Sun City Computer Club

Cyber Security SIG
May 16, 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

New Leader???

- SIG Leader replacement
- Take over
- Inclusion Zoom & Recording
- Training, Counsel
- Summers are Important
- Leader(s)???

Recent Updates

- Apple 24+ security patches
- Microsoft 60+ security patches
- Google Android & ChromeOS

SCCCCyber

Monday, May 13, 2024

Apple Updates May 13, 2024

Apple releasing many updates today: 13-May-2024.

Updates to iOS 17.5, iPadOS 17.5, iPadOS 16.7.8, macOS 14.5, Safari 17.5, iOS 16.7.8, macOS Ventura 13.6.7, macOS Monterey 12.7.5, watchOS 10.6, tvOS 17.5

New features and security updates.

Posted by John Jenkinson at 1:07 PM No comments

Friday, May 10, 2024

Google releases new version of Chrome Browser due to vulnerabilities

Google releases updates to its Chrome browser to address several vulnerabilities.

"Google is aware that an exploit for CVE-2024-4671 exists in the wild.

Users are recommended to upgrade to Chrome version 124.0.6367.201/.202 for Windows and macOS, and version 124.0.6367.201 for Linux to mitigate potential threats.

Browsers based on the Chromium engine will probably release their updates soon.

It is good practice to check for browser updates before use on any financial transactions.

Posted by John Jenkinson at 2:47 PM No comments

Thursday, May 9, 2024

Dell investigating data breach

DELL Technologies

An important message about your Dell

Cyber Security News blog

Current Browser versions

- Chrome Version 125.0.6422.61 (Official Build) (64-bit)
- Edge Version 124.0.2478.105 (Official build) (64-bit)
- Firefox Version 126.0
- Vivaldi Version 6.7.3329.31
- Tor
- Brave Version 1.66.110 Chromium: 125.0.6422.60
- DuckDuckGo 0.70.0
- Safari 17.5 19618.2.12.11.6

Passkeys

- Asymmetric cryptography
- Public Private key pair
- Both Ends
- Site Private key kept private Public key publicly viewable
- You Private key in authenticator on device(s)
- You Public key at site
- Lose a key Lose access MULTIPLE KEYS!
- No need to think password up
- No need to know password
- No password to type in No password in password vault
- Linked to site Linked to device Biometric protections
- Vendor Specific iPhone/iPad/Mac/Apple watch
- Google Titan Key Android ChromeOS
- Microsoft Account support all consumer accounts
  Windows, Android, iOS

Android Dirty Stream

- Control of app(s)
- Android Content Provider System
- Secure data exchange between applications

  strict isolation of data, permissions, path validation
- Vulnerable apps

  Change behaviour, access sensitive data, …

  4 billion installations

  Google Play Store updates

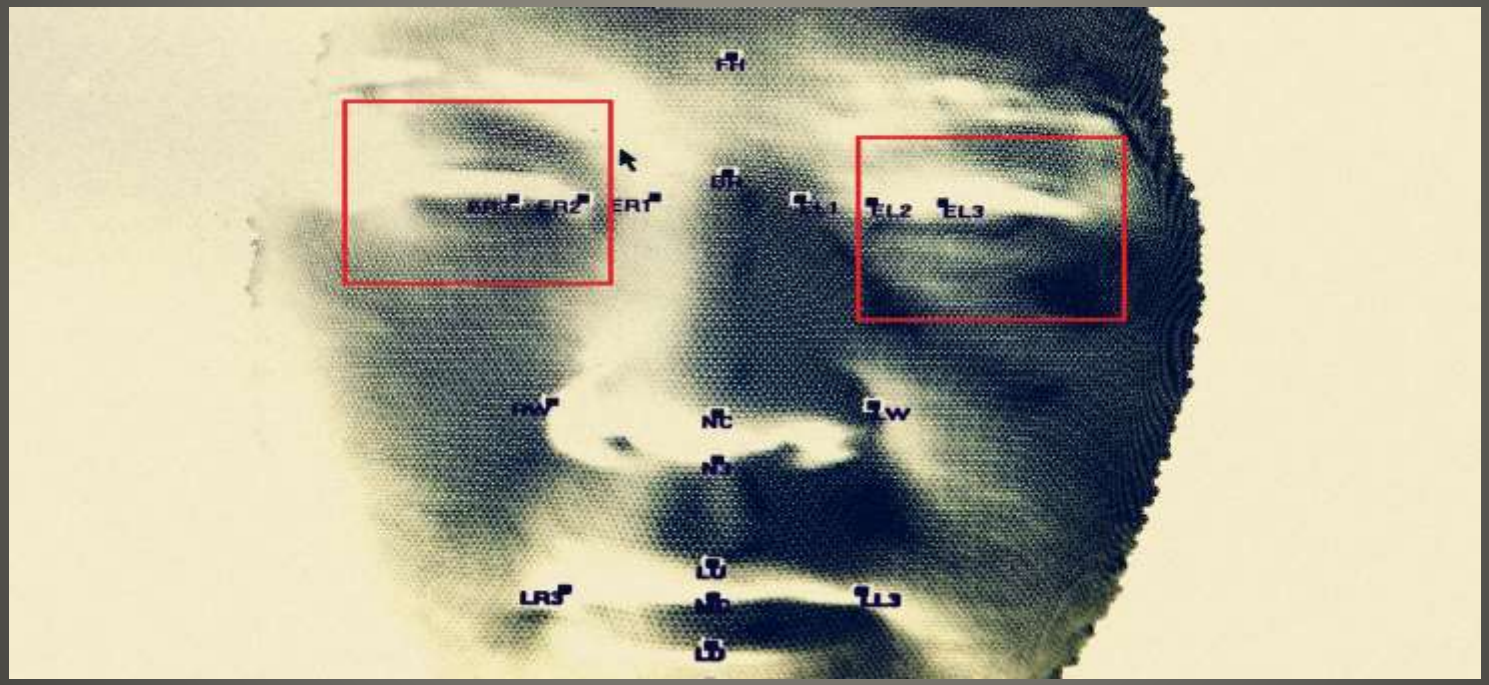
  Google Play Store security guidelines update

Current Issues

- WhatsApp usage surge in US
- GitLab
  - Attackers send password reset to ANY email address
  - Change GitLab's account email address
  - CVE-2023-7028 CVSS 10.0
- Weak DMARC policies exploited APT43 North Korea
- Responsible AI Transparency Report
  - 2023 30 responsible AI tools created
- Streamer's password sharing
  - Ancillary data
- Microsoft ZTDNS Zero Trust DNS
  - Encrypted and cryptographically authenticated
  - Administrator domain restrictions
  - One but not both
  - Windows Filtering Platform
- Bitwarden multi-factor authentication app

- Outabox Australian firm Facial Recognition bars & clubs Kiosk Covid-19 Temperature & problem gamblers "Have I Been Outaboxed?"

  Driver's license, signature, address, birthdate, club visits, gambling machine visits



Current Issues

Current Issues

- Microsoft MAI-1 New AI model
- Cuckoo macOS Infostealer
  Fails to run in Russia, Ukraine, Belarus, et al
  Disguised as music ripper
- Fax for medical records HIPPA
  Postal Annex, Computer Club, CA Member Services
  Consider privacy for FAX services on Internet
- Sun City I post Taylor Swift tickets
- Wichita, Kansas cyber attack
- Hubble Network Bluetooth connection to satellite
- Google MFA options Authenticator, hardware security keys
- UK MoD data breach
  Details current regular, reservists, former members
  Royal Navy, Army, Air Force HMRC

Current Issues

- Ascension hospitals cyber attack
- Singing River Hospital System 250,000 -> 900,000 patients
- New rules US Intelligence Agencies
  Purchase of personal information
  From data brokers
  Ability to experiment
- Tinyproxy CVE-2023-49606
- AT&T delays email delivery from Microsoft 365 Heavy SPAM
- Dell Data Breach 349 million customers
- Insulin pump software recall
  t:connect mobile app t:sli X2 insulin pump
  App crash, relaunched battery drain
  hundreds of patients injured
- Google Messages notifications
  Show names of unknown people who contact you
  Contact person with profile discovery enabled + phone number

[redacted]
May 6 at 8:42 PM ·

My account has been hacked and I have no Taylor Swift tickets for sale.

4 7 comments

Like Comment Send

All comments

[redacted]
That's what I thought....
I had a quite a conversation with "you" last Tuesday... to the point of almost transferring funds for 2 tickets, and setting up a transfer of the tickets to my Ticketmaster account.
When things sounded fishy/questionable, I reported this as a possible scam to admin on this site last week.

2

1d Like Reply Edited

[redacted] Admin Group expert +1
[redacted]he post in question was deleted earlier today -

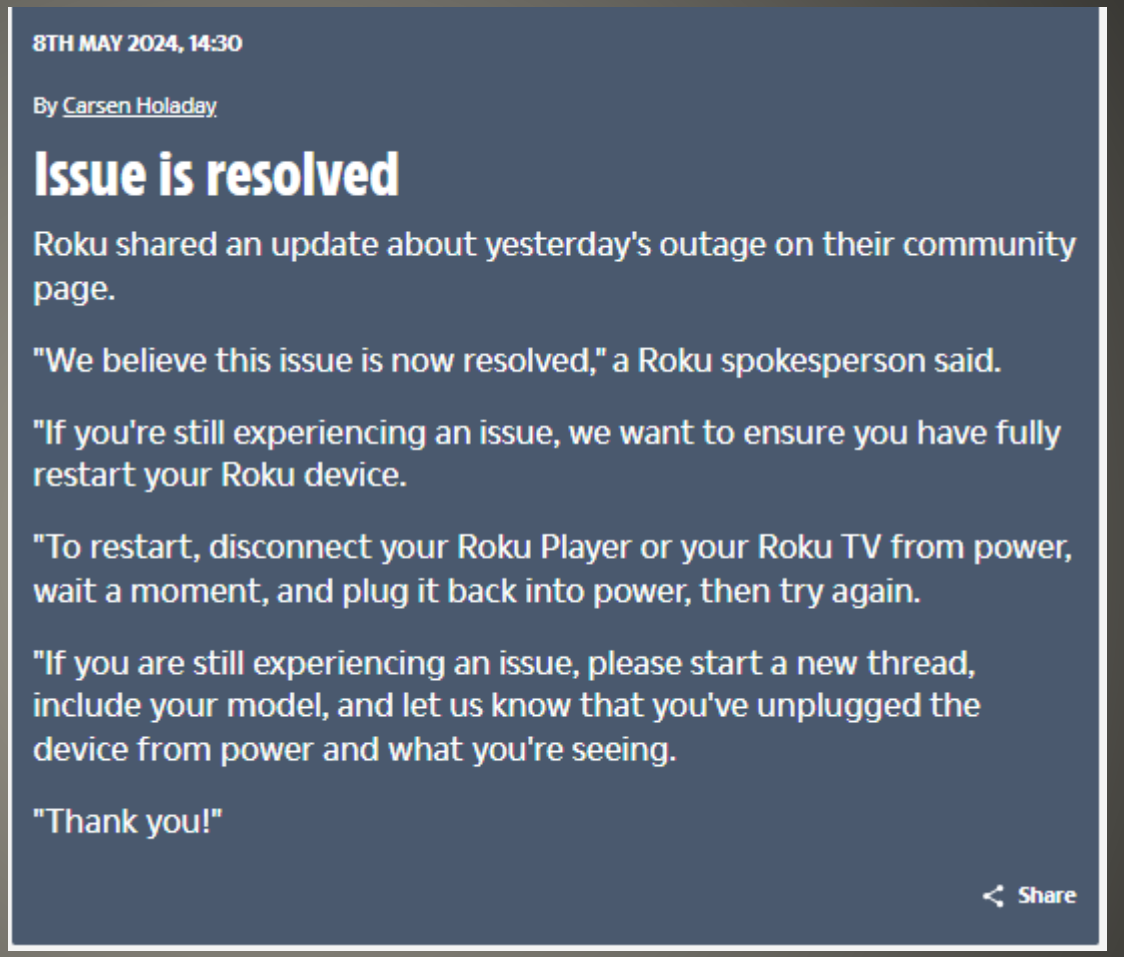
1d Like Reply

[redacted]
[redacted] there were a total of 3 of the same posts since last Tuesday.
Please check messenger for texts/messages that I sent to you in regards to my thinking this was a scam.

1d Like Reply

Netflix Certain titles Locked

- Roku down



8TH MAY 2024, 14:30

By Carsen Holaday

Issue is resolved

Roku shared an update about yesterday's outage on their community page.

"We believe this issue is now resolved," a Roku spokesperson said.

"If you're still experiencing an issue, we want to ensure you have fully restart your Roku device.

"To restart, disconnect your Roku Player or your Roku TV from power, wait a moment, and plug it back into power, then try again.

"If you are still experiencing an issue, please start a new thread, include your model, and let us know that you've unplugged the device from power and what you're seeing.

"Thank you!"

Share

Roku

8TH MAY 2024, 14:30

By Carsen Holaday

Issue is resolved

Roku shared an update about yesterday's outage on their community page.

"We believe this issue is now resolved," a Roku spokesperson said.

"If you're still experiencing an issue, we want to ensure you have fully restart your Roku device.

"To restart, disconnect your Roku Player or your Roku TV from power, wait a moment, and plug it back into power, then try again.

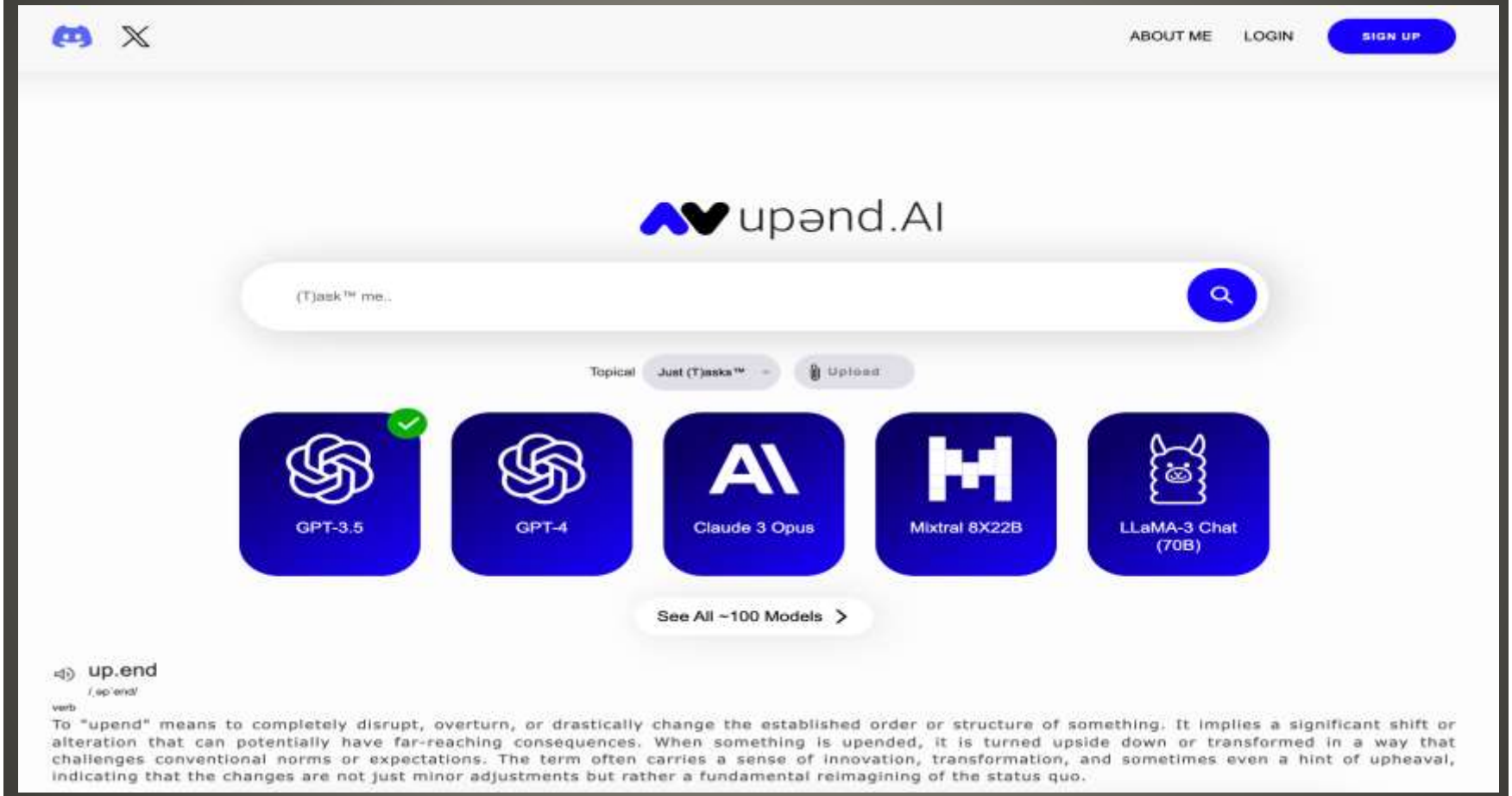
"If you are still experiencing an issue, please start a new thread, include your model, and let us know that you've unplugged the device from power and what you're seeing.

"Thank you!"

Share

Roku

- Gen AI Search



Upend

Current Issues

- LightSpeed Cache WordPress plugin
  - Create administrative accounts
  - Take control of websites
  - Email Subscribers WordPress plugin
- YubiKey 5.7 expanded passkey storage
  - More Complex PINs
- Visa using AI to combat enumeration attacks
  - $1B losses last year
  - Visa Account Attack Intelligence Score
- Contactless RFID smartphone cautions

Current Issues

- Beaconing Apps
  iPhone & Android phone 100 Apps idle 5 days
  iPhone 3,308 Android 2,323 per day
  yeahbut iPhone -> Apple 60% Android -> Google 24%
  iPhone Facebook 20 times/day Android Facebook 200 /day
  iPhone TikTok 36 Android TikTok 800
- WiFi blocking – Mirrors
- 6G 100 Gbps 300 feet
- Proton Mail end-to-end encryption yeahbut
  IP Address, payment information, alternate addresses, MFA
  ~~Tracking IP Addresses~~
  Consider recovery method privacy
- US Patent and Trademark Office
  IT configuration mistake

Current Issues

- Europe's most wanted hacker
  13 years old – 11 years later
  6 years and 3 month prison sentence
  Extortion patient data
- Ultra-wideband

WhatsApp

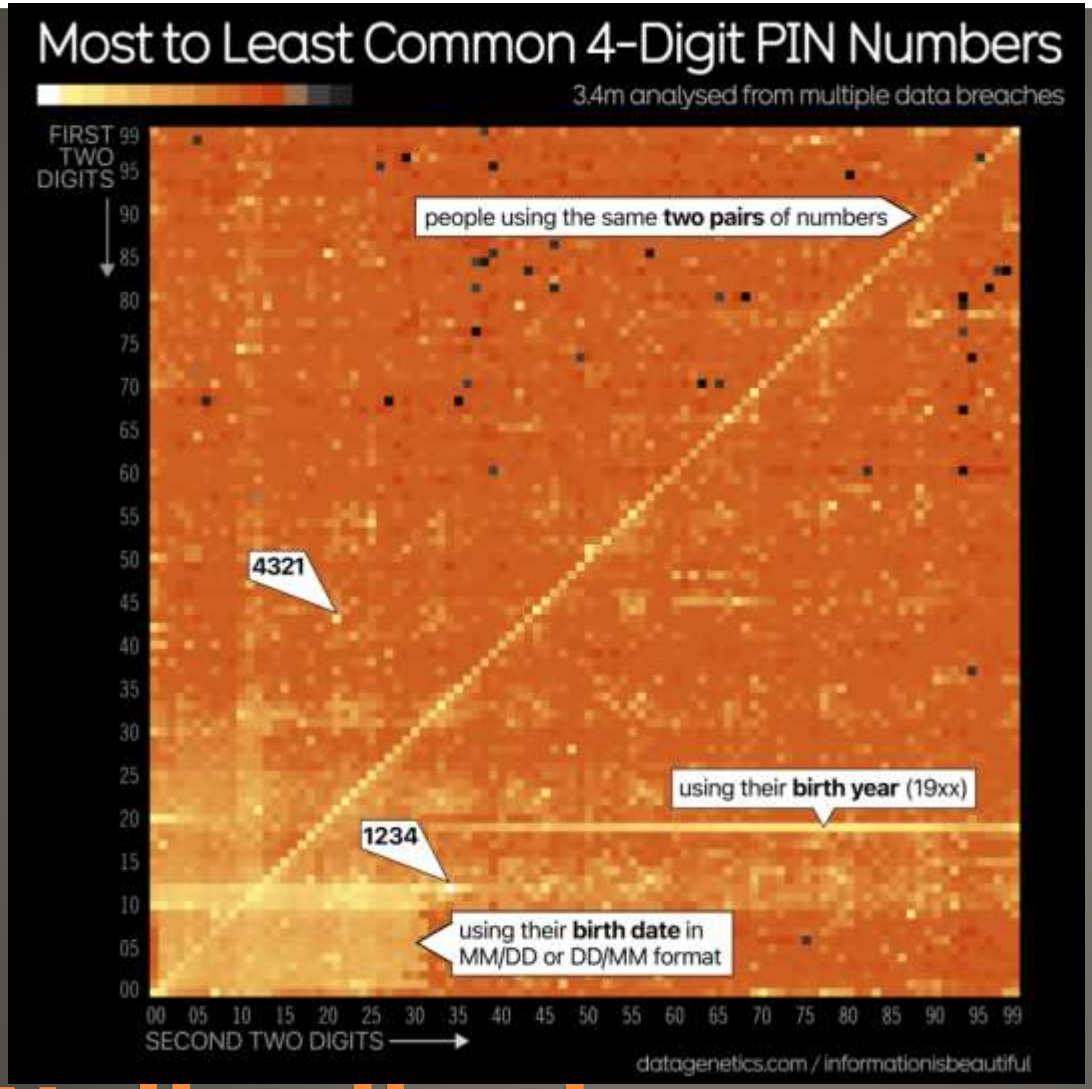
- 2 Billion active users
- Want to know where they are?
- Without them sending their location to you?

==========

- Access WhatsApp Web on PC
- Initiate a chat with them
- CMD or Terminal
- **netstat –an**
- Find the IP of them
- https://www.ipinfo.io
- Ethics?
- VPN?

Smart TV Settings
Android, webOS, other

- Motion smoothing – motion interpolation or similar
  Smart TV 60 frames/sec 24 FPS movies 30 FPS TV
  Artificially crafted frames added Adjust to suit
- Brightness, Color Contrast, Sharpness Adjust to suit
  Ambient light sensor
- Sound Bass, Treble
  Sound Bar ***Audio Return Channel***
- Game Mode Lower latency
- Screensavers & Screen dimming
  OLED screen retention QLED
- Power management
- Auto Updates



PIN distribution

VPN Attack

- TunnelVision
- NOT Linux or Android
- 2002?
- DHCP option 121
- Connection to hostile network
- Kill Switch

VPN protections NOT

- Social Media
- Phishing
- Malware
- Tracking cookies
- Online accounts digital trail

- Kill Switch?
  Connection drop, VPN kill
  Application level
  System level

Current Issues

- ZeroEyes AI detect visible firearms near real time
- Black Basta ransomware gang
  Ransomware-as-a-service
  Joint advisory
  12 of 16 critical infrastructure sectors
  Double-extorsion model encrypting exfiltrating
  Victims unique code to .onion URL
  Diversification adaptability
- China & US AI meeting in Geneva
- ChatGPT-4o (Omni) Face Inflections Emotions

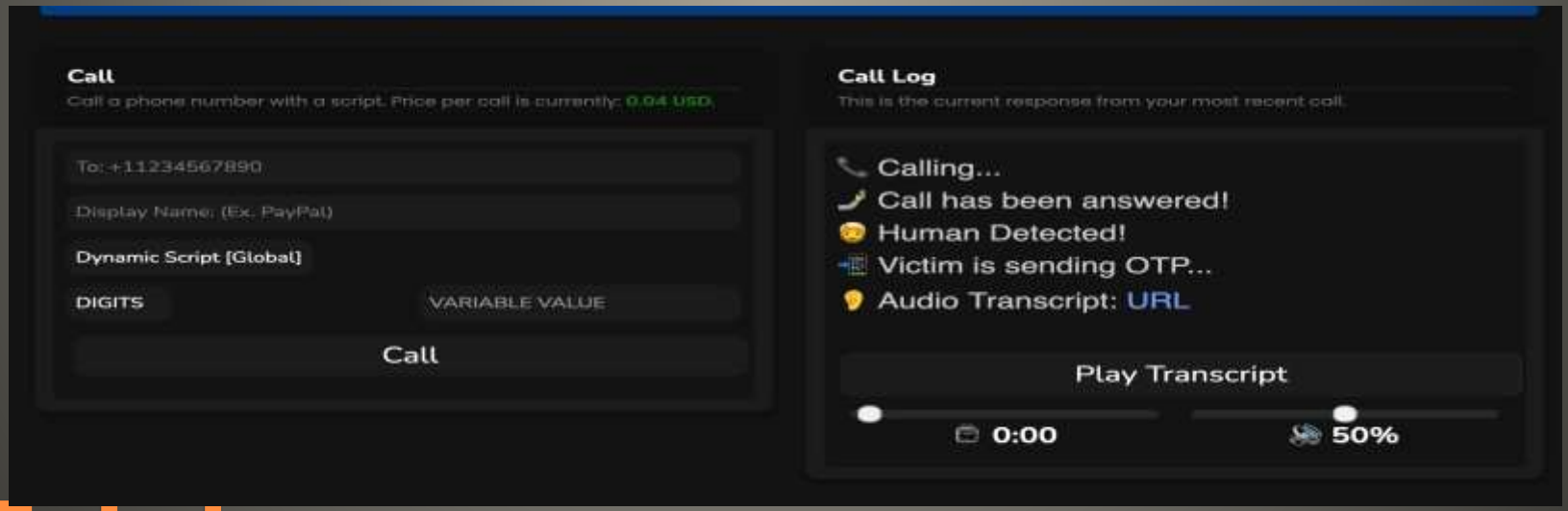
https://youtu.be/kO9Jge1z7OU Daily Show May 14, 2024

- LockBit Wichita data – sold?
- eLORAN GPS alternative "wake-up"?

Google I/O

- Project Astra
  AI Agent for everyday life
  Multi-model & long-context
- Google Photos Gemini AI assist
  Ask Photos
- NotebookLM
  Help with homework
  Learning guide, quizzes, FAQ, summarize Math
  Podcast audio
- Search video Astra for recorded video
- Veo generative video Sora competitor
- Gemini on Android Gemini Nano SPAM detection?
- Google Workspace
  Chip G-chat
  Mail – summarize conversations
  Meet – meeting highlights
  Sheets – pull specific dataset
- https://youtu.be/MzHCWZB5ZpE?t=16
- Gemini to GoogleTV suggestions, summaries, translations
- Chrome
- SynthID for watermarking
- Android

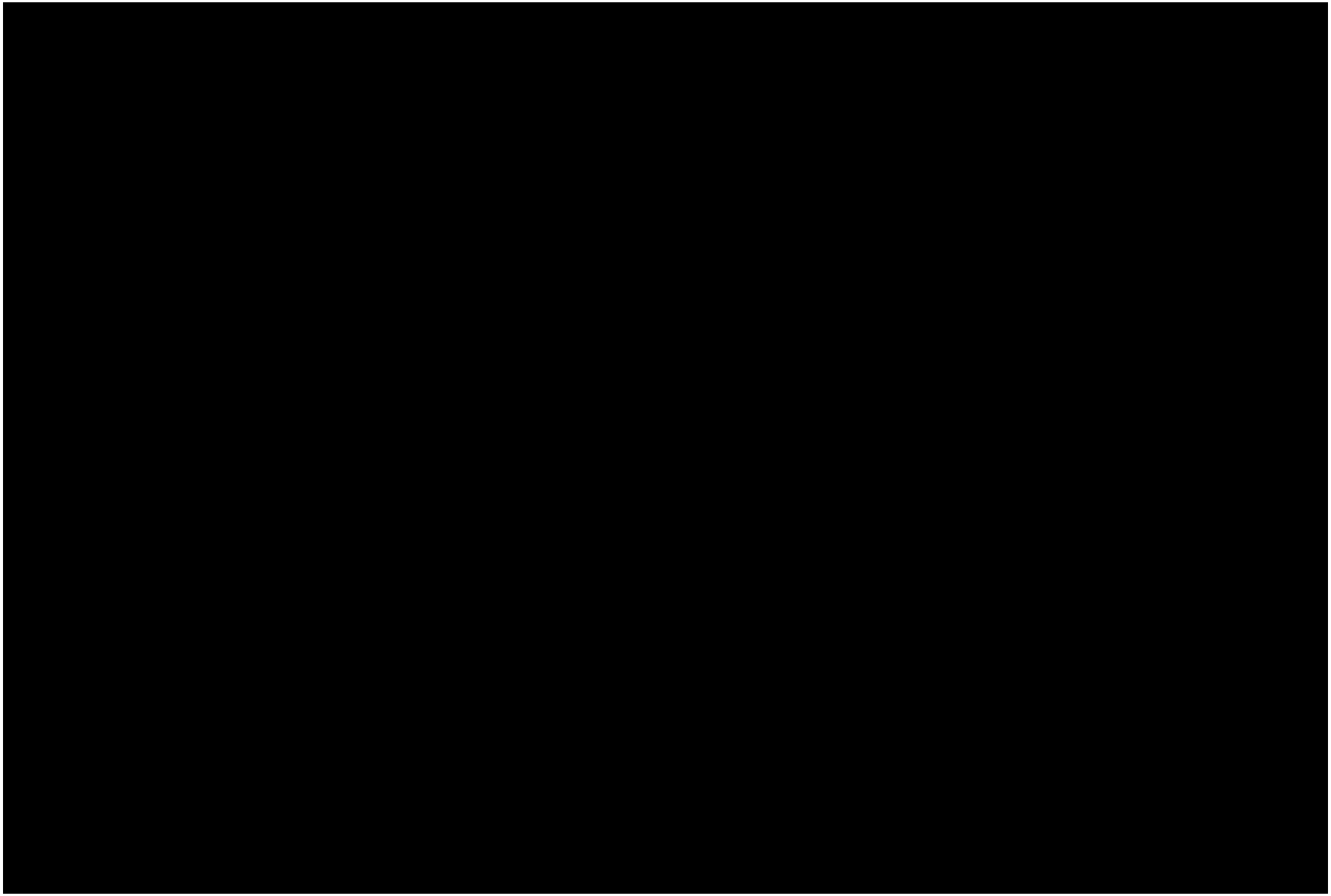
- Interception operation 2024
- One-time codes
- Phone, email, authenticator apps
- Back-end database exposed
- Stress-test resilience
- Customizations
- Referral code no logs no PII for service



Estate

Current Issues

- Android Theft Detection Lock
  AI-powered safety tool Android 15
  Detect suspicious app activities “sensitive permissions”



Android protections

- Prevent phone setup after factory reset
  Unless login details
- Private Spaces
- Disable “Find My” PIN, password, biometrics
- Lock stolen phone with phone number
  Stolen device trauma
- Live threat detection on phone
- Hide notifications & OTP when screen sharing
- Potential false cellular base station alert

- Extended Detection & Response (XDR)
- Security Information and Event Management (SIEM)
- Internet of Things SIG IoT Documentation
- False positives False negatives
- Signatures Heuristics
- Reverse Filter benign Investigate the rest

AI & Cyber Security

- 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