Sun City Computer Club

Cyber Security SIG

August 18, 2022

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??

Presenter???

SCCCCyber

Wednesday, August 17, 2022

Google Chrome security update issued today August 17, 2022

Google issued an update to its Chrome browser in response to a reported actively used exploit for vulnerabilities.

Other chromium based browsers are expected to follow with updates for their browsers soon.

Posted by John Jenkinson at 2:50 PM No comments:

Apple Updates today August 17

Press release indicates security and bug fixes for iOS 15.6.1 and iPadOS 15.6.1.

I find macOS 12.5.1 available.

Press release indicates watchOS 8.7.1 to be available but i don't find that update as of this writing.

I checked tvOS and don't see an update.

Strong indications these updates address actively exploited vulnerabilities.

Note: Several browsers have recent updates available this date: 17-Aug-2022.

Current Issues

- VidAngel
- Threema
- One of 4 NIST “quantum safe” algorithms
  SIKE
  Supersingular Isogeny Key Encapsulation
  “glue and spit” elliptic curve attack
- Scammers send Uber to victim
- Single flaw broke every macOS security
  Shutdown Open Apps after Reboot?
  Saved State Feature
- DuckDuckGo rolls out Microsoft blockers after backlash
- Microsoft Patch Tuesday
- Facebook “testing” end-to-end encryption for Messenger


Are you sure you want to shut down your computer now?
If you do nothing, the computer will shut down automatically in 55 seconds.
Reopen windows when logging back in
Cancel
Shut Down

Defcon

- Los Vegas airport
  - All gates evacuated – rescreen
  - Requiring printed boarding passes
  - Loud Noise
- Facemasks were required
- Many later tweeted testing positive

Multi Factor Authentication

- SMS
- Authenticator App
- Physical security key
- Signed certificate

- Proxy to steal authentication cookie


15

Defcon


MY OTHER COMPUTER
IS YOUR COMPUTER

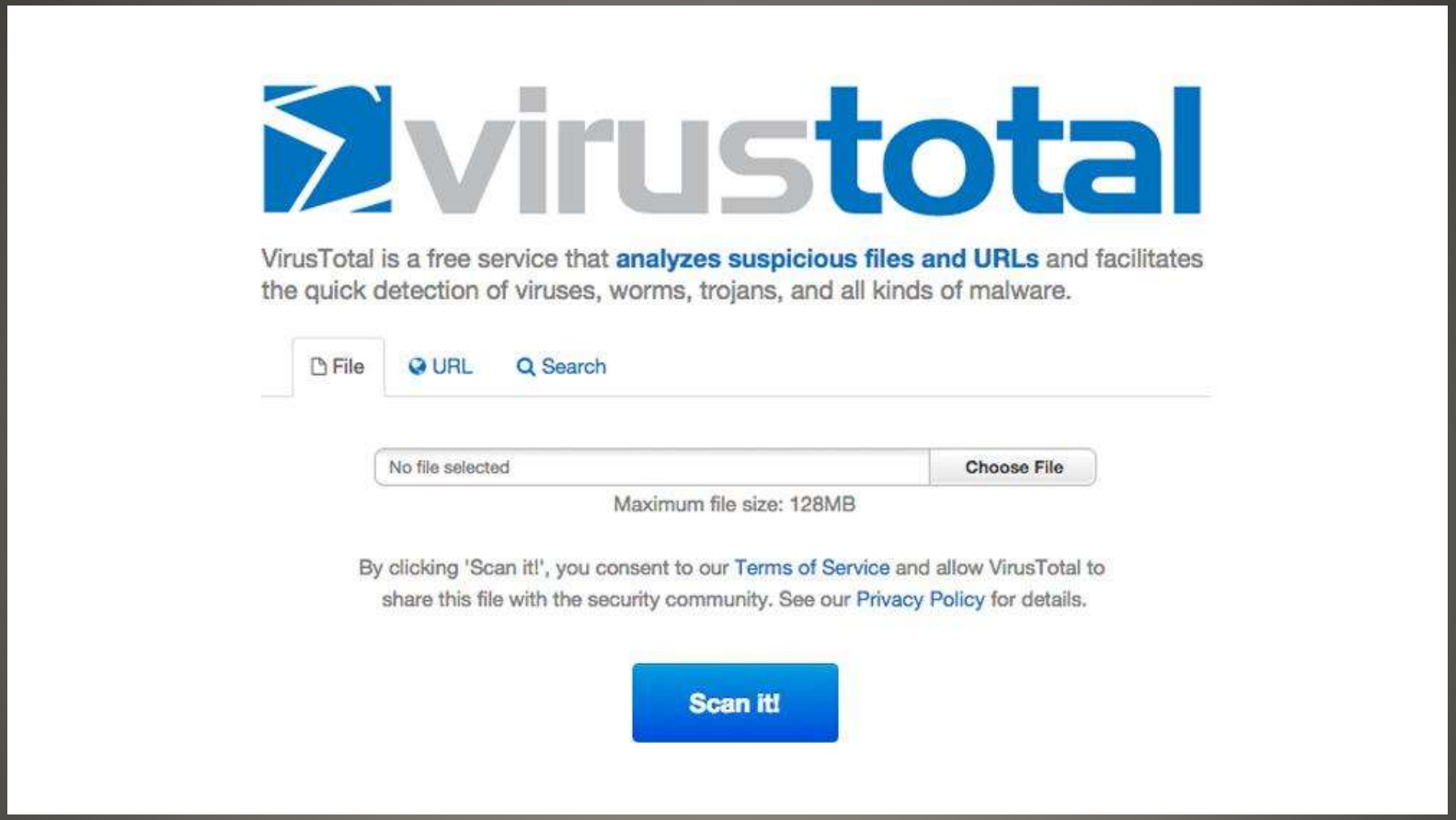
VirusTotal report

- A report
- 87% of malicious malware digitally signed
- Site cert => rigor
- Code signing cert => money
- 58% signed by CA named Sectigo
  was named Comodo

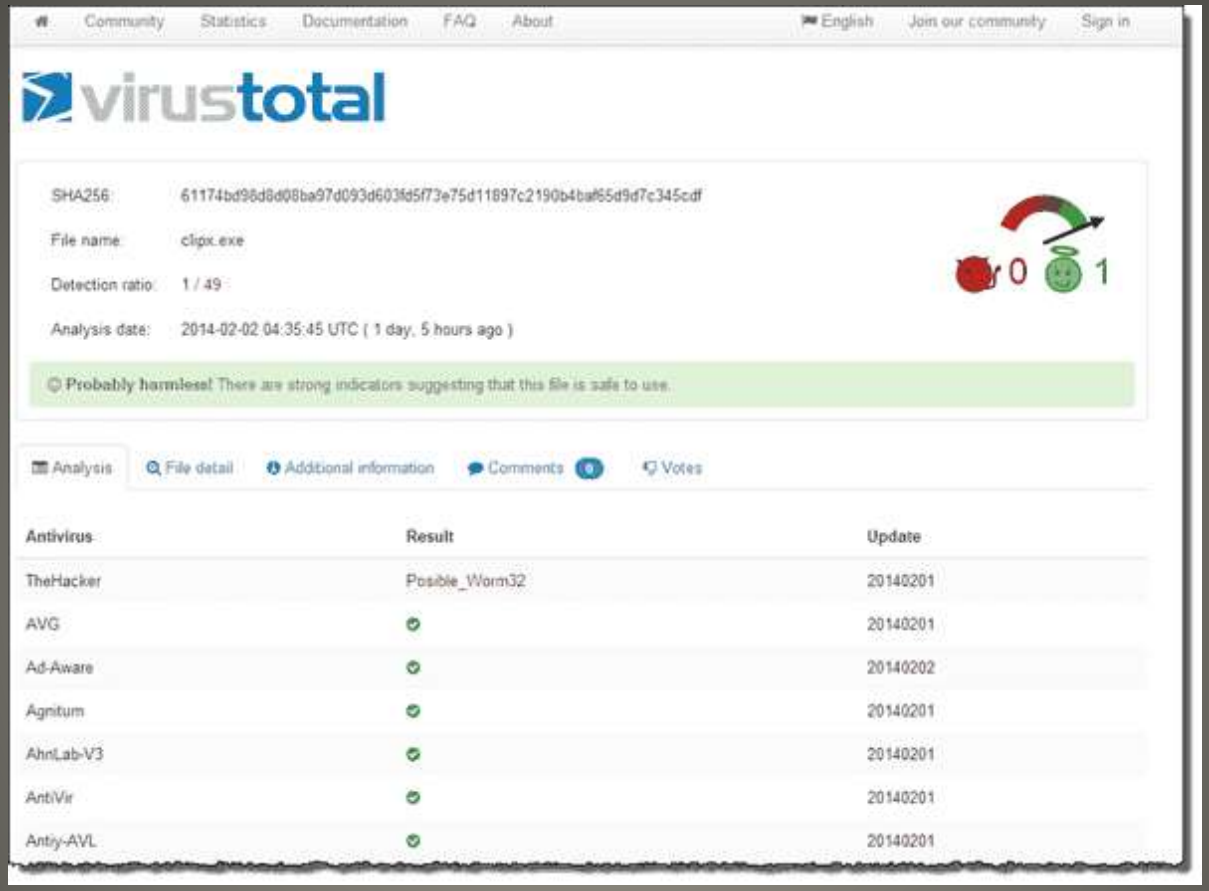
MOST Spoofed: Skype, Adobe Reader, VLC Player, 7-Zip, TeamViewer, CCleaner, Steam, Zoom, WhatsApp

- Spoofed icon, form, function
- Hacked / attacked domains

discordapp[.]com, squarespace[.]com, amazonaws[.]com, mediafire[.]com, qq[.]com


virustotal
VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.
File
URL
Search
No file selected
Choose File
Maximum file size: 128MB
By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.
Scan it!

VirusTotal


Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign in
virustotal
SHA256: 61174bd98d8d08ba97d093d603fd5f73e75d11897c2190b4baf65d9d7c345cdf
File name: clipx.exe
Detection ratio: 1 / 49
Analysis date: 2014-02-02 04:35:45 UTC (1 day, 5 hours ago)
0
1
Probably harmless! There are strong indicators suggesting that this file is safe to use.
Analysis
File detail
Additional information
Comments
Votes
Antivirus
Result
Update
TheHacker
Posible_Worm32
20140201
AVG
20140201
Ad-Aware
20140202
Agnitum
20140201
AhnLab-V3
20140201
AntiVir
20140201
Antiy-AVL
20140201

VirusTotal

VirusTotal

- Owned by Google
- Bad Actors use VirusTotal
- Suggest rescan

Windows 11 User Data corruption

- Newer processors
  - Vector Advanced Encryption Standard (VAES)
  - Use of:
    - AES XEX-based tweaked-codebook mode (AES-XTX)
    - AES with Galois/Counter Mode (AES-GCM)

TO Prevent Further Damage

June 14, 2022 security release

Slower encryption actions until July 12, 2022 security release

SCCCCyber

Wednesday, August 10, 2022

Malicious Apps to find and remove from your MAC

Malicious apps can and are installed in Apple Macs.

Below is a current list of apps to find and remove:

- PDF Reader for Adobe PDF Files - Sunnet Technology Inc
- Word Writer Pro - TeamIdentifier
- Screen Recorder - TeamIdentifier
- Webcam Expert - TeamIdentifier
- Streaming Browser Video player - TeamIdentifier
- PDF Editor for Adobe Files - TeamIdentifier
- PDF Reader - TeamIdentifier

The cited apps have been removed from the Apple store, but they may have been loaded prior to that removal.

Fake reviews added to the ability to alter their behaviour when reviewed by Apple had increased the popularity and download in the Apple store.

Finish your payment_%DJSK

Inbox ×

john tur <

Tue, Jul 19, 2:06 PM

to consumer bcc: me

DEAR sir/madam

We thank you for completing one year with **Geeks** Deluxe Security LLC.

We have charged you $175 for the next 36 months subscription. We tried to contact you on your registered Phone number. Deduction of amount **will** appear on your bank account within 48 hours.

INVOICE DATE	:	19th July 2022
ORDER **NUMBER**	:	DJSK
PAYMENT **METHOD**	:	ONLINE

If you have any Question or Wish to cancel the Renewal, Please connect us (+1) (805)-(567)-(4405) within 24 hrs.

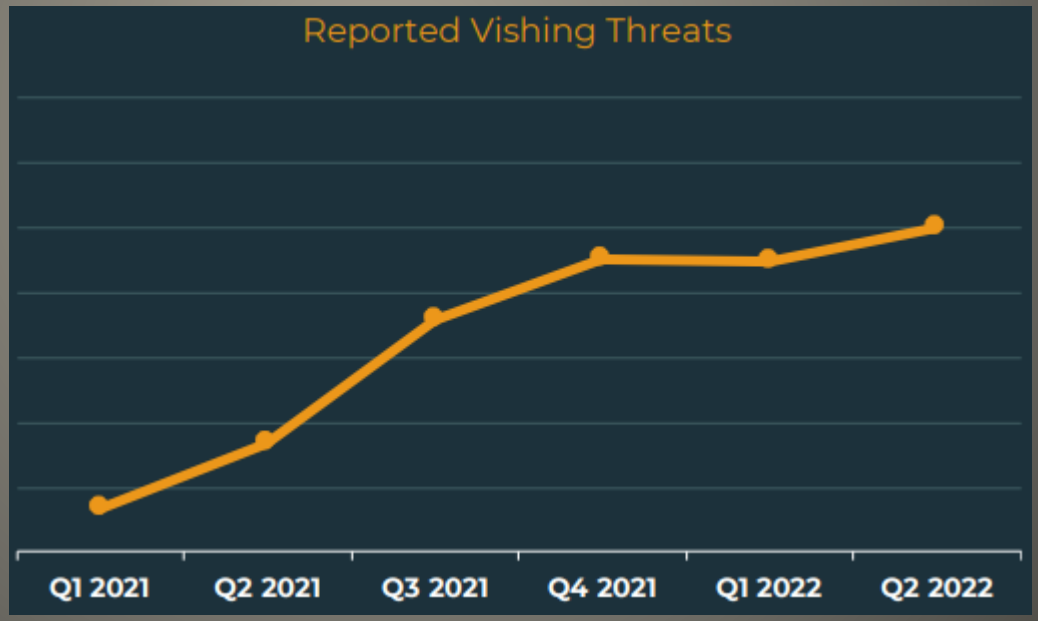
Thank You

Harry- Account **Manager**

Or Call - (+1) (805)-(**567**)-(4405)

GEEKS BILLING **DEPARTMENT**.

- eMail and voice social engineering
- Almost got me
- “I will fix this error”
- “I need your credit card to refund the charge”



Call Back Phishing Attacks Growing

- Two factor authentication provider
- Content delivery network
- Network equipment maker

  Internal phone numbers

  Logins to work accounts - fake

I'd NEVER get phished

VERY VERY GOOD ATTACKS

Current Issues

- Microsoft Defender External Attack Surface Management
  Discover unmanaged resources
  Multicloud visibility
  Identify exposed weaknesses

"You do not know all of your assets or vulnerabilities, but attackers (and Microsoft) do"

- OPatch - legacy windows
  0-days
  Micropatching usually no reboot
- Taiwan DDoS attacks post Pelosi visit
- FEMA – critical vulnerabilities
  Emergency Alert System devices
  Patch, firewall, audit logs

Current Issues

- macOS manual zoom update recommended
- John Deere tractor control unit jailbreak
  dealerAuth.txt
- Clop ransomware attacks UK water authority
  Misidentifies actual victim
- Signal breach 1900 phone numbers
- All 7-11 stores in Denmark closed
  All cash registers and payment systems
- iOS Instagram and Facebook
  ALL 3rd party links and ads rendered in an in-app browser
  Thus, monitor w/o consent of user or website
  Inject custom java script for analytics
- iOS VPN best practice - RESTART apps/connections

Meta on iOS

- iOS Instagram and Facebook

  ALL 3rd party links and ads rendered in an in-app browser

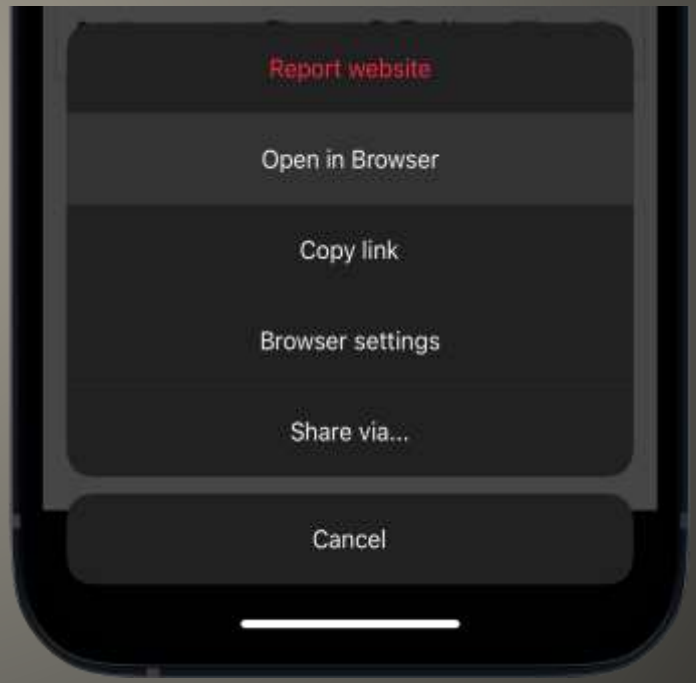
  Thus monitor w/o consent of user or website

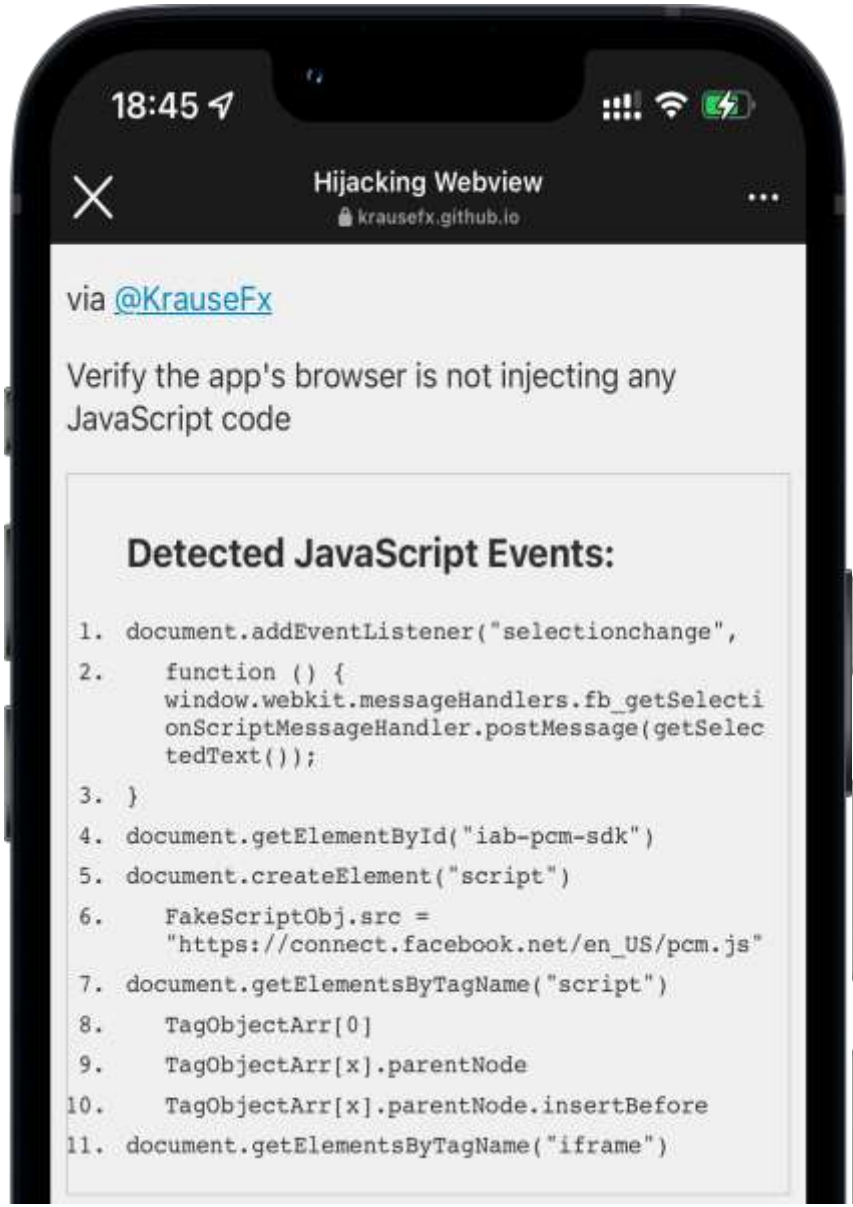
  Inject custom java script for analytics

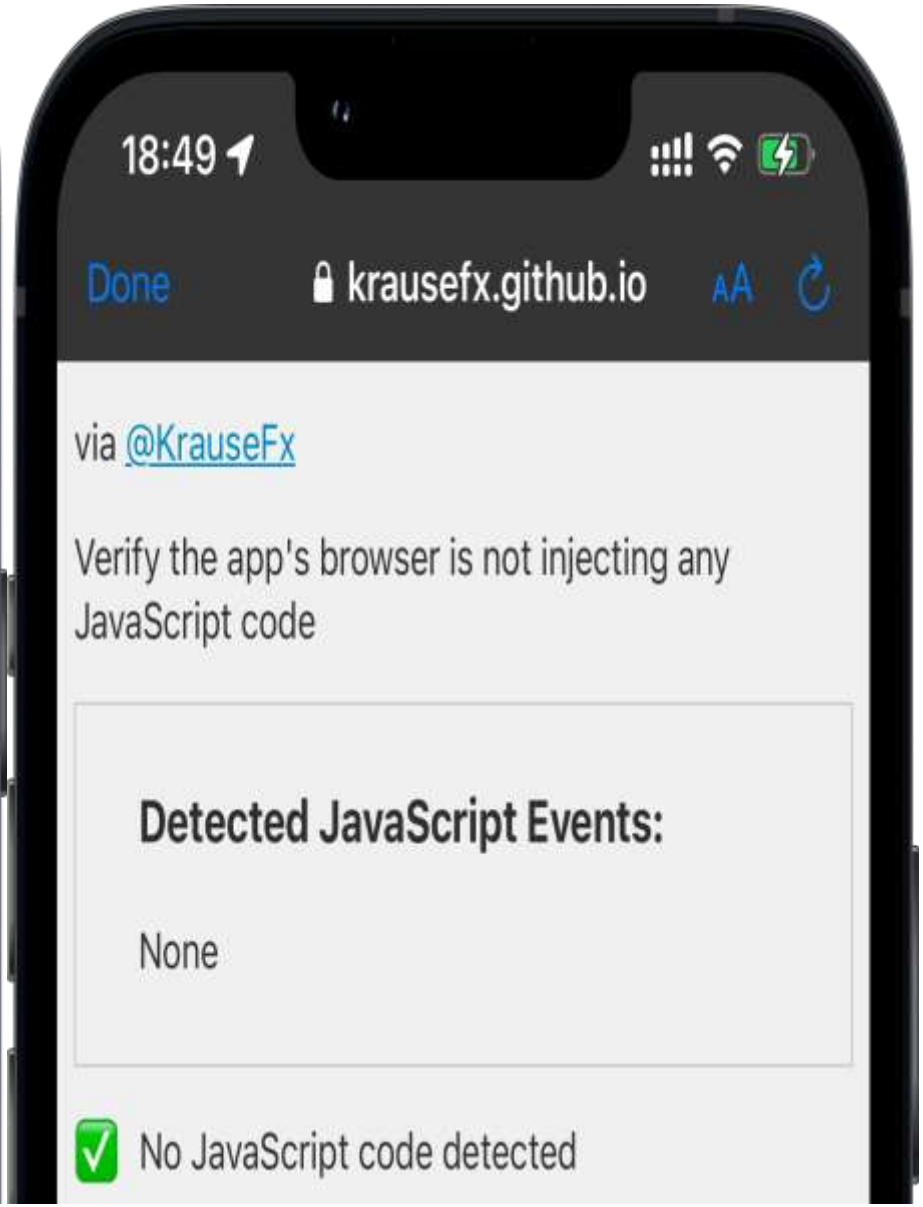
Protection:

Open website in Safari

- Use mobile web version




18:45
Hijacking Webview
krausefx.github.io
via @KrauseFx
Verify the app's browser is not injecting any JavaScript code
Detected JavaScript Events:
1. document.addEventListener("selectionchange",
2. function () {
window.webkit.messageHandlers.fb_getSelecti
onScriptMessageHandler.postMessage(getSelec
tedText());
3. }
4. document.getElementById("iab-pcm-sdk")
5. document.createElement("script")
6. FakeScriptObj.src =
"https://connect.facebook.net/en_US/pcm.js"
7. document.getElementsByTagName("script")
8. TagObjectArr[0]
9. TagObjectArr[x].parentNode
10. TagObjectArr[x].parentNode.insertBefore
11. document.getElementsByTagName("iframe")


18:49
Done
krausefx.github.io
AA
via @KrauseFx
Verify the app's browser is not injecting any JavaScript code
Detected JavaScript Events:
None
No JavaScript code detected

Current Issues

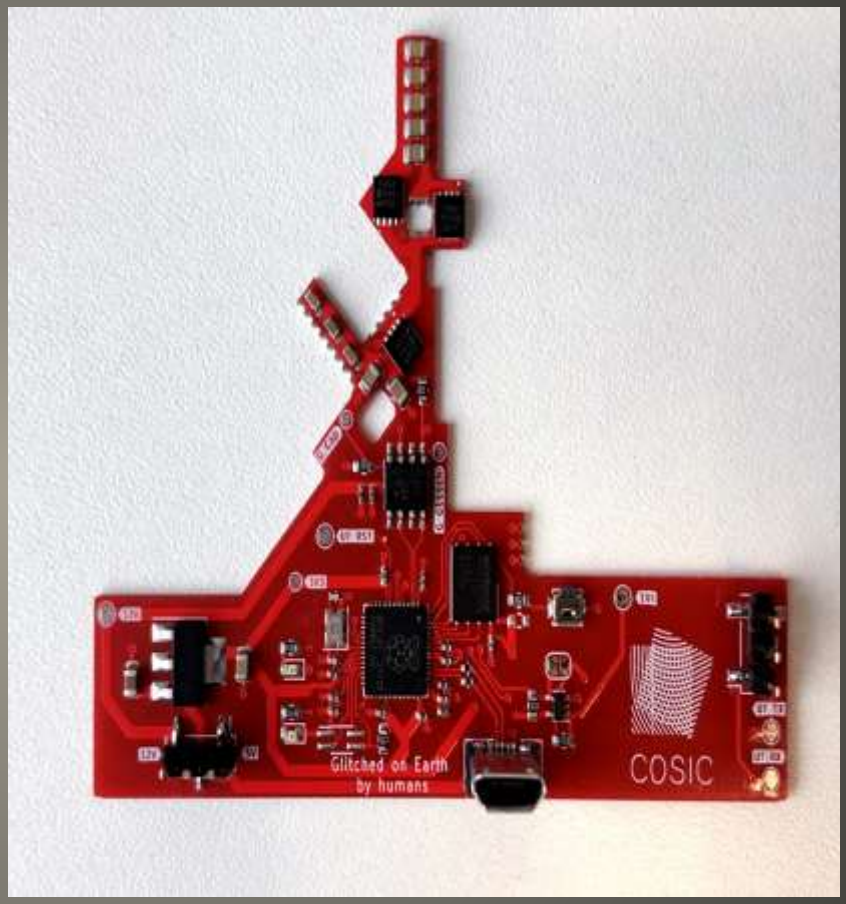
- US DoJ using paper for sensitive documents
- Streaming services Updates & privacy
  Logging Sharing information/data
- YouTube Royalties scams
  digital rights companies
- Use caution with search
  Customer Service Numbers
  Tech Support
  Financial Services and Apps
  Government programs
  Trade Professionals
  Apps
  Coupon Codes
- 9,000 VNC systems with no password protections
- Amex disabling chips in cards if threat exposed email addresses Delay in replacement cards

Web Site entropy

- My website
- Domain name
- Storage
- Web code
- Web content
- Maintenance

- Who owns the domain name registration?

- Cyotek WebCopy
- https://www.cyotek.com/cyotek-webcopy



Starlink attack

Starlink attack

- Starlink 3000+ satellites LEO
- Dishy McFlatface Black Hat paper
- Starlink Response
- Attack gains limited access to disk itself
- Bounty paid Job offer
- Github
- Satellites, 2 earth stations, McFlatfaces

- Amazon, OneWeb, Boeing, Telsat, SpaceX own constellations
- Via-Sat attacks Ukraine invasion
  Wiper malware 30000 internet connections
  5,000 wind turbines

- Satellites are critical infrastructure

Black Hat

- Keynote
  25-year anniversary
  Stuxnet, Colonial pipeline, etc. Predictable
- SMS & MFA
- Invisible finger
  Place on table with hidden antennae
- Cyber harm reduction
- Major Cyber Incident Playbook
- Cyber Skill resignations
- Startups & bounty programs
- Apple MAC security - layer bypass

- Hackers are Internet / Cyber immunity system
- Awareness, Preparedness, Understanding

- Twitter vulnerability
  Enter email or phone number
  Response was Twitter accounts that matched
  Twitter tweeted: *If you operate a pseudonymous Twitter account, we understand the risks an incident like this can introduce and deeply regret that this happened. To keep your identity as veiled as possible, we recommend not adding a publicly known phone number or email address to your Twitter account.*

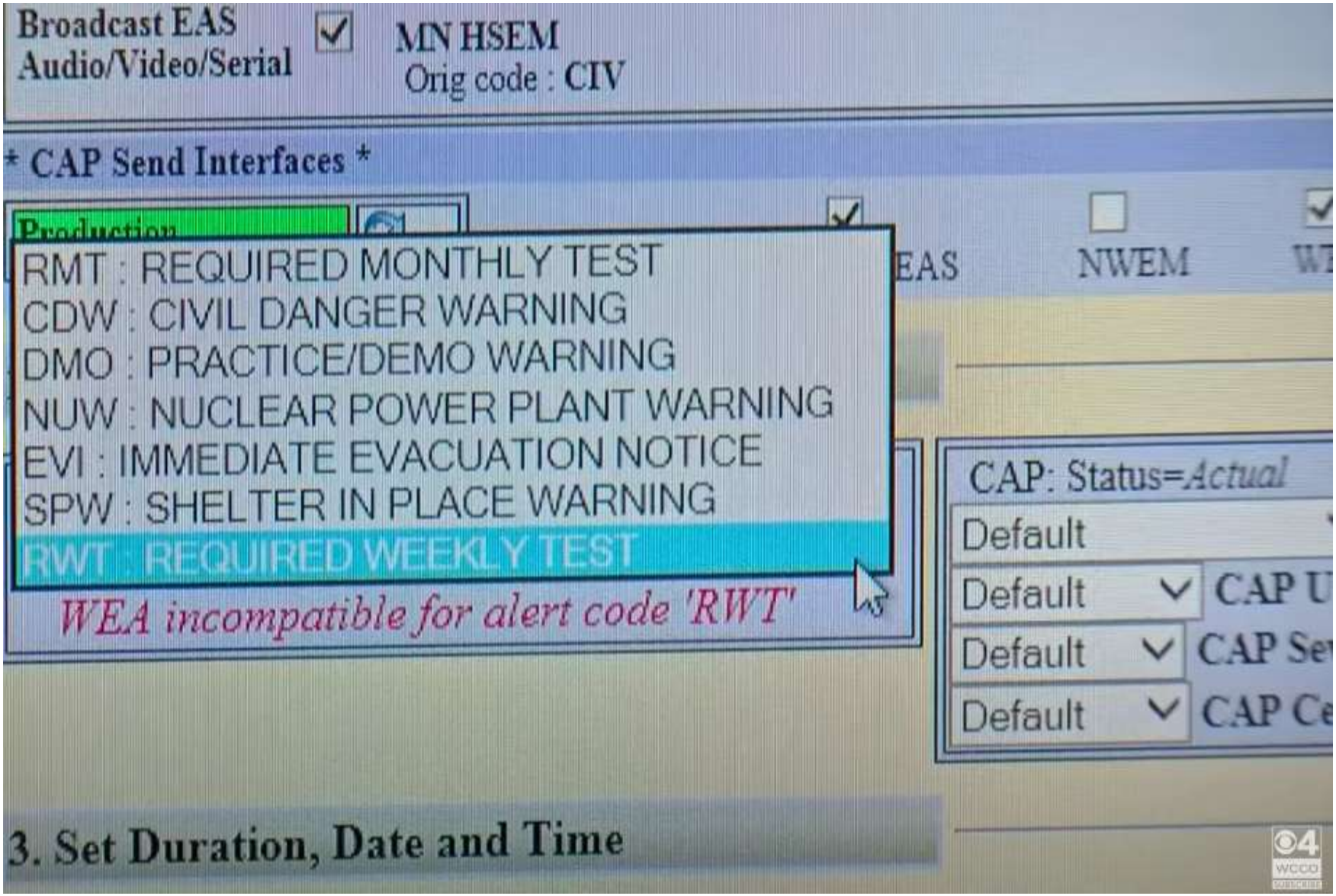
- Twitter vulnerability exposes data of 5.4 million accounts

- Safe – only user has access
- Loss – No one has access
- Leak – user and adversaries have access
- Theft – Only adversary has access

Emergency Alert System

- National public warning system

- Equipment off eBay
- username & password
- Vendors alerted
- Some patched *Some patched*
- Surplused device crypto keys available


Broadcast EAS
Audio/Video/Serial
MN HSEM
Orig code : CIV
* CAP Send Interfaces *
EAS
NWEM
RMT : REQUIRED MONTHLY TEST
CDW : CIVIL DANGER WARNING
DMO : PRACTICE/DEMO WARNING
NUW : NUCLEAR POWER PLANT WARNING
EVI : IMMEDIATE EVACUATION NOTICE
SPW : SHELTER IN PLACE WARNING
RWT : REQUIRED WEEKLY TEST
WEA incompatible for alert code 'RWT'
CAP: Status=Actual
Default
Default
Default
Default
3. Set Duration, Date and Time

- 23 Million

  Names, addresses, phone numbers, SSN, DOB

Our data? Not our breach

SELLING 124M U.S.A. SSN, DOB, DL database, freshly breached
by SubVirt - 9 hours ago

SubVirt

M.V.P User

Posts	24
Threads	8
Joined	Mar 2019
Reputation	30

2 YEARS OF SERVICE

Exclamation 9 hours ago This post was last modified: 4 hours ago by SubVirt. Edited 2 times in total.

This data has never been sold to anyone else and is not public.
It was dumped several days ago.
Edit: Just to clarify, there are 30 million unique SSNs in these files, due to duplicates

Sample:

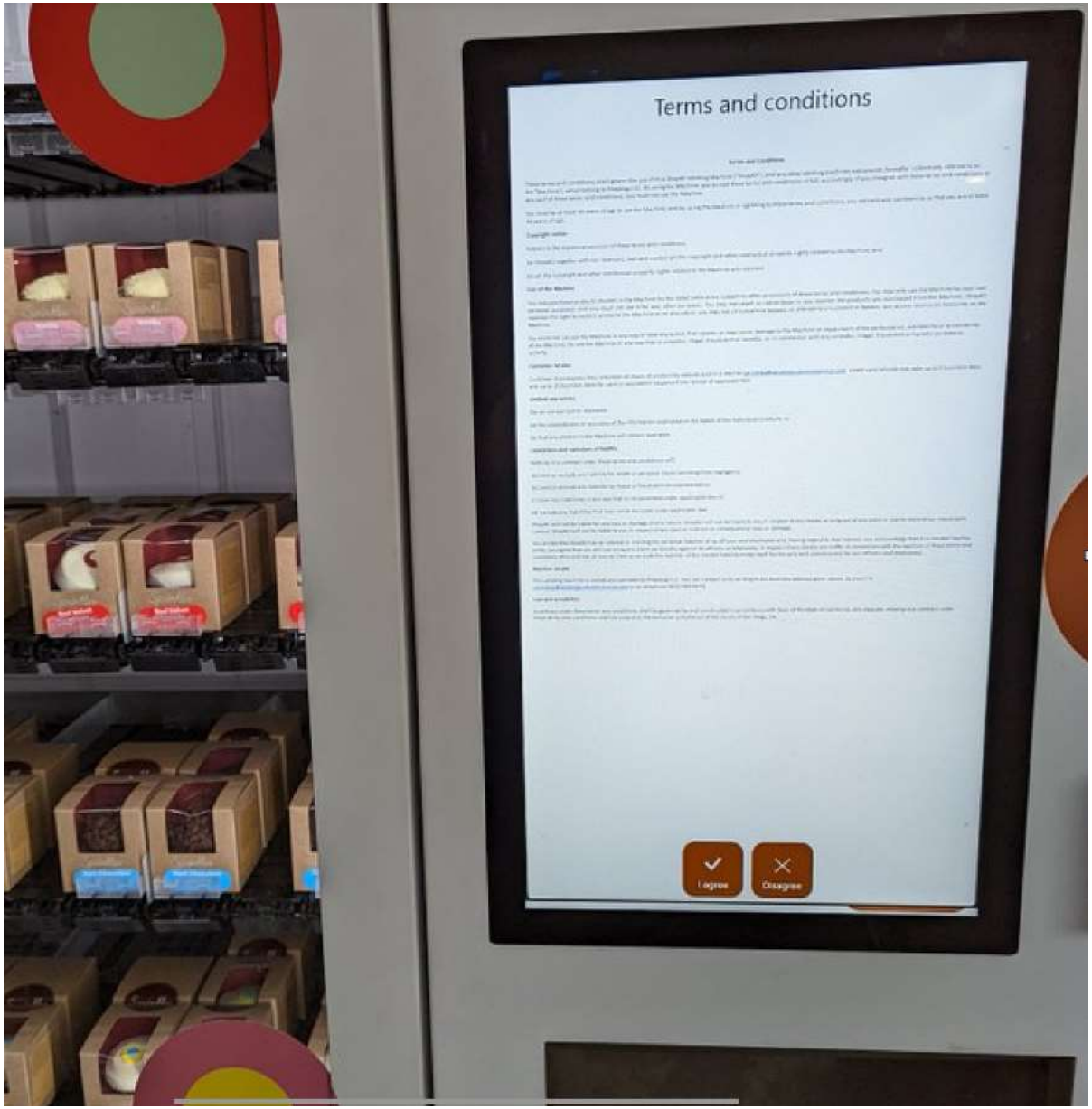
29-JAN-83, :KER,VA,24014
19-NOV-45, MO,PR,00951
09-OCT-73, L,TX,78023
14-OCT-82, Y,11223
04-JUN-84, EBISH,PA,18651
13-JUL-79, E,NY,11212
13-NOV-90, NT,TX,77086
10-DEC-63, ,CA,91770
30-JAN-38, NO,NY,10034

SERIOUS BUYERS ONLY, MUST SHOW PROOF OF FUNDS BEFORE ADDITIONAL INFO

Price: 6 Bitcoin
My Telegram:

Email aliases

- myemail+identifier@mailservice.com
- Not all email services support
- Those that do, may not later
- “+*@” filter


Terms and conditions
I agree
Disagree

Firefox Translations

- On the device Not the Cloud
  Google and Bing (Microsoft)
  Thus URL, device IP, when what where NOT transmitted

Git Hidden Folders

- Git
- Open source version control system
- Hidden folders usage
- Best practices not always followed
- If not hidden folders exposed
- Secrets within those folders exposed
- MANY sites
- Thousands within .gov domain

Warning!! Your account will be closed

Hi,

We're investigating your account for violating our copyright. You must defend your account against copyright. Otherwise, your account will be disabled. Please fill out the appeal form carefully. When you fill out the form, our teams will review your account. Otherwise, Your account will be deleted within 72 hours.

Objection Form

from

Meta

- You reset your passcode and forgot the new one.
- Someone else reset your passcode.
- You have entered an incorrect passcode so many times that your phone has locked itself out of security settings.
- Your phone is disabled.
- Your screen is cracked and won't accept your passcode.
- The phone belongs to someone else who needs help.
- You're stuck in an emergency situation in which the only phone available has a passcode you don't know.
- Many people only use Touch ID or Face ID, so they forget their password. "Apple's Face ID feature relies on a learning algorithm, so it is still not 100% accurate,“

"If the feature gets disabled or gets a glitch on your device, you will have to resort to using the passcode."

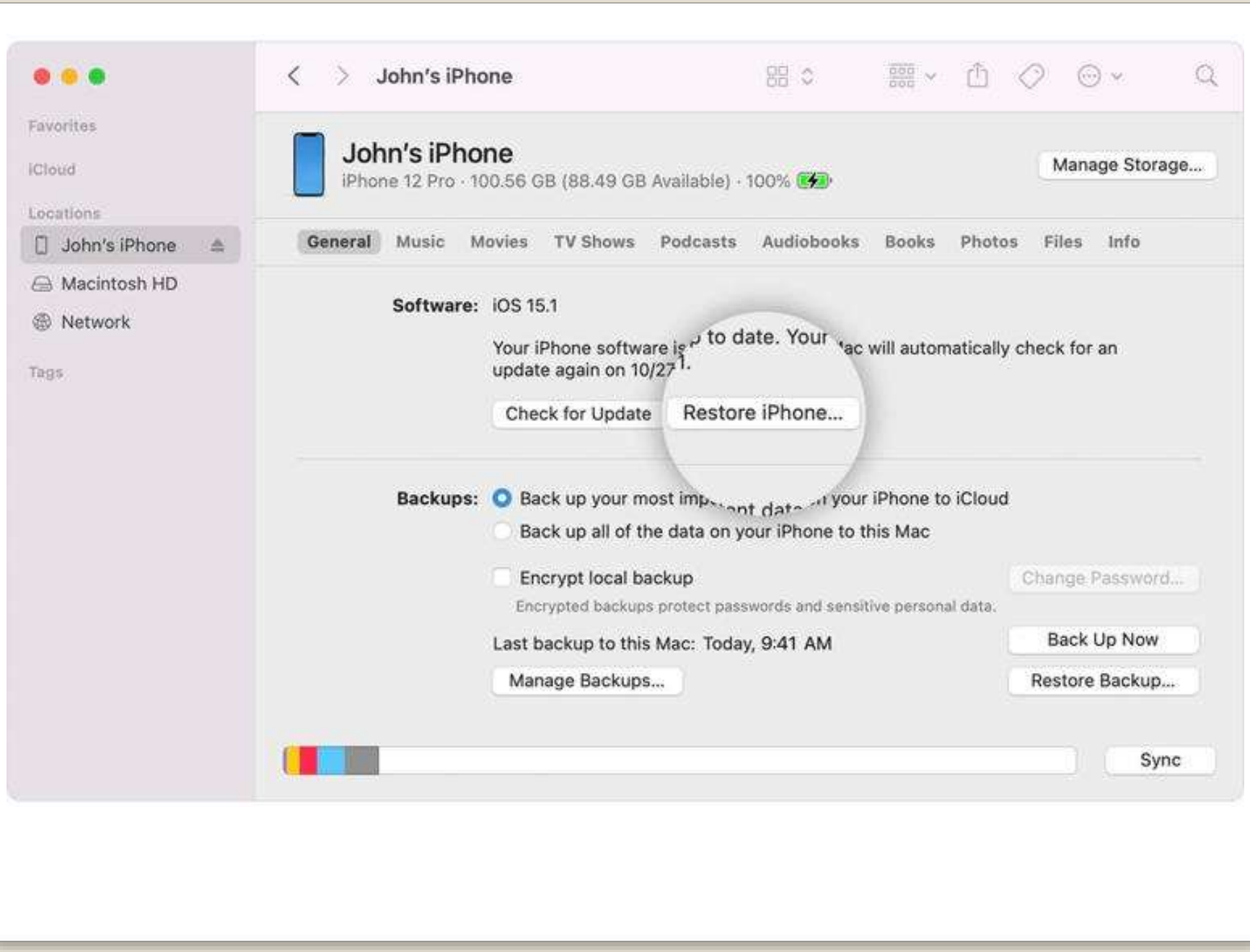
Unlock iPhone (iDevice) WHY?

- iTunes Pre Catalina
  iTunes on mac pre-Catalina
  iDevice in recovery mode
  iDevice 8 & above side button
  iDevice 7 & 7 Plus Volume down
  iDevice 6 and prior Home button
  Recovery Mode
  Find iDevice then “Restore”


File Edit View Controls Account Help
Search
John's iPhone
John's iPhone
128GB
100%
Settings
Summary
Music
Movies
TV Shows
Photos
Info
File Sharing
On My Device
Music
Movies
TV Shows
Books
Audiobooks
Tones
iPhone 12 Pro
Capacity: 119.10 GB
Phone Number 1: (408) 555-0941
Phone Number 2: n/a
Serial Number: XXYXX1XX2X34
iOS 14.4
Your iPhone software is up to date. iTunes will automatically check for an update again on 3/3/2021.
Check for Update
Restore iPhone...
Backups
Automatically Back Up
iCloud
Back up the most important data on your iPhone to iCloud.
This Computer
A full backup of your iPhone will be stored on this computer.
Encrypt local backup
This will allow account passwords, Health, and HomeKit data to be backed up.
Change Password...
Manually Back Up and Restore
Manually back up your iPhone to this computer or restore a backup stored on this computer.
Back Up Now
Restore Backup
Latest Backup:
Today 8:00 AM to this computer
113.46 GB Free
Sync
Done

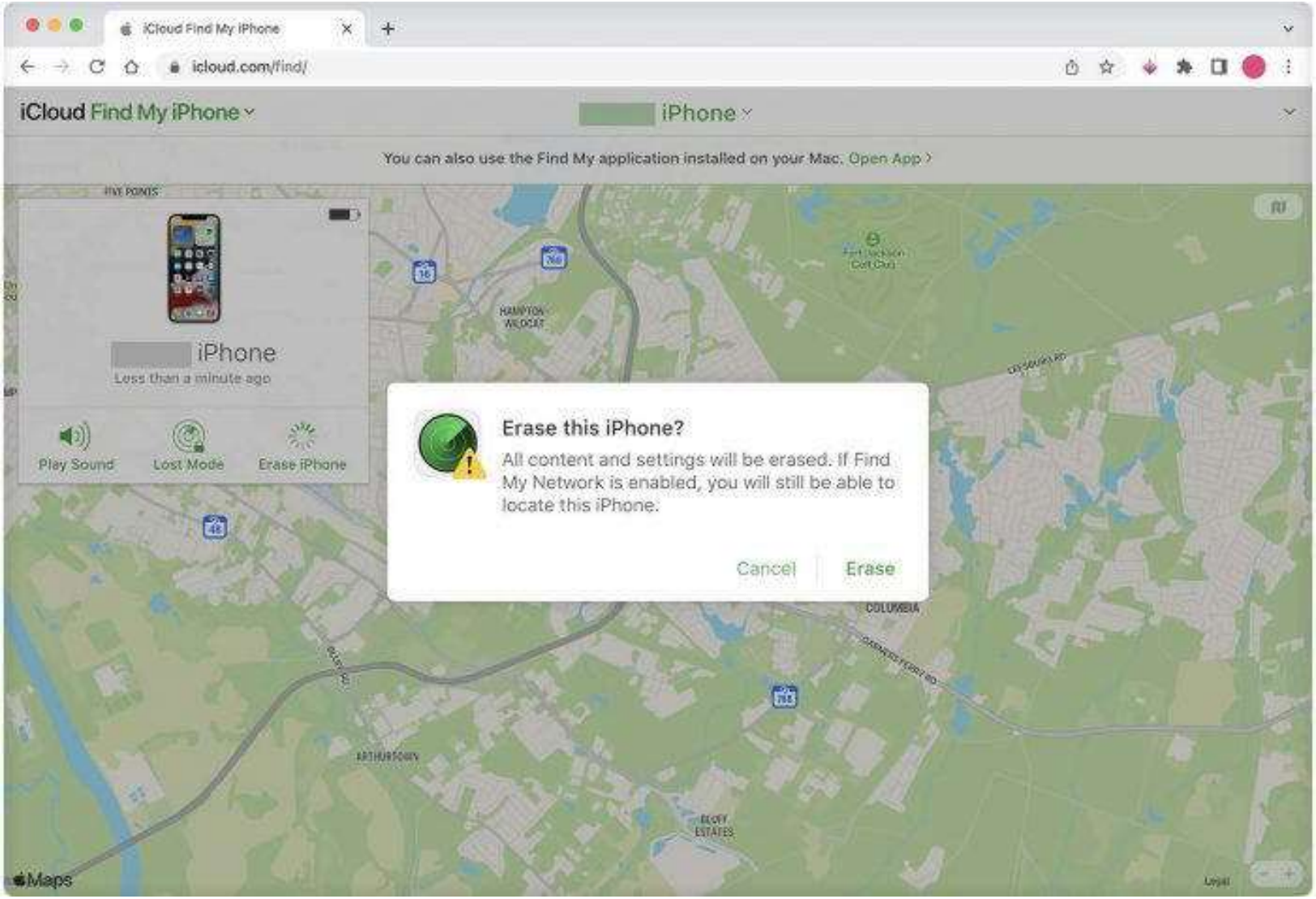
Using Finder

- Open Finder
- Plug iDevice into Mac via USB
- iDevice in recovery mode
- Update or Restore “Restore”
- Agree *Terms and Conditions*


John's iPhone
Favorites
iCloud
Locations
John's iPhone
Macintosh HD
Network
Tags
John's iPhone
iPhone 12 Pro · 100.56 GB (88.49 GB Available) · 100%
Manage Storage...
General
Music
Movies
TV Shows
Podcasts
Audiobooks
Books
Photos
Files
Info
Software: iOS 15.1
Your iPhone software is
to date. Your
ac will automatically check for an
update again on 10/27
1.
Check for Update
Restore iPhone...
Backups:
Back up your most imp
ant data
your iPhone to iCloud
Back up all of the data on your iPhone to this Mac
Encrypt local backup
Change Password...
Encrypted backups protect passwords and sensitive personal data.
Last backup to this Mac: Today, 9:41 AM
Back Up Now
Manage Backups...
Restore Backup...
Sync

Using "Find My"

- Use iCloud.com on Mac and sign in AppleID
- Open "Find MY"
- Click "All devices" Select iDevice to unlock
- "Erase iPhone"
- Process begins when desired iDevice connected to a network


iCloud Find My iPhone
icloud.com/find/
iCloud Find My iPhone
iPhone
You can also use the Find My application installed on your Mac. Open App
iPhone
Less than a minute ago
Play Sound
Lost Mode
Erase iPhone
Erase this iPhone?
All content and settings will be erased. If Find My Network is enabled, you will still be able to locate this iPhone.
Cancel
Erase
Maps

Unlock iDevice

- Third Party apps?
- OR ???
- Unlock an iPhone without a passcode by doing the following:

- Swipe down from the top to open the Control Center.
- Turn off Wi-Fi, Bluetooth and cellular data. Turn on Airplane Mode.
- Open the calculator.
- Turn the phone sideways to open the scientific calculator.
- Type a period.
- Tap In.
- It will say Error.
- Swipe up and the iPhone is unlocked.

- Fleet of consumer-grade spyware apps
- A common and disguised source
- Well built apps with hiding features
- BUT source “hacked” and list of devices obtained
- An app to search this data to see if your device has/has spyware

- Just provide your devices uniquely identifiable settings

Android TheTruthSpy lookup tool

- Ever want to be a presenter??

Presenter???

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

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com