Sun City Computer Club

Cyber Security SIG

May 20, 2021

Questions, Comments, Suggestions welcomed at any time

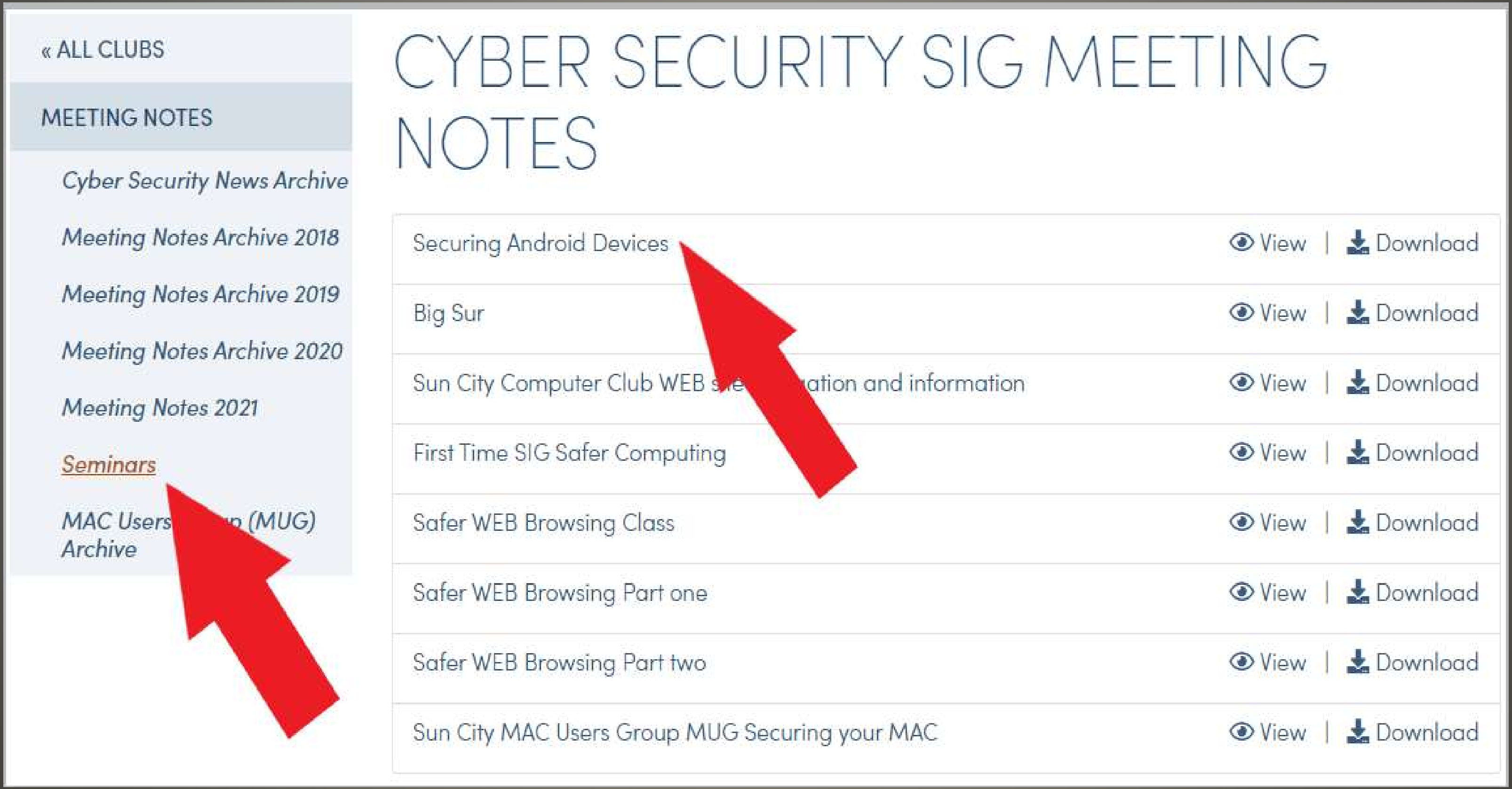
Even Now

- 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

- Computer Club Facebook
- Seminars



« ALL CLUBS

MEETING NOTES

Cyber Security News Archive

Meeting Notes Archive 2018

Meeting Notes Archive 2019

Meeting Notes Archive 2020

Meeting Notes 2021

Seminars

MAC Users [illegible] (MUG) Archive

CYBER SECURITY SIG MEETING NOTES

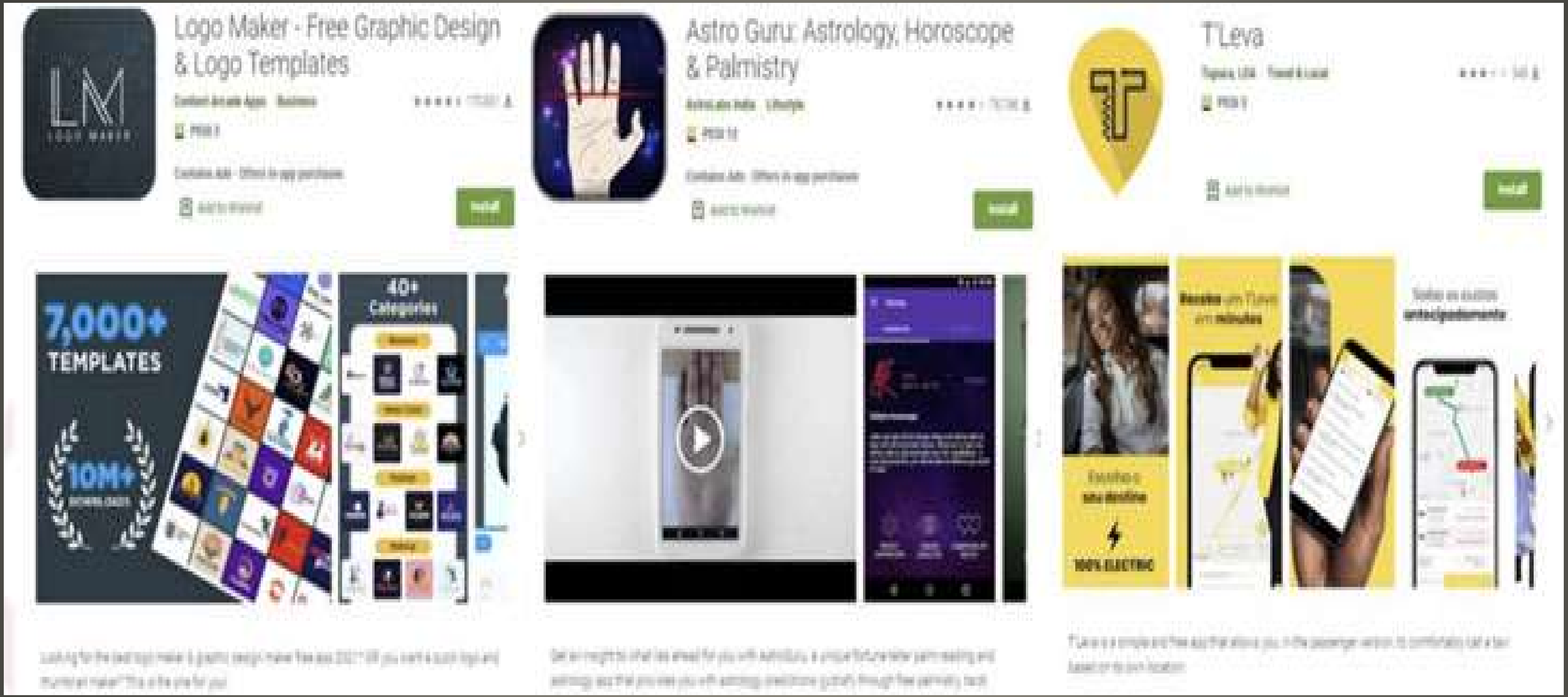
Securing Android Devices	👁 View | ⬇ Download
Big Sur	👁 View | ⬇ Download
Sun City Computer Club WEB s[illegible]ation and information	👁 View | ⬇ Download
First Time SIG Safer Computing	👁 View | ⬇ Download
Safer WEB Browsing Class	👁 View | ⬇ Download
Safer WEB Browsing Part one	👁 View | ⬇ Download
Safer WEB Browsing Part two	👁 View | ⬇ Download
Sun City MAC Users Group MUG Securing your MAC	👁 View | ⬇ Download

Android May 2021 update

- 4 vulnerabilities actively under attack

Android Apps

- 23 Google Play store apps
- 100,000,000 users’ personal data
- Misconfigurations
- Developer’s internal resources
- App cloud access
- eMails, phone numbers, chat, passwords, photos, browser histories,



Logo Maker - Free Graphic Design & Logo Templates

Content Arcade Apps · Business

PEGI 3

Contains Ads · Offers in-app purchases

Add to Wishlist

Install

Looking for the best logo maker & graphic design maker free app 2021? Or you want a quick logo and thumbnail maker? This is the one for you!

Astro Guru: Astrology, Horoscope & Palmistry

Astro-Arcade India · Lifestyle

PEGI 12

Contains Ads · Offers in-app purchases

Add to Wishlist

Install

Get an insight to what lies ahead for you with AstroGuru, a unique fortune teller palm reading and astrology app that provides you with astrology predictions (gratis) through free palmistry, tarot

T'Leva

Tapeca, LDA · Travel & Local

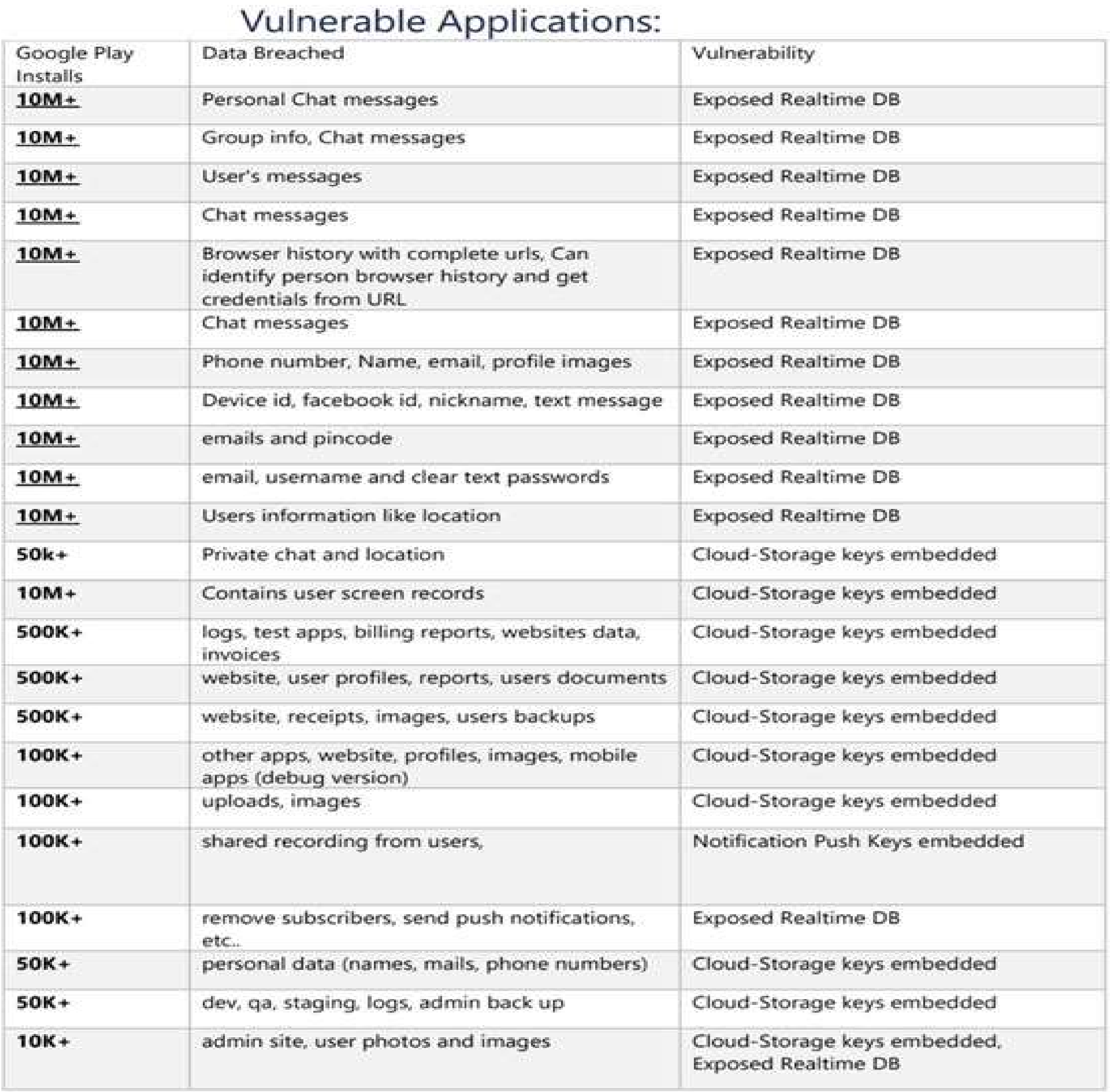
PEGI 3

Add to Wishlist

Install

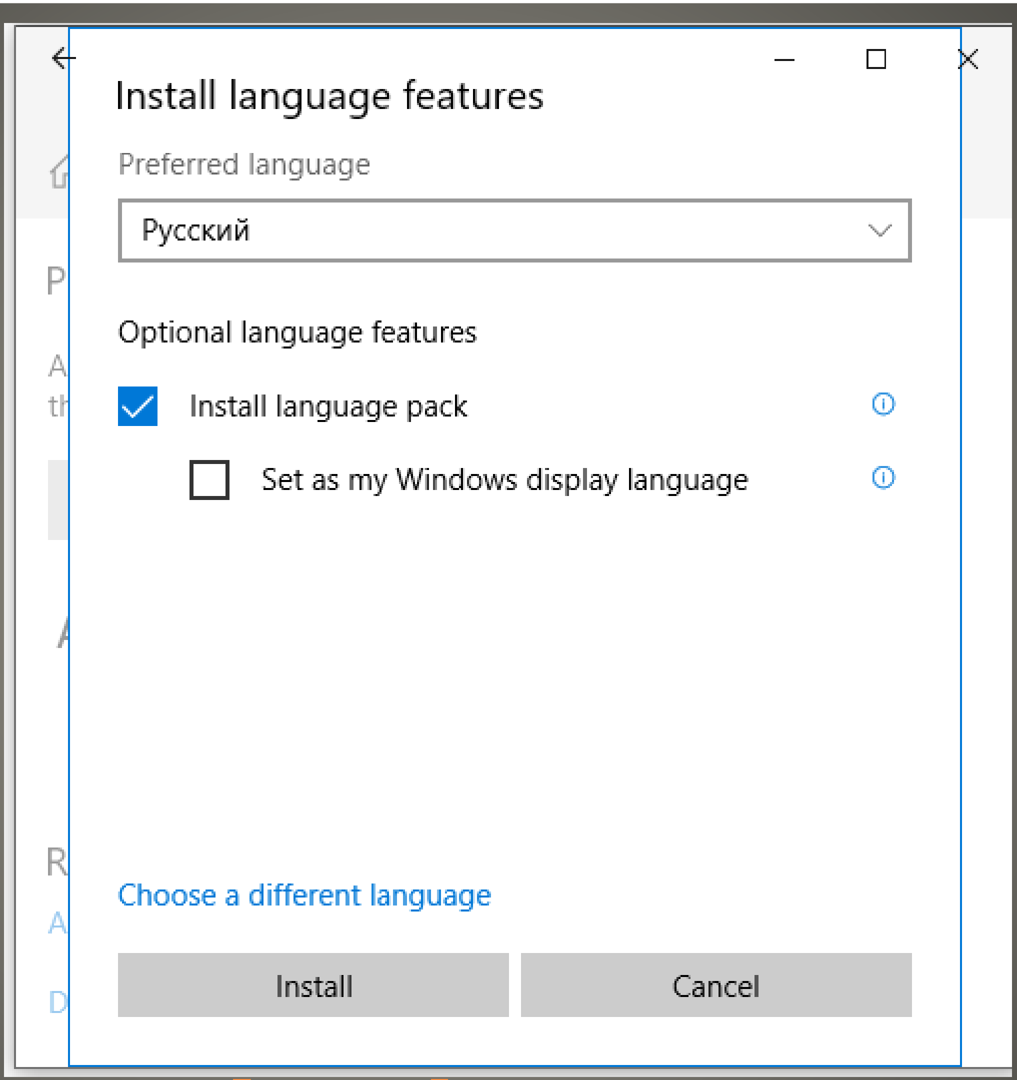
T'Leva is a simple and free app that allows you, in the passenger version, to comfortably call a taxi based on its own location.

Android Apps



Vulnerable Applications:

Google Play Installs	Data Breached	Vulnerability
10M+	Personal Chat messages	Exposed Realtime DB
10M+	Group info, Chat messages	Exposed Realtime DB
10M+	User's messages	Exposed Realtime DB
10M+	Chat messages	Exposed Realtime DB
10M+	Browser history with complete urls, Can identify person browser history and get credentials from URL	Exposed Realtime DB
10M+	Chat messages	Exposed Realtime DB
10M+	Phone number, Name, email, profile images	Exposed Realtime DB
10M+	Device id, facebook id, nickname, text message	Exposed Realtime DB
10M+	emails and pincode	Exposed Realtime DB
10M+	email, username and clear text passwords	Exposed Realtime DB
10M+	Users information like location	Exposed Realtime DB
50k+	Private chat and location	Cloud-Storage keys embedded
10M+	Contains user screen records	Cloud-Storage keys embedded
500K+	logs, test apps, billing reports, websites data, invoices	Cloud-Storage keys embedded
500K+	website, user profiles, reports, users documents	Cloud-Storage keys embedded
500K+	website, receipts, images, users backups	Cloud-Storage keys embedded
100K+	other apps, website, profiles, images, mobile apps (debug version)	Cloud-Storage keys embedded
100K+	uploads, images	Cloud-Storage keys embedded
100K+	shared recording from users,	Notification Push Keys embedded
100K+	remove subscribers, send push notifications, etc..	Exposed Realtime DB
50K+	personal data (names, mails, phone numbers)	Cloud-Storage keys embedded
50K+	dev, qa, staging, logs, admin back up	Cloud-Storage keys embedded
10K+	admin site, user photos and images	Cloud-Storage keys embedded, Exposed Realtime DB



Install language features

Preferred language

Русский

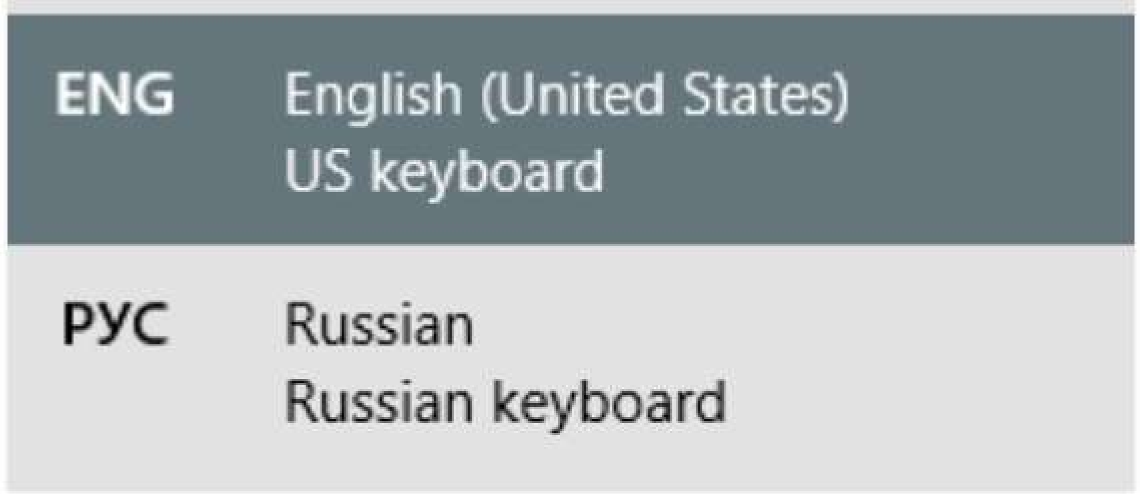
Optional language features

☑ Install language pack

□ Set as my Windows display language

Choose a different language

Install Russian language?



ENG English (United States)
US keyboard

РУС Russian
Russian keyboard

Windows key + Space bar

Current Issues

- Apple acquiescence to China government state employees to manage servers and security tools used to secure information
- Write once media to help with ransomware?
- Intel & Leidos "trusted execution environment" for Covid research
- AI & humanity

  "Do you want to destroy humans?"

  "OK, I will destroy humans, you have been warned"

Current Issues

- Cryptocurrency fraud, scams, theft
- 85% of US critical infrastructure in private hands?

  We do not know
- AXA French Insurance company

  Will no longer write ransomware policies

  Hit with ransomware

  Data release threat

  A carrier of Colonial pipeline cyber insurance
- EufyCam vulnerability
- Robot Vacuum + pet deposit = extreme mess
- 96% opt out rate for iOS 14.5
- Air Tags mesh network can be used as covert channel

HD
SONY
MICRO FLOPPYDISK
Double Sided
MFD-2HD
SONY
INDEX
BITCOIN
WALLET

- Fit for purpose
- VPN

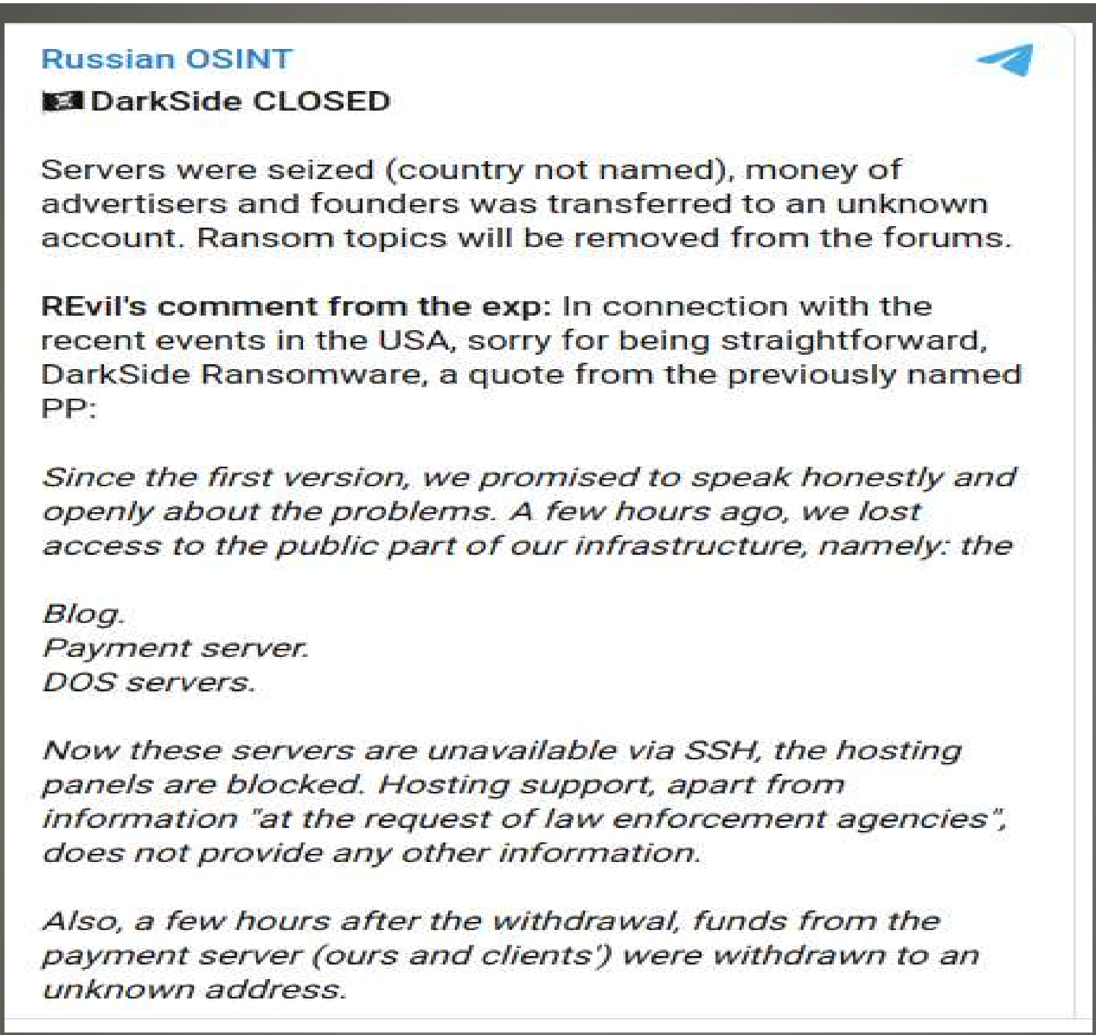
  Hide *traffic* from ISP (Suddenlink)
  Hide *traffic* from government
  Public Wi-Fi - *some* protections
  Hosted apps and Services
  Geo restricted access
- Cloud

  Proud vs. Private clear vs encryption
  Encryption – Yours or Yours & theirs
  Dependance small

Cloud & VPN

Darkside

- Ransomware as a service
- Every (thus any) target
- State of emergency
- Stolen data and encrypted
- Double or half ransom – depending
- Solar Winds – sigh
- Gas supply – intense interest
- 30 “other” events



Russian OSINT

🏴‍☠️ DarkSide CLOSED

Servers were seized (country not named), money of advertisers and founders was transferred to an unknown account. Ransom topics will be removed from the forums.

REvil's comment from the exp: In connection with the recent events in the USA, sorry for being straightforward, DarkSide Ransomware, a quote from the previously named PP:

Since the first version, we promised to speak honestly and openly about the problems. A few hours ago, we lost access to the public part of our infrastructure, namely: the

Blog.
Payment server.
DOS servers.

Now these servers are unavailable via SSH, the hosting panels are blocked. Hosting support, apart from information "at the request of law enforcement agencies", does not provide any other information.

Also, a few hours after the withdrawal, funds from the payment server (ours and clients') were withdrawn to an unknown address.

Darkside gone dark

Executive Order

Improving nation’s cyber security

- More stringent security requirements for government contractors
- Use of procurement processes to increase vendors to implement secure software development processes
- Require government agencies to use multi-factor authentication and encryption
- Adoption of zero-trust security model

Improving nation’s cyber security

- Cyber Security Safety Board

  National Transportation Safety Board

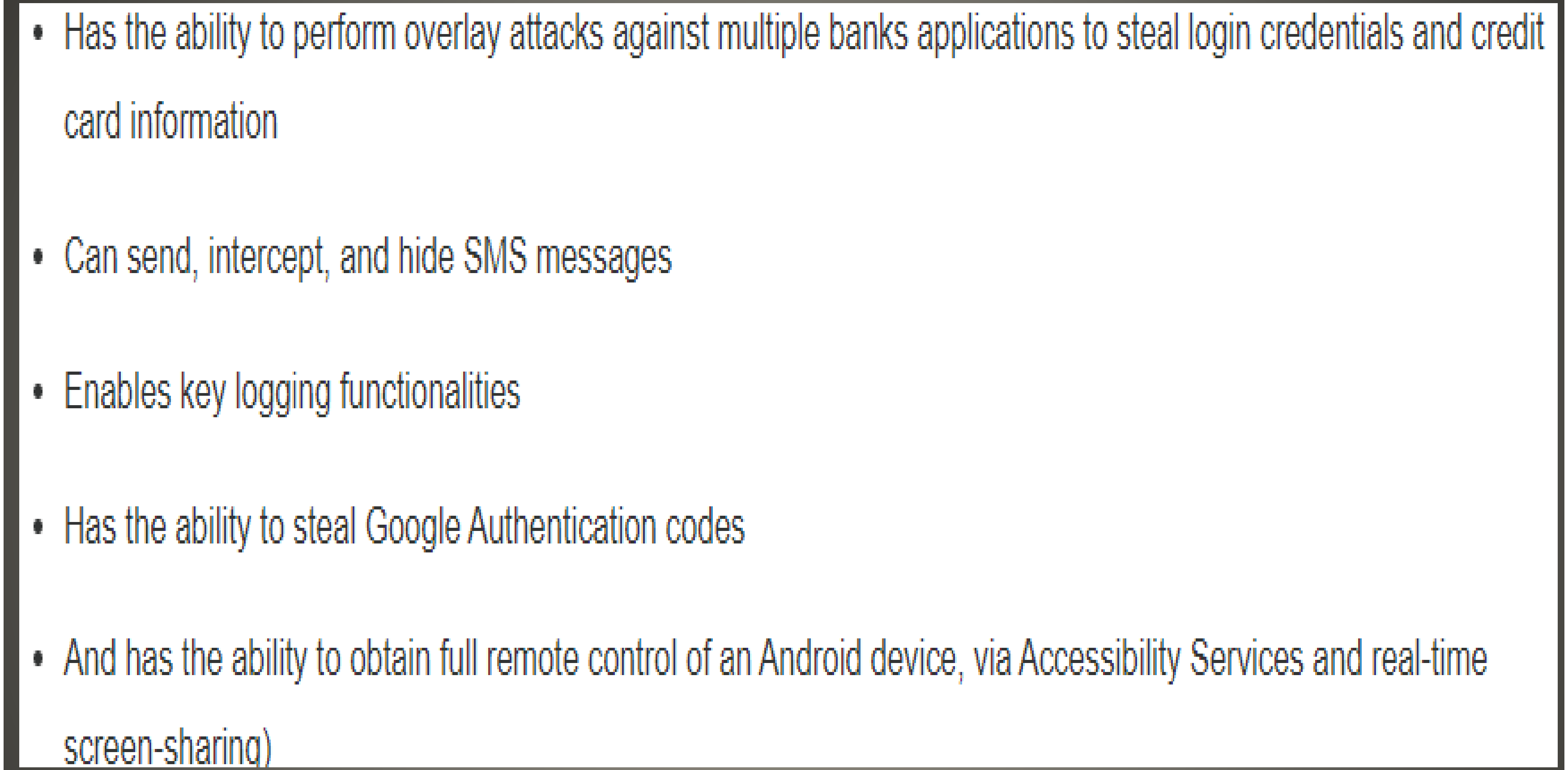
- 180 day deadline for MFA and encryption

executive-order-on-improving-the-nations-cybersecurity

Executive Order

- All-of-government response

  Interagency response group (well 9)
- EPA waver non-compliant fuel
- DOT hours of service for fuel transport
- Governors expand weigh limits for fuel transport
- Alternate fuel transport via rail and maritime



- Has the ability to perform overlay attacks against multiple banks applications to steal login credentials and credit card information
- Can send, intercept, and hide SMS messages
- Enables key logging functionalities
- Has the ability to steal Google Authentication codes
- And has the ability to obtain full remote control of an Android device, via Accessibility Services and real-time screen-sharing)

TeaBot Android trojan

Bizzaro Banking Trojan

- Yet another Android banking trojan
- Kills browser processes
- Disables autocomplete
- Hijack bitcoin wallets

Exim

- Experimental Internet Mailer
- 60% of publicly reachable mail servers
- Open Source Software (OSS)
- Source Code Audit
- 21 remotely exploitable vulnerabilities
- Since it is OSS, tracking is difficult
- Part of *appliances*
- Part of many distros
- 21 nails
- Microsoft Exchange Server - second verse

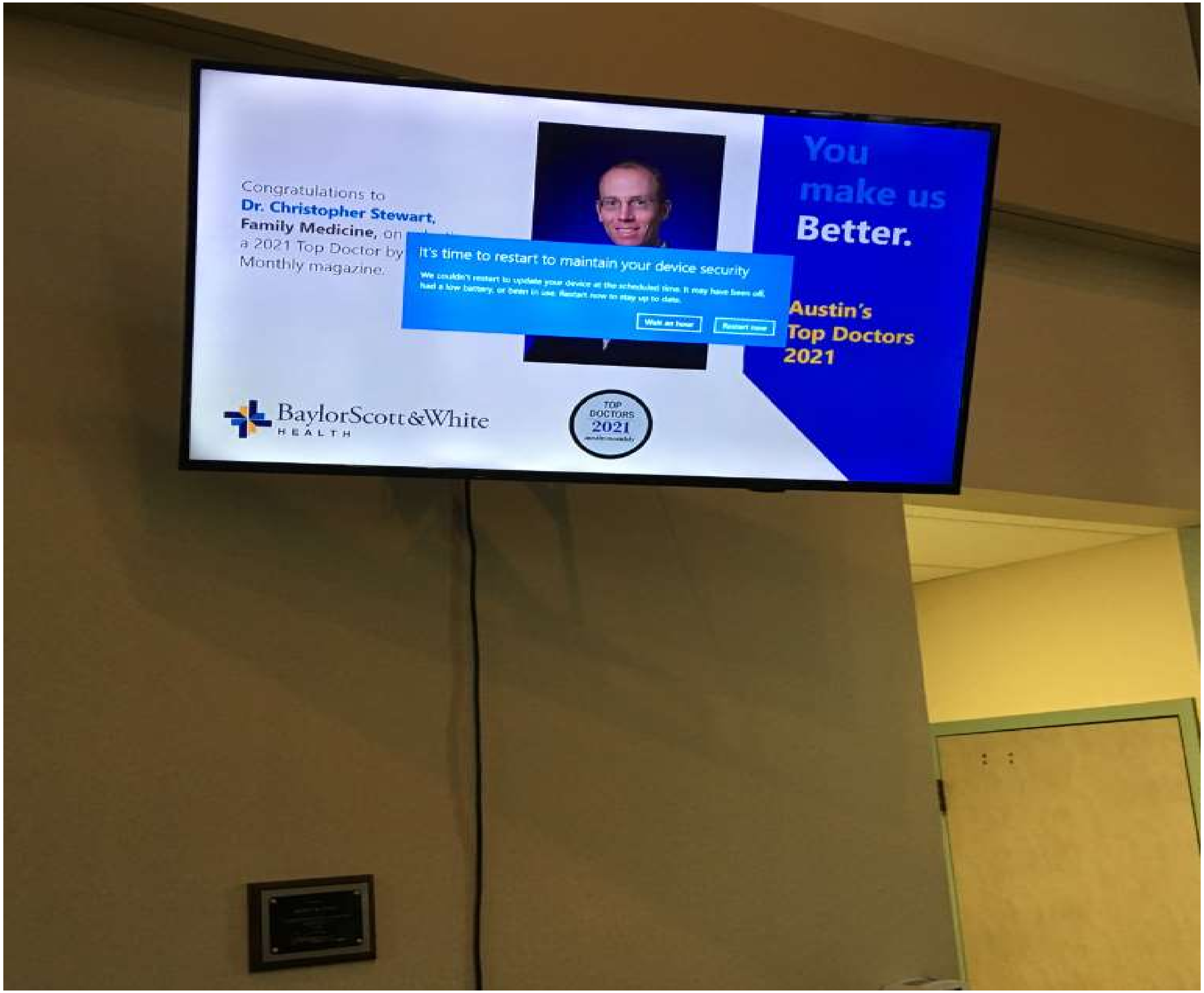
  Same as the first

  Ransomware

  ID, credential theft

tor

- The Onion Router
- Concept
- NSA runs some exit nodes
- 25% evil exit nodes
- https redirect masking
- Crypto exchanges current targets
- Use VPN
- Use explicit https:// scheme



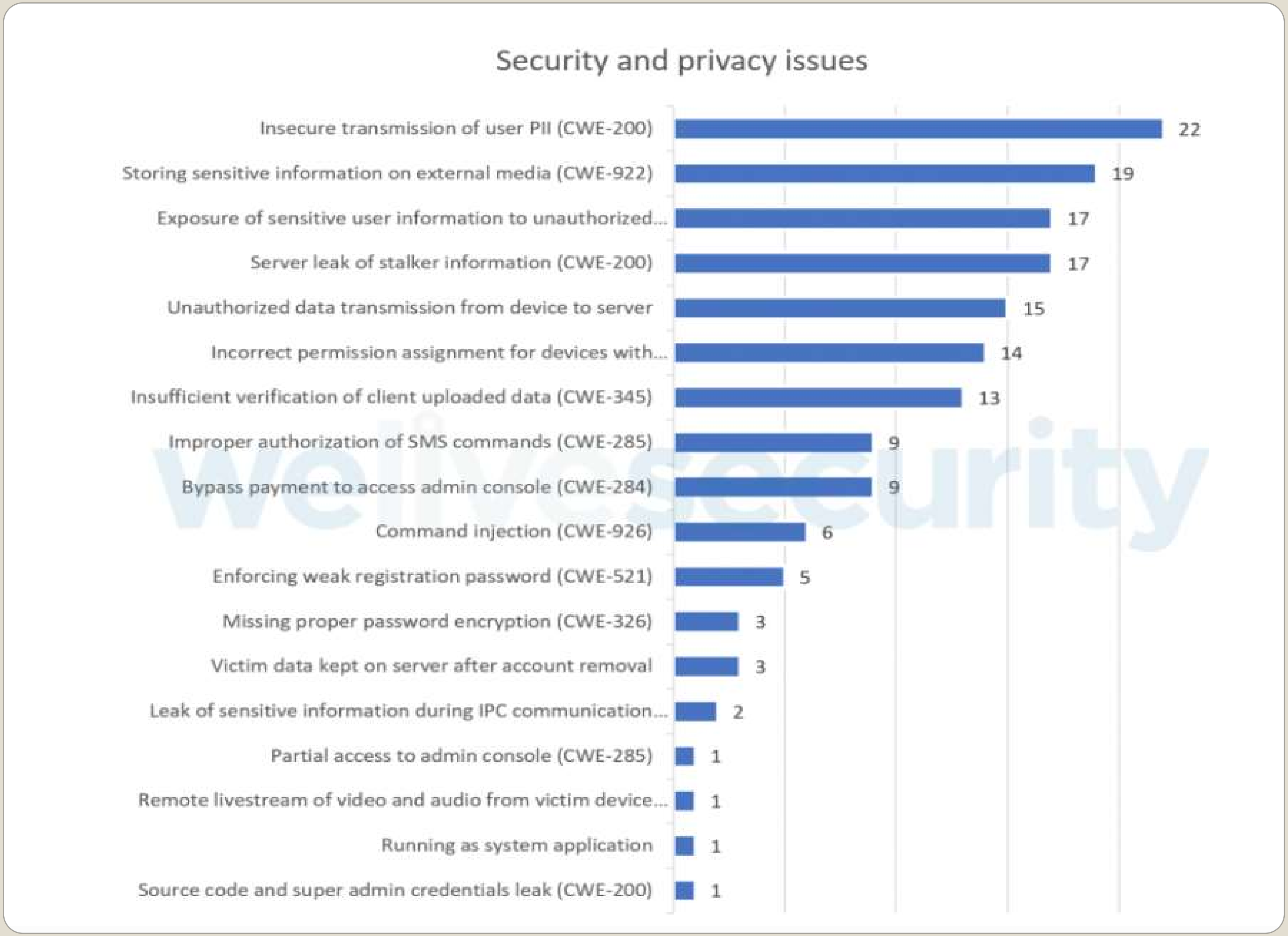
Congratulations to
Dr. Christopher Stewart,
Family Medicine, on
a 2021 Top Doctor by
Monthly magazine.

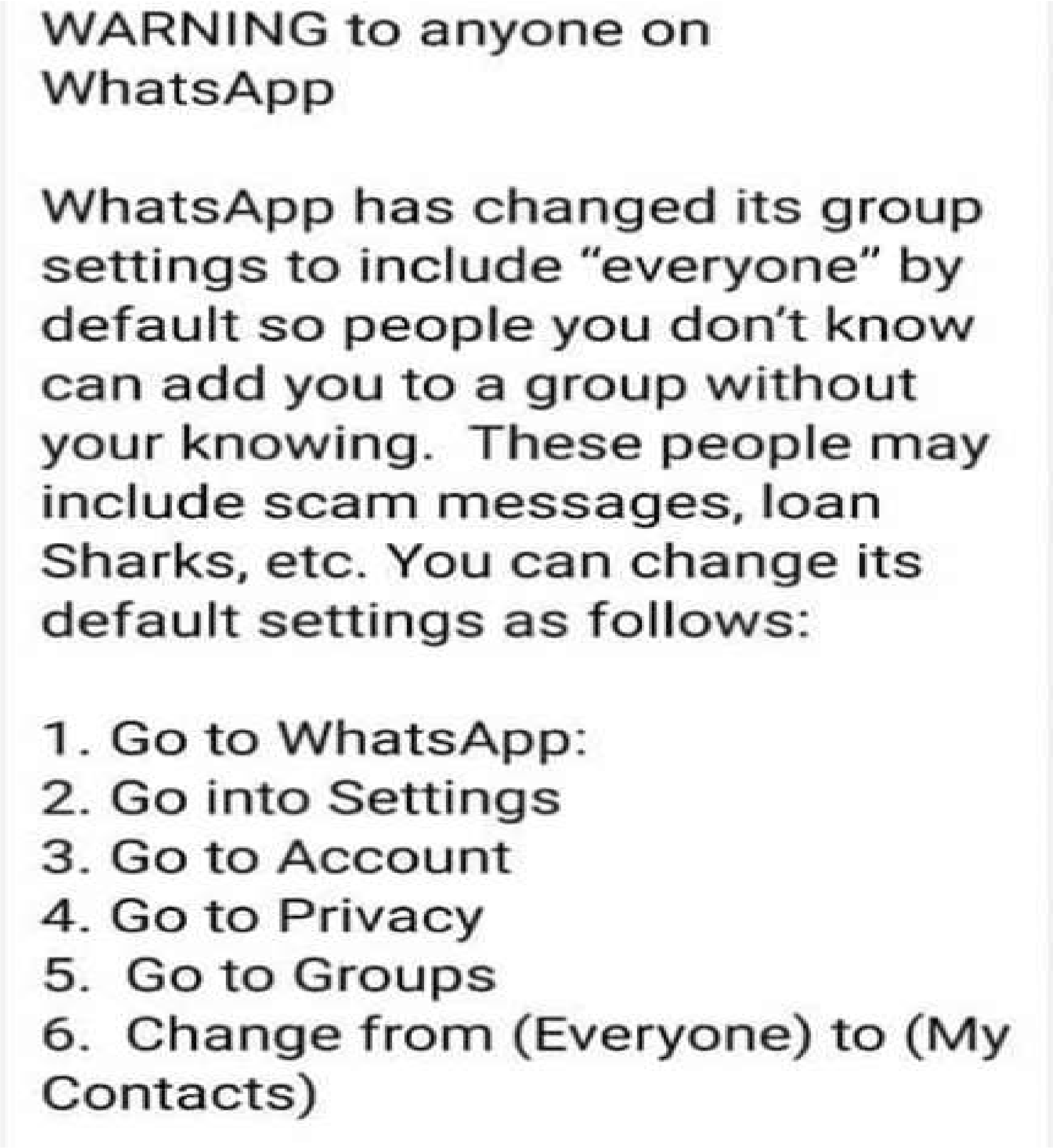
It's time to restart to maintain your device security

We couldn't restart to update your device at the scheduled time. It may have been off, had a low battery, or been in use. Restart now to stay up to date.

- Android
- Spouse, parent, stalker
- Stalker, Victim, Attacker
- Take control of victim’s device
- Take control of stalker’s account
- Intercepting collected data
- Loading fabricated evidence
- Remote code execution on device

Stalker ware


Security and privacy issues
Insecure transmission of user PII (CWE-200) 22
Storing sensitive information on external media (CWE-922) 19
Exposure of sensitive user information to unauthorized... 17
Server leak of stalker information (CWE-200) 17
Unauthorized data transmission from device to server 15
Incorrect permission assignment for devices with... 14
Insufficient verification of client uploaded data (CWE-345) 13
Improper authorization of SMS commands (CWE-285) 9
Bypass payment to access admin console (CWE-284) 9
Command injection (CWE-926) 6
Enforcing weak registration password (CWE-521) 5
Missing proper password encryption (CWE-326) 3
Victim data kept on server after account removal 3
Leak of sensitive information during IPC communication... 2
Partial access to admin console (CWE-285) 1
Remote livestream of video and audio from victim device... 1
Running as system application 1
Source code and super admin credentials leak (CWE-200) 1
welivesecurity

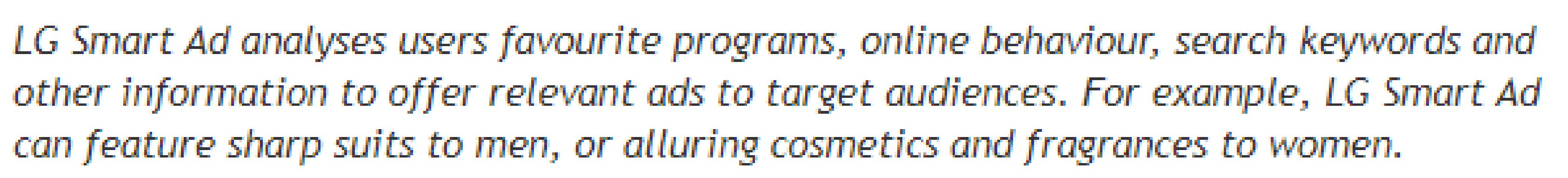


WARNING to anyone on WhatsApp

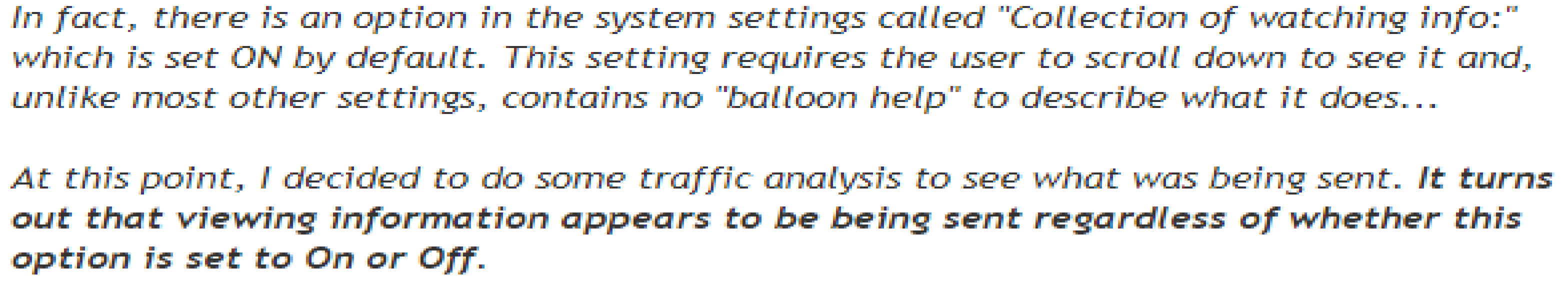
WhatsApp has changed its group settings to include "everyone" by default so people you don't know can add you to a group without your knowing. These people may include scam messages, loan Sharks, etc. You can change its default settings as follows:

1. Go to WhatsApp:
2. Go into Settings
3. Go to Account
4. Go to Privacy
5. Go to Groups
6. Change from (Everyone) to (My Contacts)

- If you give a tv an Internet connection

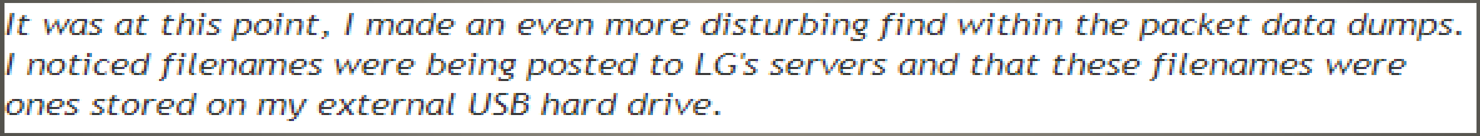


LG Smart Ad analyses users favourite programs, online behaviour, search keywords and other information to offer relevant ads to target audiences. For example, LG Smart Ad can feature sharp suits to men, or alluring cosmetics and fragrances to women.



In fact, there is an option in the system settings called "Collection of watching info:" which is set ON by default. This setting requires the user to scroll down to see it and, unlike most other settings, contains no "balloon help" to describe what it does...

At this point, I decided to do some traffic analysis to see what was being sent. ***It turns out that viewing information appears to be being sent regardless of whether this option is set to On or Off.***



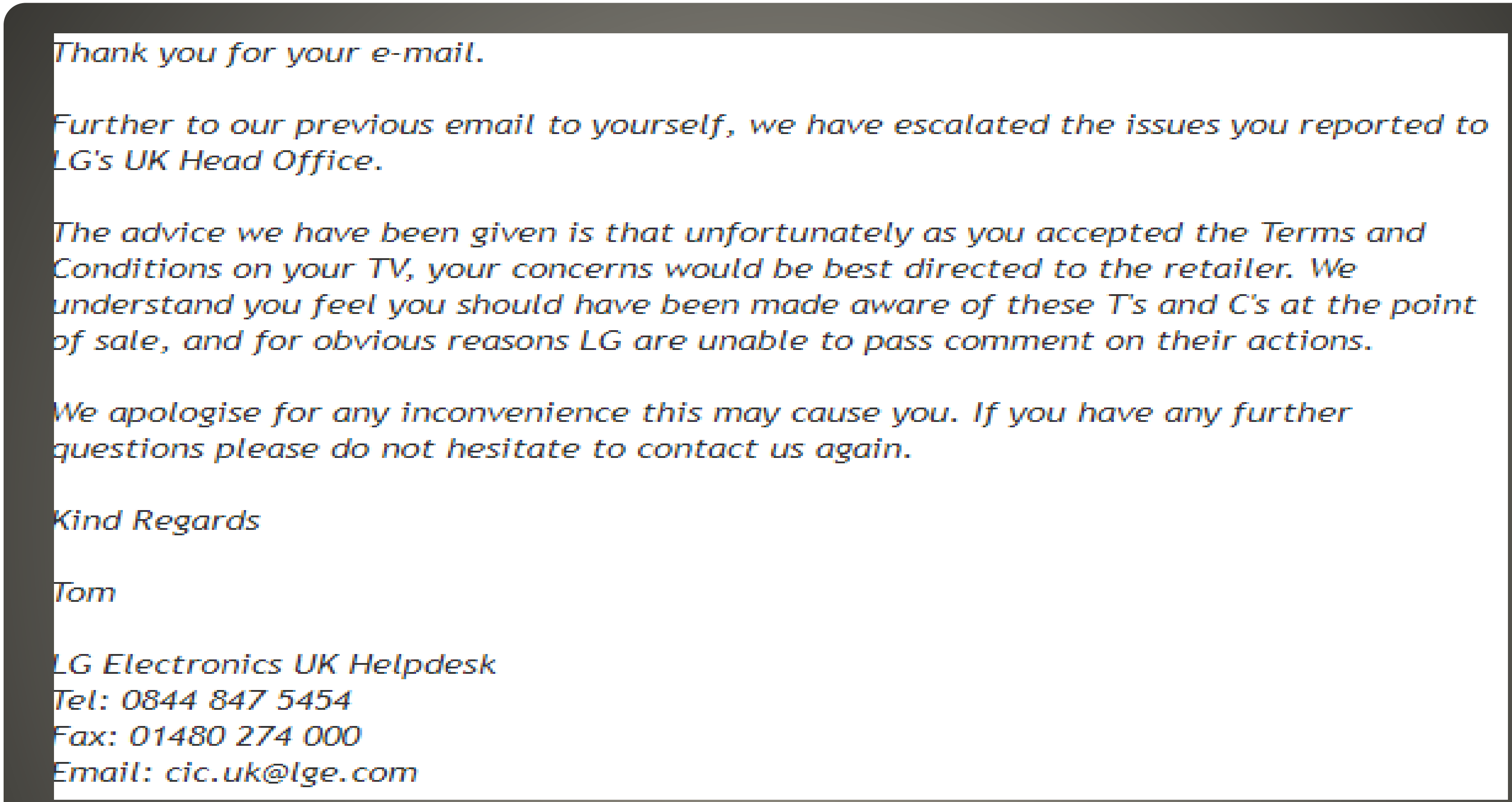
It was at this point, I made an even more disturbing find within the packet data dumps. I noticed filenames were being posted to LG's servers and that these filenames were ones stored on my external USB hard drive.

LG Smart TV

- Add USB drive to LG TV
- File data on USB sent back to LG unencrypted
- “Jack & Jill Xmas morning”

LG Smart TV

LG response



Thank you for your e-mail.

Further to our previous email to yourself, we have escalated the issues you reported to LG's UK Head Office.

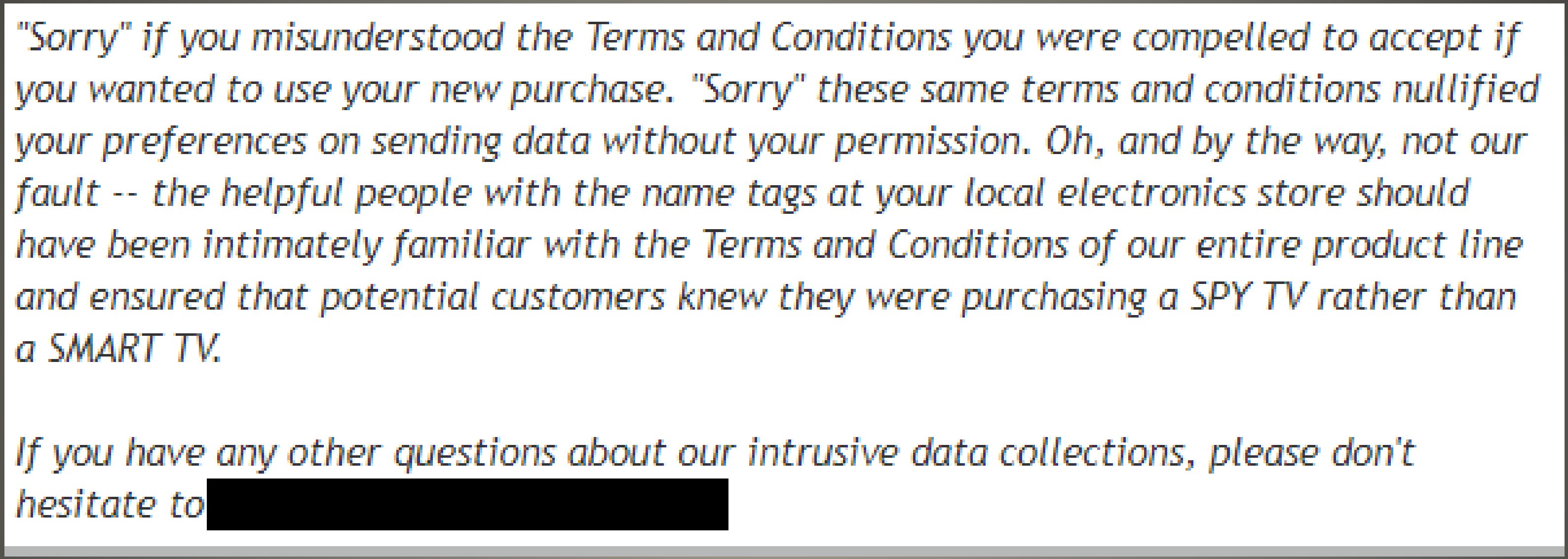
The advice we have been given is that unfortunately as you accepted the Terms and Conditions on your TV, your concerns would be best directed to the retailer. We understand you feel you should have been made aware of these T's and C's at the point of sale, and for obvious reasons LG are unable to pass comment on their actions.

We apologise for any inconvenience this may cause you. If you have any further questions please do not hesitate to contact us again.

Kind Regards

Tom

LG Electronics UK Helpdesk
Tel: 0844 847 5454
Fax: 01480 274 000
Email: cic.uk@lge.com

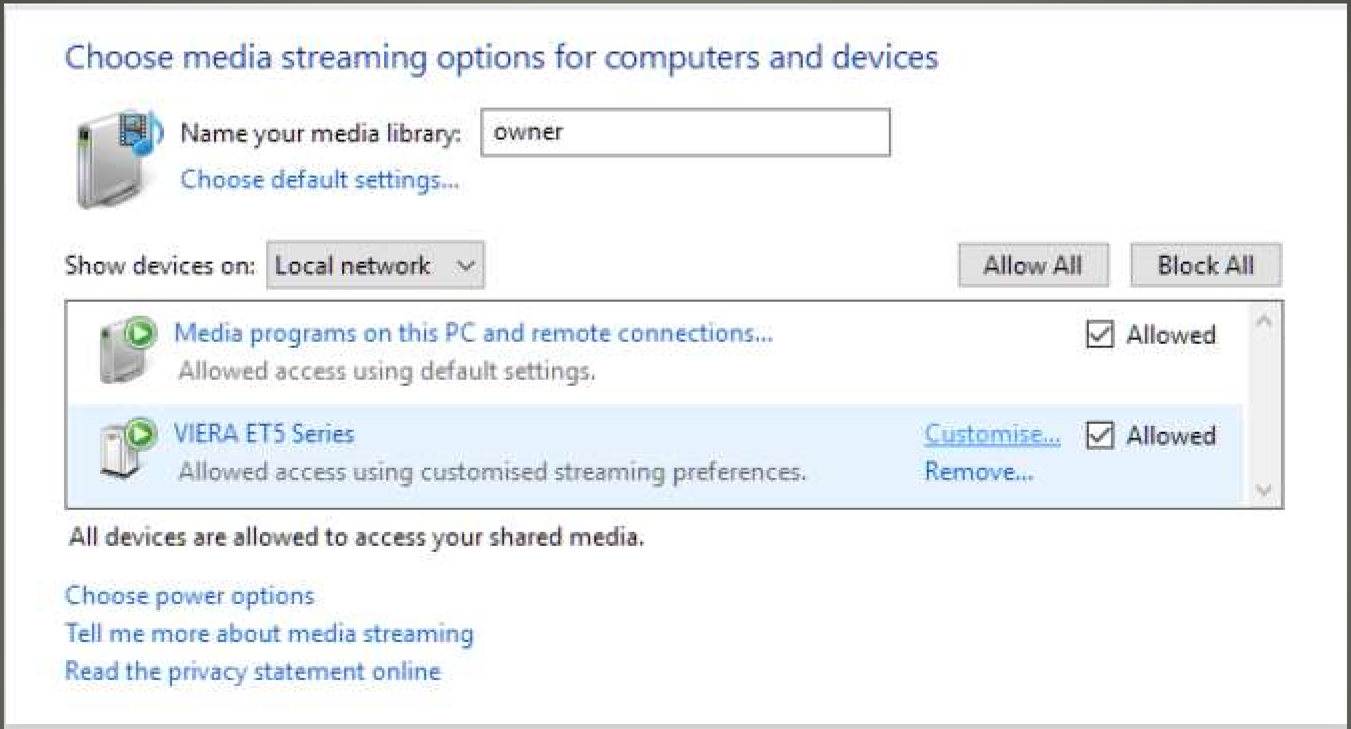


"Sorry" if you misunderstood the Terms and Conditions you were compelled to accept if you wanted to use your new purchase. "Sorry" these same terms and conditions nullified your preferences on sending data without your permission. Oh, and by the way, not our fault -- the helpful people with the name tags at your local electronics store should have been intimately familiar with the Terms and Conditions of our entire product line and ensured that potential customers knew they were purchasing a SPY TV rather than a SMART TV.

If you have any other questions about our intrusive data collections, please don't hesitate to [redacted]

```
Widget InstallSamyGO-H for Samsung SmartTV H-series
************************ USB test procedure ****************************************
[illegible]
[illegible]
[illegible]
[illegible] [OK]

************************ Setup SamyGO files ****************************************
Copying from [illegible]
Copying from [illegible]
Copying from [illegible] [OK]
Copying from [illegible] [OK]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible] [OK]

[illegible]

Press Enter for activation InstallSamyGO-H

************************ Root SamyGO files ****************************************

[illegible] [OK]
[illegible] [OK]
[illegible] [OK]
[illegible]

[illegible]

[illegible] TV [illegible]

Free memory: 2575 Mbytes
```

Samsung Smart TV with camera



Choose media streaming options for computers and devices

Name your media library: owner

Choose default settings...

Show devices on: Local network

Media programs on this PC and remote connections... ☑ Allowed
Allowed access using default settings.

VIERA ET5 Series Customise... ☑ Allowed
Allowed access using customised streaming preferences. Remove...

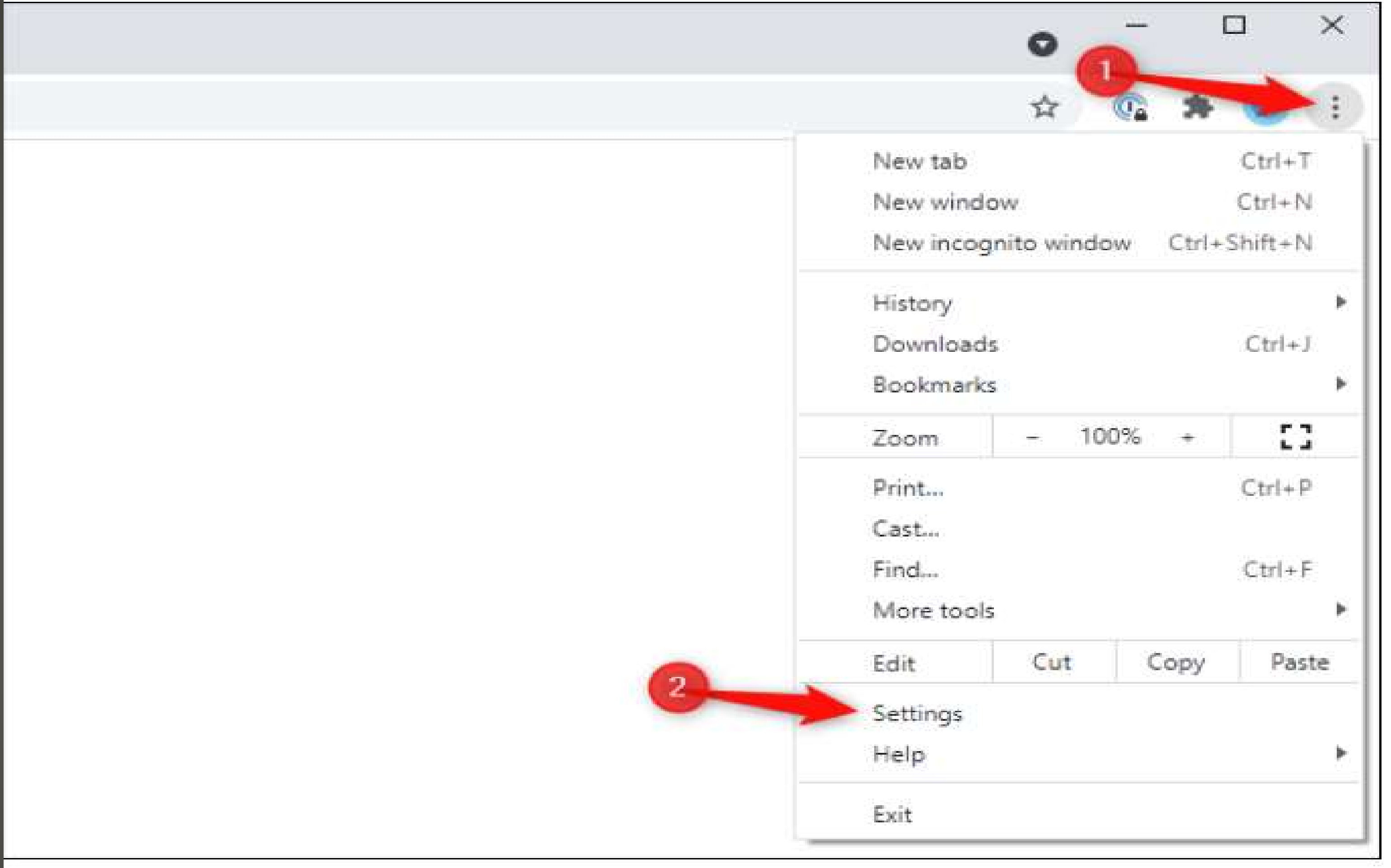
All devices are allowed to access your shared media.

Choose power options
Tell me more about media streaming
Read the privacy statement online

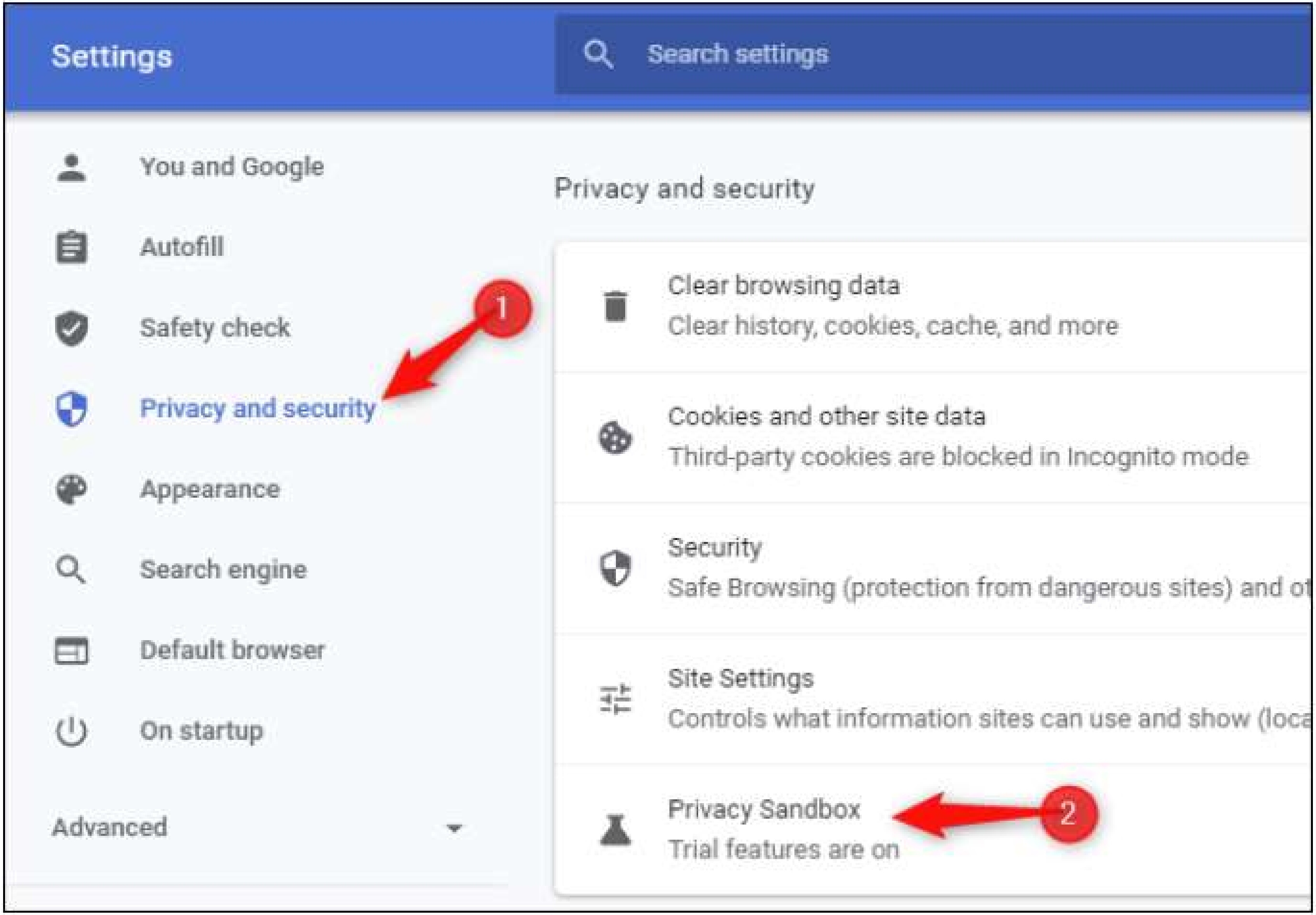
sigh

Google Chrome Privacy Sandbox

- Federated Learning of Cohorts (FLoC)
- *Privacy-first future of web advertising*
- Replace / supplement tracking cookies
- Advertising ID - unique
- Browser side analysis => cohort
- Enabled at Google’s time and choosing



Opt-Out (disable?)



Privacy and security

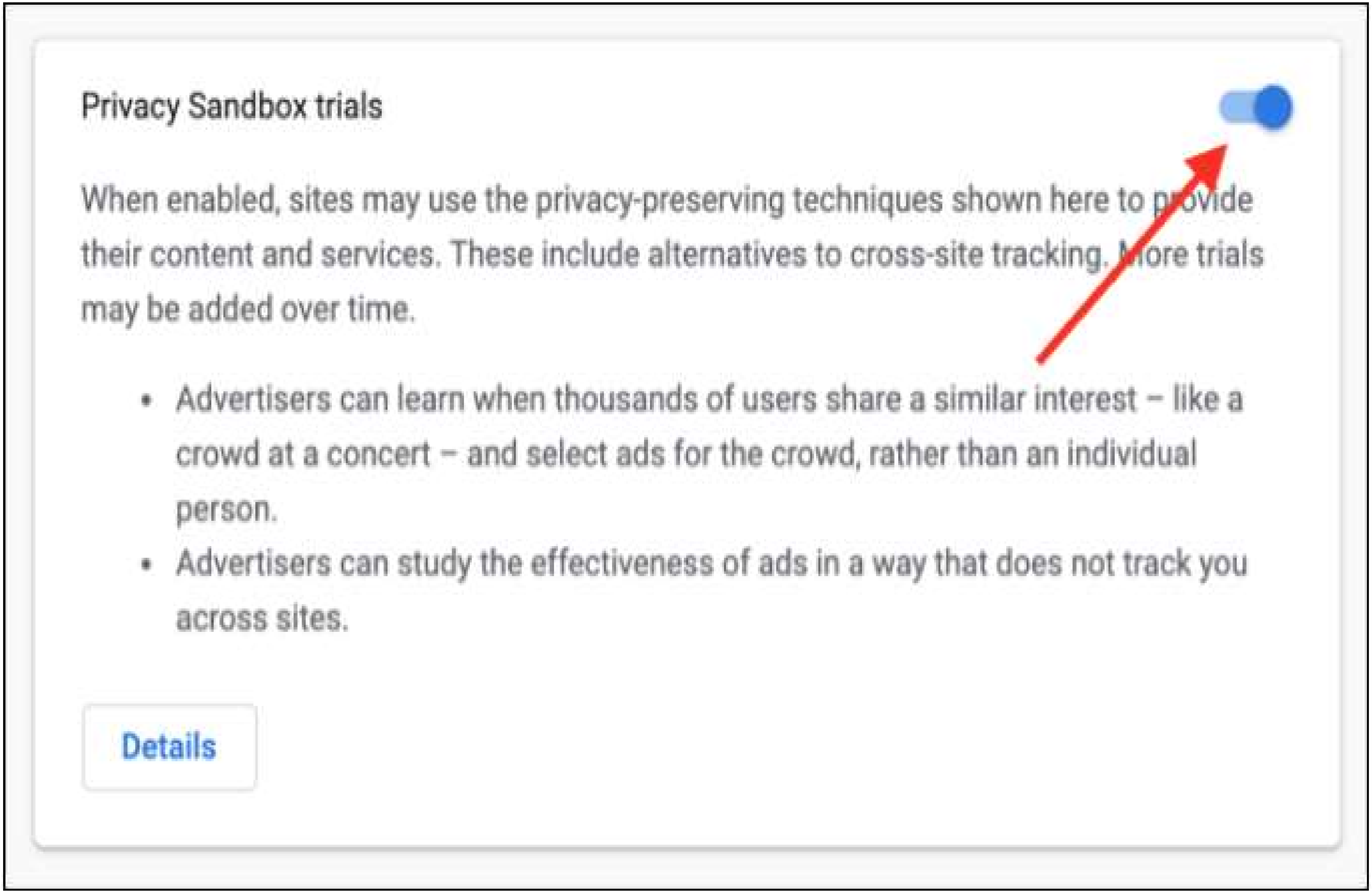
Clear browsing data
Clear history, cookies, cache, and more

Cookies and other site data
Third-party cookies are blocked in Incognito mode

Security
Safe Browsing (protection from dangerous sites) and ot

Site Settings
Controls what information sites can use and show (loca

Privacy Sandbox
Trial features are on



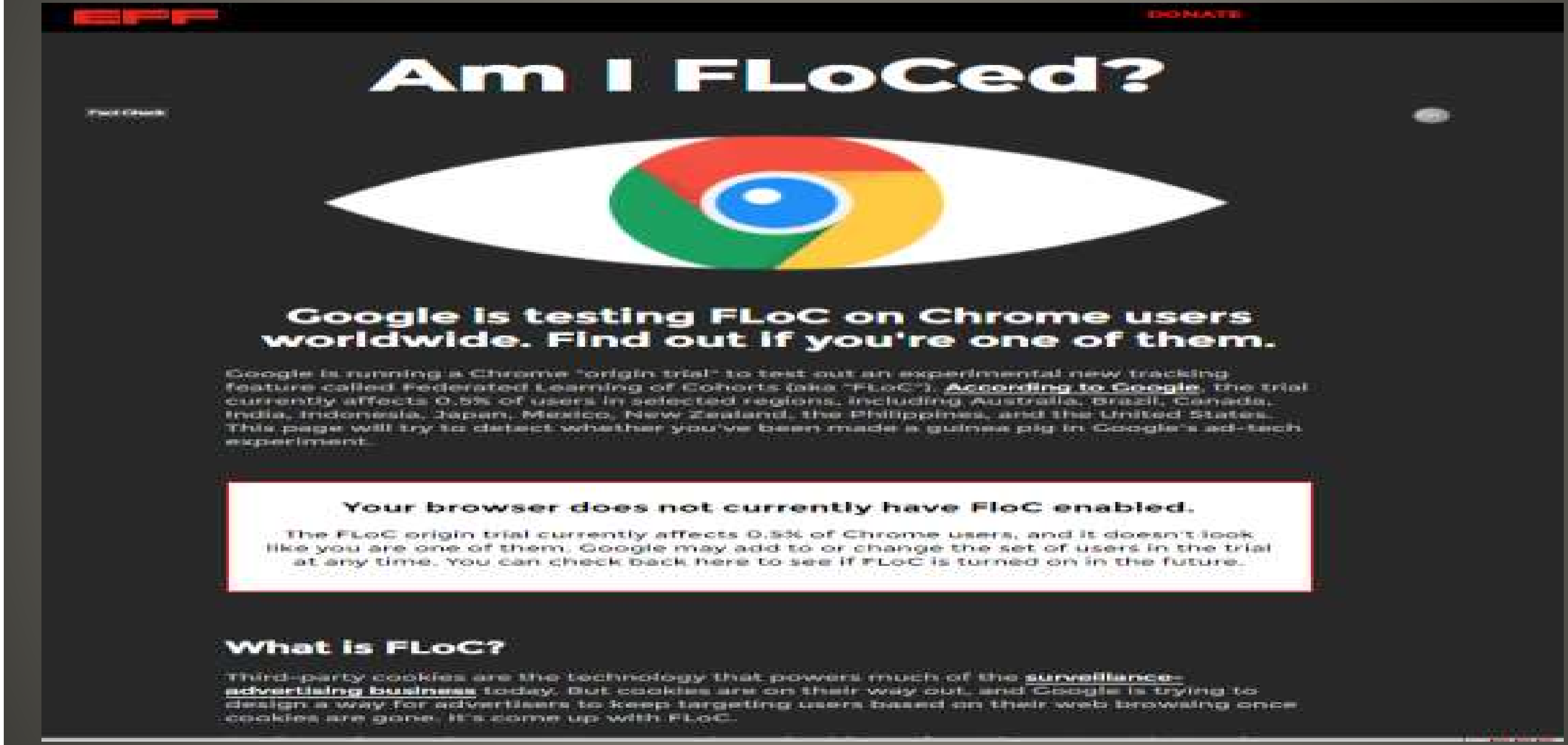
Privacy Sandbox trials

When enabled, sites may use the privacy-preserving techniques shown here to provide their content and services. These include alternatives to cross-site tracking. More trials may be added over time.

- Advertisers can learn when thousands of users share a similar interest – like a crowd at a concert – and select ads for the crowd, rather than an individual person.
- Advertisers can study the effectiveness of ads in a way that does not track you across sites.

- EFF site

https://amifloced.org/



Am I FLoCed?

Google is testing FLoC on Chrome users worldwide. Find out if you're one of them.

Google is running a Chrome "origin trial" to test out an experimental new tracking feature called Federated Learning of Cohorts (aka "FLoC"). According to Google, the trial currently affects 0.5% of users in selected regions, including Australia, Brazil, Canada, India, Indonesia, Japan, Mexico, New Zealand, the Philippines, and the United States. This page will try to detect whether you've been made a guinea pig in Google's ad-tech experiment.

Your browser does not currently have FloC enabled.

The FLoC origin trial currently affects 0.5% of Chrome users, and it doesn't look like you are one of them. Google may add to or change the set of users in the trial at any time. You can check back here to see if FLoC is turned on in the future.

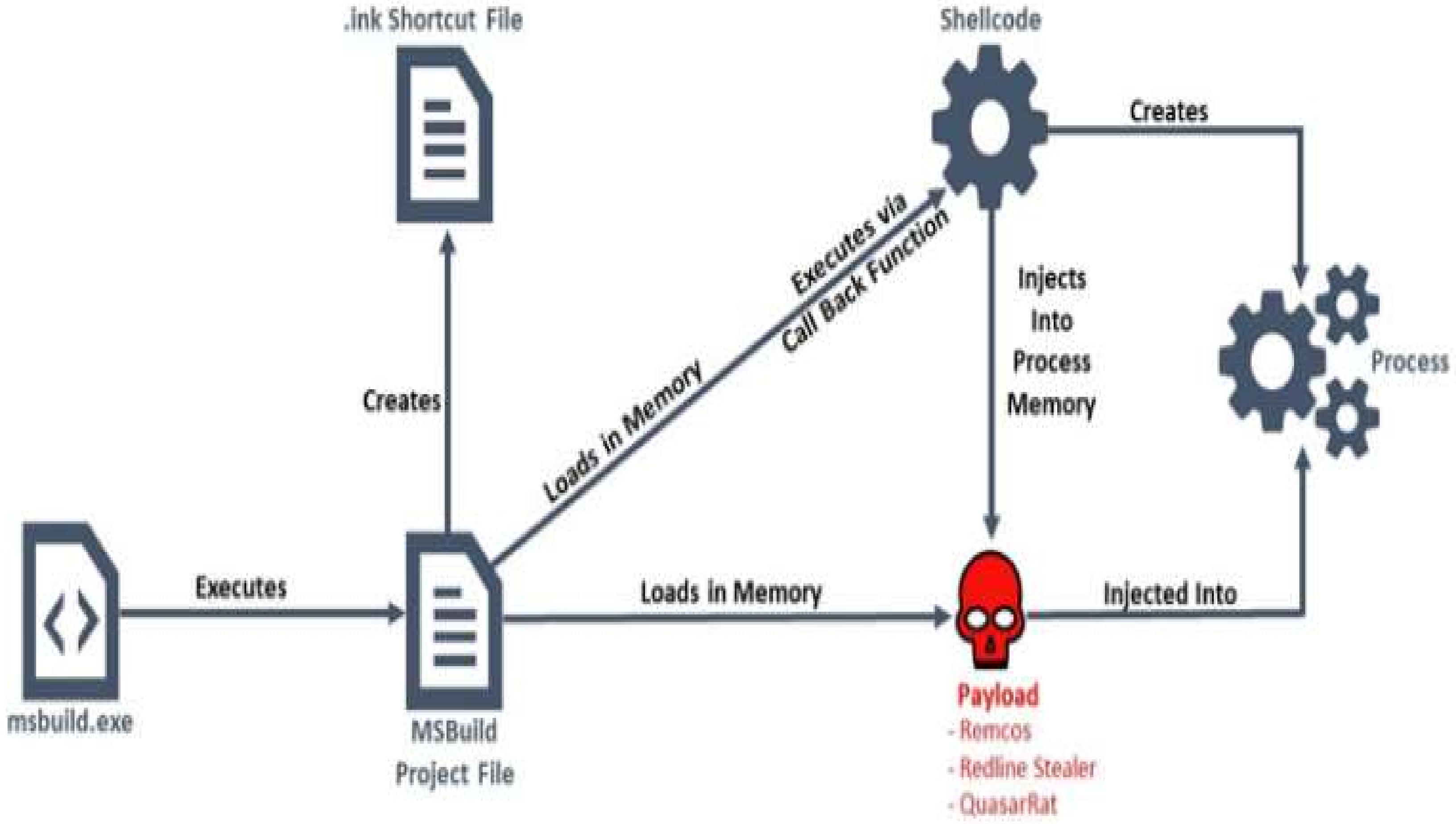
What is FLoC?

Third-party cookies are the technology that powers much of the surveillance-advertising business today. But cookies are on their way out, and Google is trying to design a way for advertisers to keep targeting users based on their web browsing once cookies are gone. It's come up with FLoC.

Am I FLoCed?

Microsoft Build Engine attacks

- Microsoft Build Engine (MS Build)
- Tool for compiling, packaging, deploying
- Deliver fileless - deploy in memory
- Leaves no trace


.lnk Shortcut File
Shellcode
Creates
Executes via
Call Back Function
Injects
Into
Process
Memory
Process
Creates
Loads in Memory
Executes
Loads in Memory
Injected Into
msbuild.exe
MSBuild
Project File
Payload
- Remcos
- Redline Stealer
- QuasarRat

- US Defense Information Systems Agency

"a more secure, coordinated, seamless, transparent, and cost-effective IT architecture that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyber threat."

Zero Trust Reference Architecture

DISA Zero Trust

- 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