Sun City Computer Club

Cyber Security SIG

November 19, 2020

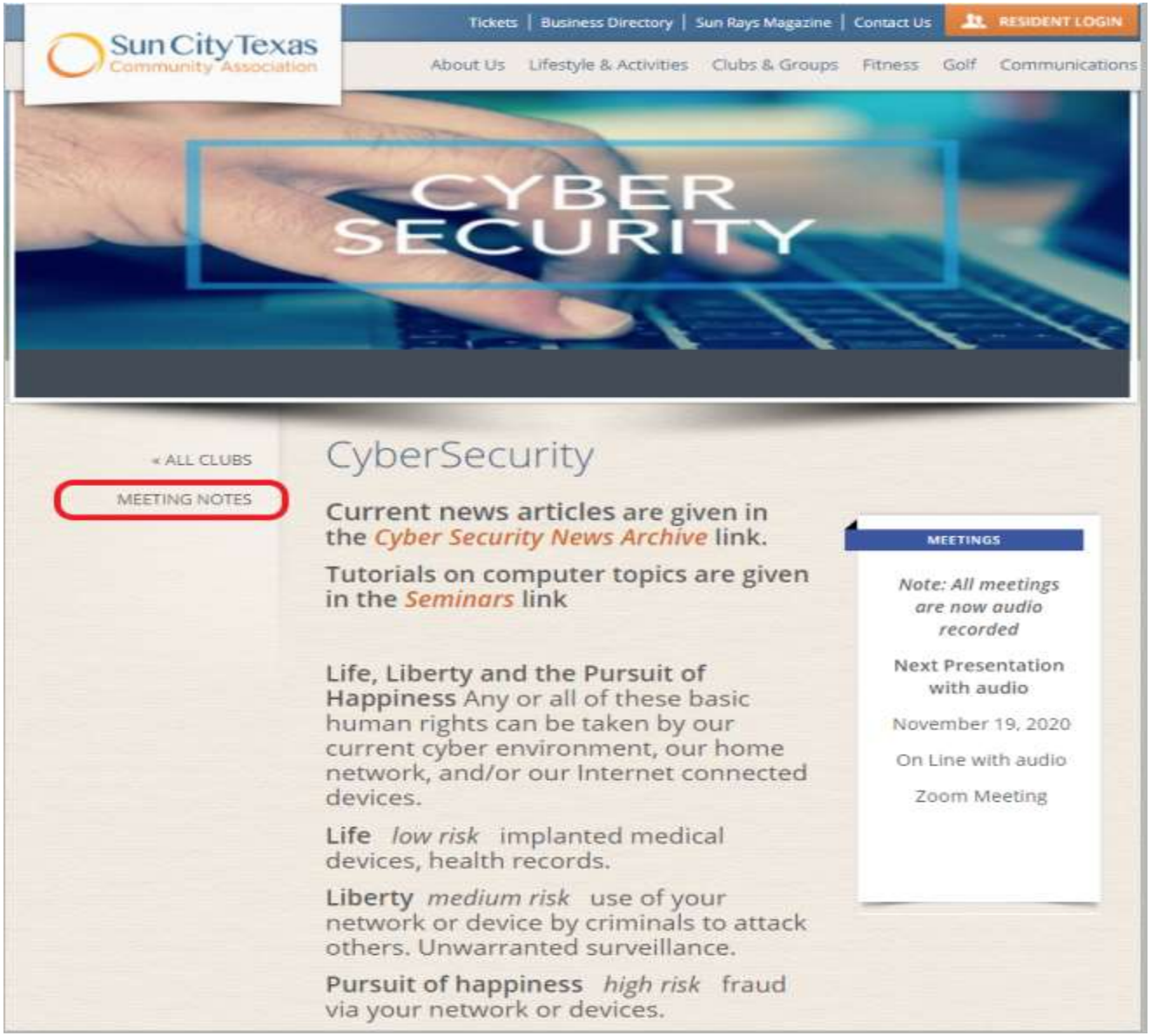
Questions, Comments, Suggestions welcomed at any time

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


Sun City Texas
Community Association
Tickets | Business Directory | Sun Rays Magazine | Contact Us
RESIDENT LOGIN
About Us Lifestyle & Activities Clubs & Groups Fitness Golf Communications
CYBER SECURITY
« ALL CLUBS
MEETING NOTES
CyberSecurity
Current news articles are given in the Cyber Security News Archive link.
Tutorials on computer topics are given in the Seminars link
Life, Liberty and the Pursuit of Happiness Any or all of these basic human rights can be taken by our current cyber environment, our home network, and/or our Internet connected devices.
Life low risk implanted medical devices, health records.
Liberty medium risk use of your network or device by criminals to attack others. Unwarranted surveillance.
Pursuit of happiness high risk fraud via your network or devices.
MEETINGS
Note: All meetings are now audio recorded
Next Presentation with audio
November 19, 2020
On Line with audio
Zoom Meeting


Sun City Texas
Community Association
Tickets | Business Directory | Sun Rays Magazine | Contact Us
RESIDENT LOGIN
About Us Lifestyle & Activities Clubs & Groups Fitness Golf Communications
CYBER SECURITY
« ALL CLUBS
MEETING NOTES
Meeting Notes Archive 2019
Cyber Security News Archive
Meeting Notes Archive 2018
Seminars
Cyber Security SIG Meeting Notes
2020
July 21 Safer Browsing Class [Download | View] | 800.65kb
January 2 Cyber Security SIG Presentation with audio [Download | View] | 655.17kb
January 16 Cyber Security SIG Presentation with audio [Download | View] | 199.42kb
February 6 Cyber Security SIG Presentation with audio [Download | View] | 399.81kb

Cyber Security SIG Meeting Notes

Big Sur [*Download* | *View*] | 700.07kb

Sun City Computer Club WEB site navigation and information [*Download* | *View*] | 2,602.35kb

First Time SIG Safer Computing [*Download* | *View*] | 126.09kb

Safer WEB Browsing Class [*Download* | *View*] | 800.65kb

Safer WEB Browsing Part one [*Download* | *View*] | 1,585.12kb

Safer WEB Browsing Part two [*Download* | *View*] | 407.06kb

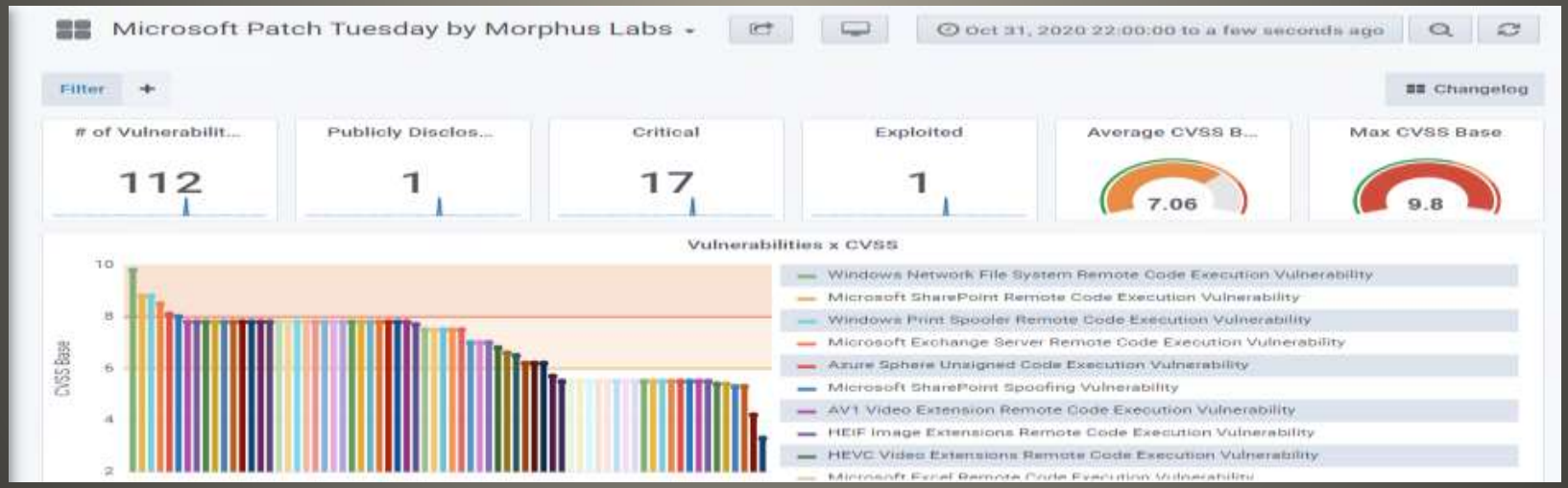
Sun City MAC Users Group MUG Securing your MAC [*Download* | *View*] | 786.08kb


Sun City Texas
Community Association
Tickets | Business Directory | Sun Rays Magazine | Contact Us
RESIDENT LOGIN
About Us Lifestyle & Activities Clubs & Groups Fitness Golf Communications
CYBER SECURITY
« ALL CLUBS
MEETING NOTES
Meeting Notes Archive 2019
Cyber Security News Archive
Meeting Notes Archive 2018
Seminars
Cyber Security SIG Meeting Notes
Browsing Class [Download | View] | 800.65kb
January 2 Cyber Security SIG Presentation with audio [Download | View] | 655.17kb
January 16 Cyber Security SIG Presentation with audio [Download | View] | 199.42kb

Current Issues

- Lawsuit Google Android cellular data
  12MB/day 16 times/hour
- TCL smart TVs with
  undocumented backdoor
  Servers with smart TV firmware files
  Android & Roku versions
- ShieldsUP nmap WAP network map
- Project Zero near zero known
- Updates abound
- Recent email scam gift cards

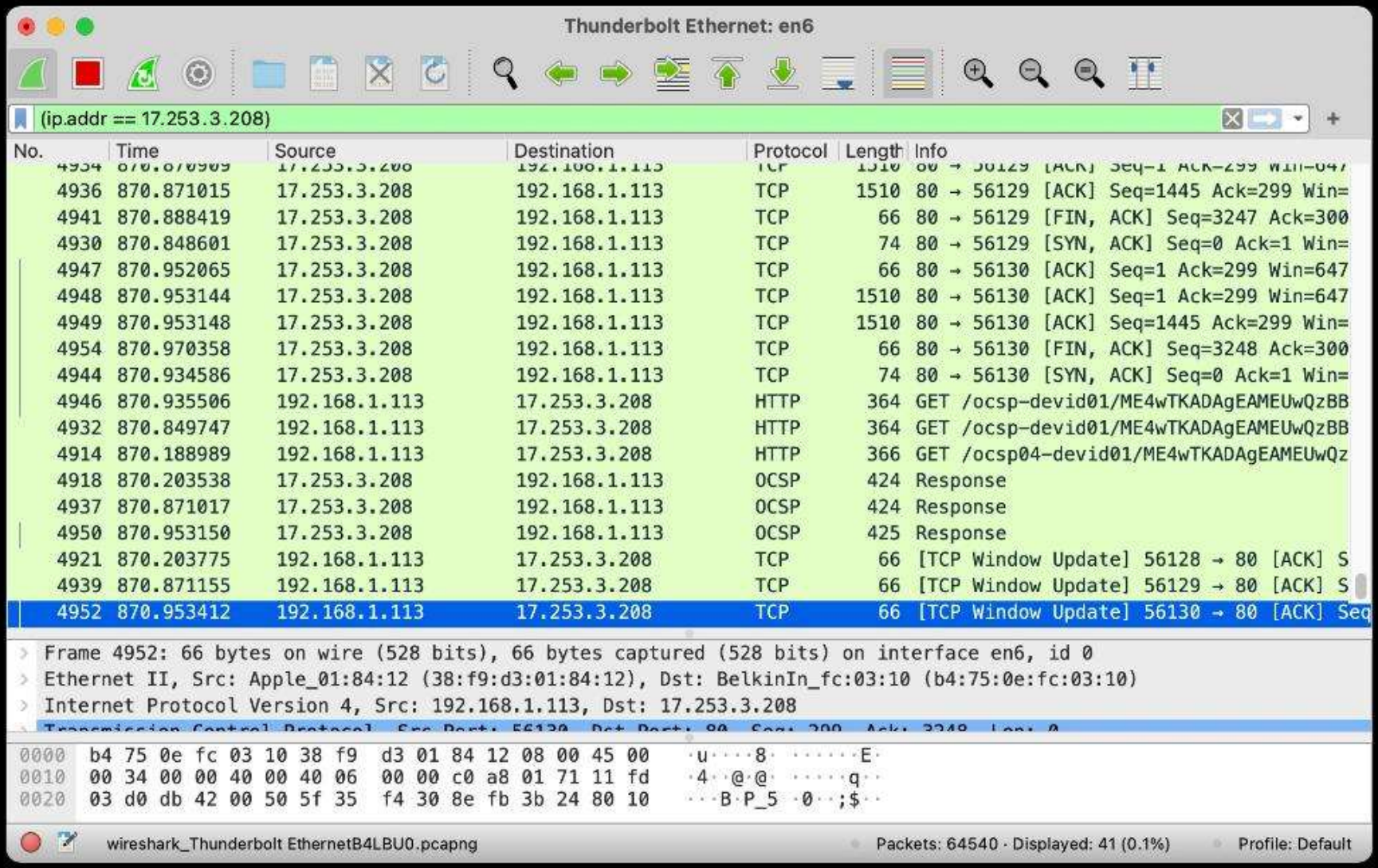
- November Windows Patch Tuesday
- 112 vulnerabilities 17 critical
- Notification format change
- Adobe
- Urgency vs Avoidance



Microsoft Patch Tuesday

Apple outages

- This week Big Sur release
- Gatekeeper apps
- ocsp.apple.com
- 2:30pm Nov 12
- Reboots slow zoom logins slow
- /etc/hosts workaround???
- Little Snitch - Big Sur
- Helpful - app certificates
- Harmful
  date, time, computer, ISP, city, state, hash
- Shared with ??


Thunderbolt Ethernet: en6
(ip.addr == 17.253.3.208)
No. Time Source Destination Protocol Length Info
4936 870.871015 17.253.3.208 192.168.1.113 TCP 1510 80 → 56129 [ACK] Seq=1445 Ack=299 Win=
4941 870.888419 17.253.3.208 192.168.1.113 TCP 66 80 → 56129 [FIN, ACK] Seq=3247 Ack=300
4930 870.848601 17.253.3.208 192.168.1.113 TCP 74 80 → 56129 [SYN, ACK] Seq=0 Ack=1 Win=
4947 870.952065 17.253.3.208 192.168.1.113 TCP 66 80 → 56130 [ACK] Seq=1 Ack=299 Win=647
4948 870.953144 17.253.3.208 192.168.1.113 TCP 1510 80 → 56130 [ACK] Seq=1 Ack=299 Win=647
4949 870.953148 17.253.3.208 192.168.1.113 TCP 1510 80 → 56130 [ACK] Seq=1445 Ack=299 Win=
4954 870.970358 17.253.3.208 192.168.1.113 TCP 66 80 → 56130 [FIN, ACK] Seq=3248 Ack=300
4944 870.934586 17.253.3.208 192.168.1.113 TCP 74 80 → 56130 [SYN, ACK] Seq=0 Ack=1 Win=
4946 870.935506 192.168.1.113 17.253.3.208 HTTP 364 GET /ocsp-devid01/ME4wTKADAgEAMEUwQzBB
4932 870.849747 192.168.1.113 17.253.3.208 HTTP 364 GET /ocsp-devid01/ME4wTKADAgEAMEUwQzBB
4914 870.188989 192.168.1.113 17.253.3.208 HTTP 366 GET /ocsp04-devid01/ME4wTKADAgEAMEUwQz
4918 870.203538 17.253.3.208 192.168.1.113 OCSP 424 Response
4937 870.871017 17.253.3.208 192.168.1.113 OCSP 424 Response
4950 870.953150 17.253.3.208 192.168.1.113 OCSP 425 Response
4921 870.203775 192.168.1.113 17.253.3.208 TCP 66 [TCP Window Update] 56128 → 80 [ACK] S
4939 870.871155 192.168.1.113 17.253.3.208 TCP 66 [TCP Window Update] 56129 → 80 [ACK] S
4952 870.953412 192.168.1.113 17.253.3.208 TCP 66 [TCP Window Update] 56130 → 80 [ACK] Seq
Frame 4952: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en6, id 0
Ethernet II, Src: Apple_01:84:12 (38:f9:d3:01:84:12), Dst: BelkinIn_fc:03:10 (b4:75:0e:fc:03:10)
Internet Protocol Version 4, Src: 192.168.1.113, Dst: 17.253.3.208
0000 b4 75 0e fc 03 10 38 f9 d3 01 84 12 08 00 45 00
0010 00 34 00 00 40 00 40 06 00 00 c0 a8 01 71 11 fd
0020 03 d0 db 42 00 50 5f 35 f4 30 8e fb 3b 24 80 10
wireshark_Thunderbolt EthernetB4LBU0.pcapng
Packets: 64540 · Displayed: 41 (0.1%)
Profile: Default

- Apple responds
  will change practices
  most data is sent encrypted
  IP address NOT logged
  ???
  most security suites work the same way

And then ...

MFA

- Authenticators
- Security keys
- SMS clear text voice

Current issues

- 27.7 million Texas drivers data exposed
  Vertafore data breach
  DL numbers, names, DOB, histories, addresses
  yet another unprotected cloud share
  DMVs can and do sell drivers data
  Drivers' Privacy Protection Act
  Chapter 123 Title 18 US code
  ah the exceptions 14 exceptions

Current Issues

- Let’s Encrypt root cross certificate expires
  September 1, 2021
  Android
- Android Chrome & …
- Apple updates
- 14.2
- 12.4.9
  Related to Chrome & Windows updates
- Zerologon & VPN
  Perfect storm? Pandemic, Election, economy, …
- NAT “SlipStream”

- DNS cache poisoning
- DNS cache crisis 2008
- Most servers today are vulnerable

Sad DNS

- Pwn2Own - China version
  Successes
  Adobe PDF reader, Apple iOS 14, CentOS, Safari 14, Chrome, Windows 10 2004, Firefox, VMware ESXi, TP-Link, …

Tianfu Cup

Ransomware

- Now not news
- Wher is the money going?
- Reporting loophole
- Stolen Facebook accounts advertise ransomware data auctions
- Ryuk 20 attacks/week
- 2 dozen RaaS
- Our economy sinks, theirs soars

- Fire risk
- Surveillance
- Jackson, Mississippi 45 day trial
- “not me, thanks” all the neighbors
- Law enforcement bite-back

Ring doorbells


QUESTIONS?

- 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