Sun City Computer Club

Cyber Security SIG

January 20, 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

- Kevin Jacob Jenkinson 44 years
- Vaccinated
- Isolated

COVID can be very serious

- Ever want to be a presenter??

Presenter???

Current Issues

- Fake iPhone shutdown
  block shutdown Fake powered off screen
  goal – persistence
- MacOS malware attacks increasing
  Browser & browser plugins
  Attack the user
- FTC – legal action for log4j mitigation
  notification via blog
- Honda Y2K22 bug
- Chrome 97 – 37 security issues
- Chromium based browsers to follow?
- Hacker "full control" of 24 Teslas
- USB drive via postal mail?
  acts as keyboard to PowerShell & malware

- Microsoft Emergency OOB patch
- Windows 10 & 11 and 7 SP1
- https://sccccyber.blogspot.com/2022/01/microsoft-windows-emergency-update.html
- Yeahbut Windows 365 still unpatched

- Not completely anonymous
- Not too complicated
- Not totally secure
- Not only for illegal activity
- Not significant slowdown
- Not all the same

VPN

Hawai'i Department of Transportation

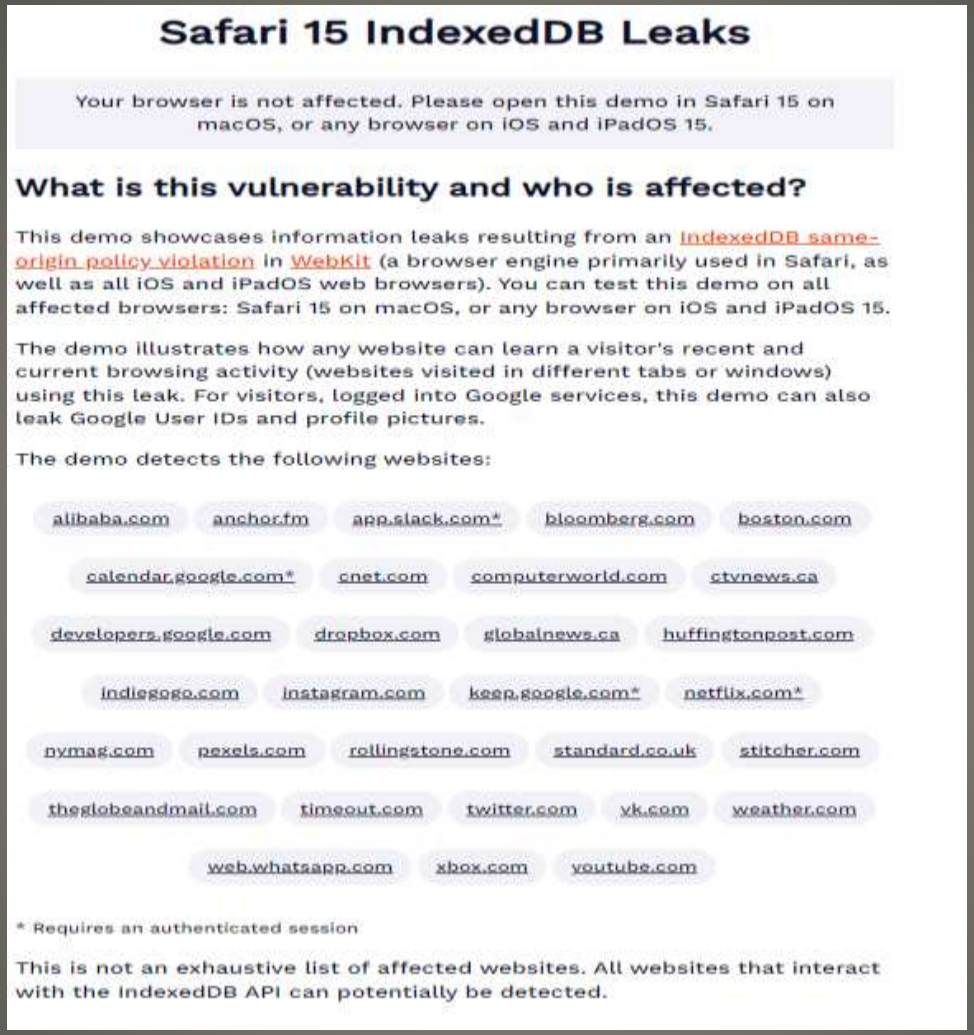
Current Issues

- Windcrest, Texas (Bexar county)
  Traffic ticket to your phone
  No Pull over
- Hack the pentagon Log4j
- DHS “us too”
- Crowdsourcing

- Open Source Software Security Summit
  11 Federal agencies
- IRS require selfies for Online access

- WordPress
- Safari or ANY browser in iOS iPadOS

- Crypto.com accounts hacked few details
- NSA expansion of role for government cyber security
- Google Play Games for PC Windows Beta
- Microsoft Activision acquisition



Safari 15 IndexedDB Leaks

Your browser is not affected. Please open this demo in Safari 15 on macOS, or any browser on iOS and iPadOS 15.

What is this vulnerability and who is affected?

This demo showcases information leaks resulting from an IndexedDB same-origin policy violation in WebKit (a browser engine primarily used in Safari, as well as all iOS and iPadOS web browsers). You can test this demo on all affected browsers: Safari 15 on macOS, or any browser on iOS and iPadOS 15.

The demo illustrates how any website can learn a visitor's recent and current browsing activity (websites visited in different tabs or windows) using this leak. For visitors, logged into Google services, this demo can also leak Google User IDs and profile pictures.

The demo detects the following websites:

alibaba.com anchor.fm app.slack.com* bloomberg.com boston.com

calendar.google.com* cnet.com computerworld.com ctvnews.ca

developers.google.com dropbox.com globalnews.ca huffingtonpost.com

indiegogo.com instagram.com keep.google.com* netflix.com*

nymag.com pexels.com rollingstone.com standard.co.uk stitcher.com

theglobeandmail.com timeout.com twitter.com vk.com weather.com

web.whatsapp.com xbox.com youtube.com

* Requires an authenticated session

This is not an exhaustive list of affected websites. All websites that interact with the IndexedDB API can potentially be detected.

Safari 15 IndexedDB leaks

Microsoft Patch Tuesday

- 97 vulnerabilities Windows
- 28 vulnerabilities Edge
- Then an out-of-band update to the update
- https://sccccyber.blogspot.com/2022/01/microsoft-windows-emergency-update.html
- Patch Tuesday Oracle, Juniper, Citrix, Cisco
- AND Apple 15.2.1 HomeKit bug & ??

Router Firmware updates

- Routers

  Netgear, TP-Link, Tenda, EDiMAX, D-Link, Western Digital

  KCode service at WAN interface

  Pwn2Own

- Limiting access to private networks
  Private Network Access PNA
  Cross-Origin access control
  External site – request access to router
  Appears to come from user browser
  INSIDE the LAN

Chrome

Current Issues

- iOS Private Relay blocked T-Mobile/Sprint cellular data

Your cellular plan doesn't support iCloud Private Relay. With Private Relay turned off, this network can monitor your internet activity, and your IP address is not hidden from known trackers or websites.

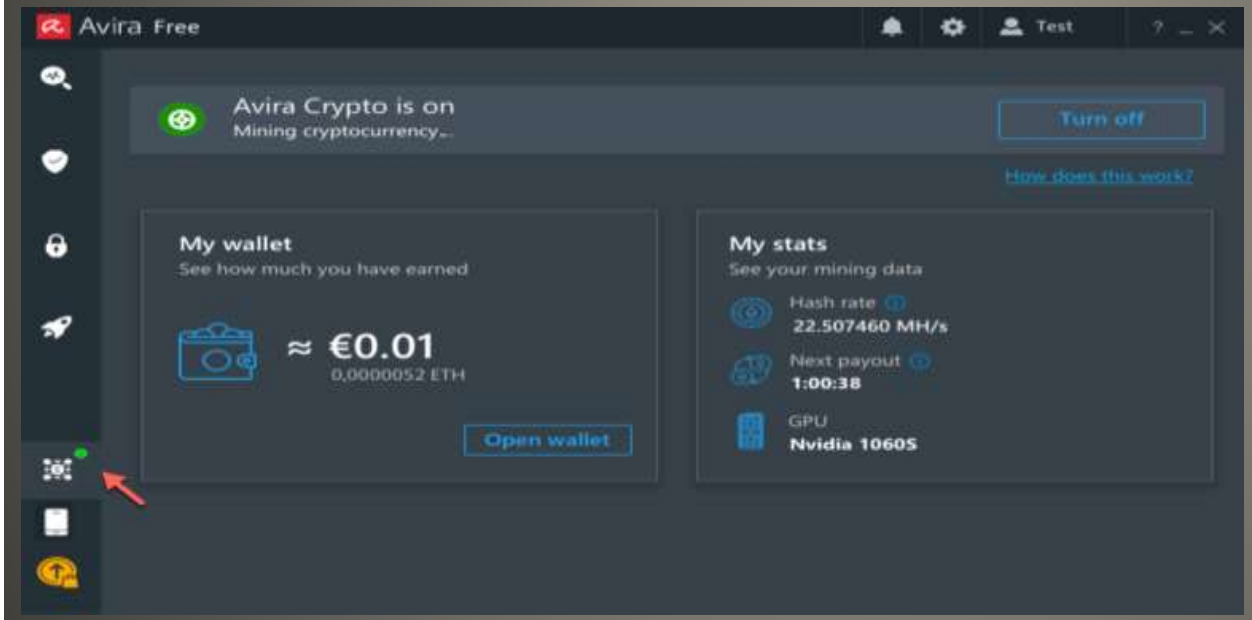
Password Managers

- LastPass attack
- Password vault Master password
- Generating strong passwords
  lessen brute force
  BUT that strong password is known to the password manager
- Zero knowledge
- BUT social engineering - account takeover
- MFA Multi Factor Authentication
- Keyloggers
- Browsers

- Cloud vs local vault
- Additional features
- RESEARCH

Password Managers

- *Norton Crypto*
  crypto currency miner
  with commissions
- AND Avira Antivirus



Norton 360

- 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