CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

September 17, 2024

“Marko Polo” Navigates Uncharted Waters With Infostealer Empire

Insikt Group identified over 30 unique scams attributed to Marko Polo, which have likely compromised tens of thousands of devices globally — posing significant financial and data security risks.

Marko Polo primarily targets gamers, cryptocurrency influencers, and software developers via spearphishing on social media — highlighting its focus on tech-savvy victims.

Marko Polo leverages a diverse toolkit — including AMOS, Stealc, Rhadamanthys, HijackLoader, and more — underscoring the need for adaptable defenses that counter its cross-platform capabilities.

Analysis cut-off date: July 25, 2024

Executive Summary

Insikt Group has identified a highly agile and adaptable cybercriminal group operating under the moniker “Marko Polo”. Our research has resulted in three previous public-facing Insikt Group reports (1, 2, 3). Marko Polo, which primarily operates on social media, has developed a sophisticated network of scams — using information stealer malware (“infostealers”; “stealware”) to target individuals and organizations worldwide — often impersonating legitimate brands in online gaming, virtual meeting and productivity software, and cryptocurrency. Following Insikt Group investigations into other projects attributed to Marko Polo, like Astration and Vortax, Insikt Group analysis has uncovered over 30 new and distinct scams, 50 unique malware payloads, dozens of malicious domains, and hundreds of fraudulent social media accounts linked to the Marko Polo operation. Insikt Group assesses that Marko Polo is actively expanding and diversifying its efforts, leading to an increase in the volume and cadence of attributed scams; however, this tempo results in greater public visibility, researcher attention, and operational security risks for Marko Polo.

Based on the widespread nature of the Marko Polo campaign, Insikt Group suspects that likely tens of thousands of devices have been compromised globally — exposing sensitive personal and corporate data. This poses significant risks to both consumer privacy and business continuity. Almost certainly generating millions of dollars in illicit revenue, this operation also highlights the negative economic effects of such cybercriminal activities. Insikt Group also notes that the primary targets of the scams identified in this report — online gaming personalities, cryptocurrency influencers, and technology professionals — are usually considered to be more technologically savvy, with better cybersecurity hygiene, than the average internet user. Despite this, these users are still susceptible to Marko Polo scams — indicating both the maturity of such scams and the broader effectiveness of social engineering as an attack vector. Individuals and enterprises may face direct financial losses, increased insurance costs, and reputational damage from breaches attributed to Marko Polo scams.

Marko Polo’s ability to pivot across different platforms and adapt its campaigns makes it a persistent criminal threat. This adaptability requires individuals and businesses to cast a much wider net, investing in more proactive cybersecurity strategies that address the underlying threats posed by Marko Polo — such as social engineering and infostealer malware. The relative success of operations like Marko Polo underscores the evolving nature of cyber threats. For executives and observers alike, this highlights the need for robust security controls that limit a user’s exposure to infection. Businesses should ensure that employees are only downloading approved software — especially for meetings and productivity, as outlined in this report.

The Marko Polo operation represents a significant and ongoing risk to both individual consumers and businesses worldwide. Its adaptability, reach, and financial success make it a prime example of the evolving threat landscape that requires continuous vigilance and investment in advanced security measures.

Key Findings

- **Over 30 Unique Social Media Scams Identified**: Insikt Group has uncovered more than 30 distinct social media scams attributed to Marko Polo, in addition to over 20 compromised Zoom meeting software builds, software cracks, and poisoned torrent downloads. These scams represent a significant threat to both individual users and businesses as many of them are still active, as of this writing.
- **Spearphishing Targeting Cryptocurrency Users and Influencers**: Marko Polo has been leveraging spearphishing tactics on social media to specifically target cryptocurrency users and influencers, leading to major financial losses. This highlights the group's focus on high-value targets within the digital finance sector.
- **Diversified Malware Toolkit**: Marko Polo employs a wide range of malware, including HijackLoader, Stealc, Rhadamanthys, and Atomic macOS Stealer (AMOS), demonstrating its ability to adapt and diversify its attack methods in cross-platform attacks. This variety makes it a versatile and persistent threat.
- **Reach and Impact**: Marko Polo's operations have likely compromised tens of thousands of devices worldwide, resulting in millions of dollars in illicit revenue. The group's ability to operate on such a large scale poses a serious risk to both personal data security and corporate integrity.
- **Increased Risk to Businesses and Consumers Alike**: The proliferation of Marko Polo's scams and malware means that both average internet users and enterprises are at risk. Consumers could face identity theft and financial losses, while businesses face potential data breaches, reputational damage, and financial effects.
- **Long-term Implications**: The adaptability and resilience of the Marko Polo operation underline the need for continuous vigilance and advanced security measures. Both individuals and organizations must prioritize cybersecurity awareness and defenses to protect against this evolving threat landscape.

Background

Insikt Group has been tracking a series of interconnected scams on social media for approximately six months. These scams are diverse in nature, impersonating Web3 projects, massively multiplayer online (MMO) games, productivity software, virtual meeting software, and more. Over the course of several investigations, Insikt Group is confident in its clustering and attributions of said scams to a single threat actor, dubbed Marko Polo. Insikt Group assesses that Marko Polo primarily leverages spearphishing on social media to proliferate its scams. Marko Polo explicitly targets cryptocurrency users, resulting in major financial losses. Insikt Group has identified scam reports indicating that Marko Polo operators have stolen victims' life savings.

Insikt Group identified a series of posts on dark web and special-access sources suggesting that Marko Polo is a financially motivated "traffer team". Traffer teams are groups of organized individuals who redirect victims' traffic to malicious content operated by other threat actors. Marko Polo is only one active traffer team among dozens in the cybercriminal underground, demonstrating the scale of this ecosystem. Marko Polo is a primarily Russian-, Ukrainian-, and English-speaking group, with administrators and operators likely located in the post-Soviet states.

Marko Polo Clustering

Insikt Group Identifier	Associated Build IDs	Attributed Scams
MP-1	`meowsup, meowparty, meowsterioland`	PartyWorld, Party Royale
MP-2	`vor`	Vortax, Vorion, Vixcall
MP-3	`cloregod`	VDeck, VMSphere, VmAxis, VmMeetHub, Voico, GoHeard, Up-Connect, Yous, WooSpeech, Vicall, Callzy
MP-4	`sneprivate, NIGHT`	NightVerse, Nortex
MP-5	`voidwalker`	Rune Online
MP-6	`wasp`	Wasper
MP-7	`DoraLands`	SpectraRoom, Room
MP-8	`N/A`	TidyMe, SupMe
MP-9	`N/A`	Zoom impersonators
MP-10	`N/A`	Unspecified Setup, Launcher, and Installer builds

***Table 1**: Marko Polo clustering referenced in this report (Source: Recorded Future)*

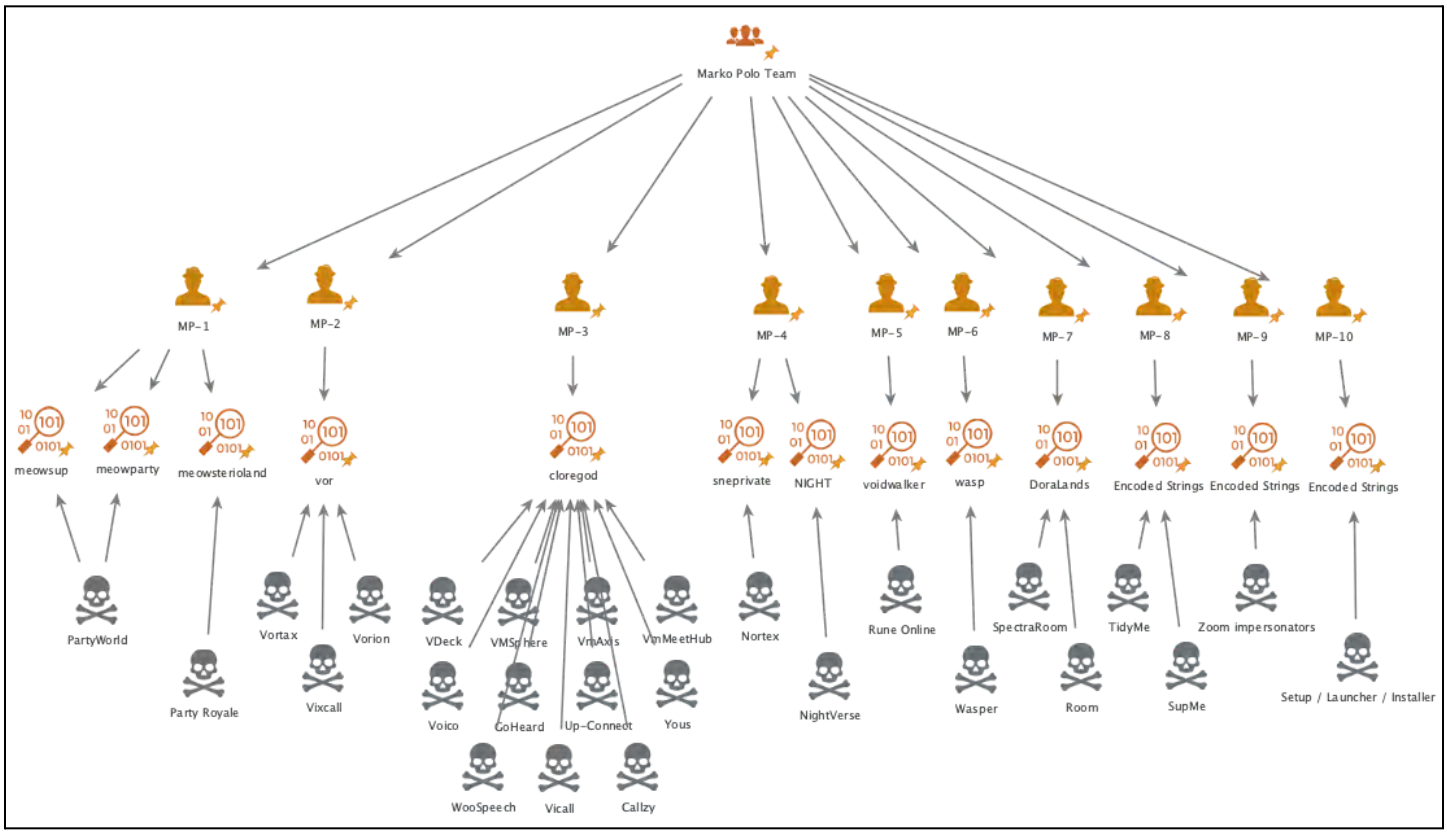

***Figure 1**: Marko Polo clustering referenced in this report (Source: Recorded Future)*

Scams Attributed to Marko Polo

PartyWorld and Party Royale (MP-1)

PartyWorld is a self-proclaimed free-to-play "lootr shootr" online video game that primarily impersonates legitimate games — including Fortnite and Party Icon — and is marketed via social media (@PartyWorldOGIX). Insikt Group first identified PartyWorld in June 2024 via social media reports of cryptocurrency scamming and infostealer malware delivery. Insikt Group assesses that PartyWorld is almost certainly a rebrand of **Party Royale** (@PartyRoyaleOGX) — a previous scam linked to Marko Polo. PartyWorld is boosted by Marko Polo operators that control fake social media accounts — purchased in bulk or harvested from the victims of account takeover (ATO) fraud.

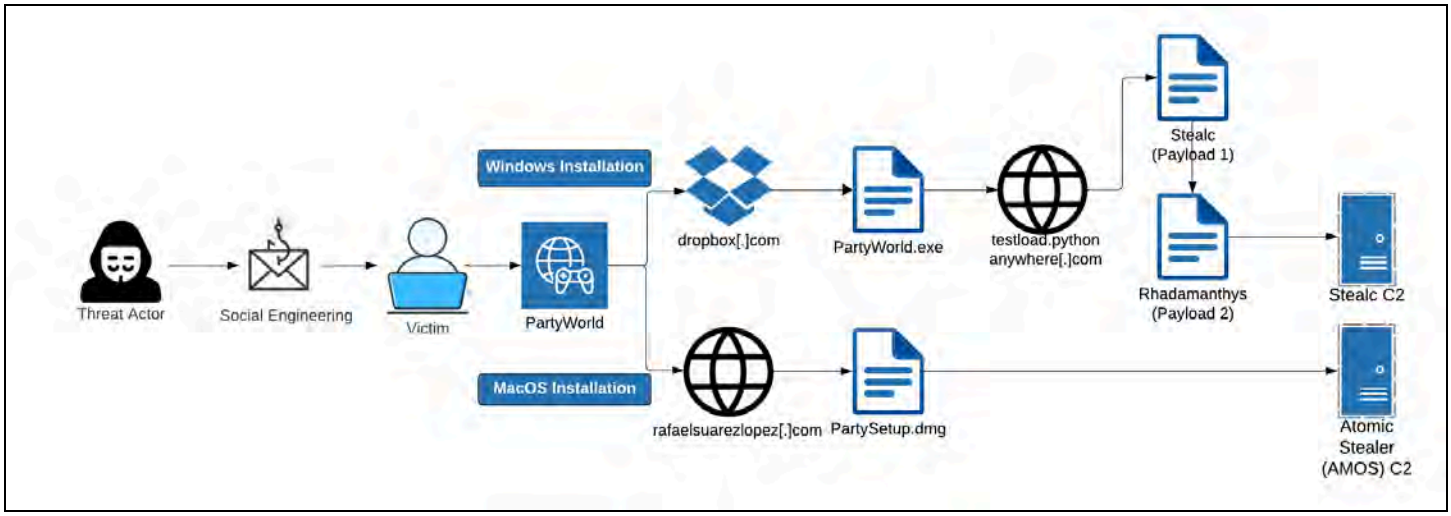

***Figure 2**: Marko Polo infection chain (Source: Recorded Future)*

Marko Polo operations follow a distinct infection chain to lure victims that generally begins with engagements via direct messages on various social media and NFT platforms, such as Discord and OpenSea. When approaching a potential victim, the operator, typically acting in the capacity of a human resources or talent acquisition representative, attempts to lure the user with a job opportunity, directing the user to go to the malicious website and obtain the project's software. In this case, upon visiting the PartyWorld website — *partyworld[.]io* — users are prompted to download the PartyWorld client for either Windows OS or macOS. For Windows OS users, the PartyWorld website contacts Dropbox (`dropbox[.]com/scl/fi/rqnd52uvolzt7t4ayefki/PartyWorld.exe?rlkey=v79iq914kkosuacpkyyio3pzs&st=b4m0fnx7&dl=1`) to download the `PartyWorld.exe` client.

For macOS users, the PartyWorld website contacts *ask-ashika[.]com* to download the `PartySetup.dmg` installation file. In mid-July 2024, the PartyWorld macOS build was moved from *ask-ashika[.]com* to *punitrai[.]com*. On or around July 25, 2024, the PartyWorld macOS build was yet again moved to *rafaelsuarezlopez[.]com*. Insikt Group notes that *rafaelsuarezlopez[.]com* is hosted on a different IP address than the previous two download locations, suggesting that Marko Polo is actively pivoting its infrastructure to avoid long-term tracking. This pivot may be related to ongoing reports of

service disruptions to bulletproof hosting (BPH) services preferred by Marko Polo operators, such as SUNHOST (AS216319) and AEZA (AS210644).

As seen in **Table 2**, the Windows OS build of PartyWorld delivers HijackLoader, Stealc, and Rhadamanthys. For macOS, PartyWorld delivers AMOS.

Filename	Malware Tags	C2	SHA256
`PartyWorld.exe`	HijackLoader; Stealc; Rhadamanthys; Build ID: `meowsterioland20`	194.116.217[.]148	5528e226b747abad7e843e6d7f92f48dda13f626a766285b2e889bd8fc746b12
`PartySetup.dmg`	N/A (AMOS)	147.45.43[.]136	0b4f5327c6c89f8aa2d642fc7a1955bc90ffcd8b41f21974517b7f58c3ed7323

***Table 2**: PartyWorld Windows OS and macOS builds (Source: Recorded Future)*

Domain	ASN	First Seen	Last Seen	Status
partyworld[.]io	CLOUDFLARENET, US (AS13335)	2021-11-28	2024-07-24	Active
partyroyale[.]io	CLOUDFLARENET, US (AS13335)	2024-04-20	2024-07-25	Active

***Table 3**: PartyWorld website infrastructure (Source: Recorded Future)*

Insikt Group notes that a previous AMOS build of PartyWorld (`PartyLauncher.dmg`) was hosted at *betbhaibetting[.]com* with the plaintext build ID `meowparty`. Based on the above indicators, Insikt Group has clustered the PartyWorld scam as **MP-1**.

Pivoting from the IP address associated with *ask-ashika[.]com* and *punitrai[.]com* (*77.91.77[.]175*), Insikt Group identified a second suspicious domain that also delivers an AMOS build of PartyWorld (*wealthgenixs[.]com*), which contacts the above AMOS C2. This finding allowed Insikt Group to pivot to other domains hosted on the same IP address, uncovering dozens of domains that deliver payloads related to other Marko Polo scams, beginning with Vorion.

Domain	IP Address	AMOS C2
rafaelsuarezlopez[.]com	147.45.43[.]197	79.137.202[.]22
ask-ashika[.]com	77.91.77[.]175	147.45.43[.]136
punitrai[.]com	77.91.77[.]175	147.45.43[.]136
wealthgenixs[.]com	77.91.77[.]175	147.45.43[.]136
betbhaibetting[.]com	79.137.197[.]159	193.233.132[.]137

***Table 4**: Domains, both current and historical, linked to the AMOS builds of PartyWorld (Source: Recorded Future)*

***Figure 3:** PartyWorld installer on Windows OS (Source: Recorded Future)*

Vorion, Vortax, and Vixcall (MP-2)

Vorion was a rebrand of the **Vortax** meeting software scam, which was the primary subject of a June 17, 2024, Insikt Group report. As with Vortax, Vorion (@vorionai) was an infostealer payload disguised as a self-proclaimed virtual meeting software that largely spread on social media via spearphishing. The Marko Polo operators assigned to Vorion focused their targeting efforts on cryptocurrency influencers — impersonating legitimate Web3 projects and engaging influencers directly with nonexistent job offers. The operators would persuade the target to download Vorion via *vorion[.]io*. The operators would also provide the target with a "Room ID" — similar to the Vortax scam — which would unlock the payload download on the Vorion website. Insikt Group identified several victims of Vorion. In mid-June 2024, Marko Polo likely abandoned the Vorion scam.

According to Recorded Future Malware Intelligence, the most recent AMOS build (Recorded Future Malware Intelligence Data) of Vorion (`VorionLauncher.dmg`) was hosted on *hoskinmetrologie[.]com* and contacted the *147.45.43[.]136* AMOS C2 at the `/joinsystem` endpoint. Insikt Group was not able to procure a Windows OS build of Vorion at the time of writing, as the project had been deprecated. However, Insikt Group believes that the Vorion Windows OS payloads are likely Stealc and Rhadamanthys, similar to Vortax.

On July 24, 2024, Insikt Group identified that Vorion had yet again rebranded to **Vixcall** (@VixcallApp). The website for Vixcall — *vixcall[.]app* — shares the same design as Vortax and Vorion, including requiring a Room ID to procure the Windows OS and macOS Vixcall downloads.

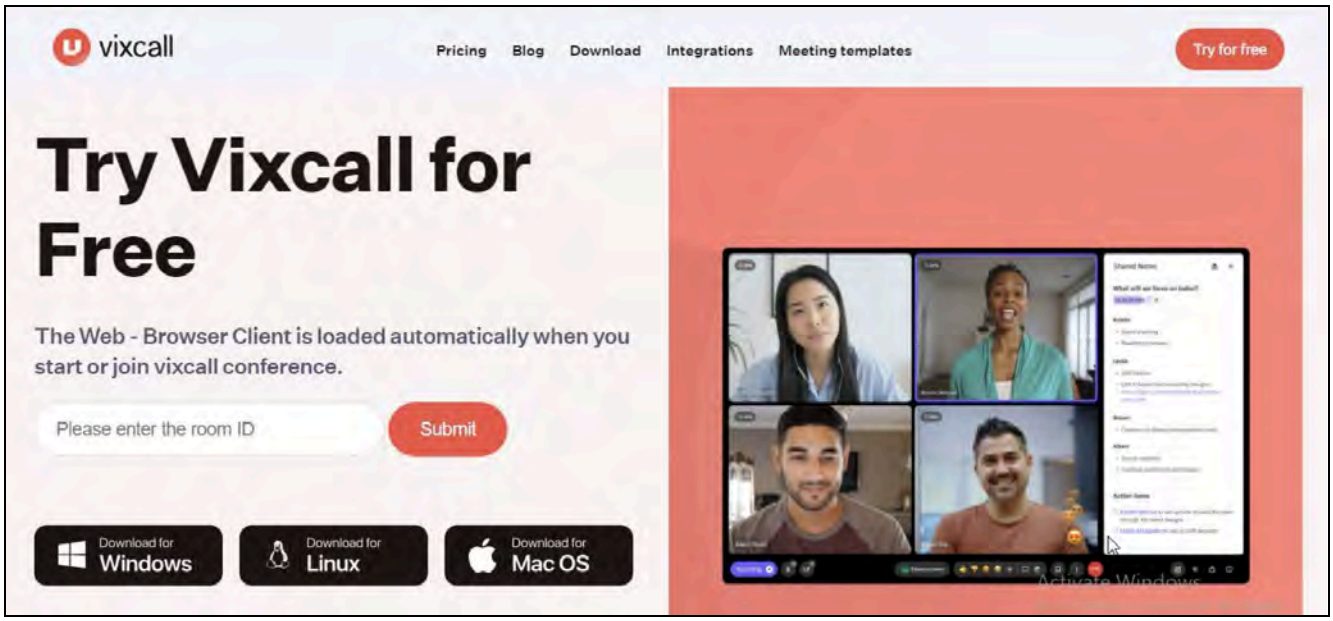

***Figure 4**: Vixcall website, which mimics the design of Vortax and Vorion — switching the color palette from purple to orange (Source: Recorded Future)*

Insikt Group notes that previous macOS downloads for Vortax (`VortaxSetup.dmg`) and Vorion (`VorionLauncher.dmg`) were previously hosted at *plumbonwater[.]com*, but pivoted to new hosting infrastructure following Insikt Group identification in June 2024. These previous builds, prior to implementing multipart/form-data encoding in its C2 POST requests, used the plaintext build ID `vor`. Based on this build ID, among other indicators, Insikt Group clustered the Vortax and Vorion scams as **MP-2**.

Domain	ASN	First Seen	Last Seen	Status
vixcall[.]app	AS-REG, RU (AS197695)	2024-07-22	2024-07-24	Active
vorion[.]io	AS-REG, RU (AS197695)	2024-05-10	2024-06-20	Defunct
vortax[.]io	AS-REG, RU (AS197695)	2024-03-01	2024-05-15	Defunct
vortax[.]app	AS-REG, RU (AS197695)	2023-12-17	2024-05-15	Defunct
vortax[.]org	AS-REG, RU (AS197695)	2023-02-14	2024-05-15	Defunct
vortax[.]space	AS-REG, RU (AS197695)	2024-01-04	2024-05-22	Defunct

***Table 5**: Vortax, Vorion, and Vixcall website infrastructure (Source: Recorded Future Data)*

Insikt Group further investigated the hosting infrastructure, structure, artifacts, and design of the Vixcall website and uncovered a possibly related scam called **PDFUnity**. According to its website — *pdfunity[.]com* — PDFUnity is a self-proclaimed enterprise-focused productivity software. As of July 24, 2024, the PDFUnity website is offline; therefore, Insikt Group is unable to procure downloads and make an attribution to **MP-2**. However, based on several unique cascading style sheets (CSS) and scalable vector graphics (SVG) artifacts found on the Vortax, Vorion, Vixcall, and PDFUnity websites, Insikt Group believes that they are related.

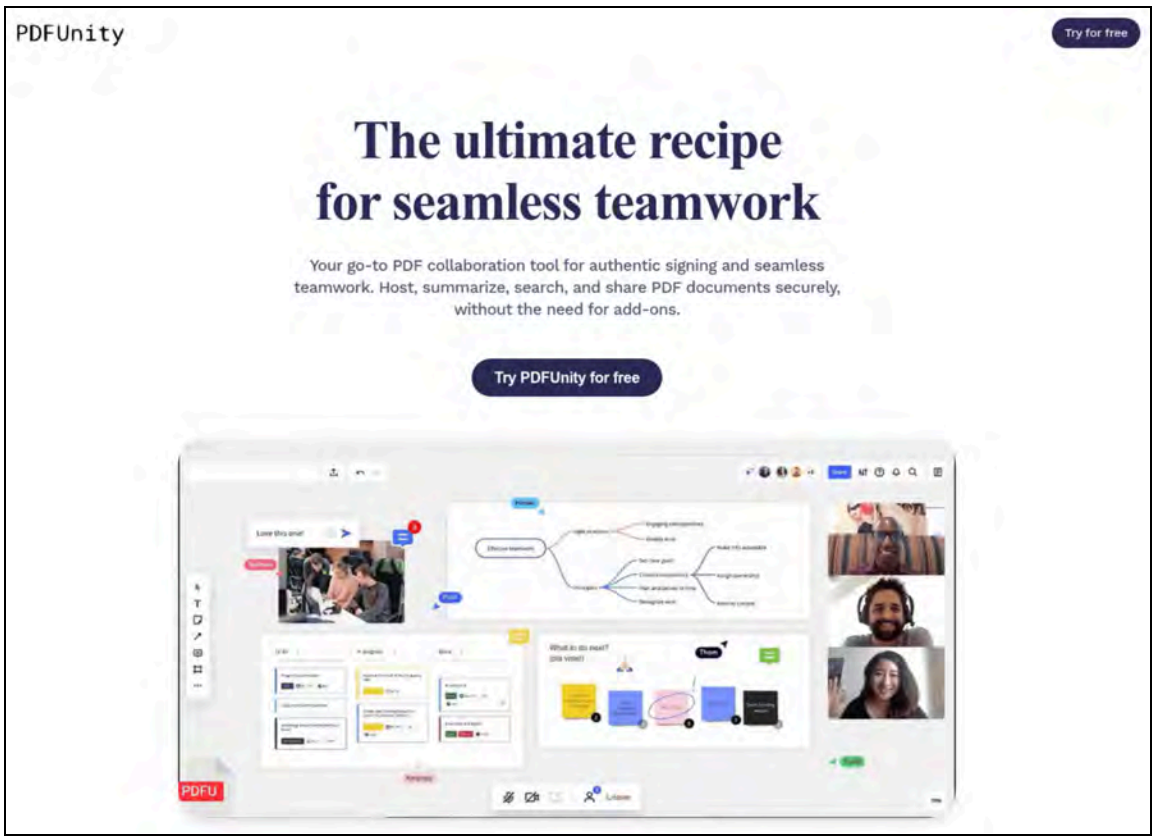

***Figure 5**: Cached image of PDFUnity, prior to it going offline (Source: Recorded Future)*

VDeck, VMSphere, VmMeetHub, and VmAxis (MP-3)

VDeck, similar to Vortax, is a self-proclaimed meeting software that is primarily spread on social media (@VDeck_app) via spearphishing. The operators assigned to VDeck focus their targeting efforts on cryptocurrency influencers, impersonating legitimate Web3 projects and engaging influencers directly with fraudulent job offers. The operators would persuade the target to download VDeck via *vdeck[.]io* or *vdeck[.]app*. The operators would also provide the target with a "Room ID" — similar to the Vortax scam — which would unlock the download on the VDeck website. Insikt Group found several Room IDs in scam reports on social media — including `VDAMA29583` and `VDF157MA`, among others — but all were inactive. However, unlike Vortax, Vorion, Vixcall, and other Marko Polo scams, the VDeck website allows visitors to create their own Room ID — allowing Insikt Group to bypass these roadblocks and procure VDeck downloads for both Windows OS and macOS.

Domain	ASN	First Seen	Last Seen	Status
vdeck[.]io	CLOUDFLARENET, US (AS13335)	2024-07-04	2024-07-24	Active
vdeck[.]app	CLOUDFLARENET, US (AS13335)	2024-01-30	2024-07-02	Defunct

***Table 6**: VDeck website infrastructure (Source: Recorded Future)*

The Windows OS build of VDeck downloads via Dropbox (*dropbox[.]com/scl/fi/2fe9tc3b8si7vq1tbfhm6/VDeck-Setup.exe?rlkey=99xfxg1tgnm1z1iwil0rj59xe&st=ny4jzm43&dl=1*) and retrieves its configuration files from *showpiecekennelmating[.]com*. This domain was previously reported by Insikt Group in connection to Vortax. The Windows OS build of VDeck delivers a Stealc payload with the hard-coded build ID `cloregod20`.

The macOS build of VDeck currently downloads from *abstractfit[.]com*. Further investigation of this domain revealed five additional staging domains for VDeck AMOS builds (**Table 8**). It is currently unclear when exactly these domains hosted VDeck, or if they will in the future.

Filename	Malware Tags	C2	SHA256
`VDeck-Setup.exe`	Stealc, Build ID: `cloregod28`	45.156.27[.]45	35be11ddfa4f1d776f0b6b814a325f50189100222fe04436a50563c89c2a02bd
`VDeck.dmg`	N/A	109.120.176[.]156	66085c5ac7b06960e90d4babc1a3e92fb57eaf557f61cc605865950039398a59

***Table 7**: VDeck builds for Windows OS and macOS (Source: Recorded Future)*

Insikt Group also discovered the following five domains in the course of investigating *abstractfit[.]com*. While these domains clearly delivered the AMOS build of VDeck at some point in time, they currently do not. They were likely staging domains for previous VDeck builds, which have since been moved to new domains.

Domain	IP Address	ASN	File
nizaj[.]com	77.91.77[.]175	SUNHOST-AS, GB (AS216319)	`VDeckInstall.dmg`
mudabirmunib[.]com	77.91.77[.]175	SUNHOST-AS, GB (AS216319)	`VDeckInstall.dmg`
egypt-pyramids[.]com	77.91.77[.]175	SUNHOST-AS, GB (AS216319)	`VDeckInstall.dmg`
chat2voice[.]com	77.91.77[.]175	SUNHOST-AS, GB (AS216319)	`VDeckInstall.dmg`
allworxusergroup[.]com	77.91.77[.]175	SUNHOST-AS, GB (AS216319)	`VDeckInstall.dmg`

***Table 8**: Domains that previously hosted the AMOS build of VDeck; as of July 24, 2024, these domains do not deliver any downloads (Source: Recorded Future)*

Insikt Group notes that a previous build of VDeck (`VDeckSetup.dmg`) was hosted at *weworkhappy[.]com* in June 2024. This previous build, prior to implementing multipart/form-data encoding in its C2 POST requests, used the plaintext build ID `cloregod` and communicated with the AMOS C2 *77.221.151[.]54*. Based on these indicators, Insikt Group has clustered the VDeck scam as **MP-3**.

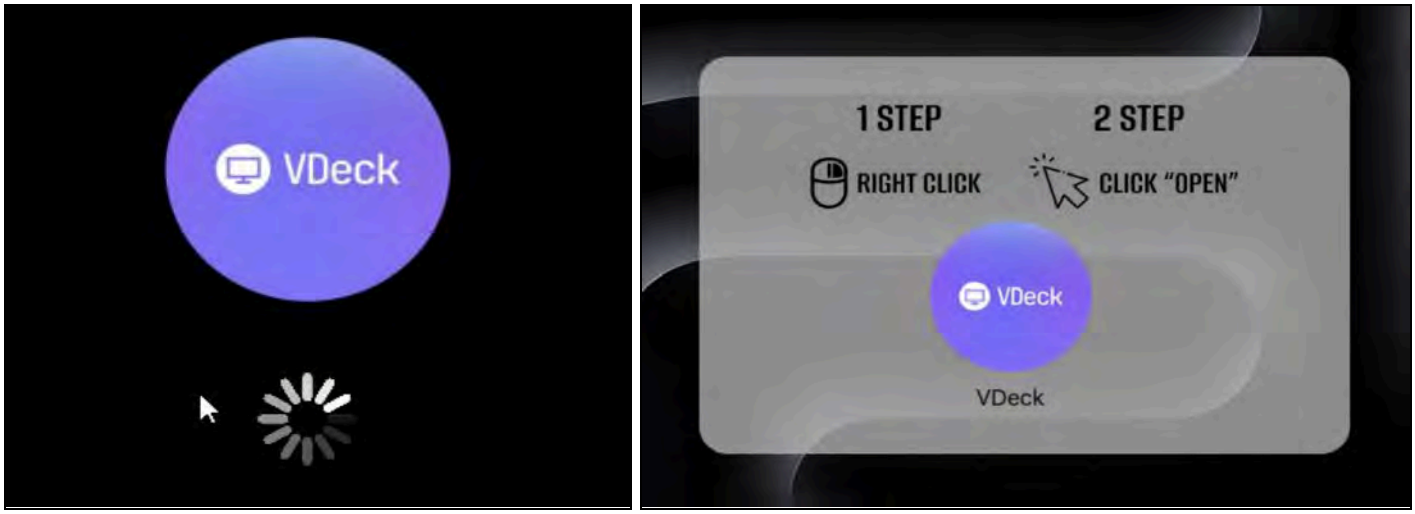

***Figure 6**: VDeck installer on Windows OS (Left) and macOS (Right) (Source: Recorded Future)*

Insikt Group identified three additional scams on social media with similar tactics, techniques, and procedures (TTPs) to VDeck: **VMSphere** (@VMSphereApp), **VmMeetHub** (@VmMeetHub), and **VmAxis** (@VmAxisCall). Insikt Group identified four active websites associated with VMSphere and VmAxis (**Table 9**). Insikt Group believes that **MP-3** is actively pivoting to this new infrastructure.

Domain	ASN	First Seen	Last Seen	Status
vmaxiscall[.]app	VIRTUO, CA (AS399486)	2024-07-13	2024-07-24	Active
vmaxismeeting[.]app	VIRTUO, CA (AS399486)	2024-07-17	2024-07-24	Active
vmaxis[.]io	CLOUDFLARENET, US (AS13335)	2024-07-16	2024-07-24	Active
vmsphere[.]app	AS-HOSTINGER, CY (AS47583)	2024-05-23	2024-07-24	Active
vmmeethub[.]app	LIMESTONENETWORKS, US (AS46475)	2024-06-25	2024-07-17	Defunct

***Table 9**: VMSphere, VmMeetHub, and VmAxis website infrastructure (Source: Recorded Future)*

Insikt Group believes that **MP-3** is attempting to avoid researcher attention by locking VMSphere, VmMeetHub, and VmAxis downloads behind Room IDs, given the relative ease of bypassing such a requirement for VDeck. These Room IDs — differing from Vortax, which were permanently set keys — are now temporary in nature, set by the operator, and linked to a specific target. All of the Room IDs identified by Insikt Group on social media are now invalid.

Further investigation into the domains listed in **Table 9** revealed connections to another Marko Polo scam — **Voico**. Voico is discussed at length below, along with related scams such as **Callzy**, **GoHeard**, **Up-Connect**, and **Vicall**, all of which Insikt Group has attributed to **MP-3**.

Up-Connect, GoHeard, WooSpeech, Vicall, Voico, Yous, and Callzy (MP-3)

During an investigation into the VDeck website and its related scams, Insikt Group identified hosting infrastructure, structural similarities, and artifacts that link VDeck to a second cluster of scams attributed to **MP-3**. These artifacts initially revealed two scams that mimic the website design of VMSphere, VmMeetHub, and VmAxis — **Up-Connect** and **GoHeard**.

Domain	ASN	First Seen	Last Seen	Status
up-connect[.]life	CLOUDFLARENET, US (AS13335)	2024-07-14	2024-07-24	Active
up-connect[.]world	CLOUDFLARENET, US (AS13335)	2024-07-14	2024-07-24	Active
up-connect[.]pro	CLOUDFLARENET, US (AS13335)	2024-07-14	2024-07-24	Active

***Table 10**: Up-Connect website infrastructure (Source: Recorded Future Data)*

Domain	ASN	First Seen	Last Seen	Status
goheard[.]digital	CLOUDFLARENET, US (AS13335)	2024-06-27	2024-07-24	Active
go-heard[.]life	CLOUDFLARENET, US (AS13335)	2024-07-11	2024-07-24	Active
go-heard[.]pro	CLOUDFLARENET, US (AS13335)	2024-07-11	2024-07-24	Active
go-heard[.]world	CLOUDFLARENET, US (AS13335)	2024-07-11	2024-07-24	Active
goheard[.]xyz	CLOUDFLARENET, US (AS13335)	2022-04-12	2024-07-24	Active
go-heard[.]eu	CLOUDFLARENET, US (AS13335)	2024-05-25	2024-07-24	Active
goheard[.]us	CLOUDFLARENET, US (AS13335)	2024-05-12	2024-07-24	Active
goheard[.]io	SERVER4-AS, RU (AS210352)	2024-02-06	2024-06-18	Defunct
goheard[.]app	AEZANET-AS, RU (AS210352)	2024-04-02	2024-05-28	Defunct

***Table 11**: GoHeard website infrastructure (Source: Recorded Future Data)*

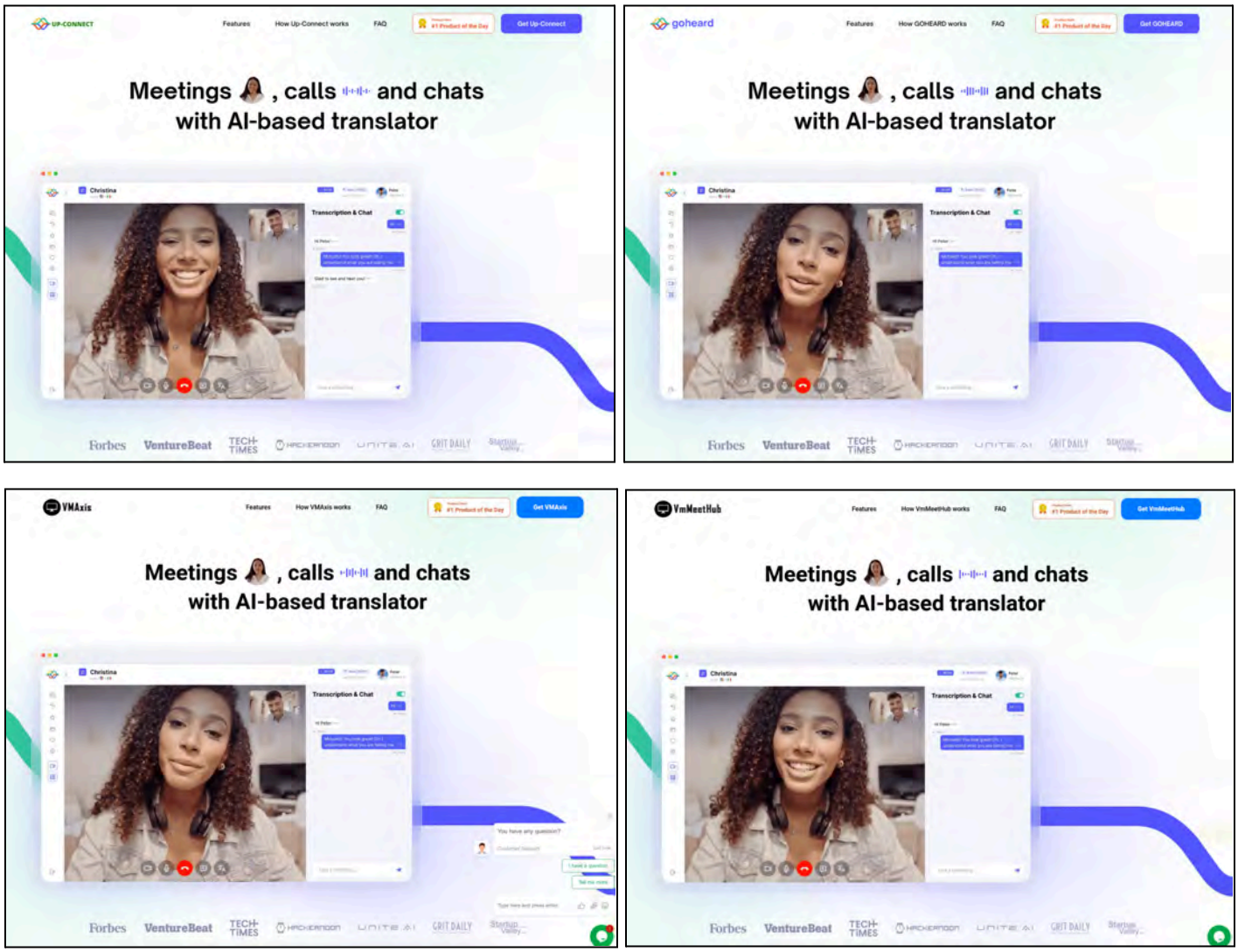

***Figure 7**: Up-Connect (Top Left), GoHeard (Top Right), VmAxis (Bottom Left), and VmMeetHub (Bottom Right) (Source: Recorded Future)*

Insikt Group discovered five additional scams linked to Up-Connect and GoHeard: **Yous**, **WooSpeech**, **Vicall**, **Voico**, and **Callzy**.

The Yous scam was likely only operated for a short period of time, maintaining only one domain — *yous[.]ai* — which was first identified in September 2022. It is unclear when the domain went offline, but it is currently defunct. The WooSpeech scam was also short-lived, with its website — *woospeech[.]top* — only existing from March 17 to March 19, 2024. This implies that Yous and WooSpeech could have served as testing for **MP-3** before **MP-3** pivoted to longer-term operations.

Insikt Group believes that **MP-3** pivoted its operations to focus on three recent scams, which were primarily spread via social media: Vicall (@VicallApp), Voico, and Callzy (@AppCallzy). Voico was the only scam without a dedicated social media account, using the @AppCallzy handle instead.

Domain	ASN	First Seen	Last Seen	Status
voicocall[.]com	CLOUDFLARENET, US (AS13335)	2024-07-17	2024-07-24	Active
voico[.]io	CLOUDFLARENET, US (AS13335)	2024-06-20	2024-07-24	Active
voico[.]site	EVILEMPIRE-AS, GB (AS216309)	2024-07-16	2024-07-17	Defunct
voico[.]app	EVILEMPIRE-AS, GB (AS216309)	2024-07-07	2024-07-16	Defunct

***Table 12**: Voico website infrastructure (Source: Recorded Future Data)*

Domain	ASN	First Seen	Last Seen	Status
vicall[.]org	AEZANET-AS, RU (AS210352)	2024-06-05	2024-07-24	Defunct
vicall[.]app	AEZANET-AS, RU (AS210352)	2024-05-28	2024-07-24	Defunct

***Table 13**: Vicall website infrastructure (Source: Recorded Future Data)*

Domain	ASN	First Seen	Last Seen	Status
callzy[.]io	CLOUDFLARENET, US (AS13335)	2024-07-20	2024-07-24	Active

***Table 14**: Callzy website infrastructure (Source: Recorded Future Data)*

As of July 24, 2024, Insikt Group believes that the Vicall scam was abandoned by **MP-3** in mid-July 2024, with Marko Polo instead opting to pursue Voico and Callzy full-time. In addition to the original *77.91.77[.]175* IP address first identified in the PartyWorld scam, Insikt Group discovered two active Marko Polo domains that deliver AMOS builds named after the Voico and Callzy scams (**Table 15**). These AMOS builds communicate with known Marko Polo AMOS C2s. Based on this finding, in addition to all of the evidence presented above, Insikt Group can definitively assess that Up-Connect, GoHeard, Yous, WooSpeech, Voico, Vicall, and Callzy are all linked to Marko Polo.

Domain	Filename	AMOS C2	SHA256
cancelspacecoastdaily[.]com	VoicoSetup.dmg	147.45.43[.]136	374fe0a3bd4b4dc99e1e07976fc0171c28a86f34d6810bc77e69bc58ccd764c7
adsotic[.]com	CallzyInstaller.dmg	109.120.176[.]156	cbfb45a16512c901cdfa9eff356bd7f139edc0c51133733ba80a7c0d9d1a2a61

***Table 15**: AMOS builds for Voico and Callzy (Source: Recorded Future Data)*

NightVerse (MP-4)

NightVerse is a self-proclaimed "cyberpunk" Web3 metaverse game that is primarily active on social media (@nightversegame), Telegram (@NightverseGame), and Discord. Cyberpunk genre games incorporate technological and scientific concepts into a dystopian future landscape. As of July 24, 2024, NightVerse claims to be "launching soon" on its official website — *nightverse[.]game* (Intelligence Card). NightVerse does not currently have a client available for download; however, Insikt Group was still able to identify two NightVerse AMOS builds currently hosted on domains linked to Marko Polo. These two builds contact different AMOS C2 domains.

Domain	Filename	AMOS C2	SHA256
an4nt[.]com	`NightVerseSetup.dmg`	109.120.176[.]156	77ee7274f0a8208fccefb013825842111355428 1bdf21e4d9f25fe6b11856dc4
metacosmoi[.]com	`NightVerseLauncher.dmg`	147.45.43[.]136	9a7a070029bb51daf70514402e9f6aeed4acd46a18c13478ddd3fa242a9f8a95

***Table 16**: NightVerse AMOS builds discovered by Insikt Group, which are currently not active on the NightVerse website (Source: Recorded Future Data)*

Insikt Group notes that one AMOS build (`NightVerseSetup.dmg`) in **Table 16** was previously hosted at *faruvinnovations[.]com*. This previous build, prior to implementing multipart/form-data encoding in its C2 POST requests, used the plaintext build ID `NIGHT` and communicated with the AMOS C2 *77.221.151[.]54*. Based on these indicators, Insikt Group has clustered NightVerse as **MP-4**.

Further investigation of *nightverse[.]game* revealed possible connections to another website, *gamepilot[.]ai* (**Figure 8**). As of July 24, 2024, the latter is offline; therefore, Insikt Group is unable to make a determination as to the nature of these connections and whether *gamepilot[.]ai* delivered AMOS at any point.

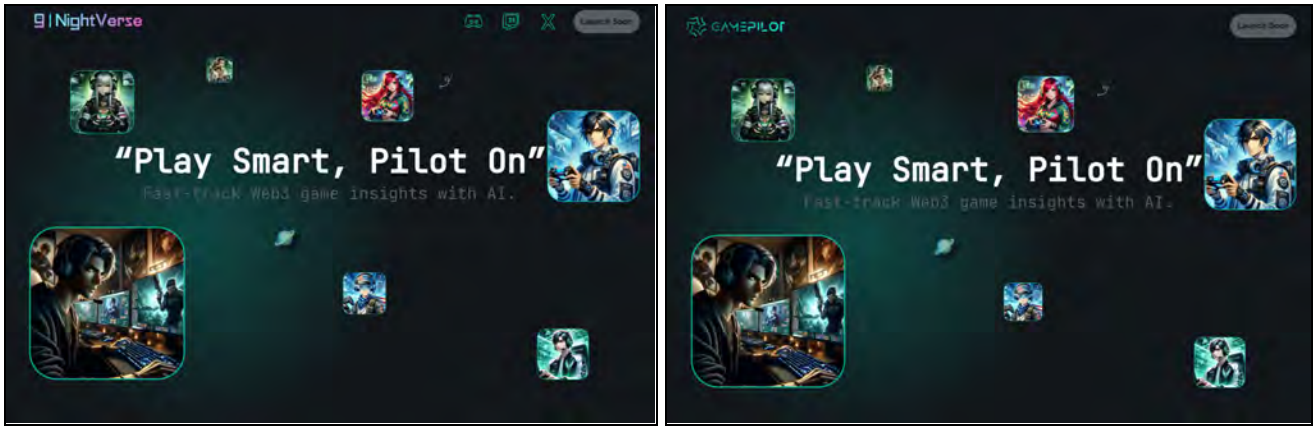

***Figure 8**: NightVerse (Left) and GamePilot (Right) (Source: Recorded Future)*

Nortex (MP-4)

Nortex (@NortexLab) is a self-proclaimed "decentralized all-in-one application for Web3 maximalists" that allegedly functions as a messaging service, productivity software, social network, and more — impersonating the legitimate Web3 project SendingMe (*sending[.]me*). In reality, Nortex does not perform any of these functions. Upon visiting its website — *nortexapp[.]xyz* — Nortex downloads a client for either Windows OS or macOS. On Windows OS, Nortex delivers HijackLoader and Stealc, whereas it delivers AMOS on macOS. Similar to VDeck and Vortax, the Windows OS build of Nortex is downloaded via Dropbox and pulls its configurations from *showpiecekennelmating[.]com*. The macOS build of Nortex pulls its download from *allieat[.]com*, which is hosted on the same IP address (*77.91.77[.]175*) linked to all of the scams above. The macOS build communicates with a known Marko Polo AMOS C2.

Filename	Malware Tags	C2	SHA256
`Nortex.exe`	HijackLoader; Stealc; Build ID: `night20`	188.130.207[.]115	fa634cee8d9b6d25081c943ca1c9156f846b7915ce2cba4f01329cc411e6e081
`NortexApp.dmg`	N/A	147.45.43[.]136	61db02e38f376e6639130ed344498b7ad190006e9e7eea46a98f83001bb419dd

***Table 17**: Nortex Windows OS and macOS builds (Source: Recorded Future Data)*

Insikt Group notes that a previous build of Nortex was hosted at *assetsreserve[.]com*. This previous build, prior to implementing multipart/form-data encoding in its C2 POST requests, used the plaintext build ID `sneprivate` and communicated with the AMOS C2 IP address *77.221.151[.]54*. This build resembles the Telegram handle and common abbreviation of Marko Polo subteam Slavic Nation ("sne"; "sneland"); therefore, Insikt Group has attributed Nortex to **MP-4**. Based on the additional shared use of the `night` build ID, which overlaps with NightVerse, Insikt Group can also tentatively attribute NightVerse to **MP-4**.

Domain	ASN	First Seen	Last Seen	Status
nortexapp[.]xyz	CLOUDFLARENET, US (AS13335)	2024-05-06	2024-07-29	Active
nortex[.]uk	CLOUDFLARENET, US (AS13335)	2018-08-13	2024-07-29	Active
nort-ex[.]lol	CLOUDFLARENET, US (AS13335)	2024-07-23	2024-07-29	Active

nort-ex[.]eu	CLOUDFLARENET, US (AS13335)	2024-07-23	2024-07-29	Active
nort-ex[.]world	CLOUDFLARENET, US (AS13335)	2024-07-23	2024-07-29	Active
nortex[.]blog	CLOUDFLARENET, US (AS13335)	2024-07-11	2024-07-29	Active
nor-tex[.]pro	CLOUDFLARENET, US (AS13335)	2024-07-11	2024-07-29	Active
nortex[.]life	CLOUDFLARENET, US (AS13335)	2024-07-05	2024-07-29	Active
nortex-app[.]pro	CLOUDFLARENET, US (AS13335)	2024-06-27	2024-07-29	Active
nor-tex[.]xyz	CLOUDFLARENET, US (AS13335)	2024-06-27	2024-07-29	Active
nortex[.]chat	CLOUDFLARENET, US (AS13335)	2024-02-16	2024-07-29	Active

Table 18: *Nortex website infrastructure (Source: Recorded Future Data)*

Pivoting on the above findings, Insikt Group identified one additional suspicious domain — *lastnuggets[.]com* — which currently displays an empty open directory. It is unclear whether this domain also delivered the malicious Nortex application at any point in time, like the domains in **Table 18**.

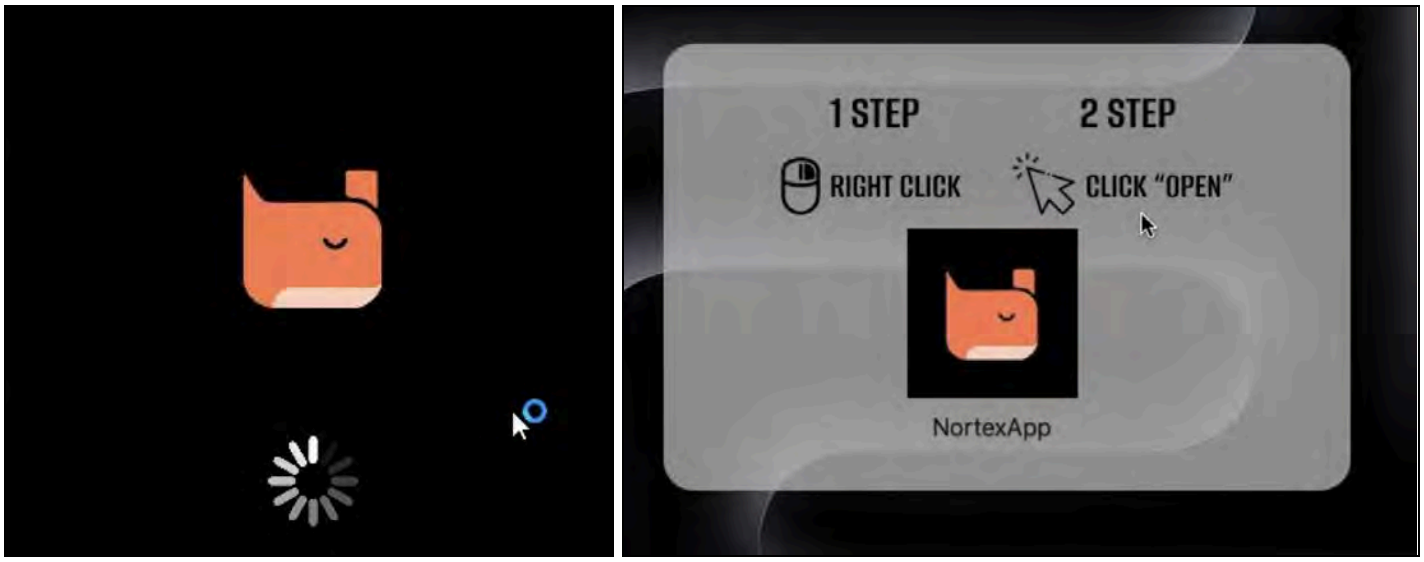

Figure 9: *Nortex installer on Windows OS (Left) and macOS (Right) Source: Recorded Future)*

Rune Online (MP-5)

Rune Online is a self-proclaimed Web3 massively multiplayer online role-playing game (MMORPG) that impersonates legitimate games, including RuneScape and Rise Online World. Rune Online has a significant social media presence relative to other Marko Polo scams. Rune Online maintains accounts on LinkedIn (Rune Online), social media (@RuneMMORPG), Instagram (@runeonlineworld), and a Discord server (*discord[.]gg/runeonline*). Rune Online also claims to operate a Twitch channel (*twitch[.]com/riseonlineworld*), but this is the legitimate account for Rise Online World.

Upon visiting the Rune Online website — *runeonlineworld[.]io* — users are prompted to download the Rune Online client for either Windows OS or macOS. Similarly to VDeck, the Rune Online Windows OS build is retrieved from Dropbox (`dropbox[.]com/scl/fi/wcl6nos8lteixi75fbm73/RuneOnlineWorld.exe?rlkey=mtt6ewrq4r2ohp8t0q81smgoq&st=2o5qx03b&dl=1`). The macOS build is retrieved from *drivelandblather[.]com*, which is hosted on the same IP address (*77.91.77[.]175*) linked to all of the scams above. The Windows OS build delivers Stealc, whereas the macOS build delivers AMOS. The macOS build communicates with a known Marko Polo AMOS C2, which is referenced several times above.

Filename	Malware Tags	C2	SHA256
`RuneOnlineWorld.exe`	Stealc; Build ID: `voidwalker20`	188.130.207[.]115	609129a9188ca3d16832594d44d746d7434e67a99c6dd20c1785aface9ed117d
`RuneInstaller.dmg`	N/A (AMOS); Build ID: `Voidwalker`	147.45.43[.]136	c0a1c698a5d84366a7f2b64751ee0a69f5e4887e0a0bc62841fae6d9f33417aa

***Table 19**: Rune Online World Steav and AMOS builds (Source: Recorded Future Data)*

Rune Online does not have any analog to previous Insikt Group reporting on Marko Polo. Insikt Group believes that Rune Online is a relatively new scam that was launched following our initial June 2024 report. As of this writing, Insikt Group can definitively attribute Rune Online to Marko Polo, but not to any other scam — therefore, Insikt Group has temporarily clustered Rune Online as **MP-5**.

***Figure 10**: Rune Online client for Windows OS, with spelling errors (such as "confrim") (Source: Recorded Future)*

Wasper (MP-6)

Wasper (@WasperSpace) is a self-proclaimed "collaborative creation and connection" software powered by generative artificial intelligence (AI) that impersonates the legitimate project AFFiNE (*affine[.]pro*). Upon visiting the Wasper website — *wasper[.]app* — users are prompted to download the Wasper client for either Windows OS or macOS. For Windows OS users, the Wasper download delivers HijackLoader and Stealc — pulling its configuration files from *showpiecekennelmating[.]com*, similar to many of the other scams listed above. For macOS users, Wasper downloads an AMOS payload from *engineeredbasementsolutions[.]com*.

Filename	Malware Tags	C2	SHA256
`Wasper.exe`	HijackLoader; Stealc Build ID: `wasp18`	194.120.116[.]197	49a924c91909318361eb7c0c5af1df5a9ebe5eaf2c38e14c84a51ce42c2586b5
`WasperLauncher.dmg`	N/A (AMOS)	147.45.43[.]136	c7fa247cd265cbaf766be6a041fc18ecf6380ee41196ad3b7d36bc61c1130118

***Table 20**: Wasper Windows OS and macOS builds (Source: Recorded Future)*

Based on the above indicators, Insikt Group is not yet able to attribute Wasper to any previously identified Marko Polo cluster. Therefore, Insikt Group tracks Wasper under the temporary identifier **MP-6**.

***Figure 11**: Wasper installer on Windows OS (Left) and macOS (Right) (Source: Recorded Future)*

SpectraRoom and Room (MP-7)

SpectraRoom (@SpectraRoom) and **Room** (@r00mapp) are self-proclaimed "open-source crypto-communications" applications that are primarily marketed via social media. As of July 24, 2024, the websites associated with these scams — *room[.]icu* and *spectra[.]land* — are currently offline; however, pivoting from the IP address previously identified in the PartyWorld scam, Insikt Group was able to procure macOS downloads for both SpectraRoom and Room that were hosted on Marko Polo-linked staging domains. As expected, these builds deliver AMOS.

Domain	Filename	AMOS C2	SHA256
columbuskitchenpros[.]com	`Room.dmg`	147.45.43[.]136	16c1c1b15f8473f1babbbcae1124c7481e9a4e25331beeae5611dc4f153e7b4b
everworldstory[.]com	`Room.dmg`	79.137.202[.]22	c6c76d3dad043e0d516d446ca438727ddec6bd978f77eea768d6eaeb216a84d1
institutoangelabatista[.]com	`SpectraSetup.dmg`	77.221.151[.]54	856979042a3c1f61050cc08e8f11856dc714ec16969bd0fc562fd47c9e6c8e4c

***Table 21**: SpectraRoom and Room builds (Source: Recorded Future Data)*

Insikt Group notes that, prior to implementing multipart/form-encoding in its POST requests, these previous builds of SpectraRoom and Room used the plaintext build ID `DoraLands2`. Based on this indicator, we can link SpectraRoom and Room together and cluster this activity as **MP-7**.

***Figure 12**: SpectraRoom (Left) and Room (Right) installers on macOS (Source: Recorded Future)*

TidyMe and SupMe (MP-8)

TidyMe (@TidyMeOrg), formerly **SupMe** (@SupMeOrg), is a "global digital economy" platform that impersonates the legitimate project PeerMe (*peerme[.]io*) and is primarily marketed on social media. Upon visiting the TidyMe website — *tidyme[.]io* — users are prompted to download the TidyMe client for macOS, which delivers AMOS. Artifacts identified in the TidyMe website link TidyMe to PartyWorld, Party Royale, Rune Online, and other Marko Polo scams; however, we are not able to attribute TidyMe to **MP-1** or **MP-5** at this time. Insikt Group has clustered and is tracking TidyMe and SupMe with the temporary identifier **MP-8**.

Domain	Filename	AMOS C2	SHA256
myfirstlovemusicfestival[.]com	`TidyMe.dmg`	79.137.202[.]22	cf8f04c3f1be5a27acbcaf08a2f0461ee48d2b4d48ddaca87904cb7c9831ab51

***Table 22**: TidyMe AMOS build (Source: Recorded Future Data)*

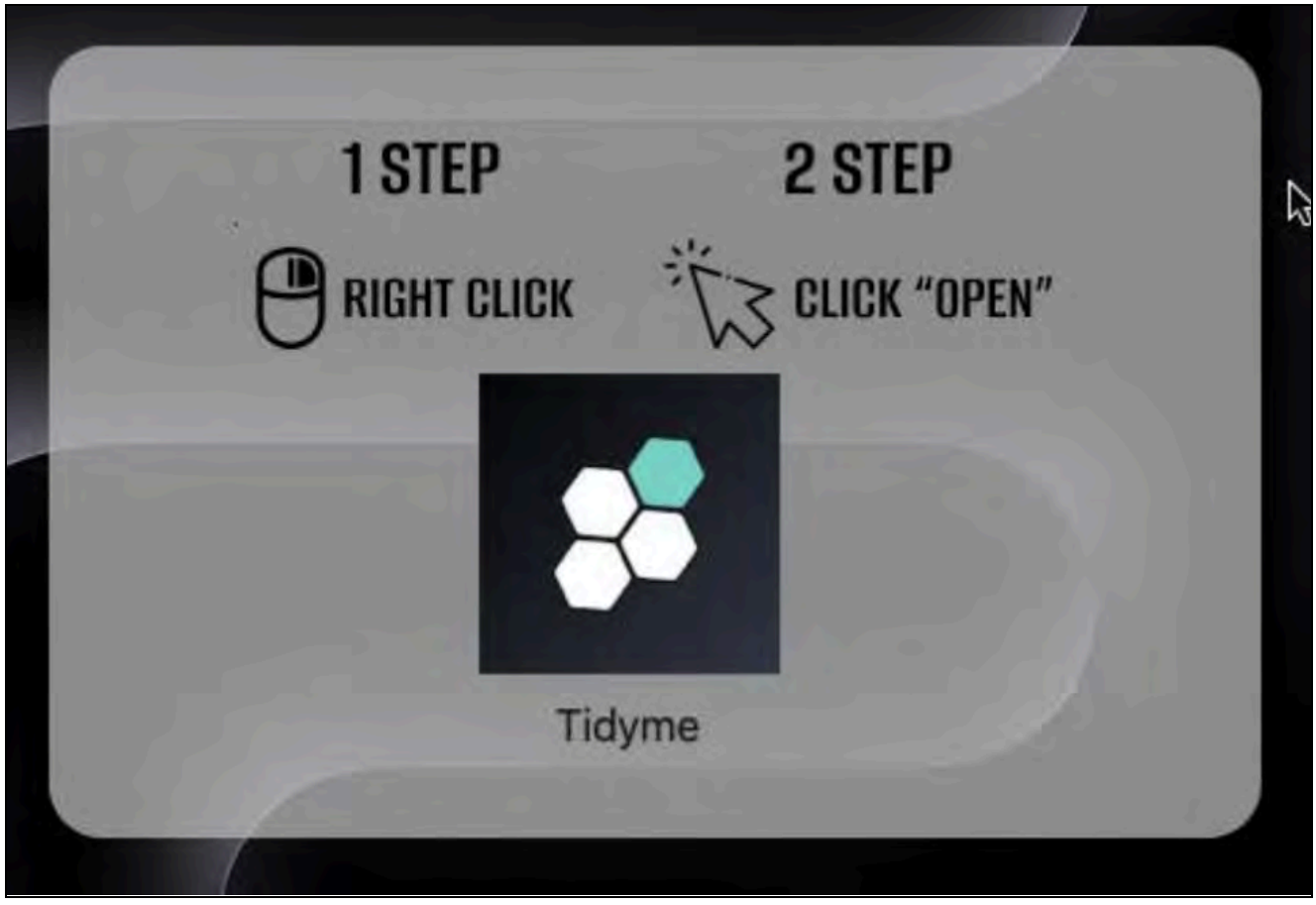

***Figure 13**: TidyMe installer on macOS (Source: Recorded Future)*

Zoom Impersonators (MP-9)

Insikt Group identified at least six domains linked to Marko Polo that distribute AMOS builds masquerading as Zoom meeting clients. Similar to Vortax, these builds are likely distributed via spearphishing on social media. Given the difficult nature of tracking these builds — relative to named scams — Insikt Group has clustered all of the identified Zoom meeting builds using the temporary identifier **MP-9**.

Domain	Filename	AMOS C2	SHA256
blocksofnews[.]com	`ZoomInstallerFull.dmg`	109.120.176[.]156	d17cb6113ccf97b7bc0d02da26afa766bea2e5067e745fab574b0b5b78880065
amigosdepomapata[.]com	`Zoom.dmg`	109.120.176[.]156	2f32a84122f86e686f93debcf02b635b0339c6d0b085e02419dff1eaa5724ec0
adelargentina[.]com	`ZoomInstall.dmg`	109.120.176[.]156	56adf4dfb61292ceef302e1988ac2ba4551109186ad1c9f3ce87d11914157b0c
virginturf[.]com	`ZoomSetup.dmg`	147.45.43[.]136	00a0cb5fb4053ba9a04920ca023aae50859af4bd15fd31286ebca6d0d97f3852
asdas1252qwdqwsd215612[.]com	`ZoomInstaller.dmg`	147.45.43[.]136	724d7e92e789640991c1066399cdd96f9ddfb7a59d42fd9d8d7e2bf48d39bc2d

***Table 23**: Zoom builds of AMOS linked to Marko Polo (Source: Recorded Future Data)*

Insikt Group notes that an AMOS build of Zoom was previously identified in June 2024 in connection to the Vortax scam. The staging domain for this build has since gone offline. Prior to implementing multipart/form-encoding in its POST requests, this build used the plaintext build ID `private1`.

Domain	Filename	AMOS C2	SHA256
novatercaagilidade[.]com	`ZoomInstaller.dmg`	77.221.151[.]54	bde29a5215e685805f00fee5f03de3478f8214195ecf93fb81562bcd6122149d

***Table 24**: Previous Zoom build identified by Insikt Group in June 2024 (Source: Recorded Future)*

Unspecified “Setup”, “Launcher”, and “Installer” Builds (MP-10)

Insikt Group identified at least thirteen domains linked to Marko Polo that deliver builds of AMOS that are unrelated to the above scams. These builds use placeholder names — including “Setup”, “Launcher”, and “Installer”, among others — and display default disk image logos when mounted. At this time, Insikt Group cannot attribute the following builds to any specific scams. Therefore, as with the cluster of Zoom impersonators above, Insikt Group has tentatively clustered the below activity with the temporary identifier **MP-10**.

Domain	Filename	AMOS C2	SHA256
biketrailtreasures[.]com	`Setup.dmg`	109.120.176[.]156	9099108338539e613d8fce7067b9e69d9cf09d1082bbedc0718c9f6d77e46288
topplayerpokermoneysang[.]com	`Installer.dmg`	109.120.176[.]156	f7dcc0c21c78db4698e03bf787c4d9329c4ec9fca1c546903a3af34d9c05d449
primejobpk[.]com	`Setup.dmg`	109.120.176[.]156	6798c877acdbcc2feec0f43fda970bc0428d8a9a7394e72325ae8cbd5e150602
mcxncdextips[.]com	`Installer.dmg`	109.120.176[.]156	5068e7c3a1822f2f66bc99a8b20d86d66a72a828c9d01214a076a415826667ce
concreteadvantagefl[.]com	`Installer.dmg`	109.120.176[.]156	66f085adee21f3c30ad6d7b8273a4ccac395b958536f7daf3a1772e768ee70cc
savvysellerstudio[.]com	`Installer.dmg`	147.45.43[.]136	0b5b9d6be11c9a806763741d52d0e186e6f0e9e54d124fa2fa0374d2465599f5
pasture2tablefarm[.]com	`Launcher.dmg`	147.45.43[.]136	257476099858ef9d284a0cf5be8e442ec59d30f4453b3807c8e5fcf091b07f6d
thanphongspring[.]com	`Launcher.dmg`	147.45.43[.]136	de78d04f0c049d53a40c4af5589a18aee85bd6a40fce7ad6114e421921ebfb93
elonmuskhouse[.]com	`Launcher.dmg`	147.45.43[.]136	222e01ce240bf795a31775bfbd74806dd904af514935308cc89188aa1c05b621
leed-consultants[.]com	`Setup.dmg`	147.45.43[.]136	9c2c9dd2cd873c8999c3631aac8a34f32f1efed54dd31fe47527d842185ff92d
hiranika[.]com	`Launcher.dmg`	147.45.43[.]136	35b9d0b528f576048ea10c9087010b4df0b5d05a9c8af8a3b88e1b88b607f08f
dixonpumpsonline[.]com	`Setup.dmg`	147.45.43[.]136	1c8705af8ea8598cf5d0b7af572d7e50540bfc146fa1c2ea0859ac554d088b0b
bestwaytoearnmoneyonline[.]com	`Launcher.dmg`	147.45.43[.]136	87806649eaabc3da46a8ef6a983d561f8716d24dee9406bf2cd68b914c6a06a3

***Table 25**: Unspecified Setup, Launcher, and Installer builds linked to Marko Polo (Source: Recorded Future)*

Mitigations

- **Enhance Endpoint Protection**: Deploy advanced endpoint detection and response (EDR) solutions to monitor for and block the execution of known malware families associated with Marko Polo — such as HijackLoader, Stealc, Rhadamanthys, and AMOS. These specific tools, in combination with social media scams, are immediate indicators of a Marko Polo attack.
- **Web Filtering and Monitoring**: Deploy web filtering solutions to block access to known malicious domains linked to Marko Polo — including all of the domains listed in this report — as well as suspicious downloads, especially those related to cracked "freemium" software.
- **Network Segmentation**: Apply network segmentation to limit the spread of malware and reduce the impact of initial access. Segment high-value assets, such as systems storing financial data or intellectual property, to prevent lateral movement.
- **Behavioral Analysis**: Use behavioral analysis tools to detect unusual activities, such as unexpected file downloads, command execution, or connections to suspicious IP addresses flagged in this report.
- **Continuous Threat Intelligence Monitoring**: Regularly update threat intelligence feeds with the latest indicators of compromise (IoCs) related to Marko Polo. Ensure that security teams are aware of the latest TTPs employed by the group.
- **User Awareness and Training**: Implement ongoing cybersecurity awareness training for employees, emphasizing the risks associated with phishing, social engineering, and suspicious downloads. Include specific modules on the risks posed by cryptocurrency-targeted attacks leveraged by Marko Polo.
- **Incident Response Planning**: Develop and regularly update incident response plans, ensuring they include scenarios involving initial access brokers. Conduct tabletop exercises to simulate potential Marko Polo-style attacks.
- **Collaboration and Information Sharing**: Collaborate with industry peers, threat intelligence organizations, and law enforcement agencies to share information on Marko Polo and similar threats. Engage in cross-sector initiatives to improve collective defenses against advanced cybercriminal groups.
- **Supply-Chain Security**: Strengthen supply-chain security by assessing the cybersecurity posture of partners and vendors. Ensure that third-party relationships do not introduce vulnerabilities, especially given Marko Polo's ability to pivot quickly across different attack vectors.
- **Strategic Threat Modeling**: Regularly update threat models to account for evolving tactics used by Marko Polo. Incorporate long-term scenarios in which the group continues to rebrand, diversify its attack methods, and collaborate with other threat actors. Plan for the potential escalation of the group's activities, including more sophisticated and targeted attacks.
- **Enhanced Regulatory Compliance**: Stay ahead of evolving regulatory requirements related to data protection and cybersecurity. Ensure that your organization's practices align with both domestic and international standards, particularly in industries like finance, where Marko Polo's attacks could have severe consequences.

- **Recorded Future**: Insikt Group recommends using Recorded Future Malware Intelligence to identify build IDs, C2 infrastructure, staging domains, and other malicious indicators associated with the Marko Polo scams described above. Leveraging Recorded Future Malware Intelligence and Recorded Future Network Intelligence can better identify and cluster infostealer activity, providing initial indications of infections, victimology, and pivoting scams. Insikt Group also recommends leveraging Recorded Future Identity Intelligence to ensure that organizations are not victimized by information stolen as part of a Marko Polo scam. Leveraging all of these tools, in combination with signatures for the malware outlined in this report, like AMOS, will provide coverage against Marko Polo.

Outlook

Insikt Group assesses that the Marko Polo cybercriminal group will almost certainly continue to be highly reactive, adaptive, and resilient in the face of potential disruptions. Marko Polo has demonstrated an exceptional ability to pivot quickly when detected by researchers, frequently rebranding and renaming its scams, updating its hosting infrastructure, and shifting tactics to evade scrutiny. This adaptability not only makes Marko Polo a persistent threat but also signals that it will likely continue evolving its methods to stay ahead of cybersecurity defenses.

For average internet users, this means an increased risk of exposure to well-crafted, sophisticated scams — especially those involved in cryptocurrency. Marko Polo's use of spearphishing, drive-by compromise, and watering hole attacks indicates that even the most cautious users could be vulnerable to infostealer infection and subsequent cryptocurrency theft. As traditional indicators of phishing and scams become less reliable — due to Marko Polo's continuous rebranding — users will need to remain vigilant and skeptical of unexpected communications, even from seemingly legitimate sources.

For enterprises, the implications are equally significant. Marko Polo's likely role as an initial access broker suggests a growing risk to corporate networks. Logs and access credentials harvested from initial attacks could be sold to other threat actors, leading to further breaches, ransomware attacks, or data exfiltration. This poses a long-term threat to corporate security, particularly if preventative measures are not continuously updated. The group's resilience and adaptability also mean that enterprises must prepare for a continuously evolving threat landscape. Advanced threat detection, response capabilities, and ongoing cybersecurity training for employees will be critical to defending against this threat.

Strategically, both individuals and organizations alike should prioritize continuous monitoring and leverage threat intelligence to stay informed about Marko Polo's activities. Proactive identification of evolving tactics will be key to mitigating risks. The ongoing threat posed by groups like Marko Polo underscores the importance of collaboration between public and private sectors to enhance the collective defense against such adaptable adversaries.

Marko Polo represents a long-term, evolving threat to both individual users and enterprises. The group's adaptability, combined with its likely role as an initial access broker, implies that its operations will

continue to pose significant risks. Proactive cybersecurity strategies and continuous vigilance will be essential to defend against the ongoing and future activities of this agile threat actor.

Appendix A — Indicators of Compromise

Domains:

```
ask-ashika[.]com
punitrai[.]com
rafaelsuarezlopez[.]com
partyworld[.]io
partyroyale[.]io
wealthgenixs[.]com
betbhaibetting[.]com
vorion[.]io
vixcall[.]app
vortax[.]io
vortax[.]app
vortax[.]space
pdfunity[.]com
vdeck[.]io
vdeck[.]app
abstractfit[.]com
nizaj[.]com
mudabirmunib[.]com
egypt-pyramids[.]com
chat2voice[.]com
allworxusergroup[.]com
weworkhappy[.]com
vmaxiscall[.]app
vmaxismeeting[.]app
vmaxis[.]io
vmsphere[.]app
vmmeethub[.]app
up-connect[.]life
up-connect[.]world
up-connect[.]pro
goheard[.]digital
go-heard[.]life
go-heard[.]pro
go-heard[.]world
goheard[.]xyz
go-heard[.]eu
goheard[.]us
goheard[.]app
goheard[.]io
yous[.]ai
woospeech[.]top
voicocall[.]com
voico[.]io
voico[.]site
voico[.]app
vicall[.]org
vicall[.]app
callzy[.]io
cancelspacecoastdaily[.]com
```

adsotic[.]com
nightverse[.]game
faruvinnovations[.]com
gamepilot[.]ai
nortexapp[.]xyz
showpiecekennelmating[.]com
allieat[.]com
assetsreserve[.]com
nortex[.]uk
nort-ex[.]lol
nort-ex[.]eu
nort-ex[.]world
nortex[.]blog
nor-tex[.]pro
nortex[.]life
nortex-app[.]pro
nor-tex[.]xyz
nortex[.]chat
lastnuggets[.]com
runeonlineworld[.]io
wasper[.]app
engineeredbasementsolutions[.]com
room[.]icu
spectra[.]land
columbuskitchenpros[.]com
everworldstory[.]com
institutoangelabatista[.]com
tidyme[.]io
myfirstlovemusicfestival[.]com
blocksofnews[.]com
amigosdepomapata[.]com
adelargentina[.]com
virginturf[.]com
asdas1252qwdqwsd215612[.]com
novatercaagilidade[.]com
biketrailtreasures[.]com
topplayerpokermoneysang[.]com
primejobpk[.]com
mcxncdextips[.]com
concreteadvantagefl[.]com
savvysellerstudio[.]com
pasture2tablefarm[.]com
thanphongspring[.]com
elonmuskhouse[.]com
leed-consultants[.]com
hiranika[.]com
dixonpumpsonline[.]com
bestwaytoearnmoneyonline[.]com

IP Addresses:
194.116.217[.]148
147.45.43[.]136
147.45.43[.]197

79.137.202[.]22
79.137.197[.]159
193.233.132[.]137
45.156.27[.]45
77.221.151[.]54
188.130.207[.]115
45.156.27[.]196

Hashes:
5528e226b747abad7e843e6d7f92f48dda13f626a766285b2e889bd8fc746b12
0b4f5327c6c89f8aa2d642fc7a1955bc90ffcd8b41f21974517b7f58c3ed7323
35be11ddfa4f1d776f0b6b814a325f50189100222fe04436a50563c89c2a02bd
66085c5ac7b06960e90d4babc1a3e92fb57eaf557f61cc605865950039398a59
374fe0a3bd4b4dc99e1e07976fc0171c28a86f34d6810bc77e69bc58ccd764c7
cbfb45a16512c901cdfa9eff356bd7f139edc0c51133733ba80a7c0d9d1a2a61
77ee7274f0a8208fccefb0138258421113554281bdf21e4d9f25fe6b11856dc4
9a7a070029bb51daf70514402e9f6aeed4acd46a18c13478ddd3fa242a9f8a95
fa634cee8d9b6d25081c943ca1c9156f846b7915ce2cba4f01329cc411e6e081
61db02e38f376e6639130ed344498b7ad190006e9e7eea46a98f83001bb419dd
609129a9188ca3d16832594d44d746d7434e67a99c6dd20c1785aface9ed117d
c0a1c698a5d84366a7f2b64751ee0a69f5e4887e0a0bc62841fae6d9f33417aa
d9f006c0b4cd266e641424865631091a125b4c95ae53b8341af1d9988de94383
c7fa247cd265cbaf766be6a041fc18ecf6380ee41196ad3b7d36bc61c1130118
16c1c1b15f8473f1babbbcae1124c7481e9a4e25331beeae5611dc4f153e7b4b
c6c76d3dad043e0d516d446ca438727ddec6bd978f77eea768d6eaeb216a84d1
856979042a3c1f61050cc08e8f11856dc714ec16969bd0fc562fd47c9e6c8e4c
cf8f04c3f1be5a27acbcaf08a2f0461ee48d2b4d48ddaca87904cb7c9831ab51
d17cb6113ccf97b7bc0d02da26afa766bea2e5067e745fab574b0b5b78880065
2f32a84122f86e686f93debcf02b635b0339c6d0b085e02419dff1eaa5724ec0
56adf4dfb61292ceef302e1988ac2ba4551109186ad1c9f3ce87d11914157b0c
00a0cb5fb4053ba9a04920ca023aae50859af4bd15fd31286ebca6d0d97f3852
724d7e92e789640991c1066399cdd96f9ddfb7a59d42fd9d8d7e2bf48d39bc2d
bde29a5215e685805f00fee5f03de3478f8214195ecf93fb81562bcd6122149d
9099108338539e613d8fce7067b9e69d9cf09d1082bbedc0718c9f6d77e46288
f7dcc0c21c78db4698e03bf787c4d9329c4ec9fca1c546903a3af34d9c05d449
6798c877acdbcc2feec0f43fda970bc0428d8a9a7394e72325ae8cbd5e150602
5068e7c3a1822f2f66bc99a8b20d86d66a72a828c9d01214a076a415826667ce
66f085adee21f3c30ad6d7b8273a4ccac395b958536f7daf3a1772e768ee70cc
0b5b9d6be11c9a806763741d52d0e186e6f0e9e54d124fa2fa0374d2465599f5
257476099858ef9d284a0cf5be8e442ec59d30f4453b3807c8e5fcf091b07f6d
de78d04f0c049d53a40c4af5589a18aee85bd6a40fce7ad6114e421921ebfb93
222e01ce240bf795a31775bfbd74806dd904af514935308cc89188aa1c05b621
9c2c9dd2cd873c8999c3631aac8a34f32f1efed54dd31fe47527d842185ff92d
35b9d0b528f576048ea10c9087010b4df0b5d05a9c8af8a3b88e1b88b607f08f
1c8705af8ea8598cf5d0b7af572d7e50540bfc146fa1c2ea0859ac554d088b0b
87806649eaabc3da46a8ef6a983d561f8716d24dee9406bf2cd68b914c6a06a3

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Initial Access: Spearphishing Attachment	T1566.001
Initial Access: Spearphishing Link	T1566.002
Initial Access: Drive-by Compromise	T1189
Execution: User Execution - Malicious File	T1204.002
Defense Evasion: Obfuscated Files or Information	T1027
Credential Access: OS Credential Dumping	T1003
Discovery: System Information Discovery	T1082
Collection: Data from Local System	T1005
Command and Control: Application Layer Protocol: Web Protocols	T1071.001
Exfiltration: Exfiltration Over C2 Channel	T1041
Exfiltration: Automated Exfiltration	T1020

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