

Sun City Computer Club

Cyber Security SIG

August 19, 2021

**Questions, Comments, Suggestions welcomed at
any time**

Even Now

- Audio recording of this session as MP4 file
- Audio recording available at link shown above

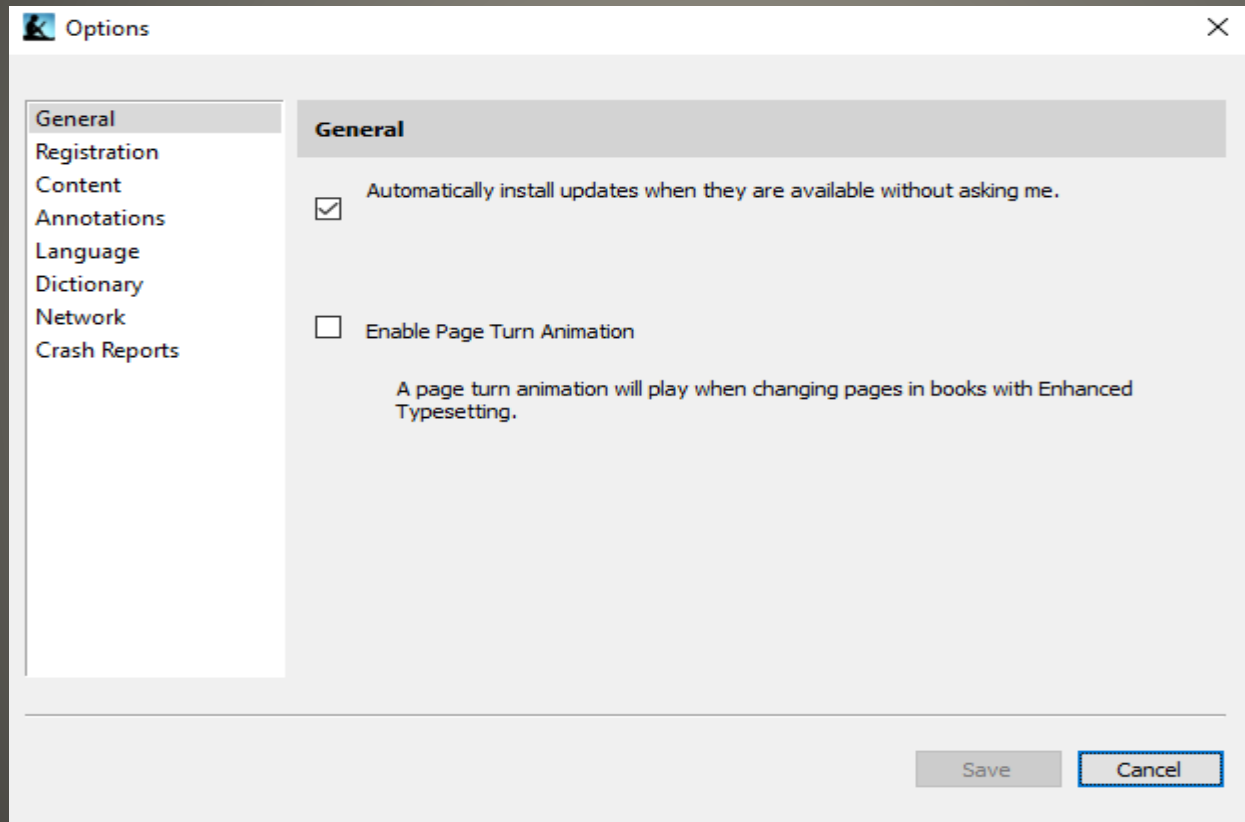
Audio Recording In Progress

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

| | |
|--|---|
| S | SeniorAdvisor Data Breach Published - Aug 12 |
| M | MacOS Big Sur 11.5.2 released today August 11-2021 Published - Aug 11 |
| A | Apple updates 26-July-2021 Published - Jul 26 |
| D | D-Link router vulnerabilities - Patch available Published - Jul 20 |
|  | Summer of SAM Windows HIVE permission vulnerability Published - Jul 20 |
| I | iOS 14.7 released today 19-July-2020 Published - Jul 19 |
| F | Firefox Version 90 release Published - Jul 14 |
|  | US Presidential Exeurity Order 9-July-2021 Published - Jul 9 |
| M | Microsoft emergency patch for PrintNightmare released today July 6 Published - Jul 6 |
|  | Microsoft PowerShell PATCH ASAP Published - Jul 6 |
| W | Western Digital woes increase Published - Jul 6 |

News archive

- Kindle
- Kindle for PC



Current Issues

Settings

98% 8:59

Profiles & Family Library
Add profile, Manage profiles

Parental Controls

Accessibility
Vision & Hearing Settings

Device Options
Language, Time, Backup, Updates

Help
Fire Tablet Help, Contact us

Legal & Compliance

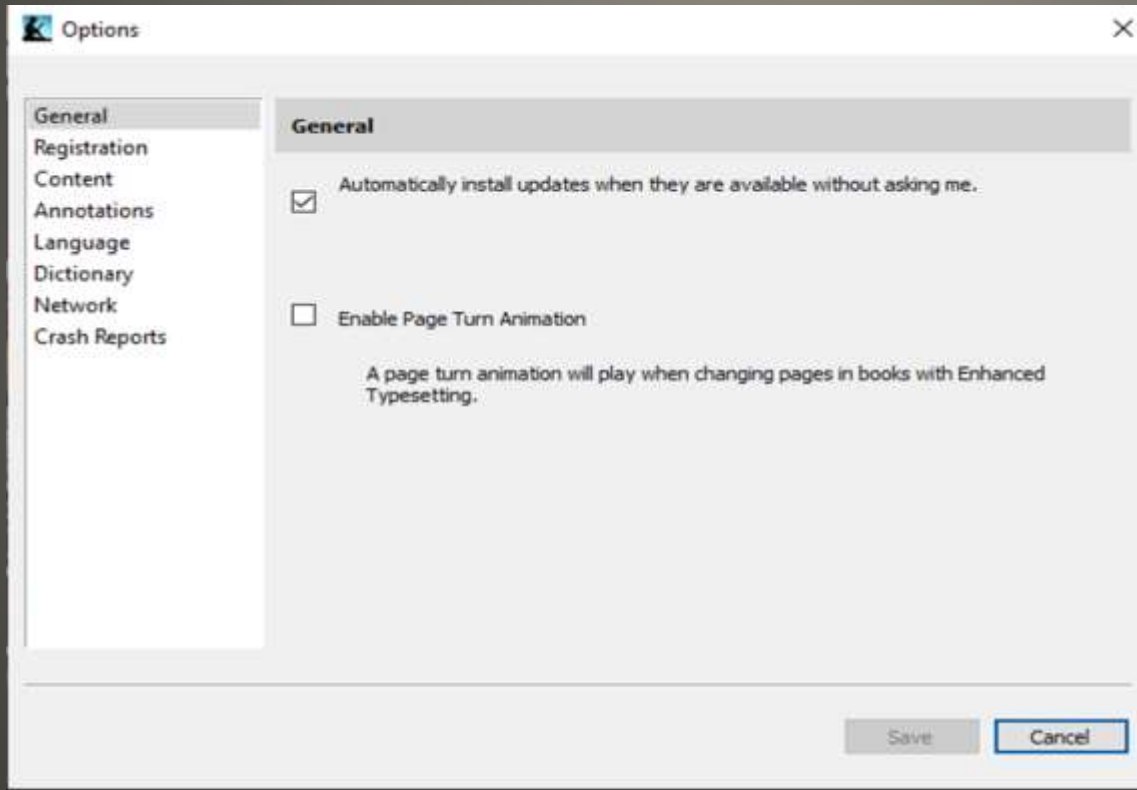
Device Options
Language, Time, Backup, Updates

Kindle Amazon Fire

- Recent discovered attack
- Load malicious content
- Take over Amazon account

Kindle update

- Version 1.30.0 59056
- Version 1.32.0 61109



Kindle for PC Update

- Facial recognition - *Master Faces*
- T-Mobile hack?
Assume your data
Identity theft – misnomer
Check “your location” for Internet service?
40Million+
Name, DOB, SSN, drivers license/ID, IMEI
- AI scale spear phishing
- Facebook end-to-end encryption
For messenger an end to an end
- PrintNightmare
- Crypto mining botnet modifies CPU – tuning
- NortonLifeLock and Avast merge
Symantec Broadcom Avira
- ASUS motherboard updates BIOS
207 different motherboard models

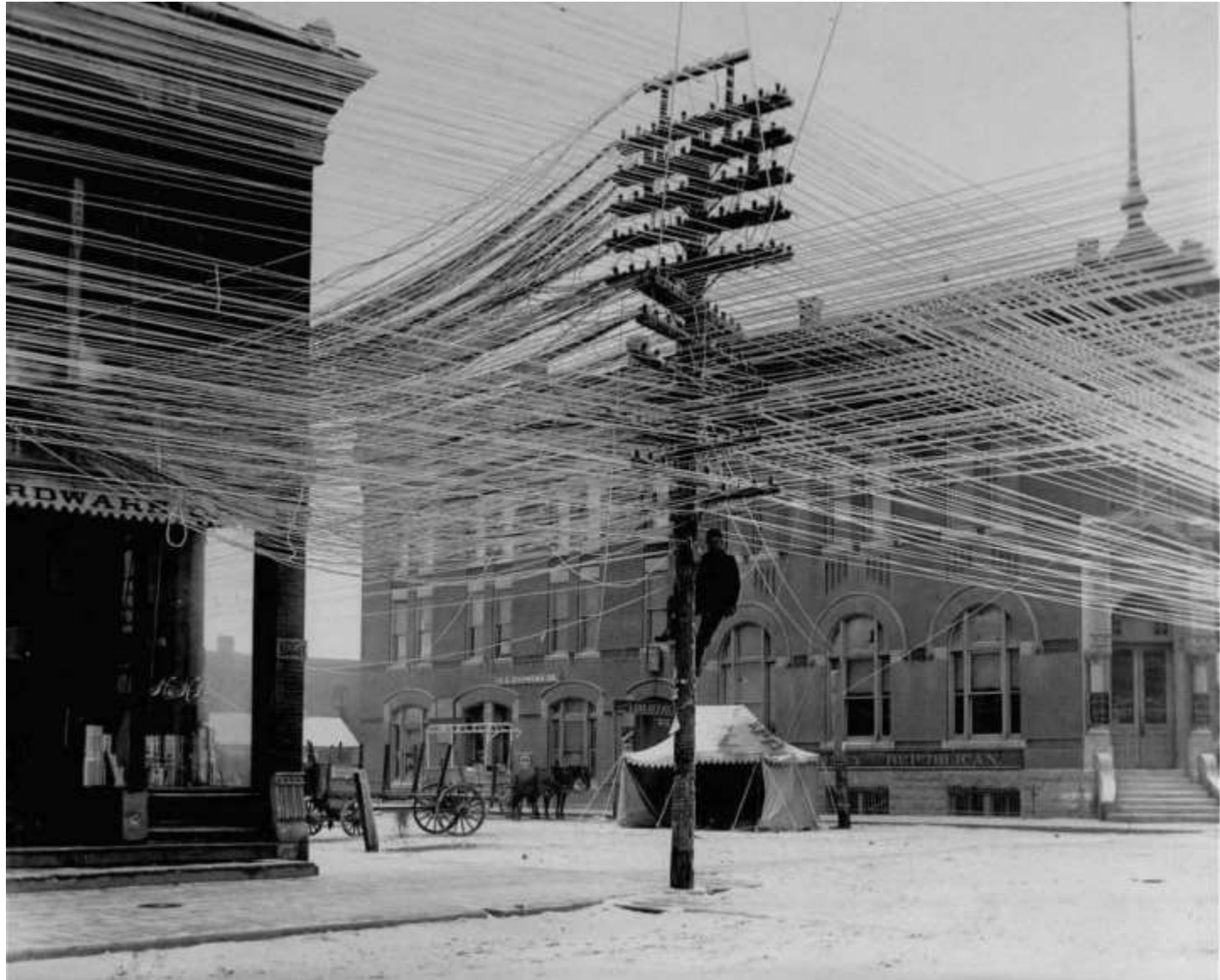
Current Issues

| Vendor | Router Device | Firmware Version |
|---------------------|------------------------------------|----------------------|
| ADB | ADSL wireless IAD router | 1.26S-R-3P |
| Arcadyan | ARV7519 | 00.96.00.96.617ES |
| Arcadyan | VRV9517 | 6.00.17 build04 |
| Arcadyan | VG7519 | 3.01.116 |
| Arcadyan | VRV9518 | 1.01.00 build44 |
| ASMAX | BBR-4MG / SMC7908 ADSL | 0.08 |
| ASUS | DSL-AC88U (Arc VRV9517) | 1.10.05 build502 |
| ASUS | DSL-AC87VG (Arc VRV9510) | 1.05.18 build305 |
| ASUS | DSL-AC3100 | 1.10.05 build503 |
| ASUS | DSL-AC68VG | 5.00.08 build272 |
| Beeline | Smart Box Flash | 1.00.13_beta4 |
| British Telecom | WE410443-SA | 1.02.12 build02 |
| Buffalo | WSR-2533DHPL2 | 1.02 |
| Buffalo | WSR-2533DHP3 | 1.24 |
| Buffalo | BBR-4HG | |
| Buffalo | BBR-4MG | 2.08 Release 0002 |
| Buffalo | WSR-3200AX4S | 1.1 |
| Buffalo | WSR-1166DHP2 | 1.15 |
| Buffalo | WXR-5700AX7S | 1.11 |
| Deutsche Telekom | Speedport Smart 3 | 010137.4.8.001.0 |
| HughesNet | HT2000W | 0.10.10 |
| KPN | ExperiaBox V10A (Arcadyan VRV9517) | 5.00.48 build453 |
| KPN | VG7519 | 3.01.116 |
| O2 | HomeBox 5441 | 1.01.36 |
| Orange | LiveBox Fibra (PRV3399) | 00.96.00.96.617ES |
| Skinny | Smart Modem (Arcadyan VRV9517) | 6.00.16 build01 |
| SparkNZ | Smart Modem (Arcadyan VRV9517) | 6.00.17 build04 |
| Telecom (Argentina) | Arcadyan VRV9518VAC23-A-OS-AM | 1.01.00 build44 |
| TelMex | PRV33AC | 1.31.005.0012 |
| TelMex | VRV7006 | |
| Telstra | Smart Modem Gen 2 (LH1000) | 0.13.01r |
| Telus | WiFi Hub (PRV65B444A-S-TS) | v3.00.20 |
| Telus | NH20A | 1.00.10debug build06 |
| Verizon | Fios G3100 | 1.5.0.10 |
| Vodafone | EasyBox 904 | 4.16 |
| Vodafone | EasyBox 903 | 30.05.714 |
| Vodafone | EasyBox 802 | 20.02.226 |

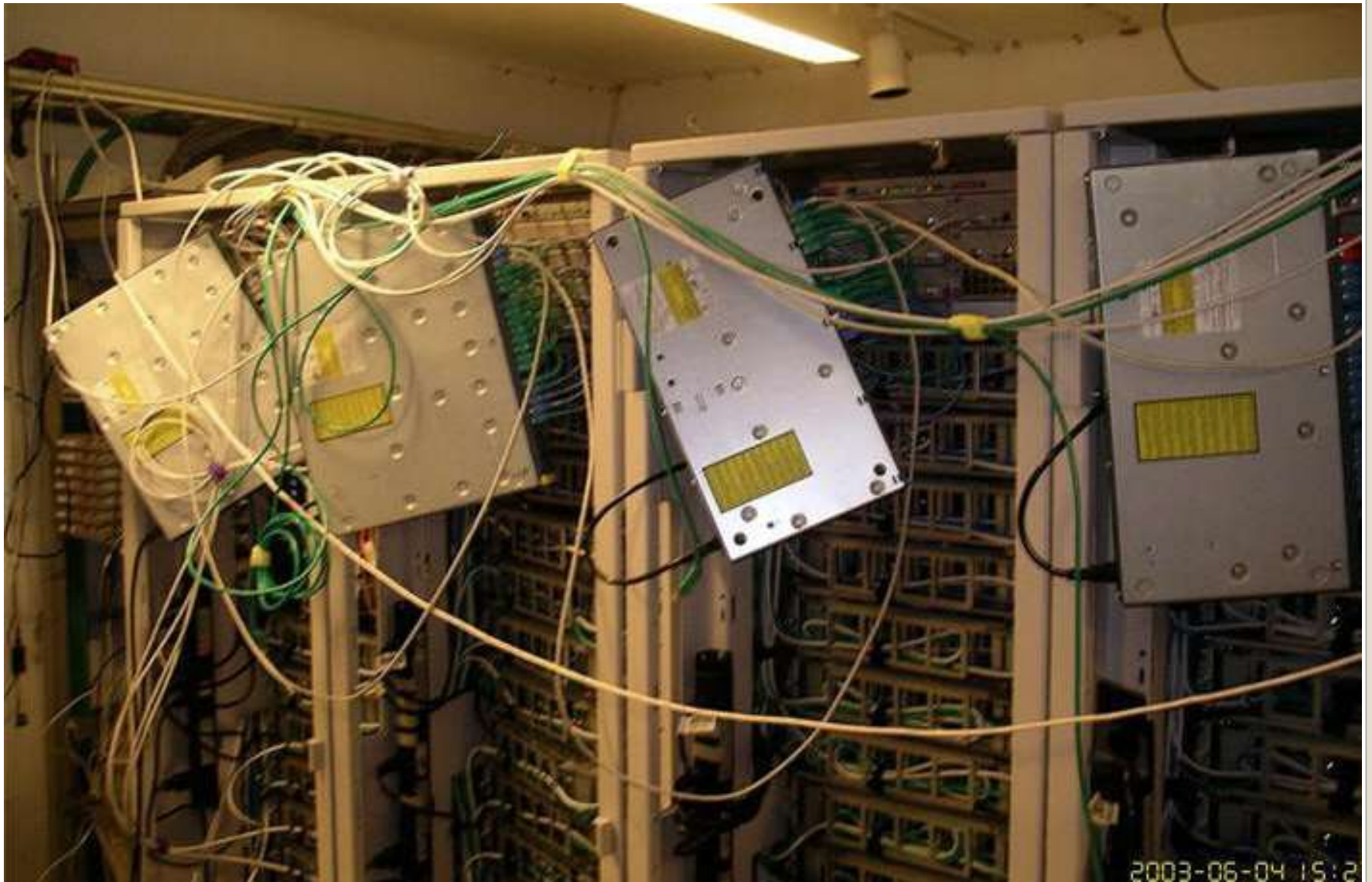
Miari botnet

- 7 year Suddenlink customer
- Asus cable modem
- One upgrade attempt
- My complex environment
- Weeklong cable modem firmware update
- Replacement cable modem via postal mail
- Home network gateway
- Turn it all in
- Netgear replacement
- Unable to have landline re-provisioned

My Suddenlink adventures







2003-06-04 15:2

- DEF CON / BLACKHAT 2021

“There’s a crack in the foundation of Internet of Things (IoT) security, one that affects 35 billion

devices worldwide. Basically, every IoT device with a hardware random number generator (RNG)

contains a serious vulnerability whereby it fails to properly generate random numbers, which undermines security for any upstream use.”

IoT RNG

- Diffie Helman key agreement
- Each side generates random number
- Uses random number to generate “key”
- These “keys” exchanged
- Combine with the side’s random number
- Yields same symmetric key
- Eavesdropper protection
Unless

IoT RNG

- Software generated random number
Never random unless seeded
seeding takes resources – including time
- IoT devices resource constrained
- Return value from hardware RNG
NOT CHECKED
Pervasive across every SDK and IoT OS
Partial entropy Uninitialized memory
NULL
- Advanced military grade encryption
with null crypto key(s)

IoT RNG

- Pulse Secure VPN
Pulse CONNECT Secure appliance
Overwrite patches
- et tu Cisco
- ANY VPN *can* have your secrets
- NicheStack TCP/IP stack OT
Widely deployed for 25 years
Shodan scan HTTP, FTP, SSH, telnet
Nation state's back pocket of vulnerabilities
Hackers are Internet's immune system

Current Issues

Windows Update



Updates available

Last checked: Today, 12:01 PM

Windows Malicious Software Removal Tool x64 - v5.92 (KB890830)

Status: Installing - 0%

2021-08 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5005033)

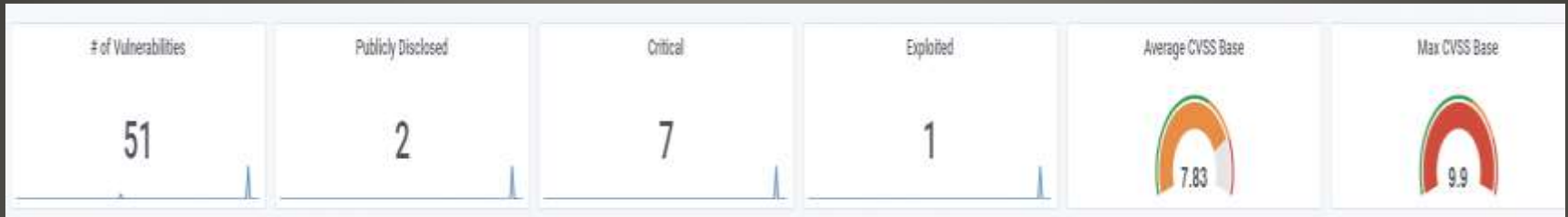
Status: Downloading - 0%

✓ Quality Updates (24)

[2021-08 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems \(KB5005033\)](#)

Successfully installed on 8/10/2021

Microsoft Patch Tuesday



[August 10, 2021—KB5005033 \(OS Builds 19041.1165, 19042.1165, and 19043.1165\) \(microsoft.com\)](#)

Microsoft Patch Tuesday

- TCP/IP Remote Code Execution Vulnerability
CVE-2021-26424
Hyper-V triggered by IPv6 ping
- Windows Update Medic Service
CVE-2021-36984
No user interaction, low attack complexity
Actively being exploited
- Print Spooler
CVE-2021-36936
Patch to all versions, even Windows 7
- Windows LSA
CVE-2021-36942
Remote exploit, no user interaction, NTLM authenticate

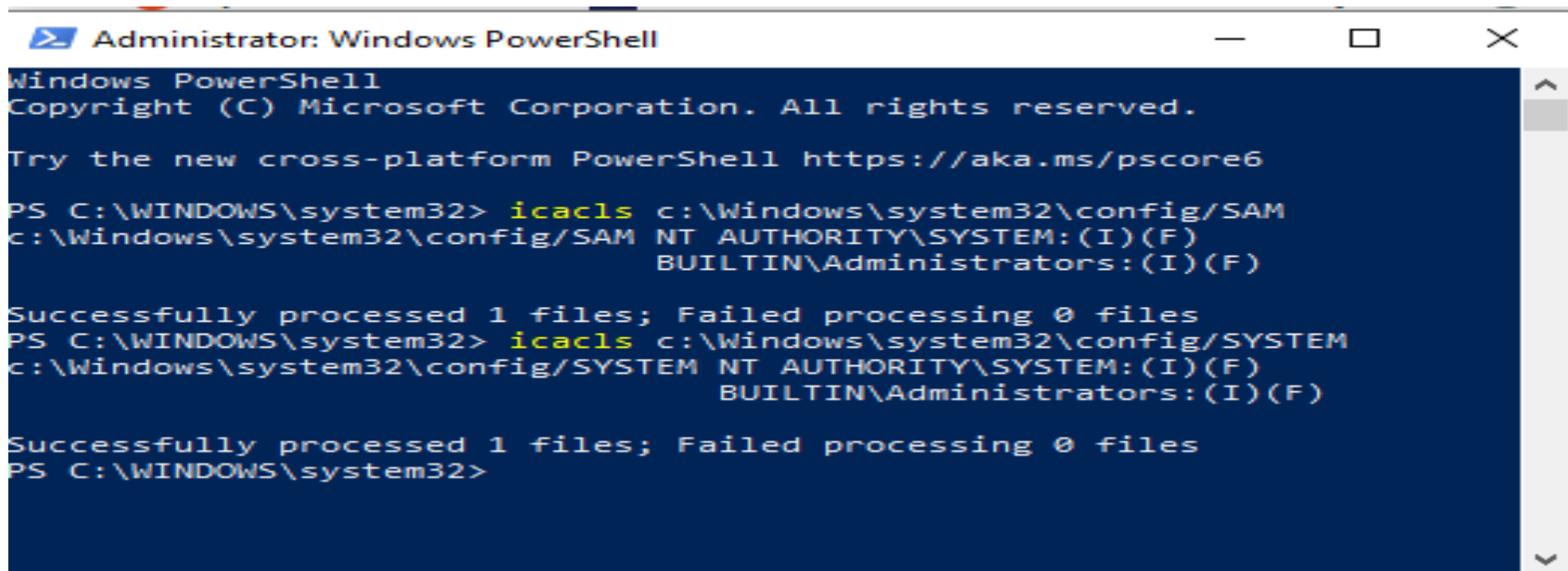
Microsoft Patch Tuesday

```
C:\Windows\system32>icacls c:\Windows\system32\config\SAM
c:\Windows\system32\config\SAM BUILTIN\Administrators:(I)(F)
                                NT AUTHORITY\SYSTEM:(I)(F)
                                BUILTIN\Users:(I)(RX)
                                APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                                APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
```

Successfully processed 1 files; Failed processing 0 files

```
C:\Windows\system32>icacls c:\Windows\system32\config\SYSTEM
c:\Windows\system32\config\SYSTEM BUILTIN\Administrators:(I)(F)
                                    NT AUTHORITY\SYSTEM:(I)(F)
                                    BUILTIN\Users:(I)(RX)
                                    APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                                    APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
```

Successfully processed 1 files; Failed processing 0 files



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a dark blue background with white text. The text content is as follows:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> icacls c:\Windows\system32\config\SAM
c:\Windows\system32\config\SAM NT AUTHORITY\SYSTEM:(I)(F)
                                BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\WINDOWS\system32> icacls c:\Windows\system32\config\SYSTEM
c:\Windows\system32\config\SYSTEM NT AUTHORITY\SYSTEM:(I)(F)
                                    BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\WINDOWS\system32>
```

Yeah, BUT Windows 11

- Layered Group Policy feature
 - Types of devices allowed
- Parallels Desktop 17
 - Windows 11 on Intel and M1 based MACs
- Oeclassic
 - Outlook Express Windows live Mail replacement
 - Recent certificate registration based in Croatia
 - Free version, then credit card
- Outlook client Outlook WEB Outlook extension
 - Active development by Microsoft

- NO Please NO

Windows 11 get yours here

Manage Patches i



Available Hidden

| | NAME | ↑ | PRODUCT | IMPORTANCE |
|-------------------------------------|--|---|----------------------------|------------|
| <input checked="" type="checkbox"/> | Oracle VirtualBox 6.1.20 for Windows (See Notes) | | VirtualBox | Critical |
| <input checked="" type="checkbox"/> | PuTTY 0.75 for Windows (See Notes) | | PuTTY | Critical |
| <input checked="" type="checkbox"/> | Wireshark 3.4.6 for Windows (See Notes) | | Wireshark | Critical |

Install

Vipre

- Settings -> Update & Security -> Windows Security

Windows Security

Windows Security is your home to view and manage the security and health of your device.

Open Windows Security

Protection areas



Virus & threat protection
No actions needed.



Account protection
No actions needed.



Firewall & network protection
No actions needed.



App & browser control
No actions needed.



Device security
No actions needed.

PUP PUA defense settings



Reputation-based protection

These settings protect your device from malicious or potentially unwanted apps, files, and websites.

Check apps and files

Microsoft Defender SmartScreen helps protect your device by checking for unrecognized apps and files from the web.

On

SmartScreen for Microsoft Edge

Microsoft Defender SmartScreen helps protect your device from malicious sites and downloads.

On

Potentially unwanted app blocking

Protect your device from low-reputation apps that might cause unexpected behaviors.

On

Block apps

Block downloads

• edge://flags

Edge | edge://flags

Search flags

Reset all

Experiments 94.0.972.0

WARNING: EXPERIMENTAL FEATURES AHEAD! By enabling these features, you could lose browser data or compromise your security or privacy. Enabled features apply to all users of this browser. If you are an enterprise admin you should not be using these flags in production.

Available Unavailable

- Automatic HTTPS**
Enables support for Automatic HTTPS, which switches connections to websites from HTTP to HTTPS. The feature can then be turned on/off or further configured at <edge://settings/privacy>. – Mac, Windows, Linux, Android
[#edge-automatic-https](#) Enabled
- Super Duper Secure Mode**
Disables the JIT and enables new security mitigations to provide a more secure browsing experience. – Windows
[#edge-enable-super-duper-secure-mode](#) Enabled

Edge Super Duper Secure Mode

- *I want that*
- Performance vs increase in security?
- No Chrome Just-In-Time component
- Half of Chrome's vulnerabilities JIT

Edge Super Duper Secure Mode

- “I don’t have anything to hide. I just don’t have anything I want you to see.”

Privacy

- Child Sexual Abuse Material
- Stop CASM being loaded into iCloud
- How?

Image hashing and known image comparison performed on user's device

Hash fingerprint non-reversible

NeuralHash similar images same NeuralHash

National Center for Missing and Exploited Children report

- Algorithm existed since iOS 14.3
- Tolerates resizing & compression
- Not cropping or rotations

Apple CASM Detection

- Tools to protect children from sending and/or receiving sexually explicit images in ANY Apple messaging
- Child accounts setup by parents
- Blurred image
- Database image analysis
- Ask OK to view or send
- Under 12 years – parents warned
- 13-17 warning, no parental notification
- Family account AND parental opt-in

Apple Communication Safety in Messages

- Virtual desktop service
- Part of Microsoft 365
- Cloud PC Dedicated to a user
- Fixed price – No consumption pricing
- Not Azure

Windows 365

- Fast Internet download (1.3Gb/s – 230 Mb/s)
- Work on large content
- MINIMAL PROTECTIONS
- Account & Passphrase
- Easy to take over
- Use Multi Factor Authentication
- Microsoft Authenticator or
- It's just out there

Windows 365

- Intent – Criminals and terrorist
- Discovered – activists, journalist, government, business
- NSO group – Israel based
- NSO hacked – installation base leaked
- 50,000 phone numbers
- Other companies also provide similar
- Jeff Bezos, Jamal Khashoggi
- Stealthy installation & surveillance
- Camera, Microphone

Pegasus

- Amnesty International
Mobile Verification Toolkit (MVT)
PC/MAC based analysis of iPhone & Android

Pegasus



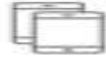
Quick Transfer



Back Up



Restore a Backup



Transfer to another Device



Manage Apps



Export All Data



Options



Update iOS



Reinstall iOS



Show Device Console



Supervision



Export Raw Files



Detect Spyware

- Microsoft/Libre Office Document
- Spoofed sender
- Macro enable “trick”
- Macro enable set & forgot


Top Exploit - methodology

legal paper.08.04.2021.doc [Compatibility Mode] - Microsoft Word

Home Insert Page Layout References Mailings Review View

Clipboard Font Paragraph Styles Editing

Security Warning Macros have been disabled Options...



This document created in previous version of Microsoft Office Word.

To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"

Page: 1 of 1 Words: 15 Russian (Russian) 100%

- Spoofed sender (trust)
- Macro enabled or Macro “trick”
- Script

eMail attachments

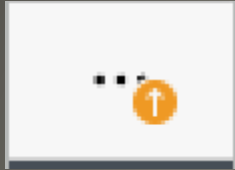
- Facebook blocks researchers
FTC privacy order?
- Apple
screen iMessage image attachments
Minor children
on-device screening
Child Sexual Abuse Material
- IoT RNG (Random Number Generator)
weaker
- Realtek chip vulnerability – well 12
65 vendors Asus, Belkin, D-Link, Netgear, ZTE,
Obscure supply chain -> attacks
Firmware patches issued
- Tetris Chinese espionage tool
Target Chinese dissidents
- Resignation problem – ransomware, data dump, etc.

Current Issues

- AdLoad 2017 -> Now
- Signed current Apple developer certificate
- Gatekeeper
- Xprotect signature bypass
- Apple "notarized"
- ADMINISTRATOR
- AdLoad - WEB site advertiser's fee
- Nuisance -> ??
- Additional protections – suites
- Practice good hygiene

Mac Attack





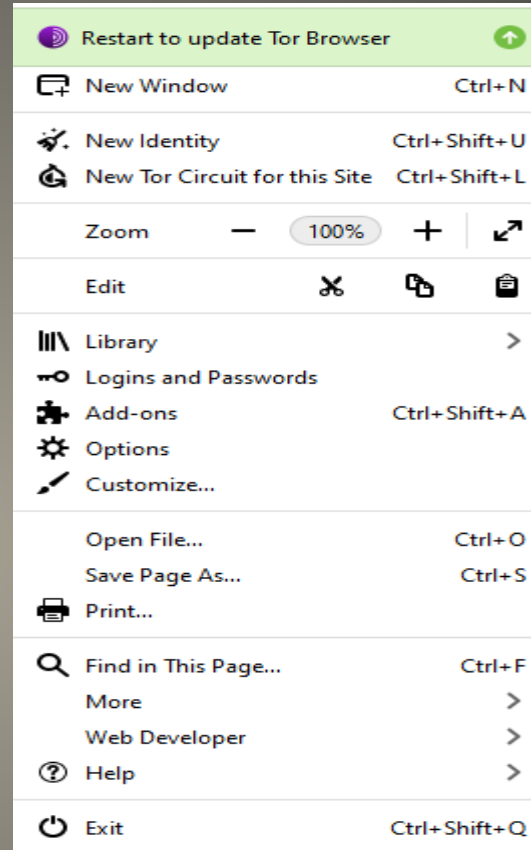
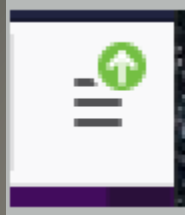
A new update is available

Microsoft Edge will be updated when you restart the browser.

Restart

Not now

Edge Update - Vivaldi



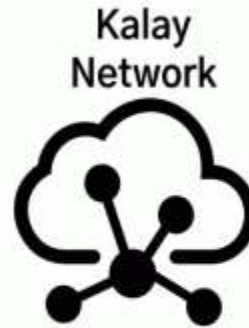
Tor Update

- ThroughTek Kalay IoT cloud
- Millions
- Video, surveillance, home automation
- View live feeds
- Take control for bot net
- ??
- CVE-2021-28372 Device impersonation
- Only UID needed

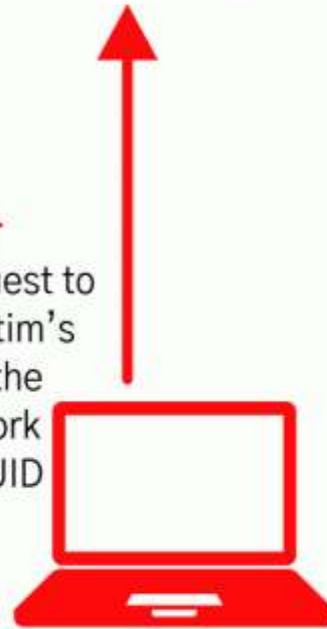
Kalay network



1. Camera sends a Kalay network registration request using its UUID



1. **Attacker**
spoofs request to register victim's camera on the Kalay network using its UUID



- Kalay security advisory

- If using ThroughTek SDK v3.1.10 and above, please enable AuthKey and DTLS (Datagram Transport Layer Security) to protect data in transit;
- If using ThroughTek SDK the older versions before v3.1.10, please upgrade library to v3.3.1.0 or v3.4.2.0 and enable AuthKey and DTLS.

[ThroughTek Kalay P2P SDK | CISA](#)

Kalay mitigation

- Data leaks
 - S3 buckets, open databases, SQL access
- Secure platforms
 - BUT customer awareness, customization
- Cloud provided VM (Virtual Machines)
- VMs connected via VPN (Virtual Private Network)

Cloud

- Losing market share
- Current version 91.0.1


Mozilla - Firefox


Strict

Stronger protection, but may cause some sites or content to break.

Firefox blocks the following:

- Social media trackers
- Cross-site cookies in all windows (includes tracking cookies)
- Tracking content in all windows
- Cryptominers
- Fingerprinters

 You will need to reload your tabs to apply these changes.

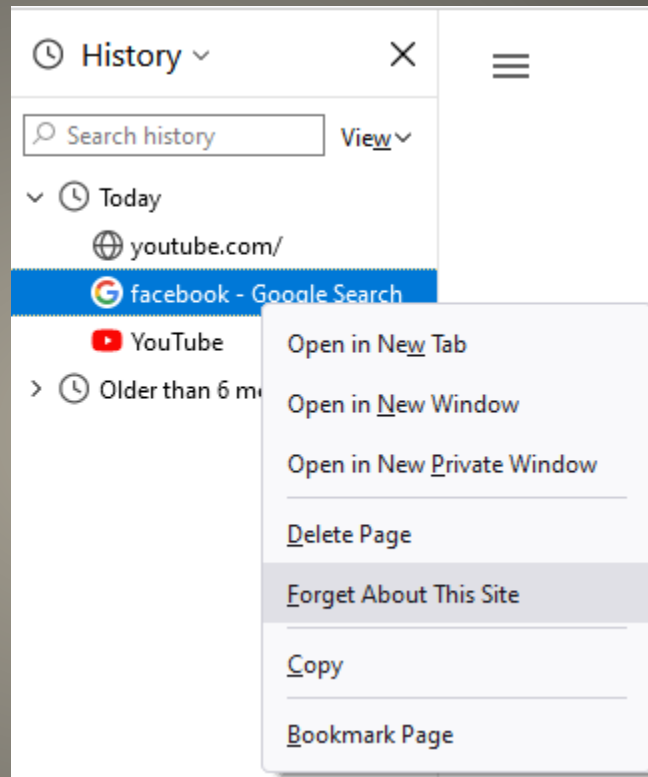
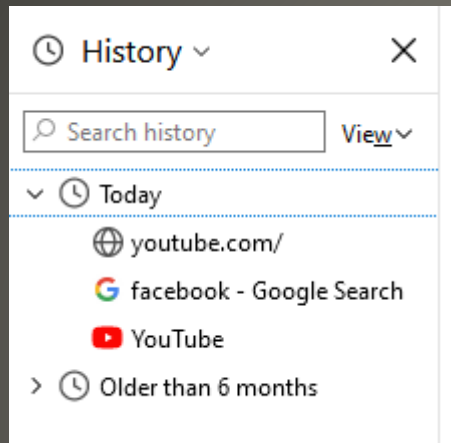
 [Reload All Tabs](#)

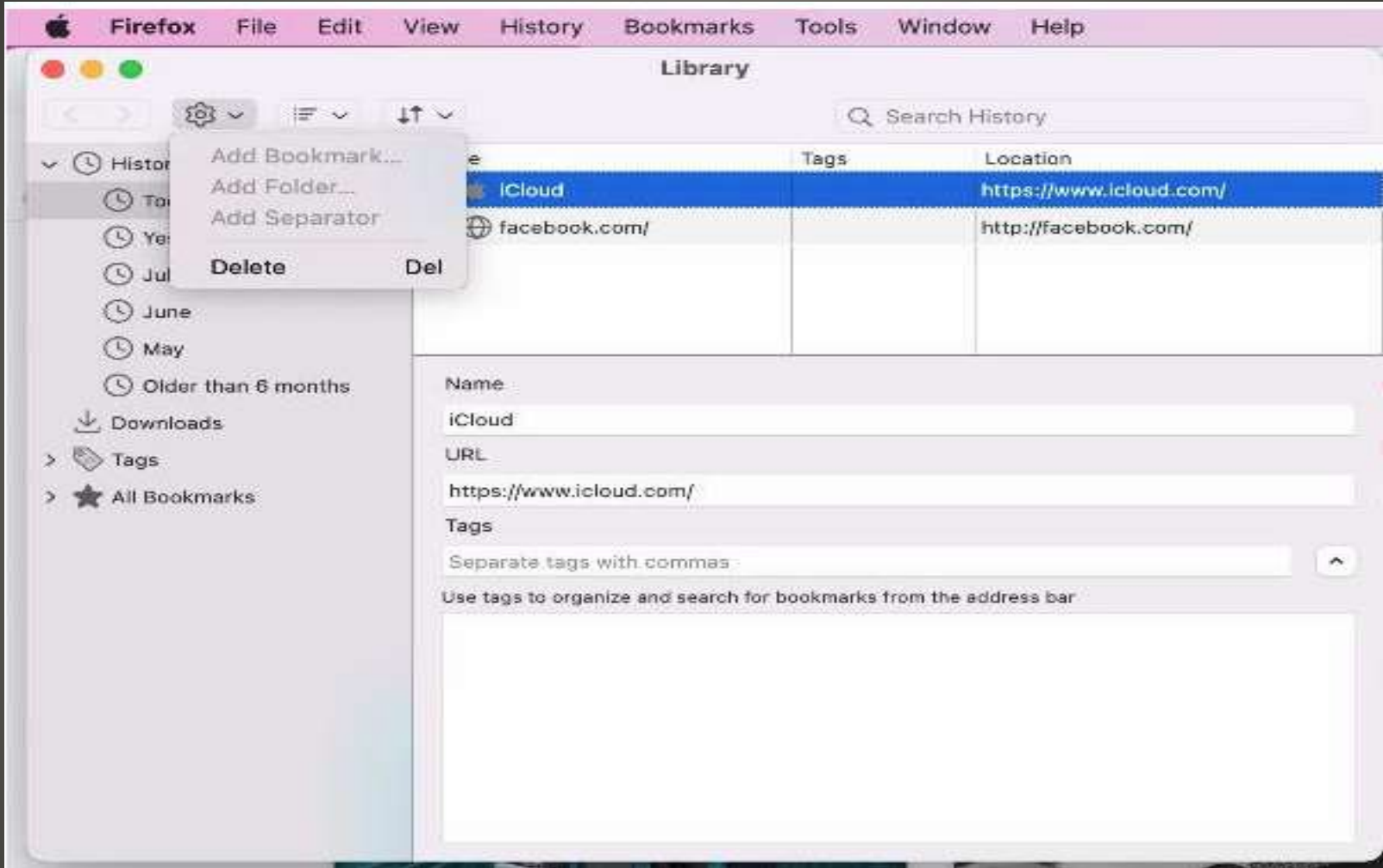
Heads up!

This setting may cause some websites to not display content or work correctly. If a site seems broken, you may want to turn off tracking protection for that site to load all content. [Learn how](#)

- Since Firefox version 86
- Cookies stored in SITE'S cookie jar
- yeahbut
 - keep your IDentity, preferences, caches, data to survive internet connectivity loss, history, settings, permissions, etc.
 - cross-site e.g. Facebook buttons
- AND THEN
 - Any and all data, history, cache, etc.
 - single repository - to be managed or deleted

Mozilla - Firefox





Firefox - MAC

- Current 14.1.2
- Beta 15.0

Safari

- 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