# r00ting Out Fraud on Telegram

Matt Meis and Kyle Yurek

# Our Backgrounds

UWM®

Lubar College of Business

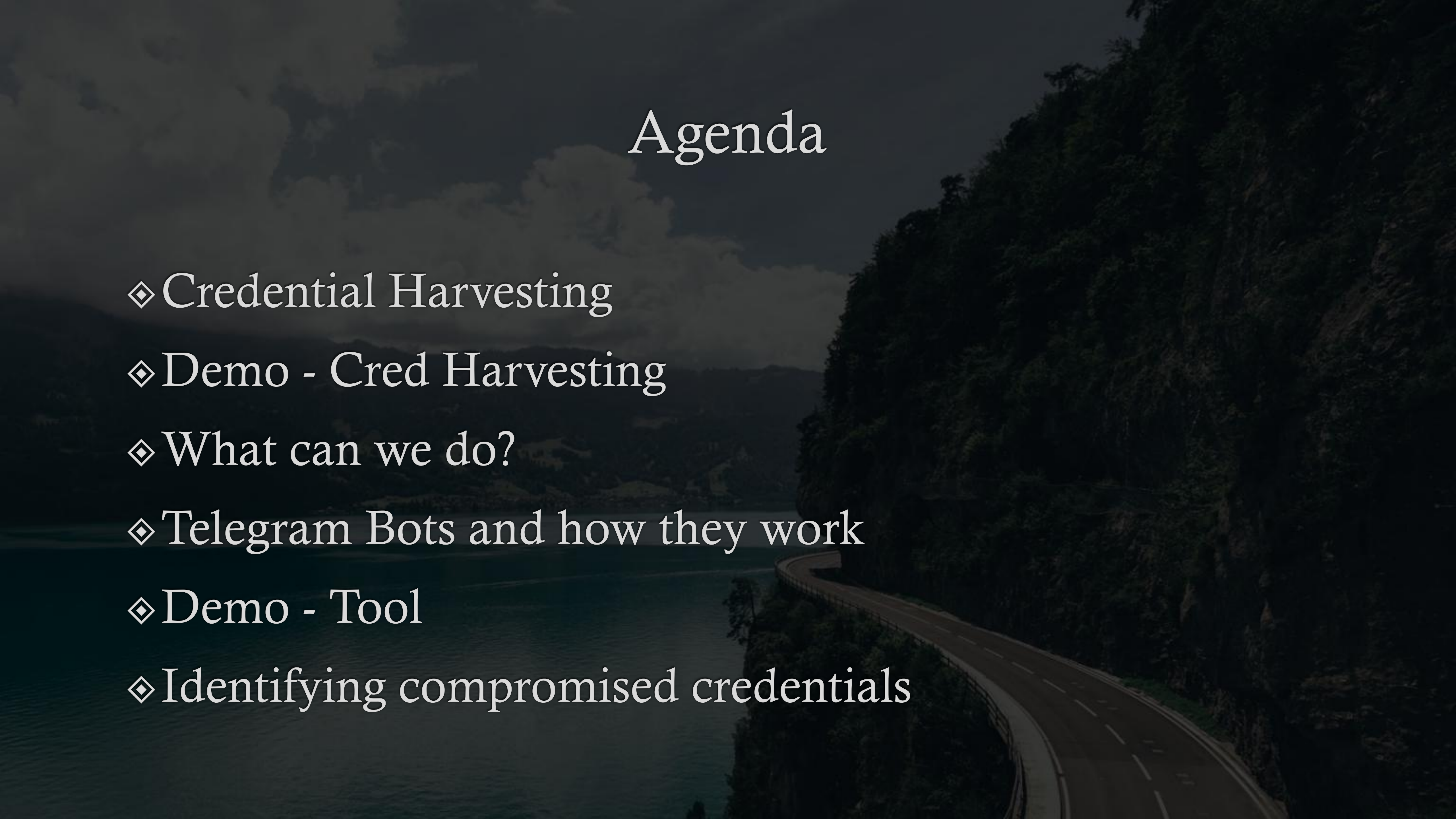
WICTRA®

summit

CREDIT UNION

UNIVERSITY OF WISCONSIN

STEVENS POINT

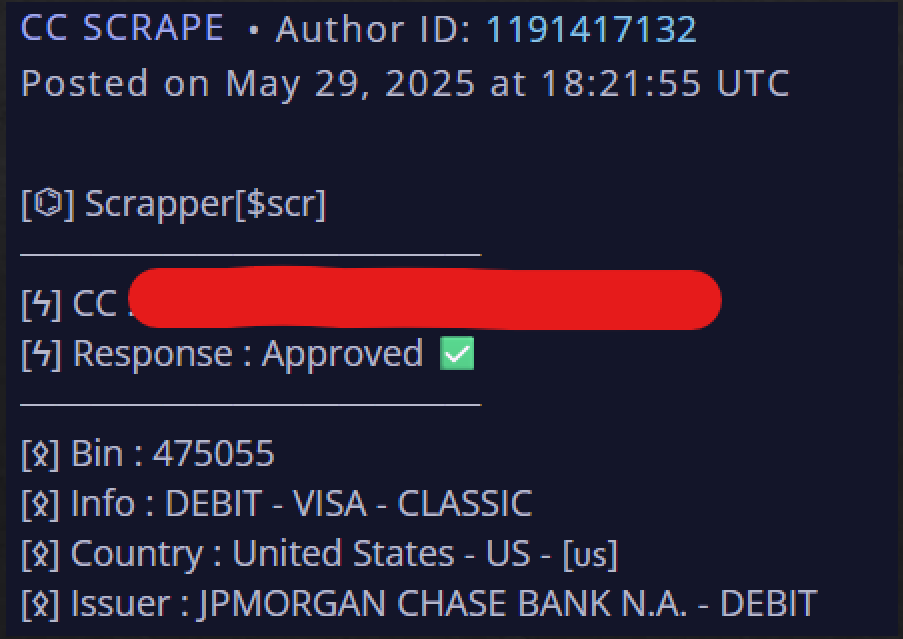


# Agenda

- Credential Harvesting
- Demo - Cred Harvesting
- What can we do?
- Telegram Bots and how they work
- Demo - Tool
- Identifying compromised credentials

# Anatomy of Credential Harvesting

- Phishing Sites
- Phish Kits Copy Cats
- Telegram as a Database (TaaD)



```
CC SCRAPE • Author ID: 1191417132
Posted on May 29, 2025 at 18:21:55 UTC


[⌬] Scrapper[$scr]
————————————————
[ϟ] CC [redacted]
[ϟ] Response : Approved ✅
————————————————
[ꗃ] Bin : 475055
[ꗃ] Info : DEBIT - VISA - CLASSIC
[ꗃ] Country : United States - US - [us]
[ꗃ] Issuer : JPMORGAN CHASE BANK N.A. - DEBIT
```

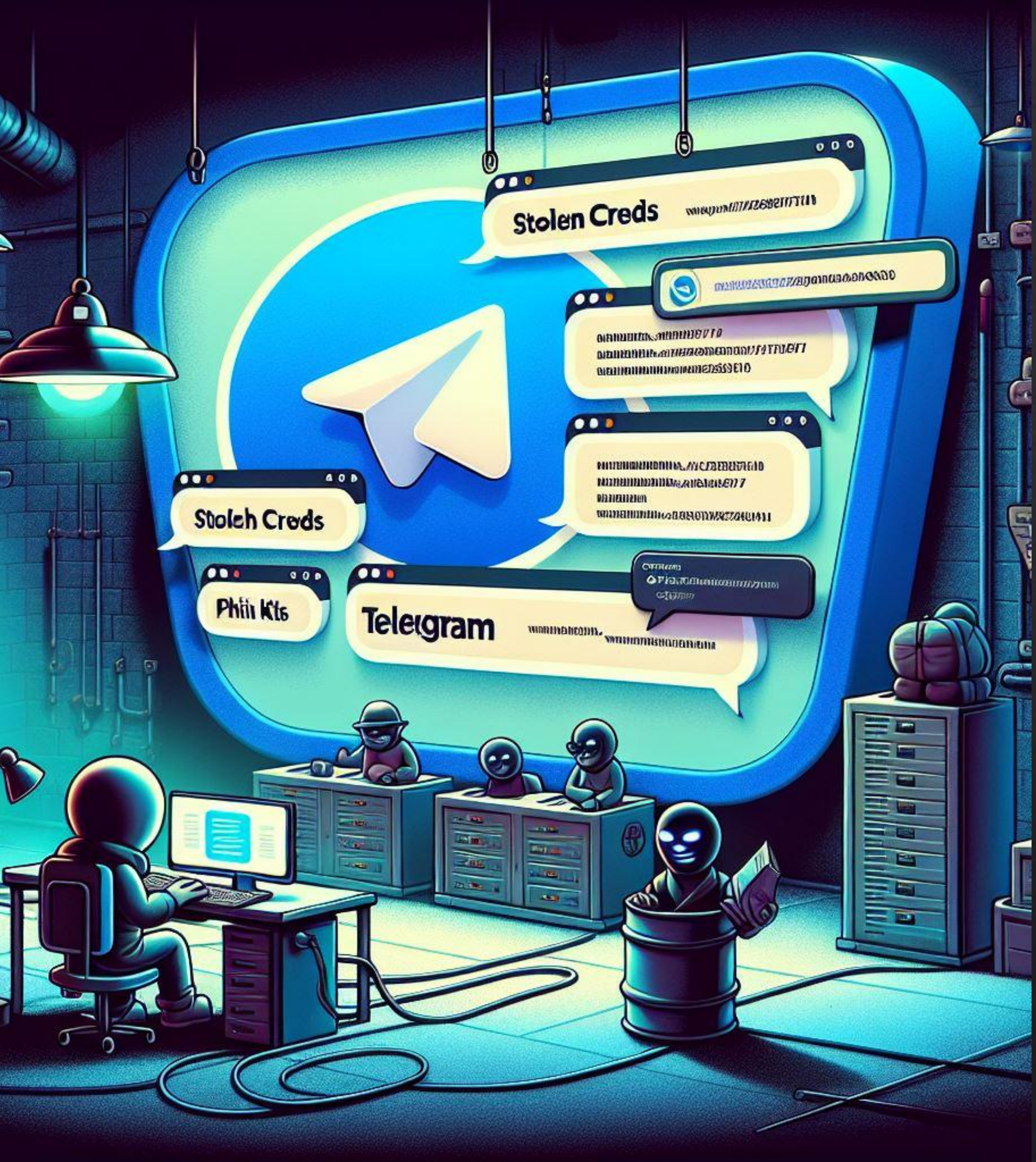
# Victim and Command View

# Demo!

- Audience Participation!
  - Enter some credentials

http://creds.meis.us/

# Why is Telegram important?



# Telegram as a Database (Taad)

- Easy to implement
- One stop shop for collecting, storing and selling information
- End-to-End Encrypted
- Anonymity

# Telegram Bots

- What is a Telegram Bot?

- Security Issues
  - Understatement of the year

# What can you do?

# New Open-Source Telegram Bot Cred Harvester

- Find your compromised users
- Recon the Enemy
- Exploit Criminal Infrastructure
- What is the tool?
  - Python
  - Telethon

# Demo!

PlunderGram
A TELEGRAM OSINT AND RECON TOOL
FOR RESEARCH USE ONLY

# Closing Thoughts

- Must still detect phishing sites and request takedowns
- Easier for users to click a link
  - GenAI is good
- Telegram usage is increasing
- Ethical and Risk considerations
  - Telegram Terms
  - Infrastructure you are running from

# Want to learn more?

- **PlunderGram GitHub Link:**
  - https://github.com/kpwnther/PlunderGram
- **SecFraudOps Newsletter:**
  - https://secfraudops.substack.com/
- **Survive Online Book:**
  - https://www.learncybersecurity.net/book
- **Contact Matt and Kyle:**
  - **matt@meis.us**
  - **kyle@yurek.pro**

https://linktr.ee/mmeis

https://hihello.me/hi/kyleyurek