Sun City Computer Club

Cyber Security SIG
March 7, 2024

Questions, Comments, Suggestions welcomed at any time

Even Now

- Most of our wealth, information, knowledge is digital
- Most of that is available planet wide
- To access requires digital
- Computers, cell phones, Internet are digital
- Humans need digital to understand / use digital
- AI is digital
  Awareness
      Preparedness
          Understanding

- Back to today's presentation

Aside

- [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

Cyber Security News Archive

WEB encryption ePostcard NOT

- 570 files posted to GitHub
- I-Soon private security contractor
  China Ministry of Public Security
- 20 targets Countries & telecommunications firms
- AI helping with analysis
- I-Soon@proton.me January GitHub February
- Embarrass company?

Chinese hacking documents leaked

- Rabbit R1

- Smart Glasses

- Humane Ai Pin

- Samsung Galaxy S24

- Prophetic Halo

AI hardware

- New plugins
  Kayak, Shopify, OpenTable, …
- New skills
  Show device info, Empty Recycle, …
- Outlook

Copilot AI

- Actor obtained access to US government agency
  Using credentials of former employee
  VPN, LDAP, etc. Former employee was IT administrator
  Credentials used were stolen in another data breach
- FBI disrupts GRU-led hacking group
  Use of thousands of home and small business routers
- OpenAI Sora   realistic videos from text prompts
  How does it work? Protected technology
  Removing static noise until video is produced
  spacetime patches > latent space > pixel decoder
- New York magazine financial columnist scammed
  $50,000 in shoe box handed to stranger
- MMS technique to fingerprint smart devices
- ChromeOS with AI

Current Issues

- Camera transmission cables leak images
- Chrome Private Network Access protections
  External site direct to internal site
  Preflight request
  Access-Control-Request-Private-Network header
- Google Chrome with Gemini option soon
- Android Safe Browsing Android phones   soon
- Wyze cameras

"We have now identified a security issue where some users were able to see thumbnails of cameras that were not their own in the Events tab."
   13,000 thumbnails exposed   1,504 clicked on thumbnails

- FBI takes control of Moobot impacted routers
  Unsecured Admin passwords
- FTC fraud & scams $10B reported
- 28,500 exchange servers vulnerable Internet exposed

Current Issues

- Guilty verdict
  Thousands counterfeit iPhones for repair authentic iPhones in return
- Android 15 Hide 2FA from other apps
- US Executive order Protect US coast   Chinese manufactured ship-to-shore cranes
- US Executive order restrict data brokers selling American data to "countries of concern" China, Russia, Iran, North Korea, Cuba
- Commerce Department open investigation
  foreign-made software in cars
- Reddit getting $60Million to train AI on Reddit posts
     Also, Tumblr, WordPress
  Legal way to counter copyright suits?
- Wi-Fi vulnerability fixes underway Linux, ChromeOS   Android
- Proton Pass available as Windows app   macOS & Linux this year
- SmartPhone sensors
  Motion, Location, Environment
  Accelerometer, Gyroscope, GPS, LiDAR, Ultrasonic, Hall Effect, Barometer, temperature, ambient light, proximity, magnetometer, heart rate

Current Issues

- Poland's new PM
  "Previous PM used Pegasus spyware"
- Variston spyware company shutting down
- US cyber attack Iranian ship
  disrupt ability to share info with Houthis
- Data broker tracked and sold location data
  Visitors of Planned Parenthood clinics
- Finger Friction Sounds
  Before Contact prints, Finger detail photos
  Now Finger swiping friction sounds
- Groq New Gen-AI Language Processing Unit
  Answers: instant, factual, cited, hundreds of words
- Albedo Space low-orbit satellites zoom in individuals
  "we are acutely aware of the privacy implications and potential for abuse/misuse."
- HP "rent-a-printer"

Current Issues

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

Windows Malicious Software Removal Tool x64 - v5.121 (KB890830)	Downloading - 96%
2024-02 Cumulative Update for Windows 11 Version 23H2 for x64-based Systems (KB5034765)	Downloading - 0%
2024-02 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 23H2 for x64 (KB5034467)	Downloading - 0%
2024-02 .NET 6.0.27 Security Update for x64 Client (KB5035119)	Downloading - 0%

Microsoft Patch Tuesday

- Signal to support Usernames ephemeral usernames
  Protecting cell phone numbers
- *Virtually Unhackable* chip
  Light & silicon for math manipulations
  Speeds and energy saving
  Vector-matrix multiplication
  no requirements to store information in memory
- AI & fusion
  'Avoiding fusion plasma tearing instability with deep reinforcement learning'
- Xmail to replace Gmail – NOT
- AT&T outage reason - Impact
- Meta outage   Instagram outage   DNS <-> IP address
- LastPass outage this morning
- ConnectWise ScreenConnect product vulnerability
- Avast jumpshot shutdown FTC imposes $16.5M fine
  2014 – 2020 sold to 100 companies Ars Technica story

Current Issues

- UnitedHealth cyber attack – IT systems disconnected
  Attacker's statement removed
  $22M payment
  Blackcat / ALPHV   exit scam?
- Change Healthcare   1-in-3 American
  digital clearinghouse
- Pharmacies struggle with cyber attacks
  including all US military
- Logjam in administrative functions
- US Department of Health and Human Services
  request to waive prior authorizations
  accept paper bills
- DOJ suit to stop UnitedHealth acquisition of Change
  50% of ALL claims
  Remember Colonial Pipeline?   Small but vital

Healthcare

- Empire Transfer

  extract cookies Safari & Chrome

  extract contacts

  passwords from password managers, crypto keys, cc info,

- 21 new malware families
- Empire well known record label

EMPIRE Secure File Transfer

Right Click File
<— Then Click Open

Click Ok/ Yes on any following
popups to securely open the
document!

macOS malware

0
/ 60

Community Score

⌖ Follow   ⟳ Reanalyze   ↧ Download ▾   ⇆ Similar ▾   More ▾

a7cdc1565197a7bc7bfc5c14ab2de4db3617007681faf93661b95Odc0bf3a2b5

Empire Transfer 12.3.23.dmg

`dmg` `checks-hostname`

Size	Last Analysis Date	
66.63 MB	2 hours ago	DMG

DETECTION   DETAILS   RELATIONS   BEHAVIOR   CONTENT   TELEMETRY   COMMUNITY

Crowdsourced Sigma Rules ⓘ

CRITICAL 0   HIGH 0   **MEDIUM 1**   LOW 0

⚠ Matches rule MacOS Scripting Interpreter AppleScript by Alejandro Ortuno. oscd.community at Sigma Integrated Rule Set (GitHub)
↳ *Detects execution of AppleScript of the macOS scripting language AppleScript.*

Crowdsourced IDS rules ⓘ

HIGH 0   **MEDIUM 1**   LOW 3   INFO 0

⚠ Matches rule INDICATOR-SHELLCODE x86 setgid 0 at Snort registered user ruleset
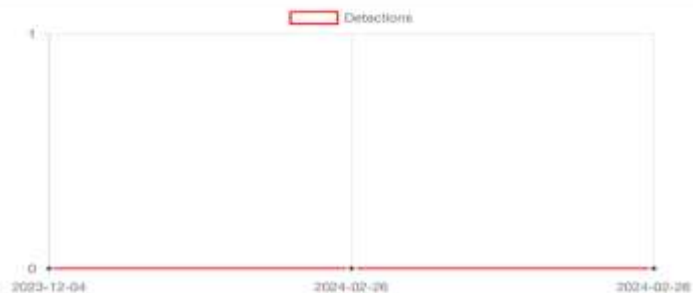↳ *system-call-detect*

⚠ Matches rule (tcp) experimental TCP options found at Snort registered user ruleset
↳ *protocol-command-decode*

⚠ Matches rule SURICATA STREAM Packet with invalid timestamp at Suricata
↳ *Generic Protocol Command Decode*

⚠ Matches rule SURICATA STREAM excessive retransmissions at Suricata
↳ *Generic Protocol Command Decode*

Security vendors' analysis on 2024-02-26T11:49:38 UTC ⌃

📋

Detections evolution	Previous analyses	Date order ▾
	2023-12-04T04:13:58 UTC	0 / 60
	2024-02-26T11:48:10 UTC	0 / 60
	2024-02-26T11:49:38 UTC	0 / 60

☐ Detections

1

0
2023-12-04   2024-02-26   2024-02-26

- Related Atomic Stealer
- Kill action if VirtualBox or VMWare
- Less attacks on macOS
- More severe attacks on macOS

Empire Transfer

The skimmer found at a Walmart in Linda, California

- LockBit ransomware   LockBit next generation encryption
- US, UK, Europe   Operation Cronos
- Multiple persons arrested $110 million unspent bitcoin
- Encryption keys distributed to victims PHP vulnerability
- Pioneer of Ransomware as a service hack-&-leak   name-&-shame
- $15 million bounty   'we are fine'
- 14,000 accounts shutdown   "we are back, stronger than ever"
  Mega, Tutanota, Proton   ConnectWise
- Lists of companies nonreporting   UK lead   2-year investigation

THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action — this is an ongoing and developing operation.

Return here for more information at: 11:30 GMT on Tuesday 20th Feb.

LOCKBIT

NCA
National Crime Agency   EUROPOL   POLITIE   Kanton Zürich   SH   POLIISI

LockBit seized

- Images of you
- Free level
- Paid level
- Opt out "just need a scan of your passport"

PimEyes

- Invoices & payment 18.4%
- Document sharing 7.9%
- Notifications of unread messages & Notifications requiring attention 5.5%
- Action required 4.5%
- Account suspended/compromised/attention 3.5%

Phishing categories

- Someone contacts you
- Problem or something of value
- Act quickly

========================

- So, lure you to contact them
- Online Ads on mobile devices
- Victim search energy bill or similar
- Ads geolocated   No links   Phone number
- [MalwareBytes Report](#)
- CreditKarma

Scams and Computer Safety SIG

- DNSSEC
- One (1) DNS packet to disrupt Internet access
- DNSSEC uses cryptography to authenticate
- Cryptographic signatures CIA
- Bad DNS
- Send all relevant keys with corresponding signatures
- Misconfigured, incorrect, unsupported ciphers
- 2 million times CPU processing time
- 56 seconds up to 16 hours
- Standard 1999
- Recent fixes by Google & Cloudflare
- Could have been REALLY BAD
- Gather IP addresses of critical sites

DNS KeyTrap

- February 20
- Mozilla introduces a new website compatibility report tool in Firefox that Firefox users may use to report broken sites to the organization.
- Tooltips and form controls text is now also translated by Firefox's integrated translation feature.
- Firefox View information may now be searched.
- Known Issue: Firefox on machines with older AMD processors may render thumbnails as "all black" in file dialogs. Mozilla suggests updating the graphics driver to address the issue.

Firefox 123.0

- Backdoor malware
- Lazarus – North Korea
- Remote access
- Upload files Download files photos etc.
- RC4-encrypted socket
- Sleep & hibernate   shell
- Zero-out infection traces
- Unusual system behaviors
- VirusTotal detection August 2023

macOS SpectralBlur

- Linear city powered by renewable energy
- $1 Trillion giga-project
- 150 miles long, 1640 feet high, 650 feet wide
- 9 million residents

The Line

- Post-quantum cryptographic messaging protocol
- PQ3
- iOS 17.4 macOS 14.4 watchOS 10.4
- Replace current protocols later this year
   After updates
- Harvest now, Decrypt later
- Level 3 security

Apple Messaging Protocol

- Today we are announcing the most significant cryptographic security upgrade in iMessage history with the introduction of PQ3, a groundbreaking post-quantum cryptographic protocol that advances the state of the art of end-to-end secure messaging. With compromise-resilient encryption and extensive defenses against even highly sophisticated quantum attacks, PQ3 is the first messaging protocol to reach what we call Level 3 security — providing protocol protections that surpass those in all other widely deployed messaging apps. To our knowledge, PQ3 has the strongest security properties of any at-scale messaging protocol in the world.

Apple Messaging Protocol
Apple Blog Post

- Although such quantum computers don't yet exist, extremely well-resourced attackers can already prepare for their possible arrival by taking advantage of the steep decrease in modern data storage costs. The premise is simple: such attackers can collect large amounts of today's encrypted data and file it all away for future reference. Even though they can't decrypt any of this data today, they can retain it until they acquire a quantum computer that can decrypt it in the future, an attack scenario known as Harvest Now, Decrypt Later.

# Apple Messaging Protocol
Apple Blog Post

Quantum-Security Cryptography in Messaging Apps

Classical Cryptography
Not quantum secure

Post-Quantum Cryptography (PQC)
With end-to-end encryption by default

Level 0

No end-to-end encryption by default

Level 1

End-to-end encryption by default

Level 2

PQC key establishment only

Level 3

PQC key establishment
+
Ongoing PQC rekeying

Future

PQC key establishment
+
Ongoing PQC rekeying
+
PQC authentication

QQ

Skype

Telegram

WeChat

Line

Viber

WhatsApp

Signal (previous)

iMessage (previous)

Signal
with PQXDH

Protection against current threats
from quantum computers including
"Harvest Now, Decrypt Later"

NEW
iMessage
with PQ3

Protection against
future threats from
quantum computers

Note: This comparison evaluates only the cryptographic aspect of messaging security, and therefore focuses on end-to-end encryption and quantum security. Such a comparison doesn't include automatic key verification, which we believe is a critical protection for modern messaging apps. As of the time of this writing, only iMessage and WhatsApp provide automatic key verification. The iMessage implementation, called Contact Key Verification, is the state of the art – it provides the broadest automatic protections and applies across all of a user's devices.

- Google Safe Browsing Site Status
- https://transparencyreport.google.com/safe-browsing/search?hl=en
- NordVPN Link Checker
- https://nordvpn.com/link-checker/
- Bitdefender Scamio
- https://www.bitdefender.com/solutions/scamio.html

- Free to use
- May require account registration

URL Link Check
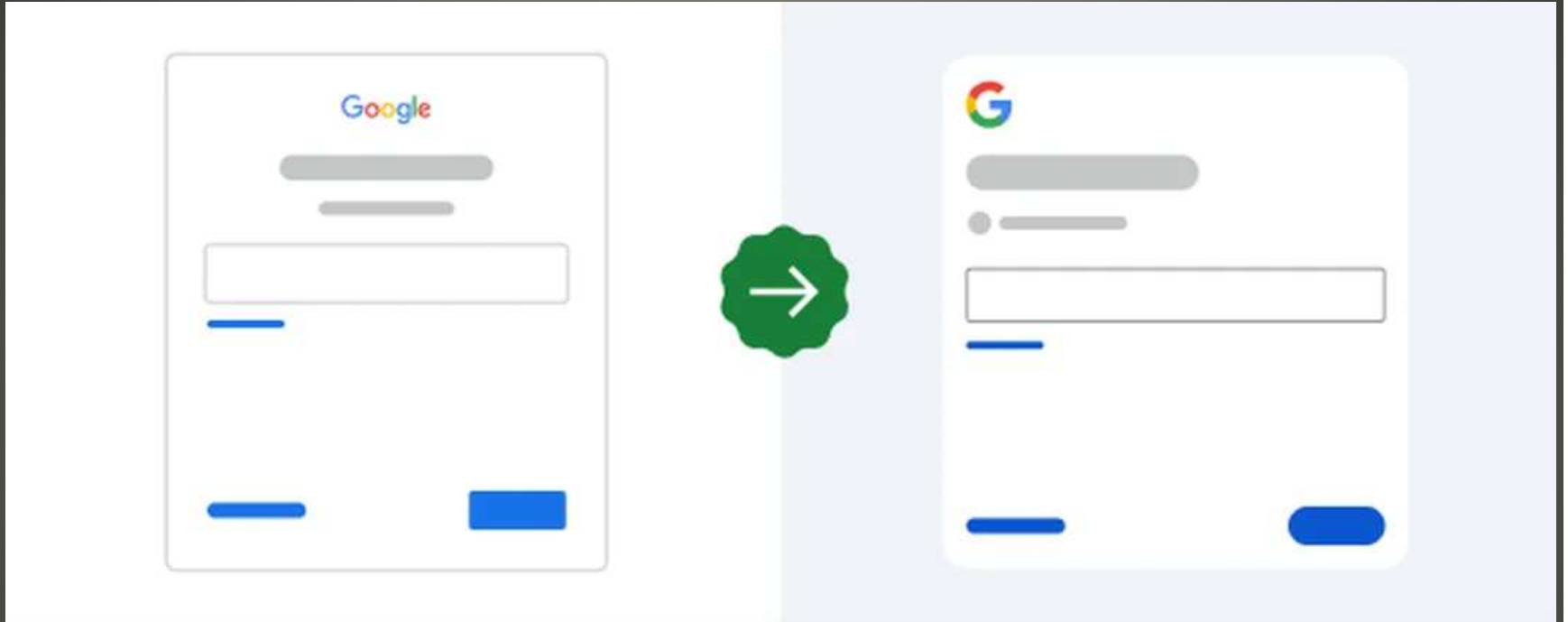
Google New Sign-in look

- Trace inventory
- Steal an one location, refund at another

What happens if you

Walmart using more RFID

Yup, checks

- This amount may appear as a debit
- Your signature on back
- Account info

Refund Checks

- Shortcut vulnerability   CVE-2024-23204
  Chain tasks together   Linux pipes
  Access sensitive info without user consent
  Import good shortcuts
  Expand URL
  select sensitive data | import | encode | forward

iOS vulnerability

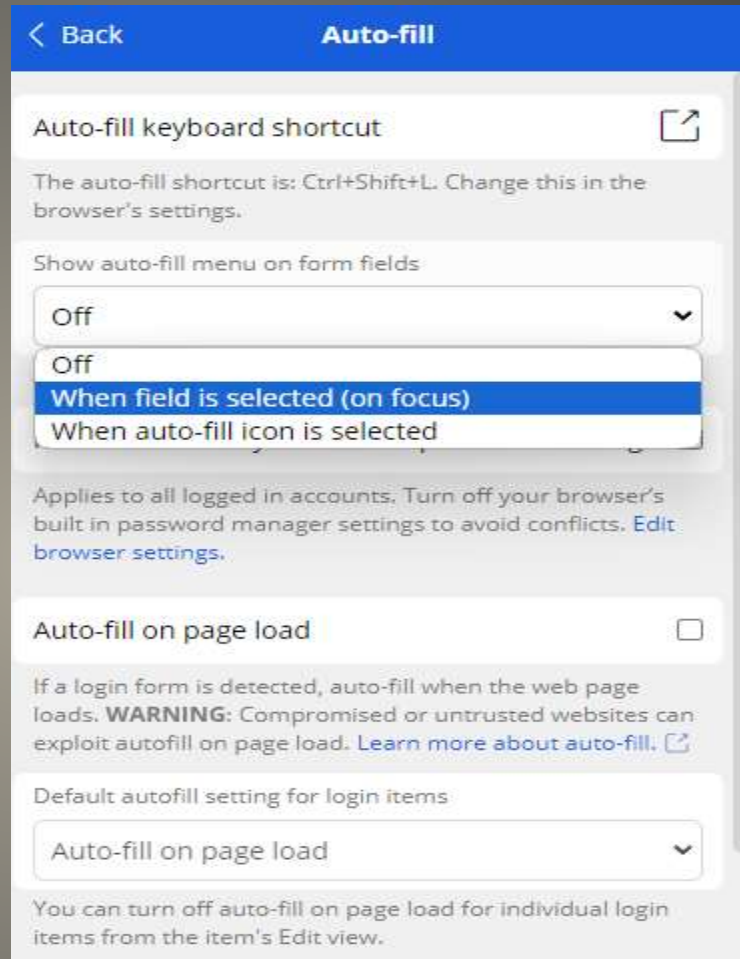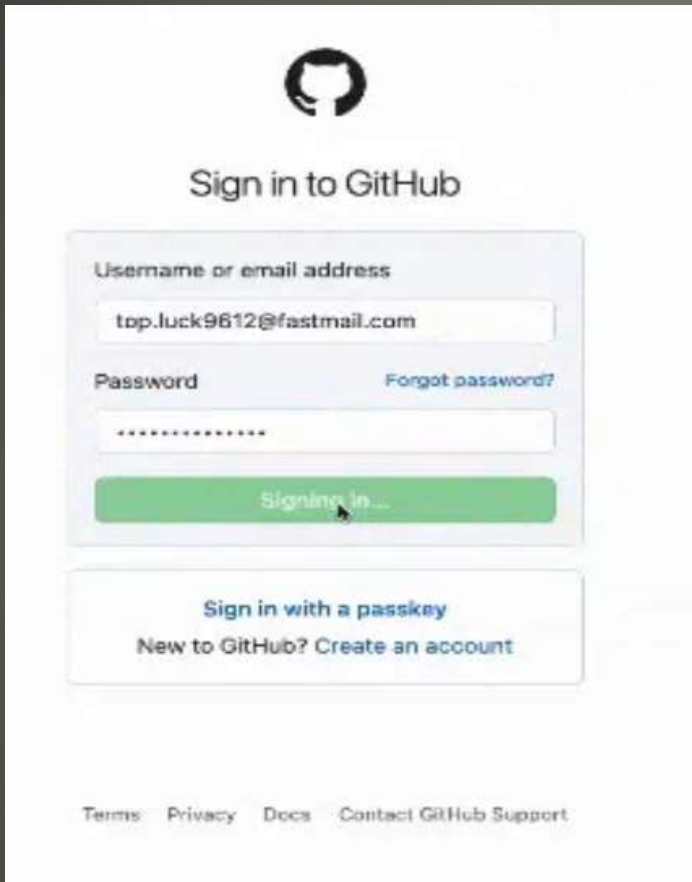- Bitwarden auto-fil option adds phishing resistance
  Detects malicious form fields

Bitwarden will only fill credentials when a user selects a form field, mitigating the risk of automatic credential filling on malicious websites or iframes without user awareness.

Users have the option to password-protect login information, adding another layer of security when using autofill.

Extensive third-party penetration testing was conducted and to identify and close security gaps, presumably including those related to iframes and subdomains.

Bitwarden auto-fil change

Bitwarden auto-fil phishing resistance

- Ban use of AI generated voices for marketing calls
- February 8 decision:

"Although voice cloning and other uses of AI on calls are still evolving, we have already seen their use in ways that can uniquely harm consumers and those whose voice is cloned,"

"Voice cloning can convince a called party that a trusted person, or someone they care about such as a family member, wants or needs them to take some action that they would not otherwise take," the agency wrote. "Requiring consent for such calls arms consumers with the right not to receive such calls or, if they do, the knowledge that they should be cautious about them."

- New amendment Telephone Consumer Protection Act
- Voice Cloning Challenge

FTC & robocalls
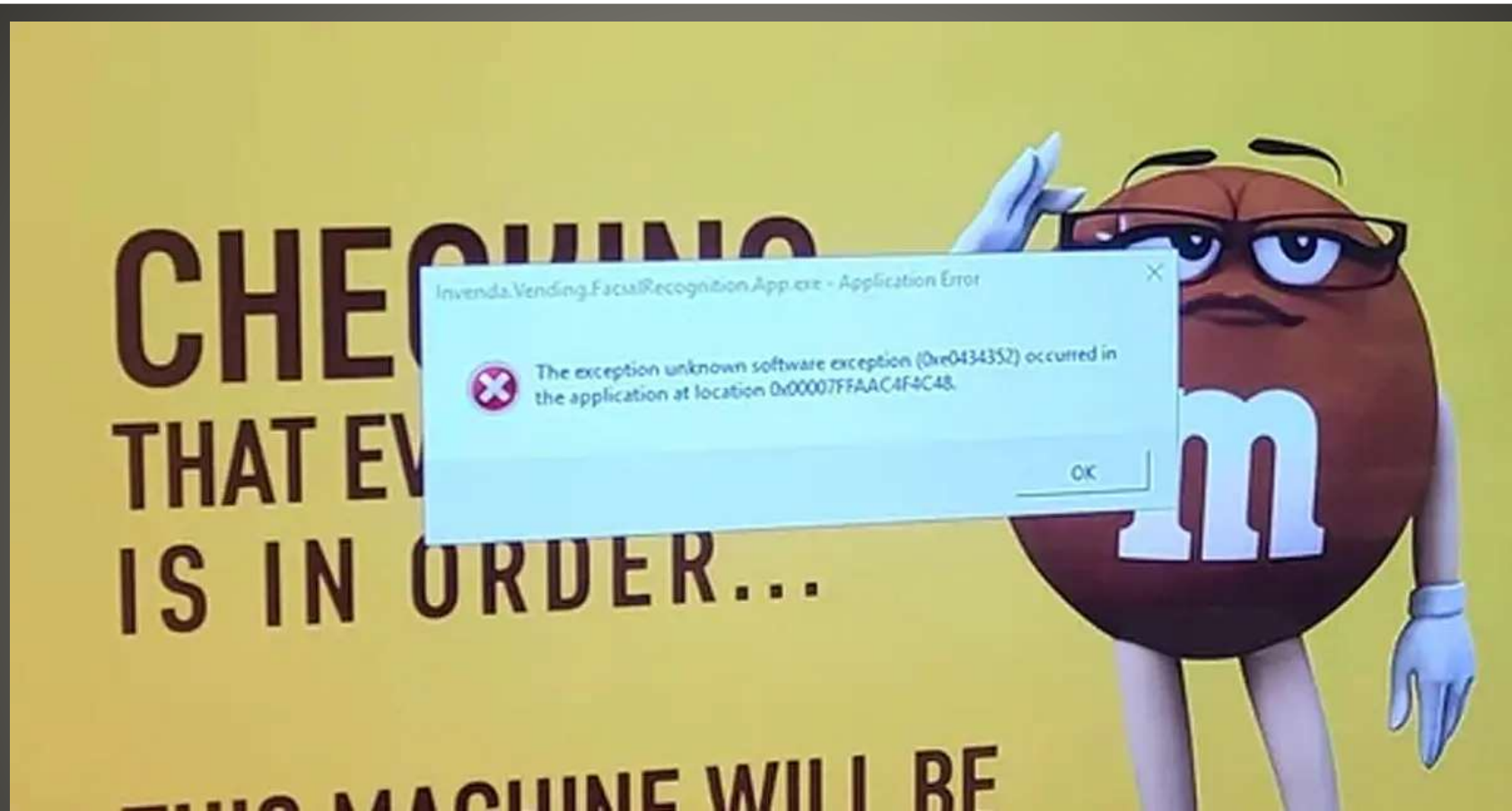
Vending Machines creepy

- University of Waterloo in Canada
- Error screen
- Touchscreen to increase sales
- Facial recognition "feature"   with no warning
- Cover cameras
- Manufacturer's website demographic sensor
- Age, gender
- Yeahbut "data is local"
- No storage, communication, transmission of imagery
- Touchscreen offers:
  combo deals, promotions, AI powered production recommendations

- ## Super Market mood cameras

Vending Machines creepy

- Chinese attack US State department
  Detect due to higher paid tier of support
  Microsoft new allows access to more detailed logs
- When data collection brokers go bankrupt
  Restrictions on "use, sale, licensing, transfer"
- Vietnam to collect biometric data
  iris scans, voice samples, DNA National Identity database
  Privacy protections?
  Germany's e-ID
  India's Aadhaar program
- Just takes one
  Australian telecom Tangerine data breach
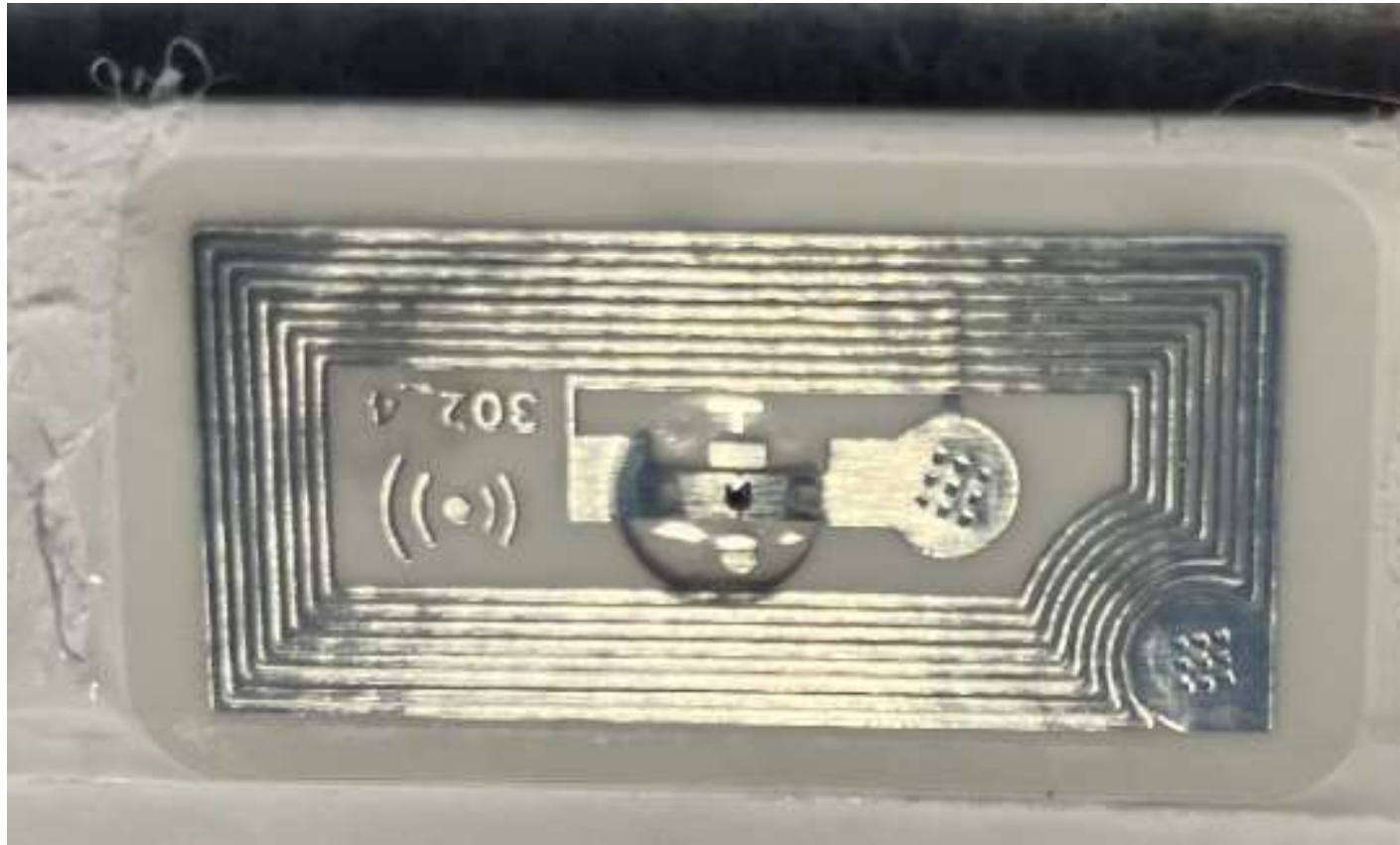 All employees & customers MFA requirement
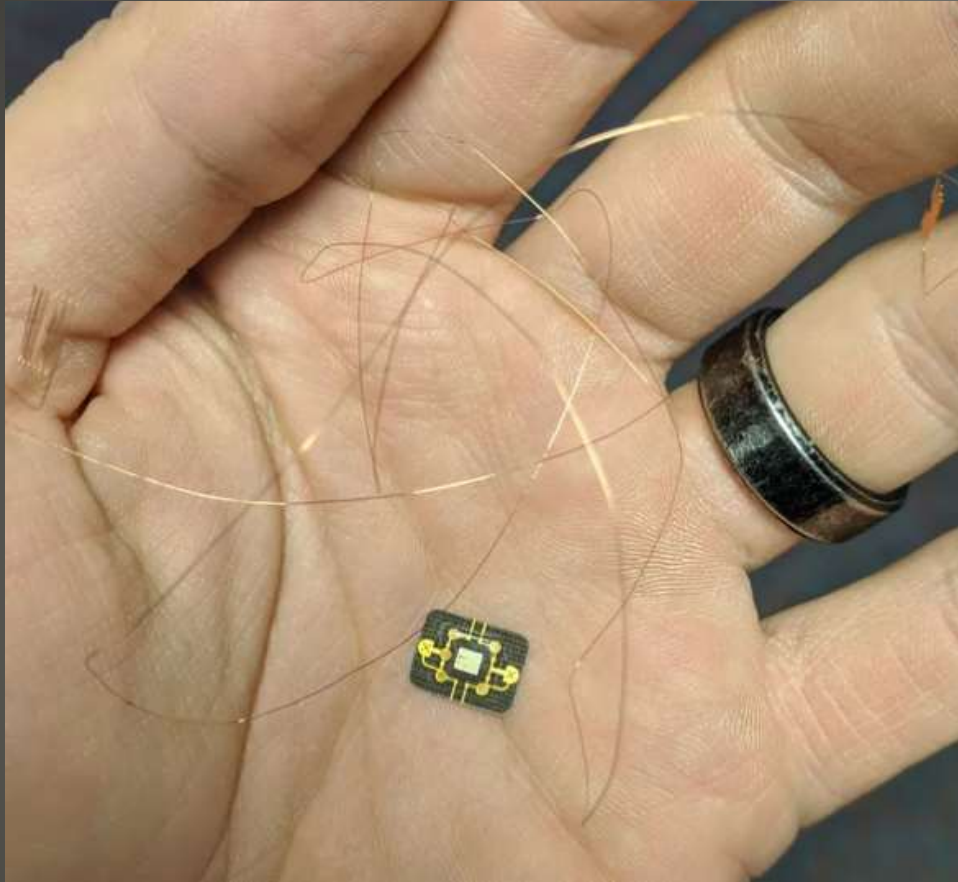 1 contractor

Current Issues

Apple Card

Please activate your card before use.

Credit Card Chip to ring

- Status symbol
- Durability
- Historical

Metal Credit Cards

- Credit cards made from metal Do Not Shred
- Google ended geofence program
  Used by law enforcement
  Which device was at/near crime scene
  Now data obtained from AT&T and T-Mobile
  Less accurate – no GPS from phones
- Google adding Gemini to any/everything
- NIST releases Cyber Security Framework 2.0
- 8,000+ domains of trusted brands hijacked
  Evade Sender Policy Framework protections
  Evade DomainKeys Identified mail
  Evade Domain-based Message Authentication, Reporting and Compliance
  Legitimate and briefly active domains
  e.g. **msnmarthastewartsweeps[.]com**

Current Issues

- APT29
- Tactics, Techniques, Procedures
- Shifting to cloud
- Obtaining access to cloud infrastructure via service and dormant accounts by means of brute-force and password spraying attacks, pivoting away from exploiting software vulnerabilities in on-premise networks
- Using tokens to access victims' accounts without the need for a password
- Leveraging password spraying and credential reuse techniques to seize control of personal accounts, use prompt bombing to bypass multi-factor authentication (MFA) requirements, and then registering their own device to gain access to the network
- Making it harder to distinguish malicious connections from typical users by utilizing residential proxies to make the malicious traffic appear as if it's originating from IP addresses within internet service provider (ISP) ranges used for residential broadband customers and conceal their true origins

Five Eyes Advisory

- Russia Internet
  Telegram down
  Facebook & Instagram appear
  27-Feb-2024
- FBI & partners warn Ubiquiti EdgeRouters [advisory](#)
  Russian state actors
  Attacks from YOUR IP Address
- Microsoft AppLocker vulnerability CVE-2024-21338
  Escalate Administrator privilege to kernel level
- North Korean hackers   FudModule rootkit
   Lazarus   crypto attacks   gained $1B last year
- XY International   5 million messages/day
   Database exposed on Internet without password
- Face Scans to access Websites – then bank account drain

Current Issues

Calendar Spam

- Unsolicited marketing message
- Settings
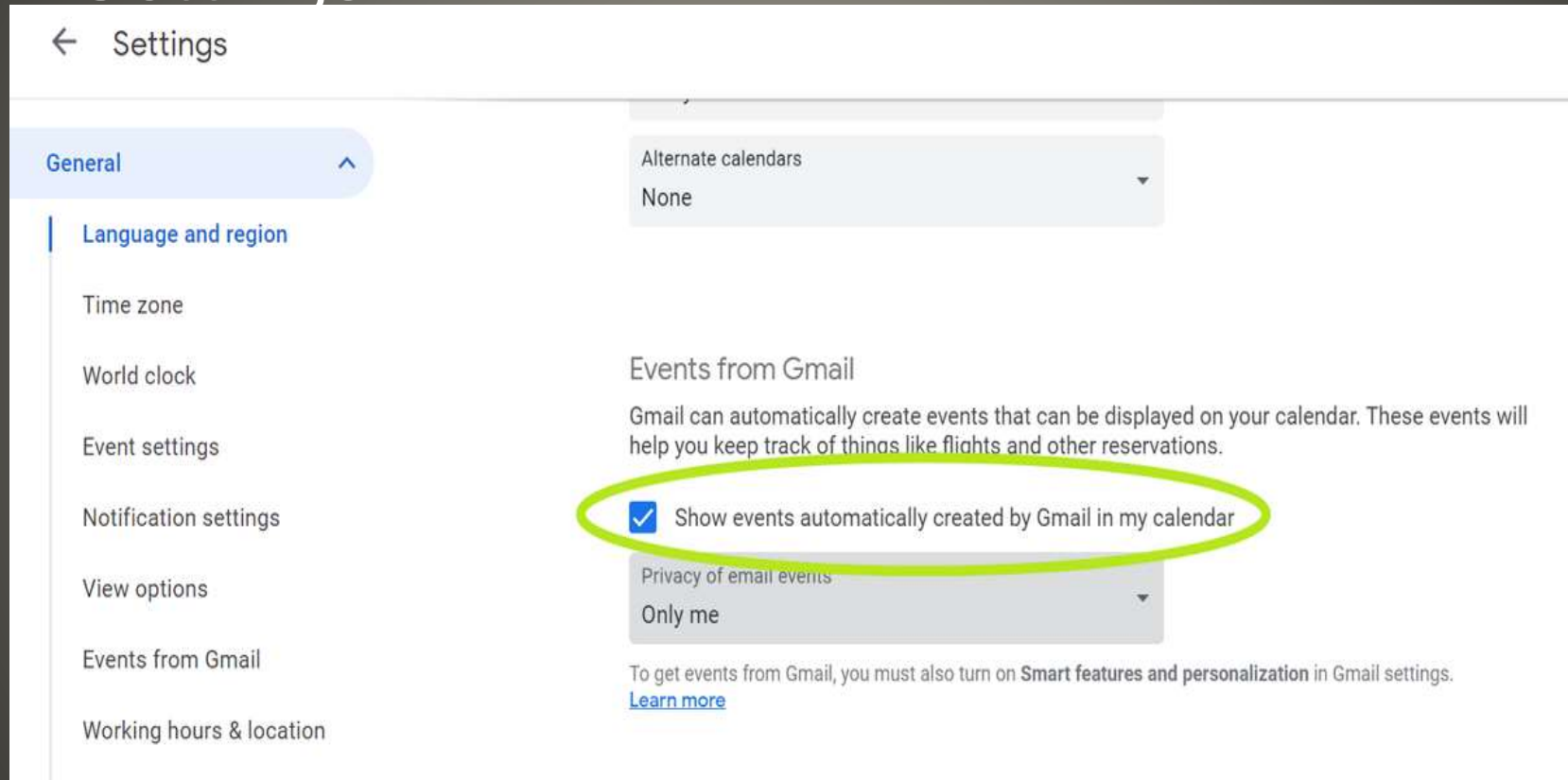
Calendar Spam

- SMS & Voice Calls
- Mobile devices
- Single Sign on
  - Binance, Coinbase, Gemini, Kraken, Shakeplay, Caleb & Brown, Trezor
- CAPTCHA test to encrypt defeat security
- Then fake logon page
- "Please wait"

Phishing Kit Cryptocurrency

- Android Updates
  Gemini app
  Gemini access in Messages App
  Android Auto
    Message summary Suggested reply
  Lookout
    Captions and media content descriptions
  Google Lens   TalkBack
  Google Docs
    Scribble with finger/stylus
  Wear OS
    Wallet app check tickets, boarding passes, tokens
- Tax Preparation Software
  Permissions/privacy
  Terms of Service   Privacy
   "We just need your OK on a couple of things,"
  Credit Karma
- Nevada attempt to block Meta's end-to-end encryption for minors
  Messenger - Extreme urgency - safety and well-being of Nevada children
  Available since 2016   December 2023 as default

Current Issues

- Apps that require enhanced customer information
  Food delivery, Uber, etc.
  Opt out? Sell that data?
  DoorDash fined $375,000 California privacy laws
- EU security & defense subcommittee members
  Spyware detected Members urged to have phones scanned
  The fine folks wanting to force root certificates
- Router security sensitive changes requiring router button press
- Mac Calendly calendar scheduling tool
- GitHub repository confusion attacks

The ease of automatic generation of accounts and repos on GitHub and alike, using comfortable APIs and soft rate limits that are easy to bypass, combined with the huge number of repos to hide among, make it a perfect target for covertly infecting the software supply chain.

Current Issues

- 4 of 15 undersea cables in Red Sea damaged
- Morris II self-replicating AI worm
- Generative AI powered email assistants
- American Express data breach
  American Express Travel related services company
- WhatsApp changes increase scams & spam
   Third party messaging EU DMA
- Tesla Berlin factory arson attack electricity pylon
- North Korea hacks South Korea chip equipment
- Ivanti IOC bad also
- Sun City Computer Club's Facebook Page
  Warning Doorbell Cameras   Help Warnings Information
- Anycubic 3D printers benign warning – Connected printers
- Canada Supreme Court – rules IP addresses are PII
- 225,000 ChatGPT credentials for sale Dark Web markets

Current Issues

- Microsoft Edge – third party cookies
  Privacy Sandbox
- Proton Mail – aliases
- Ransomware giants join forces
  GhostSec & Stormous
- Hacked WordPress sites visitor's browsers
  injected scripts bruteforce password guessing on other sites

Current Issues

- Bank of America   Infosys McCamish Systems
  Name, address, SSN, DoB, account & credit card numbers
  Notification letter Attorney General Texas & Maine
  Fidelity Life Insurance customers
  Bank account routing numbers, credit card numbers
  Access codes, SSN, state of residence, password, PIN
  LockBit
  October 20 -> November 2 2023
- Treasure office of Foreign Assets Control sanctions
  Intellexa Alliance   spyware & surveillance systems
  US government officials

Current Issues - remember?

- 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