Sun City Computer Club

Cyber Security SIG

June 17, 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

- Pulse Secure access Metropolitan Transit Authority (MTA) New York
  Efforts to hide tracks (sic)
  Backdoors left behind?
  18-month lag
- DOJ Ransomware same level as terrorism
- Computer Fraud & Abuse Act (1986)
  Police officer abuse of granted access
- US Army rescinds IoT workplace ban
- McDonalds drive-thru AI robot
- Patch Tuesday ~~Microsoft~~
  Intel, ABOBE everything
- Next Unit of Computing (NUC)
- Starlink disk shutdown at 122° F

Current Issues

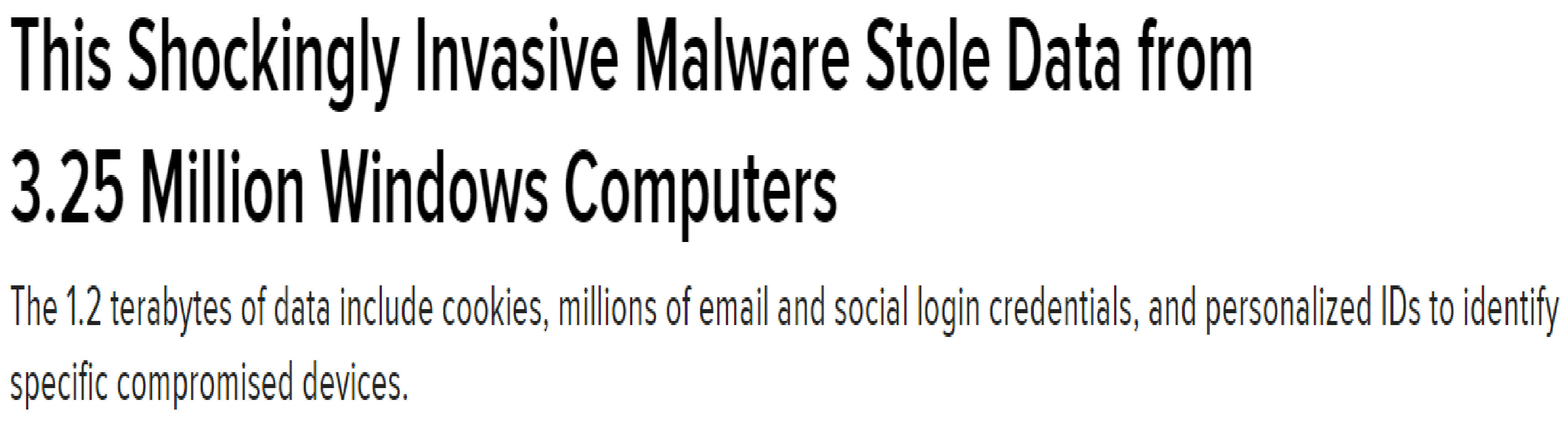
- 3M PCs data stolen & posted

credentials, cookies, autofill data, payment information, images, screenshots of users, messaging data, emails, gaming data, filesharing, …

ASSUME YOUR DATA is CLONED and AVAILABLE

- Jackware Much greater impact
  Much greater amplification
  Much easier supply chain attack
- Colonial pipeline – leaked password on Dark Web? Unused VPN service

Current Issues



This Shockingly Invasive Malware Stole Data from 3.25 Million Windows Computers

The 1.2 terabytes of data include cookies, millions of email and social login credentials, and personalized IDs to identify specific compromised devices.

Windows out of Band Patch?

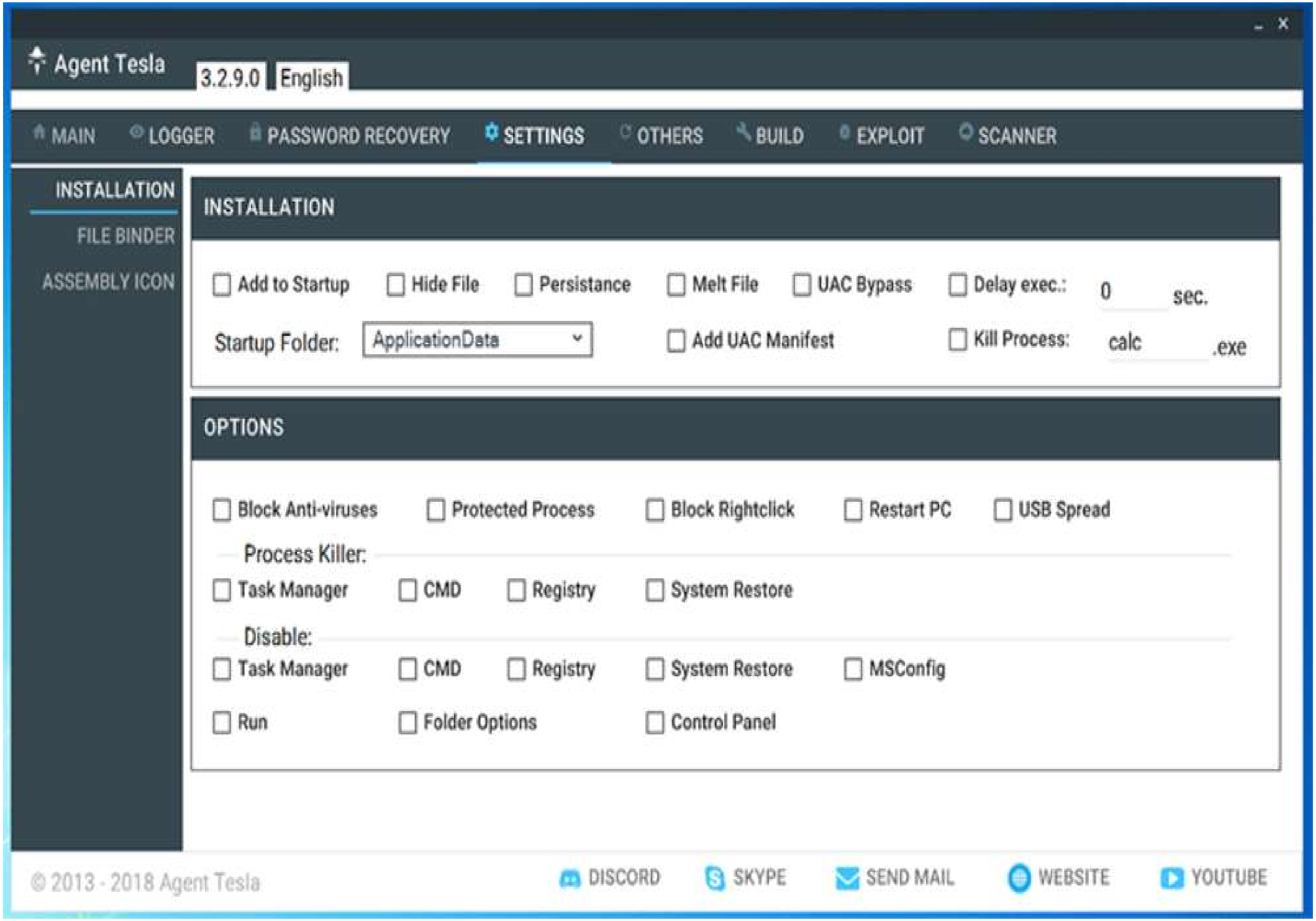
- Password stealing program
- *Strictly for monitoring your computer*
- Yeah, but

  How to evade anti-virus

  use vulnerabilities to install product

  bundle program in images, text, macros,…
- 2018 Fully functional information stealer

Agent Tesla



INSTALLATION

□ Add to Startup □ Hide File □ Persistance □ Melt File □ UAC Bypass □ Delay exec.: 0 sec.

Startup Folder: ApplicationData □ Add UAC Manifest □ Kill Process: calc .exe

OPTIONS

□ Block Anti-viruses □ Protected Process □ Block Rightclick □ Restart PC □ USB Spread

Process Killer:

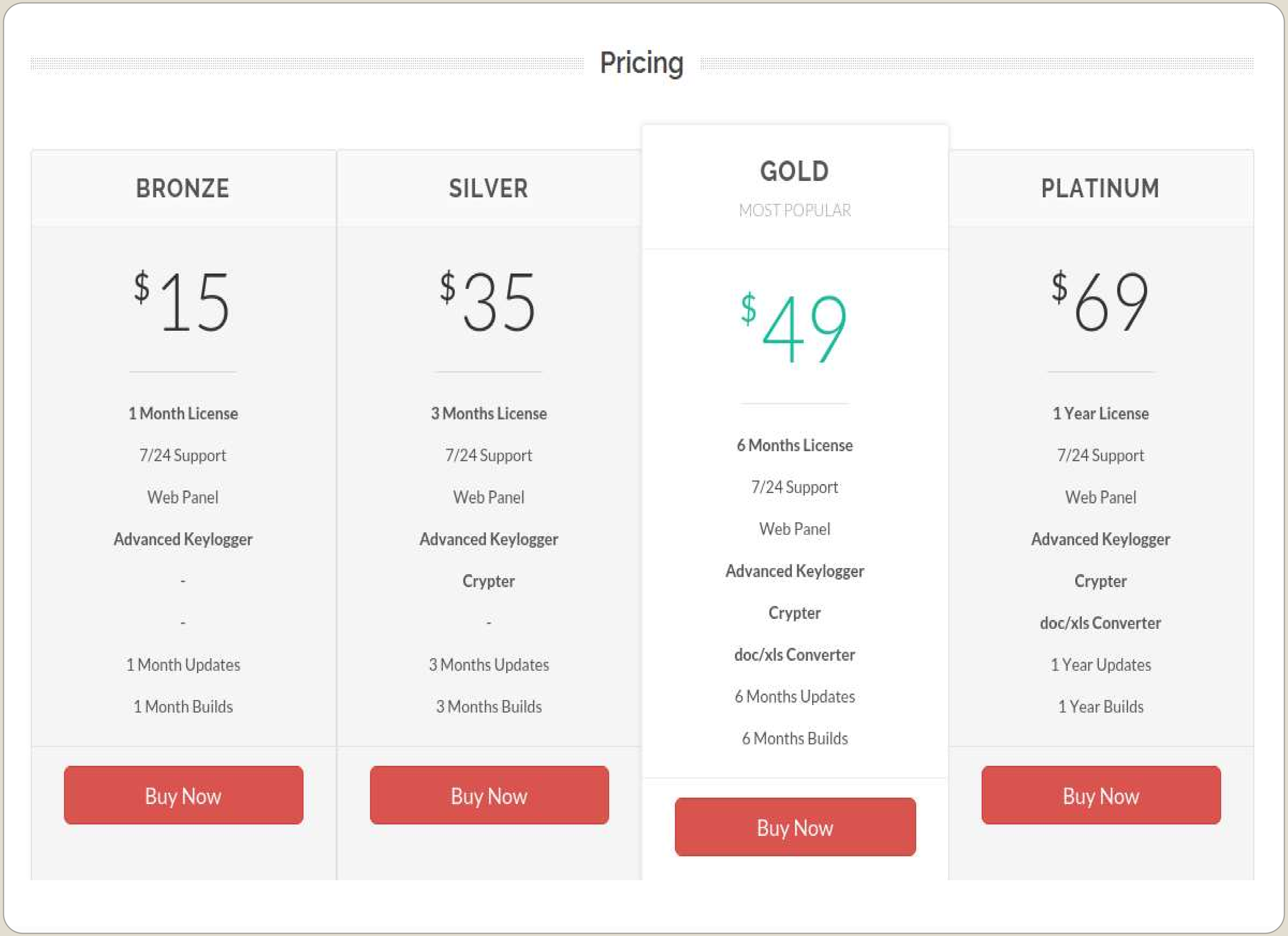
□ Task Manager □ CMD □ Registry □ System Restore

Disable:

□ Task Manager □ CMD □ Registry □ System Restore □ MSConfig

□ Run □ Folder Options □ Control Panel

© 2013 - 2018 Agent Tesla



Pricing

BRONZE	SILVER	GOLD MOST POPULAR	PLATINUM
$15	$35	$49	$69
1 Month License	**3 Months License**	**6 Months License**	**1 Year License**
7/24 Support	7/24 Support	7/24 Support	7/24 Support
Web Panel	Web Panel	Web Panel	Web Panel
Advanced Keylogger	**Advanced Keylogger**	**Advanced Keylogger**	**Advanced Keylogger**
-	**Crypter**	**Crypter**	**Crypter**
-	-	**doc/xls Converter**	**doc/xls Converter**
1 Month Updates	3 Months Updates	6 Months Updates	1 Year Updates
1 Month Builds	3 Months Builds	6 Months Builds	1 Year Builds
Buy Now	Buy Now	Buy Now	Buy Now

- Logs keys and clipboards
- Captures screens and video
- Form grabbing

- GoToMyPC, VNC, LogMeIn
- LuminosityLink

Agent Tesla

Current Issues Venmo

- Venmo

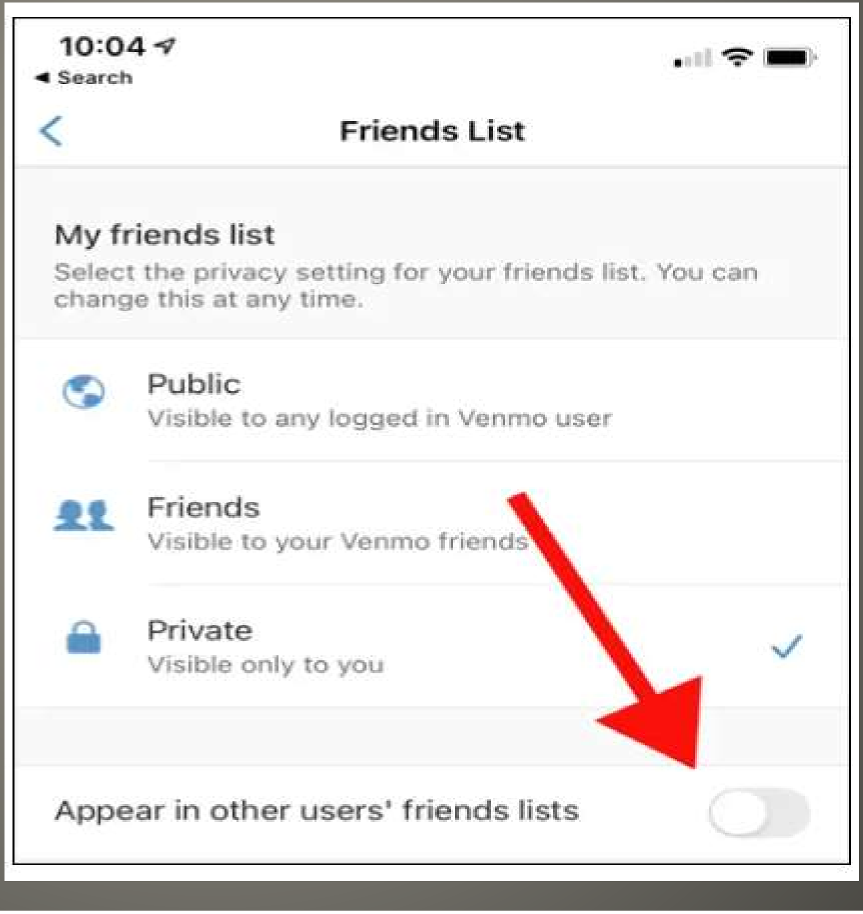
Private transactions

Friends list – not

Therapist

Political

- IF Android does NOT allow …
- Settings > Friends List Private



Friends List

My friends list

Select the privacy setting for your friends list. You can change this at any time.

Public
Visible to any logged in Venmo user

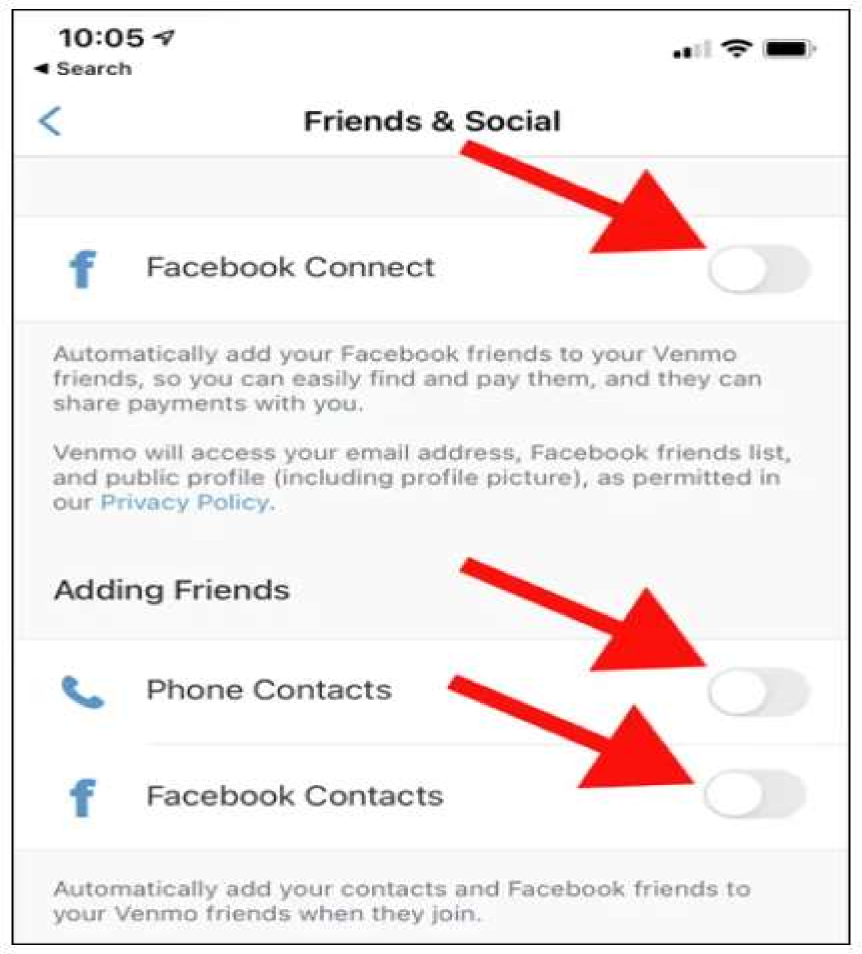
Friends
Visible to your Venmo friends

Private ✓
Visible only to you

Appear in other users' friends lists

Venmo

- Settings > Friends & Social



10:05

◂ Search

Friends & Social

Facebook Connect

Automatically add your Facebook friends to your Venmo friends, so you can easily find and pay them, and they can share payments with you.

Venmo will access your email address, Facebook friends list, and public profile (including profile picture), as permitted in our Privacy Policy.

Adding Friends

Phone Contacts

Facebook Contacts

Automatically add your contacts and Facebook friends to your Venmo friends when they join.

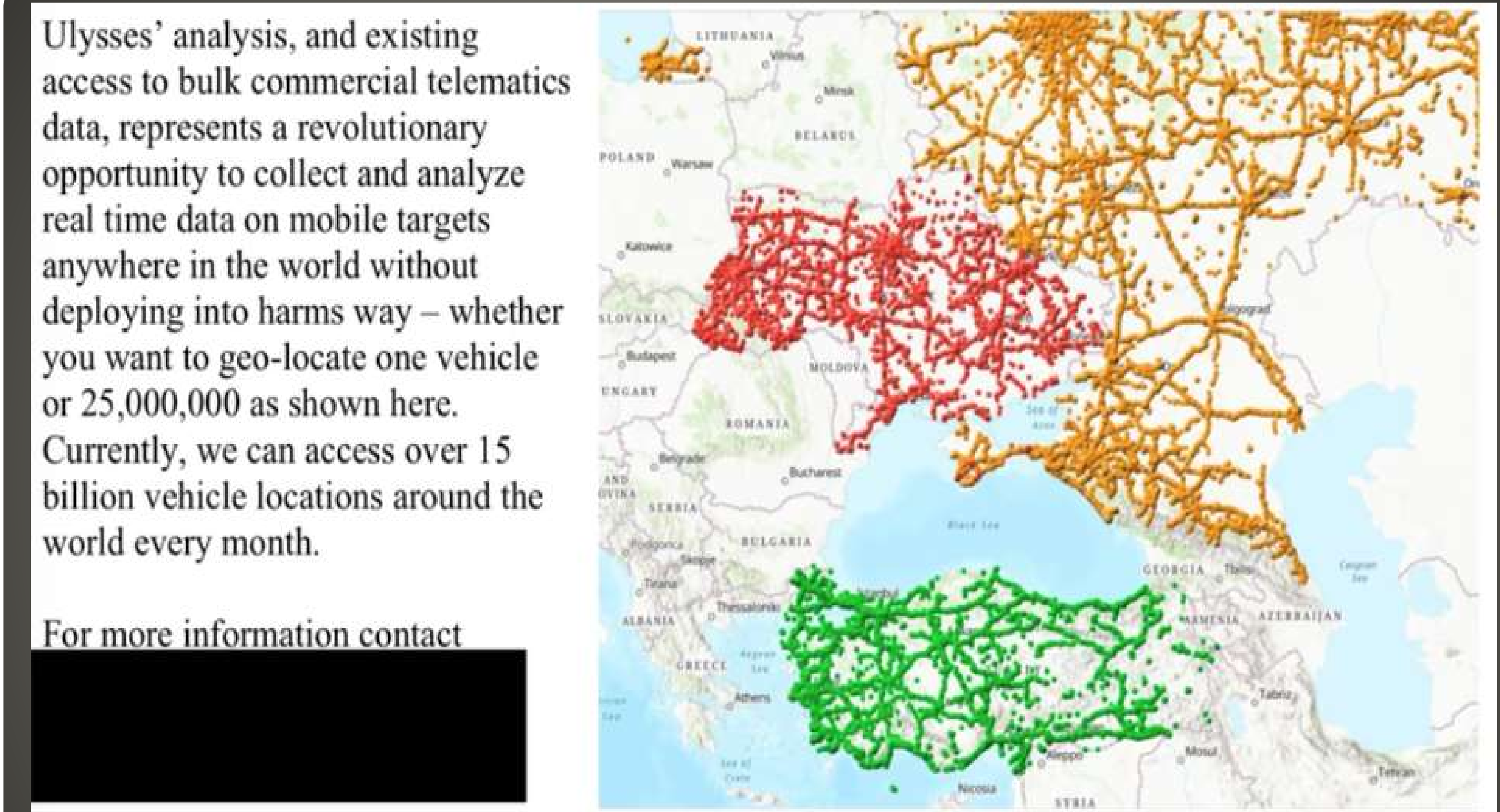
Venmo

- SolarMarker

  Search Engine Optimization PDF
- Otonomo – granular vehicle location data

  ToS – Free Trial   40 million vehicles
- Ulysses Group

Current Issues



Ulysses' analysis, and existing access to bulk commercial telematics data, represents a revolutionary opportunity to collect and analyze real time data on mobile targets anywhere in the world without deploying into harms way – whether you want to geo-locate one vehicle or 25,000,000 as shown here. Currently, we can access over 15 billion vehicle locations around the world every month.

For more information contact

[redacted]

A SECTION OF THE DOCUMENT OBTAINED BY MOTHERBOARD. IMAGE: MOTHERBOARD

Ulysses Group

- Salaat First (Prayer Times)

  Location data needed

  Location data sold
- TikTok US privacy change

  "may collect biometric identifiers and biometric information" from its users' content. This includes things like *"faceprints and voiceprints,"* the policy explained.

  Response to Illinois Biometric Information Privacy Act ?

  $92M (Facebook $650M)
- States with biometric statutes:

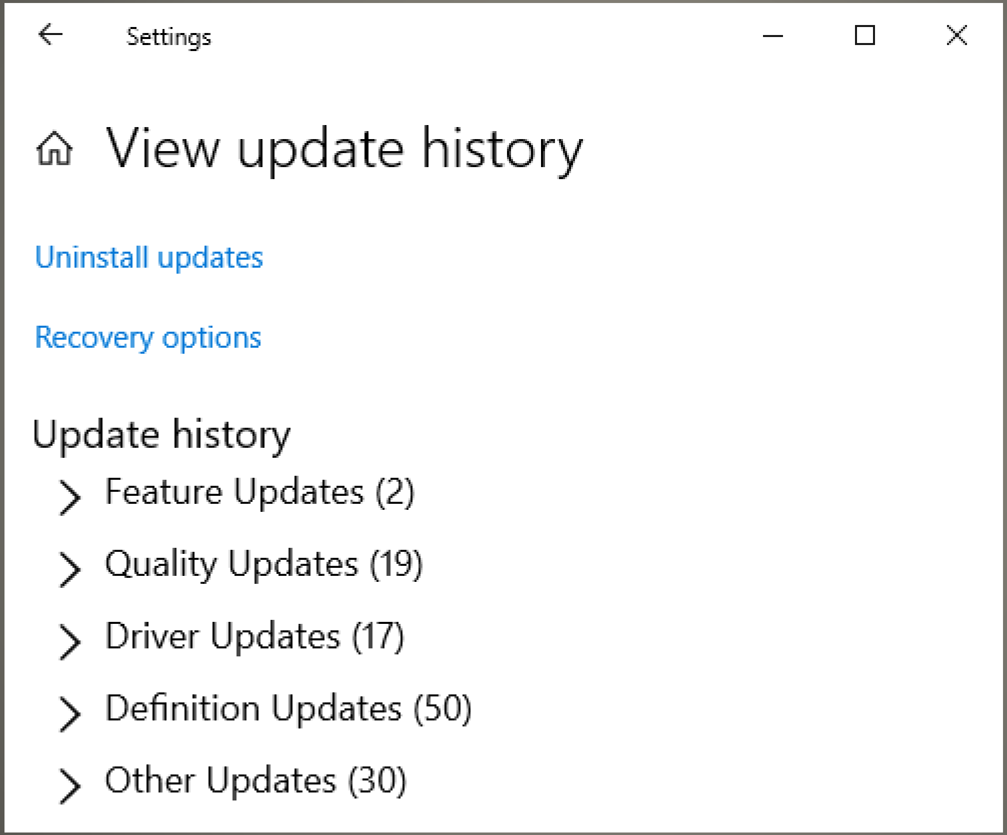
  Illinois, California, New York, Washington, Texas

Current Issues

- Windows Defender Patch
- Recent Signature updates

Current Issues

- Since May 15, 2021



Settings

View update history

Uninstall updates

Recovery options

Update history

- Feature Updates (2)
- Quality Updates (19)
- Driver Updates (17)
- Definition Updates (50)
- Other Updates (30)

Windows Defender Updates

Anom

- 800 Criminals
- 20 Countries
- 27 million messages
- 2018 –
- Unlock password wiped device
- Criminal “flipped” at demise of another service

- Scammers getting more real than real
- *Didn’t you read the presentation about this?*
- EU Court of Justice

"Under certain conditions, a national supervisory authority may exercise its power to bring any alleged infringement of the GDPR before a court of a member state, even though that authority is not the lead supervisory authority,"

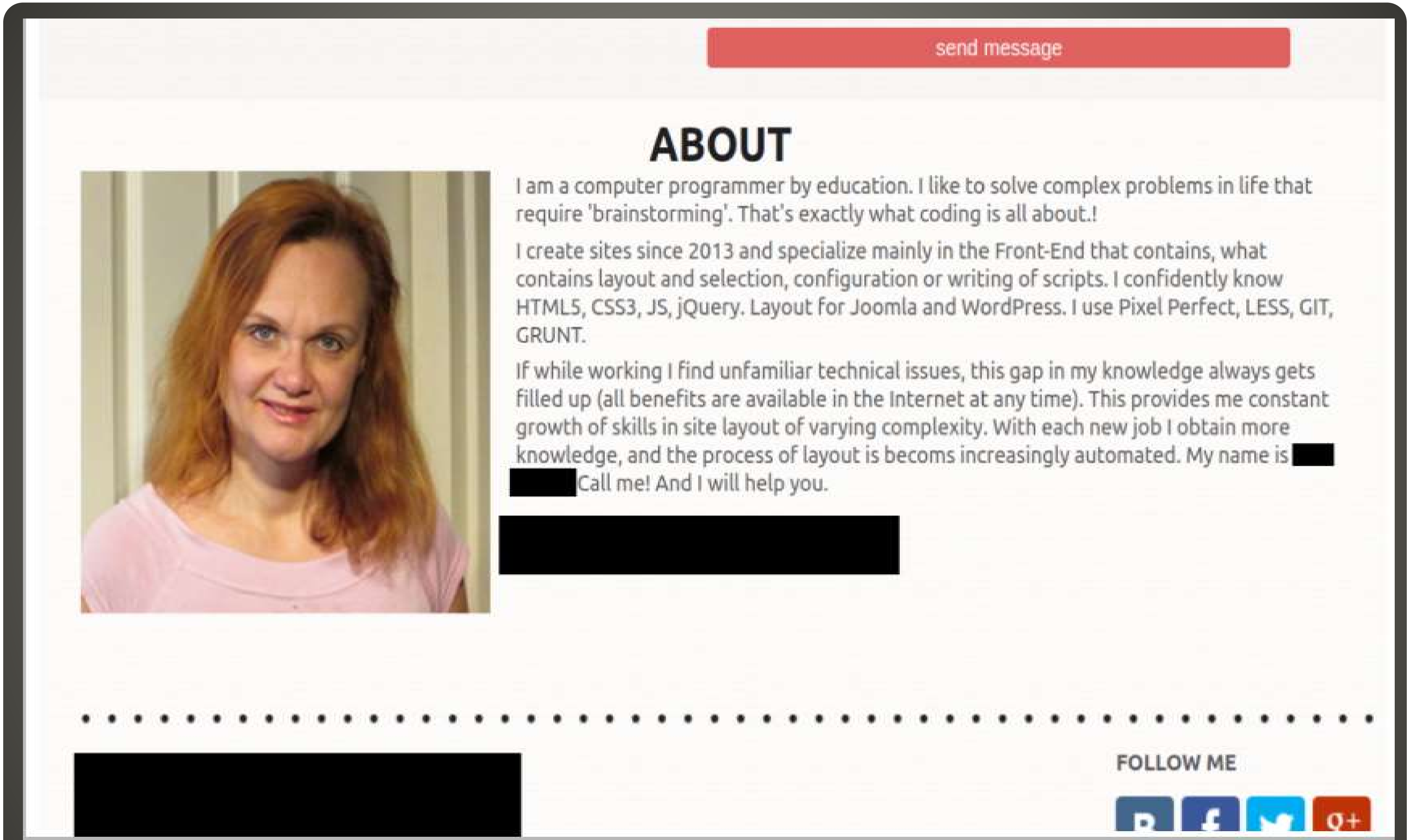
Current Issues

- VW/Audi data leak

  3.3 Million

  Name, mailing address, eMail address, phone number(s), drivers license, DoB, SSN, …
-

Current Issues



ABOUT

I am a computer programmer by education. I like to solve complex problems in life that require 'brainstorming'. That's exactly what coding is all about.!

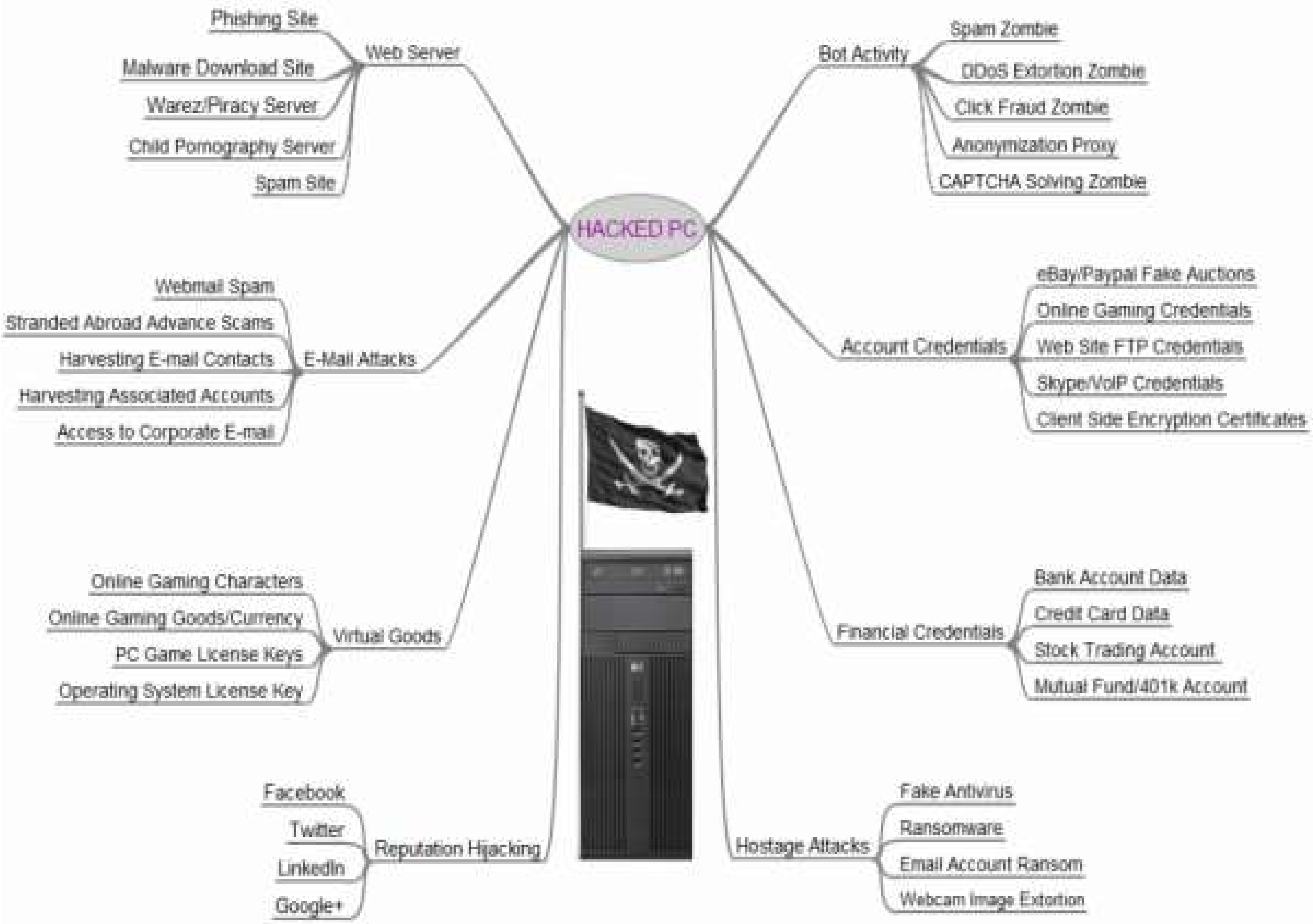
I create sites since 2013 and specialize mainly in the Front-End that contains, what contains layout and selection, configuration or writing of scripts. I confidently know HTML5, CSS3, JS, jQuery. Layout for Joomla and WordPress. I use Pixel Perfect, LESS, GIT, GRUNT.

If while working I find unfamiliar technical issues, this gap in my knowledge always gets filled up (all benefits are available in the Internet at any time). This provides me constant growth of skills in site layout of varying complexity. With each new job I obtain more knowledge, and the process of layout is becoms increasingly automated. My name is [redacted] Call me! And I will help you.

[redacted]

[redacted]

Your concept of a Ransomware Hacker

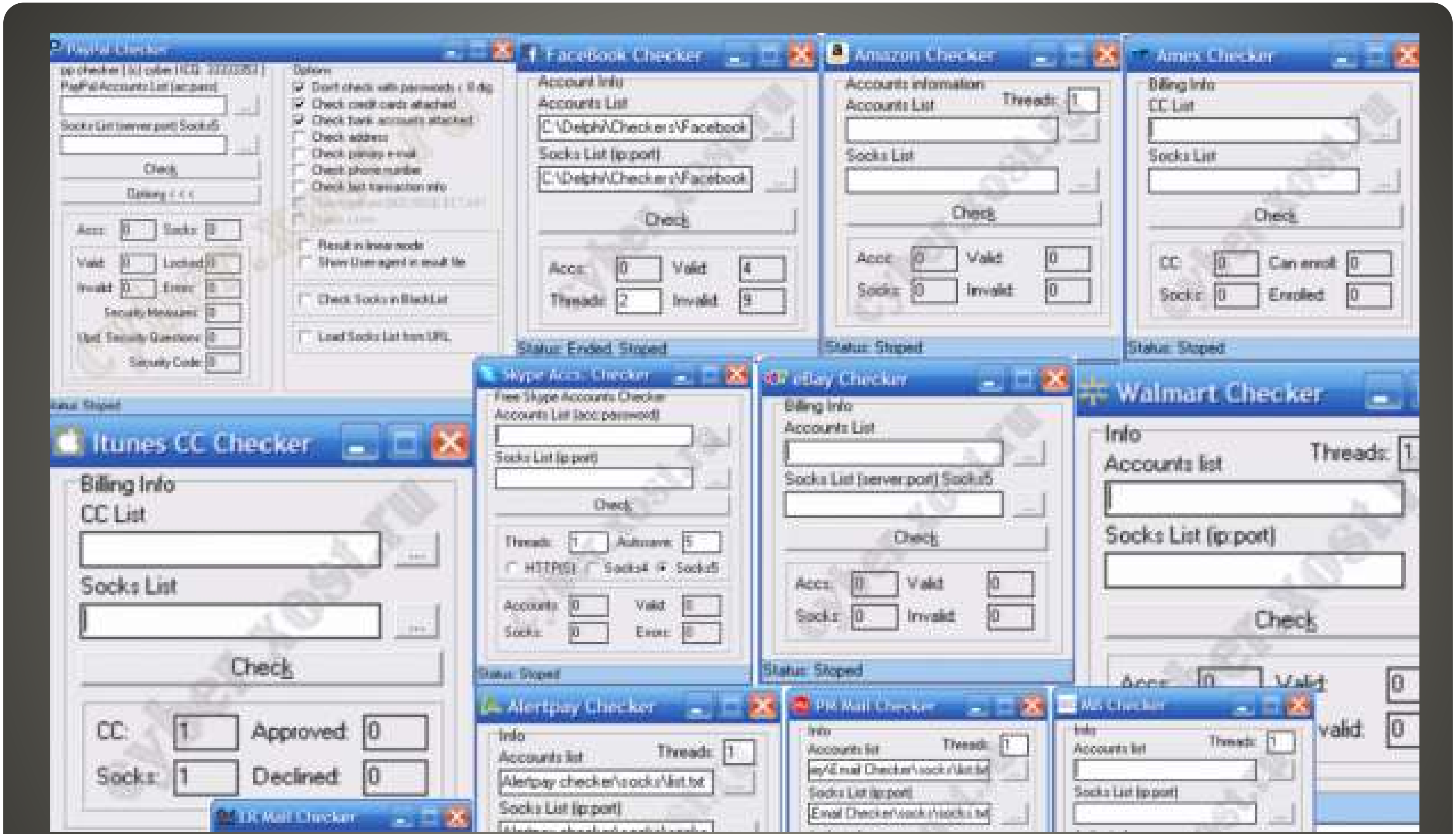


HACKED PC

- Web Server
  - Phishing Site
  - Malware Download Site
  - Warez/Piracy Server
  - Child Pornography Server
  - Spam Site
- E-Mail Attacks
  - Webmail Spam
  - Stranded Abroad Advance Scams
  - Harvesting E-mail Contacts
  - Harvesting Associated Accounts
  - Access to Corporate E-mail
- Virtual Goods
  - Online Gaming Characters
  - Online Gaming Goods/Currency
  - PC Game License Keys
  - Operating System License Key
- Reputation Hijacking
  - Facebook
  - Twitter
  - LinkedIn
  - Google+
- Bot Activity
  - Spam Zombie
  - DDoS Extortion Zombie
  - Click Fraud Zombie
  - Anonymization Proxy
  - CAPTCHA Solving Zombie
- Account Credentials
  - eBay/Paypal Fake Auctions
  - Online Gaming Credentials
  - Web Site FTP Credentials
  - Skype/VoIP Credentials
  - Client Side Encryption Certificates
- Financial Credentials
  - Bank Account Data
  - Credit Card Data
  - Stock Trading Account
  - Mutual Fund/401k Account
- Hostage Attacks
  - Fake Antivirus
  - Ransomware
  - Email Account Ransom
  - Webcam Image Extortion

- FBI (Department of Justice) recovered $2.3M US paid to Darkside
- Early notification to law enforcement
- FBI - please pay bitcoin, not Monero
- Political??

Colonial Pipeline



PayPal Checker

pp checker [c] cyber ICQ: 333333853

PayPal Accounts List (acc:pass)

Socks List (server:port) Socks5

Check

Options < < <

Acc: 0 Socks: 0

Valid: 0 Locked: 0

Invalid: 0 Errors: 0

Security Measures: 0

Upd. Security Questions: 0

Security Code: 0

Options

☑ Don't check with passwords < 8 dig

☑ Check credit cards attached

☑ Check bank accounts attached

□ Check address

□ Check primary e-mail

□ Check phone number

□ Check last transaction info

□ Result in linear mode

□ Show User-agent in result file

□ Check Socks in BlackList

□ Load Socks List from URL

Status: Stoped

FaceBook Checker

Account Info

Accounts List: C:\Delphi\Checkers\Facebook

Socks List (ip:port): C:\Delphi\Checkers\Facebook

Check

Accs: 0 Valid: 4

Threads: 2 Invalid: 9

Status: Ended. Stoped

Amazon Checker

Accounts information

Accounts List Threads: 1

Socks List

Check

Accs: 0 Valid: 0

Socks: 0 Invalid: 0

Status: Stoped

Amex Checker

Billing Info

CC List

Socks List

Check

CC: 0 Can enroll: 0

Socks: 0 Enrolled: 0

Status: Stoped

Itunes CC Checker

Billing Info

CC List

Socks List

Check

CC: 1 Approved: 0

Socks: 1 Declined: 0

Skype Accs. Checker

Free Skype Accounts Checker

Accounts List (acc:password)

Socks List (ip:port)

Check

Threads: 1 Autosave: 5

○ HTTP(S) ○ Socks4 ● Socks5

Accounts: 0 Valid: 0

Socks: 0 Errors: 0

Status: Stoped

eBay Checker

Billing Info

Accounts List

Socks List (server:port) Socks5

Check

Accs: 0 Valid: 0

Socks: 0 Invalid: 0

Status: Stoped

Walmart Checker

Info

Accounts list Threads: 1

Socks List (ip:port)

Check

Accs: 0 Valid: 0

Invalid: 0

Alertpay Checker

Info

Accounts list: Alertpay checker\socks\list.txt Threads: 1

Socks List (ip:port)

PR Mail Checker

Info

Accounts list: ay\Email Checker\socks\list.txt Threads: 1

Socks List (ip:port): Email Checker\socks\socks.txt

MS Checker

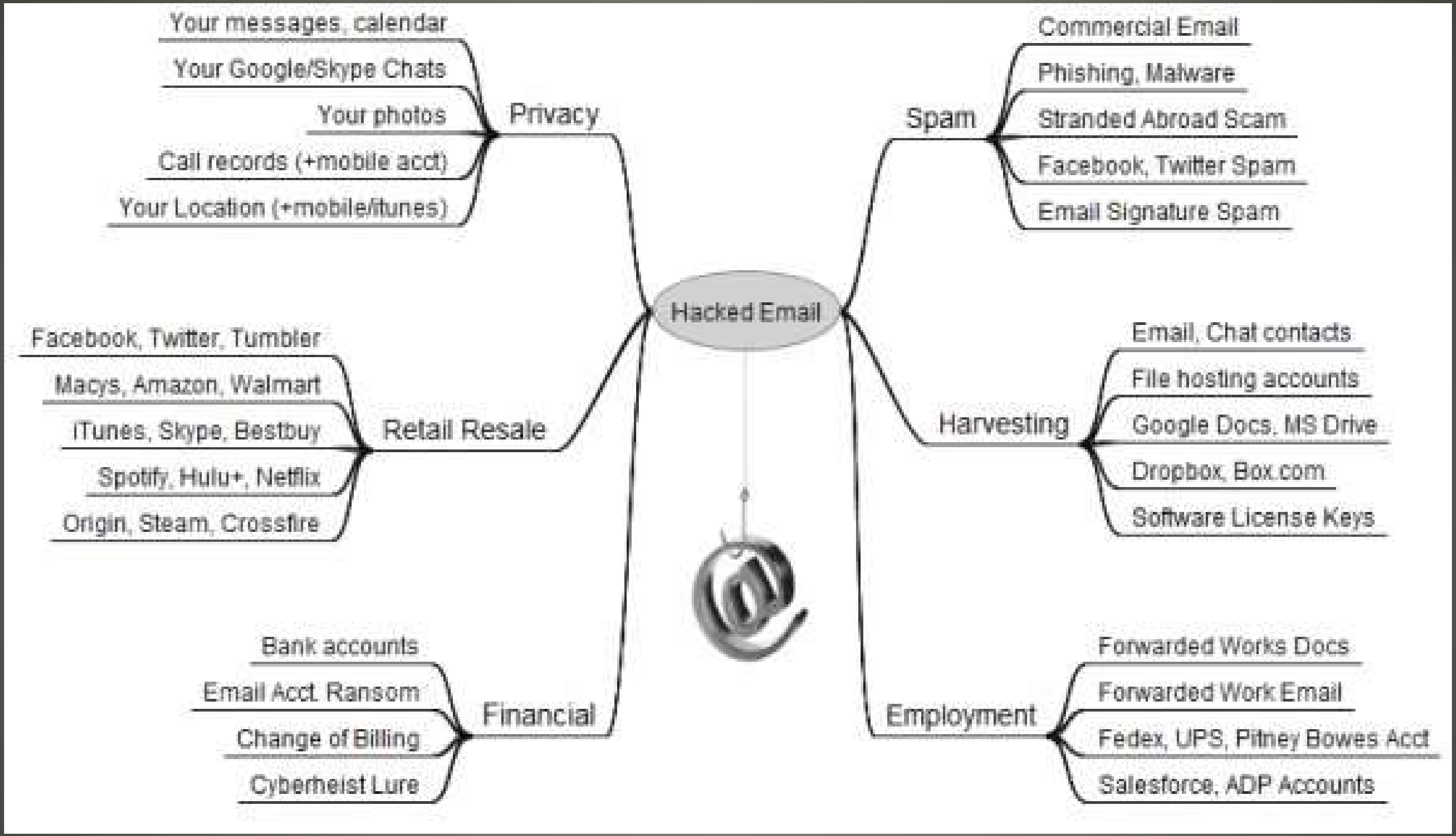
Info

Accounts list Threads: 1

Socks List (ip:port)

UK Mail Checker

Older account checking tools



Hacked Email

- Privacy
  - Your messages, calendar
  - Your Google/Skype Chats
  - Your photos
  - Call records (+mobile acct)
  - Your Location (+mobile/itunes)
- Retail Resale
  - Facebook, Twitter, Tumbler
  - Macys, Amazon, Walmart
  - iTunes, Skype, Bestbuy
  - Spotify, Hulu+, Netflix
  - Origin, Steam, Crossfire
- Financial
  - Bank accounts
  - Email Acct. Ransom
  - Change of Billing
  - Cyberheist Lure
- Spam
  - Commercial Email
  - Phishing, Malware
  - Stranded Abroad Scam
  - Facebook, Twitter Spam
  - Email Signature Spam
- Harvesting
  - Email, Chat contacts
  - File hosting accounts
  - Google Docs, MS Drive
  - Dropbox, Box.com
  - Software License Keys
- Employment
  - Forwarded Works Docs
  - Forwarded Work Email
  - Fedex, UPS, Pitney Bowes Acct
  - Salesforce, ADP Accounts

Uses for stolen eMail accounts

I’m careful – My neighbor NOT

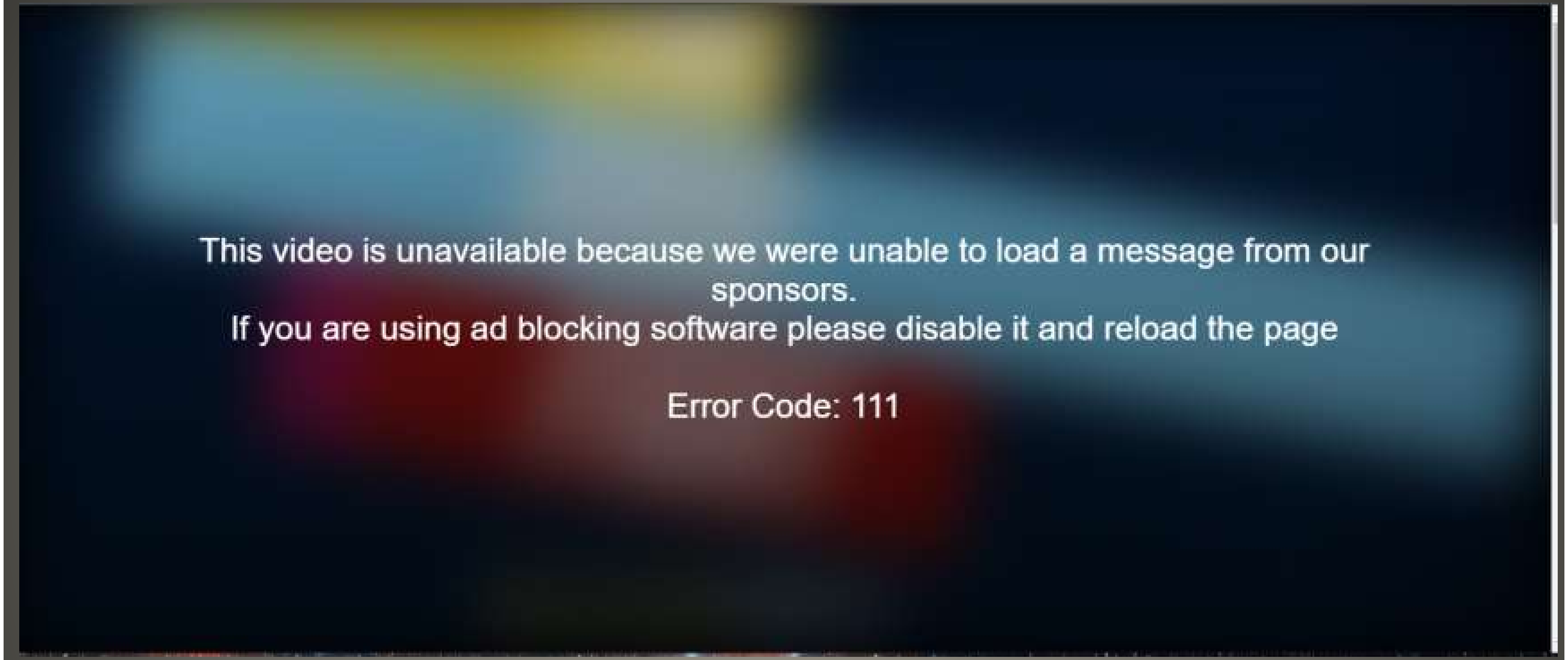
- Facebook Contacts
- Venmo – Social money transfer
- MyLife
- Venmo

- Jetpack security update to WordPress
- WordPress “Fancy Product Designer”
  “Fancy Product Destroyer”
- iOS 12.5.4 security update

iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air, iPad mini 2, iPad mini 3, and iPod touch (6th generation)

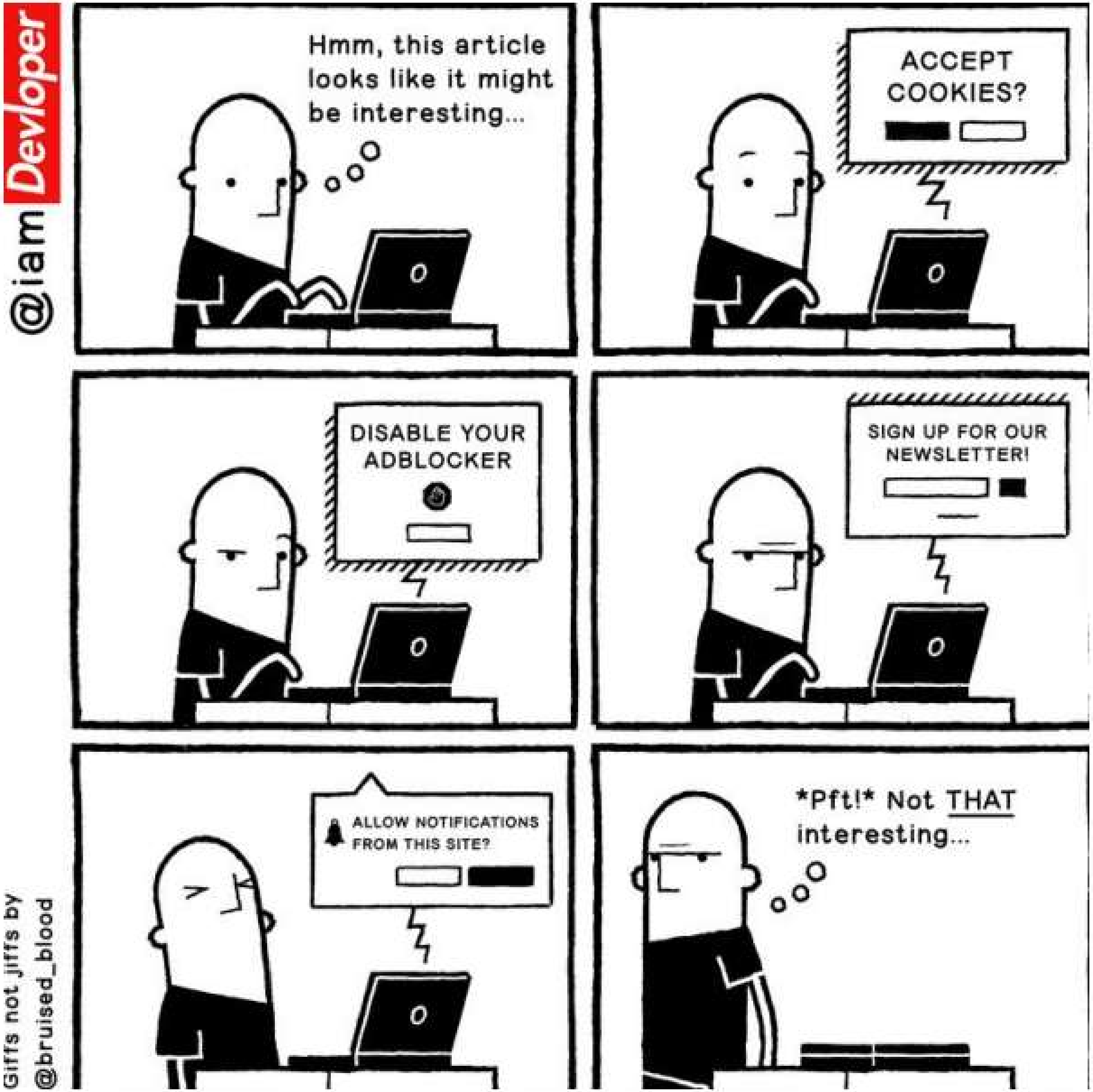
- 8 day “window” exploit tuning

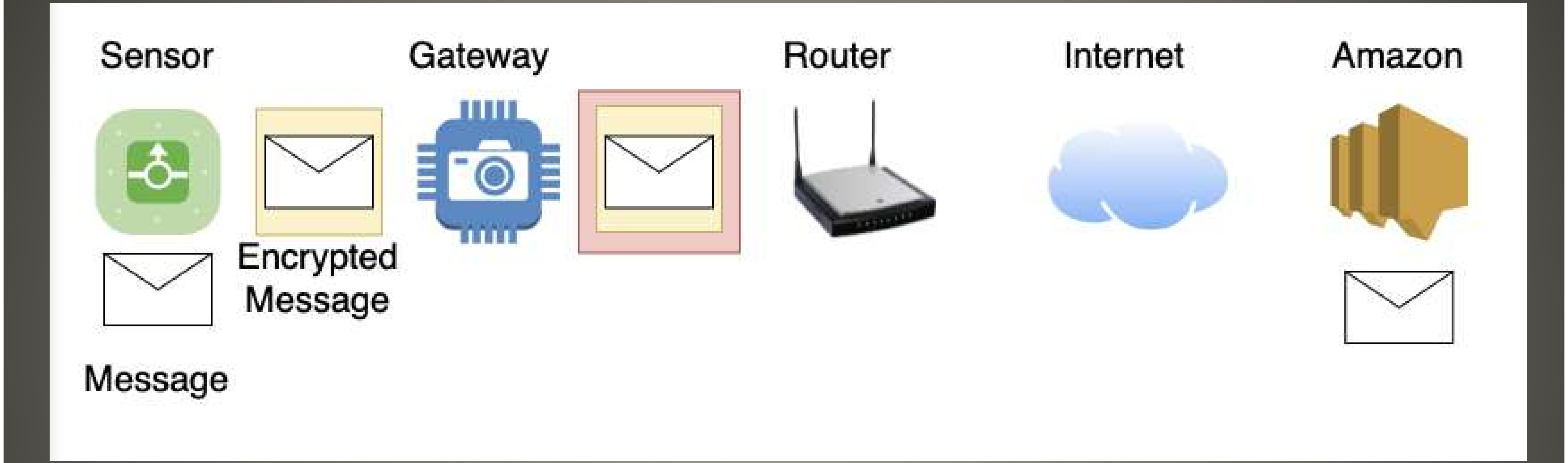
Current Issues



This video is unavailable because we were unable to load a message from our sponsors.
If you are using ad blocking software please disable it and reload the page

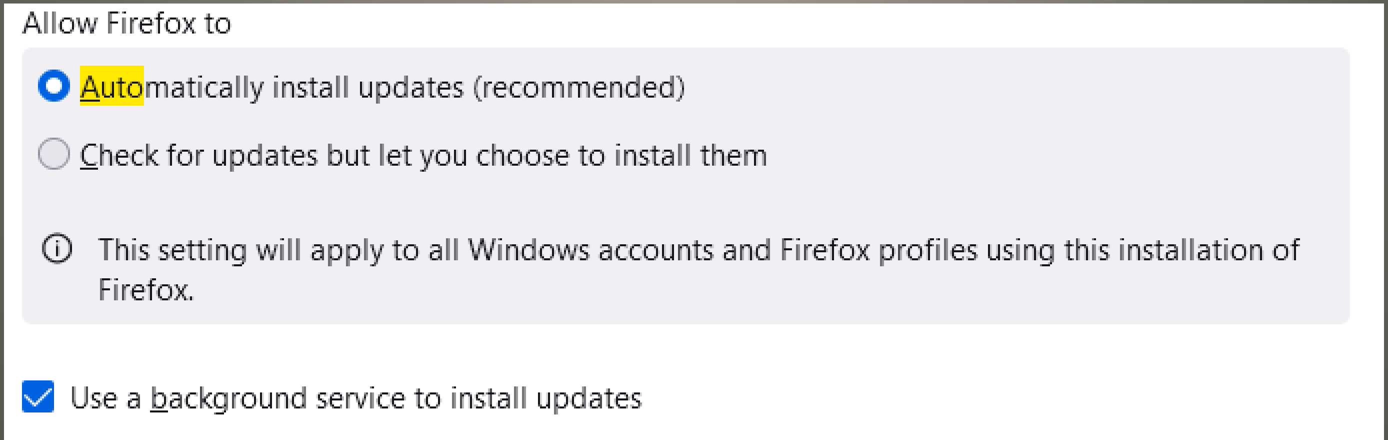
Error Code: 111


@iam Devloper
Hmm, this article looks like it might be interesting...
ACCEPT COOKIES?
DISABLE YOUR ADBLOCKER
SIGN UP FOR OUR NEWSLETTER!
ALLOW NOTIFICATIONS FROM THIS SITE?
Pft! Not THAT interesting...
Giffs not jiffs by @bruised_blood



Amazon Sidewalk

- Scheduled task
- Per user
- Check for updates, Download updates, apply updates



Allow Firefox to

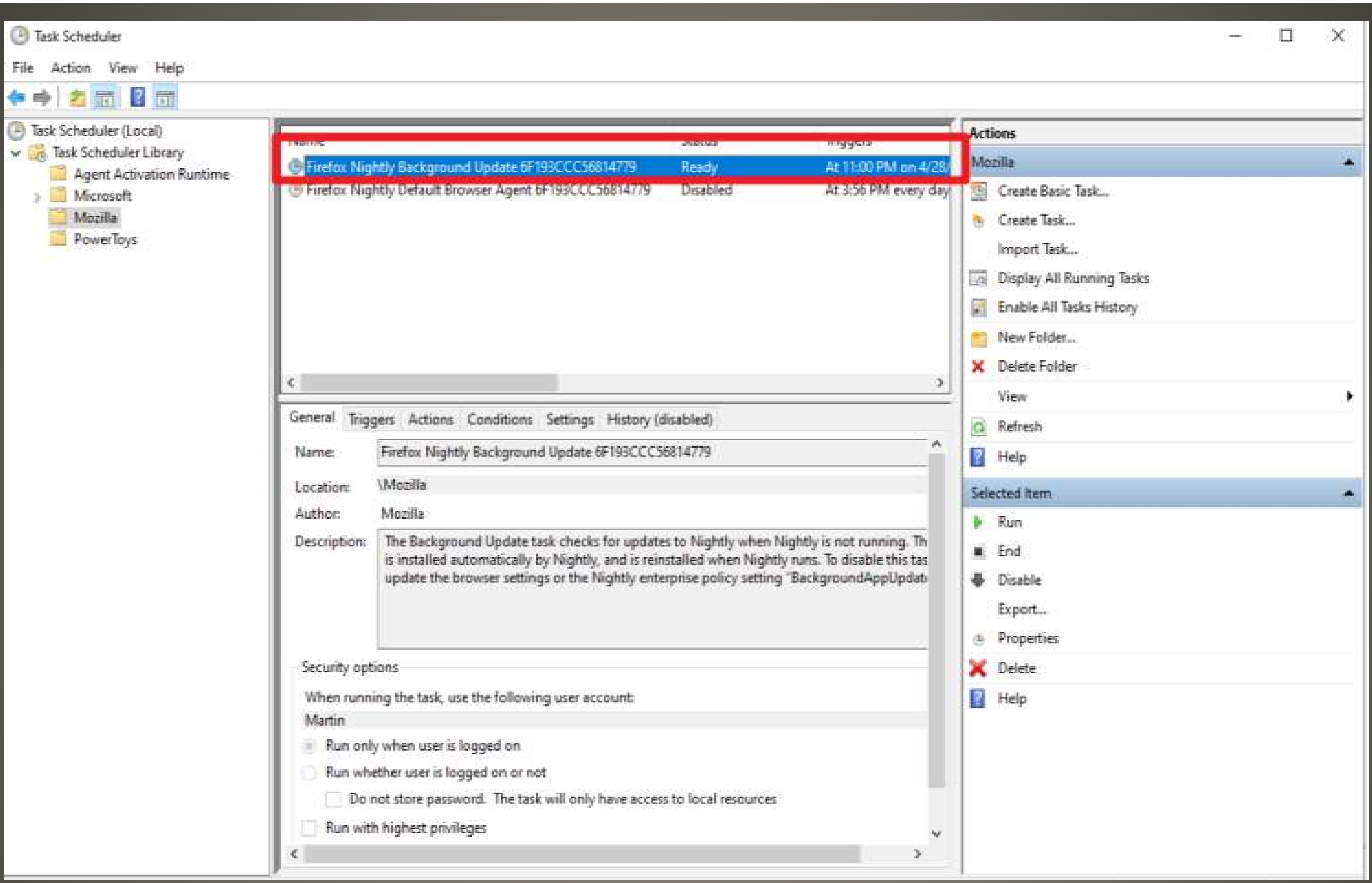
● Automatically install updates (recommended)

○ Check for updates but let you choose to install them

ⓘ This setting will apply to all Windows accounts and Firefox profiles using this installation of Firefox.

☑ Use a background service to install updates

Firefox auto update



Name	Status	Triggers
Firefox Nightly Background Update 6F193CCC56814779	Ready	At 11:00 PM on 4/28/
Firefox Nightly Default Browser Agent 6F193CCC56814779	Disabled	At 3:56 PM every day

Name: Firefox Nightly Background Update 6F193CCC56814779

Location: \Mozilla

Author: Mozilla

Description: The Background Update task checks for updates to Nightly when Nightly is not running. Th is installed automatically by Nightly, and is reinstalled when Nightly runs. To disable this tas update the browser settings or the Nightly enterprise policy setting "BackgroundAppUpdat

Security options

When running the task, use the following user account:

Martin

● Run only when user is logged on

○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local resources

□ Run with highest privileges

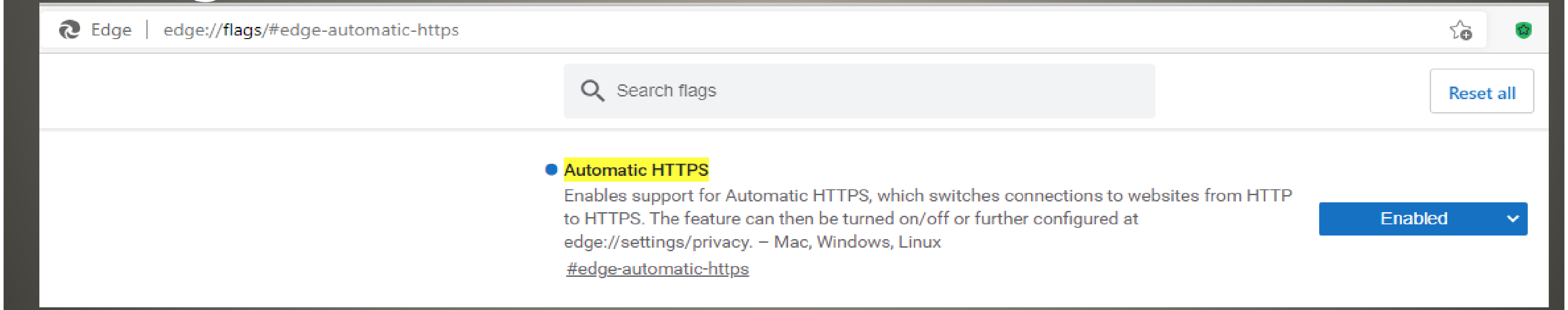
Firefox auto updates

- EVEN when Firefox is not running
- Windows only – for now
- Firefox 90

Firefox auto updates

https

- Schemeless browsing
- Sites without https capability
- Sites that redirect to https
- Sites with Strict-Transport-Security
- Browsers that “tune”
- Edge



● 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

#edge-automatic-https

- 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