

# Empowering your abusers

## The Discord case



**CHALMERS**  
UNIVERSITY OF TECHNOLOGY



UNIVERSITY OF  
GOTHENBURG

**kit**s  
keep it secure

Francisco Blas Izquierdo Riera (klondike)

# Myexia / Melusa

A Discordian Credential Stealer



**CHALMERS**  
UNIVERSITY OF TECHNOLOGY



UNIVERSITY OF  
GOTHENBURG

**kit**s  
keep it secure

Francisco Blas Izquierdo Riera (klondike)

Mandatory controversial statement

**IRC IS DEAD!**

**LONG LIVE**

**DISCORD!**




**CHALMERS**  
UNIVERSITY OF TECHNOLOGY



UNIVERSITY OF GOTHENBURG


# The setup

# Initial report by S

8/3/26, 22:22  
ha want to pry apart some malware?   
got someone that was attempting the tokenstealer thing.  
I'm playing dumb but already reported the url and dropbox link for  
abuse and malware/RAT spreading

03:27 hey hey  
how you been?  
03:31 yeah good  
work still going on as usual  
03:34 good good  
can i ask you a favor?  
03:34 oh what would that be  
21:35 ive been working on a project for past 5 month, and its out NOW! thats why i reached you  
Ive need someone to test for me and give a basic HONEST feedback, if you got some free time could you help me?  
22:03 oh what is that  
22:03 It's a small indie game I've been developing. I just need a couple of honest testers to try it for a few minutes  
and tell me what they think. If you're cool with that I can send the link  
22:05 sure  
22:11 <https://melusagame.com/> here, tysm

**The Melusa Game**  
Step into Melusa, a magical 2D platformer filled with challenges and secrets.



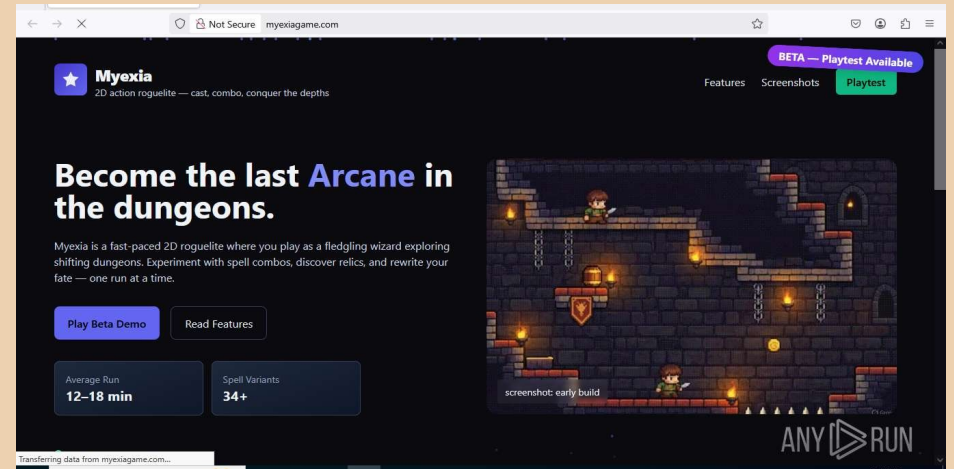
22:20 hey i have some issues getting it to work, I tried running it through Proton's translation layer but it doesnt  
do anything. What engine does it run on?

# Classical impersonation attack

- Cold opening (no prior conversation references)
- Polite (“Can I ask you a favor”)
- Time pressure (“It’s out NOW”)
- Emotional pressure (“I have worked 5 months on it”)
- Small feasible favor (“Give basic HONEST feedback”, “test only a few minutes”)
- But “personal” initial contact with bad english!

# The website

- Real game pictures  
**Archimoulin**
- Hotlinked images from  
itch.io
- Simple design
- Dropbox hosted  
payload
- Please download and  
run!



Capture from Myexia, a  
prior malware run

# First steps

- S reported the link to dropbox
- Page AND domain at hostinger reported for abuse (same host+registrar)
- They were all taken down during the analysis

klondike 8/3/26, 22:51

hum

The page is hosted by hostinger you can report abuse at <https://www.hostinger.com/report-abuse>

8/3/26, 22:54

already did lol

and the payload is on a dropbox that i also reported

klondike 8/3/26, 22:54

Which is also their registrar LOLLOLOL

8/3/26, 22:54

yeah indeed

# Static analysis

- 121 MiB: Everything and the kitchen sink!
- Electron app embedded with Node.js
- Some embedded JS
- Nothing really juicy

klondike 8/3/26, 22:57  
Lots of "SHA1 block transform for x86\_64, CRYPTOGAMS by [appro@openssl.org](mailto:appro@openssl.org)" XD  
They just have all of openssl into there xD

8/3/26, 22:59  
ah you're tearing the program apart already? 🍌

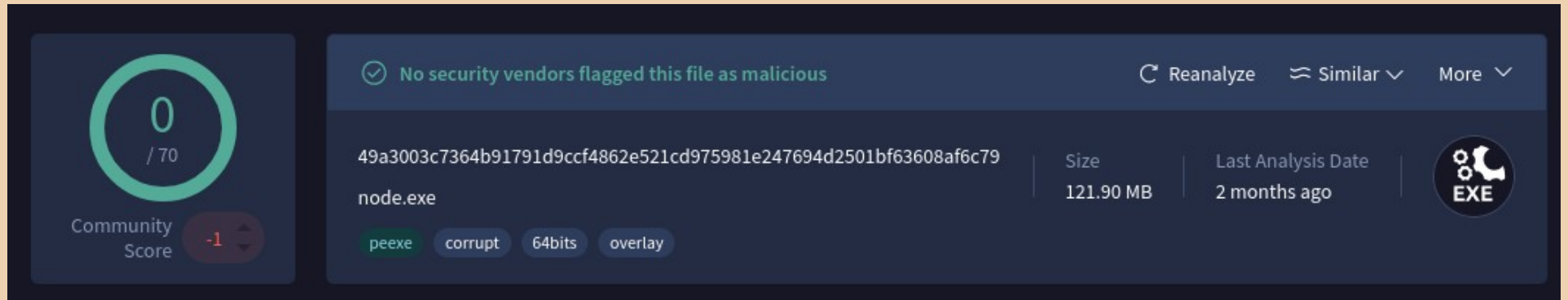
klondike 8/3/26, 23:02  
Wat!  
You gave me a toy and now complay I'm playing too hard?  
Looks like node.js with something embedded

8/3/26, 23:06  
nah its alright  
yeah i thought youd enjoy the toy

klondike 8/3/26, 23:07  
At least they are obfuscating their JS  
LOL the whole things seems to be an electron app xD

# Running VirusTotal

- Perfect 0 out of 70!
- Originally submitted as node.exe



The screenshot displays the VirusTotal interface for a file analysis. On the left, a circular progress indicator shows a score of 0 out of 70, with a 'Community Score' of -1 below it. The main area features a green checkmark and the text 'No security vendors flagged this file as malicious'. Below this, the file's SHA-256 hash is shown: 49a3003c7364b91791d9ccf4862e521cd975981e247694d2501bf63608af6c79. The file name 'node.exe' is listed, along with its size (121.90 MB) and the last analysis date (2 months ago). A file type icon for 'EXE' is visible on the right. At the bottom, there are tags for 'peexe', 'corrupt', '64bits', and 'overlay'. Action buttons for 'Reanalyze', 'Similar', and 'More' are located at the top right of the main panel.

# First attempt at dynamic analysis

- Used hybrid-analysis.com
- Lots of suspicious indicators
- Triggers WerFault.exe
- No info about the backend

Here, have fun you too!

8/3/26, 23:10

hmm any way to nuke their backend?

klondike 8/3/26, 23:17

I couldn't see any network traffic from the sandboxed run

But maybe it detected the sandbox 😞

8/3/26, 23:17

yeah could be

klondike 8/3/26, 23:18

I don't have much better at hand I haven't done real forensics in a lot

8/3/26, 23:18

ah yeah fair

# First breakthrough

- Using strings
- "name": "MyexiaGame"
- Wait wasn't this Melusa?
- More hints on malware (Myexia / Agent Tesla)

```
klondike 8/3/26, 23:21
Okay I know what it might be
Have you heard of myexia AKA agent tesla?

8/3/26, 23:22
nope

klondike 8/3/26, 23:24
Here is a different sample: https://any.run/report/012d73aab7ce2c5f6ffc4c69f369f53ee7c1041acfe17d61d457a9f6f87bae79/8b5f0927-07fd-4bc0-9201-01c5ed218ca3
```

# First roadblock

- Website down
- Any.run refuses to run large files :(

klondike 8/3/26, 23:32  
Seems the website is down

8/3/26, 23:33  
ha nice 🤔

klondike 8/3/26, 23:33  
No it is not

8/3/26, 23:33  
ah

klondike 8/3/26, 23:33  
The sandbox is dumb

8/3/26, 23:33  
aaa

# It LIVES!

- Do a url scan
- Download the file using dropbox
- Run it!
- Enjoy!

klondike 8/3/26, 23:47

Ehm

I managed to get it to run on a different way

Guess what they use to steal the tokens?

8/3/26, 23:48

no clue 🤔

im not too versed on this

klondike 8/3/26, 23:49

Discord

They literally create a zip file with all of it and upload it to discord itself

# The spiral

# Trying to nuke their backend

- Let's mail abuse
- Report including webhook and sandbox runs

A abuse@discord.com 9/3/26, 0:18

Asunto **Myxiagame variant called Melusa game abusing webhooks to steal information**

Hello,

BLUF: A malicious actor is using the webhook at <https://discord.com/api/webhooks/1480016365531299922/s2ACNpCR0n338Sdtx5YiAFfhD6q0Ebqa1pgVlkBsng-RzRVmC2LV8jCcwIxpjrZbUBk> to steal user information.

After a suspicious message from an affected user, a friend asked me to investigate a variant of the Myxiagame information stealer called MelusaGame and hosted on melusagame . com

The malware with sha256 hash 49a3003c7364b91791d9ccf4862e521cd975981e247694d2501bf63608af6c79 seems to be an information stealer based on node.js that uses a discord webhook to upload the stolen information.

The webhook used is <https://discord.com/api/webhooks/1480016365531299922/s2ACNpCR0n338Sdtx5YiAFfhD6q0Ebqa1pgVlkBsng-RzRVmC2LV8jCcwIxpjrZbUBk>

The full report from the sandboxed run can be seen at: <https://any.run/report/f540d024cea30a034586ef1b6e0af3a24b2ce7e31164a2b51762b96fe580a954/13d95cdd-39d7-4f41-aae4-2fcc8fbb8bd7>

# I guess it's just a CAPTCHA and...

Asunto **Discord welcome email**

No suele recibir correo electrónico de support@discord.com. [Por qué es esto importante](#)

Welcome to Discord Support!

We received a support ticket submission/account creation request associated with this email address.

If you didn't perform these actions or don't recognize this request, please ignore this message.

If you did make the request, you must finalize the action by clicking the link below.

<https://support.discord.com/verification/ticket/d82sHRFapIjY9ey71ZiHsF46t/>

# Not just a CAPTCHA

- Register a full new account
- Then receive an email redirecting you to a help page

Asunto **[Discord] Please Read: This email address is not currently supported**

Hello,

We appreciate you reaching out! We're unable to review email submissions to [abuse@discordapp.com](mailto:abuse@discordapp.com) / [abuse@discord.com](mailto:abuse@discord.com).

For assistance reporting abusive behavior to Discord and handling emergency situations, go here:  
<https://dis.gd/howtoreport>

If you would like to submit an appeal on a moderation decision made by Discord, or update your account's age information, go to our Appeals & Age Update Request form:  
<https://dis.gd/appeal>

For all other inquiries, or to get in contact with Discord Customer Support, select the correct contact option at our Help & Support form:  
<https://dis.gd/support>

Thank you,  
Discord

# Dead end

- Discord only allows in app reports
- Useful for messages not for webhooks
- I gave up after a reasonable effort at finding the way to report

klondike 9/3/26, 0:23

And I understand why they use discord now

Mailed their abuse address, got this back:

"Hello,

We appreciate you reaching out! We're unable to review email submissions to [abuse@discordapp.com](mailto:abuse@discordapp.com) / [abuse@discord.com](mailto:abuse@discord.com).

For assistance reporting abusive behavior to Discord and handling emergency situations, go here:

<https://dis.gd/howtoreport>

If you would like to submit an appeal on a moderation decision made by Discord, or update your account's age information, go to our Appeals & Age Update Request form:

<https://dis.gd/appeal>

For all other inquiries, or to get in contact with Discord Customer Support, select the correct contact option at our Help & Support form:

<https://dis.gd/support>

Thank you,  
Discord"

Nothing in there about how to actually report malicious use of their webhooks...




# Melusa is still out there

- Blogspot post
- Same hotlinks to itch.io
- Smaller size
- Some detects in Virustotal
- Different delivery method (Nullsoft instead of node.js)
- “Melusa is a fast-paced 2D roguelite where you play as a fledgling wizard exploring shifting dungeons”
- (Reported as I was writing the talk)


**Melusa Game**

April 19, 2026

This isn't just any mill—forget about the classic flour mill or the boring lumber mill. Make room for *The Melusa* ! A place where everything is possible: a fruit mill, a cream mill, an egg mill... whatever you need! *The Melusa* has it all. But are you brave enough to face the challenge? Embark on this journey full of exciting tasks and gather all the ingredients needed to bake the birthday cake of the century!



In this short but thrilling 2D platformer, join a young boy as he embarks on an exciting adventure through a colossal windmill, collecting all the essential ingredients to bake the ultimate birthday cake for his mother!



Due to time constraints, some features have been scaled down, but it still offers an enjoyable experience.

**IMPORTANT:** *This game is optimized for lower graphics settings by default. If your system can handle it, feel free to boost the quality to "Fantastic" through the launcher for an enhanced visual experience!*

**Download**

Download Melusa 82 MB

# The lessons

# Lessons learned

- ~~IRC~~ Discord is an amazing exfiltration tool
  - No handling of abuse reports
  - Widely used and accessible
  - Webhooks allow file uploads
- Discord is an amazing social engineering tool
- If your malware doesn't run try other sandboxes
- S is an amazing person, no wonder I love them!

# THANKS!



**CHALMERS**  
UNIVERSITY OF TECHNOLOGY



UNIVERSITY OF  
GOTHENBURG

**kit**s  
keep it secure