Sun City Computer Club

Cyber Security SIG

May 6, 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

Current Issues

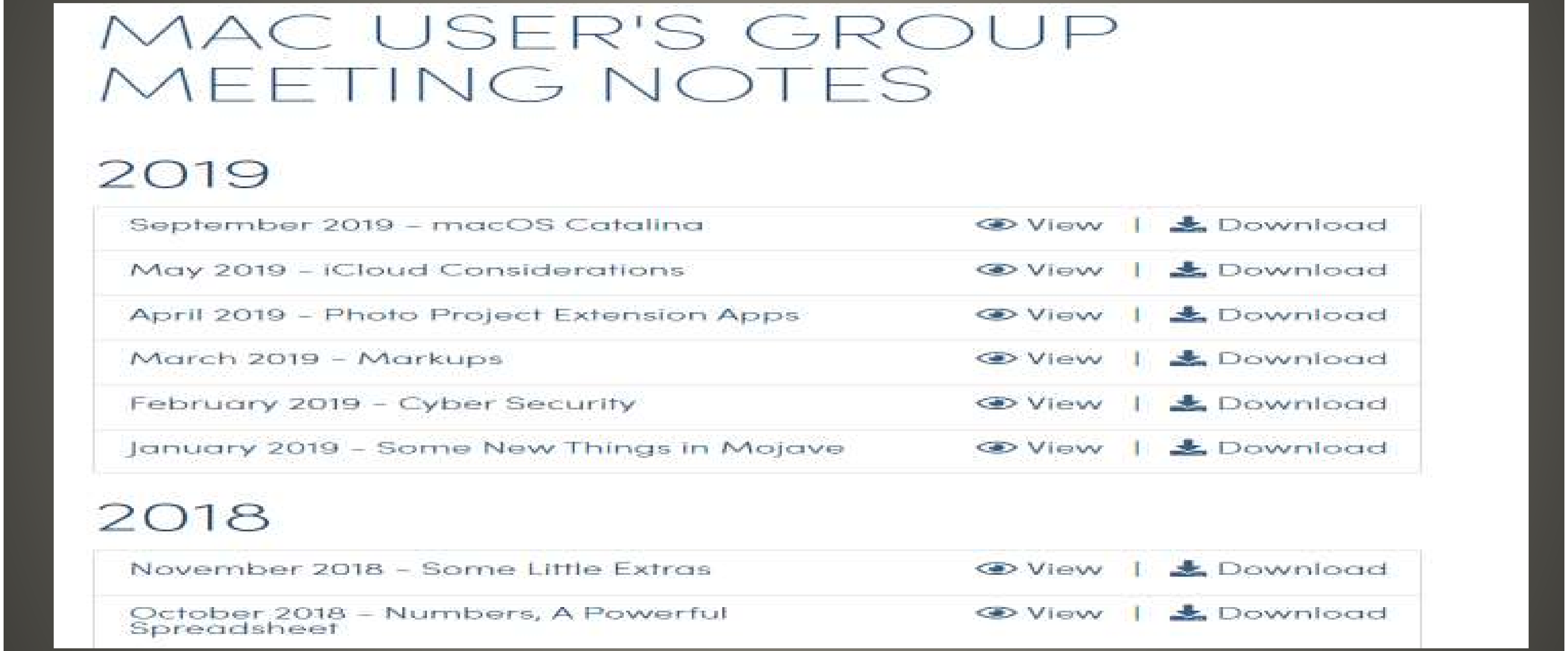
- SolarWinds
- Microsoft Exchange Server vulnerability
- COMB

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

GREAT increase of our Personal Information

Cyber Security SIG Special Alert

Sun City Texas Community Association File Library Mac User's Group Meeting Notes (sctexas.org)



MAC USER'S GROUP MEETING NOTES

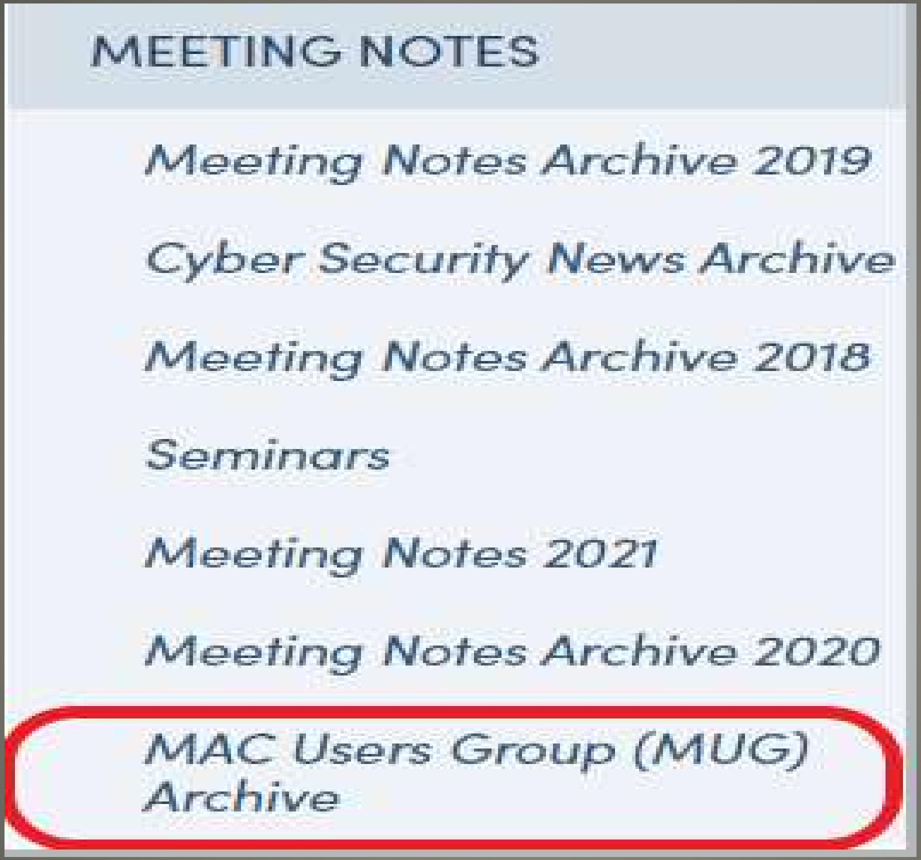
2019

September 2019 – macOS Catalina	View	Download
May 2019 – iCloud Considerations	View	Download
April 2019 – Photo Project Extension Apps	View	Download
March 2019 – Markups	View	Download
February 2019 – Cyber Security	View	Download
January 2019 – Some New Things in Mojave	View	Download

2018

November 2018 – Some Little Extras	View	Download
October 2018 – Numbers, A Powerful Spreadsheet	View	Download

MAC Users Group (MUG)



MEETING NOTES

Meeting Notes Archive 2019

Cyber Security News Archive

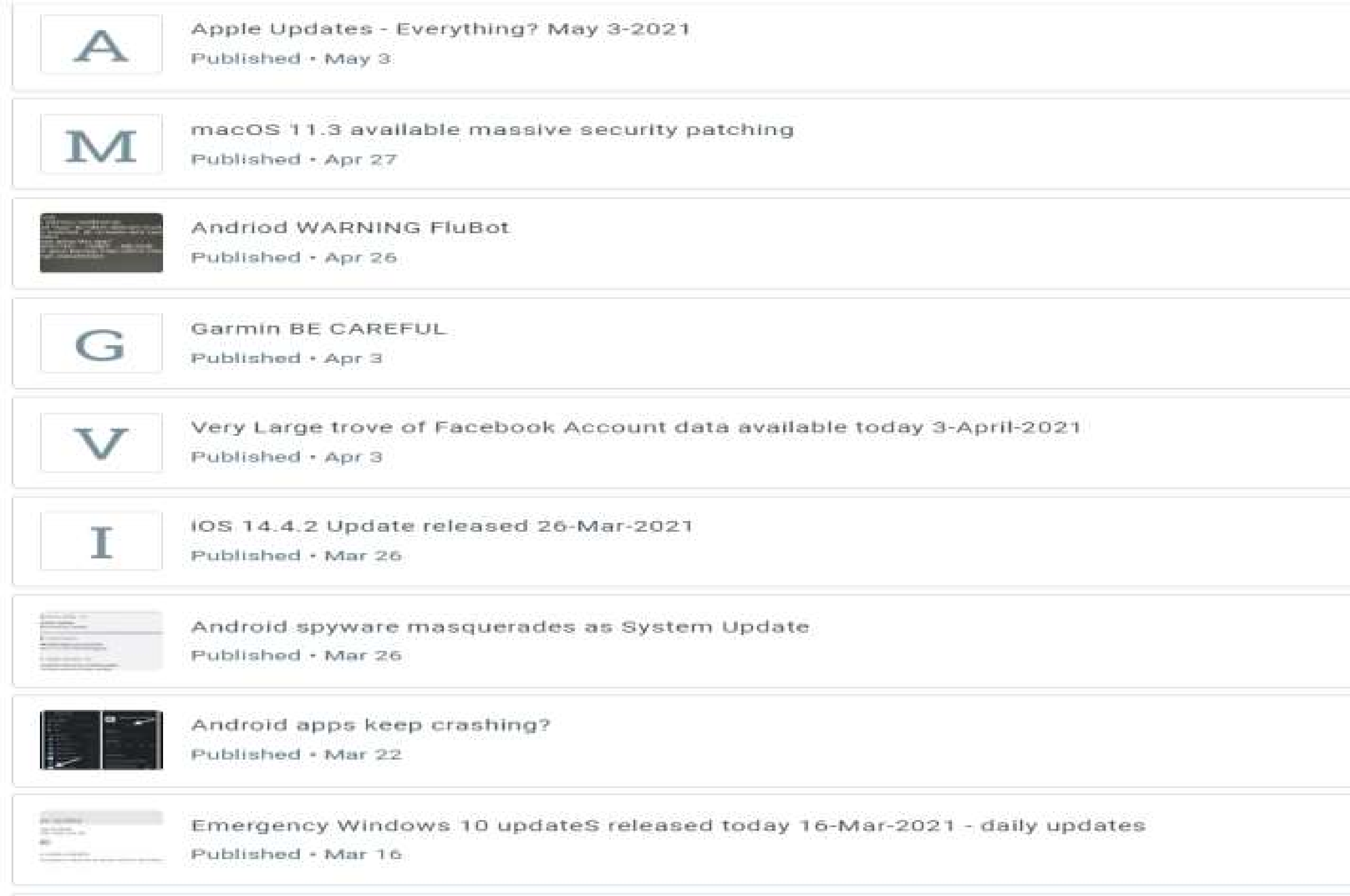
Meeting Notes Archive 2018

Seminars

Meeting Notes 2021

Meeting Notes Archive 2020

MAC Users Group (MUG) Archive



Apple Updates - Everything? May 3-2021
Published • May 3

macOS 11.3 available massive security patching
Published • Apr 27

Andriod WARNING FluBot
Published • Apr 26

Garmin BE CAREFUL
Published • Apr 3

Very Large trove of Facebook Account data available today 3-April-2021
Published • Apr 3

iOS 14.4.2 Update released 26-Mar-2021
Published • Mar 26

Android spyware masquerades as System Update
Published • Mar 26

Android apps keep crashing?
Published • Mar 22

Emergency Windows 10 updateS released today 16-Mar-2021 - daily updates
Published • Mar 16

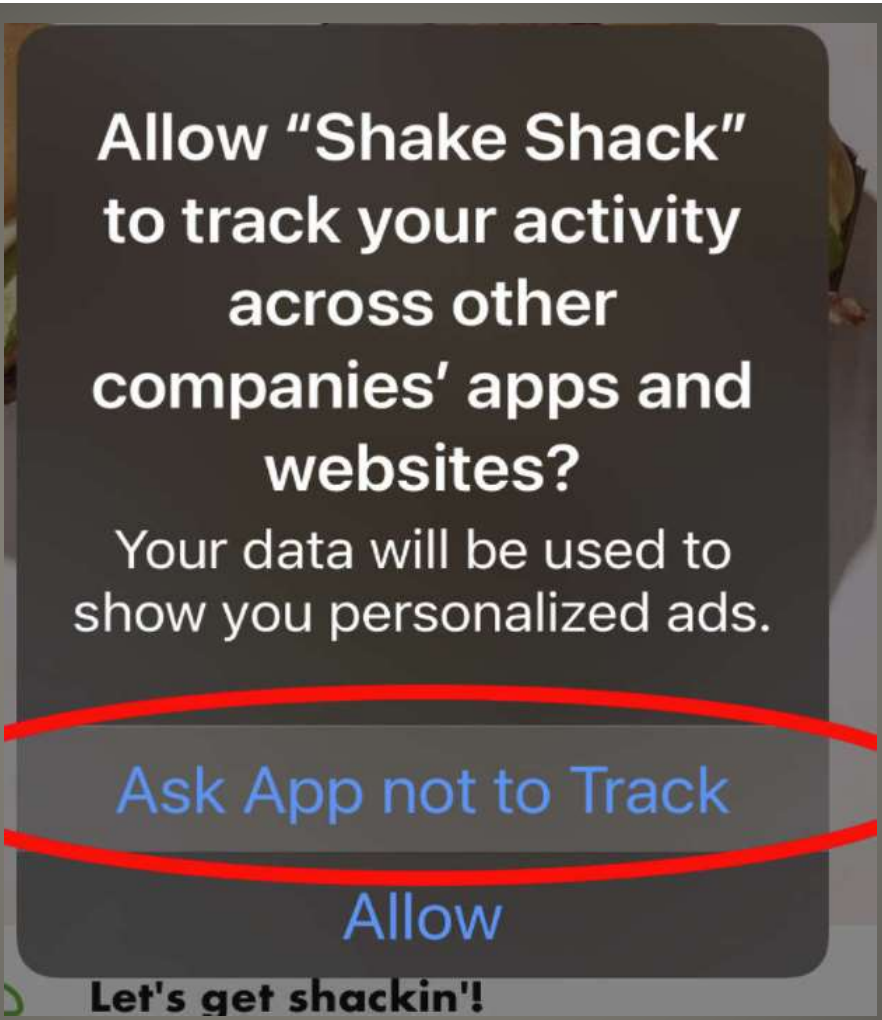
Cyber Security News Archive

Apple macOS

- macOS Update Big Sur 11.3
  Catalina and Mojave
  sneaky
  Gatekeeper – app registration
  Notarization – automated
  Application attributes
  metadata file *info.plist*
  simple script
  Massive effort to fool Apple’s vetting
  Remove application notarization
- macOS Update 11.3.1 Webkit

iDevices

- iOS 14.5.1 iPadOS 14.5.1 watchOS 7.4.1
- Older iPhones 12.5.3
- Not AppleTV

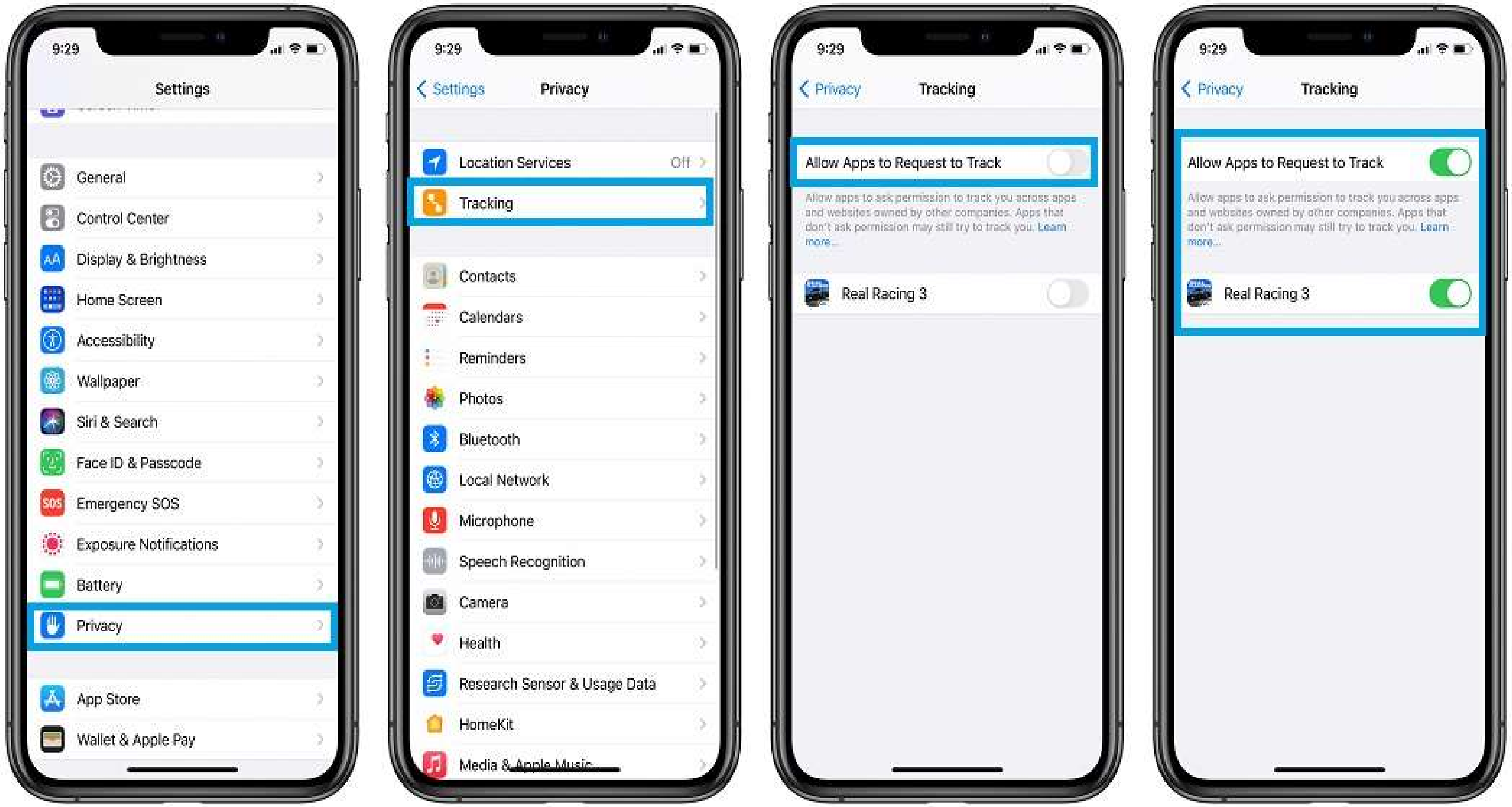


Allow “Shake Shack” to track your activity across other companies’ apps and websites?

Your data will be used to show you personalized ads.

iOS 14.5 iPadOS 14.5

- Settings -> Privacy



Allow Apps to Request to Track

Allow apps to ask permission to track you across apps and websites owned by other companies. Apps that don't ask permission may still try to track you. Learn more...

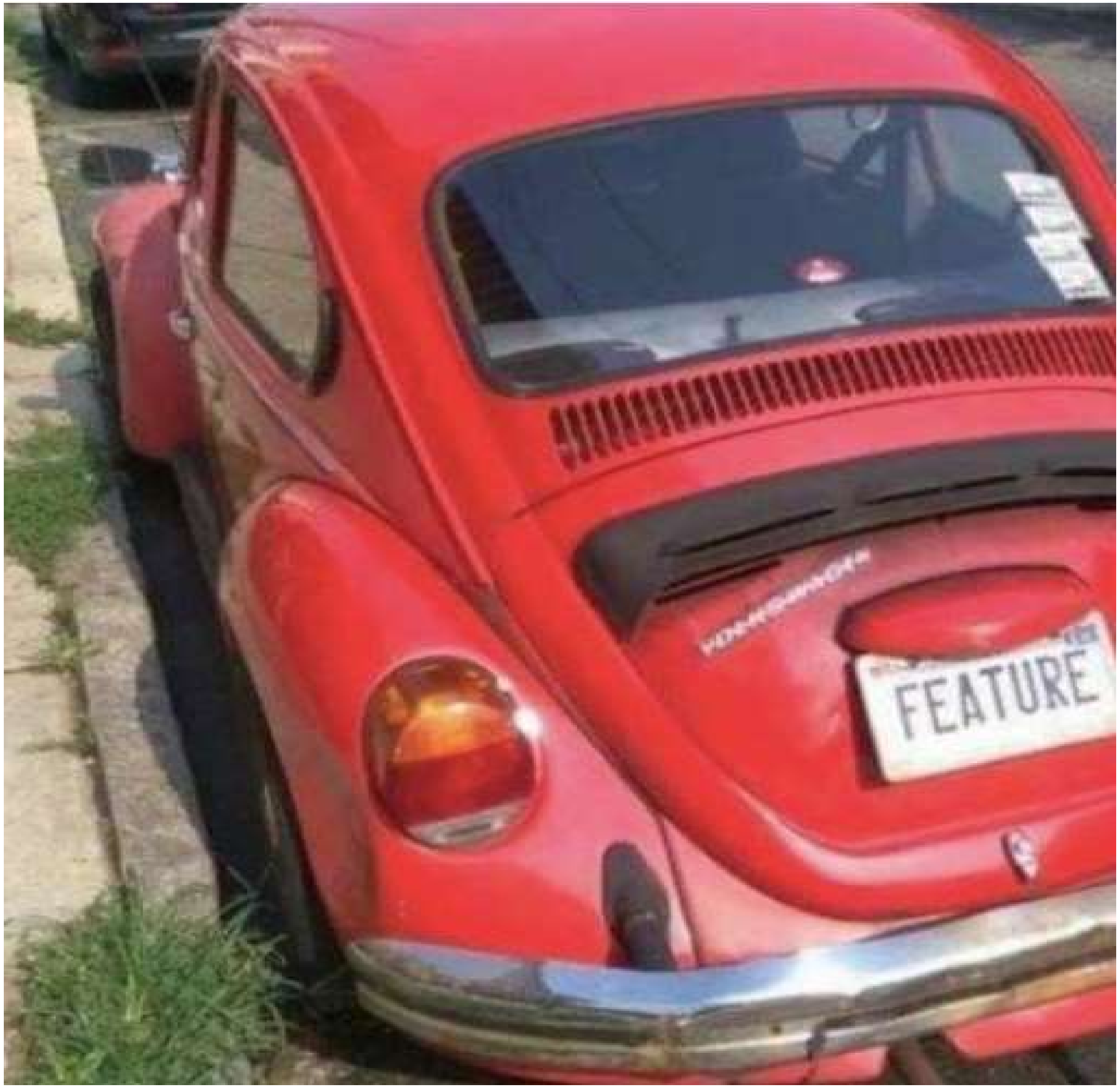
Real Racing 3

Allow Apps to Request to Track

Allow apps to ask permission to track you across apps and websites owned by other companies. Apps that don't ask permission may still try to track you. Learn more...

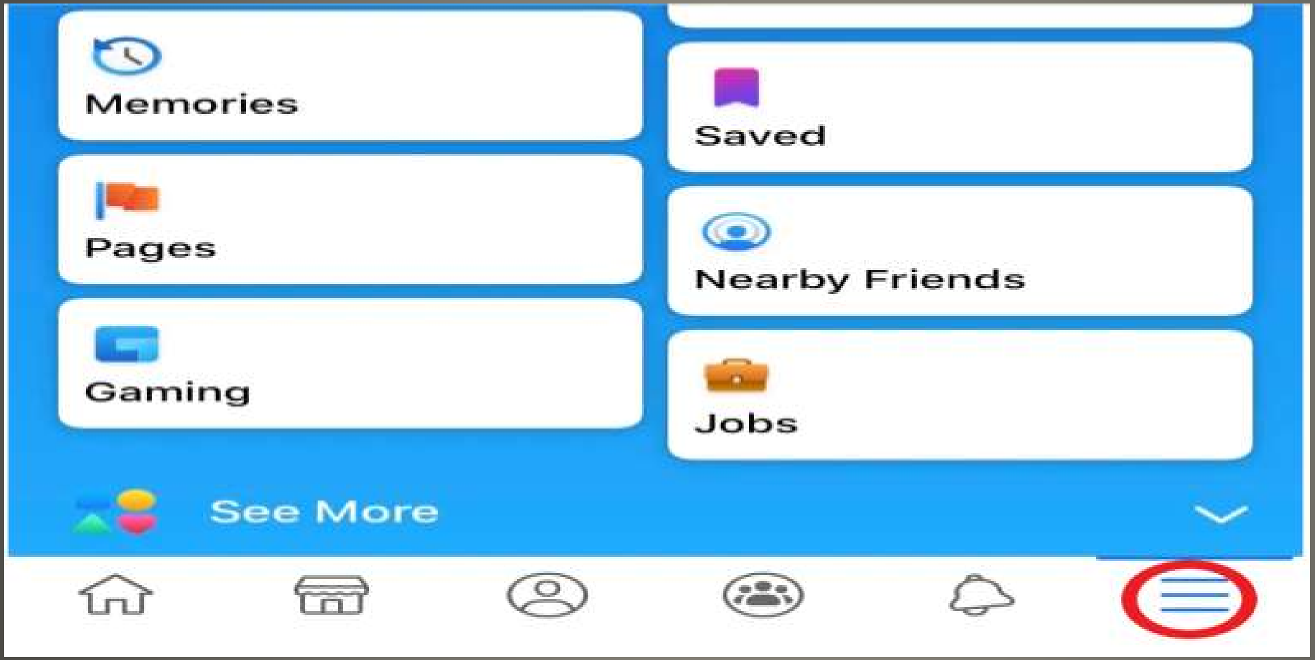
Real Racing 3

Apple iDevices


VOLKSWAGEN
FEATURE

- Facebook

  Hamburger icon



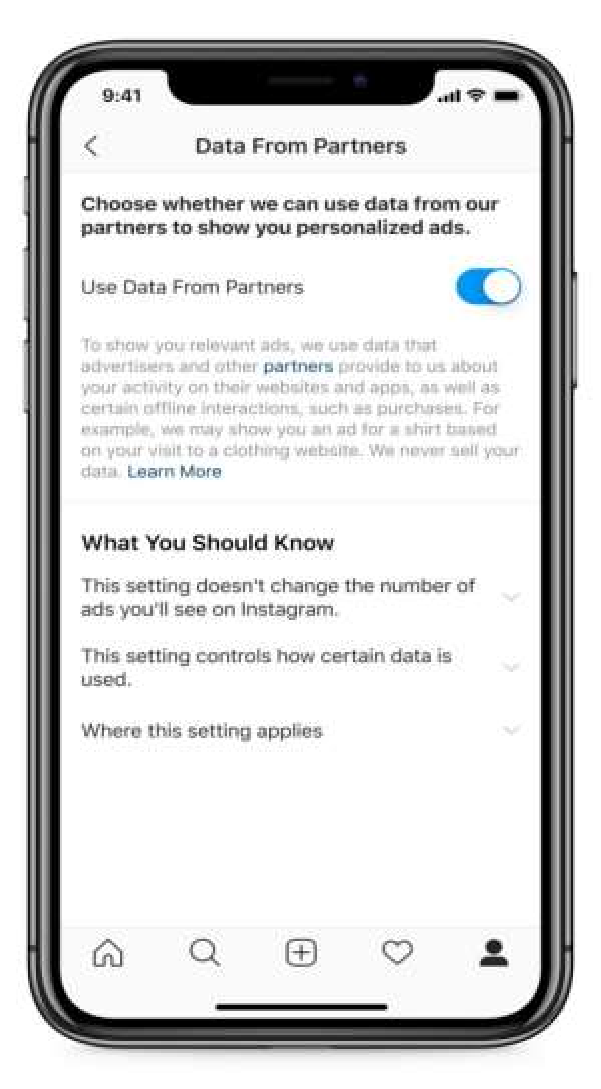
And then the popups begin
7 month delay

- Settings & Privacy -> Privacy Shortcuts
- View or clear your off-Facebook activity
  Do a “WOW”
- Manage Future Activity
- Clear History

- IFF this is your current desire

Facebook

Instagram



Data From Partners

Choose whether we can use data from our partners to show you personalized ads.

Use Data From Partners ●

To show you relevant ads, we use data that advertisers and other partners provide to us about your activity on their websites and apps, as well as certain offline interactions, such as purchases. For example, we may show you an ad for a shirt based on your visit to a clothing website. We never sell your data. Learn More

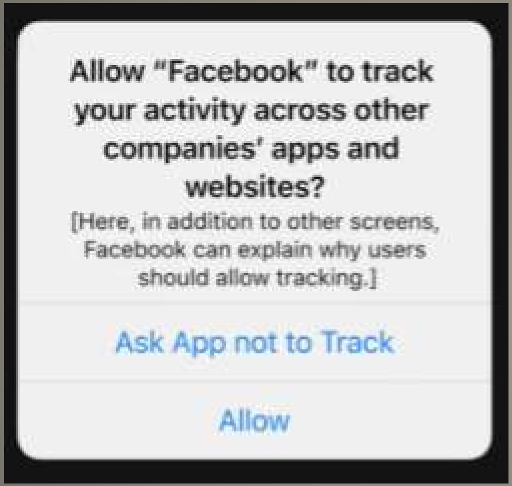
What You Should Know

This setting doesn't change the number of ads you'll see on Instagram.

This setting controls how certain data is used.

Where this setting applies

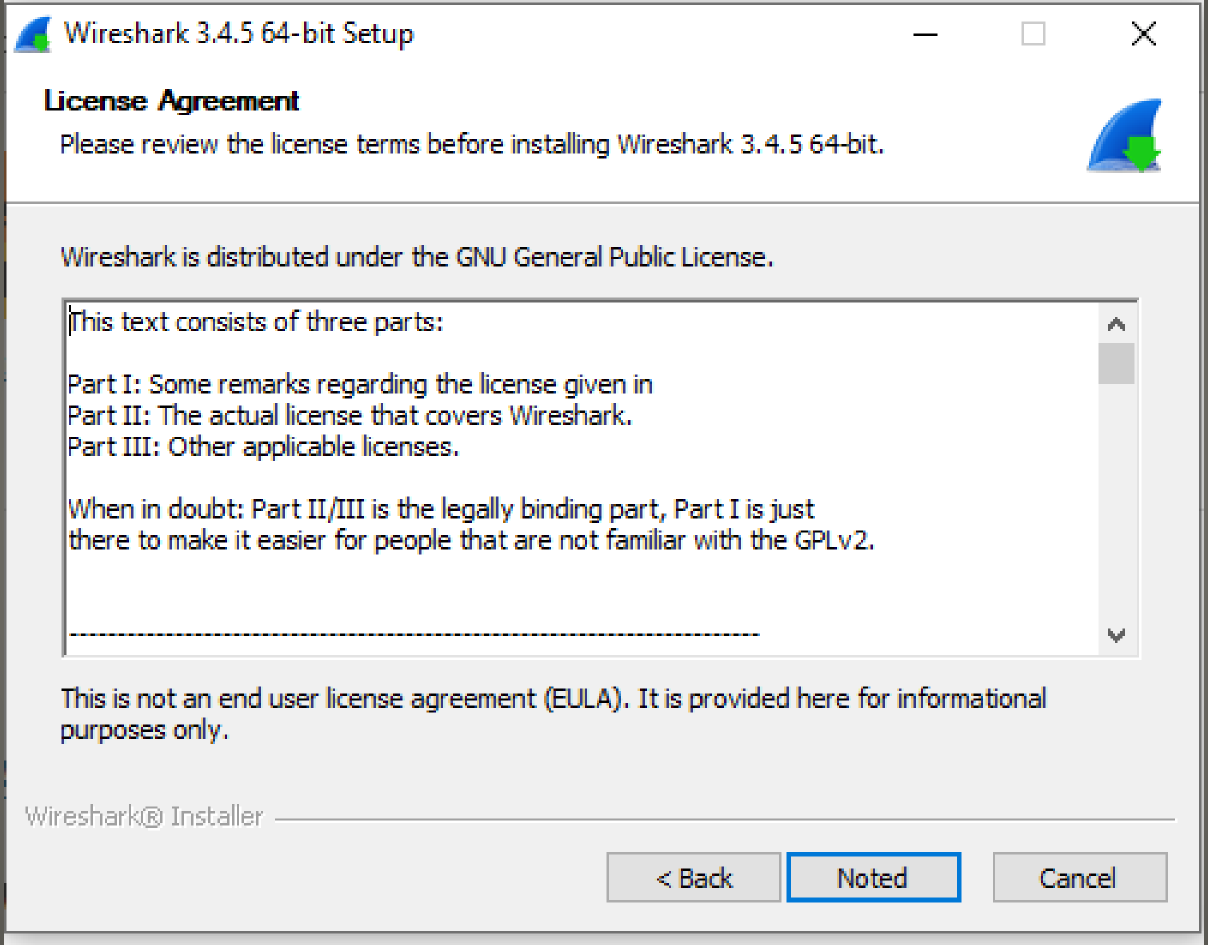
- Apple vs Facebook



Allow "Facebook" to track your activity across other companies' apps and websites?

[Here, in addition to other screens, Facebook can explain why users should allow tracking.]

App Tracking Transparency



License Agreement

Please review the license terms before installing Wireshark 3.4.5 64-bit.

Wireshark is distributed under the GNU General Public License.

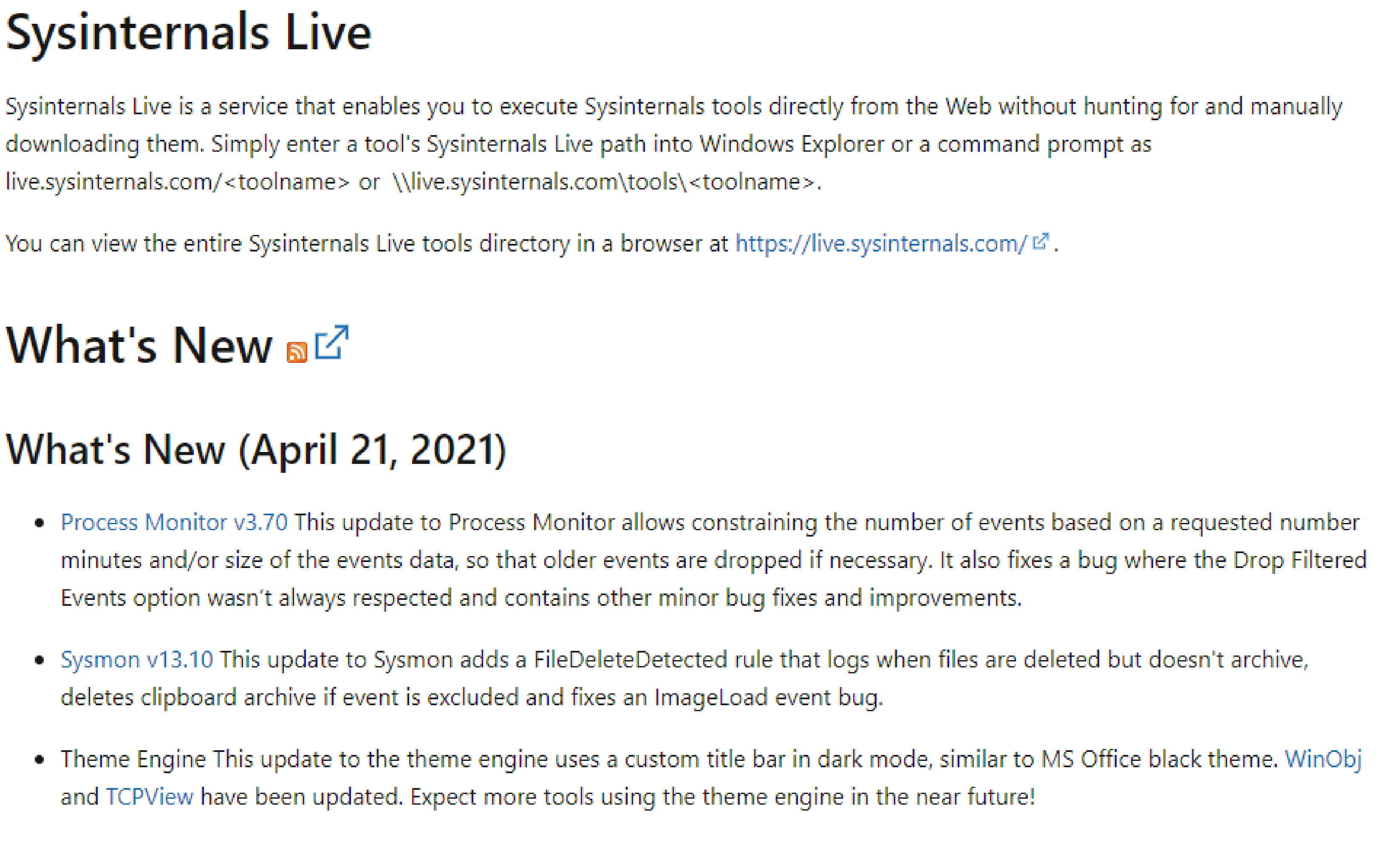
This text consists of three parts:

Part I: Some remarks regarding the license given in
Part II: The actual license that covers Wireshark.
Part III: Other applicable licenses.

When in doubt: Part II/III is the legally binding part, Part I is just
there to make it easier for people that are not familiar with the GPLv2.

This is not an end user license agreement (EULA). It is provided here for informational purposes only.

Wireshark 3.4.5 release



Sysinternals Live

Sysinternals Live is a service that enables you to execute Sysinternals tools directly from the Web without hunting for and manually downloading them. Simply enter a tool's Sysinternals Live path into Windows Explorer or a command prompt as live.sysinternals.com/<toolname> or \\live.sysinternals.com\tools\<toolname>.

You can view the entire Sysinternals Live tools directory in a browser at https://live.sysinternals.com/ .

What's New

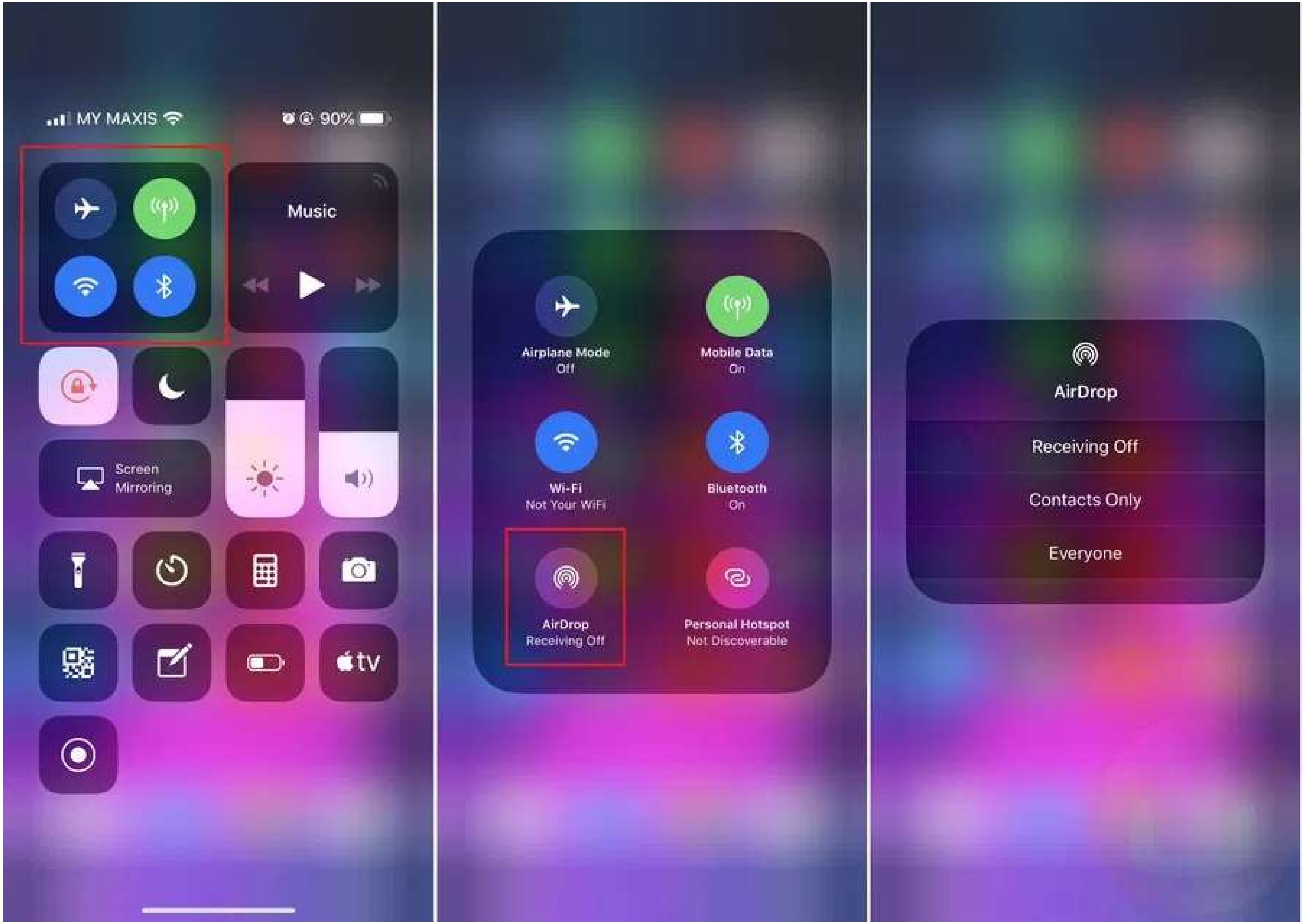
What's New (April 21, 2021)

- Process Monitor v3.70 This update to Process Monitor allows constraining the number of events based on a requested number minutes and/or size of the events data, so that older events are dropped if necessary. It also fixes a bug where the Drop Filtered Events option wasn't always respected and contains other minor bug fixes and improvements.
- Sysmon v13.10 This update to Sysmon adds a FileDeleteDetected rule that logs when files are deleted but doesn't archive, deletes clipboard archive if event is excluded and fixes an ImageLoad event bug.
- Theme Engine This update to the theme engine uses a custom title bar in dark mode, similar to MS Office black theme. WinObj and TCPView have been updated. Expect more tools using the theme engine in the near future!

Sysinternals updates

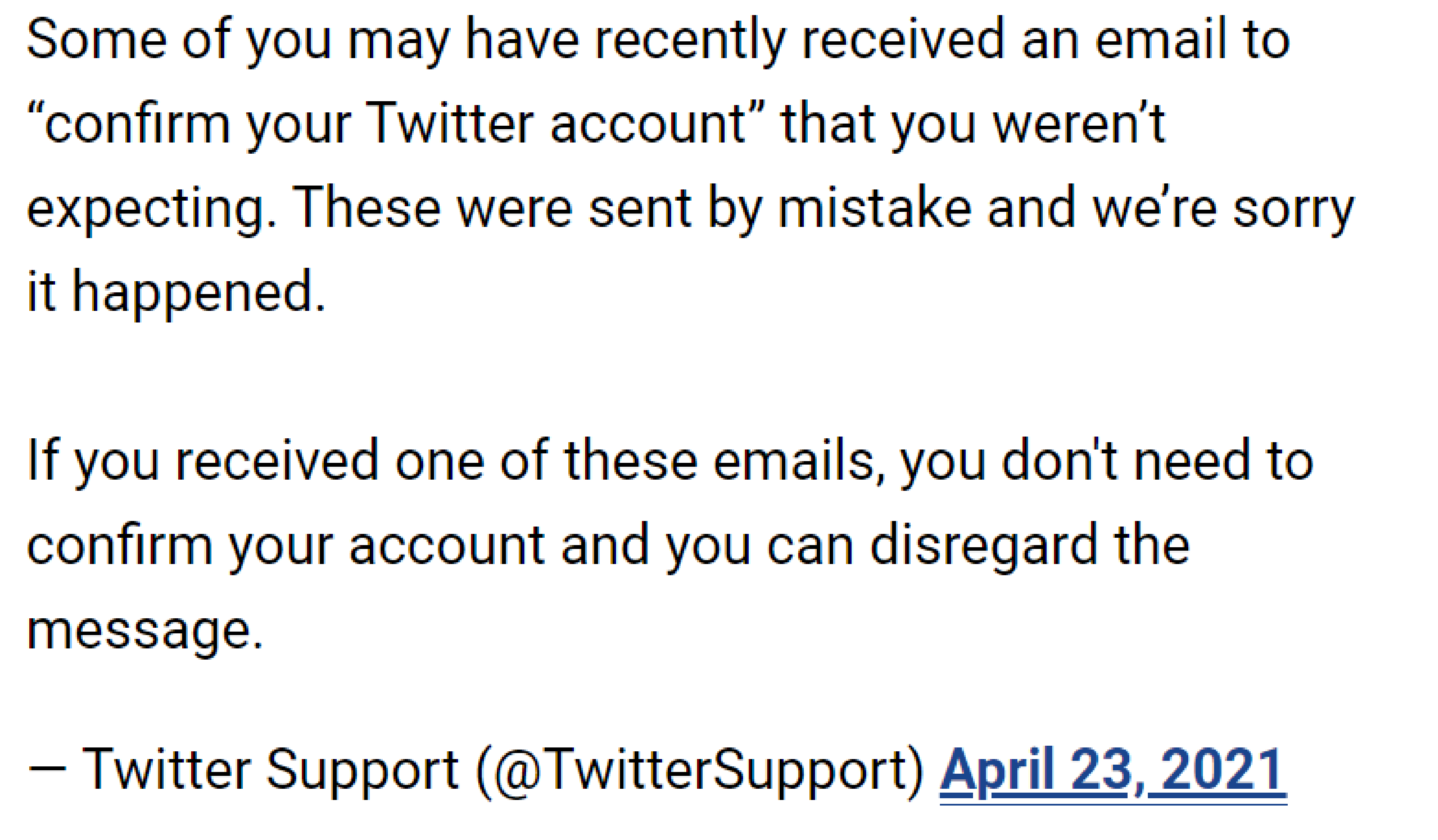
- Apple Ransomware
  Supplier Quanta $50M then $20M   aside Taiwan
- eMail Hack
  Unable to receive eMail
  Microsoft gear icon
  “Rules”
  other Settings - Forward remove
- Browser updates abound
- Emotet C&C takedown Have I Been Pwned
- RotaJakiro Linux malware undetected since 2018
  Kernel versions 5.10-rc4, 5.4.66, or 5.9.8
- AirDrop

Current Issues


MY MAXIS
90%
Music
Screen Mirroring
tv
Airplane Mode
Off
Mobile Data
On
Wi-Fi
Not Your WiFi
Bluetooth
On
AirDrop
Receiving Off
Personal Hotspot
Not Discoverable
AirDrop
Receiving Off
Contacts Only
Everyone

FluBot

- Android
- Fake delivery notification
- Install “App” to follow delivery truck
- Once infected, all contacts sent same malware
- “please allow this app”
- IF INFECTED - RESET - RELOAD
  from good backup from before infection
- Change passphrases

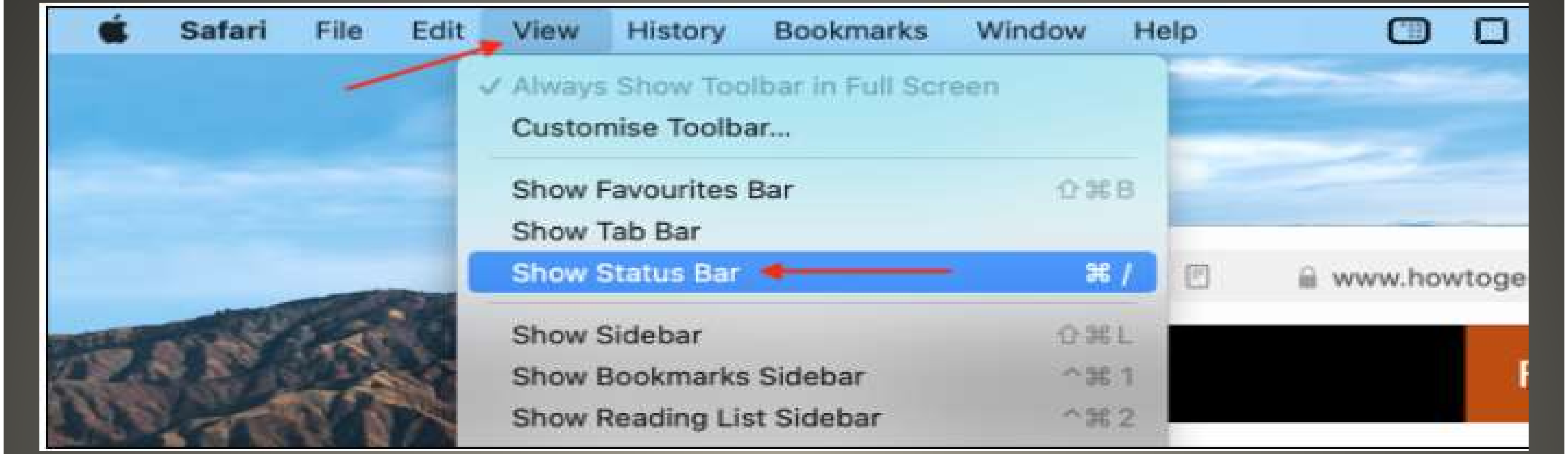


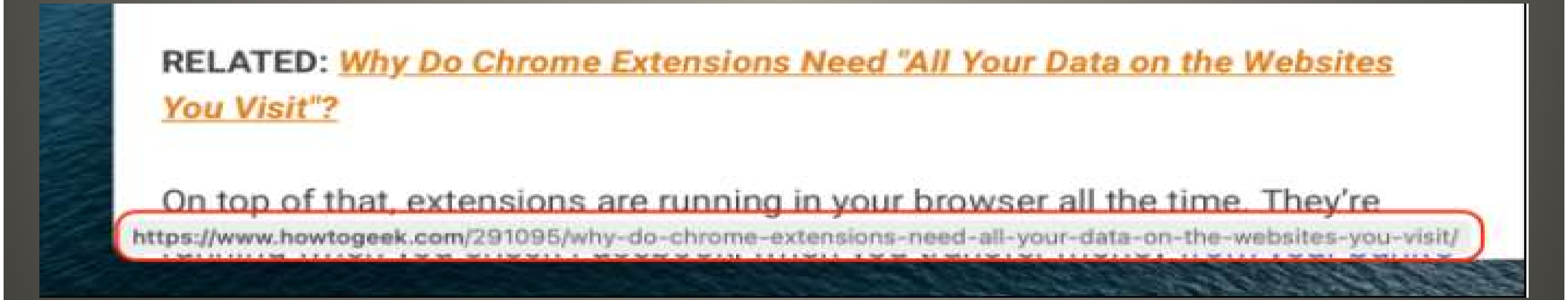
Some of you may have recently received an email to “confirm your Twitter account” that you weren’t expecting. These were sent by mistake and we’re sorry it happened.

If you received one of these emails, you don't need to confirm your account and you can disregard the message.

— Twitter Support (@TwitterSupport) April 23, 2021

Twitter eMail





RELATED: *Why Do Chrome Extensions Need "All Your Data on the Websites You Visit"?*

On top of that, extensions are running in your browser all the time. They're

https://www.howtogeek.com/291095/why-do-chrome-extensions-need-all-your-data-on-the-websites-you-visit/

Safari link preview MacOS

Current Issues

- PulseSecure VPN
- SlowPulse MFA bypass
- Signal Cellebrite feud
- Fourth Amendment is Not For Sale Act
  Clearview AI Data brokers
- Pentagon’s IP address space
  Control transferred to Florida Company
  3 minutes before Biden term to start
  175 million addresses
  Global Resource Systems LLC
  now largest AS in history   AS8003
  Legislative mandated sale failed
- Scripps Health
- Panda Stealer, Doubledrag, Doubledrop, Doubleback
  Private keys, past digital wallet transactions, NordVPN, Telegram, …
  Screenshots, browser cookies, passwords, cards, …

Current Issues

- University of Minnesota & Linux kernel
  OSS
- Passwordstate password manager
  Customer’s data (passwords) stolen
- Codecov Jan -> April   Product to find vulnerabilities
- Ransomware Task Force Report
- Law Enforcement ransom attack data
  For Sale and/or leaked
- And so many more

- FYI

  Blur

  Password Manager

  Tracker blocking

  eMail address hiding

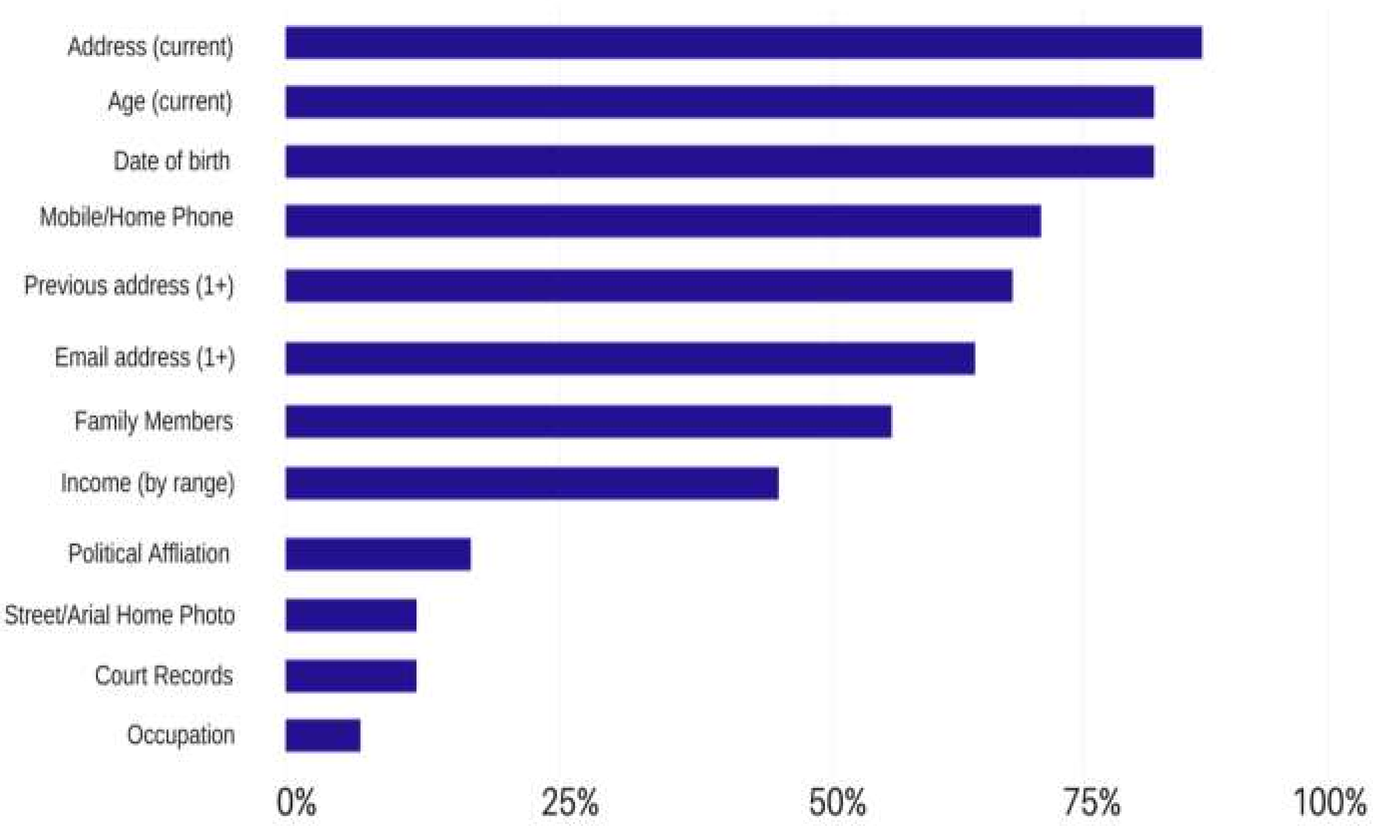
  Credit card masking

  Phone number masking
- FYI no endorsement

- TOR browsers, VPN, security suites, firewalls, browser extensions, virtual credit cards, multiple …
- Credit card numbers with limits
- Warrant canary

OnLine purchases

Chances that your data is for sale



source: DeleteMe findings at top US data brokers based on ~20 million individual opt-out requests

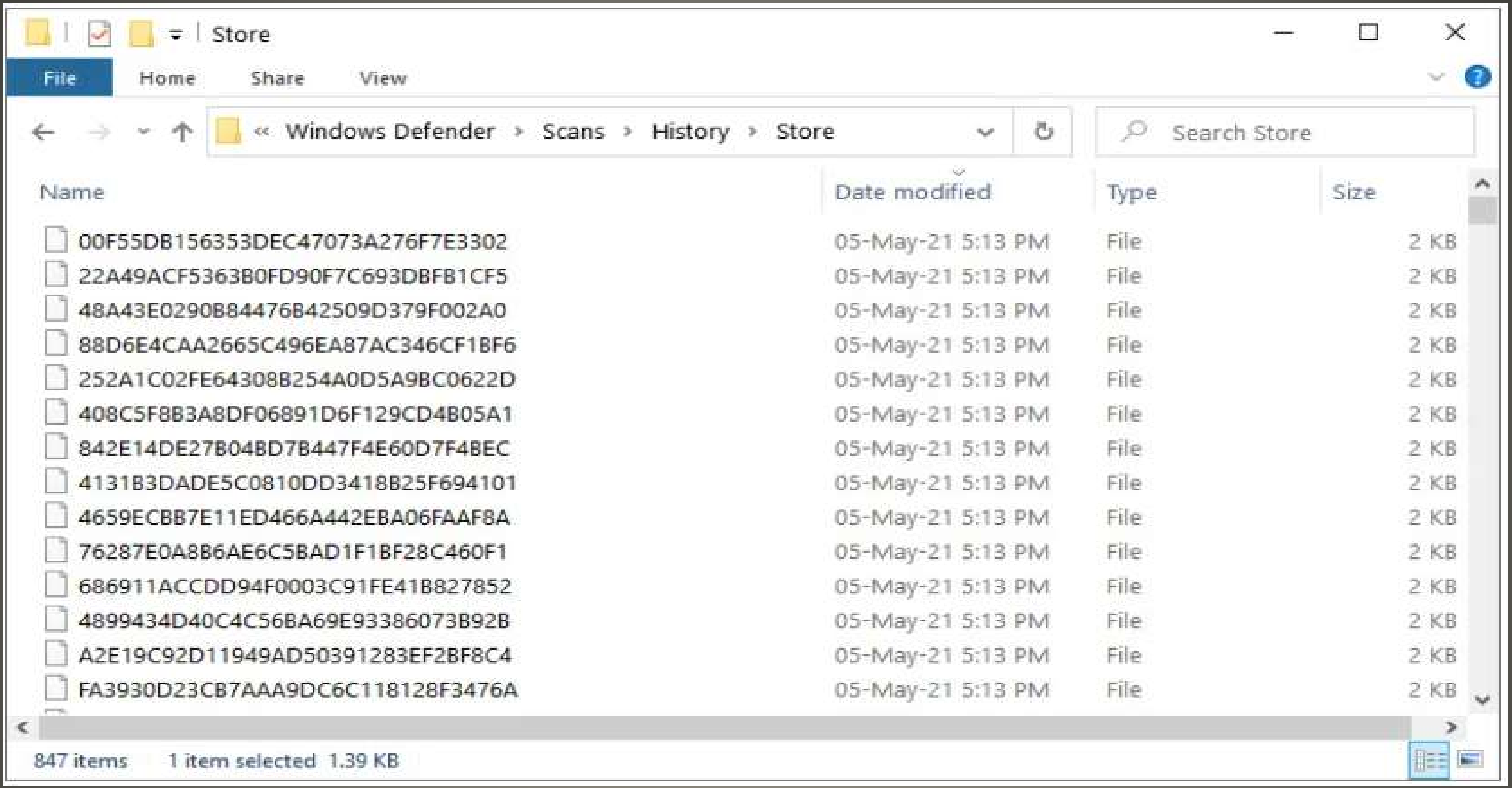
- Passwordstate password manager
  update stole data, sent to attackers
- Postal mail
  O’Connor Property Tax Reduction Experts
  Full Legal Names, Property value,
- Credit monitoring Service(s)
  Credit limit, etc. sent via unencrypted eMail
- Virginia Cyber workforce development initiative
- Dell 12-year-old driver vulnerability

Current Issues

Current Issues

- WebAssembly

  fast & secure common binary
- Google service account guidelines
- Supply chain security
- “I see Dead ?ops Leaking Secrets via Intel/AMD Micro-Op Caches”
- AirTags
- Pelotron Profiles – private?
- Adobe Flash



Name	Date modified	Type	Size
00F55DB156353DEC47073A276F7E3302	05-May-21 5:13 PM	File	2 KB
22A49ACF5363B0FD90F7C693DBFB1CF5	05-May-21 5:13 PM	File	2 KB
48A43E0290B84476B42509D379F002A0	05-May-21 5:13 PM	File	2 KB
88D6E4CAA2665C496EA87AC346CF1BF6	05-May-21 5:13 PM	File	2 KB
252A1C02FE64308B254A0D5A9BC0622D	05-May-21 5:13 PM	File	2 KB
408C5F8B3A8DF06891D6F129CD4B05A1	05-May-21 5:13 PM	File	2 KB
842E14DE27B04BD7B447F4E60D7F4BEC	05-May-21 5:13 PM	File	2 KB
4131B3DADE5C0810DD3418B25F694101	05-May-21 5:13 PM	File	2 KB
4659ECBB7E11ED466A442EBA06FAAF8A	05-May-21 5:13 PM	File	2 KB
76287E0A8B6AE6C5BAD1F1BF28C460F1	05-May-21 5:13 PM	File	2 KB
686911ACCDD94F0003C91FE41B827852	05-May-21 5:13 PM	File	2 KB
4899434D40C4C56BA69E93386073B92B	05-May-21 5:13 PM	File	2 KB
A2E19C92D11949AD50391283EF2BF8C4	05-May-21 5:13 PM	File	2 KB
FA3930D23CB7AAA9DC6C118128F3476A	05-May-21 5:13 PM	File	2 KB

847 items   1 item selected 1.39 KB

Your Windows Defender?

C:\ProgramData\Microsoft\WindowsDefender\Scans\History\Store

- 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