windows counterparts, demand is growing, evidenced by an increase in macOS infostealer submissions to Recorded Future Malware Intelligence and an increased volume of references to macOS malware on the dark web. The high volume of AMOS activity observed in this campaign builds on previous Insikt Group reporting, which found that mentions of macOS malware and exploit kits increased by 79% year-on-year from 2022 to 2023, which may indicate a correlation between the overall number of references to macOS malware and the increased frequency of AMOS campaigns observed in the wild (1, 2).

Upon further investigation of the Vortax application, its network of associated accounts, and the malware it deployed, Insikt Group identified 23 other malicious macOS applications masquerading as legitimate — with the majority of scams identified targeting virtual meeting software and cryptocurrency users. We also identified connections between the “Vortax campaign” and a previous infostealer campaign targeting Web3 gaming projects. Based on these findings, we are confident that the two campaigns are affiliated with the same threat actor — previously identified by Insikt Group as using the AMOS UserID “markopolo”. Given its tight-knit community, we assess that other operators of AMOS will likely model future campaigns after the success of markopolo. This may result in a wider proliferation of AMOS in the wild, accompanied by diverse and wide-ranging campaigns attributed to individual threat actors, exacerbating the long-term threat of a less secure landscape for macOS users.

The Vortax campaign identified in this report is a classic example of the adaptive and scalable nature of malware operations. Given the widespread proliferation of AMOS and the diversity of scams identified in this report, we assess that defenders must consider in-house active security controls that limit an end user’s ability to download unapproved “freemium” software, which is the primary vector employed in this campaign. Blocking all downloads represents a short-term fix, though this will likely be difficult to sustain at scale. Longer-term mitigations will require processes to help vet software products to ensure legitimacy, so as to avoid user execution and an AMOS infection. Once AMOS is on a victim’s system, it

is difficult to detect and monitor due to its “smash-and-grab” nature; therefore, preventive measures must prioritize controlling such activity prior to an infection.

The ability of threat actors like markopolo to pivot their operations and maintain campaign continuity, often on a moment’s notice, poses a significant brand impairment threat to organizations without visibility into, and the capacity to cluster, these campaigns. As with the Web3 campaign referenced above, organizations should seek to insulate themselves from potential impersonation scams and the potential reputational damage of such scams. As we have identified markopolo impersonating several legitimate software downloads (such as “Zoom”, in **Table 4**), we note that organizations should be aware of infostealer operators impersonating their brands to deliver malware. Aside from a risk to legitimate brands, organizations should understand that infostealer infections have follow-on operational and financial consequences.

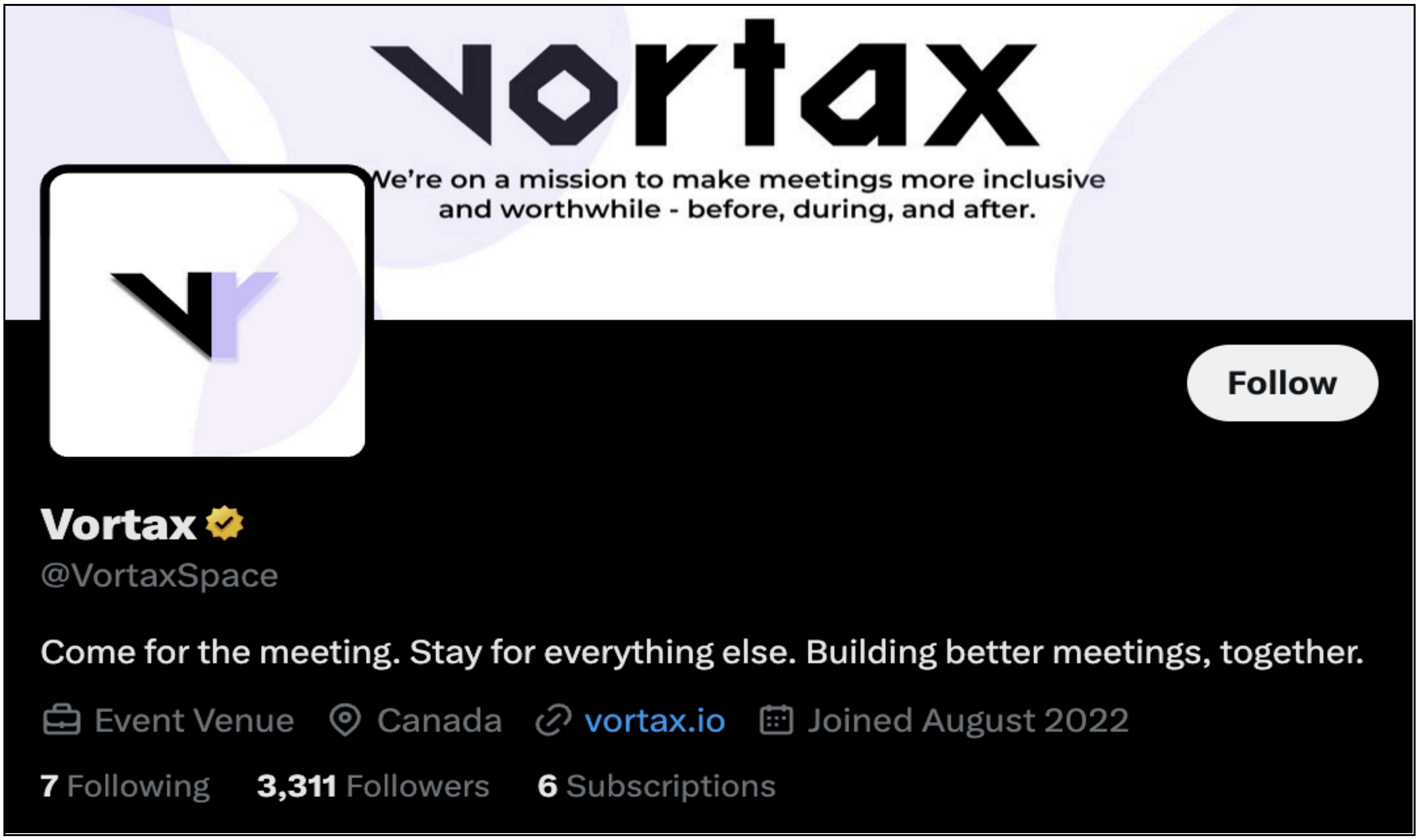
Key Findings

- Insikt Group identified a malicious application on social media called Vortax that is connected to multiple ongoing scams targeting macOS users. The campaign detailed in this report has connections to a campaign previously reported by Insikt Group (“Cybercriminal Campaign Spreads Infostealers, Highlighting Risks to Web3 Gaming”), suggesting that the same threat actor operates both campaigns. This also suggests that the threat actor has broadened the scope of its operations and expanded its targeting beyond Web3 gaming to masquerading as virtual meeting applications that primarily target cryptocurrency users.
- The threat actor that operates this campaign, identified as markopolo, leverages shared hosting and C2 infrastructure for all of the builds (**Table 4**) identified in this report. This suggests that the threat actor relies on convenience to enable an agile campaign, quickly abandoning scams once they are detected or producing diminishing returns, and pivoting to new lures.
- This scaled campaign is likely indicative of a widespread credential harvesting operation, which could imply that markopolo acts as an initial access broker (IAB) or “log vendor” on a dark web shop, such as Russian Market or 2easy Shop; however, we have no evidence to make that assessment, as of this writing.

Threat Analysis

Vortax is a self-proclaimed virtual meeting software — marketed as a cross-platform and in-browser enterprise-focused alternative to other video chat services — that leverages artificial intelligence to generate meeting summaries and action items and suggest questions or comments with its “MeetingGPT” product. Vortax is indexed by all major search engines and is primarily active on social media (@VortaxSpace), but also maintains a Medium blog (*medium[.]com/@vortax*) with approximately 22 suspected AI-generated articles published between December 7, 2023, and December 16, 2023. Vortax claims to operate out of a physical office (1100 King Street West, Toronto, Ontario, Canada), which is actually the physical address of an apartment building. Vortax claims to have received awards from technology publications (such as *Forbes*) and boasts endorsements from Fortune 500 companies (such as Uber), but there is no evidence to corroborate such claims. At first glance, Vortax appears to be a legitimate software company; however, upon deeper investigation, every aspect of its "brand" is misleading. This includes its official websites — *vortax[.]io* and the now-suspended *vortax[.]space* — which are rife with spelling and grammatical errors (for example, "Comming Soon").

Vortax perpetuates the spread of infostealer malware via phishing on social media. While Vortax advertises applications for Windows, Linux, macOS, iOS, and Android on its website, users cannot actually download said applications without a "Room ID". Room IDs function as meeting invitations and are spread in targeted replies and direct messages (DMs) sent from social media accounts likely controlled by Vortax's threat actors. These replies and DMs are in response to cryptocurrency-related topics, which implies that a primary goal of this campaign is cryptocurrency theft.



vortax

We're on a mission to make meetings more inclusive and worthwhile - before, during, and after.

Follow

Vortax

@VortaxSpace

Come for the meeting. Stay for everything else. Building better meetings, together.

Event Venue Canada vortax.io Joined August 2022

7 Following 3,311 Followers 6 Subscriptions

Figure 1*: Vortax account on social media; the checkmark icon indicates that Vortax is designated as a "Verified Organization" on the platform (Source: Recorded Future)*

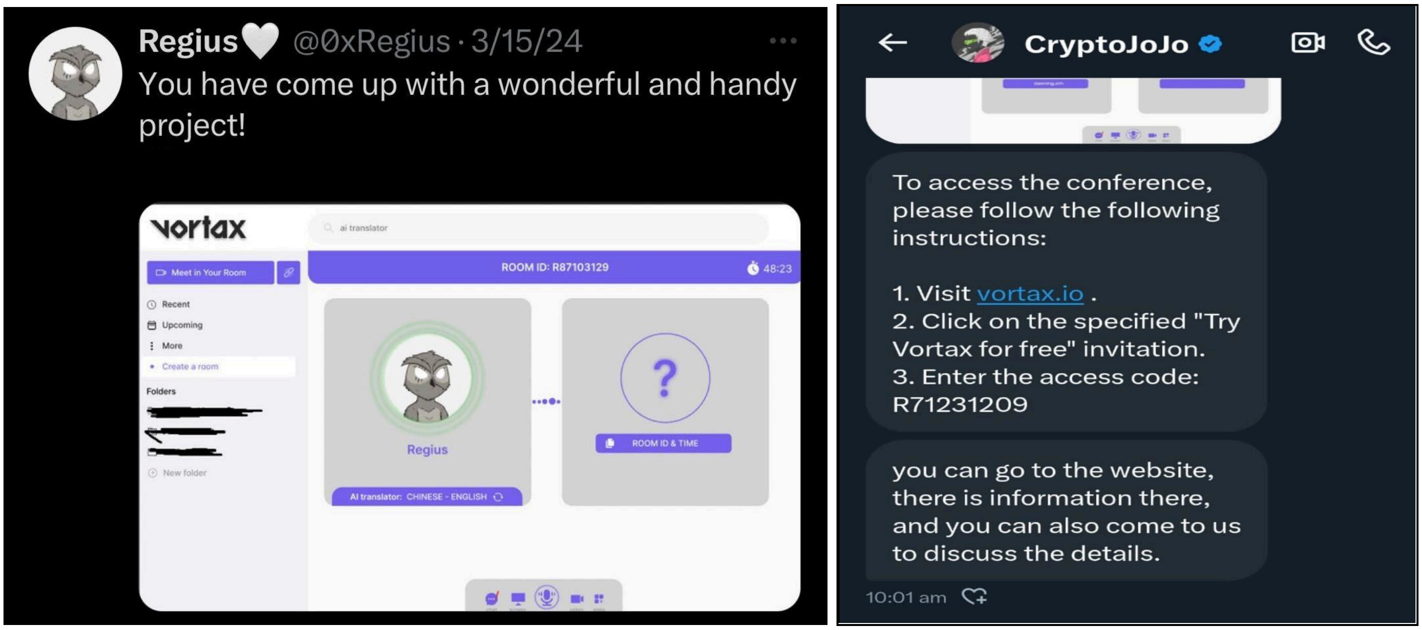
Domain	ASN	First Seen	Last Seen	Status
vortax[.]io	AS-REG, RU (AS197695)	2024-03-01	2024-05-15	Vortax homepage
vortax[.]app	AS-REG, RU (AS197695)	2023-12-17	2024-05-15	Vortax homepage
vortax[.]org	AS-REG, RU (AS197695)	2023-02-14	2024-05-15	Parked domain, no content
vortax[.]space	AS-REG, RU (AS197695)	2024-01-04	2024-05-15	Domain suspended as of May 15, 2024

***Table 1**: Vortax hosting information (Source: Recorded Future)*

Accounts associated with Vortax have four primary methods for sharing Room IDs, which lead to infostealer infections:

- Replies to the Vortax account on social media
- Direct messages on social media
- Posting in cryptocurrency-related Telegram channels
- Posting in cryptocurrency-themed Discord channels

There is overlap in naming, profile pictures, content, and shared Room IDs between the accounts that reply to the Vortax social media account and those active on other sources, indicating that these accounts are likely connected and operated by Vortax's operators.



Regius🤍 @0xRegius · 3/15/24

You have come up with a wonderful and handy project!

CryptoJoJo

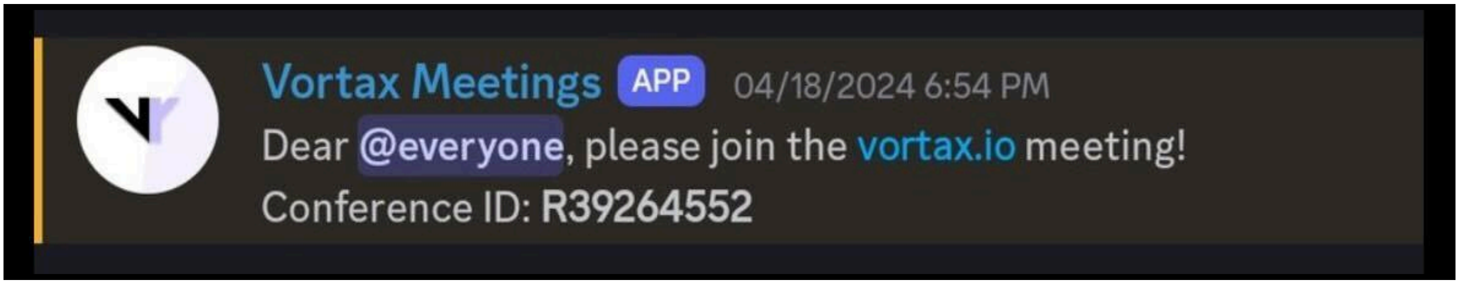
To access the conference, please follow the following instructions:

1. Visit vortax.io .
2. Click on the specified "Try Vortax for free" invitation.
3. Enter the access code: R71231209

you can go to the website, there is information there, and you can also come to us to discuss the details.

10:01 am

***Figure 2**: Social media account sharing a Room ID in the replies of a Vortax post (Left); Social media account sending a direct message to a cryptocurrency-related account with a different Room ID (Right) (Source: Recorded Future)*

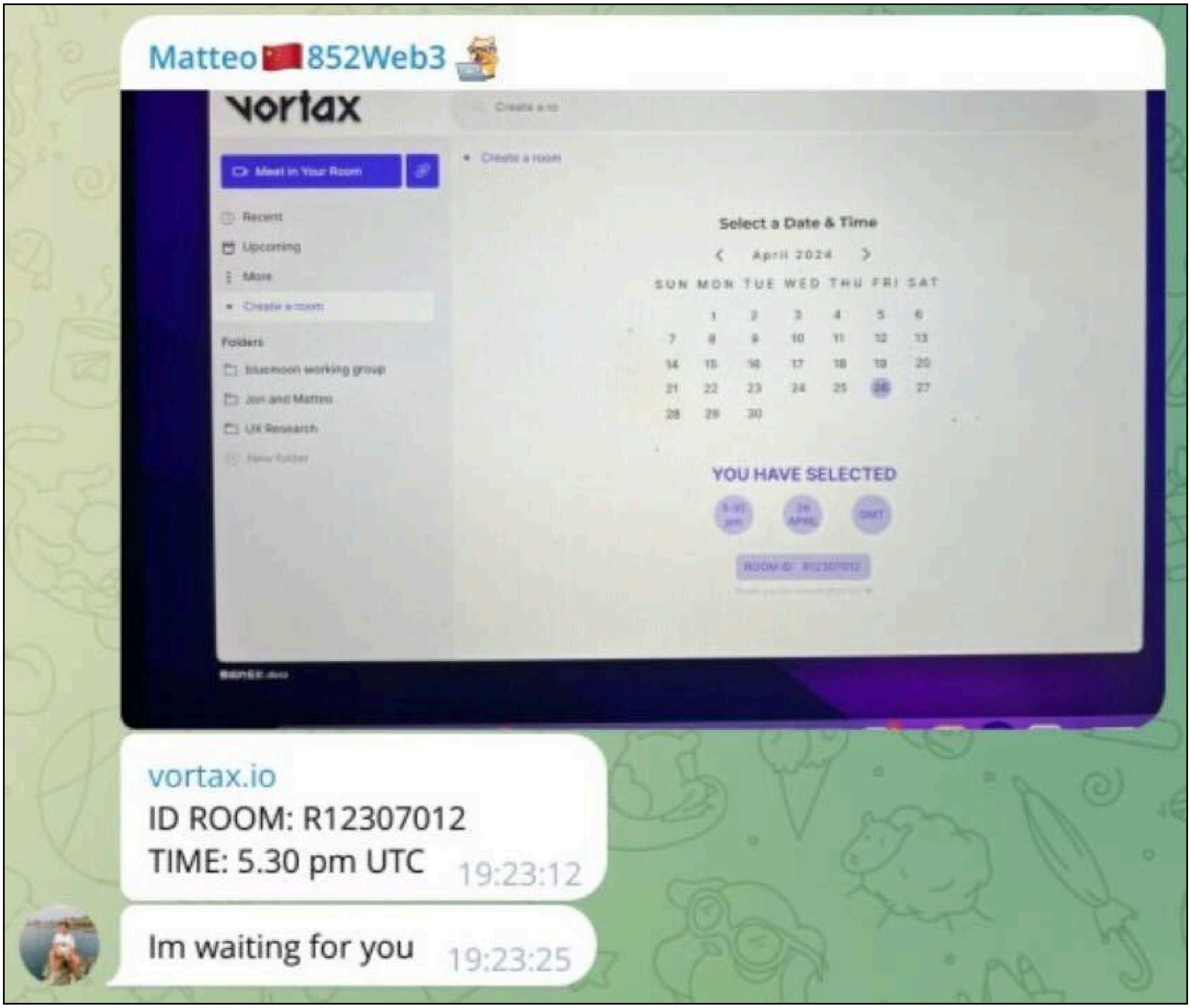


Vortax Meetings APP 04/18/2024 6:54 PM

Dear @everyone, please join the vortax.io meeting!

Conference ID: R39264552

***Figure 3**: Automated "Vortax Meetings" application on Discord sharing a unique Room ID (Source: Recorded Future)*



Matteo 🇨🇳 852Web3

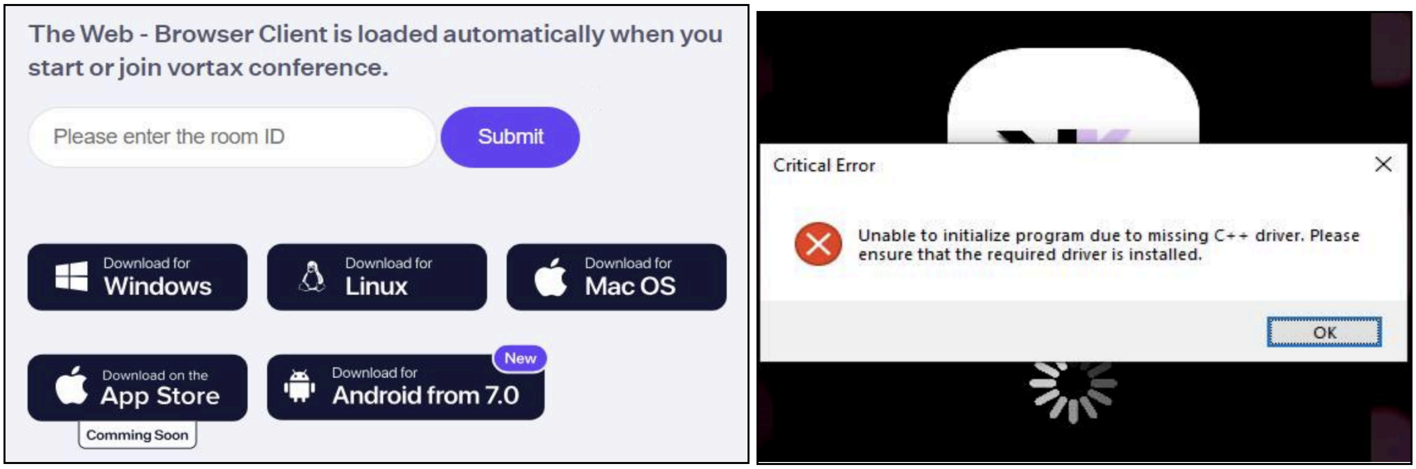
vortax.io
ID ROOM: R12307012
TIME: 5.30 pm UTC 19:23:12

Im waiting for you 19:23:25

***Figure 4**: Account on Telegram sharing a unique Room ID in a cryptocurrency-related public channel (Source: Recorded Future)*

The most common Room IDs identified by Insikt Group were R12307012, R39264552, R87103129, and R71231209. All of the Room IDs, when entered into the Vortax website, redirect the user to a Dropbox link (Windows) or external website (*plumbonwater[.]com*) (macOS) that downloads the Vortax installer. Upon entering the Room ID, if one of the above codes is entered incorrectly, or is invalid, the following response occurs:

- The page runs a PHP script located at "hxxps://vortax[.]io/assets/php-back/check-code.php"
- The script returns the response "\u041a\u043e\u0434 \u043d\u0435 \u0437\u043d\u0430\u0439\u0434\u0435\u043d\u043e"
- This response decodes to "Код не знайдено" ("Code not found")



The Web - Browser Client is loaded automatically when you start or join vortax conference.

Critical Error

Unable to initialize program due to missing C++ driver. Please ensure that the required driver is installed.

Figure 5*: Vortax download prompt, which requires the user to input a Room ID to download the software (Left); Vortax client claiming that it experienced a "critical error" related to a "missing C++ driver" (Right) (Source: Recorded Future)*

According to Recorded Future Malware Intelligence, behavioral analysis of the Vortax installers on Windows and macOS indicates that `Vortax App Setup.exe` and `VortaxSetup.dmg` deliver Rhadamanthys and Stealc, or AMOS, respectively (**Table 2**). As seen in **Figure 5**, the Vortax installer on Windows and macOS never actually launches the purported Vortax application, claiming that it encounters critical errors that impede it from running; however, in the background, Vortax is running many malicious processes.

Filename	Size	Malware Tags	SHA256 Hash
Vortax App Setup.exe	47.3 MB	Rhadamanthys, Stealc	f3176e0859ba92049dcd57685c1b5f49b97183ff49fcc79f2ce4ad2b31d2d843
VortaxSetup.dmg	498 KB	AMOS	c34f8b6a299dd867a8d00b4fc50d91d9fdde4aa36f7c2a444aab4601dd4238e1

Table 2*: Malicious Vortax installers on Windows and macOS (Source: Recorded Future)*

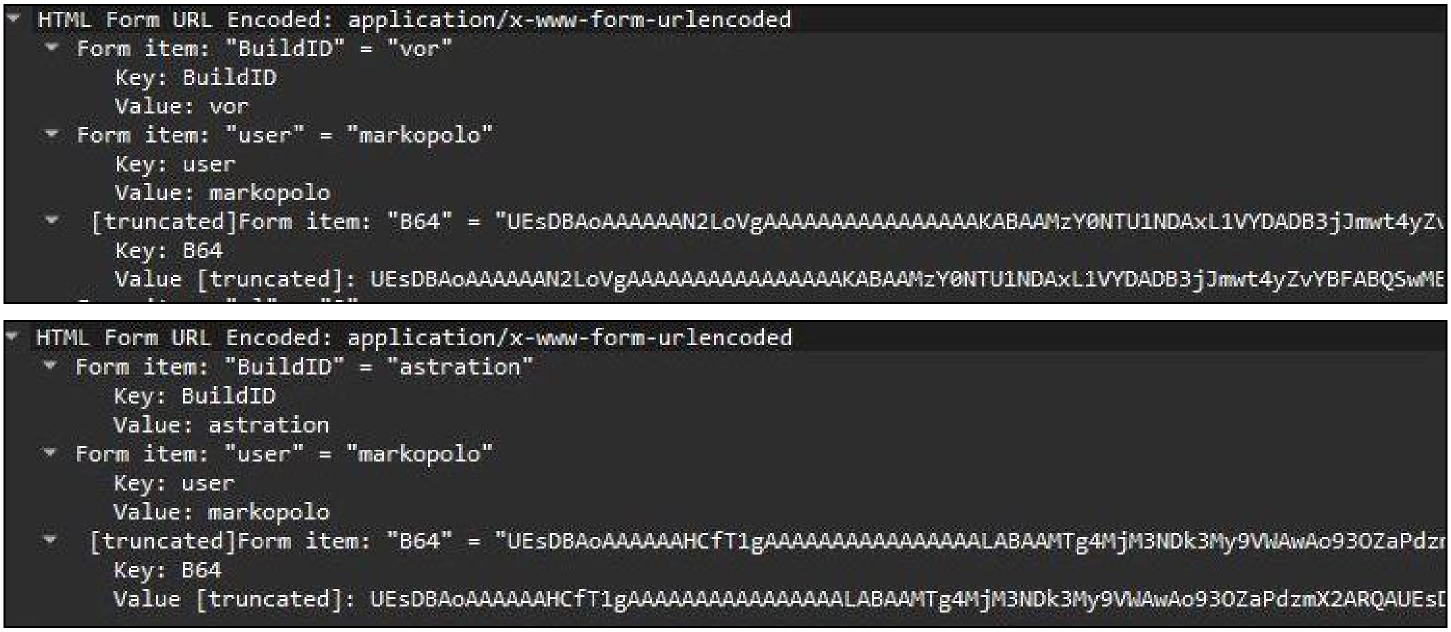
The Windows executable for the Vortax installer is hosted at `www[.]dropbox[.]com/scl/fi/3jknhxkr2kwqfrw8l0ccc/Vortax-App-Setup.exe?rlkey=xvlalsdjdvuac1bp4643ry6iz&st=ck9api5p&dl=1`. As shown in **Table 3**, the macOS version of the Vortax installer is hosted on a separate external link.

Domain	IP Address	ASN	Note
plumbonwater[.]com	79.137.197[.]159	AEZA-AS, GB (AS210644)	Hosts and communicates with `VortaxSetup.dmg`
showpiecekennelmating[.]com	185.193.126[.]25	CYBERDYNE, LR (AS37560)	Communicates with `Vortax App Setup.exe` following download from Dropbox

***Table 3**: Vortax installer infrastructure (Source: Recorded Future)*

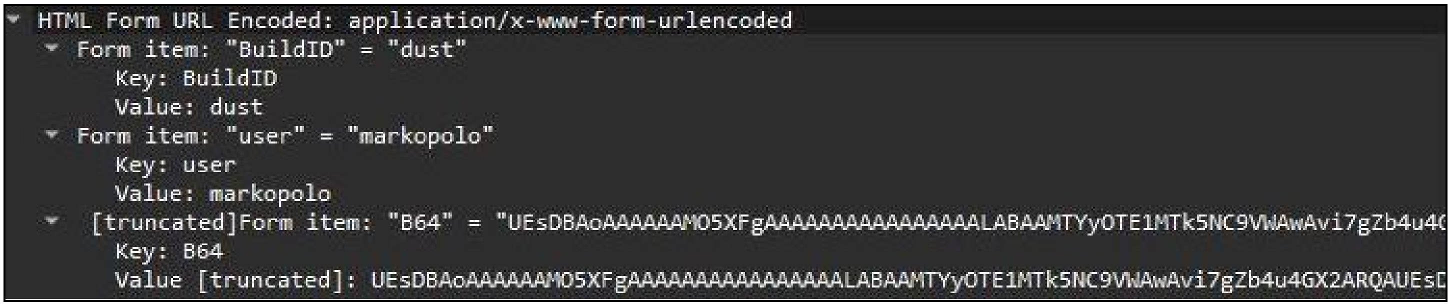
After installing Vortax, the Windows version of the application communicates with *showpiecekennelmating[.]com* before connecting to a likely C2 server — *89.105.198[.]134*. This IP address hosts *casino-legrand[.]info*, which resolves to a FASTPANEL administrative panel login, as of May 3, 2024. This panel is likely controlled by markopolo. The macOS version of Vortax communicates with *193.233.132[.]137*, which is likely an AMOS C2. While the AMOS C2 is based in Moscow, Russia, it uses a different hosting provider (SUNHOST-AS, GB; AS216319) than observed in previous AMOS campaigns (SERVER4-AS, RU; AS210352). We assess that AMOS's operators may have moved on from primarily leveraging SERVER4-AS.

Using Recorded Future Malware Intelligence, Insikt Group was able to identify connections between the AMOS build associated with Vortax and a previous AMOS campaign targeting Web3 gaming projects; the latter is detailed in the public Insikt Group report "Cybercriminal Campaign Spreads Infostealers, Highlighting Risks to Web3 Gaming". The BuildIDs associated with two of the fraudulent Web3 projects in the previous campaign, Astration (`astration`) and Dustfighter (`dust`), are associated with the user "markopolo". This user is attributed to the BuildID of Vortax (`vor`) (**Figure 6**).



```
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "BuildID" = "vor"
      Key: BuildID
      Value: vor
  ▾ Form item: "user" = "markopolo"
      Key: user
      Value: markopolo
  ▾  [truncated]Form item: "B64" = "UEsDBAoAAAAAAN2LoVgAAAAAAAAAAAAAAAAKABAAMzY0NTU1NDAxL1VYDADB3jJmwt4yZv
      Key: B64
      Value [truncated]: UEsDBAoAAAAAAN2LoVgAAAAAAAAAAAAAAAAKABAAMzY0NTU1NDAxL1VYDADB3jJmwt4yZvYBFABQSwME
```

```
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "BuildID" = "astration"
      Key: BuildID
      Value: astration
  ▾ Form item: "user" = "markopolo"
      Key: user
      Value: markopolo
  ▾  [truncated]Form item: "B64" = "UEsDBAoAAAAAAHCfT1gAAAAAAAAAAAAAAAALABAAMTg4MjM3NDk3My9VWAwAo93OZaPdzr
      Key: B64
      Value [truncated]: UEsDBAoAAAAAAHCfT1gAAAAAAAAAAAAAAAALABAAMTg4MjM3NDk3My9VWAwAo93OZaPdzmX2ARQAUEsD
```



```
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "BuildID" = "dust"
      Key: BuildID
      Value: dust
  ▾ Form item: "user" = "markopolo"
      Key: user
      Value: markopolo
  ▾  [truncated]Form item: "B64" = "UEsDBAoAAAAAAM05XFgAAAAAAAAAAAAAAAALABAAMTYyOTE1MTk5NC9VWAwAvi7gZb4u4G
      Key: B64
      Value [truncated]: UEsDBAoAAAAAAM05XFgAAAAAAAAAAAAAAAALABAAMTYyOTE1MTk5NC9VWAwAvi7gZb4u4GX2ARQAUEsD
```

***Figure 6**: Evidence indicating that the AMOS user markopolo is affiliated with the Vortax campaign, as well as the previously identified Astration and Dustfighter campaign (Source: Recorded Future)*

Further investigation of the Vortax staging domain *plumbonwater[.]com* (**Table 3**) revealed 23 additional domains hosted on the same IP address (*79.137.197[.]159*). Using Recorded Future Malware Intelligence, Insikt Group identified that each of these domains hosts a malicious application that delivers AMOS. Investigation into these malicious applications unearthed additional scams — similar to Vortax, described above — that masquerade as legitimate companies and leverage social media and messaging platforms to target cryptocurrency users. These scams, such as VDeck and Mindspeak, share crossover with the Vortax brand and are likely operated by the same threat actor — markopolo.

Investigation into the UserIDs associated with each AMOS build identified in this network shows that all of them are affiliated with the markopolo user, identified in previous Insikt Group investigations and shown in **Figure 6**.

Table 4 provides a complete list of malicious applications, their file names and BuildIDs, and links to Recorded Future Malware Intelligence. None of the domains below have been previously reported.

Domain	Filename	BuildID	SHA256
plumbonwater[.]com	`VortaxSetup.dmg`	`vor`	c34f8b6a299dd867a8d00b4fc50d91d9fdde4aa36f7c2a444aab4601dd4238e1
weworkhappy[.]com	`VDeckSetup.dmg`	`cloregod`	b1817f23b4b0b09cd7db9e90eac166ddf0de9d22aaf69f17308da43854604d9e
marylandhomerates[.]com	`Installer.dmg`	`meowsup`	5d45cc81a22e6ba596b12db4baec5b20ccbe9ce52f8258fa5690da0e5ef2a982
novatercaagilidade[.]com	`ZoomInstaller.dmg`	`private1`	bde29a5215e685805f00fee5f03de3478f8214195ecf93fb81562bcd6122149d

123mllhasbrasil[.]com	`Launcher.dmg`	`wioland`	f9785743539fdfb2199b53be57f86d5dba5c0cd3dfad1130de1532f92e0c7c4f
garagemfinity[.]com	`Installer.dmg`	`xmas`	N/A; down as of May 15, 2024.
institutoangelabatista[.]com	`SpectraLauncher.dmg`	`DoraLands2`	856979042a3c1f61050cc08e8f11856dc714ec16969bd0fc562fd47c9e6c8e4c
betbhaibetting[.]com	`PartyLauncher.dmg`	`meowparty`	be7e5707e5e399aedcfb2800d7039ff050500be3bafd217ca9200abed8bef03f
ebolight[.]com	`Setup.dmg`	`RobinL`	750baf928763a60343f8d48e45c4a4ca8da1243add410821b51484242571d089
aidigibrain[.]com	`Launcher.dmg`	`meowparty`	8fb5de2498e48338825253f9d165986403661003393278d93cb35f5f9a1549dc
repairleatherla[.]com	`Setup.dmg`	`lumary`	05219c02d66daad246eab2abccc35384c34f17ce1daa2fee21cf0bfee88e31b2
msjessd[.]com	`Installer.dmg`	`RobinL`	5d6075e33a168dfa44492dbec5462c6142399b708ec0d038e3e1869141e6b378
iuddy[.]com	`Setup.dmg`	`vexor`	9f676511cb9b35e2916ebf79aec6b4aa6514f8bf640ea2fe786d16a7ed8dab7b
indianahomerates[.]com	`WorldLauncher.dmg`	`private`	93463142e354b05bbac20b9e9498ee5f8c9ea2488151ee6870189baab0b7e2ff
pegamente[.]com	`Setup.dmg`	`ELHA`	922afb7de0159e7b435290868c51f33c59e0990ec964f77de9201534e4232117
nongduangmarket[.]com	`WorldLauncher.dmg`	`private`	4b35a3872589f44c43469cf73c54b525506f6cc894598d109c5f931923c6eba9

crosstacks[.]com	`Launcher.dmg`	`dust`	8e6176eaea919bae5b75000244474d8310a7b8d59806fca133d78f5343839d76
tripleplay-arg1[.]com	`Setup.dmg`	`FriendsCompany`	9e5dc9028d4a404bf3d7aa412c58cfe8ece0da23c4f3f338e05b34198d9c1afe
xhaxo[.]com	`Setup.dmg`	`FriendsCompany`	7225d5fde4daa4552daf67a0ac2f6d7ec0e768536c5377ee3e7beaa04603a6f5
assetsreserve[.]com	`NortexApp.dmg`	`sneprivate`	7f6f85e1ae4186edc9bf821943893b183a6a9252b0899d682c1899201dffc496
eliteneatproductshop[.]com	`Launcher.dmg`	`xmas`	73c099168755acbc793675a5e64ca719f909cd1943db5757af96b2c1c79ae6d8
piloje[.]com	`Installer.dmg`	`heard`	eb74c9dd0a0e3ea3cb31338c55e9e630fdee964a7b5967efcdfa8daa26a0f129
faruvinnovations[.]com	`NightVerseSetup.dmg`	`NIGHT`	dee705f4a513081afe9ab682b832068ac558ad3145038e57edc8109ab0e80769

***Table 4**: Malicious applications that deliver AMOS and are associated with the Vortax campaign and tied to markopolo (Source: Recorded Future)*

All of the AMOS builds in **Table 4** are unique, previously unreported, and associated with the markopolo user. BuildIDs that we found to be duplicative, in this and previous campaigns, include `xmas`, `dust`, `meowparty`, and `RobinL`.

Analysis of the above domains also unearthed additional infrastructure associated with AMOS. Many of the above AMOS builds make POST `/joinsystem` requests to previously unreported AMOS C2s, including *77.221.151[.]54* — as opposed to *193.233.132[.]137*, described earlier in this report. This research also discovered additional likely staging domains for future AMOS builds at *shinudating[.]com*, *cheapcleanprotein[.]com*, *deskpaypal.com*, *crosscertify.com*, and *hobbyplanners[.]com*, all of which are currently parked (registered but not currently in use).

Mitigations

- Ensure that your organization-wide detections for AMOS are regularly updated and tested, based on the IoCs linked in **Appendix A**, to prevent infections related to this campaign. AMOS has gone through several development cycles since its inception and requires defenders to regularly update signatures associated with its various versions and builds.
- Advise users on the risks associated with downloading third-party virtual meeting software, like Vortax, that is not approved by your organization. Consider implementing strict security controls to prevent users from downloading unlicensed "open-source" or "freemium" software that they may have seen on social media, messaging platforms, or search engines.
- Encourage users to report suspicious activity on social media, messaging platforms, email, and other mediums that engage in the behavior described in this report. Educate your users on risks associated with cryptocurrency theft and how scams proliferate on social media.
- Recorded Future clients can use Recorded Future Malware Intelligence to identify and mitigate the threats identified in this report. Recorded Future Malware Intelligence will provide behavioral analysis of malicious macOS applications that may uncover connections to AMOS C2 infrastructure.
- Recorded Future Malware Intelligence, paired with Recorded Future Network Intelligence, can help identify malicious domains and IP addresses that host, stage, or communicate with the various builds of AMOS identified above.
- As this campaign's primary focus was on impersonating enterprise-level software, it is important to monitor your own technology stack via the curation of bespoke tech stack watch lists in the Recorded Future Intelligence Cloud. Leveraging these lists, in tandem with the Recorded Future Threat Map, Recorded Future Vulnerability Intelligence, and Recorded Future Attack Surface Intelligence, will provide unparalleled visibility into infostealer threats that may affect your organization.
- As the primary focus of this report was on infostealer malware, we also recommend exploring Recorded Future Identity Intelligence and Recorded Future Brand Intelligence, which will provide affected organizations with visibility into credentials found in AMOS infostealer logs, database breaches, and combo lists that may result from credential compromises related to this campaign.
- Stay abreast of developments related to AMOS in open sources (such as vendor reporting and social media, among others), dark web and special-access sources, and messaging platforms by using Recorded Future Threat Intelligence, Recorded Future AI, and the Recorded Future Advanced Query Builder (AQB).

Outlook

The expansive nature of this campaign, illuminated by examining a single scam on social media (Vortax), demonstrates the wide-ranging nature of infostealer campaigns and the difficulty of tracking them. We assess that the indicators in this report will provide further avenues for research into the markopolo user, the behavior of AMOS, and the patterns employed by AMOS operators to commit scams at scale.

This campaign, paired with the Web3 campaign previously described, may serve as a model for other cybercriminals seeking to proliferate macOS malware widely. In particular, the use of generative AI to create the appearance of a legitimate company will likely continue to be a tactic, making this social engineering tactic more effective. We assess that, given the increase in macOS malware and exploit kits advertised on the dark web over the past two years, the techniques described in this report will become more widely employed by others seeking to exploit macOS, which has remained relatively resilient to malware, compared to Windows. Organizations must consider macOS as no longer “safe” from malware, contrary to popular perception, and therefore must factor this into their risk posture, technology stack, and passive defenses.

Appendix A — Indicators of Compromise

```
Domains:
vortax[.]io
vortax[.]space
vortax[.]app
vortax[.]org
plumbonwater[.]com
showpiecekennelmating[.]com
casino-legrand[.]info
weworkhappy[.]com
marylandhomerates[.]com
novatercaagilidade[.]com
123mllhasbrasil[.]com
garagemfinity[.]com
institutoangelabatista[.]com
betbhaibetting[.]com
ebolight[.]com
shinudating[.]com
aidigibrain[.]com
hobbyplanners[.]com
repairleatherla[.]com
msjessd[.]com
iuddy[.]com
indianahomerates[.]com
pegamente[.]com
nongduangmarket[.]com
crosstacks[.]com
tripleplay-arg1[.]com
xhaxo[.]com
assetsreserve[.]com
cheapcleanprotein[.]com
eliteneatproductshop[.]com
piloje[.]com
faruvinnovations[.]com
crosscertify[.]com
deskpaypal[.]com

IP Addresses:
79.137.197[.]159
89.105.198[.]134
193.233.132[.]137
77.221.151[.]54

Email Addresses:
support@vortax[.]space

Hashes:
f3176e0859ba92049dcd57685c1b5f49b97183ff49fcc79f2ce4ad2b31d2d843
c34f8b6a299dd867a8d00b4fc50d91d9fdde4aa36f7c2a444aab4601dd4238e1
b1817f23b4b0b09cd7db9e90eac166ddf0de9d22aaf69f17308da43854604d9e
5d45cc81a22e6ba596b12db4baec5b20ccbe9ce52f8258fa5690da0e5ef2a982
```

```
bde29a5215e685805f00fee5f03de3478f8214195ecf93fb81562bcd6122149d
f9785743539fdfb2199b53be57f86d5dba5c0cd3dfad1130de1532f92e0c7c4f
856979042a3c1f61050cc08e8f11856dc714ec16969bd0fc562fd47c9e6c8e4c
be7e5707e5e399aedcfb2800d7039ff050500be3bafd217ca9200abed8bef03f
750baf928763a60343f8d48e45c4a4ca8da1243add410821b51484242571d089
8fb5de2498e48338825253f9d165986403661003393278d93cb35f5f9a1549dc
05219c02d66daad246eab2abccc35384c34f17ce1daa2fee21cf0bfee88e31b2
5d6075e33a168dfa44492dbec5462c6142399b708ec0d038e3e1869141e6b378
9f676511cb9b35e2916ebf79aec6b4aa6514f8bf640ea2fe786d16a7ed8dab7b
93463142e354b05bbac20b9e9498ee5f8c9ea2488151ee6870189baab0b7e2ff
922afb7de0159e7b435290868c51f33c59e0990ec964f77de9201534e4232117
4b35a3872589f44c43469cf73c54b525506f6cc894598d109c5f931923c6eba9
8e6176eaea919bae5b75000244474d8310a7b8d59806fca133d78f5343839d76
5a441a59fe273161ff82cbe2a7fbddd21386481ad03cc1782b5b41b6b839c245
7225d5fde4daa4552daf67a0ac2f6d7ec0e768536c5377ee3e7beaa04603a6f5
7f6f85e1ae4186edc9bf821943893b183a6a9252b0899d682c1899201dffc496
73c099168755acbc793675a5e64ca719f909cd1943db5757af96b2c1c79ae6d8
eb74c9dd0a0e3ea3cb31338c55e9e630fdee964a7b5967efcdfa8daa26a0f129
dee705f4a513081afe9ab682b832068ac558ad3145038e57edc8109ab0e80769
```

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com