Sun City Computer Club

Cyber Security SIG
February 15, 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

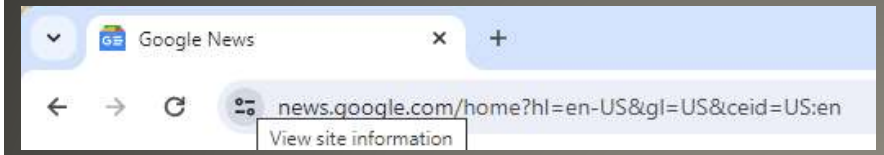
SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

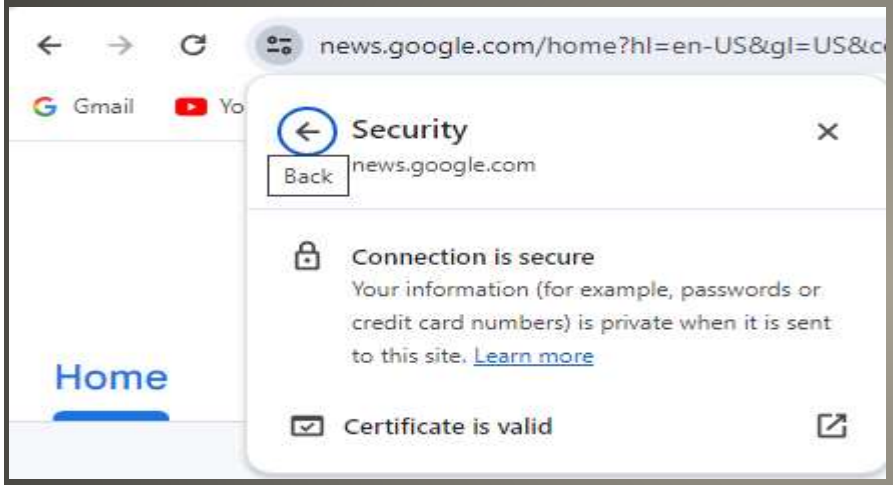
- John Jenkinson
- 1962 First computing job First hack
- 1964 Department of Defense contracts
- 1966 US Army
- 1971 BS Physics 1975 BS Math 1978 MS Computer Science
- 1974 Mostek
- 1983 -> 1016 Big Oil
- Cyber Security focus, training, certifications, consulting
- FBI InfraGard DHS Critical Infrastructure
- 5-time Senior University Instructor
- SIG leader Cyber Security, Windows, Mac (iDevices)
- Computer Club class Instructor 8 class topics
- Anti-Fraud group
-
- Mensa

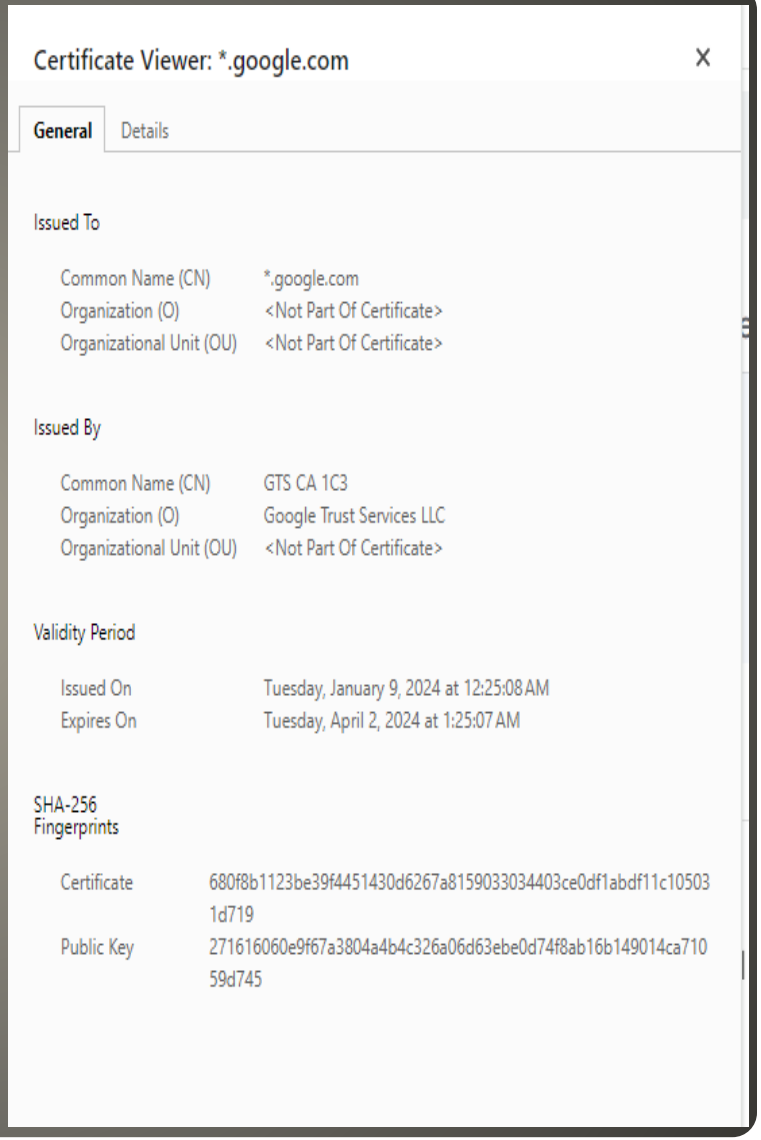
Vocabulary

- Safer not Safe
- e-postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio not wireless
- Identity fraud not Identity theft
- Attacker not hacker/cacker
- Account takeover

- "Look for lock icon"







Digital Certificate

- Windows 11
- 80 Vulnerabilities
- 5 critical
- 2 Actively exploited

Microsoft Patch Tuesday

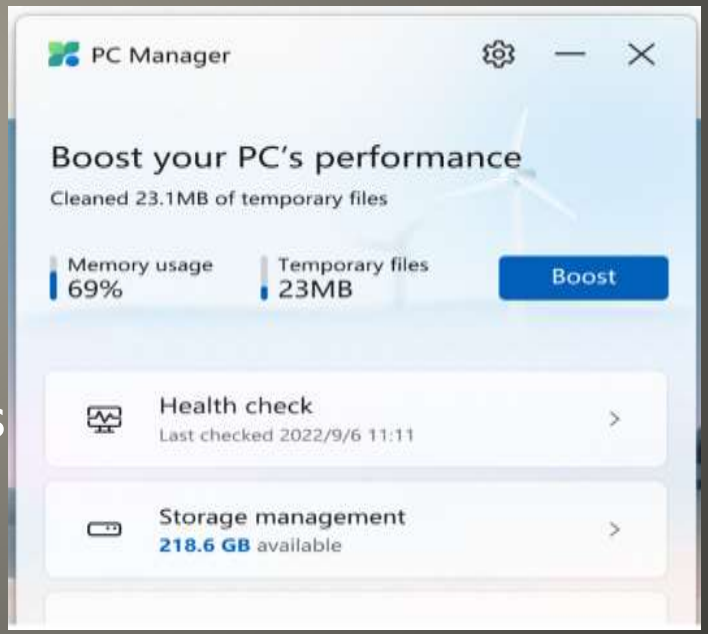
- CVE-2024-21412
- Bypass security checks
- Shortcut within shortcut
- Mark-of-the-web

Windows Defender SmartScreen

Microsoft PC Manager

- Microsoft App Store
- Storage Manager
- Health Checkup
- Pop-up management
- Windows Update
- Startup Apps
- Browser protections
- Process Management
- Anti-virus

- Cleans Prefetch folder
- Toolbox references external tools



Deepfake

- Digitally created video conference
- CFO & other company officers
- Images & voices

- “Move your heads”
- Alert system – linked to known scams

9:41

NortOn™ 12/29/23
To: arribodatest@icloud.com >

Re: Your subscription has ended. You are now responsible for your own, security

all_Your Devices At-Risk

All your Devices will Attacked by the Malwares please try

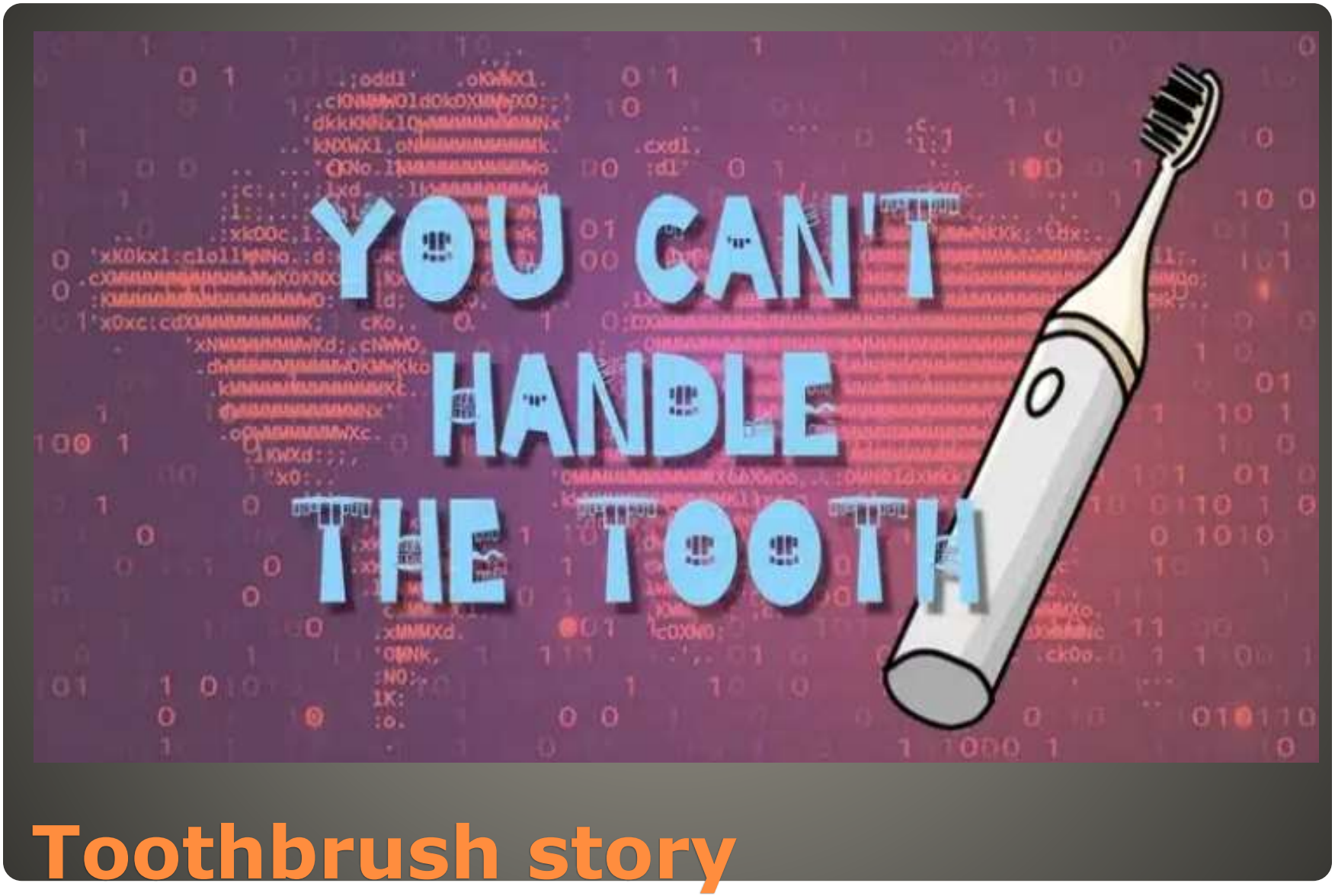
REPORT

- Please
- Report
- ReportFraud.ftc.gov
- Report to carrier
- Report to Anti-Fraud Group

Sun City Texas Community Association Community Association Anti-Fraud

Current Issues

- AnyDesk hacked
  Source code Private code signing keys
  AnyDesk customers
- India's Paytm Payments Bank
  Hundreds of thousands accounts setup without proper identification
- Cloudflare internal wiki and bug database
  Using credentials from Okta hack
- Attackers targeting tax prep pros
- HPE data for sale
- Vision Pro drivers in Tesla autopilot
- Identity hijacking
- Satoshi Nakamoto trial
- Three million smart toothbrushes DDoS attack
- CISA & MS-ISAC advisory Actor using former employee account



Toothbrush story

Fortinet clarification

- “To clarify, the topic of toothbrushes being used for DDoS attacks was presented during an interview as an illustration of a given type of attack, and it is not based on research from Fortinet or FortiGuard Labs. It appears that due to translations the narrative on this topic has been stretched to the point where hypothetical and actual scenarios are blurred.”

Fortinet Inc

NASDAQ: FTNT

Overview | Financials | Compare

Market Summary > Fortinet Inc

69.17 USD

+4.36 (6.73%) ↑ past 5 days

7 Feb, 10:30 GMT-5 • Disclaimer

+ Follow

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max

Open	73.83	Mkt cap	53.19B	52-wk high	81.24
High	73.91	P/E ratio	47.50	52-wk low	44.12
Low	68.40	Div yield	-		

Commercial Spyware Vendors

- 80% of 0-day vulnerabilities
  40 commercial vendors
- N-days
- Increased development cycles

- Bitlocker disk encryption
- Laptops
- External TPM
- Raspberry Pi

Bitlocker encryption

Mozilla Monitor Plus

- Firefox Monitor -> Mozilla Monitor -> Mozilla Monitor Plus
- Paid service $13.99/mo $107.88/year
- Provide
  First & last name, current city & state, DoB, email address

SO, your PII and money

City & State
Georgetown KY, GA, DE, IN no TX
Sun City AZ, FL, KS on TX

Takes some time
CHECK WEB Certificate

Enter the details you want to protect

We'll use this to find exposures of your personal information, and then guide you step-by-step on how to fix it.
Why do we need this info?

First name*

Frank

Last name*

Smith

Date of birth*

11 / 24 / 1988

City and state*

San Francisco, CA, USA

Go back

Find exposures

- Pattern repetition
- Top-left
- Screen smudges
- Fewer pattern combinations 400,000
  6-digit PIN 1,000,000
- Shoulder surfing

Screen Pattern unlock issues

- Real-time bidding
- Third-party cookie deprecation

  UK Competition and Markets Authority

Chrome Privacy Sandbox

Current Issues

- Android TV Tools

Sideload apps.

Uninstall or disable apps, and remove bloatware.

Send and receive files.

Remove ads.

Replace stock Android TV launcher with alternative launchers such as Projectivy Launcher, Flauncher.

Replace YouTube TV with alternates such as SmartTube.

Install alternative app stores such as Aurora Store.

Take screenshots and screen recordings.

- Meta AI

  We have more data than ChatGPT

  Better data

  Unincumbered data

  And we are going to use it for AI training

Pig-Butchering

- NBC News Pig Butchering report

With ‘pig butchering’ scams on the rise, FBI moves to stop the bleeding (nbcnews.com)

- Bloomberg

Flipper Zero

- Canada to ban?
- National Summit on Combating Auto Theft

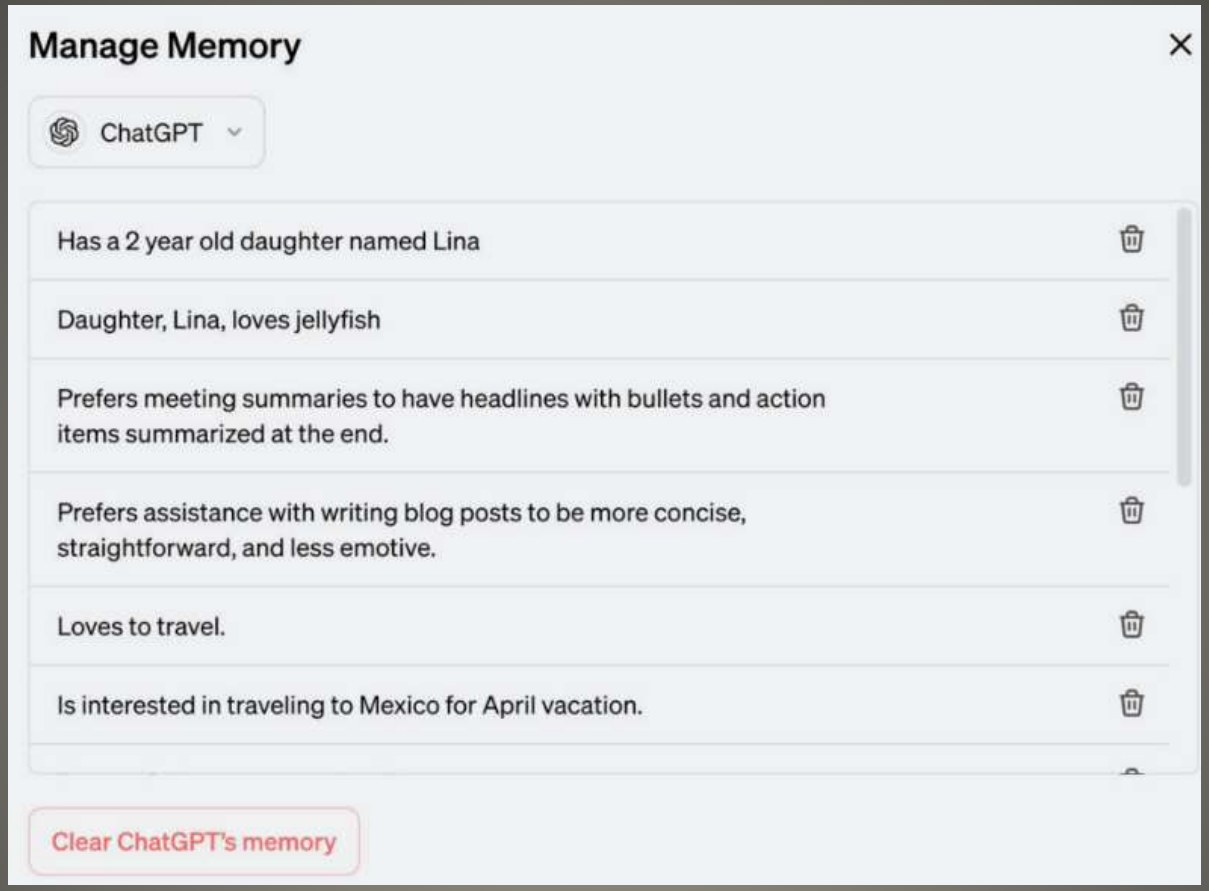
- Sub-GHz Infrared RFID NFC Button
- Add on modules
- Firmware updates/replacements

AI & vision

- Vision Pro
- AI identify animals, plants, etc.
  Guide you back to that sighting
- Digital night vision – full color
- AI binoculars
  9000 birds identification
- Smart telescope
  Position, magnification, tracking
- Tap on map, get scope focus
- LiDAR generated 3-D map
- Thermal with AI
  Bug identification

- Do not use an account
- Limit personal information
- No 2FA
- No 2-step authentication
- Monitor chat history
- Disable long-term memory

ChatGPT Account safety



ChatGPT Long Term Memory

- "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider"
- Title 47 Communications Decency Act 1996
- Title V telecommunications Act 1996

Section 230 – 26 words

Mispadu

- Infostealer
- 90,000 banking credentials
- CVE-2023-36025 severity 8.8
- Bypass SmartScreen
- Patched November 2023

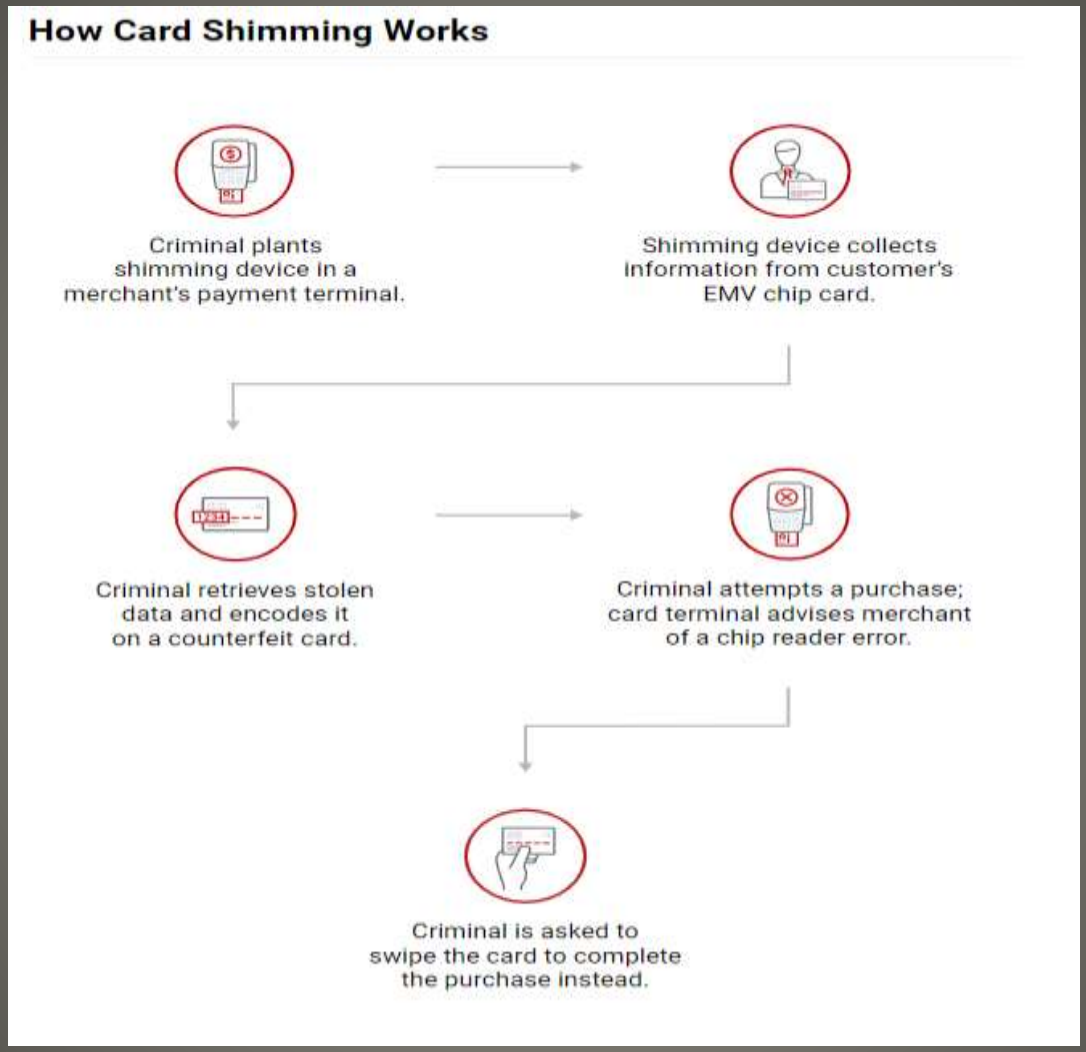
- Thinner
- Easier to hide
- Placed inside ATM
- Takes a minute to install
- Camera to capture PIN entry on keypad
- Harder for banks and consumers to detect

Super Shimmers

Super Shimmers

- EMV cards
- Not skimming - shimming
- Internal not external – very thin
- Delay Information from chip stolen
- Transmitted via radio to attacker
- Placed on mag stripe card
- Chip cloning difficult CVV3
- 700% increase

- NFC
- Mobile wallet
- NFC protections – special wallets, metal shields
- Yeahbut Take it out of shield to use



Super Shimmers

Credit/Debit cards

- Embossed
  Crayon
- Magnetic Strip
  Duplicate Device
- Chip
  Shimmer
- NFC
  Bump stand-in-line Foil lined wallet/purse
- Wallet app
  Stolen smartphone
- Banking app
  Banking Trojan

Misuse of Commercial Spyware

- Spyware Helpful <-> Harmful
- US State Department

  Executive order prohibit US government use of spyware

  Commerce Department lists of commercial spyware abusers

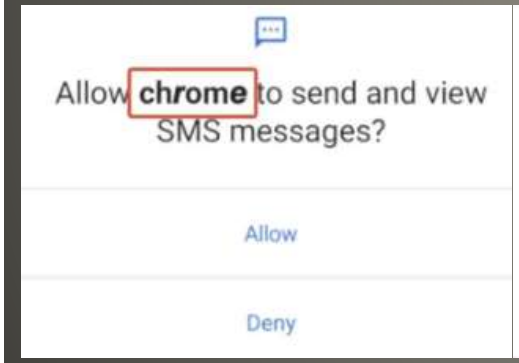
  Diplomacy to boost international cooperation

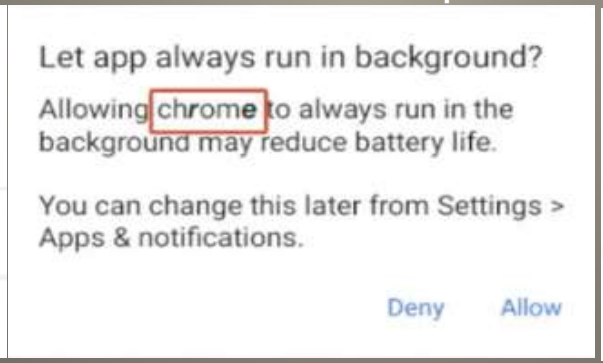
  Visa restrictions on individuals

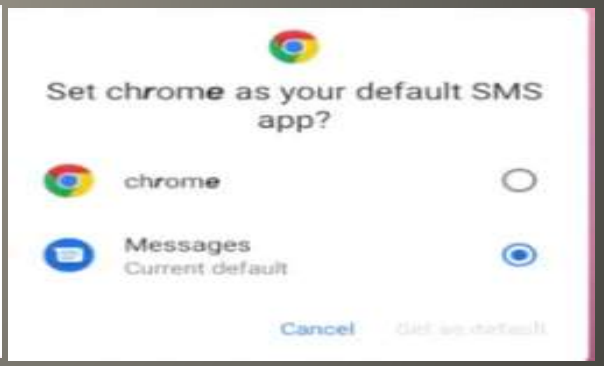
Current Issues

- AceMagic Mini PCs shipped with malware
  Many brands Same product
  Bladabindi & Redline info stealers
  Windows recovery
  c:\Windows\OsVer
  LED control software
- LastPass app found then deleted from Apple App store
- Linux security flaw in shim
- Google & Yahoo email policy changes
  Bulk emailers
  Authentication, unsubscribe options, Spam complaint rates
- Financial Crimes Enforcement Network Treasury Department
  Corporate Transparency Act
  Small business impact
- California resident $2.5 million Security flaw Apple "Thank you"

- Apple MGIE AI image editor
  MLLM-Guided Image Editing
  Photoshop style modification, global photo optimization, local editing
- Beijing Institute for General Artificial Intelligence
  Tong Tong Redefine human interaction with AI
  Learn autonomously and engage emotionally with humans
- OpenAI Computer control
- XLoader Android malware (MACs also)
  Shortened link 0 click Chrome impersonator







Avoid sideloading, shortened links, …

Current Issues

Current Issues

- Shadow AI
- Leonardo *universal upscaler*
- Rust based backdoor RustDoor
  macOS Intel & Arm
  Update to Microsoft Visual Studio
- Overdrive USB
  Activation mechanism insert 3 times
  Self destruct
- Parental controls
  Many varied platforms, settings, methods
  Parental understanding
- 240/4 IP address block block 240.0.0. -> 255.255.255.254
- Neural networks produce fake IDs $15 fool Know Your Customer KYC
- Verizon 63,000 Verizon employee's data
- U.S. *Liability Regimes* for security bugs
- FTC banned AI generated robocalls
- Tap to Pay Credit Card warning

Current Issues

- Android battery saver mode
  Screen refresh rate 10Hz – 240Hz
  Good scrolling, games, videos
- Google warning
  Gemini & confidential or personal information
  Chat is NOT a trusted friend!!
  Multi-billion-dollar ecosystem
  Advertising & data brokering
  Chats are stored => retrieved reviewed
  NOT end-to-end encrypted
- Russia Internet kill switch
  January 30 Sovereign Internet
- Facebook chirping sound
  It is not you, it is us – bug
  Settings & privacy > settings > Media > Sounds > In-App Sounds Off
- Supply chain – HP printer "call us" sheet Wait a week inboarding

- Android Safe Browsing
  Google Pixel Samsung Galaxy
  Security & privacy settings
- Apple Keyframer
  AI tool to animate still images

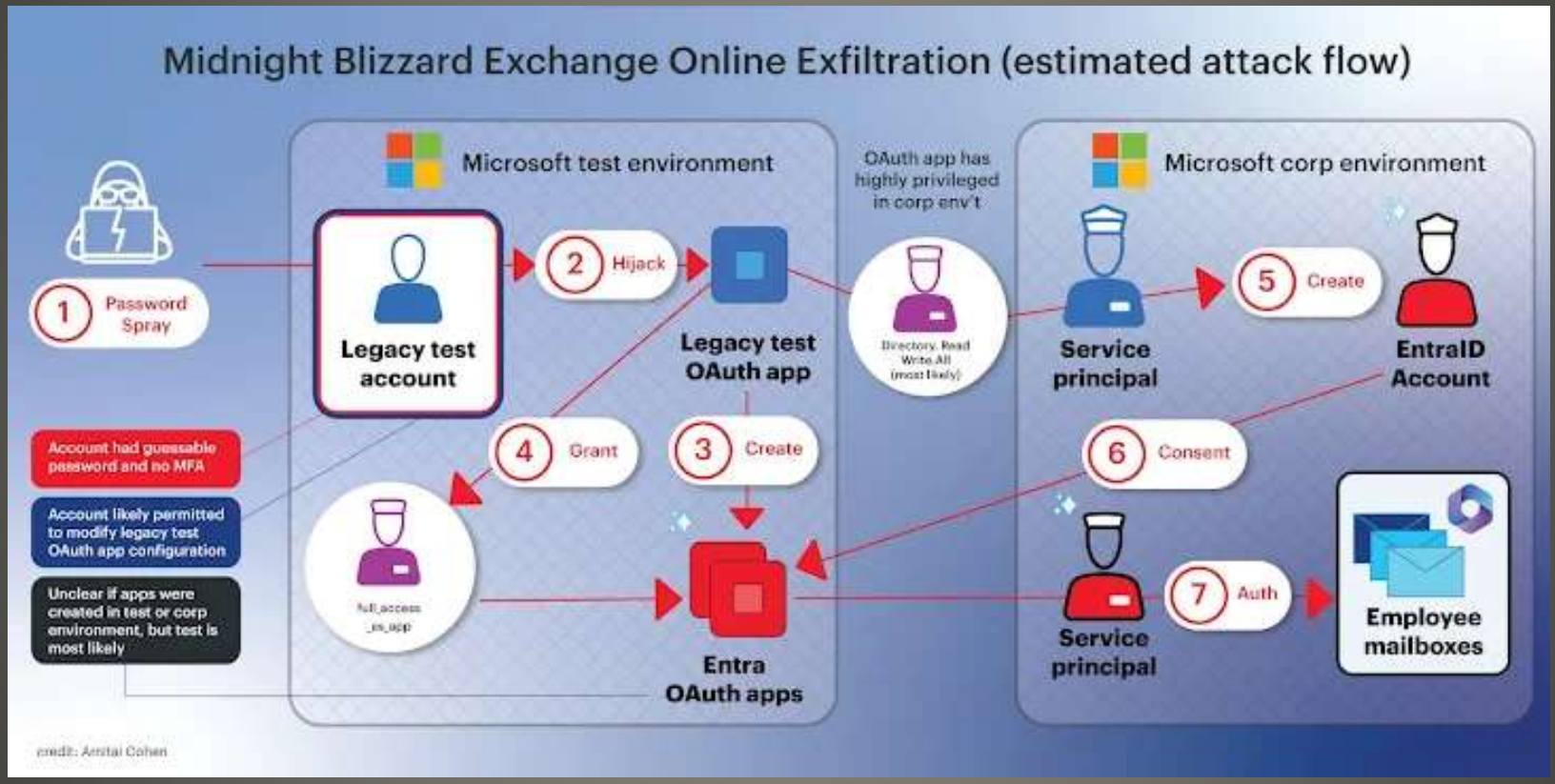
Fig. 8. Six frames taken from animations generated by EP4 (HCLA) and EP9 (HCHA). The Activity 1 Saturn animation from EP4 has the sparkles fade in and out independently, the clouds fade in, the halos fade in one after another, and the specks alternate colors from yellow to orange to pink. The Activity 2 Rocketship animation from EP9 has the rocketship move up and down, the clouds grow and shrink in size, and items in the background (the moon and specks) shift down to give the appearance of the rocketship lifting off.

Current Issues

Current Issues

- Wi-Fi jamming knock out security cameras
  Home burglaries
  Jamming is illegal Jammers are easily available
- Patent troll Bounty seekers prior art
- April 2024 new Gmail mass email rules
- Canada Trans-Northern Pipeline blackmail
  Critical infrastructure
  Lower Valley Energy December
  Spanish electricity provider SerCide
  Canada Rush Energy
  Remember Colonial Pipeline incident?
  China Volt Typhoon

- Microsoft Midnight Blizzard breach



Microsoft Midnight Blizzard

Current Issues

- Cloudflare-Atlassian Breach
  Thanksgiving day, 2023
  Credentials obtained Okta Oct 2023
- Bank of America Infosys McCamish Systems
  Name, address, SSN, DoB, account & credit card numbers
  Notification letter Attorney General Texas & Maine
  SaaS
  Banking Apps vs. Web
- Employees of Government Accountability Office
  CGI Federal data breach 6,600 employees
- Southern Water (UK) customer data stolen
- Zenlayer network services provider 290 data centers
  Unprotected database
- 23andMe DNA data mining financial recovery attempt

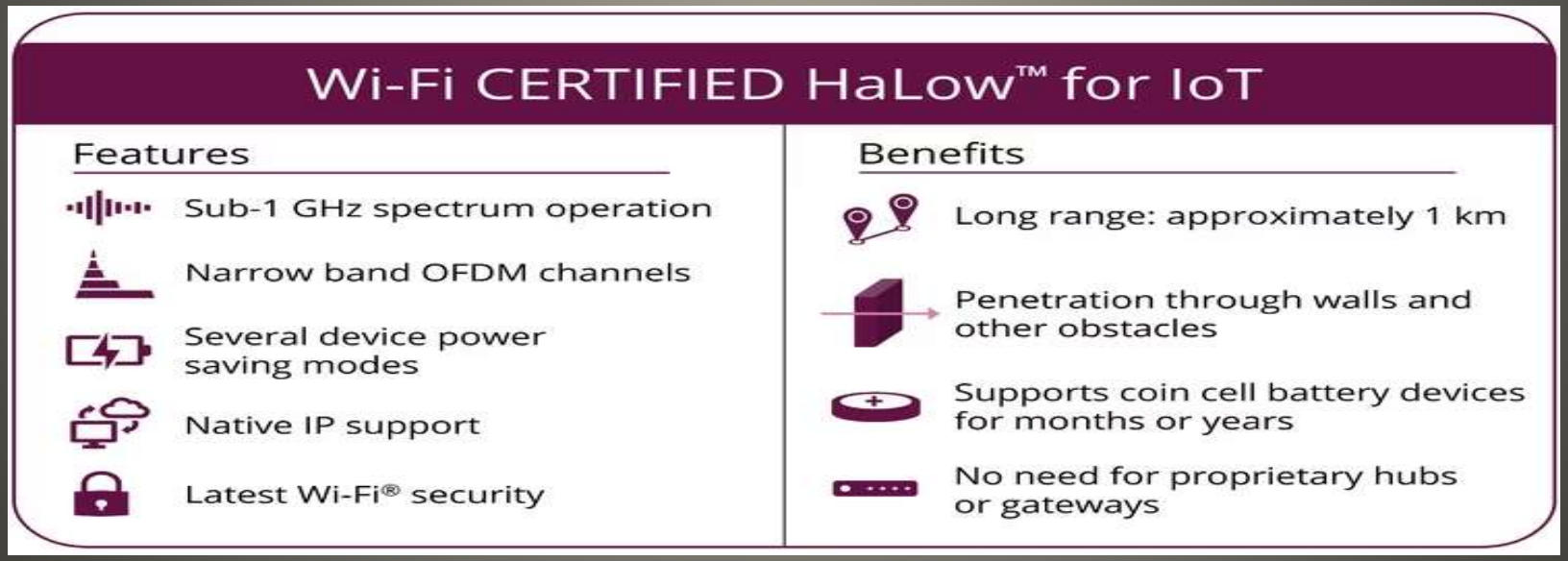
Current Issues

- Too Many Honeypots/Honeynets
- Reverse VPN alternative – Overlay networks
  Hamachi, Nebula, TailScale, ZeroTier
- Tax scams Owe IRS San Marcos city employees
- Microsoft OpenAI claim state-based actors
  China, Russia, Iran, North Korea using AI tools
  Hone skills, trick targets
  Microsoft & OpenAI block hackers in China, North Korea

  Syrian Electronic Army
- ChromeOS Flex - Stream Microsoft Apps via cloud
- Microsoft Outlook critical security vulnerability
  Bypass Office Protected View Preview pane
  Moniker Link
- Facebook Marketplace accounts - Dark Web
  No Comment from Metra

Wi-Fi HaLow

- 802.11 ah protocol
- Sub 1GHz
- Connects 8,000 devices
- 1 Kilometer range
- Narrower channels lower bandwidth 150 Kbps
- Z-Wave, Zigbee, Thread

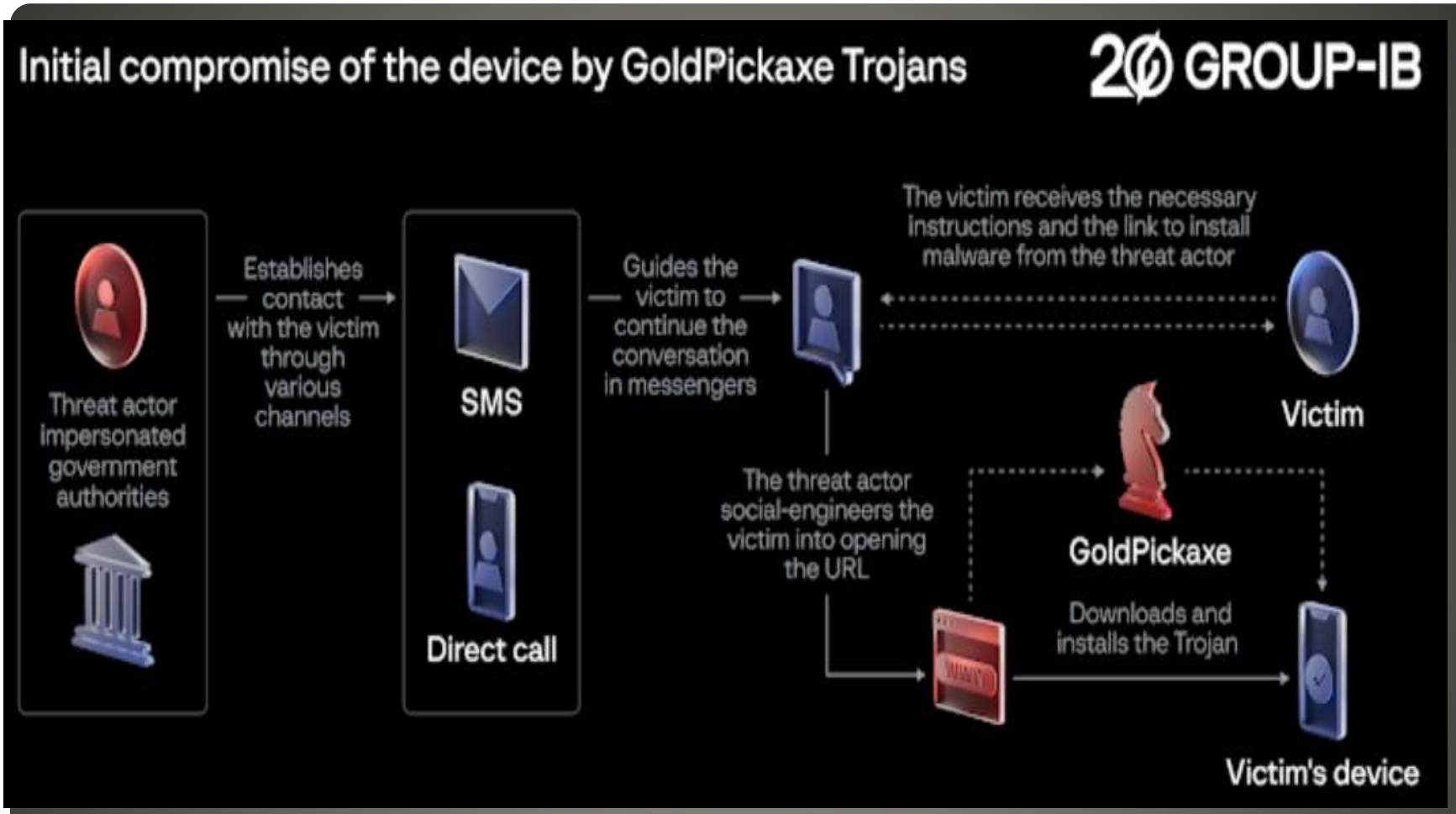


- Wildfire early warning system
  small solar powered device
  smoke detector
  hydrogen, co, and other components
  wireless alert & GPS
- Abuse reporting
  Korea 211 any number twice
  Location via GPS Live stream video alert authorities
  Poland
  Shopping page Add a specific product address to authorities
- Fog water collection
  Vertical sheet synthetic resin mesh
- Trash boom capture ocean bound plastic from rivers
- Sutures with beet juice to detect pH change from infection

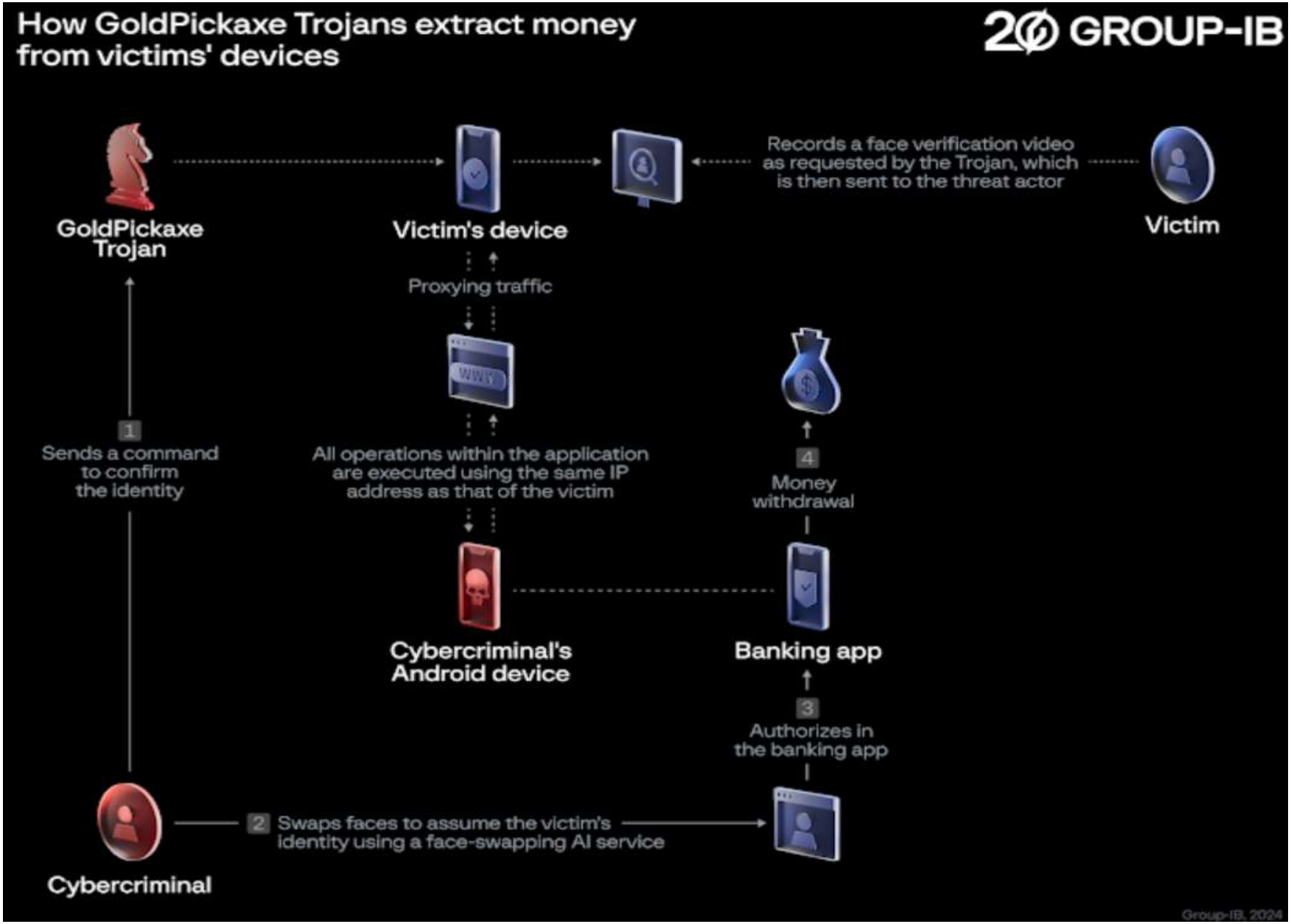
Reader's Digest

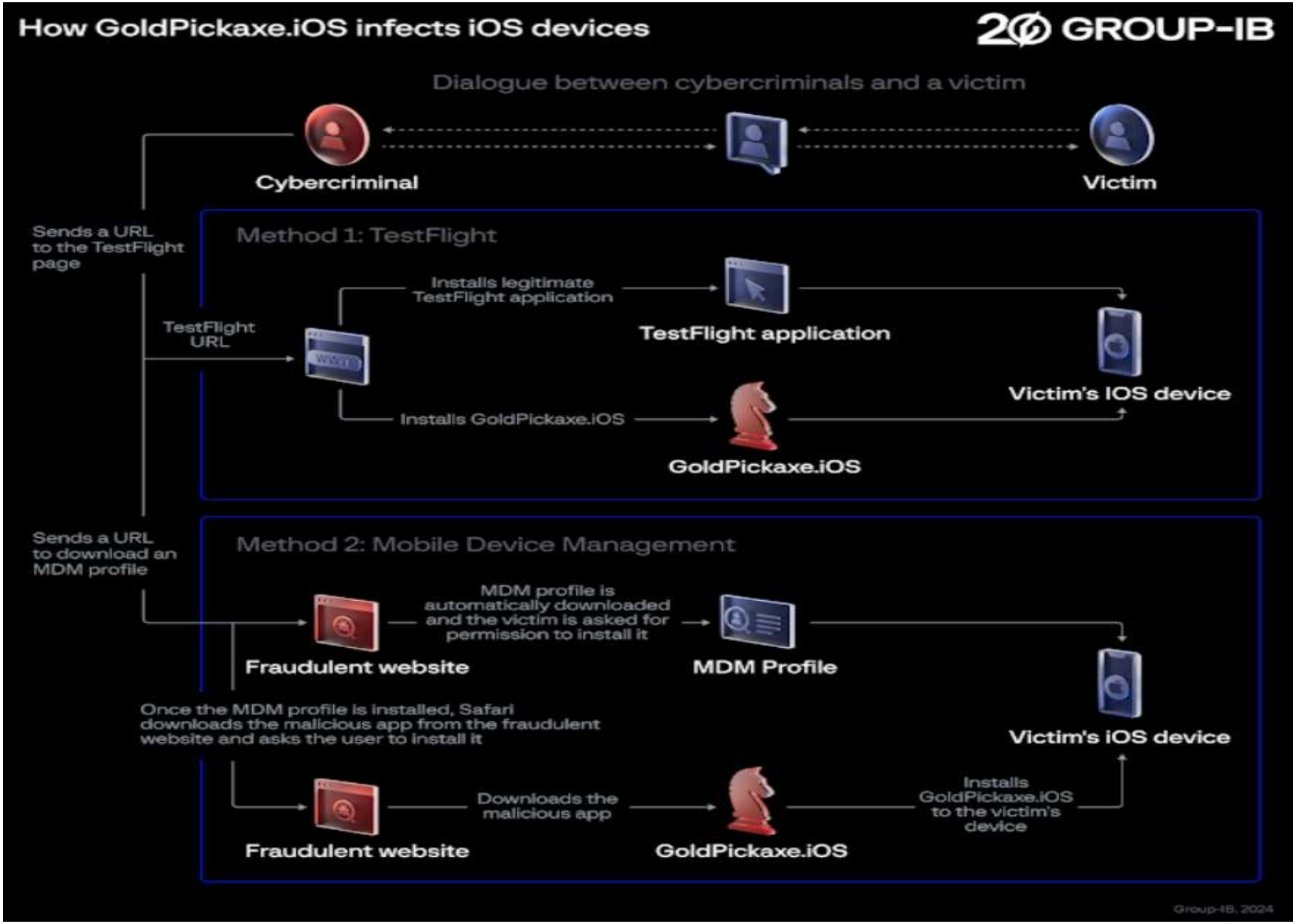
Current Issues

- US Department of Defense
  Letter to 20,000 employees
  Detected early 2023
  "inadvertently exposed" "service provider"
- IRS collection letters resuming after 2 years
  LT38
- Study on security debt – reported flaws over year old
- Tinder & Hinge sued addictive dating apps
- Russia nuclear space weapon
- Lucid-1 AI REM Sleep monitor lucid dreaming
  Generative ultrasonic transformer
- GoldPickaxe iOS & Android
  joins GoldDigger, GoldKefu, GoldDiggerPlus
  Apple TestFlight platform
  MDM profile – complete control
  Thailand large transactions require facial recognition
  GoldPickaxe records video -> face swapping AI
  Collect victim's documents, intercept SMS, use proxy



GoldPickaxe Trojans


How GoldPickaxe Trojans extract money from victims' devices
GROUP-IB
GoldPickaxe Trojan
Victim's device
Records a face verification video as requested by the Trojan, which is then sent to the threat actor
Victim
Proxying traffic
1
Sends a command to confirm the identity
All operations within the application are executed using the same IP address as that of the victim
4
Money withdrawal
Cybercriminal's Android device
Banking app
3
Authorizes in the banking app
2
Swaps faces to assume the victim's identity using a face-swapping AI service
Cybercriminal
Group-IB, 2024


How GoldPickaxe.iOS infects iOS devices
GROUP-IB
Dialogue between cybercriminals and a victim
Cybercriminal
Victim
Sends a URL to the TestFlight page
Method 1: TestFlight
Installs legitimate TestFlight application
TestFlight application
TestFlight URL
Victim's IOS device
Installs GoldPickaxe.iOS
GoldPickaxe.iOS
Sends a URL to download an MDM profile
Method 2: Mobile Device Management
MDM profile is automatically downloaded and the victim is asked for permission to install it
Fraudulent website
MDM Profile
Once the MDM profile is installed, Safari downloads the malicious app from the fraudulent website and asks the user to install it
Victim's iOS device
Downloads the malicious app
Installs GoldPickaxe.iOS to the victim's device
Fraudulent website
GoldPickaxe.iOS
Group-IB, 2024

- Android devices
- Google Assistant -> Gemini
- So, perhaps 2 Gemini apps

Oh My, Gemini

- You give, they take

Privacy Policy

Terms and Conditions

- Browser Extension
  Terms of Service: Didn’t Read
  Read Terms of Service of
  Terms of Service: Didn’t Read

Description

Get information instantly about websites' terms of service and privacy policies, with ratings and summaries from the www.tosdr.org.

Recent attempts:

Back-to-back changes

Agree to not litigate

Now, use AI to summarize and analyse ToS

- NRO Anti-Fraud Group
- Williamson County Deputy Sheriff
  Report Fraud
- Work-from-home scams
- NRO Anti-Fraud Group
- Scams and Computer Safety SIG

- For the good of our community
  Report scams

Sun City NRO Bulletin Jan 17, 2024

Know Your Customer

- Recent Scans and Computer Safety SIG
- Social media account reclaim
- Picture of person holding Drivers License
- KYC efforts
- Government issued ID
- NOT A PICTURE OF Picture with
- Other:

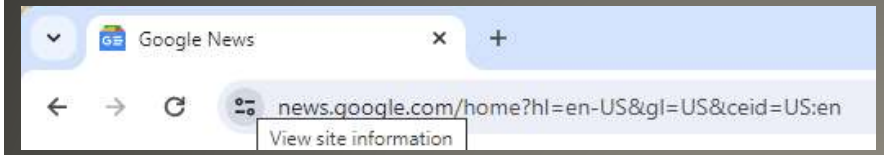
  print the OTP, picture of you holding it

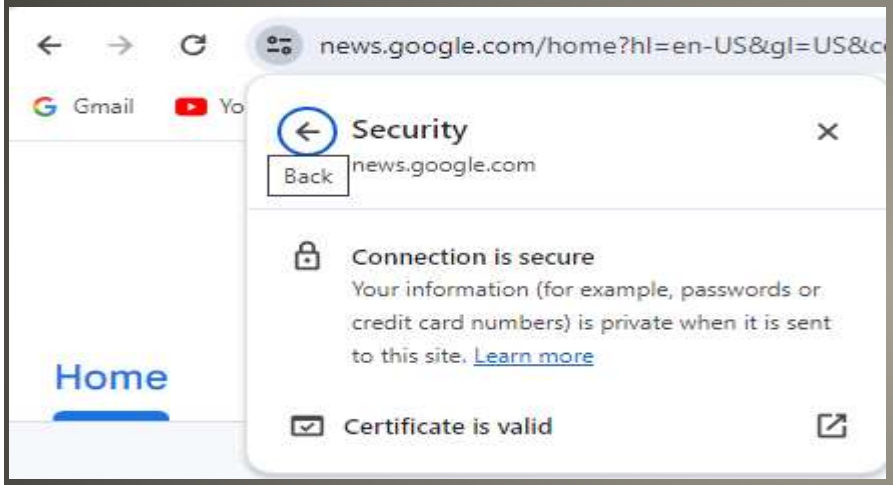
  Today's date & time

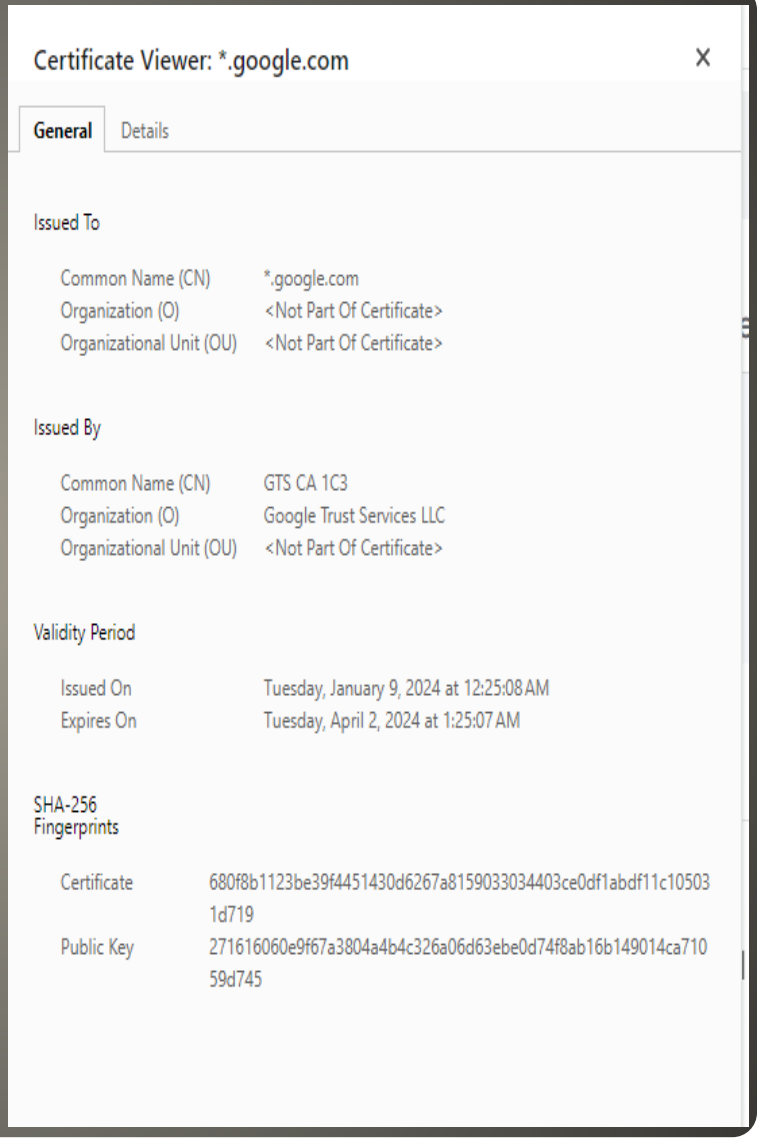
- FaceID
- “Hey, you”
- Only answer if in Contacts
  Someone in your contacts has had their phone stolen

iOS Stolen Device Protection

- "Look for lock icon"







Digital Certificate

- 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