Sun City Computer Club

Cyber Security SIG

June 3, 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

- Smart devices “smell”
  Burt food – ovens, microwave
  Spoiling food – refrigerators
- Patch Tuesday – last 55 vulnerabilities
  BUT a 9.8
  wormable – PoC published IIS
  AND a 9.9 Hyper-V
  sigh, 4 additional in Exchange server
- Bitdefender & Colonial Pipeline
- Nobelium – yet again
  US Agency for International Development
  Really DID come from USAID
  Recent rash of phishing eMails REALLY did come from Friend

U.S. Agency for International Development

May 25, 2021

USAID Special Alert:

Donald Trump has published new documents on election fraud

View documents

Current Issues

- App – good rating, enjoy bad rating – try again
- Linux based NAT routers (DD-WRT?)
- Fragmentation WiFi vulnerability
- Remote access to either ONLY WHEN NEEDED
- Mean Time to Inventory
  Vulnerability Scan 15 minutes
- Disk wiper targets Israel
- WSL
- Major improvements to browsers
  Firefox 98 Chrome 91 Opera 76 Edge 91
  Tor 10.0.16 Brave 1.25.69 Safari 14.1.1
  Vivaldi 3.8.2259.42
  Security and SPEED
- Denmark media report US spying on European leaders
  Operation Dunhammer
- WhatsApp & India

Current Issues

- Have I Been Pwned
  Open Source & FBI info sharing
- M1RACLES - EL0 register - 2 bits
- US Army IoT device awareness
- Digital Flash Card apps
  US Nuclear Weapons Secrets
  Camera GPS, patrol frequency, badge IDs, codewords,
- Federal Network Hygiene - "disappointment"
  US Cyber Security Executive Order
- DHS/TSA Pipeline Security Directive

- Paste clipboard content into browser ??
- Browser commands in URL

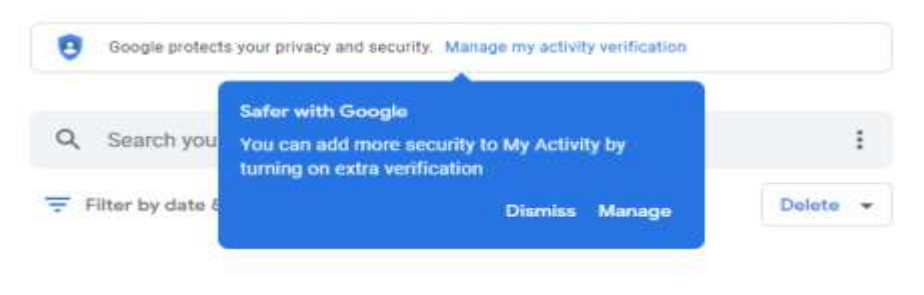
  Run Chrome Safety check

  Manage Google Account

  Delete History

  Wipe cookies

https://myactivity.google.com/myactivity



Browser Chromium based

Google

- Delete activity 3, 18, 36 months
- Interested in topic?

  Google search

  Incognito mode - History PERIOD

  DuckDuckGo Search

INTERNET SPEED RECOMMENDATIONS

Activity	Required Speed	Recommended speed
Email	1 Mbps	1 Mbps
Web browsing	3-5 Mbps	5-10 Mbps
Social media	3-5 Mbps	10 Mbps
Video calls and conferencing	3-5 Mbps	10-20 Mbps
HD streaming	5-10 Mbps	10-20 Mbps
Online gaming	3–6 Mbps	25-35 Mbps
4K streaming	25 Mbps	35 Mbps

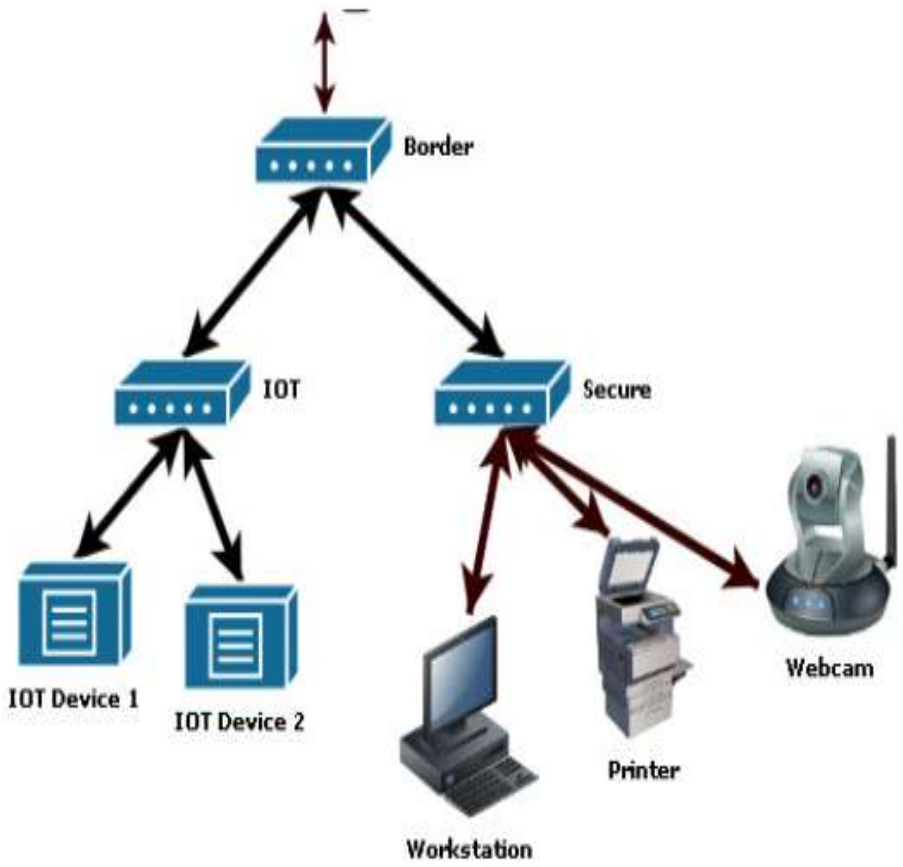
Internet Service Provider (ISP)

- 300 baud acoustic coupler
- Could not use phone AND dial-up
- How many devices are you using
- How many devices will you be using
- Asymmetric speeds
- Upload (video conferencing, gaming, …)
- Cable cluster – neighbors
- Speed to end device limited by slowest device
- Throttling
- Fiber, cable, LEO satellite, 5G, DSL, satellite, Fixed wireless, Dial-up

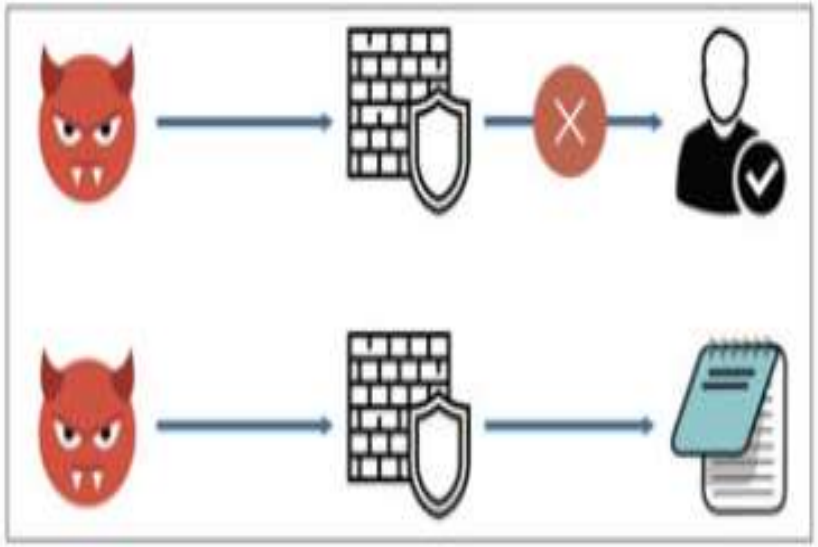
Cable

- Cable Modem – Router – Wireless Access Point
- Cable Modem with VoIP
- Rent your cable modem?
- Cable Modem firmware – ISP ISP You You
- Cable Modem access from LAN side
- Docsis 3.1
- Suddenlink link
- https://www.suddenlink.com/suddenlink-internet-using-your-own-modem

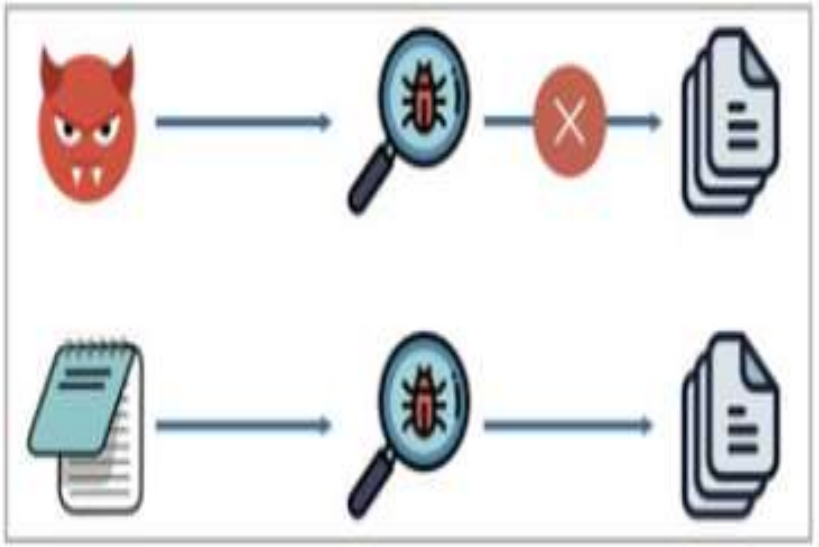
Manufacturer: Various



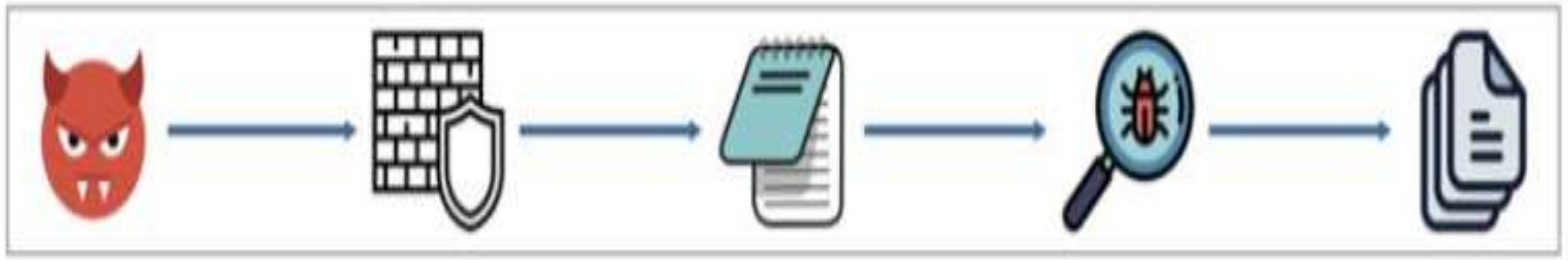
- Latency
- Neighbors
- Devices OFF switch in OFF position



(a) Ransomware's messages to high IL applications are blocked by UIPI (*top*); but ransomware can send messages to trusted applications (*bottom*).



(b) Ransomware's write attempts to protected files are blocked by AVs (*top*); however, trusted applications can write on these files (*bottom*).



Phone Apps

- Facebook credential stealers

  FlashlightWallpapers Padenatef
  Wallpaper Level Contour Level Wallpaper
  iPlayer & iWallpaper Video Maker
  Color Wallpapers Pedometer
  Powerful Flashlight Super Bright Flashlight
  Super Flashlight Solitaire Game
  Accurate Scanning of QR Code Synthetic Z
  File Manager Composite Z
  Screenshot Caputre Wuxia Reader
  Daily Horoscope Wallpapers Plus Weather
  Anime Live Wallpaper iHealth Step Counter
  Com.tqyapp.fiction

Phone Apps

- GasBuddy - Location data of course
  Privacy policy change
  Opt-in service *Drive*
  driving habits – distance, speed, acceleration, braking, etc.
- TikTok US Government ban
  Hardware ID, memory usage, list of other apps, IP address, recent Wi-Fi
- Angry Birds Snowden warn NSA, GCHQ
  call logs, political info.,

Phone Apps

- IPVanish VPN
  REALLY vet your VPN service(s)
- Facebook Instagram
- 4 GB RAM Memory Booster – Applock
  RAM Booster (Memory Cleaner)
- CamScanner

Phone Apps

- Android Apps
  Age Face Altar Message
  Antivirus Security — Security ScanBeach
  CameraBoard picture editing Climate SMS
  Certain Wallpaper Collate Face Scanner
  Cute Camera Dazzle Wallpaper
  Declare Message Display Camera
  Great VPN Humour Camera Ignite Clean
  Leaf Face Scanner Mini Camera
  Print Plan Scan Rapid Face Scanner
  Reward Clean Ruddy SMS Soby Camera
  Spark Wallpaper

  Apps purchased from Developer, then turned malicious

- YouVersion Bible
- Randonautica

Phone Apps

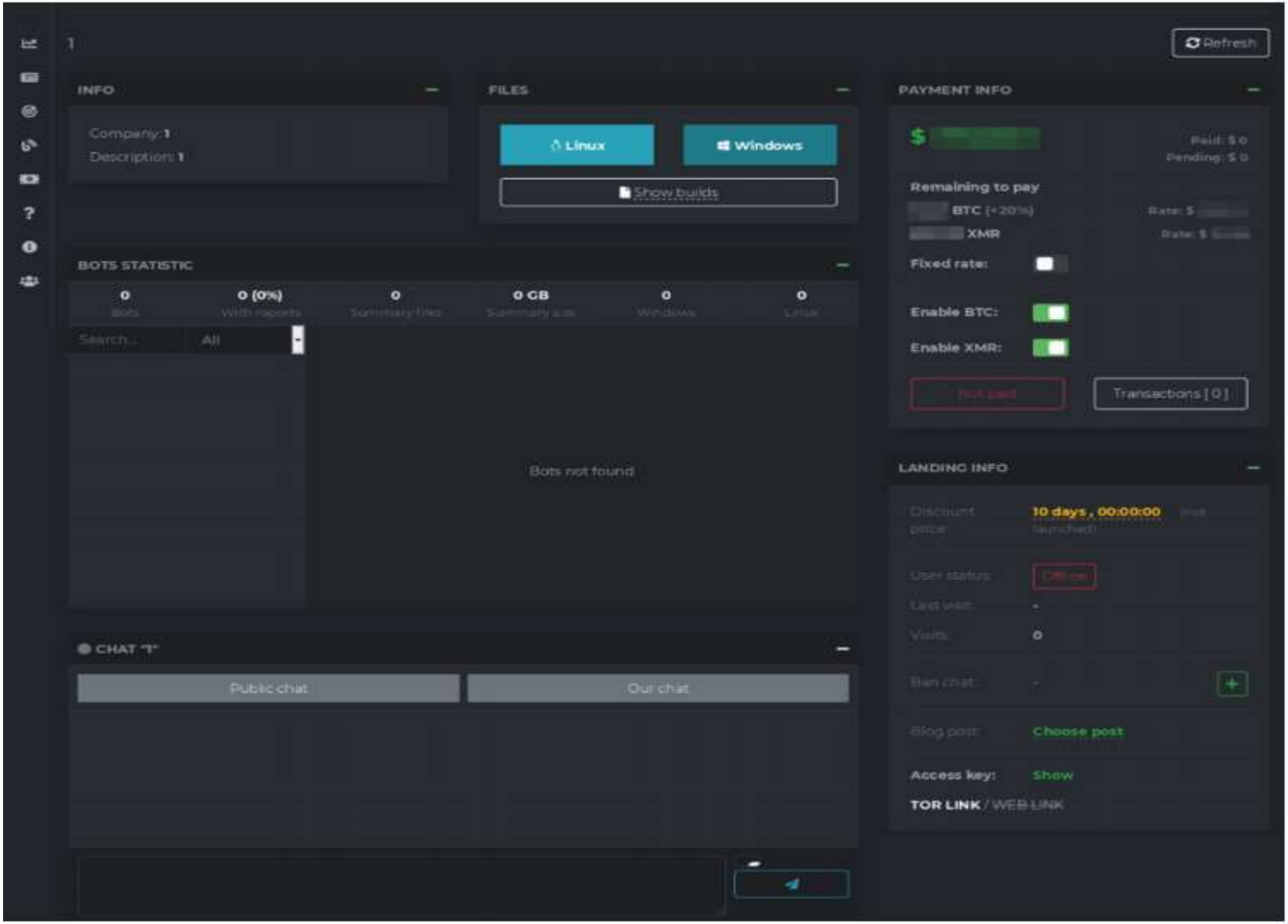
DarkSide

- Ransomware as a Service RaaS
- Advertising - Advertising forums "no thanks"
- NEW ADDED Services - DDOS, Build a platform, Post stolen data, sliding fee, Windows or Linux – your choice, double encryption, victim communication, support, peer reviews, …
- Listed victim list (public stock)
  Then profit from stock fluctuations
- Tactics, Techniques & procedures (TTPs)
- Exim, Microsoft Exchange, SolarWinds, COMB
- Ethics statements & practice
- JBS ransomware Ireland's Health Care System
- Ransom paid, Decryption of little use
- Emisoft Decryption tool

DarkSide

- Crypto wallet traffic
- Hydra – cash out
- Crypto mixing services
- Toshiba attack?
- DarkSide, at least two promoters, under DDOS attack

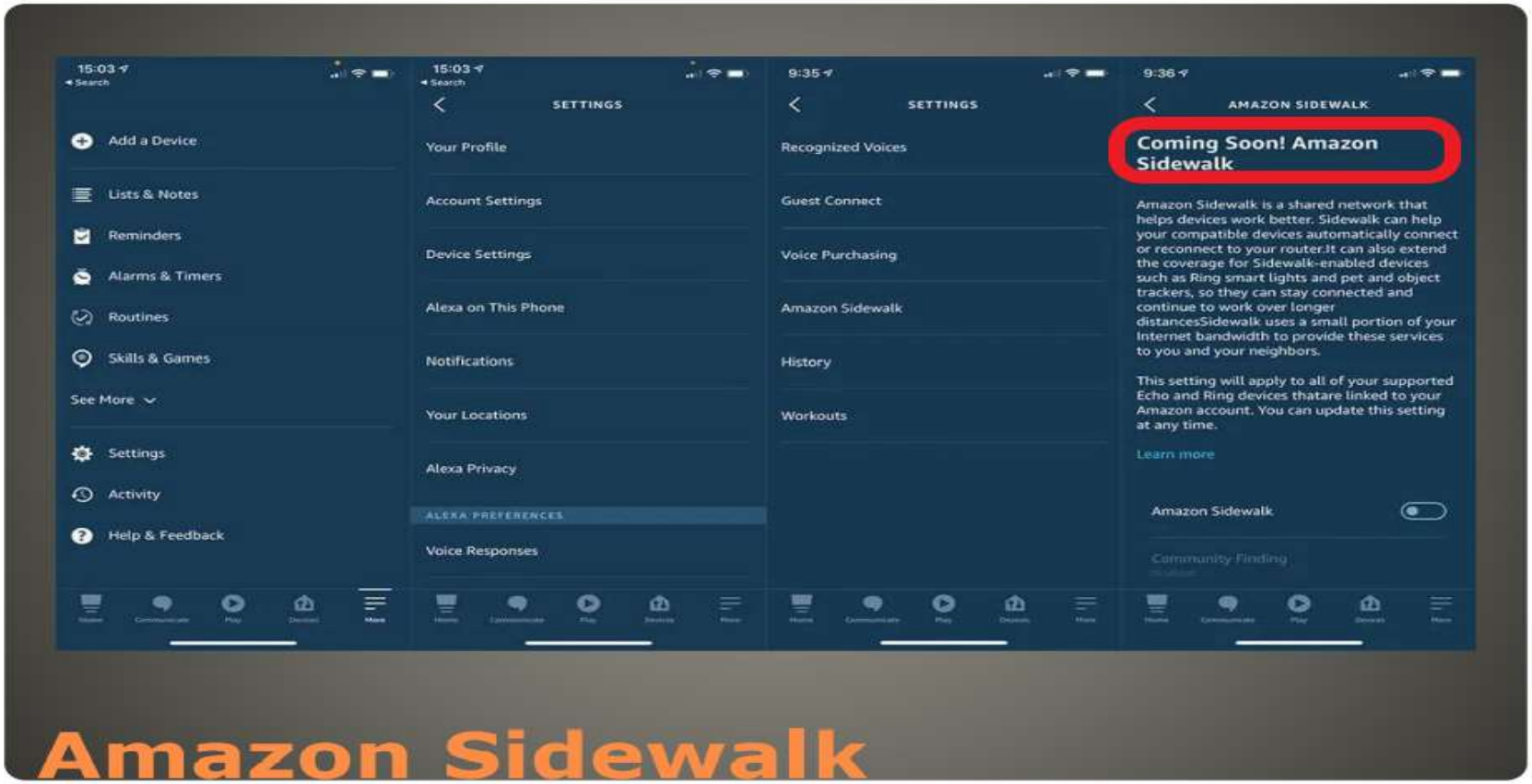
- 2203 posted ransomware attacks
- “leak my data, please” I can’t


1
Refresh
INFO
Company: 1
Description: 1
FILES
Linux
Windows
Show builds
PAYMENT INFO
Paid: $ 0
Pending: $ 0
Remaining to pay
BTC (+20%)
XMR
Fixed rate:
Enable BTC:
Enable XMR:
Transactions [0]
BOTS STATISTIC
0
Bots
0 (0%)
With reports
0
Summary files
0 GB
Summary size
0
Windows
0
Linux
Search...
All
Bots not found
LANDING INFO
Discount price
10 days , 00:00:00
User status:
Offline
Last visit:
Visits:
0
Ban chat:
Blog post:
Choose post
Access key:
Show
TOR LINK / WEB LINK
CHAT "1"
Public chat
Out chat

Wi-Fi Frag attacks

- Protocol design
- Protocol implementation errors
- EVERY device has at least one, most several
- *Adversary in range*
- KRACK (worst security threat yet)
  Key Reinstallation AttaCK)
- Cellular data vs Wi-Fi
- How often do you check mobile devices
  Wi-Fi on and associated?
- Unencrypted frames injected to encrypted network

- December 3, 2020, Presentation



Amazon Sidewalk

Amazon Sidewalk

- Bi-directional sharing heavily-encrypted low bandwidth 900 MHz LoRa & Bluetooth
- Go Live June 8
- Enabled by default
- Echo, Ring, Floodlight cams, Spotlight cams
- Alexa Settings > Account Settings > Amazon sidewalk
- Ring > Control Center > Sidewalk
- Low bandwidth signaling App
- AirTags

Testing VPNs

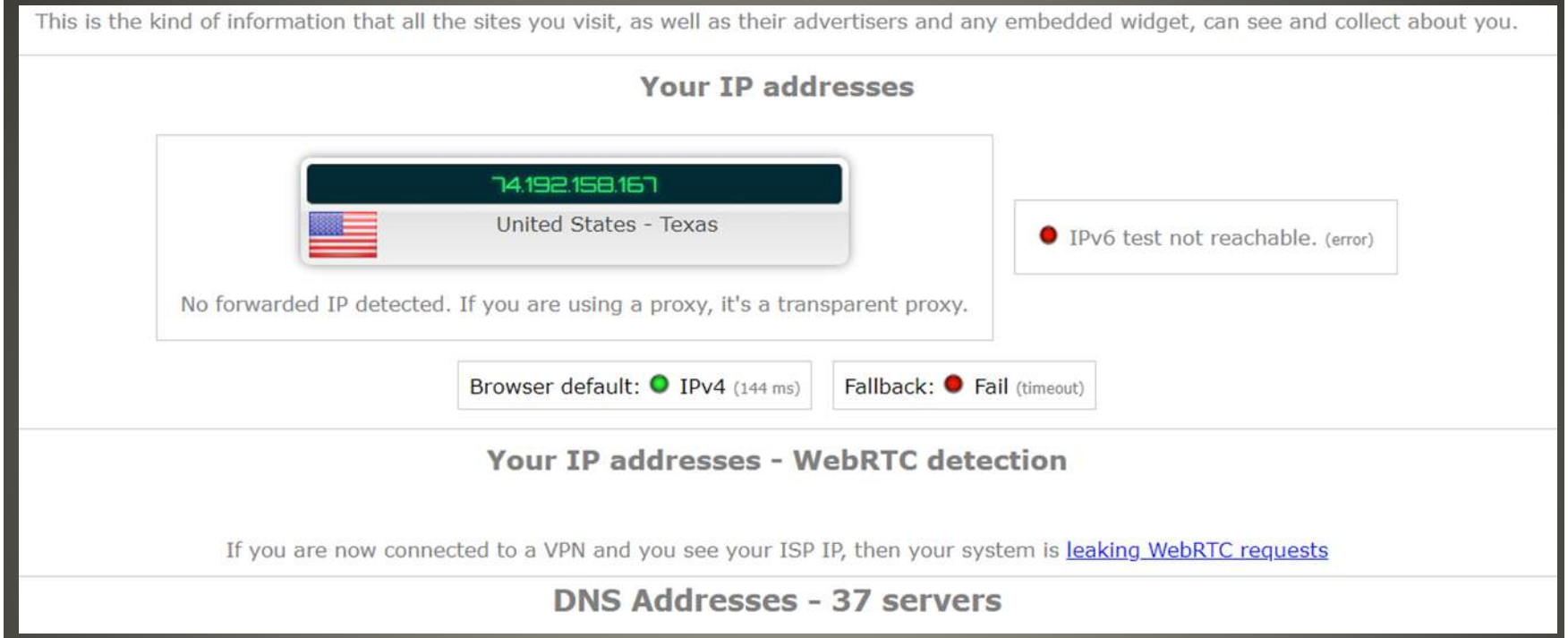
- Leaking of your real IP Address
  - IPv6
  - WebRTC
  - DNS

Testing VPNs

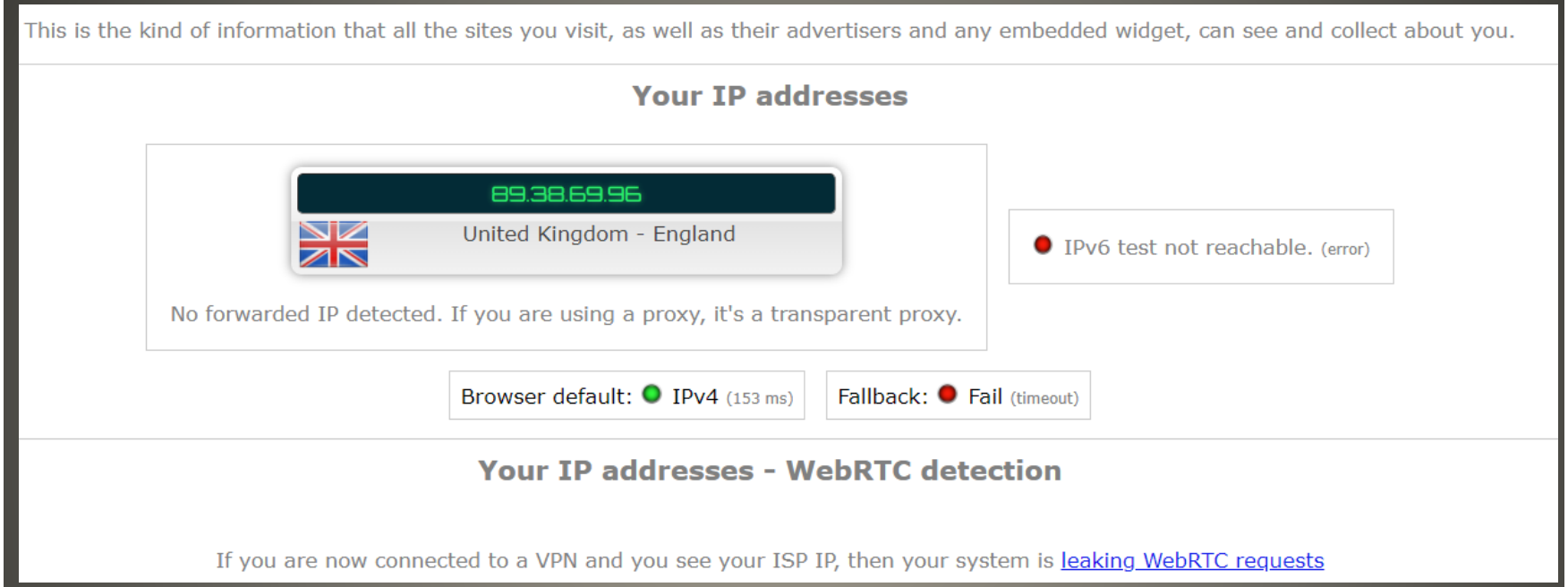
- IPv6 check vendor site
  Nord – protection
  Proton – not
  Yours?
- WebRTC
  per Browser
  Edge about:flags edge:flags

Testing VPN

- WebRTC
  Firefox media.peerconnection.enabled
  Safari Developer – Experimental
  Remove Legacy WebRTC API
- Some browser features will fail
- DNS use 1.1.1.1 or 9.9.9.9

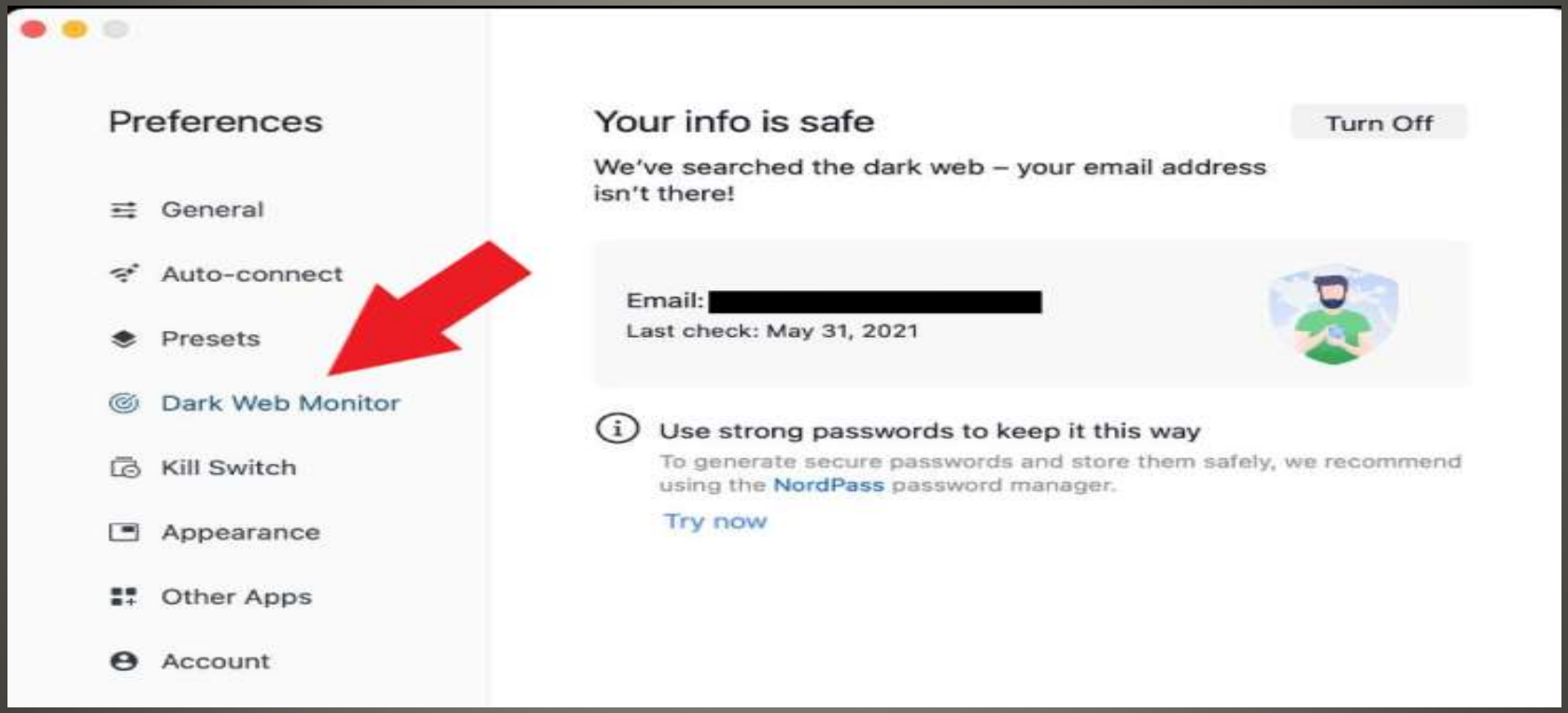


Before - Nord VPN

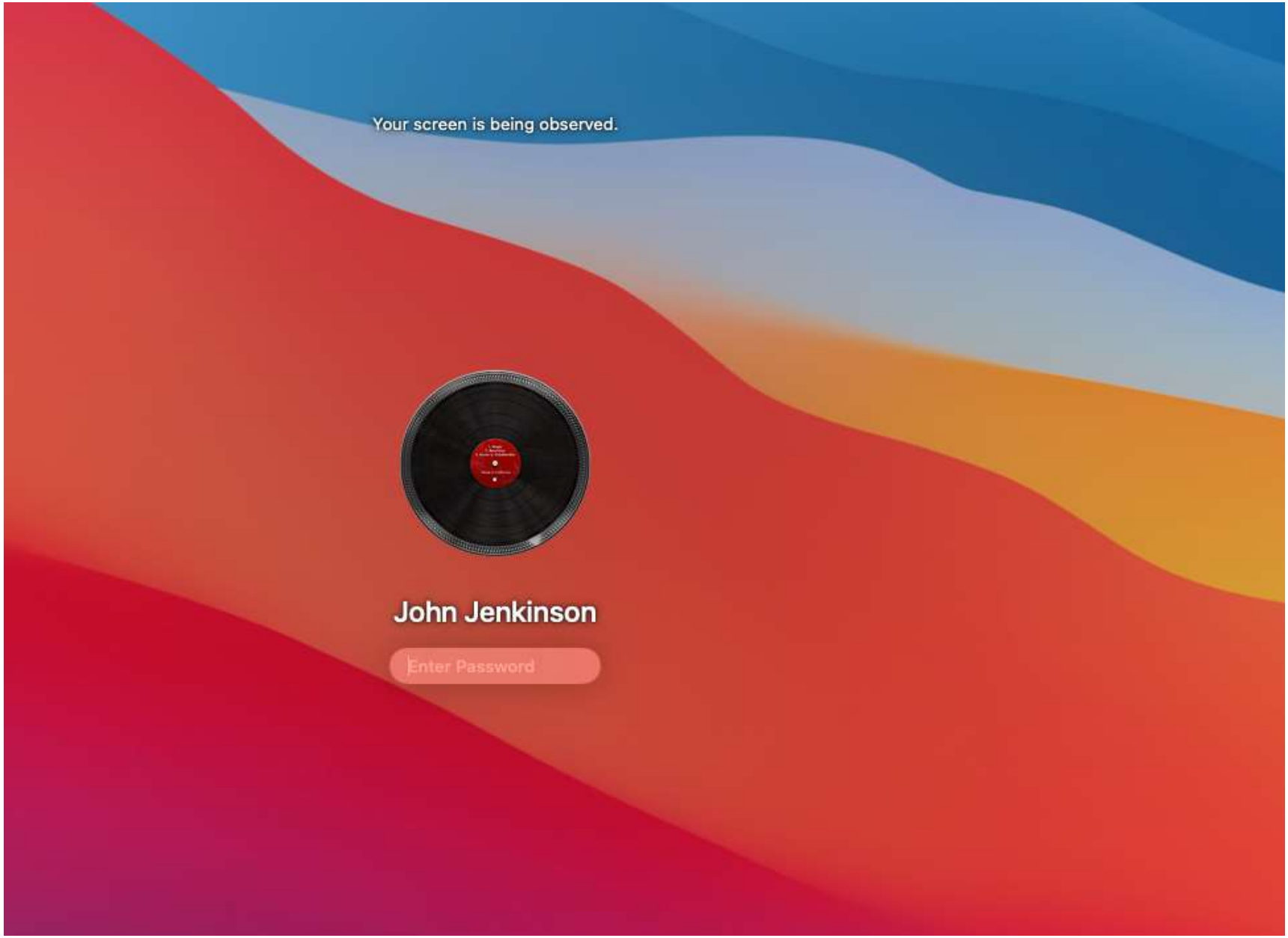


After – Nord VPN

- Windows 6.37.2
- MacOS 6.4.1



Nord VPN


Your screen is being observed.
John Jenkinson
Enter Password

Android banking trojans

- TeaBot
- Bizzaro

- "Fake" Apps
  Adblockers, eBook readers, VPNs,
  Names, logos, etc. may match real apps
- Click on links - no
- Open eMail attachments – no
- "well, that can't be done"
- True – use EXTRA caution

eMail problems on the rise

- COMB + SolarWinds + Exchange + Exim
- Assume your eMail Identity
- Forward via rule or Filter
- Warn friends AND their vendor

- Facebook and Social Media
  - Use same name and public viewable contacts

- Darkside drama
- Cryptocurrency Escrow

"Hooked a big fish? Want to keep more of what you're about to earn? Consider encrypting your target's network with Newbieware... we only take 5%! We also have the fastest encryption around so your target will never know what hit them. And we have big pipes, hosting your ill gotten goods on AWS, the industry's most reliable cloud storage."

RaaS

- 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