

Questions, Issues,  
Concerns, Suggestions  
Welcome at any time  
Even Now

# Sun City Computer Club

Windows SIG

August 28, 2018

- Safer not Safe
- E-postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio not wireless

**Vocabulary**

- KB4100347 8/21 Problems??
- DNS rebinding
- Security camera serial number
- “sandbox” desktop
- Outlook “usefulness”

**Breaking News**

- My apology for last month's missed meeting
- Switch from Gmail to Computer club's email
- Survey
  - 1) I can't wait to patch Windows
  - 2) I avoid patching as long as possible
  - 3) I patch when I get a



**SIG News**

**Vulnerable device  
manufacturers<sup>1</sup>**

**Representative  
manufacturers**

**Estimated number of vulnerable  
devices, worldwide<sup>2</sup>**

**87%**

of switches, routers,  
and access points

Aruba  
Avaya  
Cisco  
Extreme  
Netgear

14 million

**78%**

of streaming media  
players/speakers

Apple  
Google  
Roku  
Sonos

5.1 million

**77%**

of IP phones

Avaya  
Cisco  
Dell  
NEC  
Polycom

124 million

**75%**

of IP cameras

Axis Communications  
GoPro  
Sony  
Vivotek

160 million

**66%**

of printers

Hewlett Packard  
Epson  
Konica  
Lexmark  
Xerox

165 million

**57%**

of smart TVs

Roku-integrated  
Samsung  
Vizio

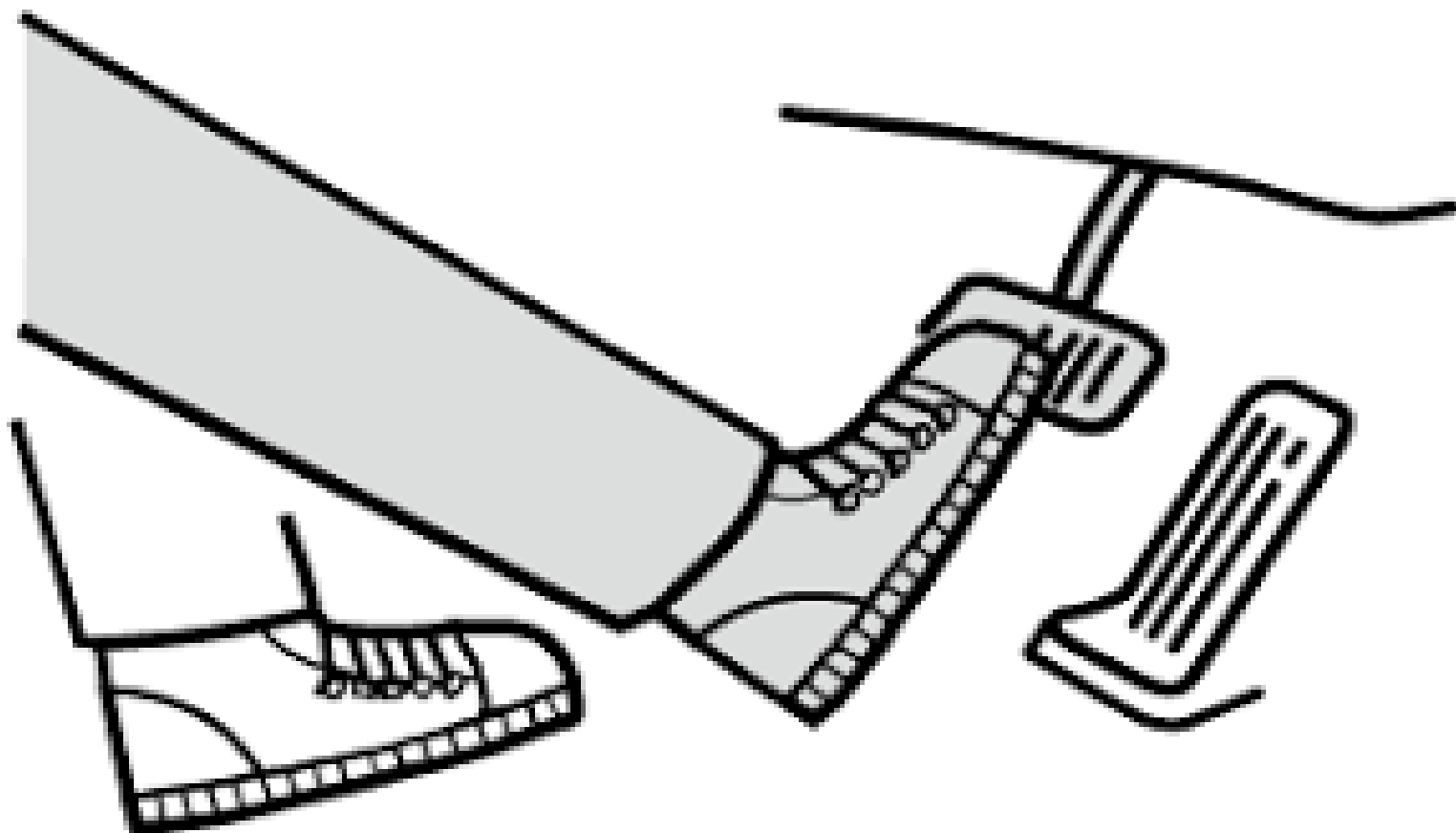
28.1 million

©2018 Armis, Inc Research on estimated exposure of enterprise devices by DNS Rebinding

*% of devices impacted by manufacturer and estimated global enterprise exposure*

- Venmo public by default
- Google Docs
- CCleaner yet again
- Browser site isolation
- DC Police surveillance camera hack
- Police department ransomware - thrice

## Current Issues





- File - computer resource for recording data
- Folder - file of file names  
Directory
- File system  
NTFS, FAT, exFAT, Live File System, ReFS  
FAT File - Allocation Table 8.3  
subdirectories, attributes, r/w/e/d  
NTFS  
ACL, links, multiple streams, quota,  
encryption, compression, ...

## Files and Folders

- SMB Server Message Block
- V1 V2 V3
- CIFS “share”

Common Internet File System  
NAS Network Attached Server

**SMB Server Message Block**

- Data of data
- Filename.extension  
e.g. myfile.txt, myfile.dat, myfile.jpg
- Application to extension mapping
- Right click “Open With”
- File Explorer

**MetaData**

- Magnetic drum
- Cassette tape
- Paper tape
- Floppy disk
- Hard disk
- Optical disk
- Solid state
- Flash drive

**Storage media**

- Hardware presents a series of “blocks”
- Filesystem allocates blocks to files
- As blocks fill, more blocks are added to the series of blocks
- When file is deleted, the blocks are marked “free”
- There is unused space in a block
- Over time disk is fragmented

## Filesystem abstraction

File Explorer window showing the left sidebar with Quick access links (Desktop, Downloads, Documents, Pictures, Music, Videos, OneDrive, This PC, 3D Objects) and a list of items (Desktop, Documents, Downloads, Music, Pictures, Videos, HP (C:), FACTORY\_IMAG).

**Optimize Drives**

You can optimize your drives to help your computer run more efficiently, or analyze them to find out if they need to be optimized. Only drives on or connected to your computer are shown.

Status

Drive	Media type	Last run	Current status
HP (C:)	Hard disk drive	Running...	20% analyzed
FACTORY_IMAGE (	Hard disk drive	8/8/2018 11:35 AM	OK (0% fragmented)
SYSTEM	Hard disk drive	8/8/2018 11:27 AM	OK (0% fragmented)

Stop

Scheduled optimization

**On**

Drives are being optimized automatically.

Frequency: Weekly

Change settings

Close

**HP (C:) Properties**

Security | Previous Versions | Quota

General | Tools | Hardware | Sharing

Error checking

This option will check the drive for file system errors.

Check

Optimize and defragment drive

Optimizing your computer's drives can help it run more efficiently.





Optimize



OK Cancel Apply

## Optimize Drives

You can optimize your drives to help your computer run more efficiently, or analyze them to find out if they need to be optimized. Only drives on or connected to your computer are shown.

### Status

Drive	Media type	Last run	Current status
 WINDOWS (C:)	Solid state drive	7/18/2018 4:06 PM	Optimization not available
 RECOVERY (D:)	Solid state drive	Never run	Optimization not available
 Windows (F:)	Hard disk drive	8/8/2018 9:17 PM	OK (0% fragmented)
 Recovery Image (G:)	Hard disk drive	8/8/2018 9:18 PM	OK (0% fragmented)


 Analyze Optimize

### Scheduled optimization

**On**

Drives are being optimized automatically.

Frequency: Weekly

 Change settings

Close

- Hard disk  
head sector track
- Solid state disk  
RAM -> Flash

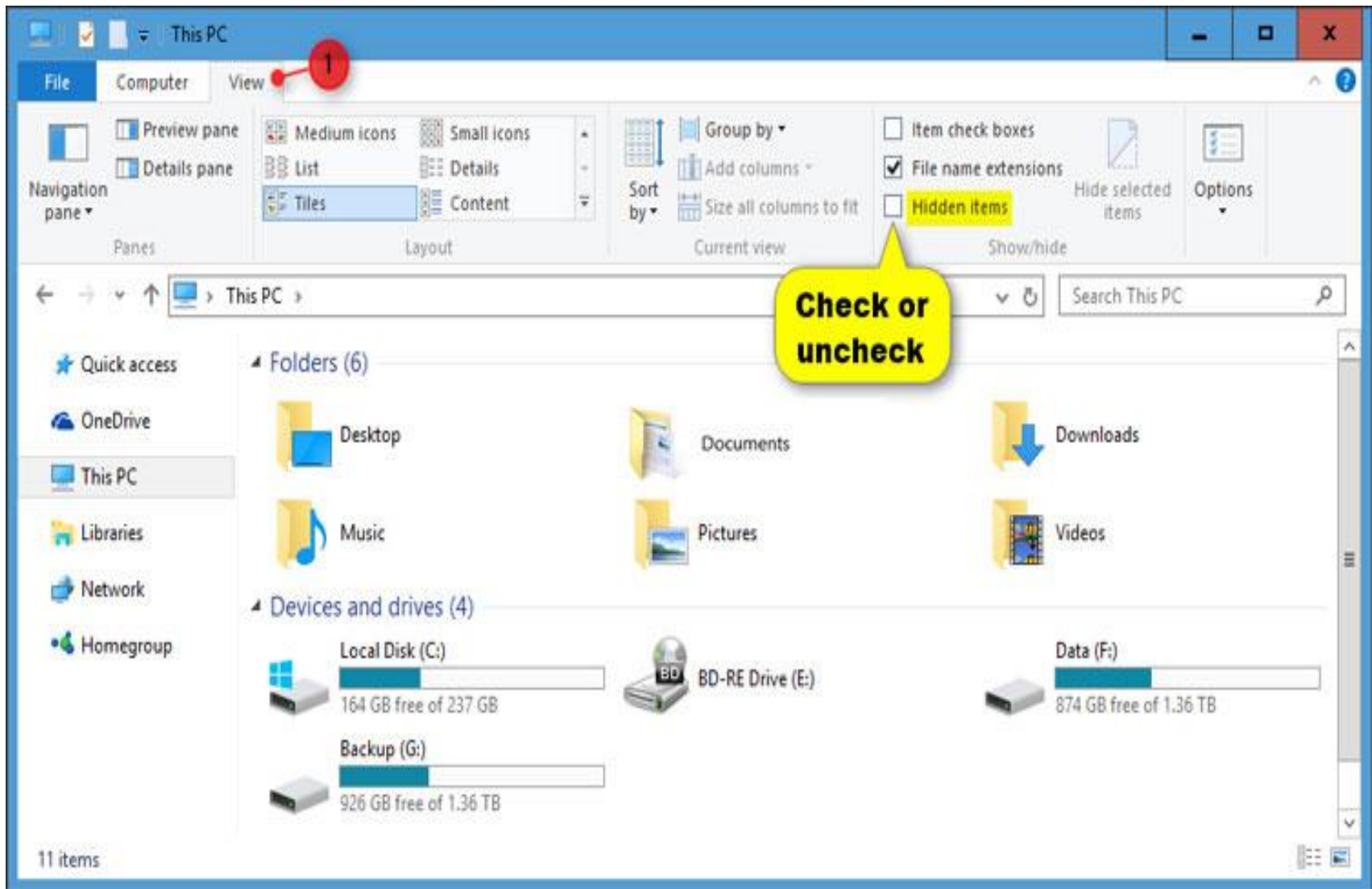


# Drive technology



- Hard disk
  - mechanical
  - defects
  - seek time latency
  - horizontal then vertical magnetic domains
  - controller optimization
- Solid state disk
  - no seek time
  - capacitance based cells finite life
  - cheaper

## Disk Technology



Choose Details



Select the details you want to display for the items in this folder.

Details:

- ☒ Name
- ☒ Date modified
- ☒ Type
- ☒ Size
- ☐ #
- ☐ 35mm focal length
- ☐ Account name
- ☐ Album
- ☐ Album artist
- ☐ Album ID
- ☐ Anniversary
- ☐ Assistant's name
- ☐ Assistant's phone
- ☐ Attachments
- ☐ Attributes



Move Up

Move Down

Show

Hide



Width of selected column (in pixels):

272

OK

Cancel

- Share a file/folder
- Map a Network Drive
- Homegroup workgroup
- Network Attached Storage NAS
- MacOS Command+K  
smb://<IP of Windows>
- Security ransomware, snoop SID

**SMB**

- The good  
Internet zone for downloads  
File Classification Infrastructure

```
C:\Tools\DiskTools\Streams>streams c:\test\TestFile2.txt  
  
Streams v1.56 - Enumerate alternate NTFS data streams  
Copyright (C) 1999-2007 Mark Russinovich  
Sysinternals - www.sysinternals.com  
  
c:\test\TestFile2.txt:  
:SecondStream:$DATA 27
```

- The bad  
malicious data hidden from normal view
- How many? thousands

## Alternate Data Stream ADS

- Questions, suggestions, comments?
- Please wait for microphone
- Next Meeting September 25
- Help with Chairs You know the drill  
front row to front of room  
stack 7 high
- Chicken Little
- Tortoise and hare
- Each of us safer, all of us safer
- Do nothing no problem  
    <most of us>
- Do everything - catastrophic