MAKSRAT Breakdown

A Break Down Of Another Minecraft MaaS provider

Java malware, although uncommon to make the news if it's not for a new Android app being discovered to be a botnet or spyware in disguise, is beginning to infect the famous block game that many of you might have played, Minecraft. Although the first major news coverage of Minecraft malware was from the *Fracturizer* stealer/worm in 2023, Minecraft Malware has been around for a lot longer than that. With just a simple search on GitHub, I was able to find old stealers from 2021, and I'm sure there were earlier versions that, but over the years, GitHub staff probably removed them due to obvious reasons. Many of the Minecraft-focused stealers began surging in popularity sometime after Discord's launch of their webhook feature in 2020, which allows a free and easy way for attackers to exfiltrate data from a victim's PC.

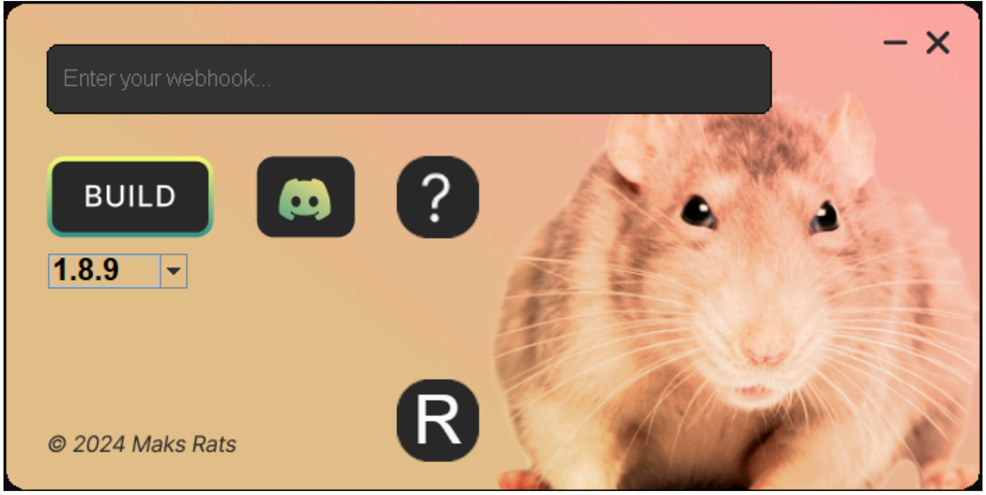
In 2020, I began my deep dive into Java and Java deobfuscation. When I began to find Java stealers disguised as mods, many of them had no obfuscation, which revealed the attacker's Discord webhook in plaintext when looked at with a Java bytecode editor like Recaf. With a plain text Discord webhook URL, you could easily delete the webhook by just sending a DELETE request to that URL. In 2020 and early into 2021, I got a good laugh out of deleting the webhooks of attackers who had skills closer to a script kiddie than any actual threat. This was until a new Java obfuscator was released in November 2021. Called *Skidfuscator*, this new obfuscator was free and easy to use, exactly what the unskilled threat actors needed.

Slowly, the days of plain text webhooks began being replaced by stealers' obfuscated.
Since the release of things such as Discord's webhooks and *Skidfuscator*, Minecraft malware has slowly begun spreading across the mod space. Minecraft, unlike other games, has a large majority of its player base using mods, either to just increase the game's performance or add new features to the game entirely. With the majority of Minecraft's player base using mods, the threat of malicious mods is greater than with other games, and it seems that skilled threat actors are beginning to realize that.

ILoveRat is a 17 year old threat actor who says their name is Max (yes, they do give us all that information publicly in their code, which I will go over later), is the owner of a large MaaS provider for Minecraft Malware. It's hard to believe that they alone developed this stealer since their OPSEC is so terrible, leaking multiple screenshots of their username for games like Valorant and Steam, as well as leaking their last name as Vavrik in yet another screenshot sent to a public Discord server. Finally, due to them having many of their games in Russian, I'm going to assume they are from Russia.

ILoveRat's community has stolen credentials from well over 2.5 thousand users in the Minecraft community (this number is based on the number of "hits" they post each "hit" in one of their Discord channels). As I examined his malware, I began to realize this was one of the worst-protected Minecraft stealers that were being sold in mass. His malware didn't have even the most basic protections against debugging, traffic capturing, and didn't even try to implement VM detection. With nothing more than basic obfuscation from the Skid classic *Skidfuscator,* it wasn't too hard to get a good idea of what all this malware was capable of, especially with the added bonus of them not removing all the logging they used.

Getting into the actual malware builder, I noticed that most of their traffic was directed over sockets, something that *Mitmproxy* couldn't intercept, meaning I would have to switch over to *Wireshark*. When opening their builder, I was presented with a GUI that gave me 2 options: I could either submit a Discord webhook to have my stealer sent to, or I could submit a code that I later learned was to gain access to their "Premium jar access". Below this paragraph, you can see an image of what their builder looks like (It's worth noting that to build their stealer, you must download a .jar and run it on your pc).



MAKSRAT Breakdown

A Break Down Of Another Minecraft MaaS provider

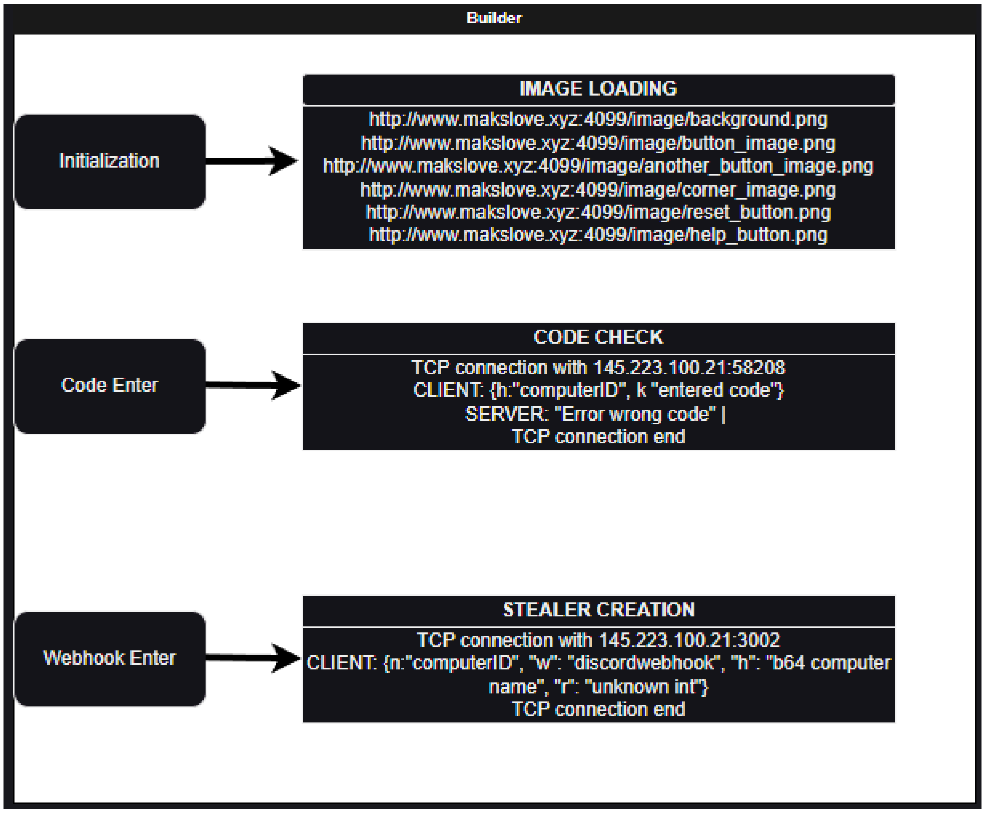


IMAGE LOADING

```
http://www.makslove.xyz:4099/image/background.png
http://www.makslove.xyz:4099/image/button_image.png
http://www.makslove.xyz:4099/image/another_button_image.png
http://www.makslove.xyz:4099/image/corner_image.png
http://www.makslove.xyz:4099/image/reset_button.png
http://www.makslove.xyz:4099/image/help_button.png
```

CODE CHECK

```
TCP connection with 145.223.100.21:58208
CLIENT: {h:"computerID", k "entered code"}
SERVER: "Error wrong code" |
TCP connection end
```

STEALER CREATION

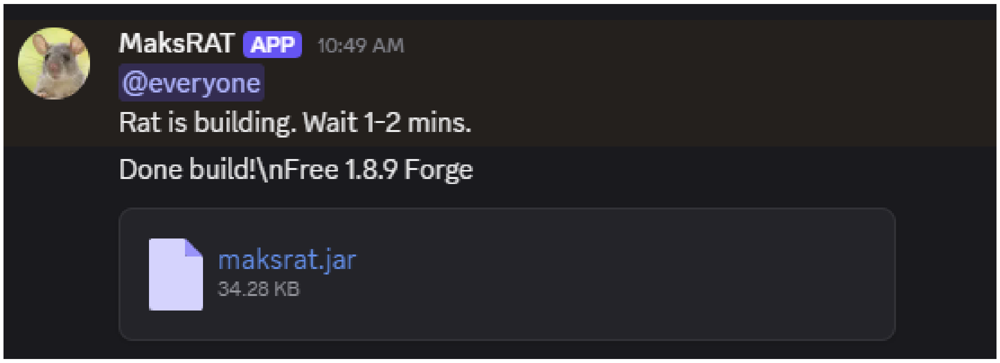
```
TCP connection with 145.223.100.21:3002
CLIENT: {n:"computerID", "w": "discordwebhook", "h": "b64 computer name", "r": "unknown int"}
TCP connection end
```

To the Left, you are able to see all observed connections that the builder makes.

Due to my obviously not wanting to give this person any money, I couldn't test what the server would return if I had the correct code, so that is still unknown.

The *computerID* you see me reference, I was able to figure out by looking through the builder after deobfuscation in Recaf. There I learnt that the computer ID was made up of 3 key things that the program got by using "System.getenv"; those things are "user.name", "COMPUTERNAME", and "PROCESSOR_IDENTIFIER", after it gets all white space and commas removed. All this information is then put together into a single string and encrypted with base64

When a Stealer is built with their builder, it will quickly be sent to the webhook you input and appear like this



MaksRAT APP 10:49 AM
@everyone
Rat is building. Wait 1-2 mins.

Done build!\nFree 1.8.9 Forge

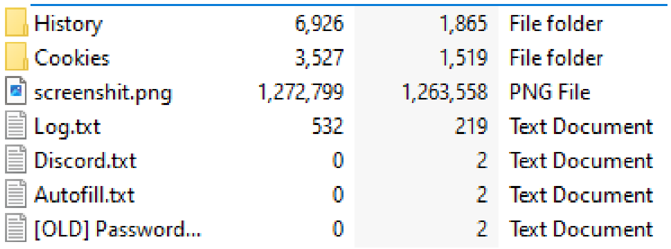
maksrat.jar
34.28 KB

When getting into the actual stealer that affiliates will get access to, you can quickly see that with a file size of close to 35kb, this has to be a multi-stage stealer. What I will call the initiation file can be run in 2 different ways: either by running it as a Minecraft mod or by double-clicking it. When running the initiation file, it will quickly query their server for 2 additional files, those being "discord" and "download", which I will be referring to as "Discord" (very creative), and "Main".

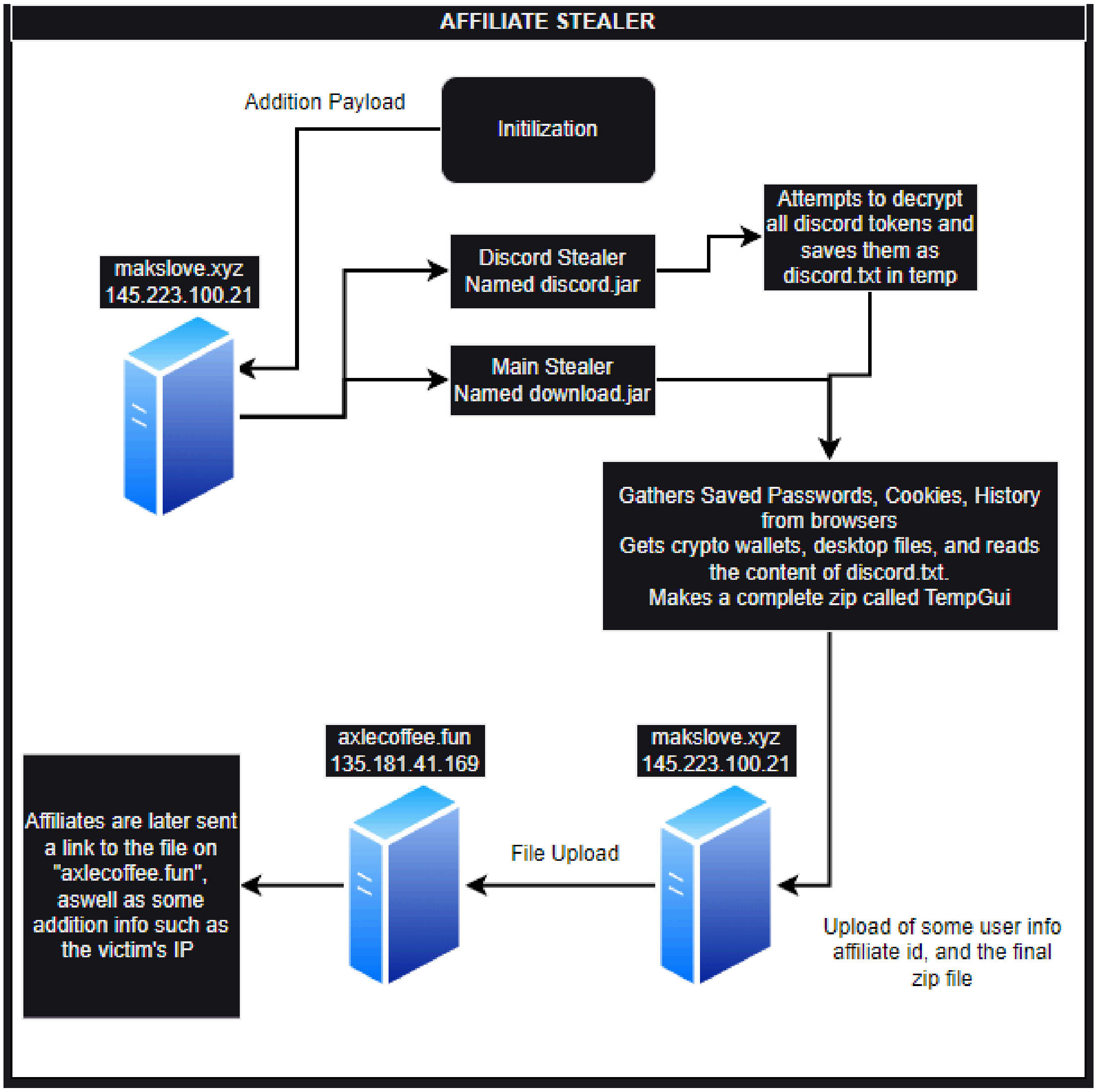
When running, the Discord jar begins decrypting Discord tokens from the victim's pc, both attempting to get them from the Discord client and the Firefox browser. If a token is found 2 things can happen if the victim is in ILoveRat's discord server it will simply print in console telling the user to not test the rat on themselves than save the token in a file called discord.txt in the temp directory, or if the victim isn't in the server it will begin using their discord token to mass message all the victim's added friends promoting their server, and attempt to send a message in every server that the user is in also promoting their server, finishing by writing the decrypted discord token in the same file discord.txt

When the Main jar gets executed, it begins scraping all the info that it can. Starting with a screenshot, then going for different Minecraft clients (Lunar, IAS, CursedForge, to name a few), then moving onto possible crypto wallets, finishing up by going through the victim's browsers, attempting to get all the autofill credentials the user has.

When Main has finished storing all the data that it can grab, it does 2 things: one of those is attempting to inject the rat into the Discord client, so that whenever the user launches Discord, it sends all the info all over again, and it creates a folder in temp called "TempGui" then adds an additional folder called "ilr-{computer name}" is where all the data is dumped.
This data is later compressed into a zip file and uploaded to the attackers' server, then uploaded to a secondary server that provides a download link that the affiliates use.



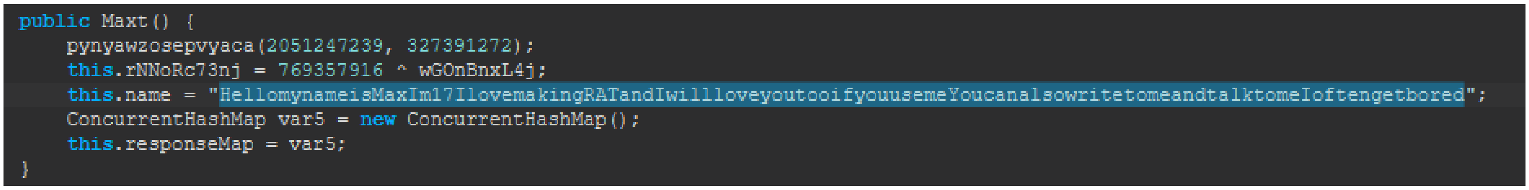
History	6,926	1,865	File folder
Cookies	3,527	1,519	File folder
screenshit.png	1,272,799	1,263,558	PNG File
Log.txt	532	219	Text Document
Discord.txt	0	2	Text Document
Autofill.txt	0	2	Text Document
[OLD] Password...	0	2	Text Document


AFFILIATE STEALER
Addition Payload
Initilization
makslove.xyz
145.223.100.21
Discord Stealer
Named discord.jar
Attempts to decrypt all discord tokens and saves them as discord.txt in temp
Main Stealer
Named download.jar
Gathers Saved Passwords, Cookies, History from browsers
Gets crypto wallets, desktop files, and reads the content of discord.txt.
Makes a complete zip called TempGui
axlecoffee.fun
135.181.41.169
makslove.xyz
145.223.100.21
Affiliates are later sent a link to the file on "axlecoffee.fun", aswell as some addition info such as the victim's IP
File Upload
Upload of some user info affiliate id, and the final zip file

MAKSRAT Breakdown

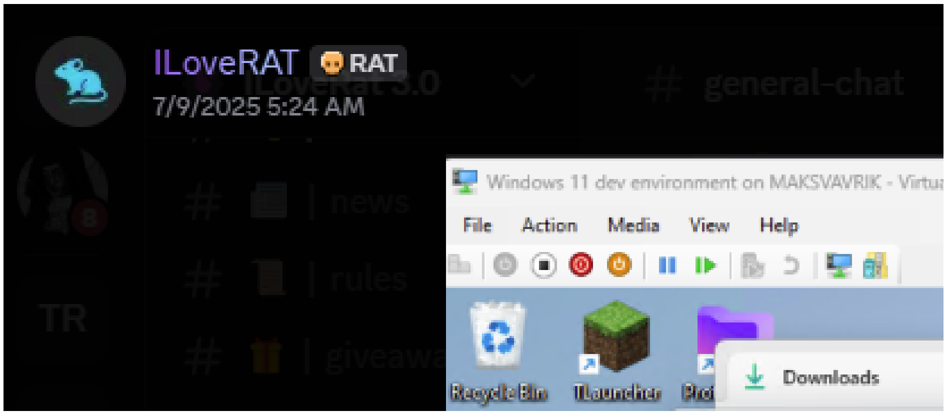
A Break Down Of Another Minecraft MaaS provider

Now with all the technical break down of this stealer over with I can go over all the funny things I found while working, and obviously clown the creator of this stealer ILoveRat. While first going over this stealer I was looking into the Main jar file, and after removing all the packaged libraries I ran it through a deobfuscator to make my life a little easier finally loading it into Recaf. One of the first strings I saw when looking at it was "HellomynameisMaxIm17IlovemakingRATandIwillloveyoutooifyouusemeYoucanalsowritetomeandtalktomeIoftengetbored"



```
public Maxt() {
    pynyawzosepvyaca(2051247239, 327391272);
    this.rNNoRc73nj = 769357916 ^ wGOnBnxL4j;
    this.name = "HellomynameisMaxIm17IlovemakingRATandIwillloveyoutooifyouusemeYoucanalsowritetomeandtalktomeIoftengetbored";
    ConcurrentHashMap var5 = new ConcurrentHashMap();
    this.responseMap = var5;
}
```

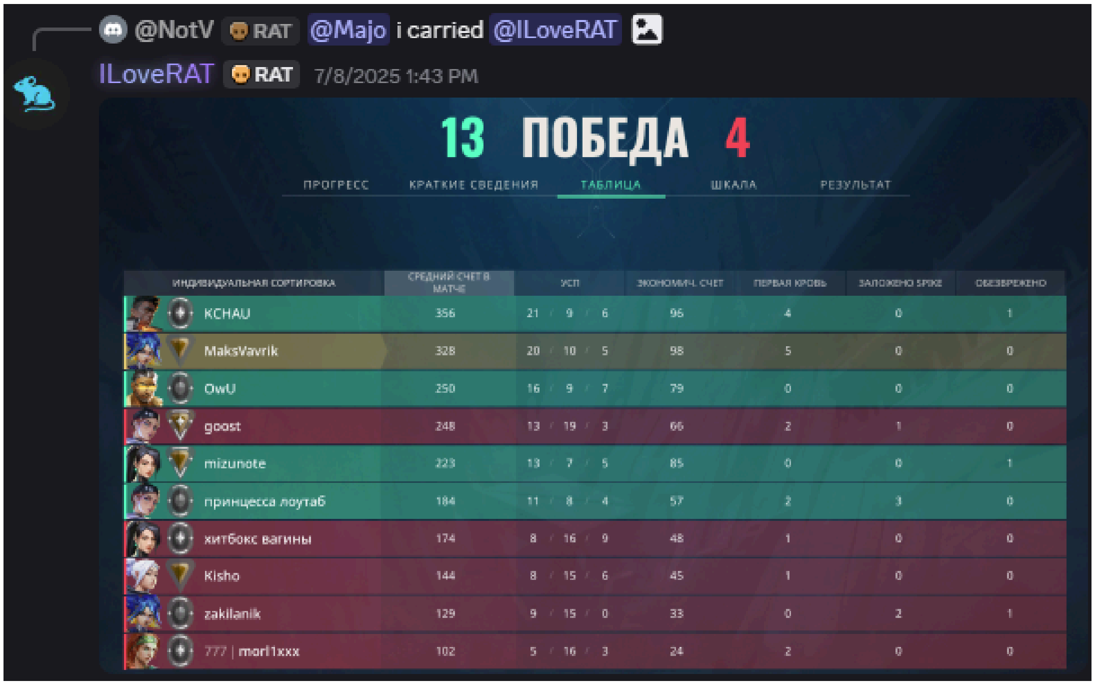
No I wasn't kidding earlier when I said before that he told me all this in "his" code when looking into his messages of his discord servers I found some other things. Either due to his stupidity or over confidence there were two screenshots he sent that just displayed how poor his OPSEC is.



ILoveRAT RAT
7/9/2025 5:24 AM

Looking at this screenshot we can see clearly that ILoveRAT posted it and by looking at the name of the VM he is on you can read "MAKSVAVRIK". At this point I was lost for words he has given us his entire name which is risky enough just normally being on the internet, but when your the owner of a almost 300 member community that spreads stealer software words cant describe how dumb that is.

Just incase you didn't realize how little he cares about OPSEC here is another image posted by him revealing that same name again but on Valorant. As you can see these two screenshots are only a day apart revealing just how much private information he enjoys leaking.



@NotV RAT @Majo i carried @ILoveRAT

ILoveRAT RAT 7/8/2025 1:43 PM

13 ПОБЕДА 4

ИНДИВИДУАЛЬНАЯ СОРТИРОВКА	СРЕДНИЙ СЧЕТ В МАТЧЕ	УСП	ЭКОНОМИЧ. СЧЕТ	ПЕРВАЯ КРОВЬ	ЗАЛОЖЕНО SPIKE	ОБЕЗВРЕЖЕНО
KCHAU	356	21 / 9 / 6	96	4	0	1
MaksVavrik	328	20 / 10 / 5	98	5	0	0
OwU	250	16 / 9 / 7	79	0	0	0
goost	248	13 / 19 / 3	66	2	1	0
mizunote	223	13 / 7 / 5	85	0	0	1
принцесса лоутаб	184	11 / 8 / 4	57	2	3	0
хитбокс вагины	174	8 / 16 / 9	48	1	0	0
Kisho	144	8 / 15 / 6	45	1	0	0
zakilanik	129	9 / 15 / 0	33	0	2	1
777 | morl1xxx	102	5 / 16 / 3	24	2	0	0

Builder

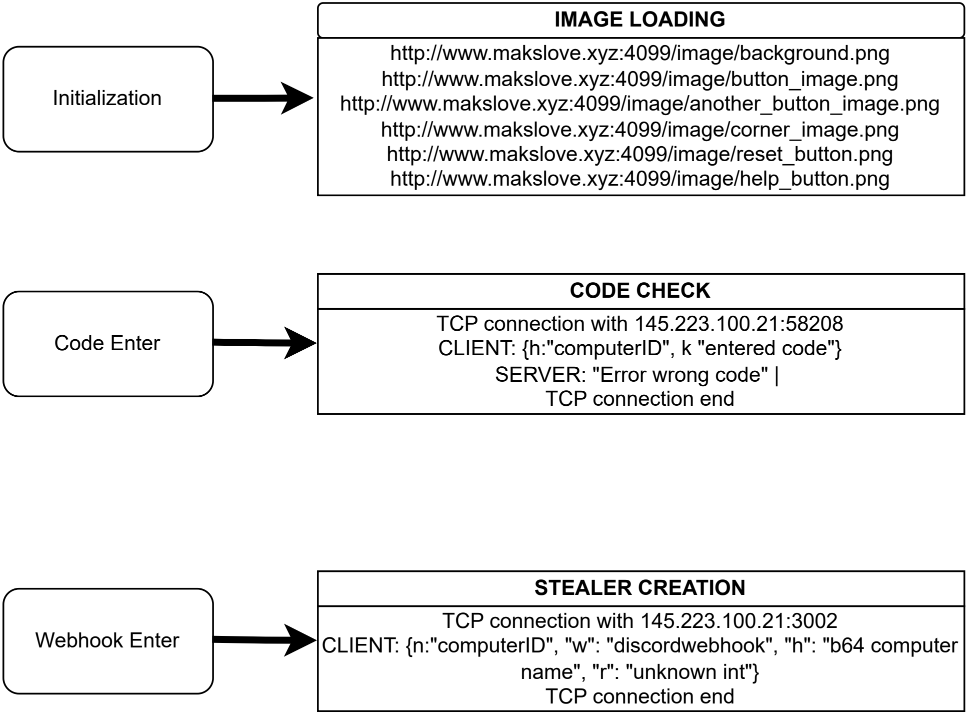


IMAGE LOADING

http://www.makslove.xyz:4099/image/background.png
http://www.makslove.xyz:4099/image/button_image.png
http://www.makslove.xyz:4099/image/another_button_image.png
http://www.makslove.xyz:4099/image/corner_image.png
http://www.makslove.xyz:4099/image/reset_button.png
http://www.makslove.xyz:4099/image/help_button.png

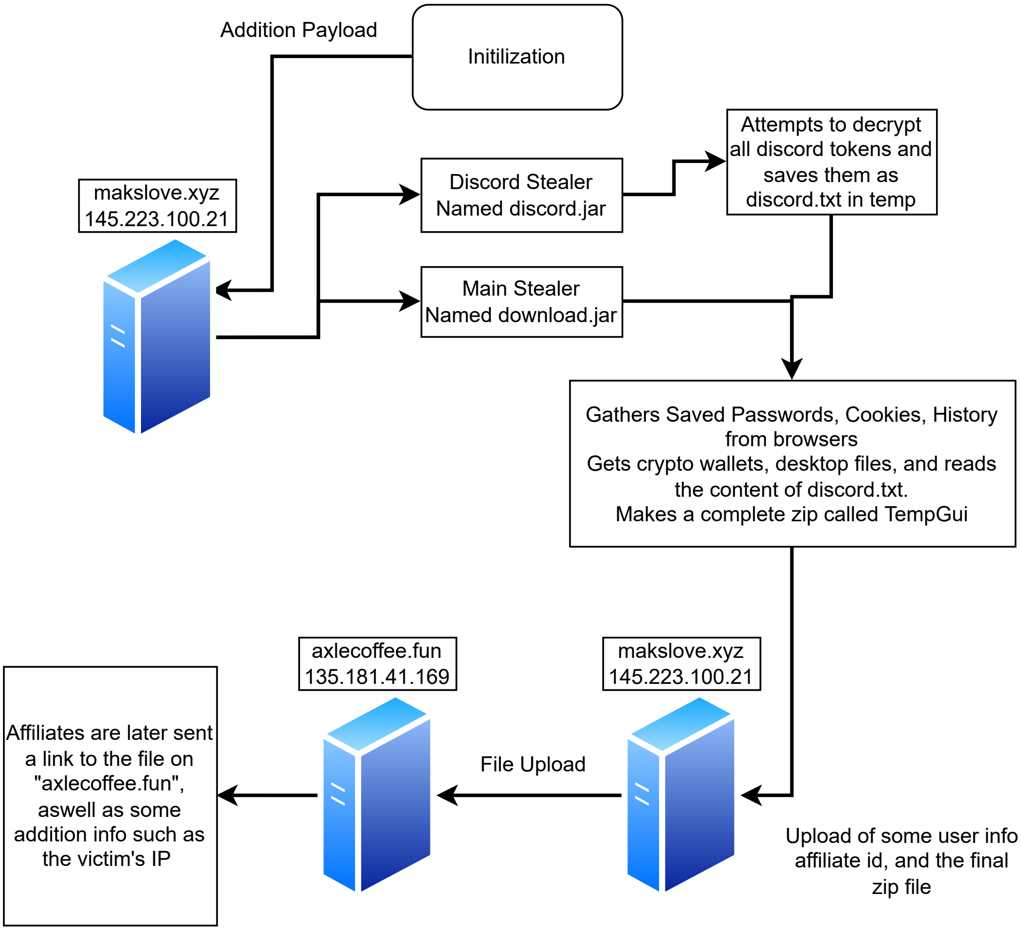
CODE CHECK

TCP connection with 145.223.100.21:58208
CLIENT: {h:"computerID", k "entered code"}
SERVER: "Error wrong code" |
TCP connection end

STEALER CREATION

TCP connection with 145.223.100.21:3002
CLIENT: {n:"computerID", "w": "discordwebhook", "h": "b64 computer name", "r": "unknown int"}
TCP connection end

AFFILIATE STEALER



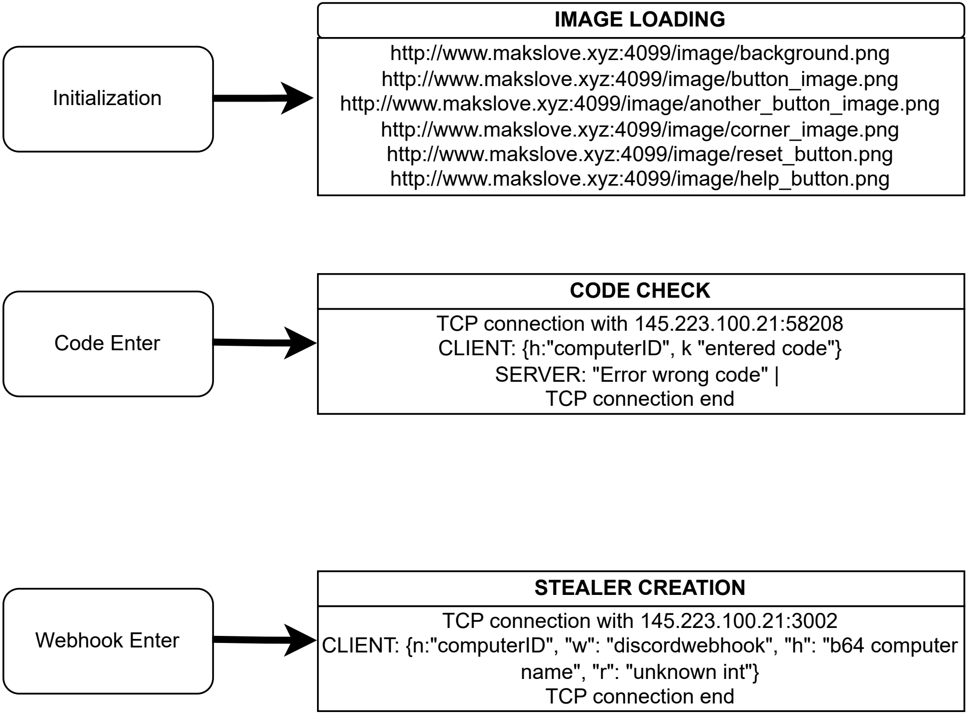
Attempts to decrypt all discord tokens and saves them as discord.txt in temp

Gathers Saved Passwords, Cookies, History from browsers
Gets crypto wallets, desktop files, and reads the content of discord.txt.
Makes a complete zip called TempGui

Affiliates are later sent a link to the file on "axlecoffee.fun", aswell as some addition info such as the victim's IP

Upload of some user info affiliate id, and the final zip file

Builder



Initialization

IMAGE LOADING

http://www.makslove.xyz:4099/image/background.png
http://www.makslove.xyz:4099/image/button_image.png
http://www.makslove.xyz:4099/image/another_button_image.png
http://www.makslove.xyz:4099/image/corner_image.png
http://www.makslove.xyz:4099/image/reset_button.png
http://www.makslove.xyz:4099/image/help_button.png

Code Enter

CODE CHECK

TCP connection with 145.223.100.21:58208
CLIENT: {h:"computerID", k "entered code"}
SERVER: "Error wrong code" |
TCP connection end

Webhook Enter

STEALER CREATION

TCP connection with 145.223.100.21:3002
CLIENT: {n:"computerID", "w": "discordwebhook", "h": "b64 computer name", "r": "unknown int"}
TCP connection end