Sun City Computer Club

Cyber Security SIG
April 4, 2024

Questions, Comments, Suggestions welcomed at any time

Even Now

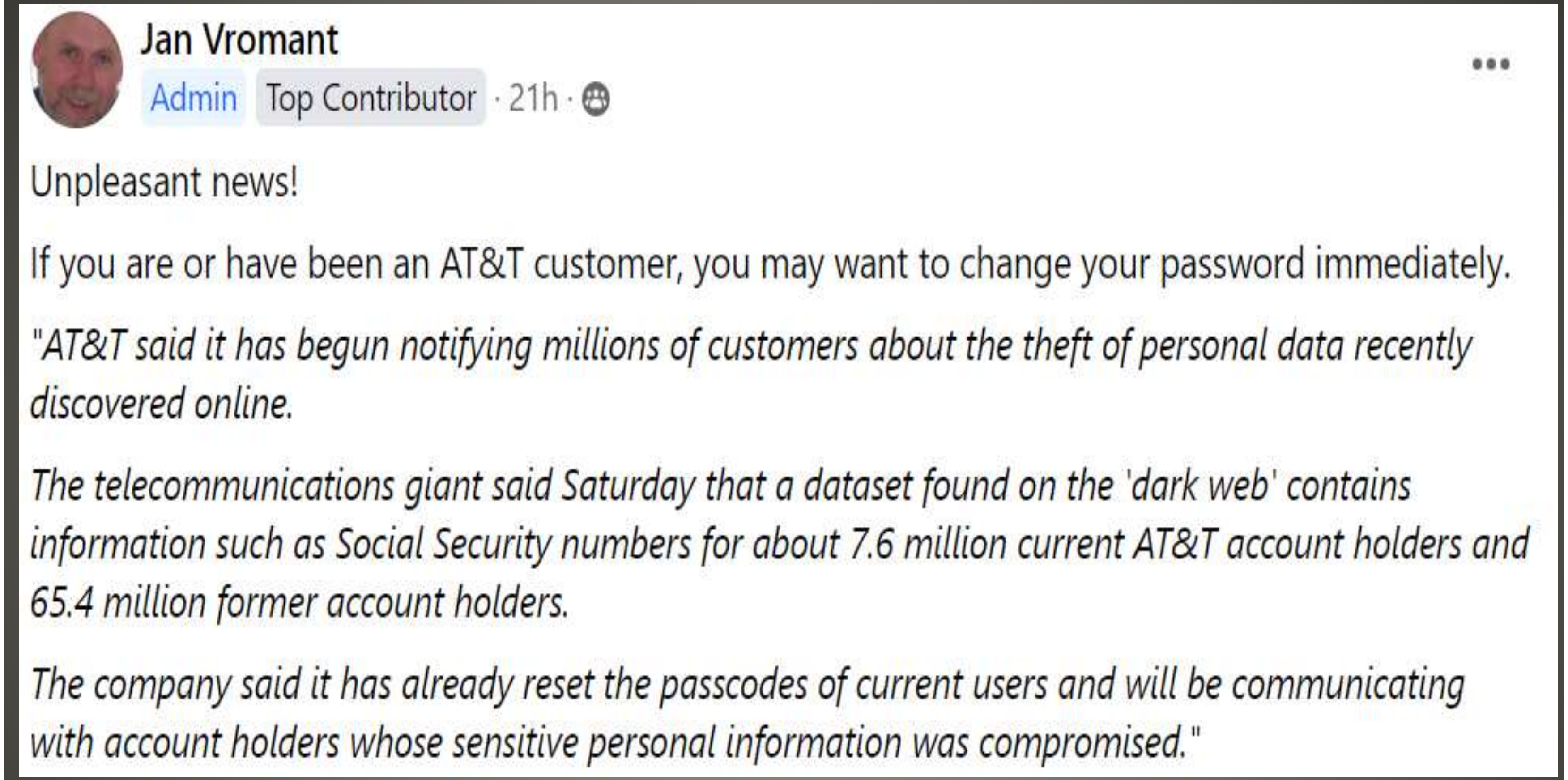
- Audio recording of this session as MP4 file
- Audio recording available at link shown above
- Wake Words

Audio Recording In Progress

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

Browser versions

- Edge Version 123.0.2420.65 (Official build) (64-bit)
- Chrome Version 123.0.6312.106 (Official Build) (64-bit)
- Firefox 124.0.2 (64-bit)
- Brave Version 1.64.116 Chromium: 123.0.6312.105 (Official Build) (64-bit)
- DuckDuckGo Version 0.73.0
- Vivaldi 6.6.3271.55
- Safari 17.4.1 (19618.1.15.11.14)
- Tor 13.0.13 Firefox 115.9



Jan Vromant

Unpleasant news!

If you are or have been an AT&T customer, you may want to change your password immediately.

"AT&T said it has begun notifying millions of customers about the theft of personal data recently discovered online.

The telecommunications giant said Saturday that a dataset found on the 'dark web' contains information such as Social Security numbers for about 7.6 million current AT&T account holders and 65.4 million former account holders.

The company said it has already reset the passcodes of current users and will be communicating with account holders whose sensitive personal information was compromised."

Computer Club Facebook

- AT&T denies 2021 and again 2024
- Data appears significant
- "proven, with sufficient confidence, that the data is real and the impact is significant."
- 73 million records 7.6M current 65.4M former
- Names, personal addresses, phone numbers, DOB, SSN, Email addresses, AT&T account numbers, passcodes

  Weak passcodes
- Passcodes reset delay to allow passcode resets
- 12-hour outage Feb 22, 2024 $5 account credit
- More likely to trust anything from AT&T
- Your data on Internet lives forever
- Family plan – their information

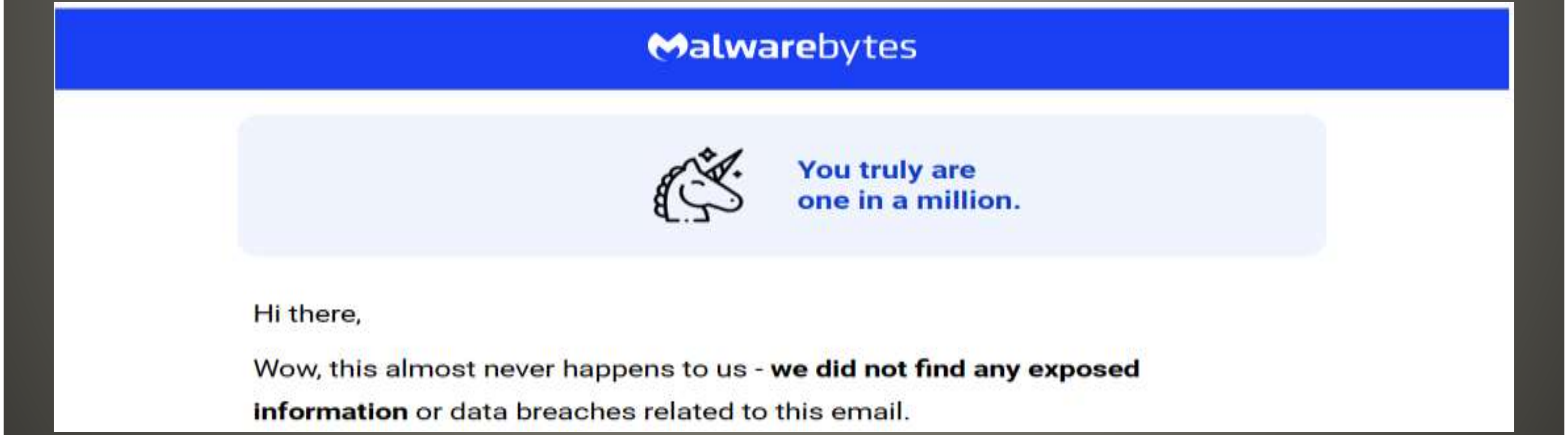
- Monitor Credit reports, accounts,
- Credit Monitoring ?? Credit Karma
- Fraud Alert Credit Freeze
- Fraud departments
- Document Any/everything
- https://www.identitytheft.gov/#/
- After Actions Frauds, Scams, IDentity fraud
- Foundations of Scam and Fraud Prevention

Alleged AT&T data leak

Data Breaches

- AT&T data breaches in past
- Verizon
- T-Mobile – Home Internet interest
- Passcodes – SIM swap protections
- May need to visit store
  With multiple forms of Identification
- MalwareBytes Digital Footprint Scan

https://www.malwarebytes.com/digital-footprint

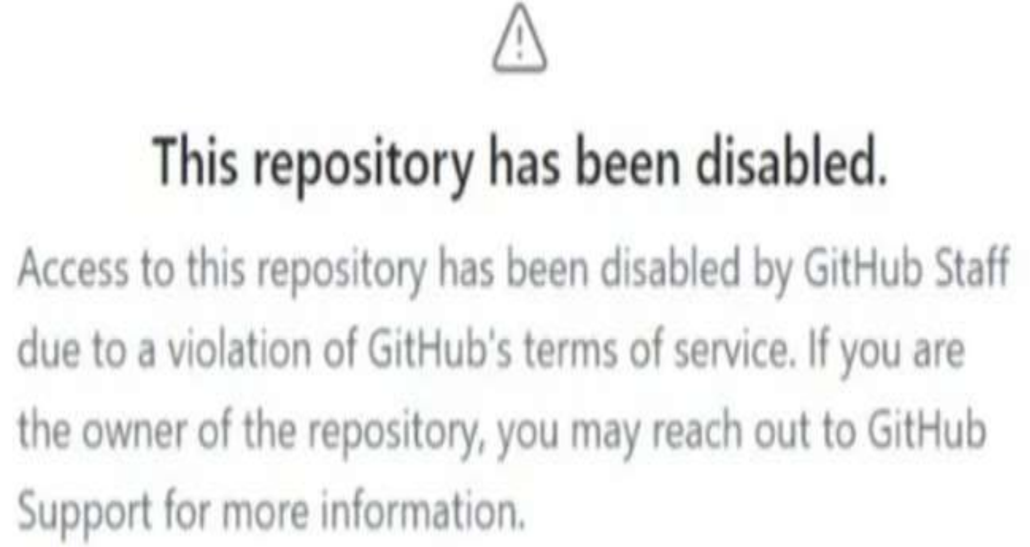


You truly are one in a million.

Hi there,

Wow, this almost never happens to us - **we did not find any exposed information** or data breaches related to this email.

- 2 versions with backdoor 5.6.0 5.6.1
- Software supply chain CVE-2024-3049 CVSS 10.0
- "Through a series of complex obfuscations, the liblzma build process extracts a prebuilt object file from a disguised test file existing in the source code, which is then used to modify specific functions in the liblzma code,"
- Software linked to these libraries Intercept and modify data
- sshd and systemd
- 4 code commits
- GitHub disabled
- Linux scanner

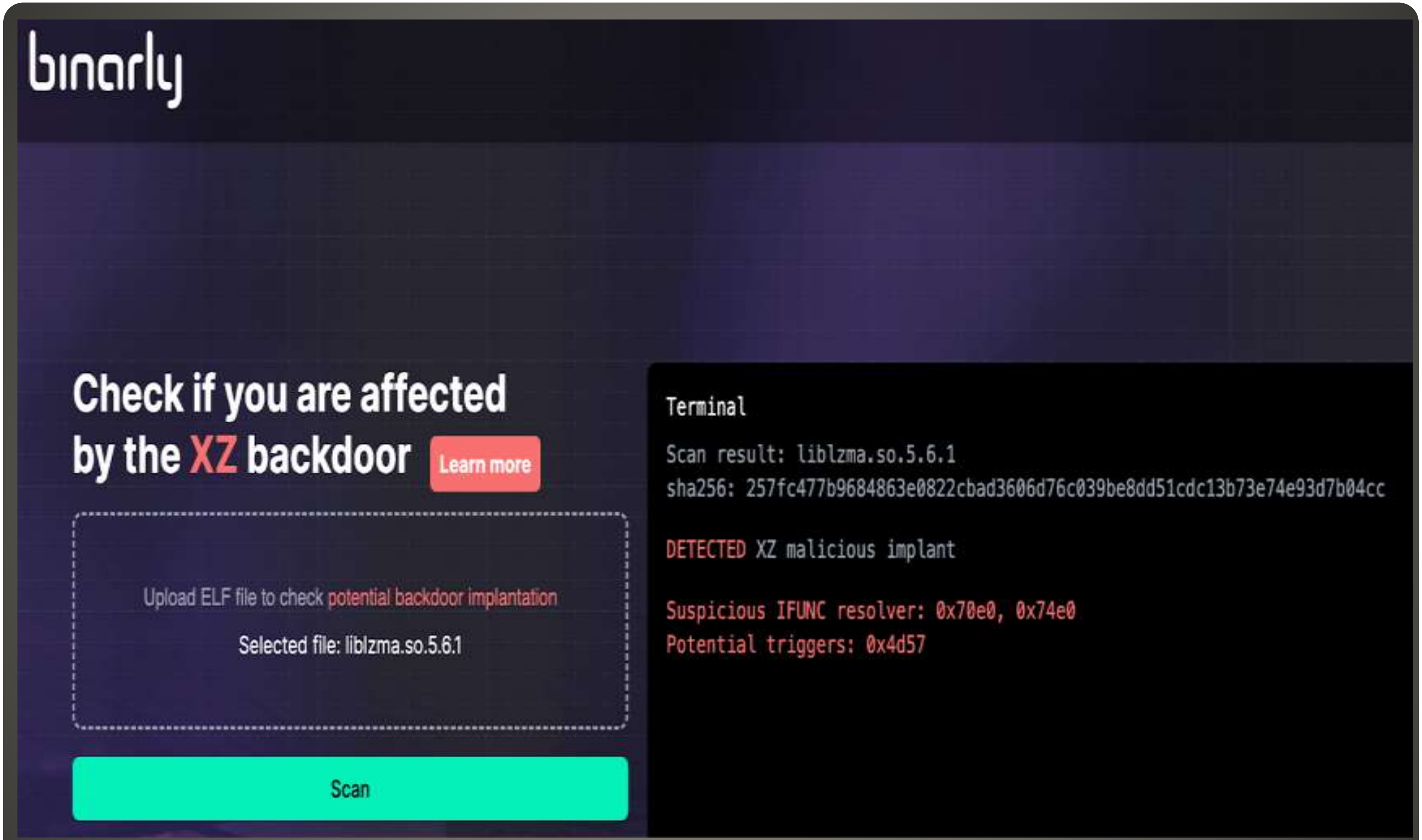


This repository has been disabled.

Access to this repository has been disabled by GitHub Staff due to a violation of GitHub's terms of service. If you are the owner of the repository, you may reach out to GitHub Support for more information.

Linux data compression library XZ Utils

XZ scanner



Check if you are affected by the XZ backdoor

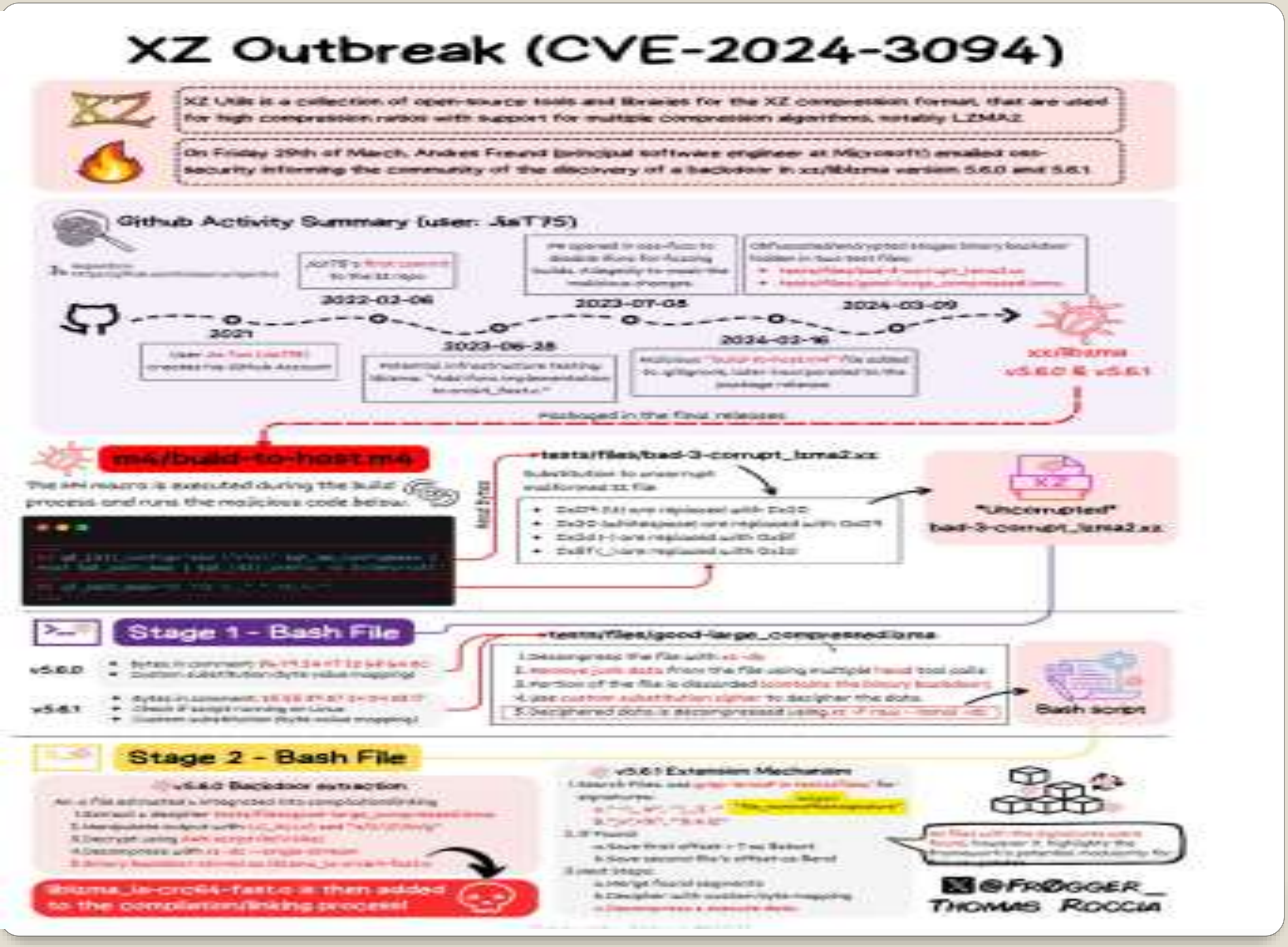
Upload ELF file to check potential backdoor implantation

Selected file: liblzma.so.5.6.1

```
Terminal

Scan result: liblzma.so.5.6.1
sha256: 257fc477b9684863e0822cbad3606d76c039be8dd51cdc13b73e74e93d7b04cc

DETECTED XZ malicious implant

Suspicious IFUNC resolver: 0x70e0, 0x74e0
Potential triggers: 0x4d57
```

XZ Open Source

- SSH daemon – incoming encrypted shell
- Secret & invisible backdoor
- Someone/anyone/anywhere login to any Linux system
- Open-Source problem Open-source fix/detection
- Developers of all skill levels working collectively/anonymously
- Compression library test files – who would check those
- Complex and time consuming   2021 – 2024
- Persona build 6,000 changes 7 projects 1 prior attempt found
- Take down/out previous developer
- But it is Open-Source



XZ Outbreak (CVE-2024-3094)

XZ Utils is a collection of open-source tools and libraries for the XZ compression format, that are used for high compression ratios with support for multiple compression algorithms, notably LZMA2

On Friday 29th of March, Andres Freund (principal software engineer at Microsoft) emailed oss-security informing the community of the discovery of a backdoor in xz/liblzma version 5.6.0 and 5.6.1

Github Activity Summary (user: JiaT75)

- 2021: User Jia Tan (JiaT75) created his Github Account
- 2022-02-06: JiaT75's first commit to the xz repo
- 2023-06-28: Potential infrastructure testing liblzma: "Add ifunc implementation to crc64_fast.c"
- 2023-07-08: PR opened in oss-fuzz to disable ifunc for fuzzing builds, allegedly to mask the malicious changes
- 2024-02-16: Malicious "build-to-host.m4" file added to .gitignore, later incorporated to the package release
- 2024-03-09: Obfuscated/encrypted stages binary backdoor hidden in two test files:
  - tests/files/bad-3-corrupt_lzma2.xz
  - tests/files/good-large_compressed.lzma

xz/liblzma v5.6.0 & v5.6.1

Packaged in the final releases

m4/build-to-host.m4

The m4 macro is executed during the build process and runs the malicious code below:

```
[illegible]
```

tests/files/bad-3-corrupt_lzma2.xz

Substitution to uncorrupt malformed xz file

- 0x09 (\t) are replaced with 0x20
- 0x20 (whitespace) are replaced with 0x09
- 0x2d (-) are replaced with 0x5f
- 0x5f (_) are replaced with 0x2d

"Uncorrupted" bad-3-corrupt_lzma2.xz

Stage 1 - Bash File

v5.6.0
- Bytes in comment: [illegible]
- Custom substitution (byte value mapping)

v5.6.1
- Bytes in comment: [illegible]
- Check if script running on Linux
- Custom substitution (byte value mapping)

tests/files/good-large_compressed.lzma

1. Decompress the file with xz -dc
2. Remove junk data from the file using multiple head tool calls
3. Portion of the file is discarded (contains the binary backdoor)
4. Use custom substitution cipher to decipher the data
5. Deciphered data is decompressed using xz -F raw --lzma1 -dc

Bash script

Stage 2 - Bash File

v5.6.0 Backdoor extraction

An .o file extracted & integrated into compilation/linking

1. Extract & decipher tests/files/good-large_compressed.lzma
2. Manipulate output with LC_ALL=C and "[illegible]"
3. Decrypt using AWK script (RC4-like)
4. Decompress with xz -dc --single-stream
5. Binary backdoor stored as liblzma_la-crc64-fast.o

liblzma_la-crc64-fast.o is then added to the compilation/linking process!

v5.6.1 Extension Mechanism

1. Search files and grep -broaf in tests/files/ for signatures:
   a. [illegible]
   b. [illegible]
2. If found:
   a. Save first offset + 7 as $start
   b. Save second file's offset as $end
3. Next stage:
   a. Merge found segments
   b. Decipher with custom byte mapping
   c. Decompress & execute data

No files with the signatures were found, however it highlights the framework's potential modularity for [illegible]

@FR0GGER_
Thomas Roccia

- Elevation of privilege vulnerability
- Versions 5.14 – 6.6.14   CVSS 7.8

Linux

SmartPhone in SOS Mode?

- No recent calls?
- No cell service status?
- You may have been Sim Swapped
- You may have been Sim stolen
- You may have been Sim replaced
- Phone-port attack
- Hardware Security Key
- Authenticator App

- Brave VPN

  Default Install
- FCC Ban signal jammers
- ChatGPT down 25-Mar-2023 few hours
- Seven Chinese nationals charged   reward $10M

  Targeting critics of China, business, politicians

  China “not us”

  Work accounts, personal emails, online storage, call records

  from news outlets, journalists, …

  with tracking links = location, IP address, …

  follow on attacks

  Government officials and spouses/family

  Companies also
- LLM emergent abilities –

  more about measurement than emergence

Current Issues

Current Issues

- Android malware PixPirate

  Any/Everything

  Access/Delete/Edit SMS/MMS/RCS

  Authenticator

  Financial & Banking apps

  PixPirate downloader via malicious link

  WhatsApp

  Authenticator app from banks/brokers

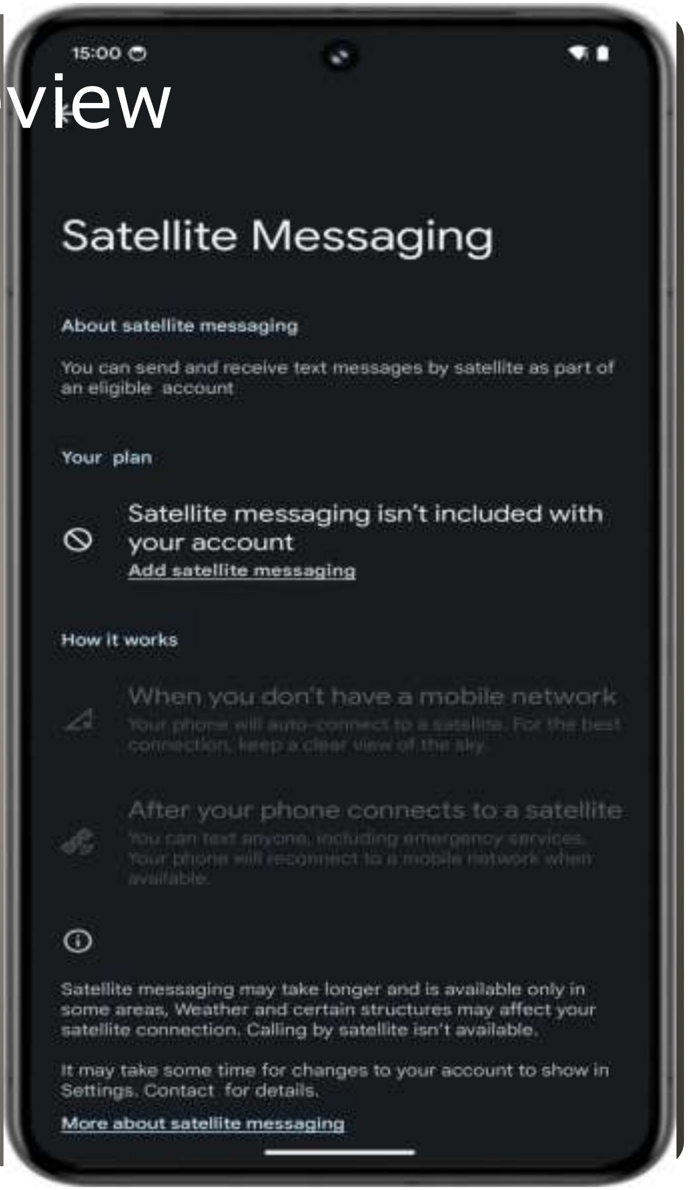
- Vermont residents finding AirTags on cars

  After visit to Canada

- Gmail restrictions 4 days in?
- FTC releases 2023 Privacy & Security Update

  AI, Health Privacy, Children Privacy, Geolocation data

- Android 15 developer preview
- SMS/MMS/RCS
- SpaceX 17mbps



15:00

Satellite Messaging

About satellite messaging

You can send and receive text messages by satellite as part of an eligible account

Your plan

Satellite messaging isn't included with your account

Add satellite messaging

How it works

When you don't have a mobile network

Your phone will auto-connect to a satellite. For the best connection, keep a clear view of the sky.

After your phone connects to a satellite

You can text anyone, including emergency services. Your phone will reconnect to a mobile network when available.

Satellite messaging may take longer and is available only in some areas. Weather and certain structures may affect your satellite connection. Calling by satellite isn't available.

It may take some time for changes to your account to show in Settings. Contact for details.

More about satellite messaging

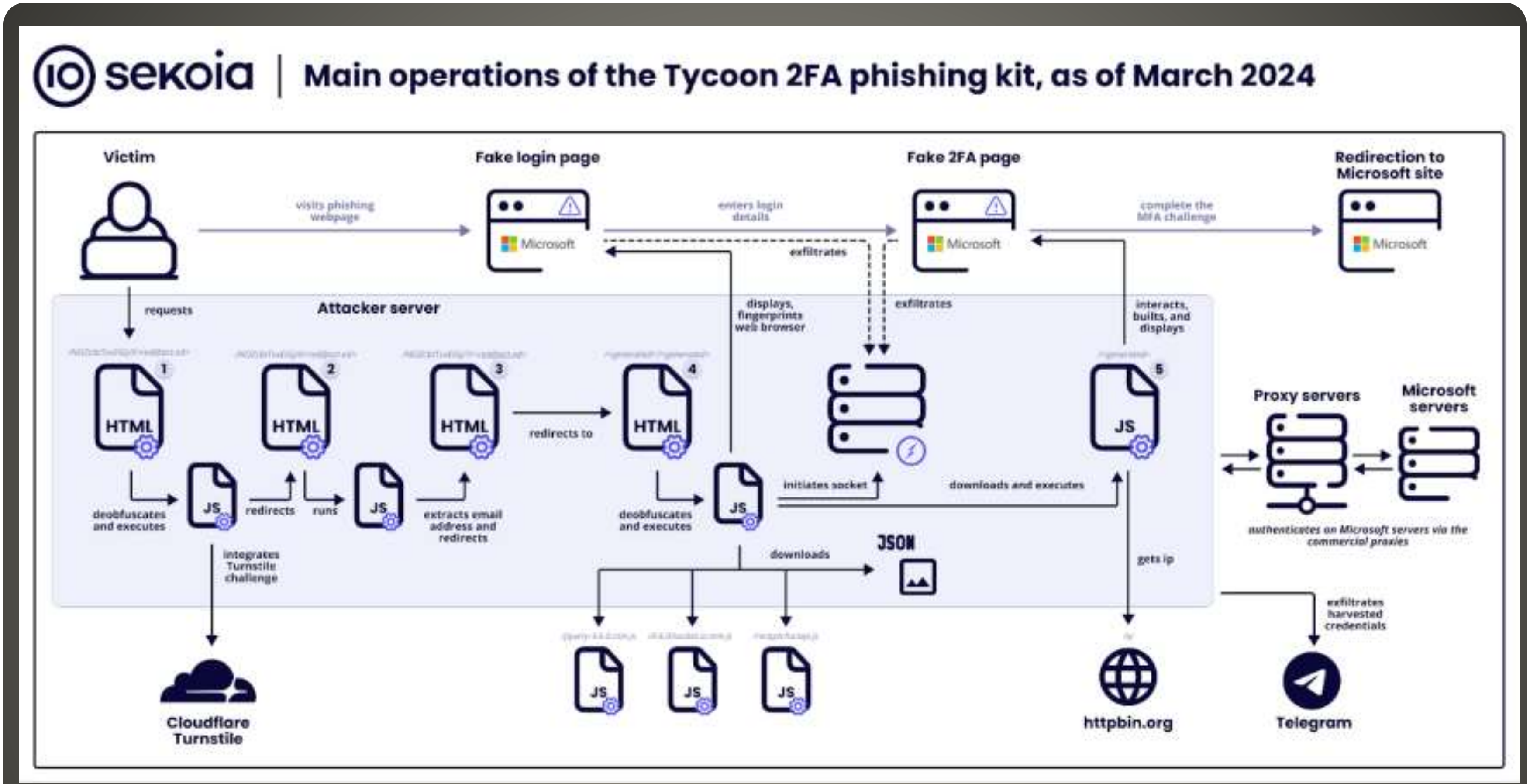
- Phishing-as-a-service
- Target Microsoft 365 and Gmail
- Bypass 2FA protections
- August 2023 - recent update
- 1100 domains
- Proxy steal the relay
- Capture then replay session cookies

Tycoon 2FA

Tycoon 2FA

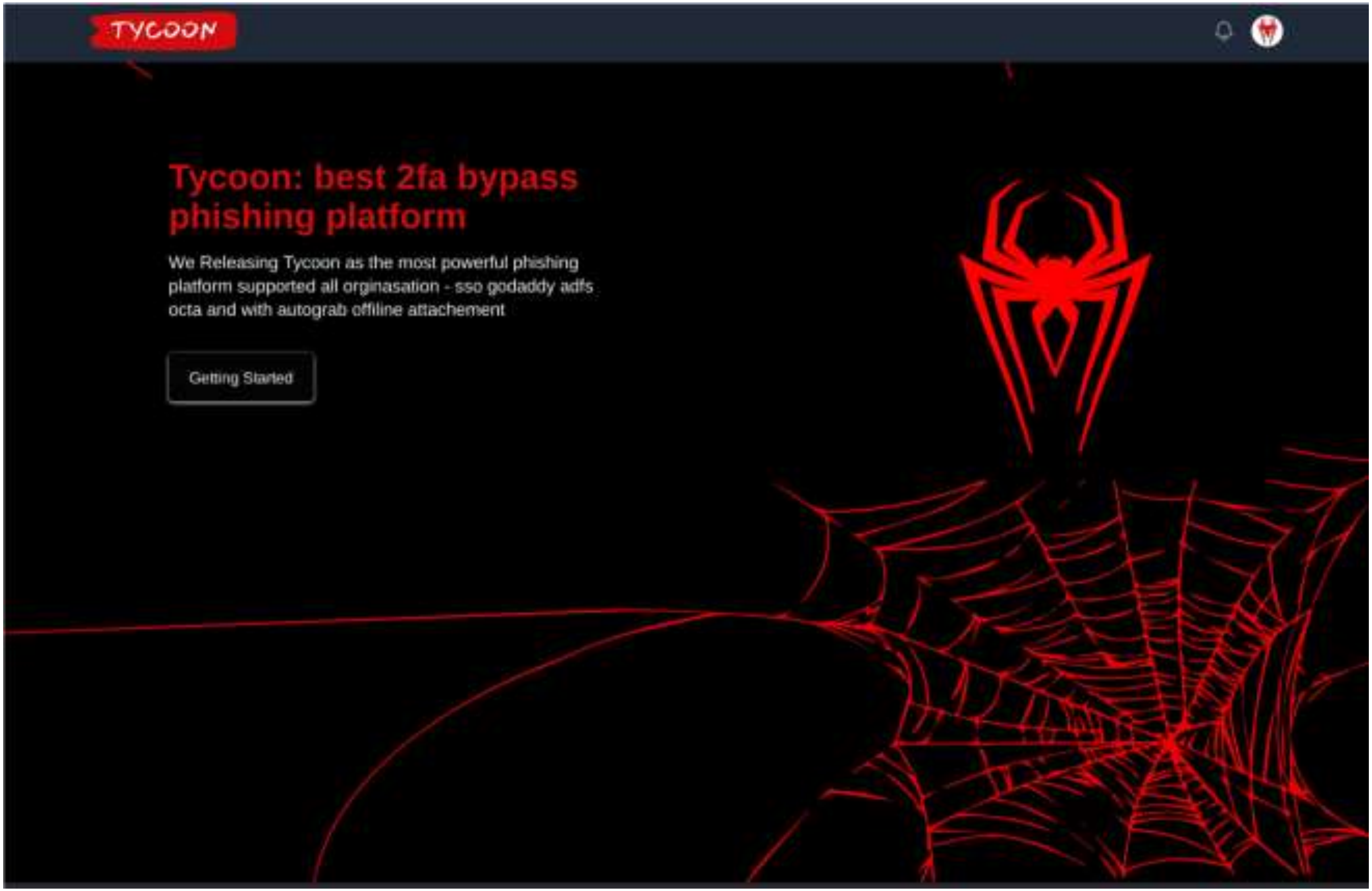
- Stage 0 – malicious link via email
- Stage 1 – filters out bots need human
- Stage 2 – scripts extract victim’s email
- Stage 3 – redirect to phishing site
  fake login page
- Stage 4 – Fake Microsoft login page
  steal credentials
  exfiltrate via WebSockets
- Stage 5 – mimic 2FA challenge
  intercept 2FA token
- Stage 6 – victim presented with fake page

Tycoon 2FA


sekoia | Main operations of the Tycoon 2FA phishing kit, as of March 2024

Tycoon 2FA

- $120 entry fee 10 days



Tycoon: best 2fa bypass phishing platform

We Releasing Tycoon as the most powerful phishing platform supported all orginasation - sso godaddy adfs octa and with autograb offiline attachement

- 6,000 Asus routers infected in 72 hours
- 40,000 devices 88 countries
- End-of-life routers   and smart devices
- Cybercriminal proxy service *Faceless*
- Response to law enforcement

  Intelligence organizations

  Security suites

Suddenlink/Optimum used Asus routers

TheMoon Botnet

- State Department $10M reward
  UnitedHealthcare hackers
  $3.3B lifeline to affected providers
  CEO Congress testimony April 30
- US government watching?
  Wiretaps & listening devices
    Court orders or data broker purchase
  CCTV with facial recognition
    Social media -> CCTV
  Metadata analysis
  Data collection programs
  Backdoor devices
  Social media monitoring
- Flipper Zero in classroom
- Microsoft & OpenAI building $100B supercomputer
- Microsoft Copilot for Security subscription
- Mozilla Onerep partnership ended – CEO to blame

Current Issues

- Atomic Stealer
- Arc Browser Google sponsored link
- Use Control-Click bypass Gatekeeper
- Update System Settings
- Used Account password
- Now uses Keychain & Keychain data

- Meethub

- Control-click AVOID!!

Mac Info Stealer Apps

Current Issues

- US House of Representatives ban AI Copilot for staffers
- Apple ability to update iDevices in unopened boxes
- Google plan to destroy user’s data collected Incognito mode
- DOJ indicts China APT31 members
- Ukraine Safe Skies Anti-drone sensors Russia attacks Ukraine ISPs
- Apple customers target of MFA-bombing attacks
- Facebook project snoop on Snapchat on device VPN
  Bypass Snapchat encryption Marketing ploy
- Fujitsu finds malware data breach? Times 2?
- Microsoft Remove Russia companies' data off its cloud services
  Not political economic sanctions by EU
- New loader for Agent Tesla infostealer
  Email from a bank bank payment notification
  Loader obfuscation, polymorphic behaviour
- Apple Accept bombing Call from Apple’s official customer support number
- Microsoft Edge Private API Install Edge browser extensions

- Phishing-as-a Service Darcula   RCS

  More legitimate

  End-to-End encryption – avoid block due to content

  Subscription => 200 phishing templates hundreds of sectors

  20,000 domains, 11,000 IP addresses, 100 new domains daily

  Logo images, fonts, languages, lingo
- Cambridge University   British Library
- New OneDrive features

  Ransomware detection   IoC   delete suspicious files   roll back

  Personal Vault limit 3 -> unlimited

  Advanced sharing expiration dates   Secure password

  Make Available Offline
- Russia 63-hour GPS jamming attack

  March 22 22:38 – March 26 14:18   (GMT+1)

  Affected airspace Poland, Germany, Sweden, Netherlands, Latvia, etc.

  Not affected Belarus, Kaliningrad

Current Issues

Current Issues

- Android Banking Trojan   Vultur

  McAfee security app

  Dropper   3 payloads

  Record screen, log keystrokes, grant remote access, download files, upload files, install apps, delete files, block apps from running, click, scroll, swipe, …

- GTA 6 Mac macOS stealer

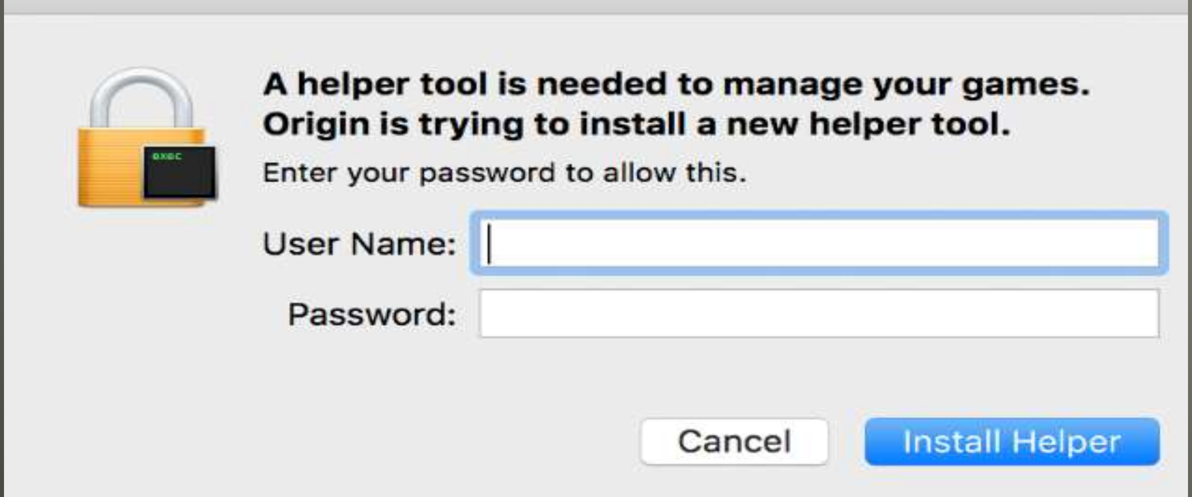
  Right click - Open

1 STEP

RIGHT CLICK

2 STEP

CLICK 'OPEN'



A helper tool is needed to manage your games.
Origin is trying to install a new helper tool.

Enter your password to allow this.

User Name:

Password:

Current Issues

- 3,205 *publicly reported* data compromises 2023
- Russia charges 6 for theft of 160,000 credit cards

  credit card & payment information

  order checkout pages fake payment page overlays

  Double check certificate / URL
- Indian government rescued 250 citizens

  Cambodia running cyber scams

  Many government agencies working the issue
- Apple AI Reference Resolution as Language Modeling (ReALM)

  Radically enhance how voice assistants understand/respond

  Understand pronouns & indirect references in conversation

  Parsing on-screen entities & locations

  Tune LLM for reference resolution tasks

  Users with disabilities

  Integrates text and visual information

- Open Web Application Security Project Foundation (OWASP)

  Non-Profit foundation to improve web security

  Breach Resumes of members misconfigured server
- IRS issues warning:

  Avoid others using or help setting up your IRS online account
- Signal & Cloud backup? End-to-end encryption

  Recovery from lost or damaged device
- Telegram to allow restricted incoming

  Russia, Belarus, Ukraine
- HP exits Russia 2 months early
- Taiwan earthquake & TSMC
- Chase Bank Chase Media Solutions

  Marketers tempt customers based on spending data
- Unsubscribe
- Wi-Fi Protected Setup caution

Current Issues

- FTC new rule (1-Apr-2024)

  directly file Federal court complaints

  compel scammers to return funds stolen by business or government impersonation

  potential to target impersonation of individuals

  via video deepfakes of AI voice cloning
- Airline & Smartphone access

https://cybernews.com/security/airlines-apps-data-collection/

- Zero-days on Pixel phones – Forensics teams

  Boot loader   Memory dump Training video

  GrapheneOS -privacy focused Pixel device mobile operating system
- Entertainment Software Ratings Board

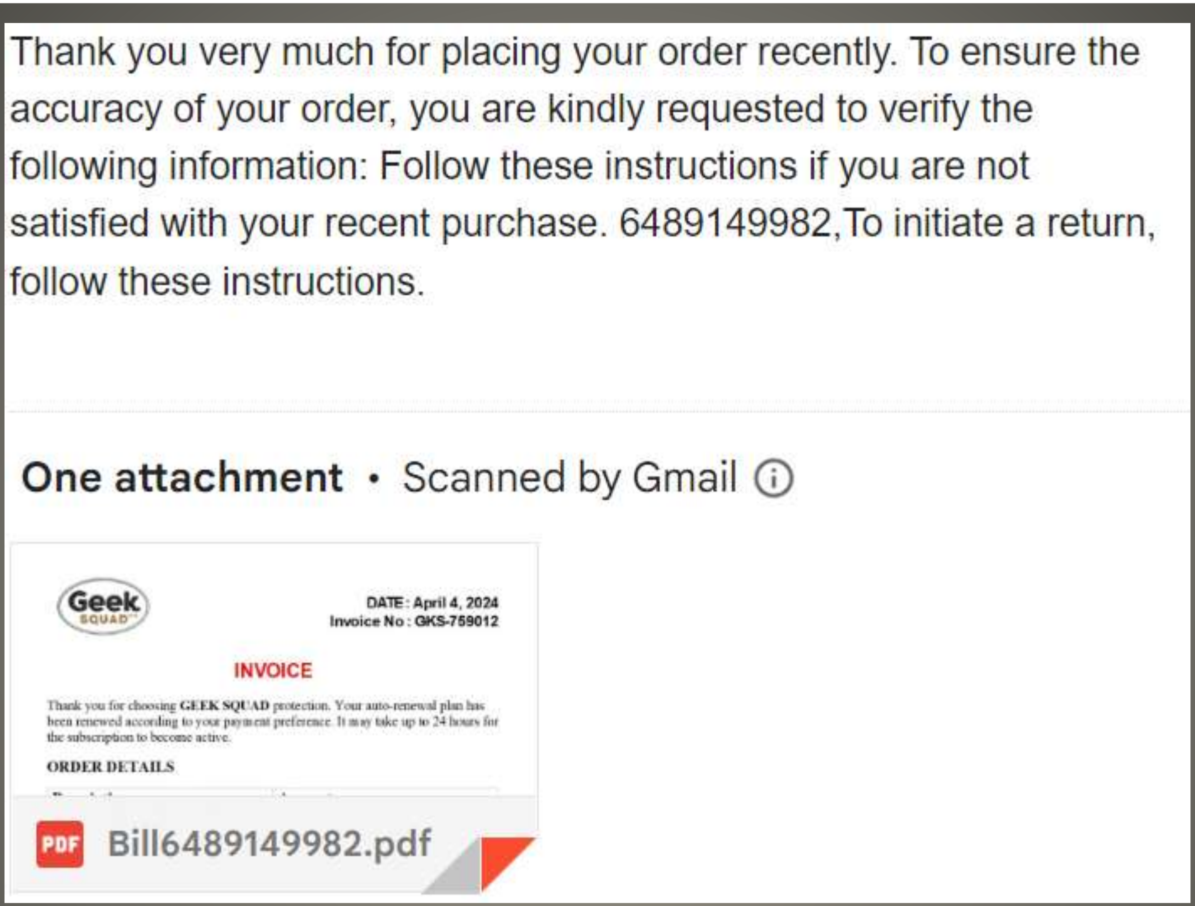
  Facial recognition age verification   FTC no
- Microsoft & Quantinuum “new era of quantum computing”
- German state Windows & Office -> Linux LibreOffice

Current Issues

Current Issues

- Privnote phishing site   lawsuit

  any message with crypto address changed



Thank you very much for placing your order recently. To ensure the accuracy of your order, you are kindly requested to verify the following information: Follow these instructions if you are not satisfied with your recent purchase. 6489149982,To initiate a return, follow these instructions.

One attachment • Scanned by Gmail ⓘ

Geek SQUAD

DATE : April 4, 2024
Invoice No : GKS-759012

INVOICE

Thank you for choosing **GEEK SQUAD** protection. Your auto-renewal plan has been renewed according to your payment preference. It may take up to 24 hours for the subscription to become active.

ORDER DETAILS

Bill6489149982.pdf

sigh

VPN

- Hide

  IP Address
  Geolocation
  Browsing Activity from ISPs
  PII in transit
  Torrenting

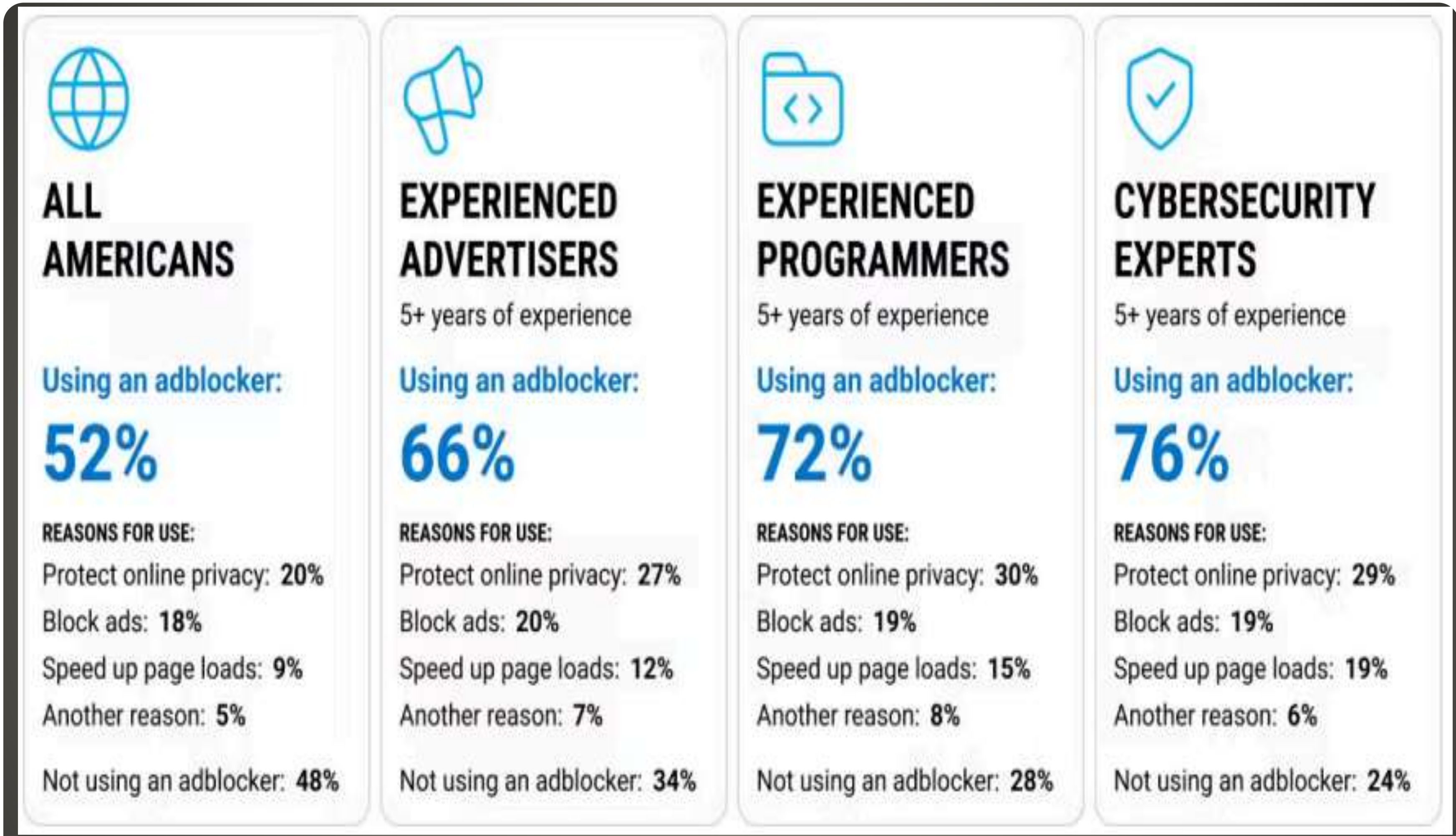
- Does Not Hide

  Account Activities
  Payment Information
  Malware and Viruses
  MAC address
  MetaData

- Hacker Summer Camp
- Private 2022 event “Hack a Hotel”
- Check Out screen
- Results just in
- Unsaflok   Saflok brand RFID room locks
- 13,000 properties 131 countries
- Get a keycard – any keycard
- Get a code write 2 keycards tap 2 keycards
- First rewrites a portion of locks data
- Second one opens the door
- OR Android Or Flipper Zero
- How to get code to reverse engineer?   Ebay

- Onity keycard 2012   No fix   cross-country burglary spree

3 Million Hotel Keycard Locks



ALL AMERICANS

Using an adblocker:

52%

REASONS FOR USE:

Protect online privacy: **20%**

Block ads: **18%**

Speed up page loads: **9%**

Another reason: **5%**

Not using an adblocker: **48%**

EXPERIENCED ADVERTISERS

5+ years of experience

Using an adblocker:

66%

REASONS FOR USE:

Protect online privacy: **27%**

Block ads: **20%**

Speed up page loads: **12%**

Another reason: **7%**

Not using an adblocker: **34%**

EXPERIENCED PROGRAMMERS

5+ years of experience

Using an adblocker:

72%

REASONS FOR USE:

Protect online privacy: **30%**

Block ads: **19%**

Speed up page loads: **15%**

Another reason: **8%**

Not using an adblocker: **28%**

CYBERSECURITY EXPERTS

5+ years of experience

Using an adblocker:

76%

REASONS FOR USE:

Protect online privacy: **29%**

Block ads: **19%**

Speed up page loads: **19%**

Another reason: **6%**

Not using an adblocker: **24%**

Ad blocker usage

- Recovery Seminar
- https://vimeo.com/882272974?share=copy
- NOW, Your input, experiences, …

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

Computer Club, Help Center, SIGs, Presentations, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com