

Sun City Computer Club

Cyber Security SIG

August 5, 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**

Your privacy

California residents have certain rights with regard to the sale of personal information to third parties. Guardian News and Media and our partners use information collected through cookies or in other forms to improve experience on our site and pages, analyze how it is used and show personalized advertising.

At any point, you can opt out of the sale of all of your personal information by pressing

Do not sell my personal information

You can find out more in our [privacy policy](#) and [cookie policy](#), and manage your choices by going to 'California resident – Do Not Sell' at the bottom of any page.

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"/>	Oracle VirtualBox 6.1.22 for Windows (See Notes)	VirtualBox	Important
<input checked="" type="checkbox"/>	Wireshark 3.4.7 for Windows (See Notes)	Wireshark	Critical

Install

Vipre

- Security Account Manager SAM
- Registry HIVE
- Contents: PASSPHRASES, etc.
The *good stuff*
- Locked and protected at boot
Linux can clear passwords in SAM
- RX access to every user
- Everyone every user
everyone on the planet
- BUT Volume Shadow Copy (VSS) can be read
- Pass-the-hash
- Decrypt ALL computer private keys

Summer of SAM SeriousSAM

- Force remote Windows servers to authenticate with attacker
Sharing NT LANMAN authentication details
AND certificates
- Abuse of MS-EFSRPC
Encrypted File System
Remote Procedure Call
- Island hopping Domain Controllers
- Active Directory takeover

PetitPotam

- NotPetya
- MEDoc
- Wiper, not ransomware
- Luckily kill switch
- Global Data pandemic?
- Data Ark
- Large portion of our knowledge, data, wealth
- Used to be
 - Many computer systems, operating systems,
- Now centralized

What, me worry?

- \$320K per day
Telecom lobby
- California broadband middle mile \$3B
- NSO's Pegasus
Pegasus hacked
Determined adversary
Insider
- Candiru
- Telegram crypto weak
- FBI Trojan Shield No US arrests
geofenced cooperation with Australia
Fast and Furious ATF firearm trace
Charges in US justice system – evidence in discovery
- Instacart - Product recall
- No More Ransomware help for millions
- Power cycle devices
- Windows Hyper-V vulnerability CVE-2021-28476
- Manifesto of the inhabitants of Crimea IE AND office macro

Current Issues

- ...up to \$10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, participates in malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA).
- Dark Web reporting channel
- Hardening US institutions
- Cash out cryptocurrencies more difficult
- Better international cooperation
- [StopRansomware.gov](https://www.stopransomware.gov)

**US State Department
Rewards for Justice**

- Consumer Reports
- Broadband Together
- PRIVACY

Join the Fight for Fair Internet



Slow Speeds? High Prices? No Choices?

Join the fight for fair, affordable internet service. All you need is a copy of your internet bill and a few minutes to answer some questions. To get started, you will create a free CR membership account. Let's do this!

ESTIMATED TIME: 7 MINUTES

Current Issues

- FCC Speed Test App
- Apple Store Google Play
- Fact check provider provided test results



FCC WANTS your speed test results

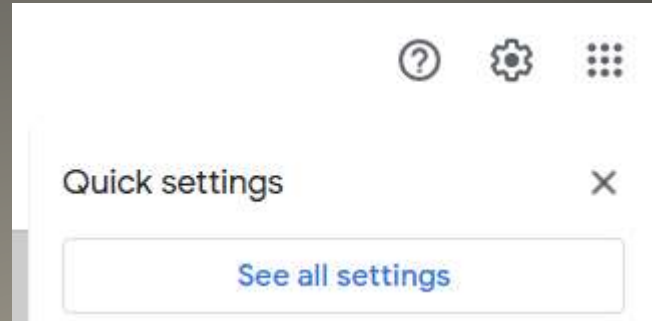


- Hide YOUR callerID
*67(XXX)-XXX-XXX

Settings *82 to un hide



Current Issues



General Labels Inbox Accounts and Import Filters and Blocked Addresses Forwarding and POP/IMAP

Spelling suggestions off

Autocorrect: Autocorrect on
 Autocorrect off

Smart Compose: Writing suggestions on
(predictive writing suggestions appear as you compose an email) Writing suggestions off
[Feedback on Smart Compose suggestions](#)

Smart Compose personalization: Personalization on
(Smart Compose is personalized to your writing style) Personalization off

Gmail psychoanalysis

- Kaseya requires NDA before universal decoder
- REvil gone quiet
- EVERY browser updated
- Edge password health



Current Issues



Add "Microsoft Outlook" to Microsoft Edge?

The extension can:

- Read and change all your data on the websites you visit
- Display notifications

Add extension

Cancel

Outlook Extension Edge



Digital Currency mining machines

El Arroyo



**DON'T WORRY
PASSWORD,
I'M INSECURE
TOO**

HOW BLOCKCHAIN WORKS

@agrassoblog

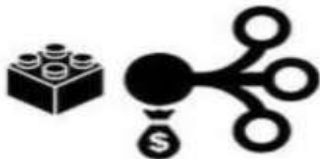
Jim wants to send money to Mary



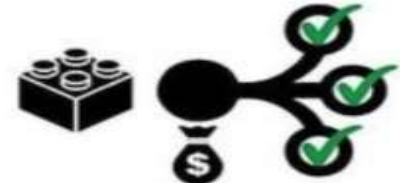
The transaction is represented online as a block



The block gets distributed across the network



The network verifies the transaction is valid



The block is added to the chain, reconciling across the network and creating a permanent record



Jim's record of ownership of the money moves to Mary





OPERATION TROJAN SHIELD: COUNTRIES WITH ACTIVE DEVICES INTERNATIONAL OVERVIEW



Anom devices were active in more than 100 countries. (Courtesy of U.S. Department of Justice)

FBI Trojan Shield



A photo of bricks of cocaine stamped with the Batman logo was sent from one Anom user to another in January 2020. (Search warrant photo)

- Matter – universal smart home standard
Apple, Google, Samsung, Amazon, ...



Current Issues

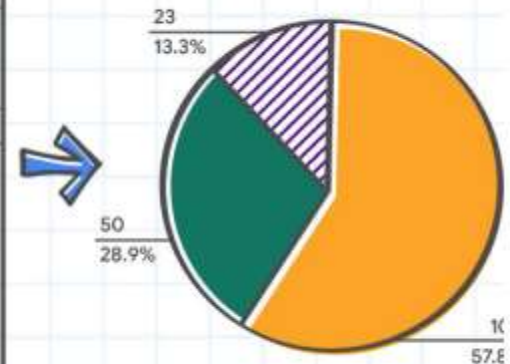
- Massive Internet Outage 22-July-22
Akami DNS
FedEx, Delta, Steam, Fidelity, Airbnb, UPS, LastPass, Amazon, ...
Centralization
- XCSSET macOS -> Chrome Telegram
- Russia disconnects from global Internet tests June 15 – July 15
- TSA pipeline directive #2
- CISA/FBI advisory China US Oil & Gas companies
- China Microsoft Exchange attack
- Apple iOS/iPadOS 14.7.1 macOS 11.5.1
- Amnesty International Surveillance tech moratorium
- Iran aerobics instructors profile

Current Issues








China QR code

- Image processing PER PIXEL
- Upwards of 14 million pixels
- Color hash map
- M92 faster



Chrome anti-phishing



Safe Browsing

- Enhanced protection**
Faster, proactive protection against dangerous websites, downloads, and extensions. Warns you about password breaches. Requires browsing data to be sent to Google. ^
-  Predicts and warns you about dangerous events before they happen
 -  Keeps you safe on Chrome and may be used to improve your security in other Google apps when you are signed in
 -  Improves security for you and everyone on the web
 -  Warns you if passwords are exposed in a data breach
-  Sends URLs to Safe Browsing to check them. Also sends a small sample of pages, downloads, extension activity, and system information to help discover new threats. Temporarily links this data to your Google Account when you're signed in, to protect you across Google apps.
-
- Standard protection**
Standard protection against websites, downloads, and extensions that are known to be dangerous. v
-
- No protection (not recommended)**
Does not protect you against dangerous websites, downloads, and extensions. You'll still get Safe Browsing protection, where available, in other Google services, like Gmail and Search.

Chrome Safe Browsing

Brave

Safe Browsing

- Standard protection**
Standard protection against websites, downloads, and extensions that are known to be dangerous.
 -  Detects and warns you about dangerous events when they happen
 -  Checks URLs with a list of unsafe sites stored in Brave.
- No protection (not recommended)**
Does not protect you against dangerous websites, downloads, and extensions.

Chromium Browsers

- Printer driver HP, Samsung, and Xerox
- Since 2005 380 different models
- Loaded even if cancelled
even if printer off or removed
- SSSPORT.SYS
- In Band <print.me>
- Out of Band <landscape>
- Apps need/want <landscape>
- Microsoft allows drivers (and other) to accept and process input to kernel level code

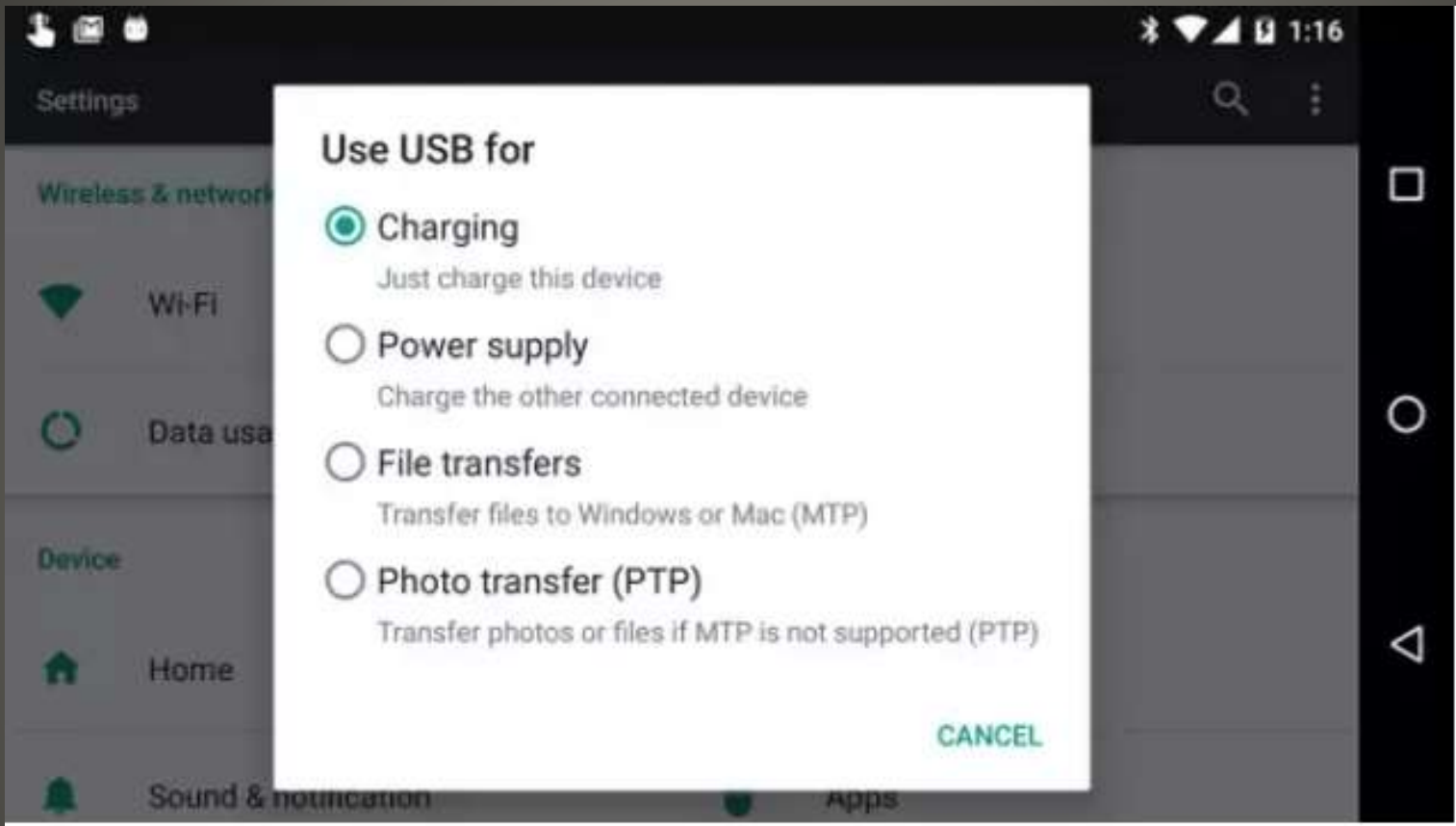
PrintNightmare - wait



- USB Restricted Mode
Settings > Face ID & Passcode
Settings > Touch ID & Passcode
USB Accessories OFF



iPhone



Android

- Protection Criminal LE Foreign actors
- Catastrophe Kids Dementia

Auto Erase ?

- Prevalent on windows
- Moved to MacOS
- XLoader
- Malware as a service
- \$49/mo.
- Standard protections apply
 - NEVER click on links in unsolicited eMails
 - ONLY download from reliable sources
 - Security suites
 - Signatures up to date
 - Defense in depth

Formbook / XLoader

- Certain cellular
- Utility
- Gym, etc.
- Cable
- Streaming services
- Annual subscriptions

Auto Pay cautions

- Android banking trojan
- Google Play Store
- Screen mirroring - not overlay
- Back button Hide icon

Vultur

Vultur

Android Banking Trojan

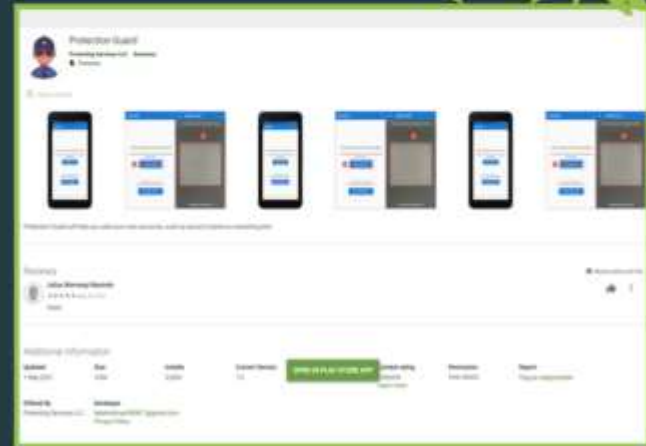


Vultur: new Android Banking Trojan

- RAT with VNC module and keylogger
- Fraud vector: on device fraud
- Distributed via Google Play Store!
- New Trojan belongs to Brunhilda Threat Actor group

MITRE Mobile (TTP highlights):

- T1475 Deliver Malicious App via Authorized App Store (GP)
- T1444 Masquerade as Legitimate Application (dropper)
- T1513 Screen capture (RAT)
- T1417 Input Capture (Keylogger)



Vultur

- On victim code assembly
- Bypass perimeter protections
- Cloud hosting of day-to-day work tools

HTML smuggling

- Gmail apps
- Google trackers 75% of top million web sites

Tracker	Owner	Seen on websites
> doubleclick.net	Google	104
> google-analytics.com	Google	96
> googletagmanager.com	Google	85
> googleadservices.com	Google	64
> facebook.net	Facebook	60
> googlesyndication.com	Google	56
> googletagservices.com	Google	52
> 2mdn.net	Google	38
> adnxs.com	AppNexus	38
> scorecardresearch.com	comScore	38

Gmail

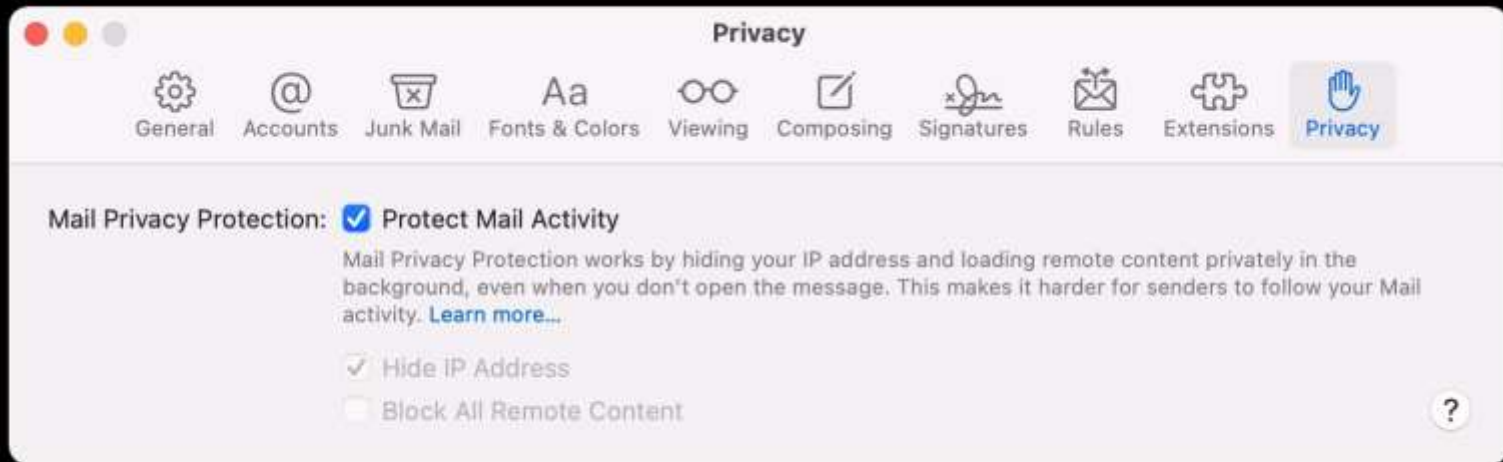
- Trackers embedded in eMail

Gmail

- iOS 15 iPadOS 15 MacOS 12.0 (Monterey)

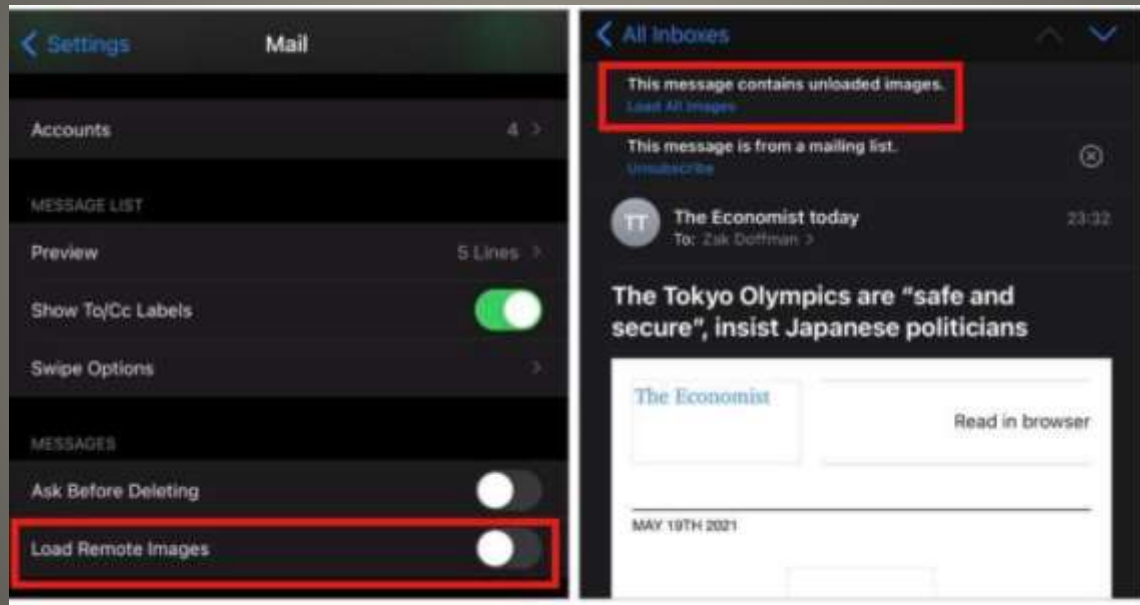


Apple eMail Privacy Protection



MacOS Monterey

- Text based eMail reader
- Turn off automatic image loading



eMail

Apple Mail (Data Linked to You)

App Functionality	
	Contact info Email Address Name
	Identifiers User ID

Google Gmail (Data Linked to You)

Third-Party Advertising	Analytics	Product Personalisation	App Functionality
			
Location Current Location	Purchases Purchase History	Contact info Email Address	Purchases Purchase History
			
Identifiers User ID	Location Cookie Location	Contacts Contacts	Location Current Location
			
Usage Data Advertising Data	Contact info Email Address	User Content Emails or Text Messages Audio Data	Contact info Email Address Name
			
	User Content Webinar Videos Audio Data Customer Support Other User Content	Search History Search History	Contacts Contacts
			
	Search History Search History	Identifiers User ID Device ID	User Content Emails or Text Messages Photos or Videos Audio Data Customer Support Other User Content
			
	Identifiers User ID Device ID	Usage Data Product Interactions	Search History Search History
			
	Usage Data Product Interactions Advertising Data		Identifiers User ID Device ID
			
	Diagnostics Crash Data Performance Data Other Diagnostic Data		Usage Data Product Interactions
			
	Other Data Other Data Types		Diagnostics Crash Data Performance Data Other Diagnostic Data
			
			Other Data Other Data Types

- DarkSide -> BlackMatter
- DoppelPaymer -> Grief
- Avaddon -> Haron

- Tailscale & WireGuard -> OpenVPN & IPSec

- Zoom proposed settlement
Class action
Lying about end-to-end encryption
\$15 - \$25
Current zoom app version 5.7.4

Current Issues

- https://media.defense.gov/2021/Jul/29/2002815141/-1/-1/0/CSI_SECUREING_WIRELESS_DEVICES_IN_PUBLIC.PDF
NSA Guidance on Wireless Device Security
- **Biden Memorandum**
Cybersecurity and Infrastructure Security Agency
National Institute of Standards and Technology
Develop benchmarks for entities managing critical infrastructure
- **Archive.org “way back machine”**
- SolarWinds actors breached US Federal prosecutor’s eMail accounts

Current Issues

- 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