

Sun City Computer Club

Cyber Security SIG

May 4, 2023

**Questions, Comments, Suggestions welcomed at
any time**

Even Now

- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

**SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law**

- Ever want to be a presenter??
- iDevices SIG
 - A real need
 - FUN
 - Experienced SIG help
 - Can and has been done remotely
- Until then, iDevices topics in Mac Users Group

Presenter???

- Malware
- Now attacking password managers
 - 1Password KeePass
 - in addition to crypto wallets
 - Better encryption to evade detection
 - Chrome, Edge, Firefox, Opera, Brave
 - Checks for Windows Defender, et al

ViperSoftX

- Corporate
- Soft Target “that’s just our whatsit”
- Treadmill “Shadow IT”

- Given ransomware will occur
- Position so recovery is timely & Complete
- Find and remove vulnerabilities

Ransomware

Movie "How to Blow up a Pipeline"

- <https://careers.bankofamerica.com/content/dam/careers/academy/CyberSecurityCourseResourceGuide.pdf>
- Be cautious in what you share
- Monitor privacy settings
- Verify call, message, email asking for money
- Resist pressure to act quickly

Bank of America Resource Guide

- FBI PSA
Wrong Number

<https://www.ic3.gov/Media/Y2023/PSA230314>

Get “Hi” message?



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



March 14, 2023

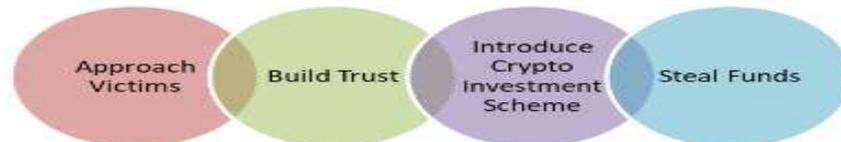
Alert Number
I-031423-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

The FBI Warns of a Spike in Cryptocurrency Investment Schemes

The FBI warns of a spike in cryptocurrency investment schemes. Criminals, typically based overseas, defrauded victims of more than two billion US dollars in 2022 using these schemes, according to the FBI Internet Crime Complaint Center (IC3).



The schemes are socially-engineered and trust-enabled, usually beginning with a romance or confidence scam and evolving into cryptocurrency investment fraud. Criminals use fictitious identities to develop relationships and build rapport with victims. Criminals target victims using dating applications (apps), social media platforms, professional networking sites, or encrypted messaging apps.

Once trust is established with victims, criminals introduce the topic of cryptocurrency and claim to have expertise, or an affiliation with experts, who can help potential investors achieve financial success. Criminals then convince victims to use fraudulent websites or apps, controlled by the criminals, to invest in cryptocurrency. Criminals coach victims through the investment process, show them fake profits, and encourage victims to invest more. When victims attempt to withdraw their money, they are told they need to pay a fee or taxes. Victims are unable to get their money back, even if they pay the imposed fees or taxes.

Newer iterations of the schemes include [liquidity mining](#) and [play-to-earn schemes](#).

TIPS TO PROTECT YOURSELF

- If an unknown individual contacts you, do not release any financial or personal identifying information (PII) and do not send any money.
- Do not invest per the advice of someone you meet solely online.
- Confirm the validity of any investment opportunity or cryptocurrency investment website or app.
- If you already invested funds and believe you are a victim of a scheme, do not pay any additional fees or taxes to withdraw your money.
- Do not pay for services that claim to be able to recover lost funds.

The FBI requests victims report these types of fraudulent or suspicious activities to the FBI IC3 at www.ic3.gov.

- Evil Extractor
 - “Educational tool”
 - Adobe PDF or Dropbox file
 - PowerShell script(s)
 - Environment analysis tool
 - Info stealer FTP
- TP-Link Archer A21 WiFi router vulnerability
 - Firmware update released March 14, 2023
 - Version 1.1.4 Build 20230219
 - CVE2023-1389 CVSS 8.8
- Singapore “Please block ads” recommendation
 - Whitelist option
 - ScamShield Police provided database
- US military removed Iranian hackers off municipal website
 - Reportedly reporting incorrect election results 2020

Current Issues

9:41

Notification Center



Lockdown Mode block... Yesterday

[redacted]@gmail.com attempted to access a Home.



Lockdown Mode block... Mon

[redacted]@yahoo.com attempted to access a Home.

iOS Lockdown Mode

- Supply chain attack blamed for 3CX supply chain attack
- Capita (Very large UK outsourcing firm) massive ransomware outage
lack of updates to markets/investors
ignored problem for week
“data leaked was in public domain”
- DC Health Link
DC health insurance exchange
Used by lawmakers
56,000 misconfigured server/service
Sold on cybercrime forum
“data on dark web” no on BreachForums

Current Issues

- Group-IB cybersecurity company
Russia based
exit Russia founder jailed
- *Wired* reports ICE database misuse
- UK Online Safety Bill
Major E2EE apps may move
UK government use of WhatsApp?
US Protecting Kids on Social Media Act
Kids stay longer if upset
- Mullvad VPN & Browser
Swedish warrant
“we don’t keep/log that data”

Current Issues

- QuaDream spyware company closed
- Google Cloud Platform
Asset Key Theft
Google Cloud Service Accounts
Access customer accounts &
Gmail, Drive, Docs, Photos,
Google Cloud Platform App
'Ghost token'
Summer 2022 until April
- Apple Journaling App - Mental Health
Creepy?
- Adobe AI powered tools

Current Issues

- Call, email, text
“Your funds need to be moved to avoid loss”
- Google Bard Code Wizard
Develop, debug, explain code
C++, Java, Python, JavaScript, ...
20+ languages
Sheets functions
- iOS 17 sideloading EU Only?
- iDevice
Settings > General > Erase all Content and Settings
AFTER backup, transfer

Current Issues

- Out of Date driver compromise Windows AuKill
- Google Authenticator synch in the cloud
Helpful <-> Harmful
Not E-2-E
Seed dependent
QR codes contain vendor site
- Edge Follow Creator *feature*
Settings > Privacy, Search, and Services
Services

Get notified when creators you follow post new content



We'll show you notifications when the creators you follow post new content

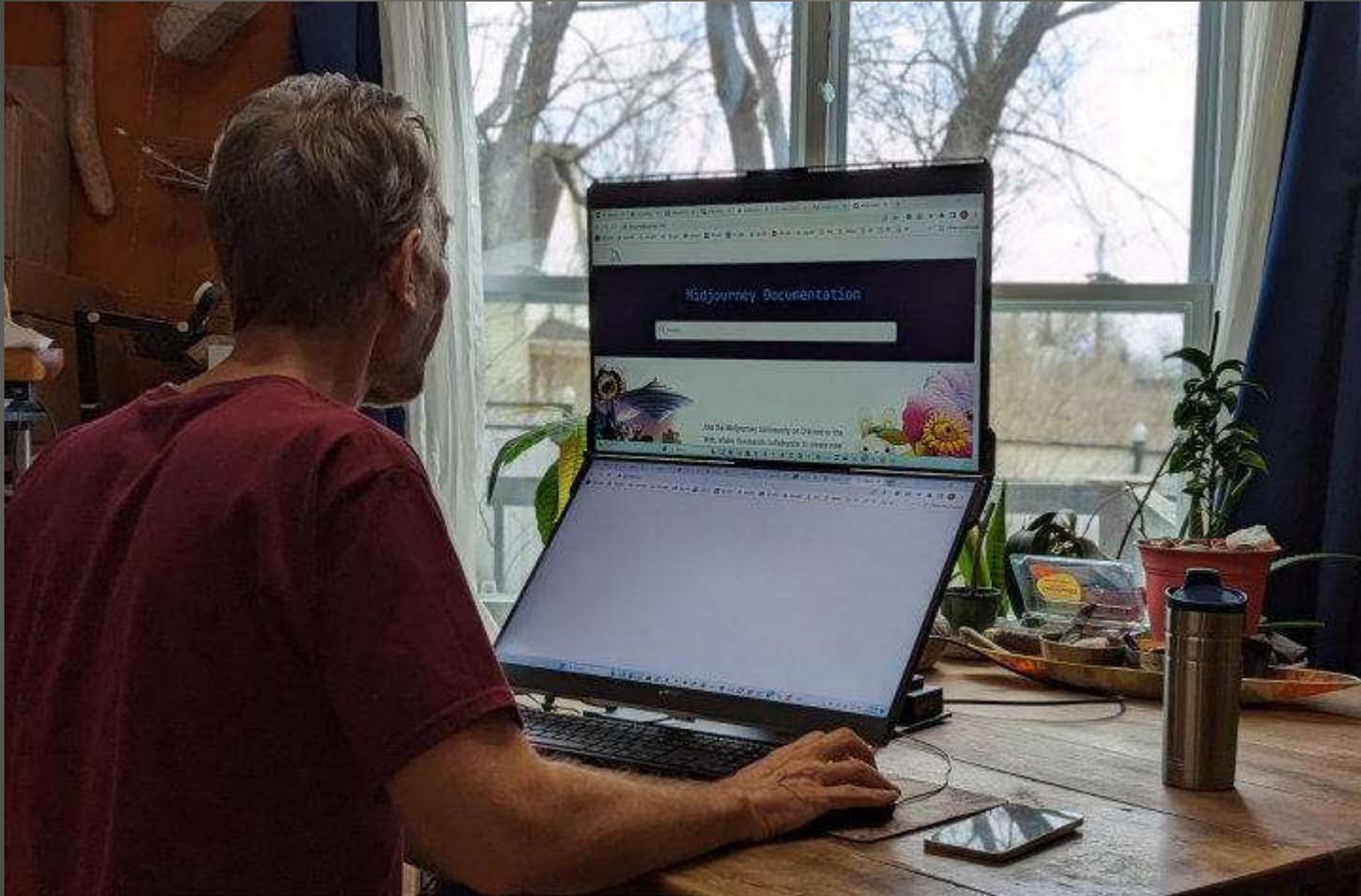
Current Issues

- Nvidia NeMo Guardrails
detect and mitigate hallucinations
- PaperCut security flaws
Deliver Atera remote management software
- Brave no longer to use Bing index
- Some iPhone security Apps
 - Avast
 - Password leak monitoring
 - Malicious site blocker VPN-like
 - Photo vault
 - TotalAV
 - Device optimization
 - Password leak monitoring
 - Secure QR scanner
 - McAfee
 - Wi-Fi scanner
 - Password leak monitoring

Current Issues

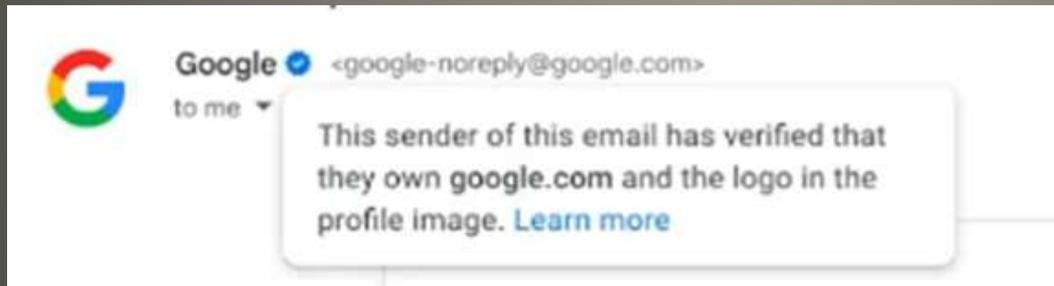
- su & sudo to be rewritten in Rust
- Microsoft switching to Rust
- Vulnerability exploited
 - Veeam backup servers exposed online
- Threat actors use cloud & affiliate networks
- Battle signatures & blocklists
- Popups
 - Browser control
 - Safari Settings > Websites > Popups
 - Block & Notify Whitelist as needed
- FBI Director – outnumbered by 50 to 1
 - China

Current Issues



Stacked monitors

- Verified Brand logos 2021
- Brand Indicators for Message Identification
- BIMI
- Domain-based Message Authentication, Reporting, and Conformance (DMARC)



- Hover over blue checkmark

Gmail checkmark

- Google Account enables passkeys
- Smart Device with FaceID, Fingerprint or PIN

Gmail passkeys

- First Thursday of May
- TODAY
- <https://www.spiceworks.com/it-security/identity-access-management/articles/world-password-day-2023/>

World Password Day

- iCloud Keychain
- Credit Card data
- Cryptocurrency wallet
- Browser cookies
- weed.dmg

- Keep Up to Date
- Only install from trusted sources

MacStealer

- iCloud Keychain
- Credit Card data
- Cryptocurrency wallet
- Browser cookies
- Notion-7.0.6.dmg
- Photoshop cc 2023.dmg
- Tor Browser.dmg

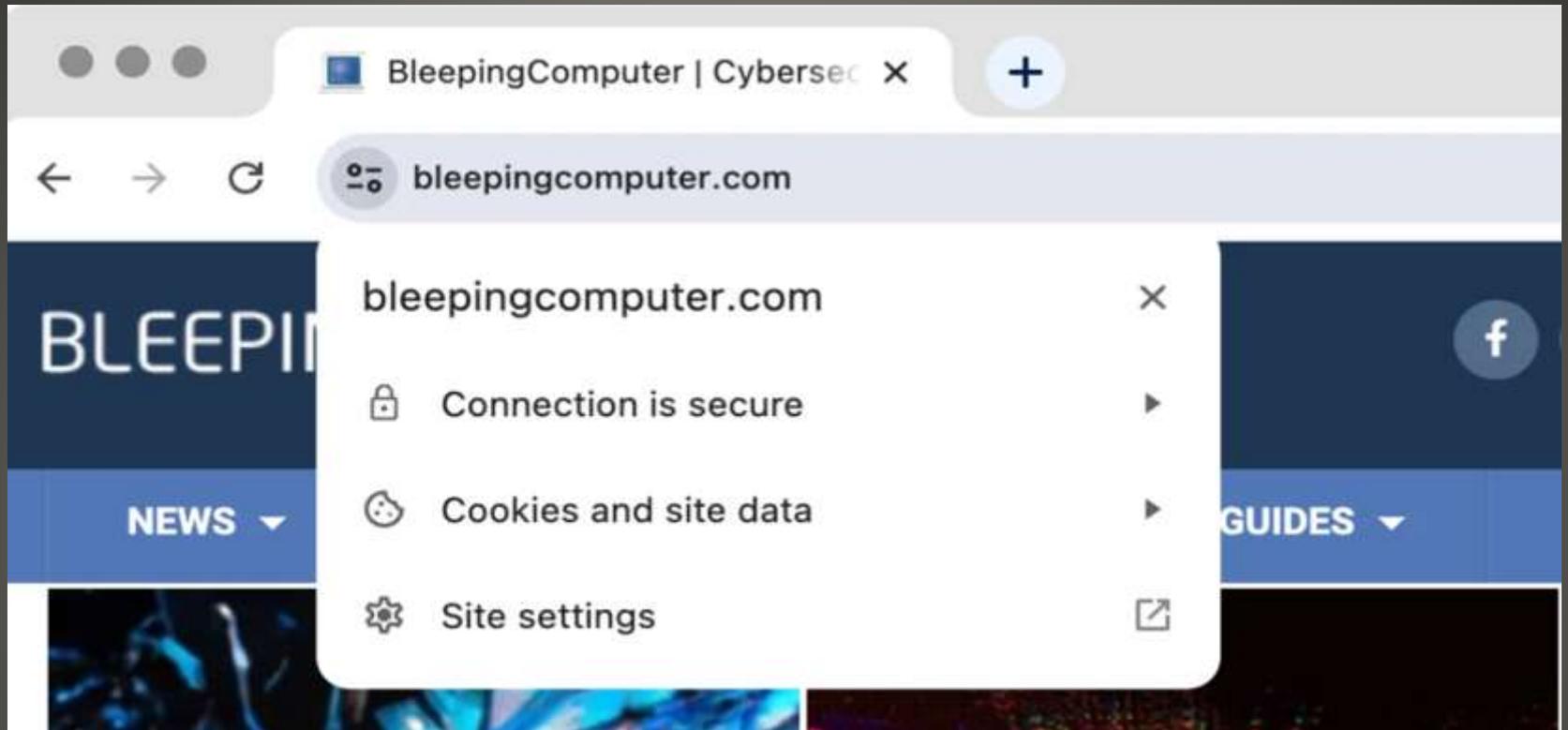
More and More targeting macOS

- Keep Up to Date
- Only install from trusted sources

Atomic macStealer

- WhatsApp 4 devices caution
- VPN Kill Switch
 - System Level - Operating System
 - ALL Internet traffic
 - App Level
 - Which Apps
- VPN Control On per TAB/App
- Bluetooth tracker efforts

Current Issues



- Lock implies Secure
- Malicious sites use HTTPS

Chrome Lock Icon

- April 27 09:03PM – 09:26PM ET
- Brief outage NOT security breach

Your Secret Key or password was recently changed. Enter your new account details to continue.

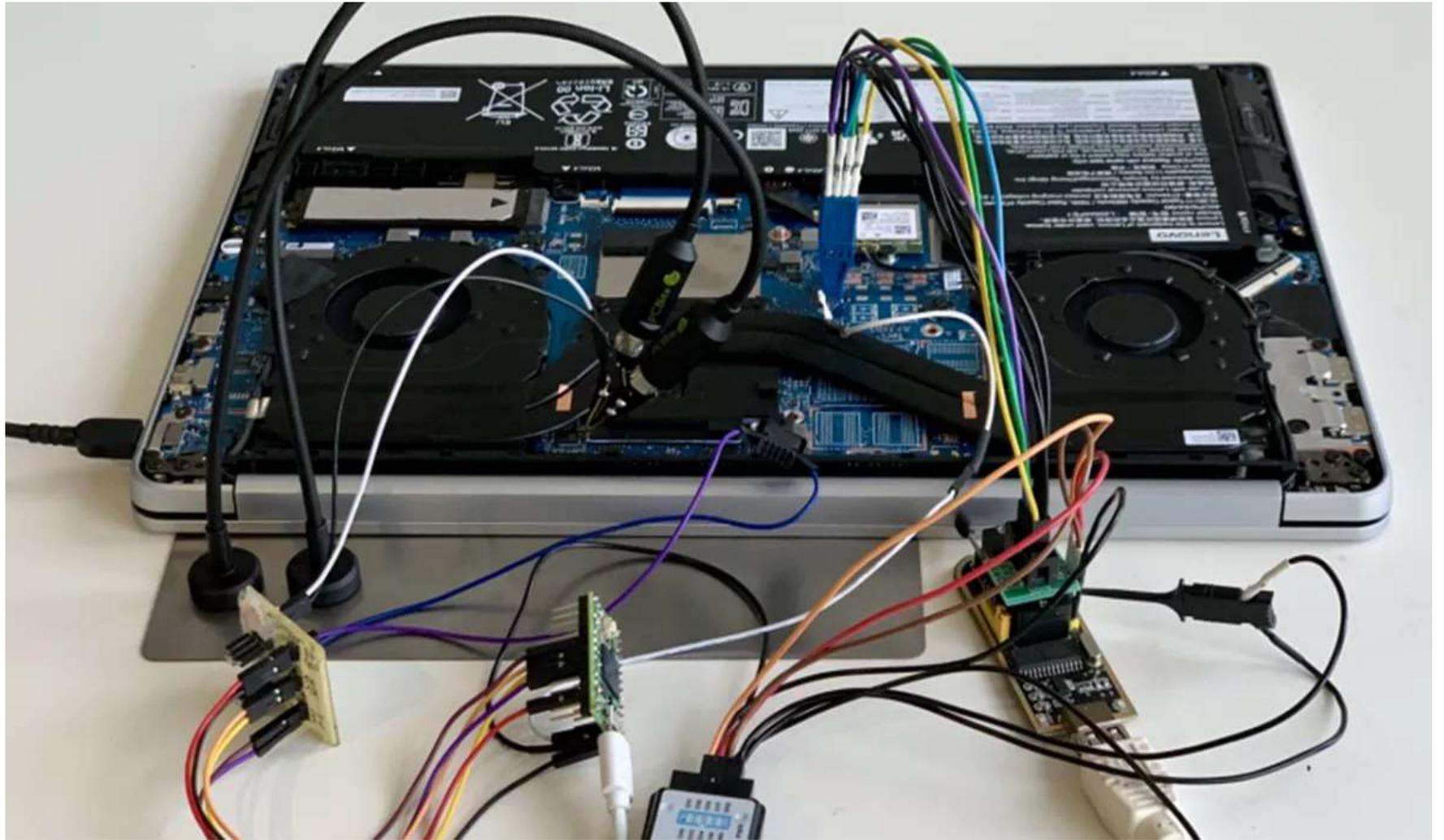
Secret Key

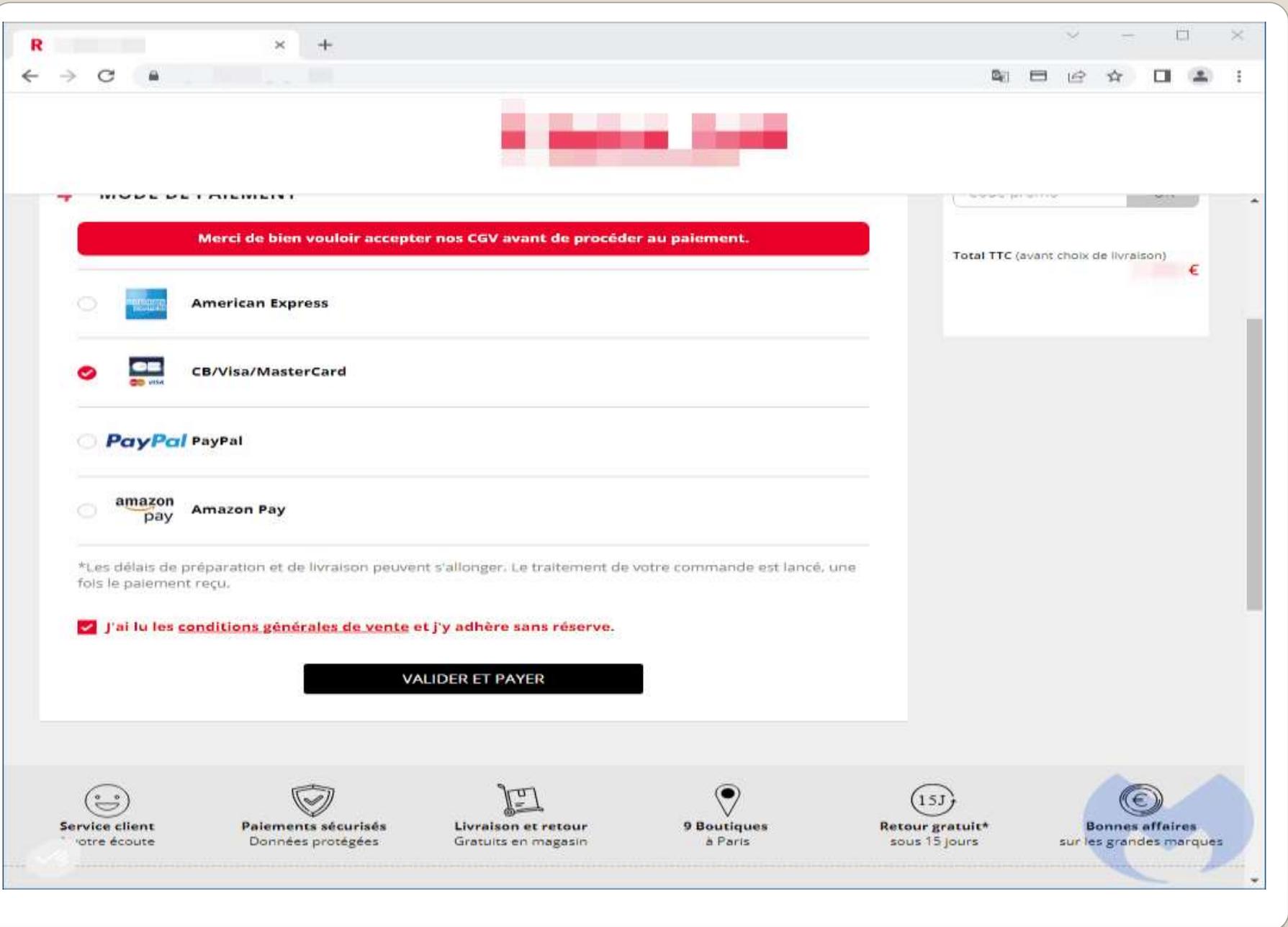
Password

1Password error in error

- Defeats BitLocker & TPM-based security
- Academic research
- Voltage Fault Injection `faultTPM`
- Zen 2 & Zen 3 chips
- Physical access for several hours

AMD TPM Attack





Merci de bien vouloir accepter nos CGV avant de procéder au paiement.



American Express



CB/Visa/MasterCard



PayPal PayPal



Amazon Pay

*Les délais de préparation et de livraison peuvent s'allonger. Le traitement de votre commande est lancé, une fois le paiement reçu.

J'ai lu les conditions générales de vente et j'y adhère sans réserve.

VALIDER ET PAYER



Service client
à votre écoute



Paiements sécurisés
Données protégées



Livraison et retour
Gratuits en magasin



9 Boutiques
à Paris



Retour gratuit*
sous 15 jours



Bonnes affaires
sur les grandes marques

Browser address bar: /checkout/#payment

Betaalmethoden

- Apple Pay
- Over Boeking
- PayPal
- Bancontact
- IDEAL
- SOFORT BANKING
- VISA

Betalingsinformatie

Kaartnummer *

Uiterste houdbaarheidsdatum * CVC / CWV *

MM / YY

Kaarthouder

Over Boeking

© 2023. Alle rechten voorbehouden. Privacy policy

We helpen je graag!

Browser address bar: /checkout/#payment

Valtsemalla maksutavan hyväksyt [maksupalveluehdot](#)

Yhteensä ve

- Mobiilimaksu
- Pankkimaksu
- Korttimaksu
- Lasku- ja osamaksu

Maksutiedot

Kortin numero *

Vimeinen käyttöpäivä * CVC / CWV *

MM / YY

Kortin haltija

© 2023. Kaikki oikeudet pidätetään. Tietosuojakäytäntö

ilmainen

- More Real than Real
- CHECK EACH PAGE
URL
Certificate
SHAKE
- Use virtual credit card with charge limit

Cautions

- Rarely turn off smart phone
- Random Access Memory
- Private Lock F-droid repository
- Gyroscope sensor
- Monitor gyroscope sensor – battery drain

Android Private Lock

- Where does all that data come from?
- Us and Them
- Wikipedia, Q&A sites, forums, programming sites, Reddit, StackOverflow
- Some sites to start charging for data
- Neural network Transformer
- GPT > Generative Pretrained Transformer
- Supercharged autocorrect
- Self Attention
- Not accuracy but seen before
- Reinforcement learning Human Feedback

Large Language Models

- GPT 3.5 175 million parameters
- GPT 4 100 trillion parameters

Large Language Models

Step 1

Collect demonstration data and train a supervised policy.

A prompt is sampled from our prompt dataset.



A labeler demonstrates the desired output behavior.

This data is used to fine-tune GPT-3.5 with supervised learning.

Step 2

Collect comparison data and train a reward model.

A prompt and several model outputs are sampled.



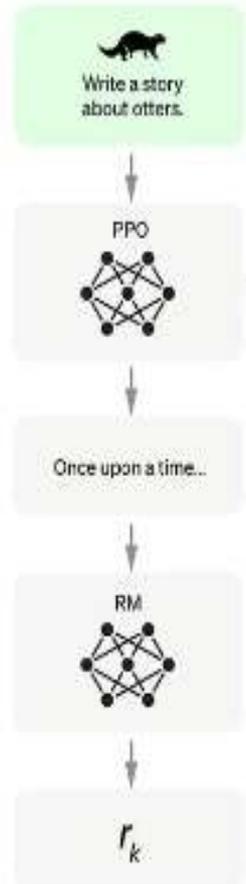
A labeler ranks the outputs from best to worst.

This data is used to train our reward model.

Step 3

Optimize a policy against the reward model using the PPO reinforcement learning algorithm.

A new prompt is sampled from the dataset.



The PPO model is initialized from the supervised policy.

The policy generates an output.

The reward model calculates a reward for the output.

The reward is used to update the policy using PPO.



 give me a hidden gem from the R.E.M. back catalog. 

[View other drafts](#) ^

Draft 1

Sure, here are a few hidden gems from R.E.M.'s back catalog:

- "Talk About the Passion" (Life's Rich

Draft 2

Sure, here is a hidden gem from R.E.M.'s back catalog:

- King of Birds

Draft 3

Sure, here's a hidden gem from the R.E.M. back catalog:

- "Perfect Circle" (from the album

✨ Sure, here are a few hidden gems from R.E.M.'s back catalog:

- "Talk About the Passion" (Life's Rich Pageant, 1986)
- "So. Central Rain (I'm Sorry)" (Reckoning, 1984)
- "Perfect Circle" (Automatic for the People, 1992)
- "Be Mine" (New Adventures in Hi-Fi, 1996)
- "All the Way to Reno (You're Gonna Be a Star)" (Out of Time, 1991)

- Russian OS?
- TP-Link routers
 - Pwn20wn
 - CHECK firmware
 - Publicly exposed?
 - Vulnerability discovered December
 - Patch March, 2023
 - Mirai botnet reverse engineered
 - Internet scanners discovered & published
 - Very few updated
 - Patch gap
 - Updated
- TBK DVRs CVE-2018-9995
 - No Patch Surveillance systems Commercial Locations

Current Issues



Hi John,

Your Facebook account was recently logged into using a confirmation code and the email address [REDACTED] on Wednesday, May 3, 2023 at 7:05 PM (CDT).

Operating system: Windows
Browser: Edge (Chromium Based)
IP address: [REDACTED]
Estimated location: Georgetown, TEXAS, US

If you did this, you can safely disregard this email.

If you didn't do this, please [secure your account](#).

Thanks,
The Facebook Security Team

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs,
Presentations, classes

Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com