JOURNEY OF A CRYPTO SCAMMER

NFT-001

MORPHISEC
Breach Prevention Made Easy

morphisec.com

Introduction

What do Paris Hilton, Jimmy Fallon, and Justin Bieber all have in common? Collectively they all spent millions on a popular non-fungible token (NFT) called the Bored Ape Yacht Club (BAYC).

Depending on how they store their NFTs, they could also become high-profile targets for cybercrime. Already, in December 2021, a BAYC collector lost $2.2 million after his BAYC and Mutant Ape Yacht Club NFTs were stolen by a hacker.

Bored Ape NFT collection up for sale (image: OpenSea)

Source: *OpenSea a popular crypto wallet site*

People walk by a Bored Ape Yacht Club NFT billboard in New York City's Times Square Tuesday. (Photo by Noam Galai/Getty Images) [-] GETTY IMAGES

This was not an isolated incident. With the NFT market booming (NFT trading volume increased by over 20,000% from 2020 to 2021), cybercriminals have rushed to adapt their strategies to exploit this still relatively new trend. From imitating social media accounts for NFT creators to making fake Google ads, hackers are exploring all avenues to make away with people's cryptos and NFTs.

However, one emerging threat vector for crypto crimes that the Morphisec Research Team has noticed and that is particularly worrying is happening through the Discord app. Last year, we analyzed the BABADEDA Crypter, a crypter that specifically targets crypto and NFT communities through malicious Discord bots. Not only have the attackers behind this campaign evolved their attack methods since then (using other crypters besides the BABADEDA), but we have also recently noticed an increasing number of stopped attacks on Morphisec's customers' devices which originated from this particular NFT campaign.

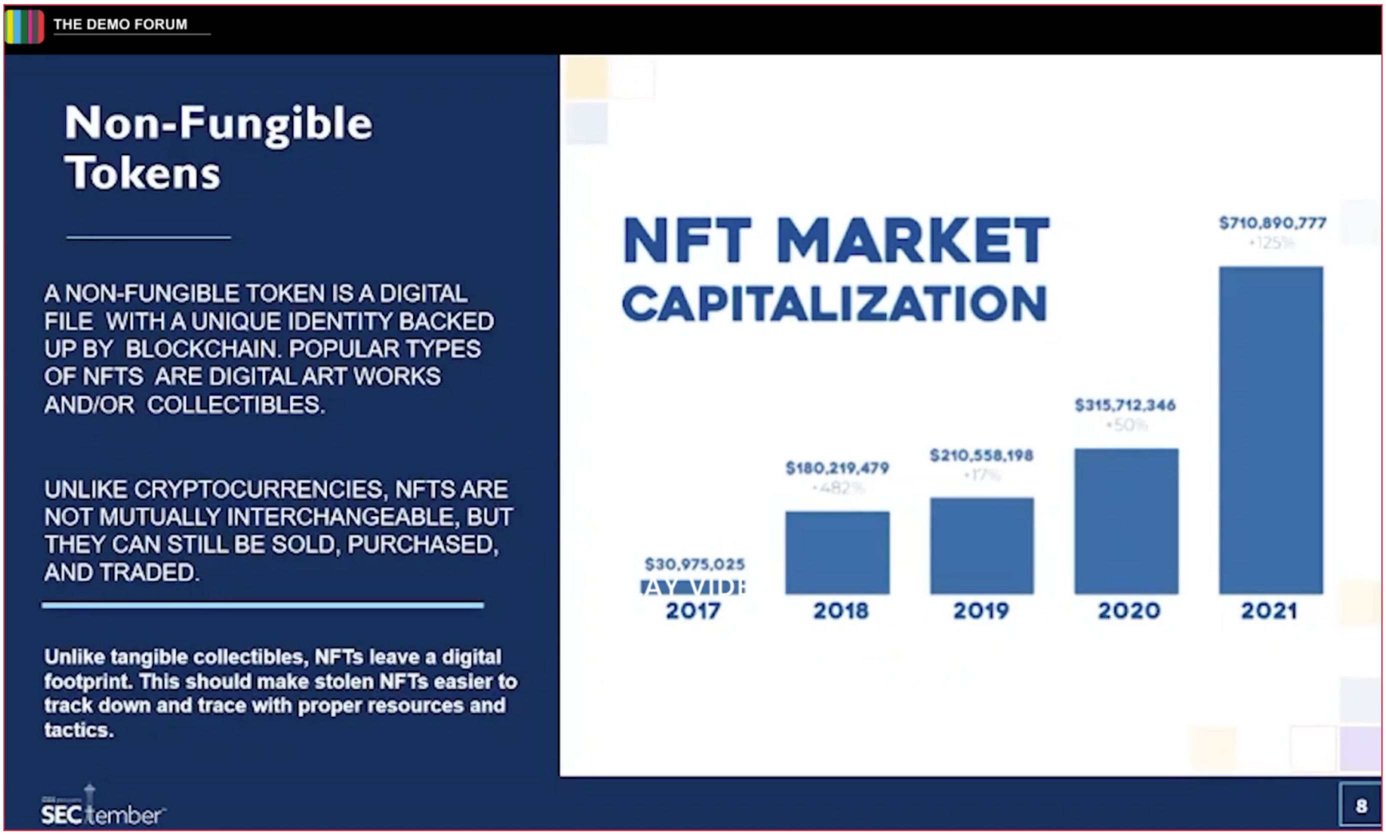
In this report, we pick up where we left off in November 2021, taking a closer look at the attacker's motivations, infrastructure, and activities. We also explain why Next-Generation Anti-Virus (NGAV) and Endpoint Detection and Response (EDR) solutions are not able to protect against these types of campaigns and how Moving Target Defense technology can keep your devices safe from this dangerous threat.

Wait... WHAT is an NFT???

Non-fungible tokens (NFTs) are digital files that, like cryptocurrencies such as Bitcoin or Ethereum, exist on a blockchain, a form of digital ledger. NFTs can be any type of digital object, from artwork and memes to tweets and audio. In some instances, NFTs may also be tied to physical objects.

Each NFT has a digital signature that acts as proof of ownership. However, unlike cryptocurrencies, NFTs are non-fungible, meaning that they can't be equally exchanged for something else, nor can they be reproduced. In this way, NFTs can be likened to limited edition Baseball cards or rare minted coins, where rarity/scarcity equals value.

Compounded by increased interest in cryptocurrency (the underlying foundation to creating and tracking NFTs), this has caused a 125% increase in NFT growth, and everyone is jumping in to grab a piece of the pie.



THE DEMO FORUM

Non-Fungible Tokens

A NON-FUNGIBLE TOKEN IS A DIGITAL FILE WITH A UNIQUE IDENTITY BACKED UP BY BLOCKCHAIN. POPULAR TYPES OF NFTS ARE DIGITAL ART WORKS AND/OR COLLECTIBLES.

UNLIKE CRYPTOCURRENCIES, NFTS ARE NOT MUTUALLY INTERCHANGEABLE, BUT THEY CAN STILL BE SOLD, PURCHASED, AND TRADED.

Unlike tangible collectibles, NFTs leave a digital footprint. This should make stolen NFTs easier to track down and trace with proper resources and tactics.

SECtember

8

Source: *Cloud Security Alliance SECtember, 2021 via* The Demo Forum

An Expanding Metaverse

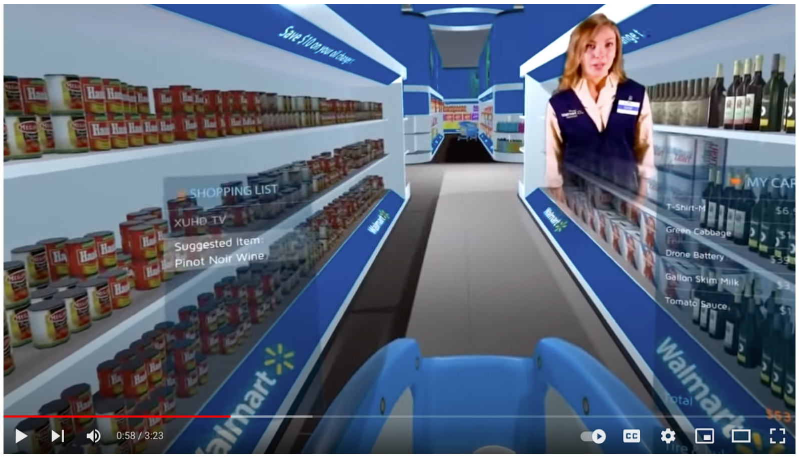
Part of what is propelling the growth of NFT adoption is the promise of the metaverse. The metaverse will be an online, three-dimensional universe that combines multiple virtual spaces. Although it doesn't yet exist, many see it as a future version of the internet. Accessing these 3D spaces via smartglasses, mobile apps, gaming consoles, and other metaverse-friendly devices, users, represented as 3D avatars, will be able to collaborate, shop, play games, and socialize, much in the same way they do already in the real world.

The Roblox x Nike Nikeland.

CREDIT: COURTESY OF NIKE

Source: *Nike*

As an immersive virtual economy, the metaverse will rely on cryptocurrencies as a mode of payment, with each metaverse likely to have its own set of coins. Users will be able to use these coins to pay for goods and services within the metaverse, including NFTs, virtual real estate, shoes, and more. Walmart, Adidas, Gucci, and other popular brands have already invested millions as they make a giant leap into the realm of virtual goods.



Source: *YouTube -* #Metaverse | Walmart VR Virtual Shopping Experience SXSW

More Money, More Problems

One unforeseen consequence of the growing interest in cryptocurrencies, NFTs, and the metaverse is the rising number of scams. Considering that the NFT market is worth $7 billion and that stealing NFTs can net malicious actors millions of dollars overnight, this is not surprising.

As users and businesses continue to embrace this new form of e-commerce, criminals are finding new ways to exploit them. We cover this trend in detail in the next section.

Early Warnings - Findings from the Morphisec Research Team

Not long ago, the Morphisec Research Team investigated an NFT and crypto crime campaign known as the BABADEDA Crypter, which we discovered during a new crypter research study. During our investigation, we focused on the crypter's mechanism and capabilities while also briefly discussing a new campaign targeting the crypto and NFT communities.

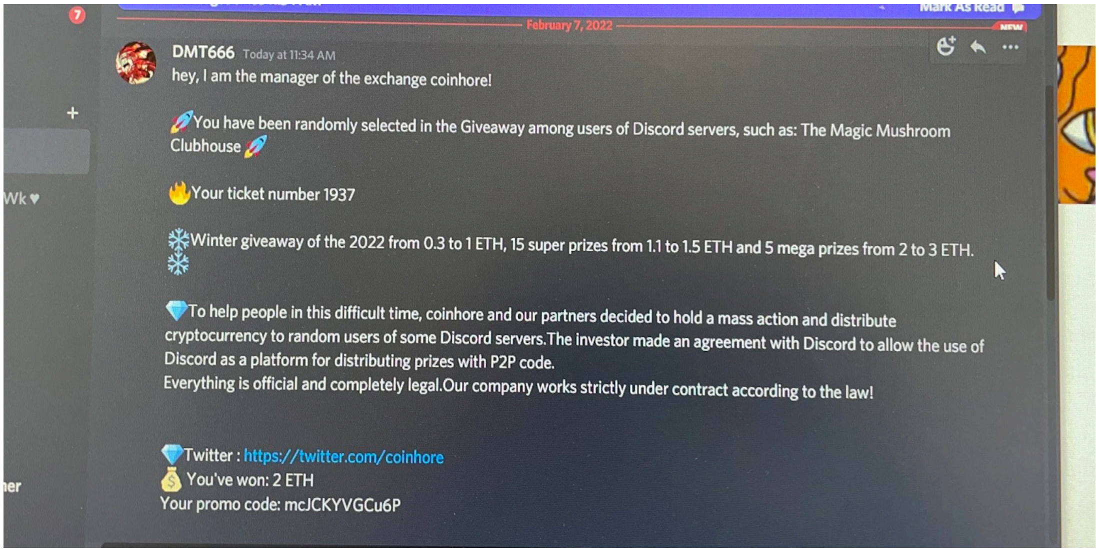
The recent surge in NFT scams and crypto crime activities, as well as a rising number of attacks on our customers' devices (fully prevented by Morphisec) linked to this NFT campaign, has prompted us to dive deeper into the attacker's infrastructure and dissect its activity.
In this report, we will walk you through the progression of the attacker's infrastructure and capabilities since November 2020, the first evidence of its activity, until today.

Infection Strategy

Before moving forward, we need to understand the attacker's workflow, starting with who their target victims are, up until the point they steal their funds.

In this campaign, we identified that the attacker's targets are Crypto and NFT communities (as per our previous investigation). We know that the actor impersonates existing Crypto/NFT services with a Discord channel. Thus, their victims are members of such communities.

Here is an example of a real scam conducted on a popular Discord forum on February 7, 2022.



February 7, 2022

DMT666 Today at 11:34 AM

hey, I am the manager of the exchange coinhore!

🚀You have been randomly selected in the Giveaway among users of Discord servers, such as: The Magic Mushroom Clubhouse 🚀

🔥Your ticket number 1937

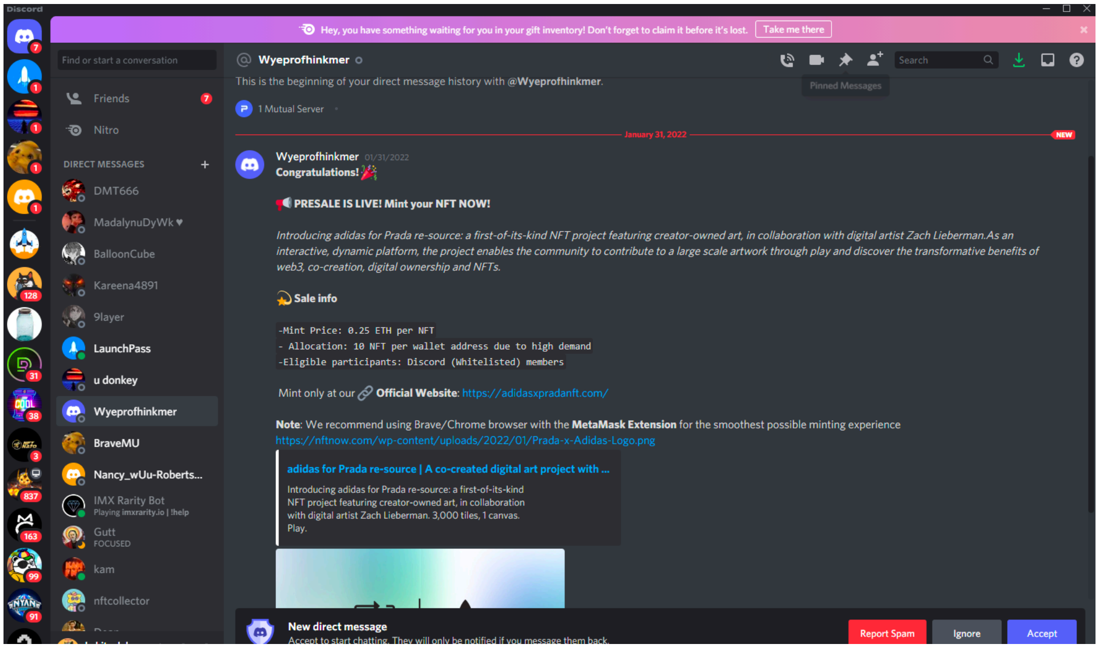
❄Winter giveaway of the 2022 from 0.3 to 1 ETH, 15 super prizes from 1.1 to 1.5 ETH and 5 mega prizes from 2 to 3 ETH. ❄

💎To help people in this difficult time, coinhore and our partners decided to hold a mass action and distribute cryptocurrency to random users of some Discord servers.The investor made an agreement with Discord to allow the use of Discord as a platform for distributing prizes with P2P code.
Everything is official and completely legal.Our company works strictly under contract according to the law!

💎Twitter : https://twitter.com/coinhore
💰 You've won: 2 ETH
Your promo code: mcJCKYVGCu6P

Source: *Discord*

Here is another example.



Wyeprofhinkmer

This is the beginning of your direct message history with @Wyeprofhinkmer.

1 Mutual Server

January 31, 2022

Wyeprofhinkmer 01/31/2022

Congratulations! 🎉

📢 **PRESALE IS LIVE! Mint your NFT NOW!**

Introducing adidas for Prada re-source: a first-of-its-kind NFT project featuring creator-owned art, in collaboration with digital artist Zach Lieberman.As an interactive, dynamic platform, the project enables the community to contribute to a large scale artwork through play and discover the transformative benefits of web3, co-creation, digital ownership and NFTs.

💫 **Sale info**

```
-Mint Price: 0.25 ETH per NFT
- Allocation: 10 NFT per wallet address due to high demand
-Eligible participants: Discord (Whitelisted) members
```

Mint only at our 🔗 **Official Website**: https://adidasxpradanft.com/

Note: We recommend using Brave/Chrome browser with the **MetaMask Extension** for the smoothest possible minting experience
https://nftnow.com/wp-content/uploads/2022/01/Prada-x-Adidas-Logo.png

adidas for Prada re-source | A co-created digital art project with ...

Introducing adidas for Prada re-source: a first-of-its-kind NFT project featuring creator-owned art, in collaboration with digital artist Zach Lieberman. 3,000 tiles, 1 canvas. Play.

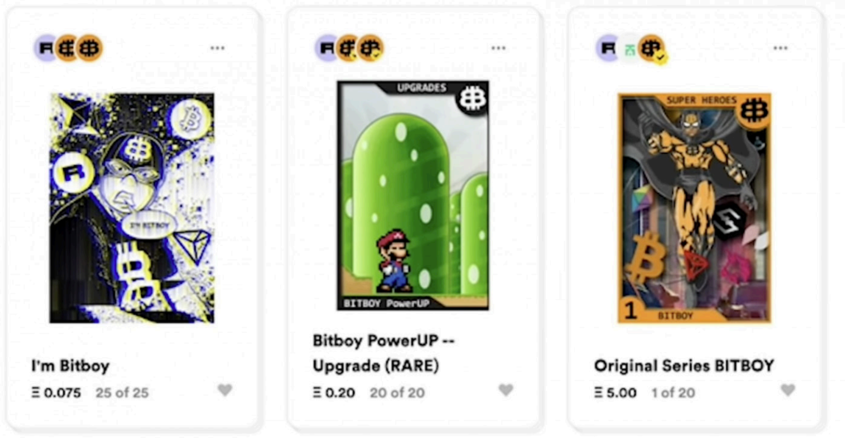
New direct message

Accept to start chatting. They will only be notified if you message them back.

Source: *Discord*

Can You Spot a Fake?

Take the example below. Two of the three NFTs are fakes. Can you tell which ones?



Source: Benzinga

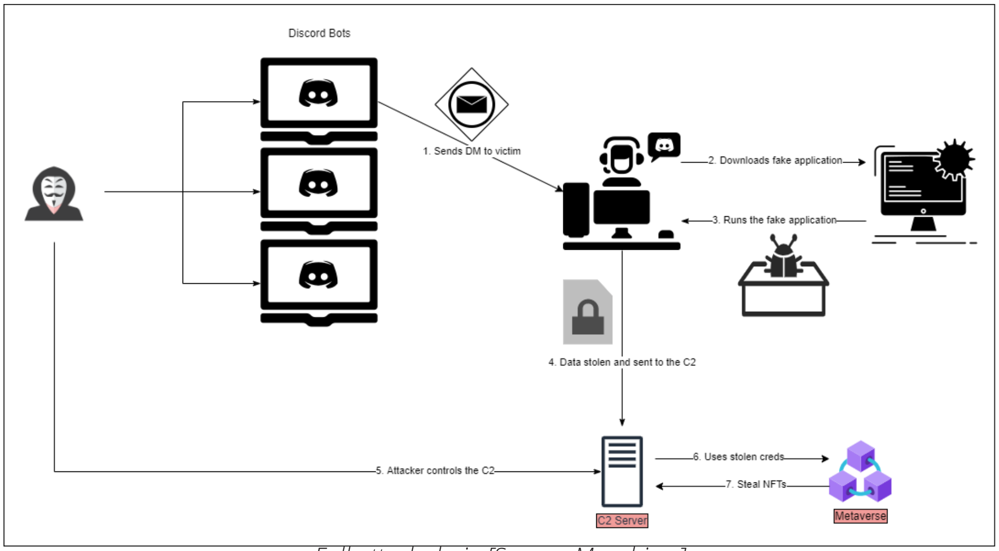
The leftmost NFT is sold by an artist with a stolen profile picture. We know this NFT is a scam because it doesn't have a yellow verification check mark in the upper left-hand corner.

The NFT in the middle is also a fake. However, it is obvious that it was created by a more sophisticated criminal because they were able to fake the verification check mark. Nevertheless, if you zoom in, you can tell the difference between this verification check mark and a real check mark (the NFT on the right, with the verification check mark extending outside the avatar).

The sophistication of these types of scams, along with the attacks that follow, is increasing every day.

You’ve Been Scammed, Now What?

By looking at the full attack chain, we can infer that the actor wants to steal high-value NFTs and cryptocurrencies. Their motives explain why they chose the kind of malware delivery method they did.


Discord Bots
1. Sends DM to victim
2. Downloads fake application
3. Runs the fake application
4. Data stolen and sent to the C2
5. Attacker controls the C2
6. Uses stolen creds
7. Steal NFTs
C2 Server
Metaverse

Full attack chain [Source: Morphisec]

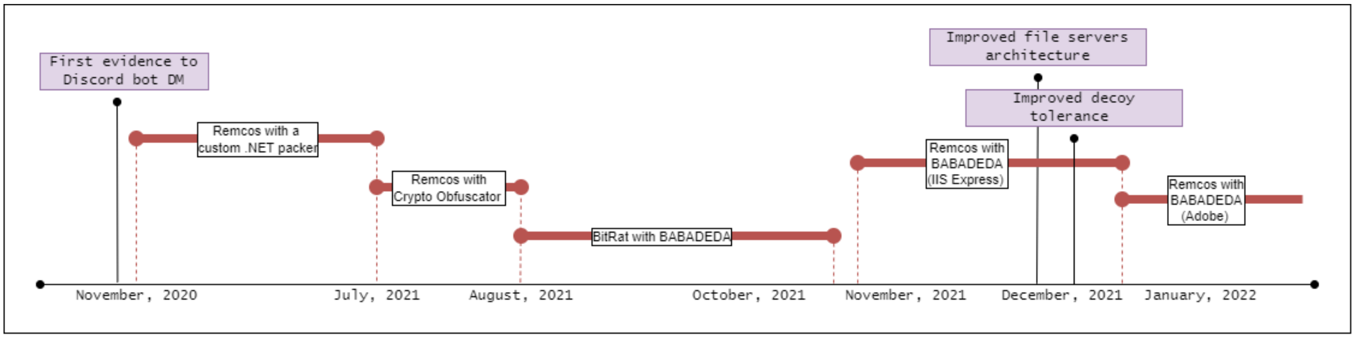
The attack chain comprises several components, and each one can be used as a standalone or as a service. This means that the actor stealing funds from a particular victim is not necessarily the developer of these components. The fact that the components are independent gives the attacker the ability to improve or change tactics quickly.

We will cover the following components in the following sections:

- The attacker creates Discord bots that, to the uninitiated eye, may look like they are owned by one of the official community administrators.
- The bots send private messages to channel members inviting them to download the new desktop application from an official-looking website that is actually owned by the attacker.
- The website is a perfect copy of the real site with one major change - a download button to the fake desktop application.
- Even when the application is downloaded and executed, victims still have no idea something is wrong. Under the hood, however, the malware unpacks itself and loads the final payload.
- The final payload, usually RAT, is used to steal the victim’s browsing data and install keylogger and other surveillance functionalities, including ones that give the attacker complete control over the victim’s machine.
- The attacker can use the stolen data to take over the victim’s identity and transfer their possessions to their own wallet/account.

Malicious bots facilitate over 90% of NFT scams. These bots can be easily obtained through Discord forums, Twitter, and underground exchange communities on the dark web. They are easy to operate and are very lucrative. A motivated bot operator can purchase a program for 0.2 Ethereum ($600 at the time of this writing) and get a 15x+ return in only one week. This return compounds as experience and efficiencies are gained.

Evolution of the Threat Actor



Campaign Timeline

Although an attack chain has many components, when looking at the evolution of the campaign, two main components jumped out:

1. Improved architecture (both decoy servers and file servers)
2. The final payload used once successful infection is achieved.

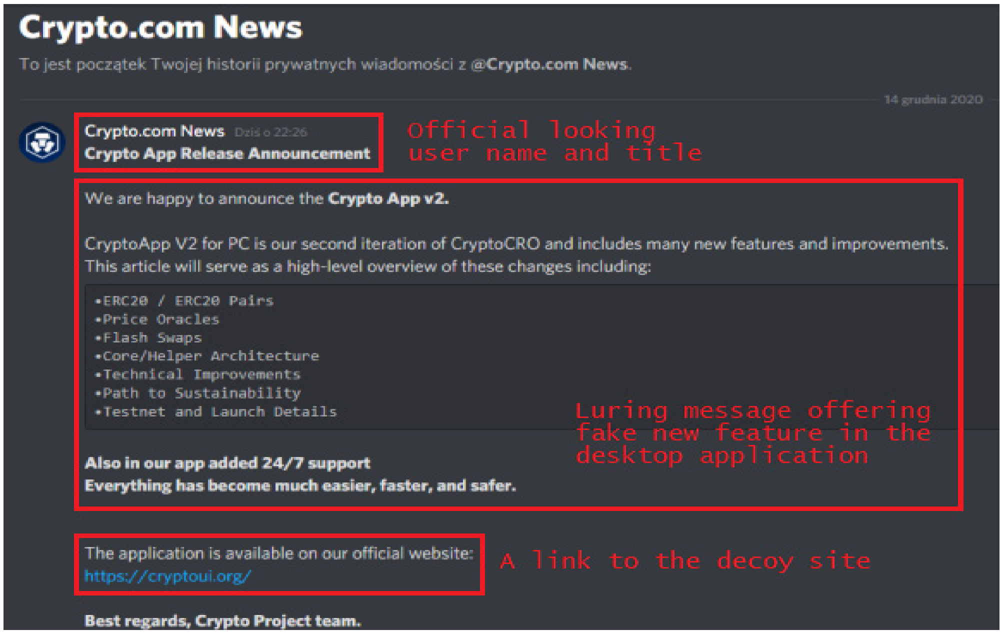
In this section, we'll explain each component and its progression over time:

- Infrastructure - the DevOps and networking infrastructures required from start to finish.
- Execution Methods - which Crypter is being used to deliver the final payload.
- Final Payloads - what final payload the actor used.

Infrastructure

Discord Bots

The actor uses Discord bots to reach their victims. They do so by sending official-looking DMs in targeted Discord channels:



Crypto.com News

To jest początek Twojej historii prywatnych wiadomości z **@Crypto.com News**.

14 grudnia 2020

Crypto.com News Dziś o 22:26
Crypto App Release Announcement

Official looking user name and title

We are happy to announce the **Crypto App v2.**

CryptoApp V2 for PC is our second iteration of CryptoCRO and includes many new features and improvements. This article will serve as a high-level overview of these changes including:

```
•ERC20 / ERC20 Pairs
•Price Oracles
•Flash Swaps
•Core/Helper Architecture
•Technical Improvements
•Path to Sustainability
•Testnet and Launch Details
```

Also in our app added 24/7 support
Everything has become much easier, faster, and safer.

Luring message offering fake new feature in the desktop application

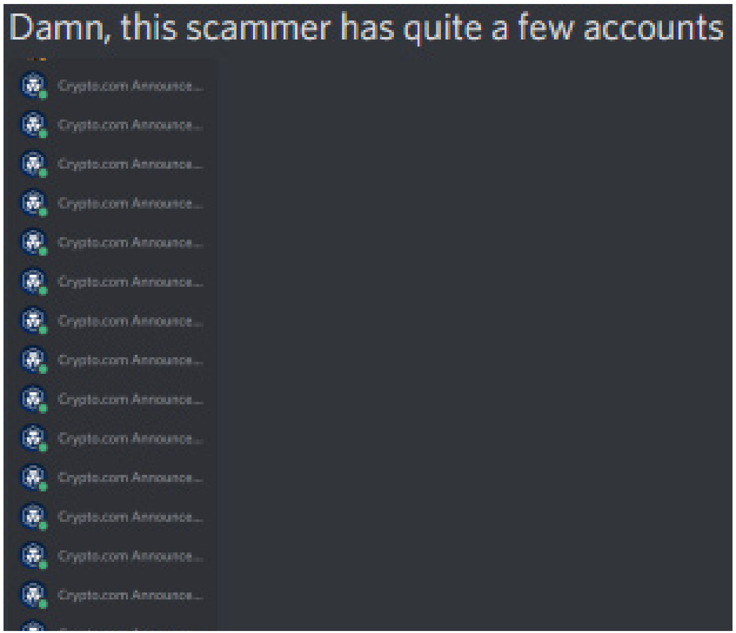
The application is available on our official website:
https://cryptoui.org/

A link to the decoy site

Best regards, Crypto Project team.

Discord private message luring a user to download a malicious app

To do this, the actor creates dozens of Discord bots that automatically send these messages to potential victims. However, spamming a forum with bots raises suspicions immediately.

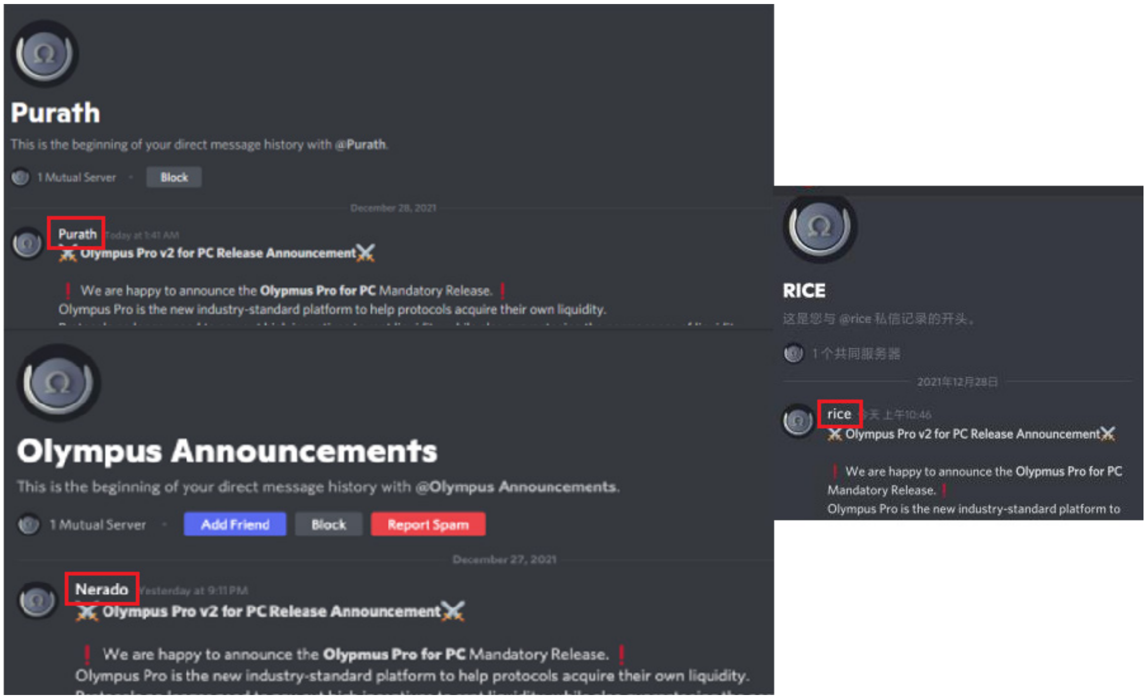


Damn, this scammer has quite a few accounts

Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...
Crypto.com Announce...

Bots accounts discovered by a user

Previously, finding and blocking the spamming bots was relatively easy - as shown on the previous page - leading the actor to use better naming conventions.



Purath

This is the beginning of your direct message history with **@Purath**.

1 Mutual Server · Block

December 28, 2021

Purath Today at 1:41 AM
⚔ Olympus Pro v2 for PC Release Announcement ⚔

❗ We are happy to announce the **Olypmus Pro for PC** Mandatory Release. ❗
Olympus Pro is the new industry-standard platform to help protocols acquire their own liquidity.

Olympus Announcements

This is the beginning of your direct message history with **@Olympus Announcements**.

1 Mutual Server · Add Friend · Block · Report Spam

December 27, 2021

Nerado Yesterday at 9:11 PM
⚔ Olympus Pro v2 for PC Release Announcement ⚔

❗ We are happy to announce the **Olypmus Pro for PC** Mandatory Release. ❗
Olympus Pro is the new industry-standard platform to help protocols acquire their own liquidity.

RICE

这是您与 @rice 私信记录的开头。

1 个共同服务器

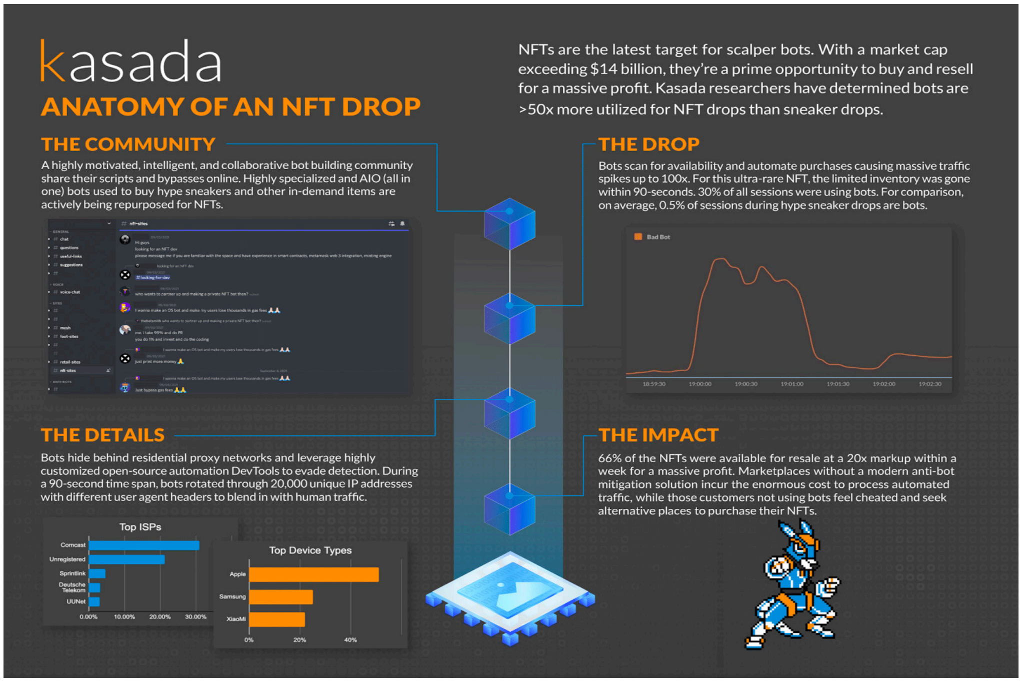
2021年12月28日

rice 今天 上午10:46
⚔ Olympus Pro v2 for PC Release Announcement ⚔

❗ We are happy to announce the **Olypmus Pro for PC** Mandatory Release. ❗
Olympus Pro is the new industry-standard platform to

Different names to the bots

The latest campaign shows the actor using different content within these messages and randomized yet still valid looking usernames. This suggests that the actor actively improves their phishing capabilities and develops their infection method over time.



kasada

ANATOMY OF AN NFT DROP

NFTs are the latest target for scalper bots. With a market cap exceeding $14 billion, they're a prime opportunity to buy and resell for a massive profit. Kasada researchers have determined bots are >50x more utilized for NFT drops than sneaker drops.

THE COMMUNITY

A highly motivated, intelligent, and collaborative bot building community share their scripts and bypasses online. Highly specialized and AIO (all in one) bots used to buy hype sneakers and other in-demand items are actively being repurposed for NFTs.

THE DROP

Bots scan for availability and automate purchases causing massive traffic spikes up to 100x. For this ultra-rare NFT, the limited inventory was gone within 90-seconds. 30% of all sessions were using bots. For comparison, on average, 0.5% of sessions during hype sneaker drops are bots.

THE DETAILS

Bots hide behind residential proxy networks and leverage highly customized open-source automation DevTools to evade detection. During a 90-second time span, bots rotated through 20,000 unique IP addresses with different user agent headers to blend in with human traffic.

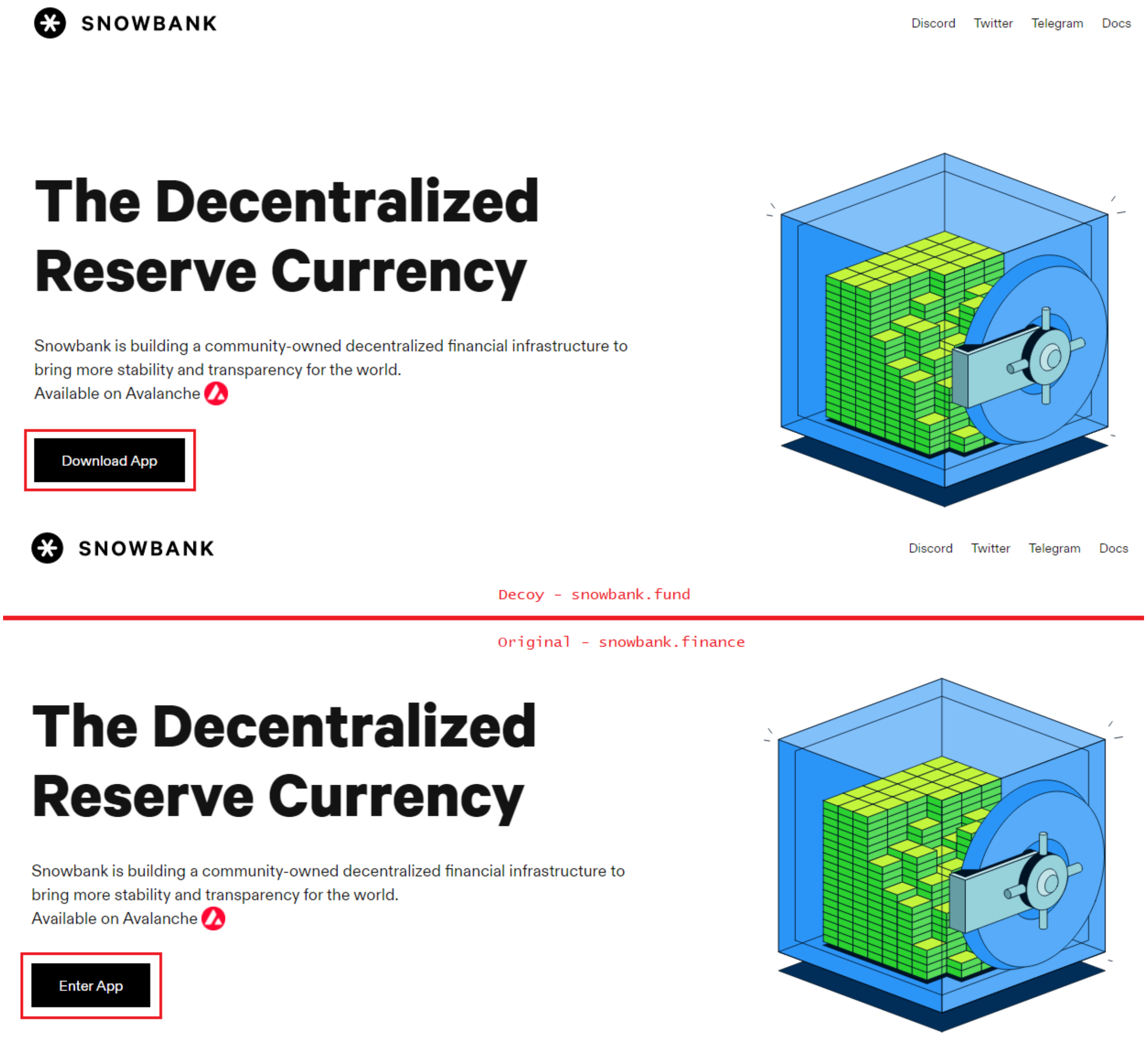
THE IMPACT

66% of the NFTs were available for resale at a 20x markup within a week for a massive profit. Marketplaces without a modern anti-bot mitigation solution incur the enormous cost to process automated traffic, while those customers not using bots feel cheated and seek alternative places to purchase their NFTs.

Source: Kasada

Decoy Sites

The main purpose of these fraudulent Discord messages is to lure the victim into downloading the “new official desktop application” from the “official site.” Keeping its real intentions hidden, the attacker creates an identical copy of the home page. The only thing they change is the CTA button.



The Decentralized Reserve Currency

Snowbank is building a community-owned decentralized financial infrastructure to bring more stability and transparency for the world.
Available on Avalanche

The Decentralized Reserve Currency

Snowbank is building a community-owned decentralized financial infrastructure to bring more stability and transparency for the world.
Available on Avalanche

Decoy vs. Original Site

Although the technique for creating decoy sites hasn't changed, the targeted apps did. The attacker changes the active decoys according to the community it's currently targeting.

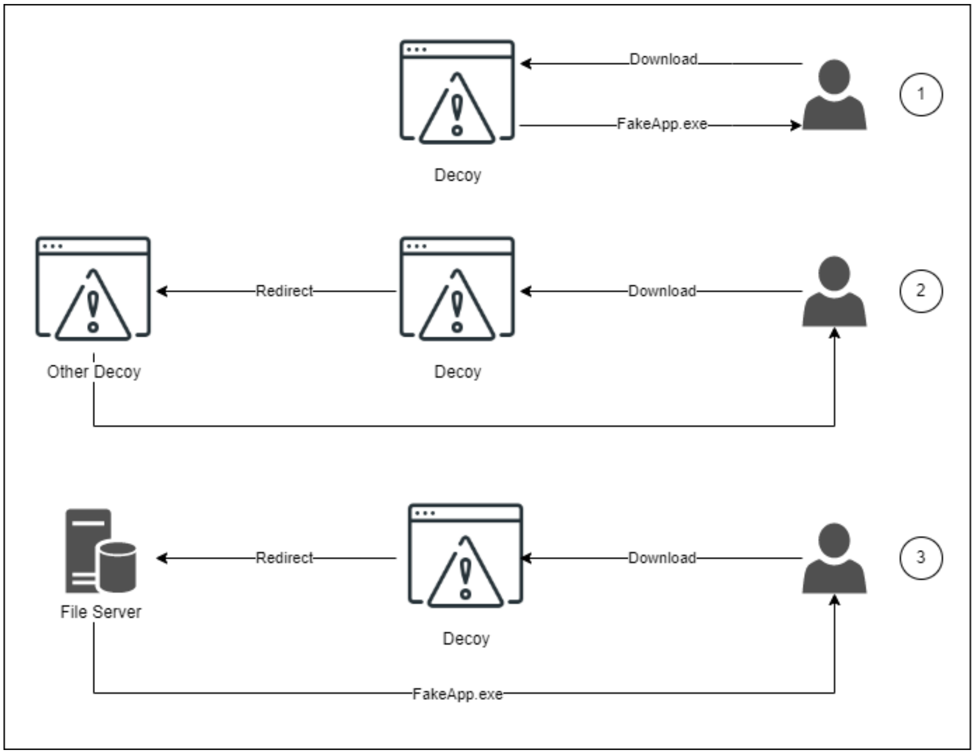
The figure below illustrates the changes the attacker made between December 2021 to February 2022.

December	January	February
spookyswap[.]fund	orca[.]mba	pegaxy[.]fund
popsicle[.]fund	xyfinance[.]fund	torix[.]fund
snowbank[.]fund	osmosiszone[.]fund	jonesdao[.]net
alchemists[.]fund	grim[.]fund	cocosbcx[.]fund
abracadabra[.]run	polychainsmonsters[.]com	gitcoin[.]fund
zapp3r[.]com	viper[.]fund	sushi-v3[.]app
olympus-dao[.]fund	woofsolana[.]fund	meritcircle[.]fund
debank[.]fund	steps[.]fund	biconomy[.]fund
polygon-project[.]com	strongblock[.]fund	oxdao[.]net
ring-finance[.]com	blocto-portto[.]fund	vvsfinance[.]fund
terra-money[.]com		thor[.]fund

It is not clear why the attacker changes the targeted applications and communities. However, we can assume they do so when their scam is revealed or when they are trying to find a better attacking landscape in new and unaware communities.

File Servers

The third step of the infection is responsible for delivering the executable to the victim. During our research period, we tracked architectural changes in this mechanism. It looks like the attacker tested several approaches, and now they converge these into their final version.



Fake application delivery methods

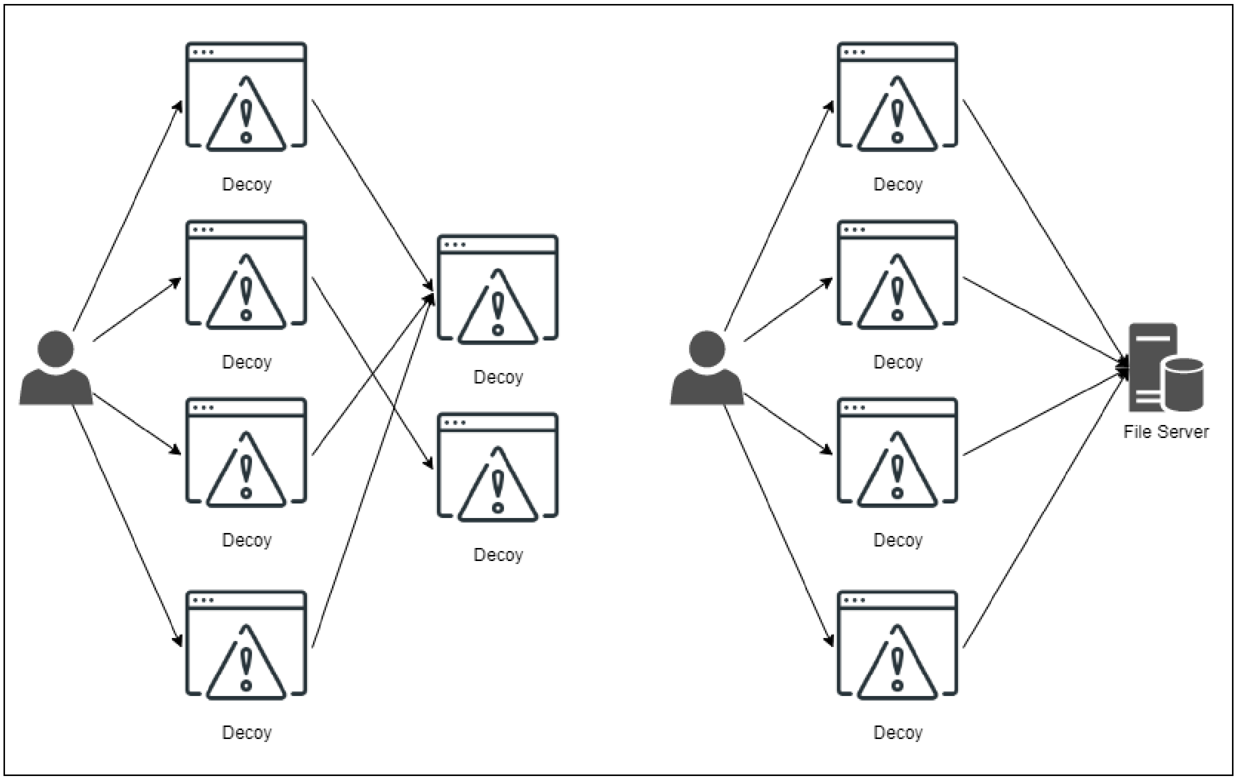
Version 1: The attacker hosted the fake application inside its respective decoy site. For example, **`terra-money[.]net`** served the file **`Terra_Station_Setup_1.2.1.exe`** when making a request to **`terra-money[.]net/station/Terra_Station_Setup_1.2.1.exe`** route.

Version 2: Cybersquatting. Decoy site A redirects the traffic to decoy site B that holds its malware. For example, **`safemoone[.]net`** is a decoy site to the original **`safemoon.net`** redirected by **`larvaslab[.]com`** to download the fake application from **`safemoone[.]us/download/LarvaLabs-App_v2.1.1-setup.exe`** route.

Version 3: All decoys download from the same centralized file server. As of writing this report, the file servers used in this campaign are:

Date Down	Domain	IP
17/12/2021 - 10/01/2022	veeffriends[.]com	46.30.40[.]105
12/01/2022 - Active	download-app-v2[.]fund	46.30.40[.]108
01/02/2022 - Active	server-storage-dwl[.]com	46.30.44[.]84

There's a clear shift between the methods used. In the beginning, the actor used the simplest working solution. We assume that the second method is a transition step to the third method - we saw a large number of decoy sites downloading from only two other decoy sites. Observing the third method, we can see that the attacker has evolved to use the "right" way from a distributed application's architecture



Fake application delivery methods

point of view.

Although the third method allows greater flexibility for the attacker to update their malware due to a centralized repository, the problem with this method is that it opens one point of failure - once the currently active file server is down, the attack chain breaks.

Hosting Services

The actor uses EuroByte's services as its preferred hosting service to deliver their fake applications. We have found references of other cybercriminals using EuroByte's services to host DCRat botnet controller (asos[.]click), Emotet (azatop[.]ru, korechok[.]ru, ...), AutoKMS (kmsmatrix[.]info), etc.

Domain	IP	Decoy Site?	Country	Hosting Service
spiritswaps[.]com	46.30.40[.]105	Yes	Russia	EuroByte.ru
splinterslands[.]com	46.30.40[.]105	Yes	Russia	EuroByte.ru
safemoone[.]us	46.30.40[.]105	Yes	Russia	EuroByte.ru
babydogescoin[.]com	46.30.40[.]105	Yes	Russia	EuroByte.ru
veeffriends[.]com	46.30.40[.]105	No	Russia	EuroByte.ru
download-app-v2[.]fund	46.30.40[.]108	No	Russia	EuroByte.ru
server-storage-dwl[.]com	46.30.40[.]84	No	Russa	EuroByte.ru

Files Delivered

The downloaded files have a similar naming convention, size, and icon as their legitimate counterparts. The naming convention and the icon help fool the victim into believing it's a legitimate application. On the other hand, a similar size may help evade scanning engines.

Domain	File Name	Size	Icon
grim[.]fund	GrimFinance-dApp-v2.3.1.exe	118MB	
metaverses-pro[.]com	MetaversePro-App-v2.0.exe	122MB	
debank[.]fund	DeBank-dApp-v2.2-release.exe	122MB	
helium-app[.]com	Helium-App-v2.2-release.exe	116MB	
moonebeam[.]com	MoonbeamApp-v2.1.0_release.exe	108MB	

Execution Methods

After mapping the infrastructure used throughout the campaign, we dug into the actor's execution methods. This campaign was first revealed when our team researched a new crypter used in the wild, but that's not the only crypter used.

At the beginning of the campaign (see the table below), we saw evidence of the actor using custom .NET Crypters and Crypto Obfuscator. However, starting from August 2021, it looks like the actor has moved to use BABADEDA Crypter as their main crypter of choice.

Although we don't think this threat actor is the developer behind BABADEDA Crypter, we found that they are the first to use the latest variants. This may suggest that this threat actor purchased a private stub or that there is a close relationship between the two.

By now, we know who the victims are, and we are also aware of the attacker's goal. What's left is understanding how the goal was achieved. To answer this question, we traced the final payload from the beginning of the campaign to the end. This resulted in three different RATs used as the final payload - Remcos, BitRAT, and AsyncRAT.

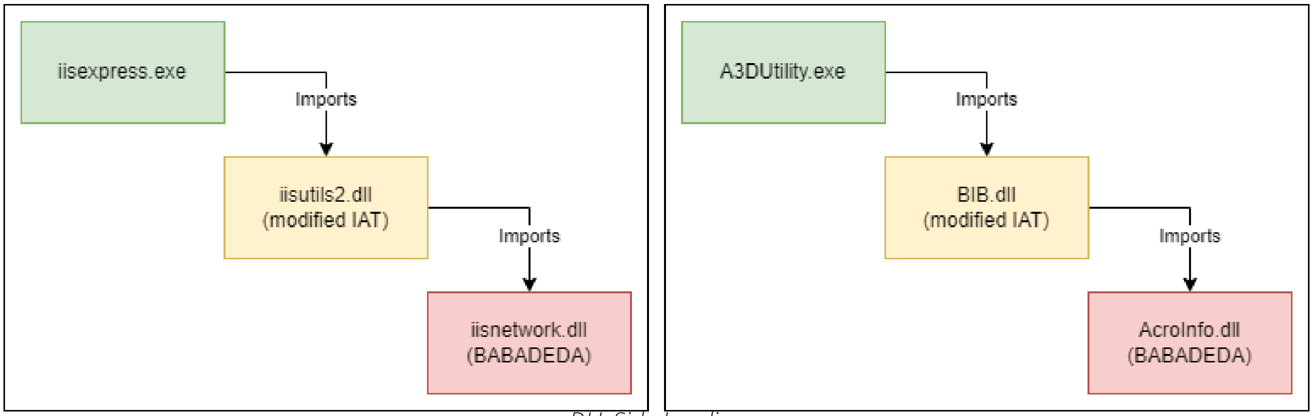
This can be seen in the following table:

Date	Packer/Crypter	Payload	C2	Port
11/2020 - 07/2021	Custom .NET packer	Remcos	95.217.114[.]96 37.48.89[.]8 94.23.218[.]87	4782 4783
07/2021 - 08/2021	Crypto Obfuscator (.NET)	Remcos	135.181.17[.]47	4783
08/2021 - 10/2021	BABADEDA	BitRAT	135.181.140[.]182 135.181.140[.]153 135.181.6[.]215	7777
11/2021 - 12/2021	BABADEDA using DLL sideloading with IIS Express	Remcos AsyncRAT	65.21.127[.]164	4783 4449
12/2021 - *Active	BABADEDA using DLL sideloading with Adobe/TopoEdit	Remcos	193.56.29[.]242	4783
01/2022 - *Active	BABADEDA using DLL sideloading with Link.exe	Remcos	157.90.1.54	4783

*Active - At the time of writing

Technical Details

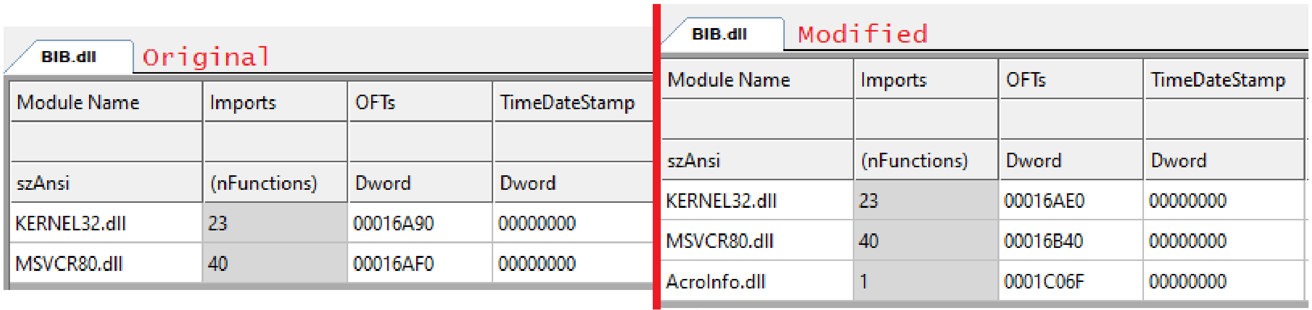
One of the more recent features added to the attack chain is the usage of a DLL sideloading attack to inject the final payload into a benign application. In our previous research, we explained in detail the inner workings of the BABADEDA Crypter. During our current investigation, we observed that all fake applications utilize a DLL Side-Loading technique on trusted applications such as **`iisexpress.exe`** (IIS Express), **`A3DUtility.exe`** (Adobe Acrobat Reader), and **`TopoEdit.exe`** (Microsoft tool)



DLL Side-Loading

The additional layer allows attackers to run the BABADEDA Crypter under a legitimate process instead of a fake one, as done previously. As shown in the figure above, a new DLL is loaded into the process.

First, the fake application's installer will unpack the files to the destination directory. Then it launches the benign executable, for example, **`A3DUtility.exe`**. Inside the executable's import table, we will find **`BIB.dll`** import. This is a modified version of the original **`BIB.dll`**, used for sideloading the first stage of the malicious payload. This version of **`BIB.dll`** isn't signed and has another entry in its IAT - an import of **`AcroInfo.dll`**.

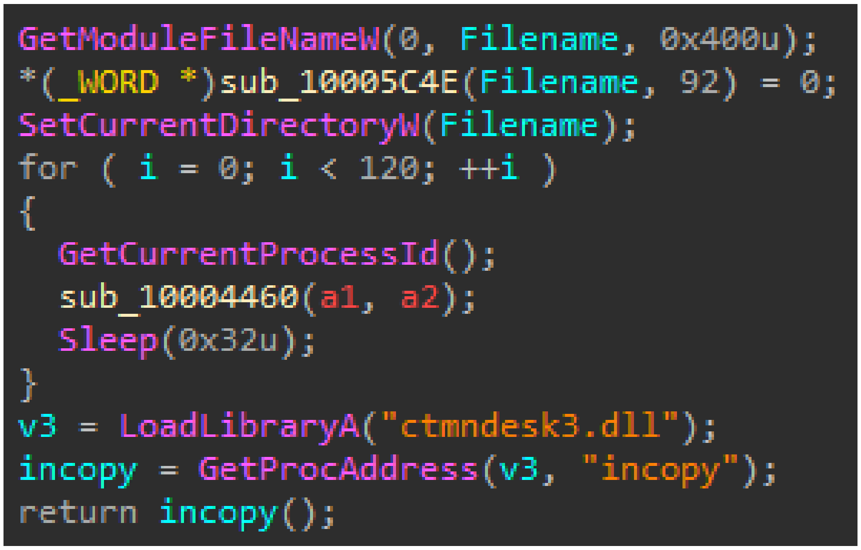


Module Name	Imports	OFTs	TimeDateStamp
szAnsi	(nFunctions)	Dword	Dword
KERNEL32.dll	23	00016A90	00000000
MSVCR80.dll	40	00016AF0	00000000

Module Name	Imports	OFTs	TimeDateStamp
szAnsi	(nFunctions)	Dword	Dword
KERNEL32.dll	23	00016AE0	00000000
MSVCR80.dll	40	00016B40	00000000
AcroInfo.dll	1	0001C06F	00000000

IAT comparison

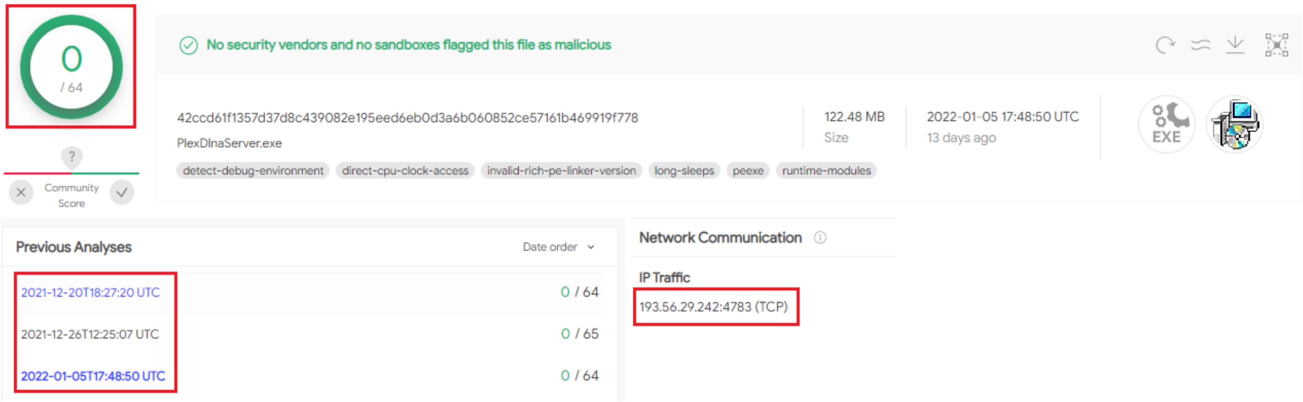
Although the name may trick you into thinking this file is part of a benign Adobe Reader installation, in reality, this DLL loads the BABADEDA Crypter we covered in our previous research.



```
GetModuleFileNameW(0, Filename, 0x400u);
*(_WORD *)sub_10005C4E(Filename, 92) = 0;
SetCurrentDirectoryW(Filename);
for ( i = 0; i < 120; ++i )
{
  GetCurrentProcessId();
  sub_10004460(a1, a2);
  Sleep(0x32u);
}
v3 = LoadLibraryA("ctmndesk3.dll");
incopy = GetProcAddress(v3, "incopy");
return incopy();
```

Loading BABADEDA Crypter's DLL

BABADEDA Crypter already had a low detection rate in VT, and the new variant helps keep it totally FUD for multiple scans, as seen below.



No security vendors and no sandboxes flagged this file as malicious

42ccd61f1357d37d8c439082e195eed6eb0d3a6b060852ce57161b469919f778
PlexDlnaServer.exe

122.48 MB
Size

2022-01-05 17:48:50 UTC
13 days ago

detect-debug-environment · direct-cpu-clock-access · invalid-rich-pe-linker-version · long-sleeps · peexe · runtime-modules

Previous Analyses — Date order

2021-12-20T18:27:20 UTC	0 / 64
2021-12-26T12:25:07 UTC	0 / 65
2022-01-05T17:48:50 UTC	0 / 64

Network Communication

IP Traffic
193.56.29.242:4783 (TCP)

Totally FUD Remcos payload taking with its C2

Options to Prevention and Response

Gaining Insights

Hacked credentials and crypto accounts are among the most sought-after and valuable items for purchase on the dark web and underground communities. Due to the skyrocketing prices of BTC, ETH, and other cryptocurrencies, hacked accounts may hold large sums of coin-based currency and cash, protected by relaxed security measures after the initial verification process. This can then be cashed in for NFTs and other high-value goods in the metaverse and the physical world.

Crypto	$ Average Price (USD) 2021
Hacked Coinbase verified account	$610
USA verified LocalBitcoins account	$350
Cypto.com verified account	$300
Coinfield.com verified account	$410
Kraken verified account	$810
Cex.io verified account	$710
Blockchain.com verified account	$310
Binance verified account	$410

Example listings of hacked cyptocurrency site accounts being sold.

Source: Privacy Affairs Dark Web Price Index

Morphisec Insights, as well as Morphisec Threat Intelligence, can act as an early warning system for your enterprise to give you visibility into criminals that are targeting your employees and organization. Credential theft and account takeover is a common entry point for criminals to establish a foothold into your organization and move laterally, further enforcing more damage to business operations and critical assets. The industry best practice is to monitor the areas where criminals operate to mitigate attacks before they occur.

Moving Target Defense

As a prevention-focused solution, Morphisec Guard morphs device memory to confuse and trap attacks that avoid NGAV solutions. As a result, defenders can automatically protect assets like NFTs and cryptocurrencies against zero-day threats like the crypters discussed in this report.

When All Else Fails

In many cases, we have found that it is already too late to prevent this type of attack from occurring, and incident response (IR) is needed. Morphisec Incident Response team works collaboratively with client organizations to triage critical security incidents and conduct forensic analysis to solve immediate cyberattacks, as well as provide recommendations for reducing your organization's risk exposure.

The Morphisec IR team will leverage this insight to:

- Help contain in-progress incidents and reduce damage.
- Provide recommendations for long-term risk reduction.
- Audit critical infrastructure to ensure you have the lowest possible risk of exposure to a cyberattack.

Contact the Morphisec IR Team

Conclusion

As demonstrated above, these highly dangerous crypters can have a devastating effect. Targeting cryptocurrency users through trusted attack vectors gives its distributors a fast-growing selection of potential victims. Because crypters can masquerade as known applications with complex obfuscation techniques, anyone relying on traditional signature-based malware detection has no way of knowing if a crypter is on their machine and can't stop it from executing. Machine learning and behavior-based endpoint protection platforms (EPP) or endpoint detection and response (EDR) solutions may also have a difficult time detecting this type of attack, as they are not as effective against in-memory attacks.

Mitigating the threat posed by a crypter requires securing the device memory it targets. Morphisec does this through Moving Target Defense (MTD), a technology that creates a dynamic attack surface and morphs process memory to trap crypters like BABADEDA before they are able to deploy.

IOCs

More IOCs can be found in our previous blog.

Decoy Websites

Domains

alchemists[.]fund
metaverses-pro[.]com
ragnarok.vercel[.]fund
woofsolana[.]fund
babyswap[.]fund
spookyswap[.]fund
polygon-project[.]com
viper[.]fund
osmosiszone[.]fund
popsicle[.]fund
snowbank[.]fund
grim[.]fund
spartacadabra[.]fund
ring-finance[.]com
helium-app[.]com
zapp3r[.]com
terra-money[.]com
wonderlaned[.]com
jadeprotocol[.]fund
strongblock[.]fund
avaxbridge[.]fund
polychainsmonsters[.]com
debank[.]fund
steps[.]fund
abracadabra[.]run
boredpeyachtclub[.]com
vercel[.]fund
orca[.]mba
blocto-portto[.]fund
spartacus[.]fund
thorswap[.]fund
xyfinance[.]fund
olympus-dao[.]fund
invictusdao[.]fund
traderjoexyz[.]fund
pegaxy[.]fund
torix[.]fund
jonesdao[.]net
cocosbcx[.]fund
gitcoin[.]fund
sushi-v3[.]app
meritcircle[.]fund
biconomy[.]fund
oxdao[.]net
vvsfinance[.]fund
thor[.]fund
marinade[.]fund
paragonsdao[.]net
avalaunch-app[.]com
pancakeswaps[.]fund
diviprojects[.]com
runonflux[.]net

IP Addresses

185.212.130[.]108
185.212.130[.]109
185.212.130[.]110
185.212.130[.]111
185.212.130[.]157
185.212.130[.]129
185.212.130[.]199
185.212.130[.]132
185.212.130[.]133
185.212.130[.]218

File Servers

Domains

veeffriends[.]com
download-app-v2[.]fund
server-storage-dwl.com

IP Addresses

46.30.40[.]105
46.30.40[.]108
46.30.44[.]84

C2 Servers

95.217.114[.]96
37.48.89[.]8
94.23.218[.]87
135.181.17[.]47
135.181.140[.]182
135.181.140[.]153
135.181.6[.]215
65.21.127[.]164
193.56.29[.]242
157.90.1[.]54

Fake Applications

```
7e827e1981d2ccaec16a5b646976b0d492d555a20b9ba5dd4ba0d605dfcab2f7
c62d330c24d04b2a915529ed78ea6692360b18918886d73081300e8f97f3c544
ee8ebd97891ca6492355cfd5c964405a3269f428f91396a7c68b8aba965b4dab
a17be0cd6fe63cef8d742895c8f7a8b5ce3d4568b68c62c852388276f9d39462
4fed886fb15c2b8013471dd3a00f1dd4f92c1222d7e901e7712bc51a4e8553cf
4805e9e5317478e816c0d951dc5fa960abb2b49944ebcaac2a01b92cacd4c0e6
332a687e95a47bbae4ce2952ff288055bd8c32731a823e2a8fae04f127afd3a0
df332e7ab12e8616cc372e67a333a2e7bb8767f30918724f34d23a684db6bcb4
e5b90abfcc0bdd325d547473c30cce977dcd41906d1b5ee52569fced477343c2
14da3566bc9f211528c1824330c46789396447c83c3c830bb91490d873025df8
a19c03d7ca8f50a2c840f10631d26e1b40742c46e05964b60852e9eb8c697234
2e5455e268cf12ebc0213aa5dacb2239358c316dda3ec0f99d0f36074f41fb09
bcaaab0cd2178acdf025c7f23f10ab01906a99aca5d07e3a7e261928f8f91695
a63b3acebe111d575cdbdfeb657989ae6a92e9e41671abbf7d8e26a8fb9c38f9
2eb4b9d985bc1fad0566cb51ac504841358918aa3ea2c8062c3916d576711bb3
457753d6d5c69ddf06528bbfa0d8c9170ea5e7fac9cb87297c1eaf39c57e760b
b1865018b392f374c7237bebcdf38b72d31668ad8b1c6376eeb3a405e11ce6a2
2e3355742ee27347ec089d645a0697068c833ed7ea8fdef10d6aa1b0f87ab692
c33e81267dbc9ff93e82492a8d826e95788fd2fc8fcc79053d31d17e5c7ea8f3
2a8bf9c645496e62b71a8e3a74aebb68f8fbeae3b5b7712d36ddd2a234561a3c
d7bf594ca3051dc2c809d69254ddf00497df644e44a8b30af65318e146f35f81
7aece75112f882c05c6742213d816c2a3cc54aee9df445a21da8fd35dae2dfc2
0115ba0f26a7b7ca3748699f782538fa761f7be4845a9dc56a679acea7b76cd3
be87ab0b64d89333e96ed8f97cd5d67c374df13183b573f9a7f206217780f667
214d6681f5d82d4fa43e7a8676935ef01ddab8d0847eb3018530aedffe7ebb55
18c01e1f6e0185752dbf8c9352d74ade56ac40d25ae701d4a5954b74d0c7aeea
44b1c156635bc6cd0bfc9b784077fe4b912df90298e3cfc8bc4f98af5450e846
41f1f642353b024f2c1d709e58e0c2c7b8699a6b24f12a4f9c0ff36f86bdf2d7
466609938501952b9818091551e4d297718d03b65aa081c1af8c7ca7fc90b282
d360daf106314561e9ec57075dd4f544ad52680678a644e186758650a405b765
bfd7dac0fdd4cc92f11d775e9d27399c30e81cb6d7515f7b255d180499bfc0ca
4a289a5f0342365442564bbe9a09f7a1a3f23af0769a01769f58dd49504cca87
992aed6d1cfe2f07530deb7c6279faff141a46838165b88f73bcce5dacf8ee12
a2cd8d088ca9d67617ee4fe198232ca6b4eeec01419f2c3fbb1b543f8f166ecf
4fc19e9319a6af5c4568a1b019f06a000232892ee8e5eb8fc8c1f0d48e8c8199
f5f8917076a7ed3e13386a95904a235eedf281d8f5cc06748816b577eb5dc6ff
1da341ec03b5f70da9a6016dfefb298bffb4522408b9486314afd7fc02d0017f
3c844e66f0dafdced0861a8e2ff54fd762ba170bf5082fb2c38cdbbac5a7fecb
e99d32952bda84f32425681229ec544849156e479b7247e3e480f3a23a39c915
d6abbfbd4b7f1e84e2e9833a912b86ffc5b9ca6165ed4fe874d0071181b55353
7506a8784ac064884072a2aba84524ca27cd0b5ab66b7156d54926585673f9bf
```