Empowering your abusers

The Discord case

CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF
GOTHENBURG

kits
keep it secure

Francisco Blas Izquierdo Riera (klondike)

Myexia / Melusa

A Discordian Credential Stealer

CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF
GOTHENBURG

kits
keep it secure

Francisco Blas Izquierdo Riera (klondike)

Mandatory controversial statement

IRC IS DEAD!
LONG LIVE
DISCORD!

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?

CHALMERS UNIVERSITY OF TECHNOLOGY

kits keep it secure

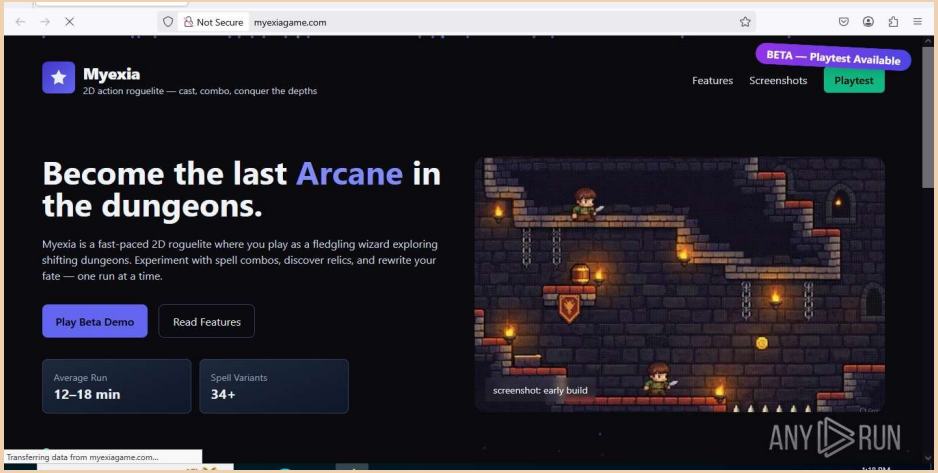
UNIVERSITY OF GOTHENBURG

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

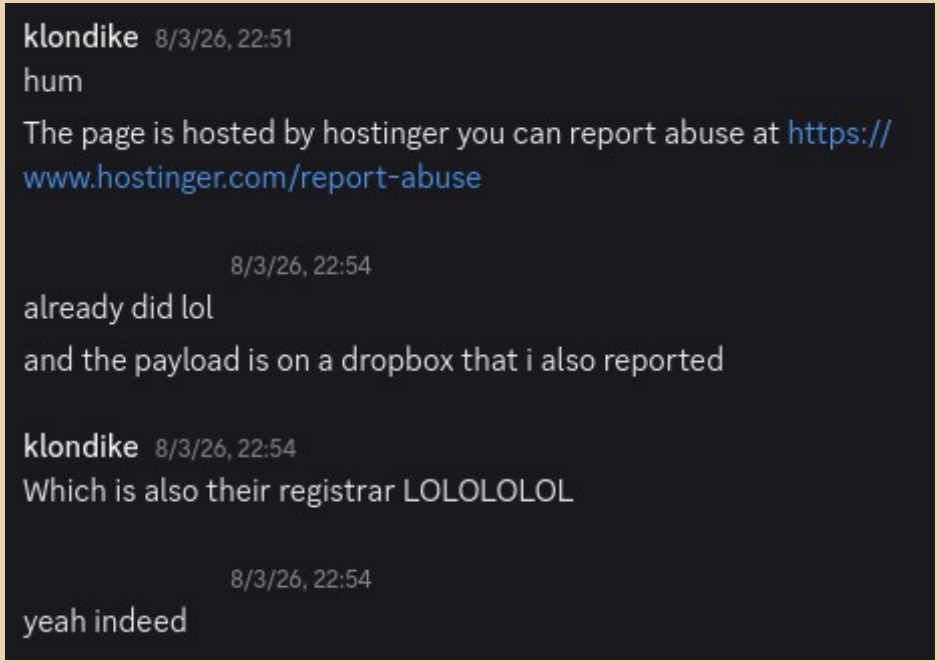
- Real game pictures Archimoulin
- Hotlinked images from itch.io
- Simple design
- Dropbox hosted payload
- Please download and run!



Capture from Myexia, a prior malware run

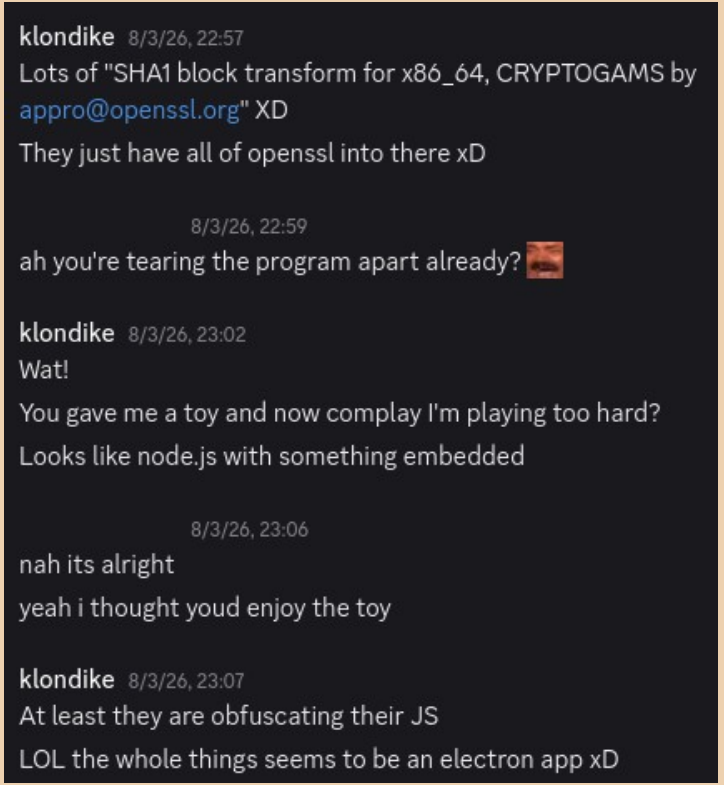
First steps

- 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



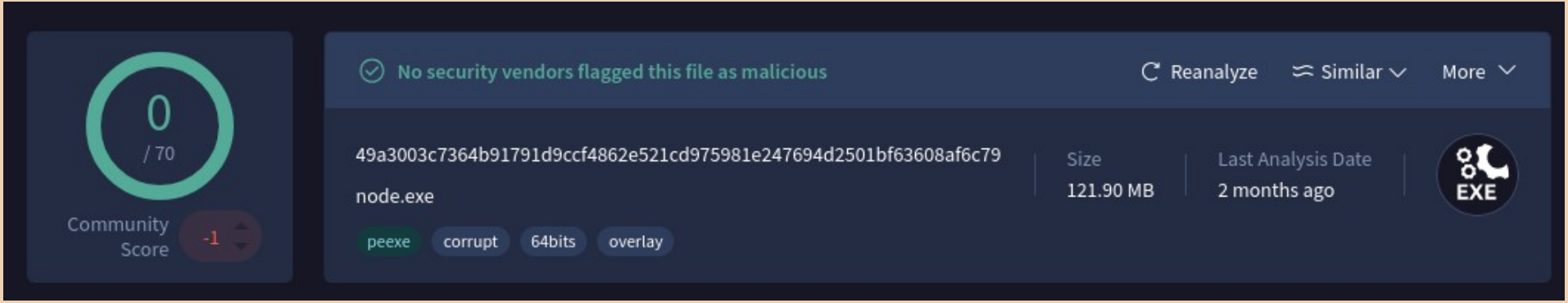
Static analysis

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



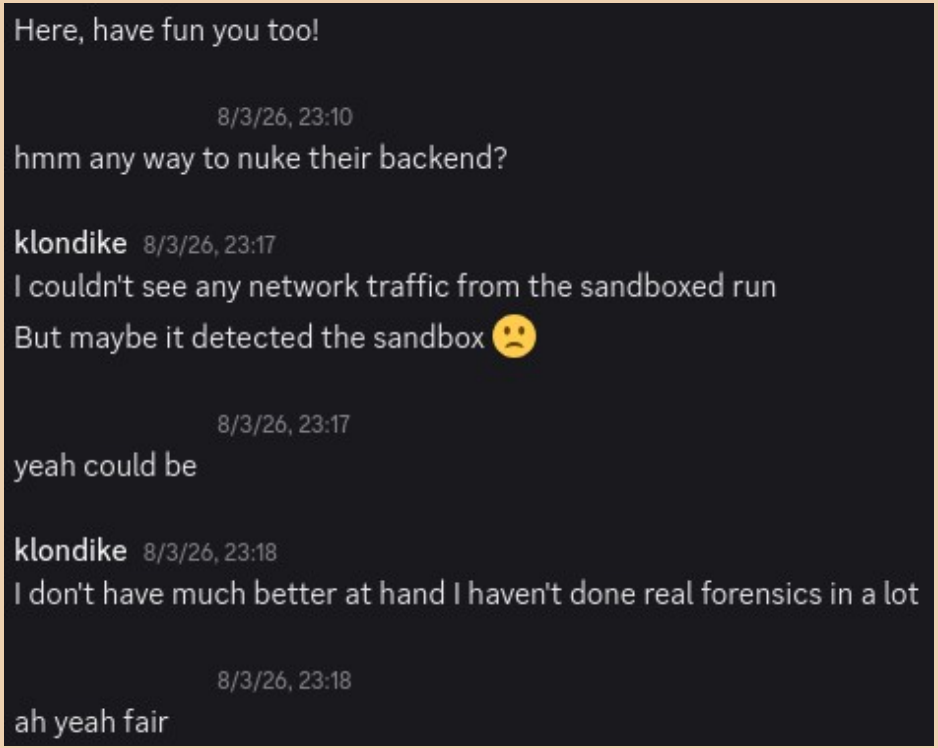
Running VirusTotal

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



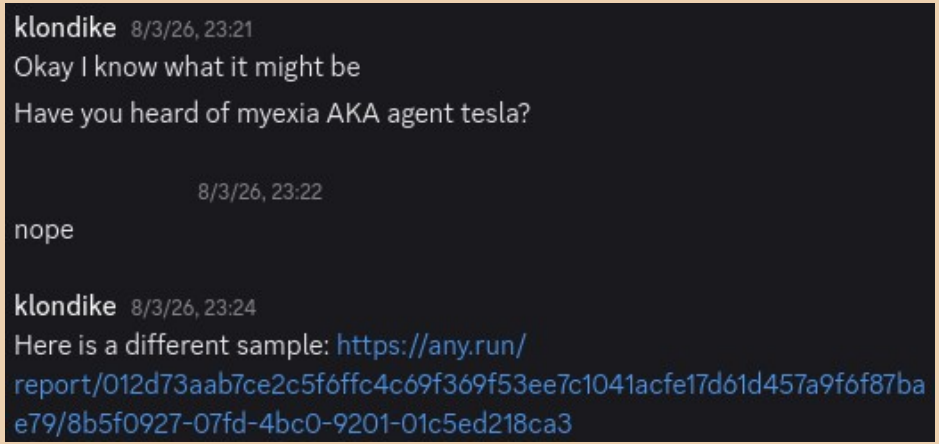
First attempt at dynamic analysis

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



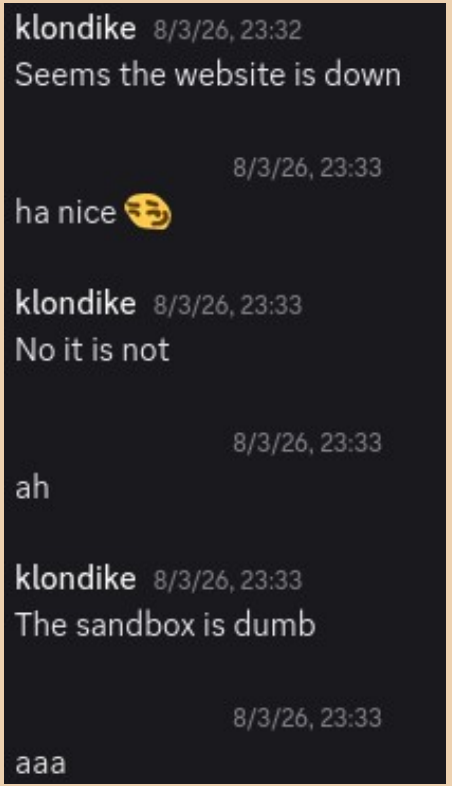
First breakthrough

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



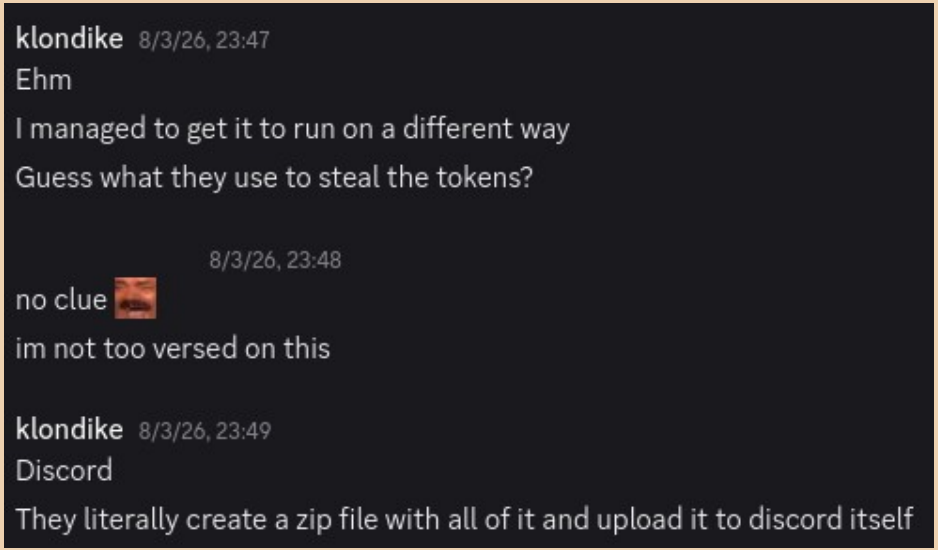
First roadblock

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



It LIVES!

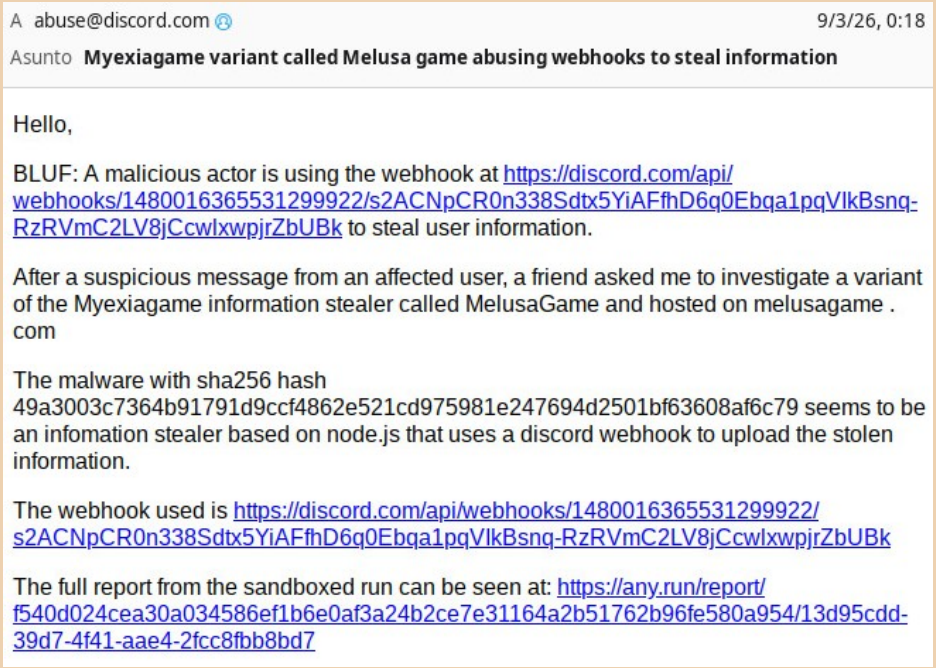
- Do a url scan
- Download the file using dropbox
- Run it!
- Enjoy!



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 **Myexiagame 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/s2ACNpCR0n338Sdtx5YiAFfhD6q0Ebqa1pqVlkBsnq-RzRVmC2LV8jCcwlxwpjrZbUBk to steal user information.

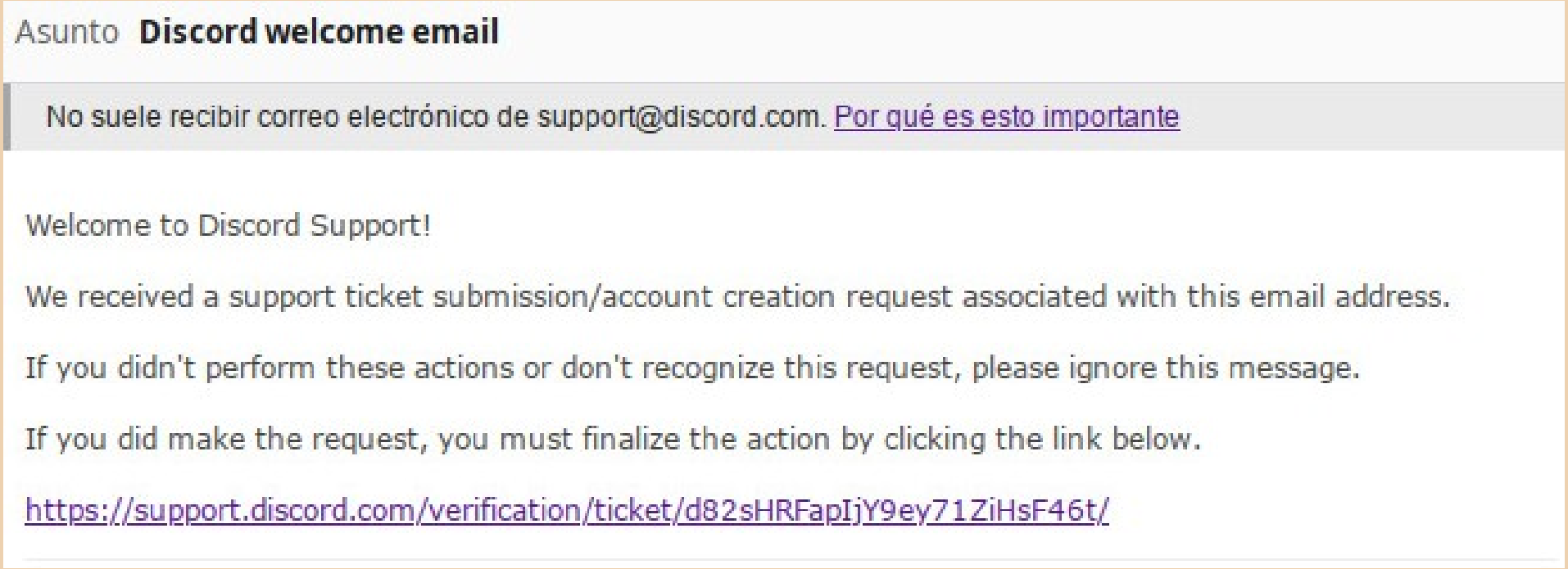
After a suspicious message from an affected user, a friend asked me to investigate a variant of the Myexiagame information stealer called MelusaGame and hosted on melusagame . com

The malware with sha256 hash 49a3003c7364b91791d9ccf4862e521cd975981e247694d2501bf63608af6c79 seems to be an infomation 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/s2ACNpCR0n338Sdtx5YiAFfhD6q0Ebqa1pqVlkBsnq-RzRVmC2LV8jCcwlxwpjrZbUBk

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.

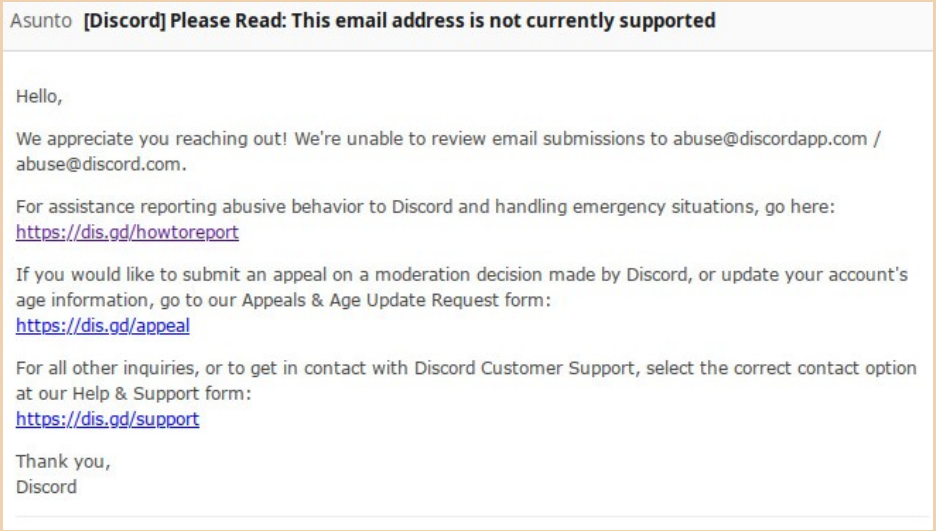
If you didn't perform these actions or don't recognize this request, please ignore this message.

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 / abuse@discord.com.

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

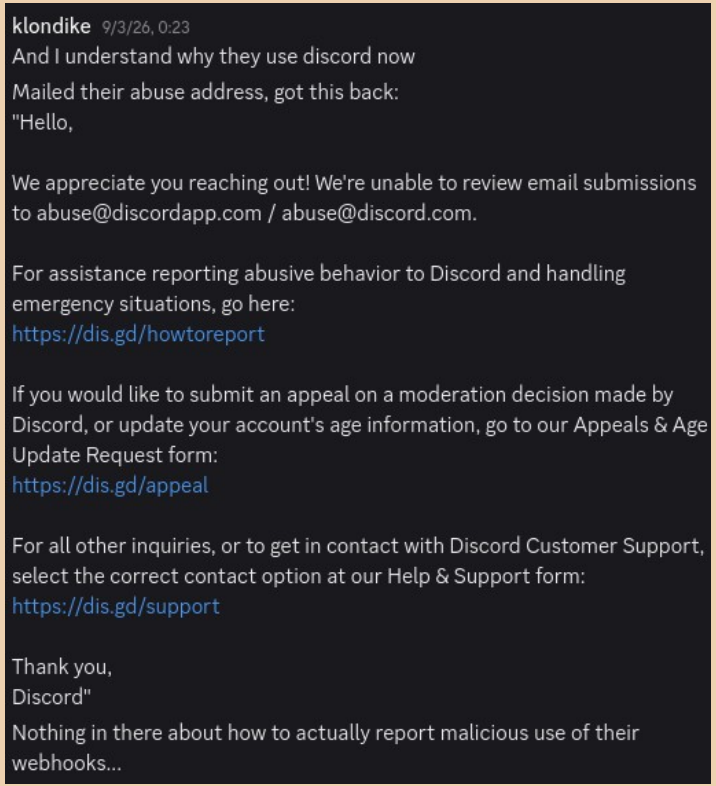
If you would like to submit an appeal on a moderation decision made by Discord, or update your account's age information, go to our Appeals & Age Update Request form:
https://dis.gd/appeal

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

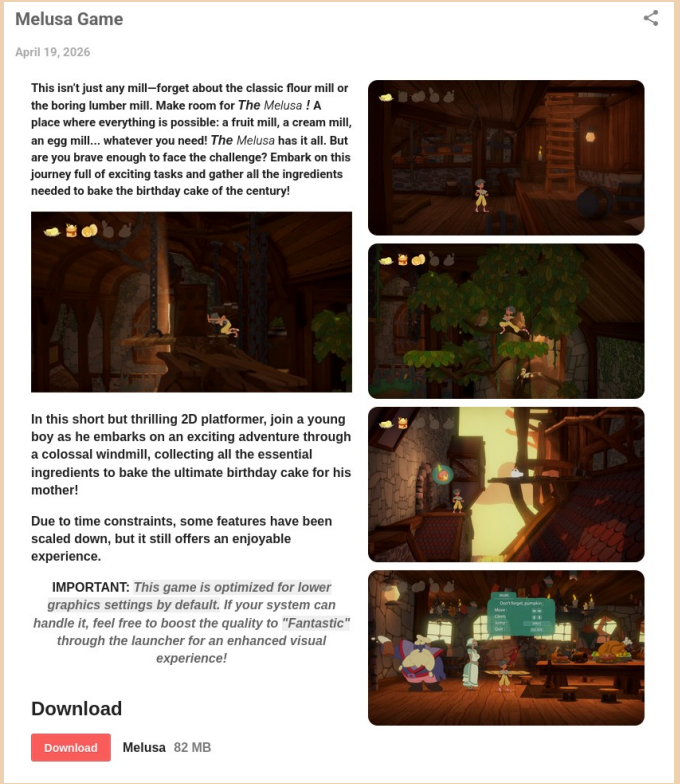
Dead end

- 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



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)



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

kits
keep it secure