Sun City Computer Club

Cyber Security SIG

July 1, 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

SIG News

- Cyber Security News Archive Articles
  - Snapchat on iPhone update
  - LastPass issues/problems
  - Optional Updates for windows
  - Update iOS 12.5.4 - older Apple devices
- In Person meetings
- No Camera? Don’t start video
- No Computer – use phone
- No time – view recorded sessions

NSA-CISA-NCSC-FBI Joint Cybersecurity Advisory on Russian GRU Brute Force Campaign

07/01/2021 07:16 AM EDT

Original release date: July 1, 2021

The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and the UK's National Cyber Security Centre (NCSC) have released Joint Cybersecurity Advisory (CSA): Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments.

The CSA provides details on the campaign, which is being conducted by the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS). The campaign uses a Kubernetes® cluster in brute force access attempts against the enterprise and cloud environments of government and private sector targets worldwide. After obtaining credentials via brute force, the GTsSS uses a variety of known vulnerabilities for further network access via remote code execution and lateral movement.

CISA strongly encourages users and administrators to review the Joint CSA for GTSS tactics, techniques, and procedures, as well as mitigation strategies.

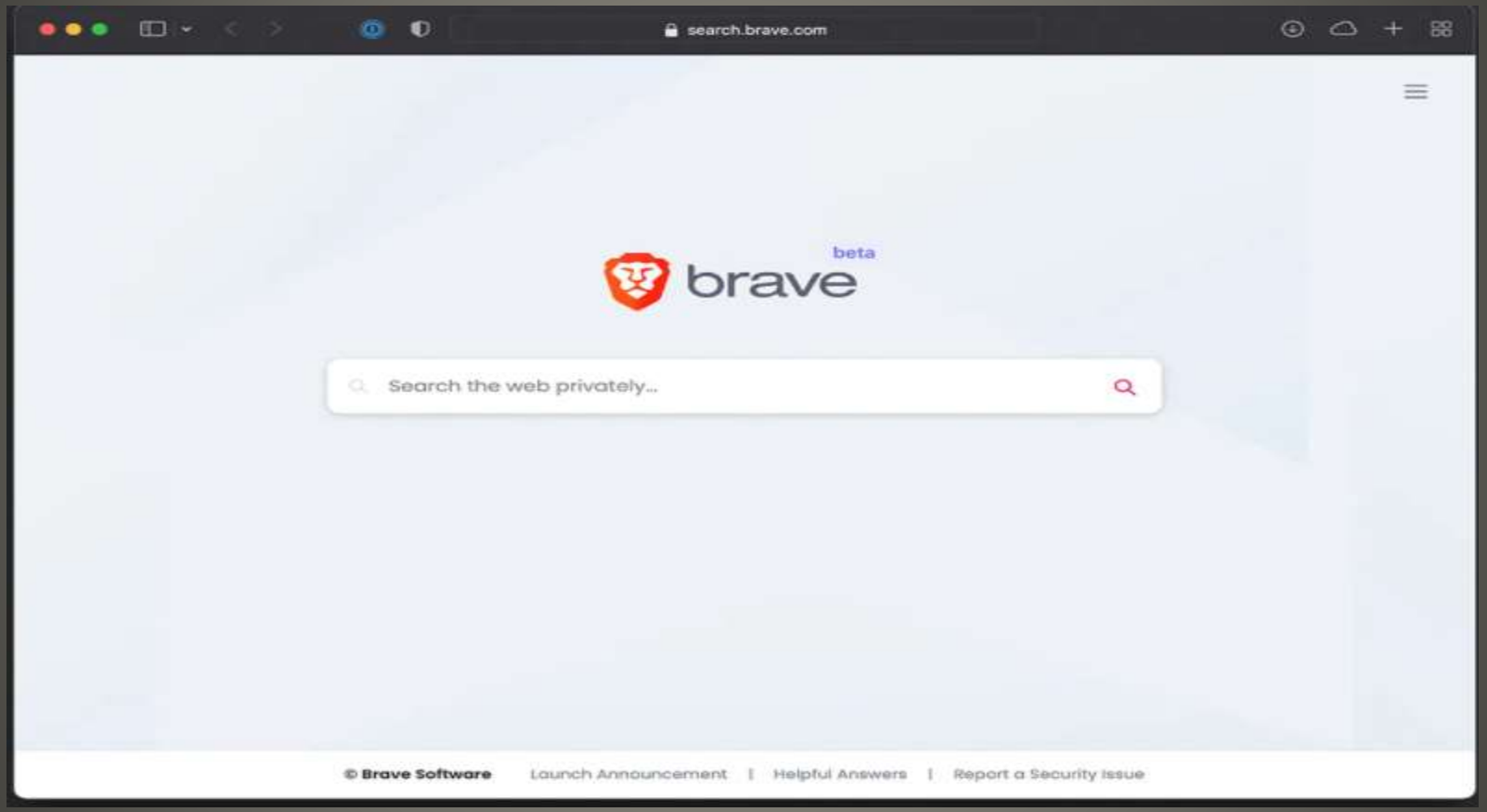
Joint Advisory Brute Force

Firmware

- Suddenlink cable modem woes
- Unsure this related

  Post card detailing replacement cable modem to arrive
- Firmware - attacks increasing

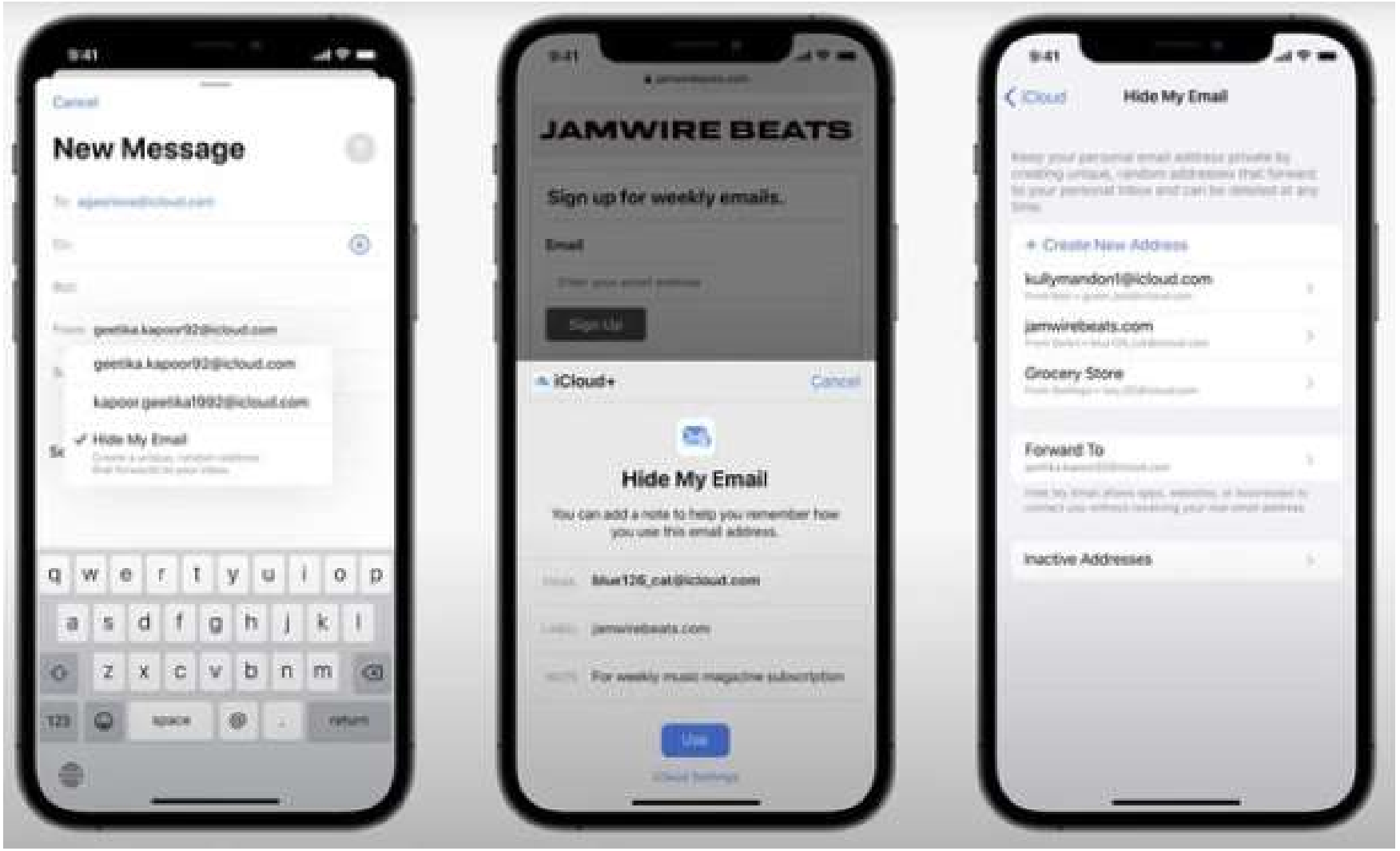
- https://search.brave.com



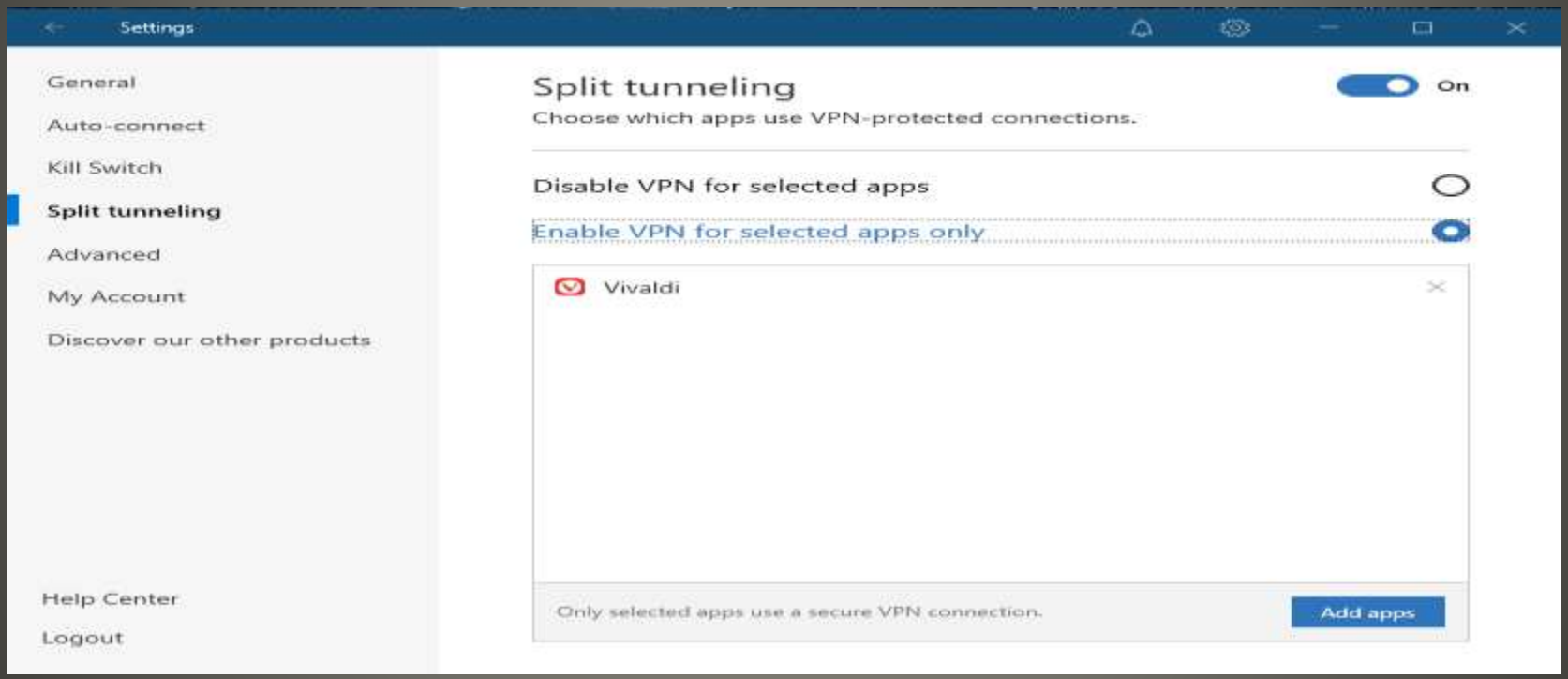
Brave search engine - Beta

iCloud+

- Security code if your device is lost
- “Digital Legacy” choose who can access your files after your death
- HomeKit for security camera feed storage
- Hide My Email
  Unique Random eMail address
  Forwarded to your chosen eMail address
  Delete at any time
- Private relay
  Safari Tor


9:41
Cancel
New Message
geetika.kapoor92@icloud.com
kapoor.geetika1992@icloud.com
Hide My Email
JAMWIRE BEATS
Sign up for weekly emails.
Email
Sign Up
iCloud+
Cancel
Hide My Email
You can add a note to help you remember how you use this email address.
For weekly music magazine subscription
Use
iCloud Settings
iCloud
Hide My Email
+ Create New Address
kullymandon1@icloud.com
jamwirebeats.com
Grocery Store
Forward To
Inactive Addresses

- Pick and choose
- Best for ???



Split tunneling - VPN


TURN
POSTED
NO HUNTING
FISHING
TRESPASSING
ONE WAY
STOP
ONE WAY
KEE
LEFT
getty images

Current Issues

- *Marvel's Avengers* patch 1.8b
  Shows real IP address PS5
- NSA collaboration center
  NSA restrictions
  Give and Take
  Industry
- June 30 deadline for Stir/Shaken
  Secure Telephone Identity Revisited
  Signature based Handling of Asserted Information using Tokens
  Stir – protocol
  Shaken – framework for tracking
  Caller ID signed
- Microsoft signed driver Netfilter
  Targeting gaming in China Really signed mistake?
- FTC vs Facebook
- LinkedIn data for 700 Million users for sale
- NVIDIA GeForce Experience – remote data access, manipulation, and deletion

Current Issues

- Spoofing
  eMail, WEB addresses, IP addresses, callerID
  Your Area code, IRS, Sherriff, etc.
  Legal iff no intent to cause harm
  Law enforcement, victims of domestic violence, medical,

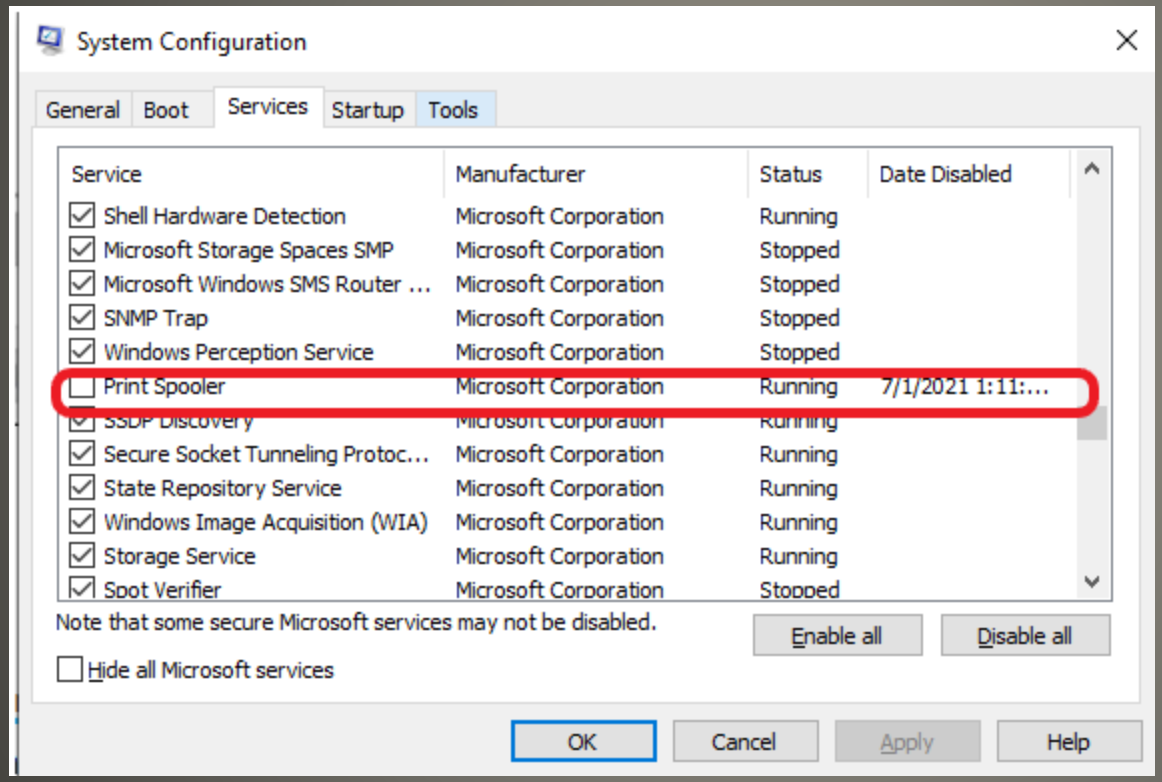
Telephone Robocall Abuse Criminal Enforcement and Deterrence Act
Traced Act December 2019 18 month
Extension requests denied
but, small providers June 30, 2023
Switch to those smaller providers
Obtain "close enough" callerID

Deter Obnoxious Nefarious and Outrageous Telephone Act
Do Not

Print Nightmare

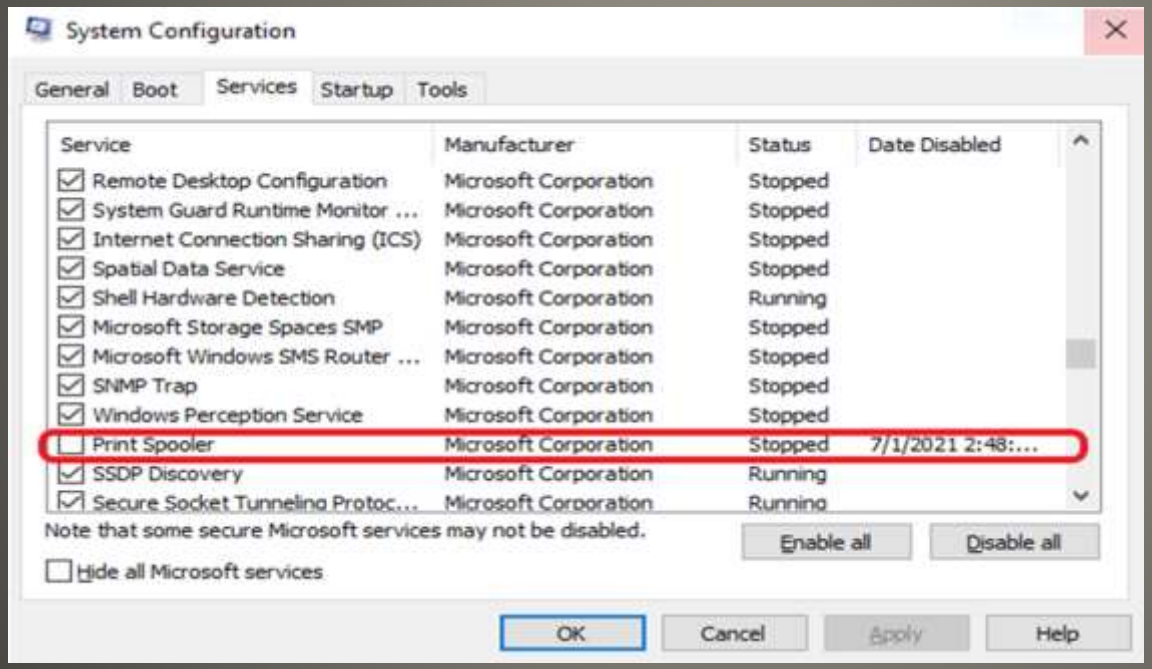
- Microsoft Print Spooler vulnerabilitie(s)
- Elevation of Privilege (EoP)
- ALL versions of Windows
- *Remember Administrator caution ?*
- PoC published after a patch
- Bug elevated Remote Code Execution (RCE)

- Disable / Stop print Spooler service
- Run > msconfig



PrintNightmare

- Reboot
- IFF needed, reenable & reboot AFTER patch



PrintNightmare

- CMD Run as Administrator

```
C:\Users\duck>sc query Spooler

SERVICE_NAME: Spooler
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

```
C:\Users\duck>sc config Spooler start= disabled
```

```
C:\Users\duck>>sc query Spooler

SERVICE_NAME: Spooler
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

PrintNightmare


Stealing your cookies... bye,bye!
OK

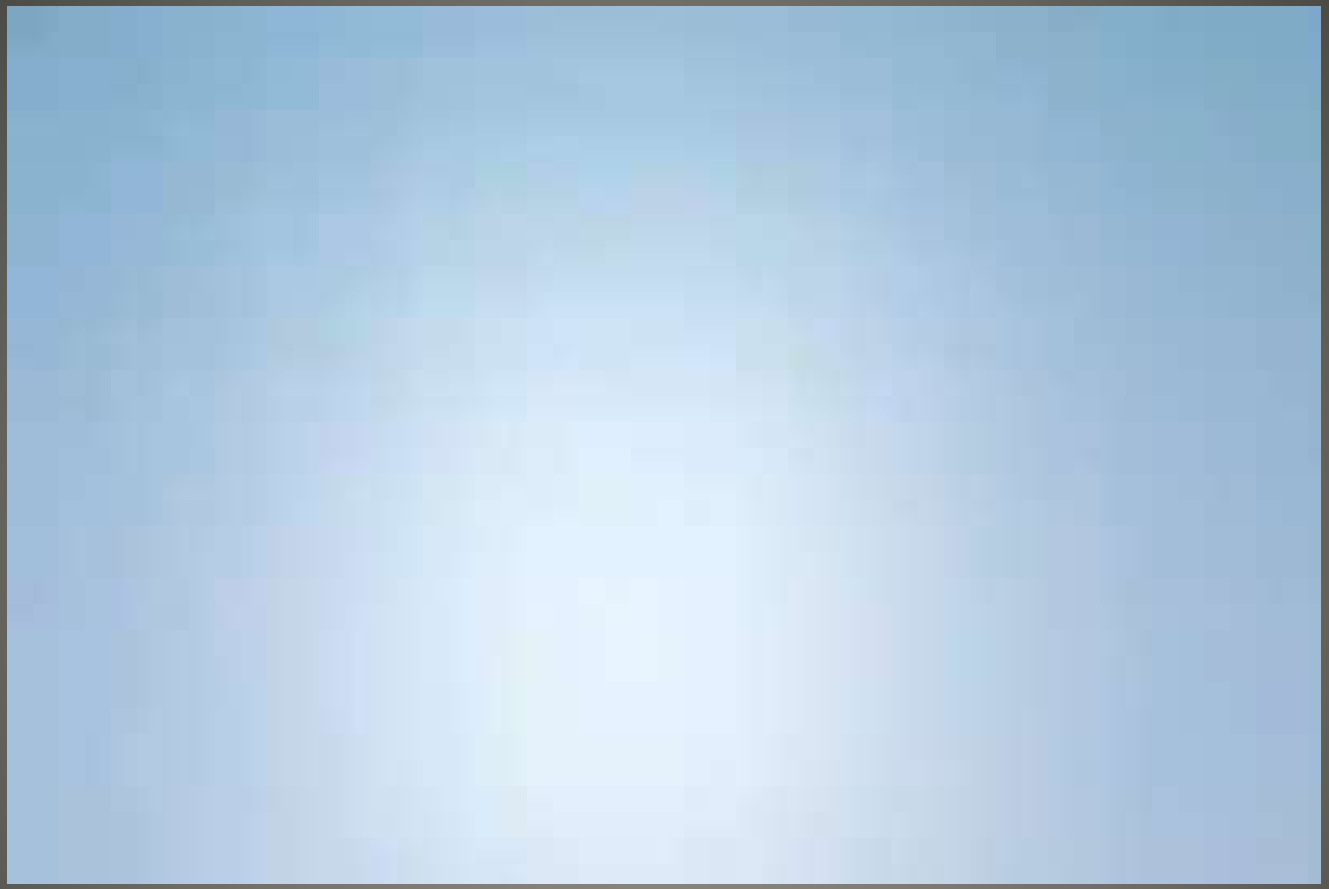

POC FACEBOOK XSS ACCOUNT TAKEOVER CVE-2021–34506
Watch later
Share
Recordar contraseña
Vansh Devgan (Mayank Sharma)
Intro

Edge vulnerability

- Microsoft Translator
  Universal cross site scripting
  3-June first report
  24-June patch
  $20,000 reward

Current Issues

- IoT
  Power switch App China based
- Sidewalk
- FLoC
- Ireland's Health Care system ransomware
  Ireland's high court
  "give it all back" "tell us who" "turn yourself in"
  $20M ransom $120M recovery $600M cost
  Consulting professionals - decryptor supplied



Windows 11

Windows 11

- The last version of windows (sic)
- 64-bit, 4GB RAM, 64GB storage
- No 32-bit support
- Windows 10 support end Oct 14, 2025
- Windows 11 lure

  SHA256hash

B8426650c24a765c24083597a1eba48d9164802bd273b678c4fefe2a6da60dcb

- Beware Insider ToS

Windows 11

- UEFI, secure boot capable
- TPM V2.0 or greater
- Home edition – Microsoft account & Internet
- Microsoft store 12% fee or no fee
  Apple App store & Google Play 15-30%
  Android apps Amazon's Appstore
- App store Updates moved to Library icon

Windows 11 Android Apps Your Phone

- Automatic HDR (High Dynamic Range)

Xbox features

- Direct storage

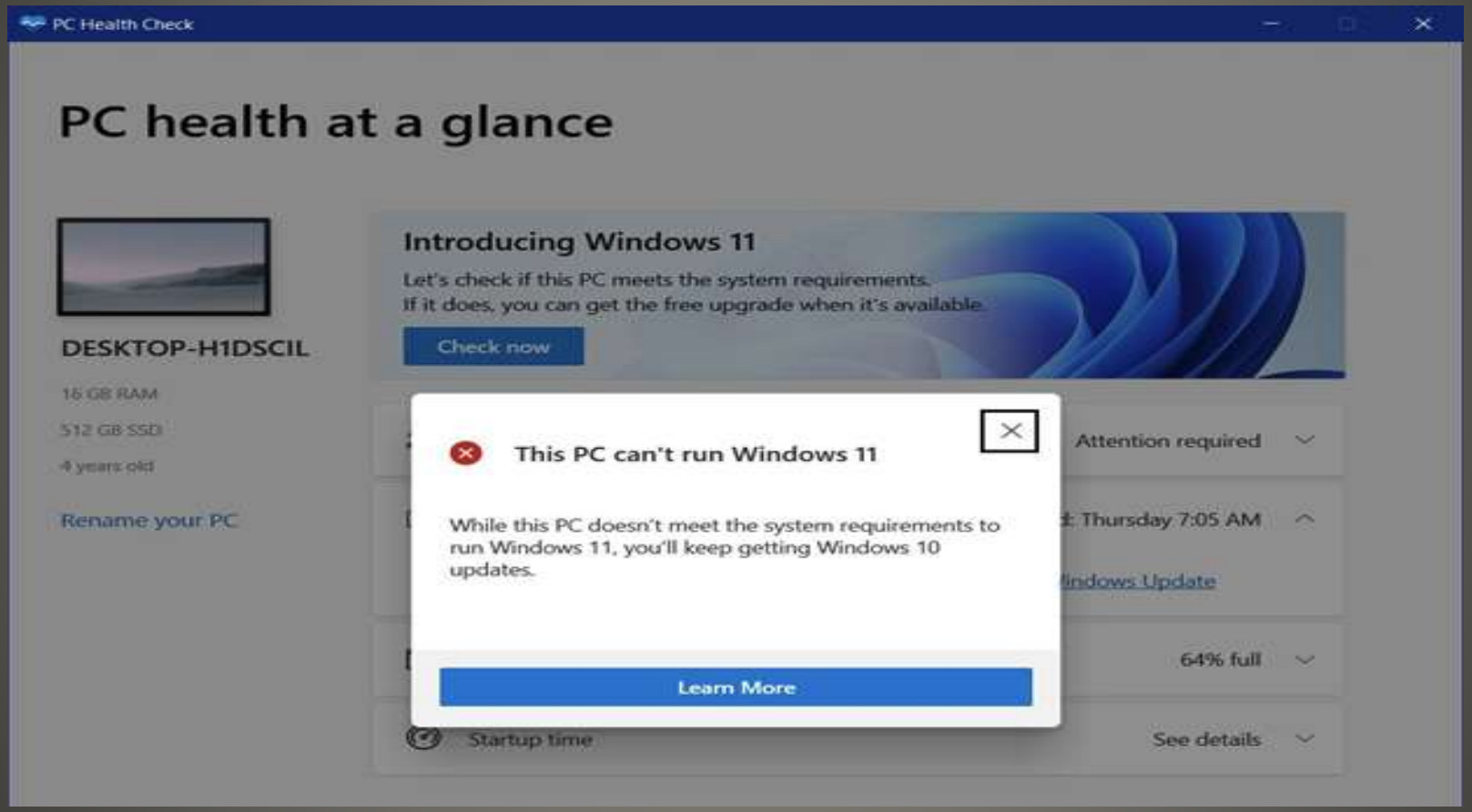
  Large game worlds loaded from speedy drives
- Xbox game pass

Xbox Features Windows 11

Windows 11 features

- Windows widgets
- Windows Teams
- Snap layouts
- Rounded corners
- Feature updates one per year
- “Holiday Season” release
- Trusted Platform Module (TPM V2.0)
- Firmware attacks
- Modern CPUs, Secure boot, virtualizations

- https://aka.ms/GetPCHealthCheckApp



PC Health Check

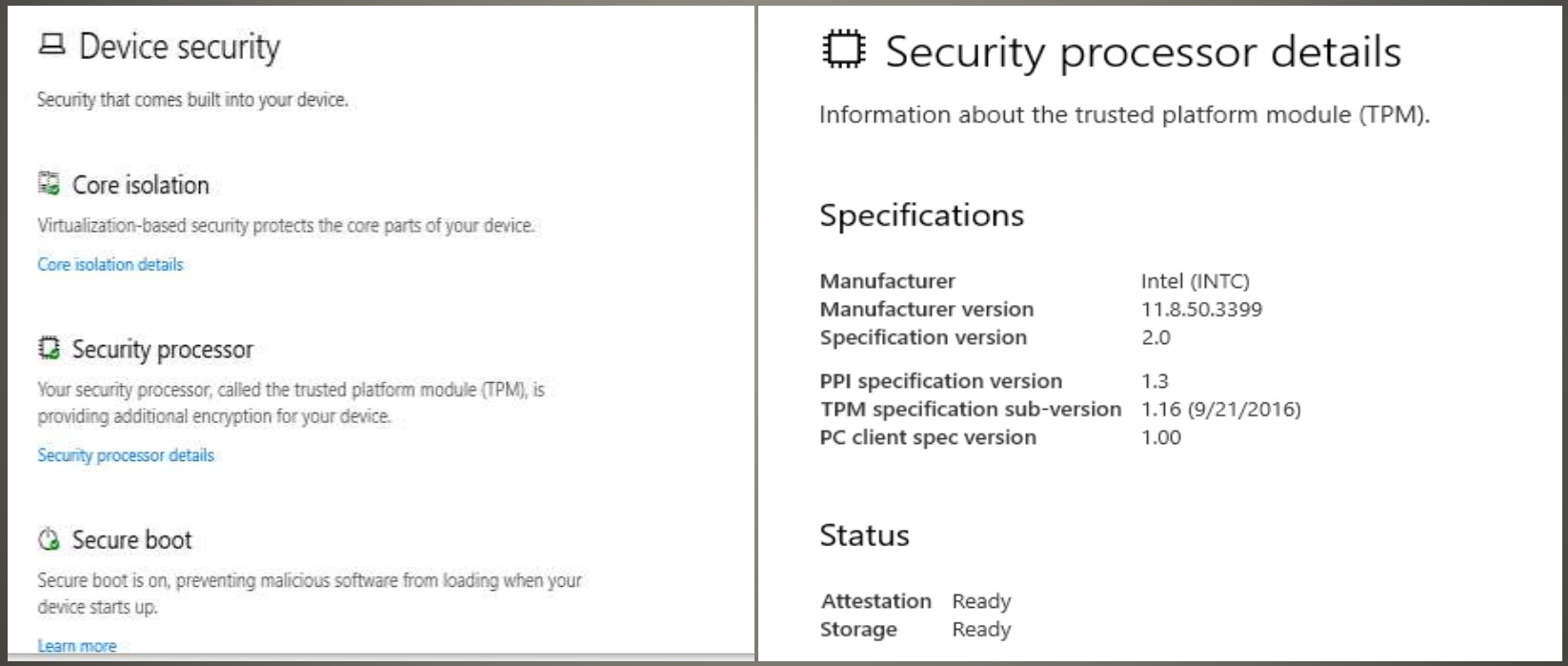
Windows 11 features

- Snap layouts
- Snap groups
- Taskbar teams
- Teams update
- Widgets
- Enhanced touchscreen, pen, voice
- Xbox
- Design/Interface
- Android App integration
- Virtual desktop improvements
- Smaller security updates

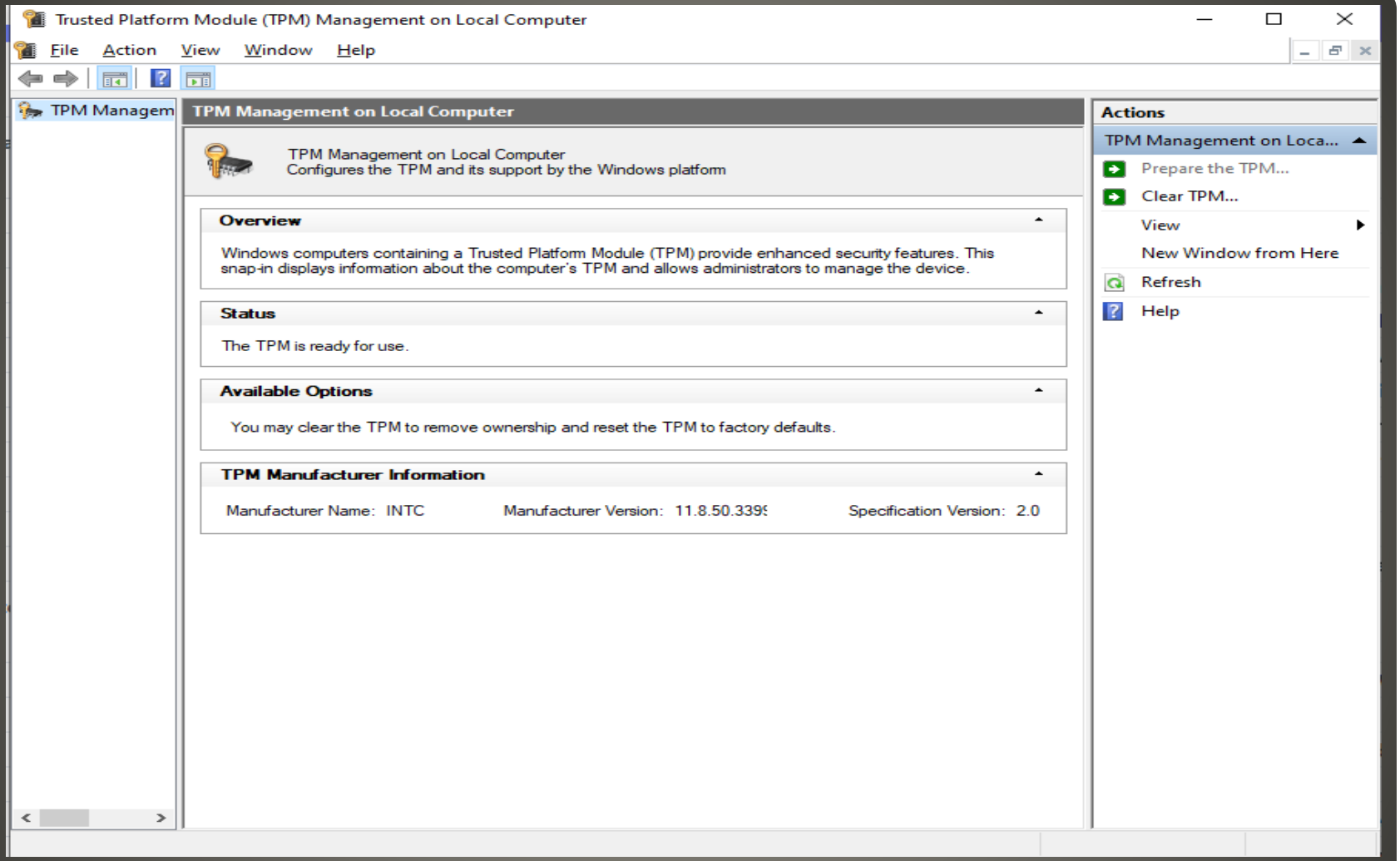
- Windows 10
  4.4.0-19041
- Windows 11
  4.19.128 -> 5.10.16.3

Windows 11 WSL

- Windows Security > Virus & threat Protection > Device Security
- Device Security



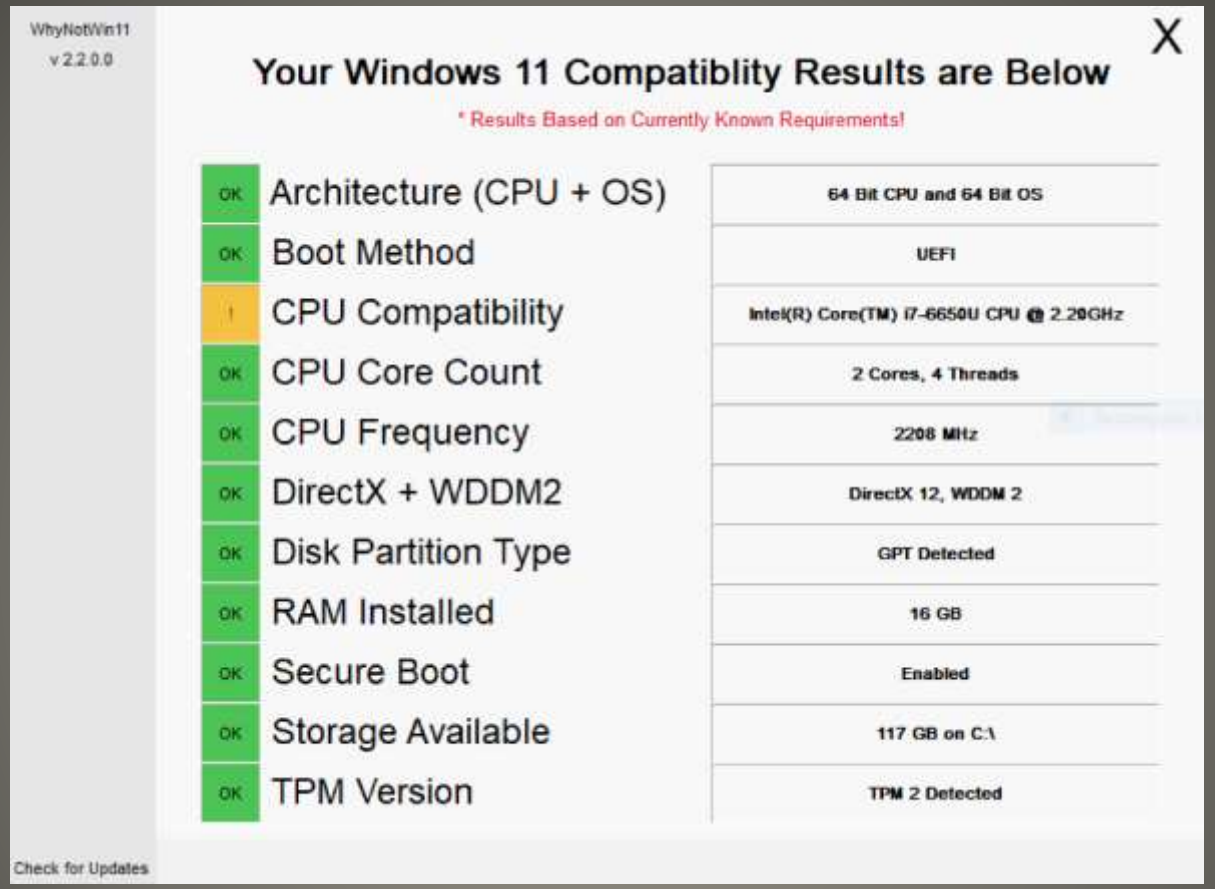
TPM


Trusted Platform Module (TPM) Management on Local Computer
File Action View Window Help
TPM Managem
TPM Management on Local Computer
TPM Management on Local Computer
Configures the TPM and its support by the Windows platform
Overview
Windows computers containing a Trusted Platform Module (TPM) provide enhanced security features. This snap-in displays information about the computer's TPM and allows administrators to manage the device.
Status
The TPM is ready for use.
Available Options
You may clear the TPM to remove ownership and reset the TPM to factory defaults.
TPM Manufacturer Information
Manufacturer Name: INTC
Manufacturer Version: 11.8.50.339
Specification Version: 2.0
Actions
TPM Management on Loca...
Prepare the TPM...
Clear TPM...
View
New Window from Here
Refresh
Help

tpm.msc

- Intel Platform Trust Technology (PTT)
- AMD Ryzen fTPM
- Can add?
- FOLLOW STEPS

TPM


WhyNotWin11
v 2.2.0.0
Your Windows 11 Compatiblity Results are Below
* Results Based on Currently Known Requirements!
OK Architecture (CPU + OS)
64 Bit CPU and 64 Bit OS
OK Boot Method
UEFI
! CPU Compatibility
Intel(R) Core(TM) i7-6650U CPU @ 2.20GHz
OK CPU Core Count
2 Cores, 4 Threads
OK CPU Frequency
2208 MHz
OK DirectX + WDDM2
DirectX 12, WDDM 2
OK Disk Partition Type
GPT Detected
OK RAM Installed
16 GB
OK Secure Boot
Enabled
OK Storage Available
117 GB on C:\
OK TPM Version
TPM 2 Detected
Check for Updates

WARNING!!!

TPM & such

TPM 1.2 and 2.0

Crypto-processor
- Random number generator.
- RSA/ECC key generator.
- HMAC generator.
- SHA-1/SHA-256 hash generator.
- Signature engine

- **Platform integrity.** Makes sure the boot process is correct.
- **Disk encryption.** The encryption key used for dis encryption is fully or partially defined by the SRK.
- **Password protection.** The storage of the user's password in the chip.

Versatile memory:
- Platform Configuration Registers (PCR).
- Attestation Identity Keys (AIK).
- Storage Keys.

Persistent memory:
- Endorsement Key (EK). A private key from a key pair. A user wishing to send a message to this TPM uses the public key to encrypt. Public key is also stored on TPM.
- Storage Root Key (SRK). Used to encrypt disk storage.

TPM & such

- Trusted boot environment
- Endorsement key pair
- Storage Root key pair
- RSA (usually)
- Used to encrypt AES key for encryption
- Return of Coppersmith Attack
  week RSA prime number generator
  Estonia e-ID
  Static ID -> Mobile devices

Apple

- T2 chip
- Soldered on motherboard
- Secure enclave
- Storage and biometric and sound microphone disabled with lid closed

Dropped support for “old”

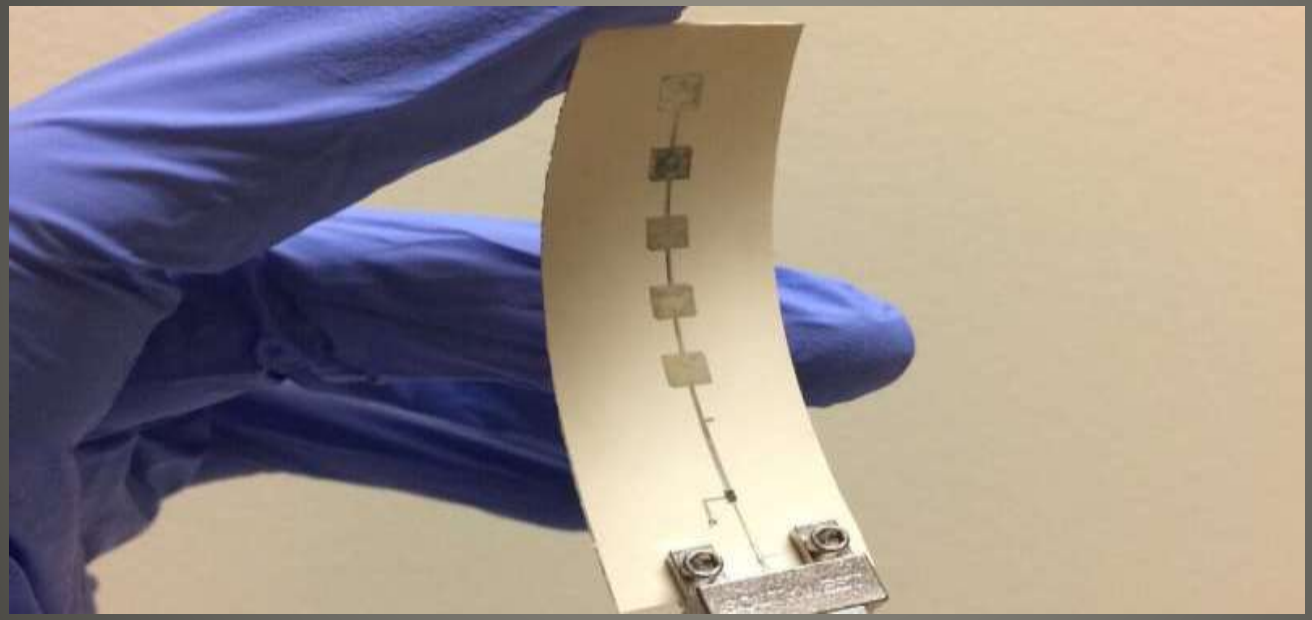
Beta updates
Big Sur 11.4 Beta Big Sur 11.5 Beta 4
Monterey Beta

- depends

Linux

Current Issues

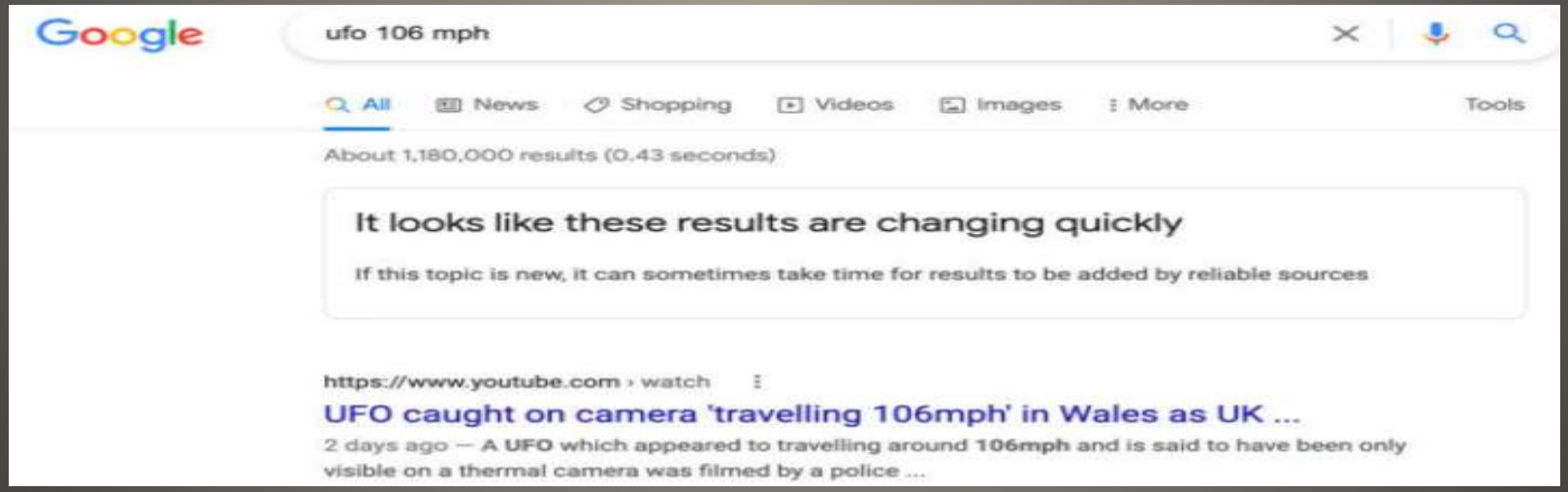
- Microsoft customer-server agents breach Subsequent attacks using customer info
- Backscatter IoT 5G low power



Backscatter IoT

- Energy harvesting
- 0 power wearable/implant sensors
- Smart home temperature, humidity, gases
- Agriculture frost, soil nutrients, livestock tracking

- Western Digital My Book Storage Devices
  Remotely wiped
- Google Search – reliability and rapid change warning
  Google aware – you should be too



Current Issues

Current Issues

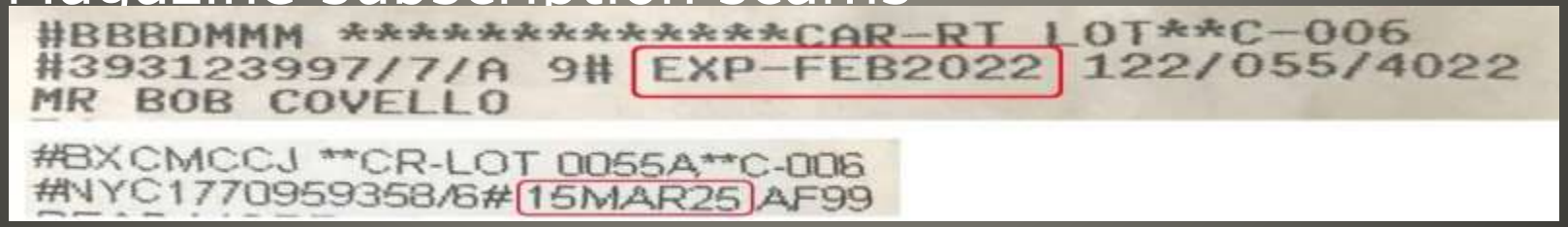
- Browser Updates
- Ransomware

  ProofPoint Report

  The First Step: Initial Access Leads to Ransomware

  Buy & Sale
- Tactical High Power Operational Responder

  THOR Drone defense hundreds at a time
- DMCA & security researchers
- Magazine subscription scams

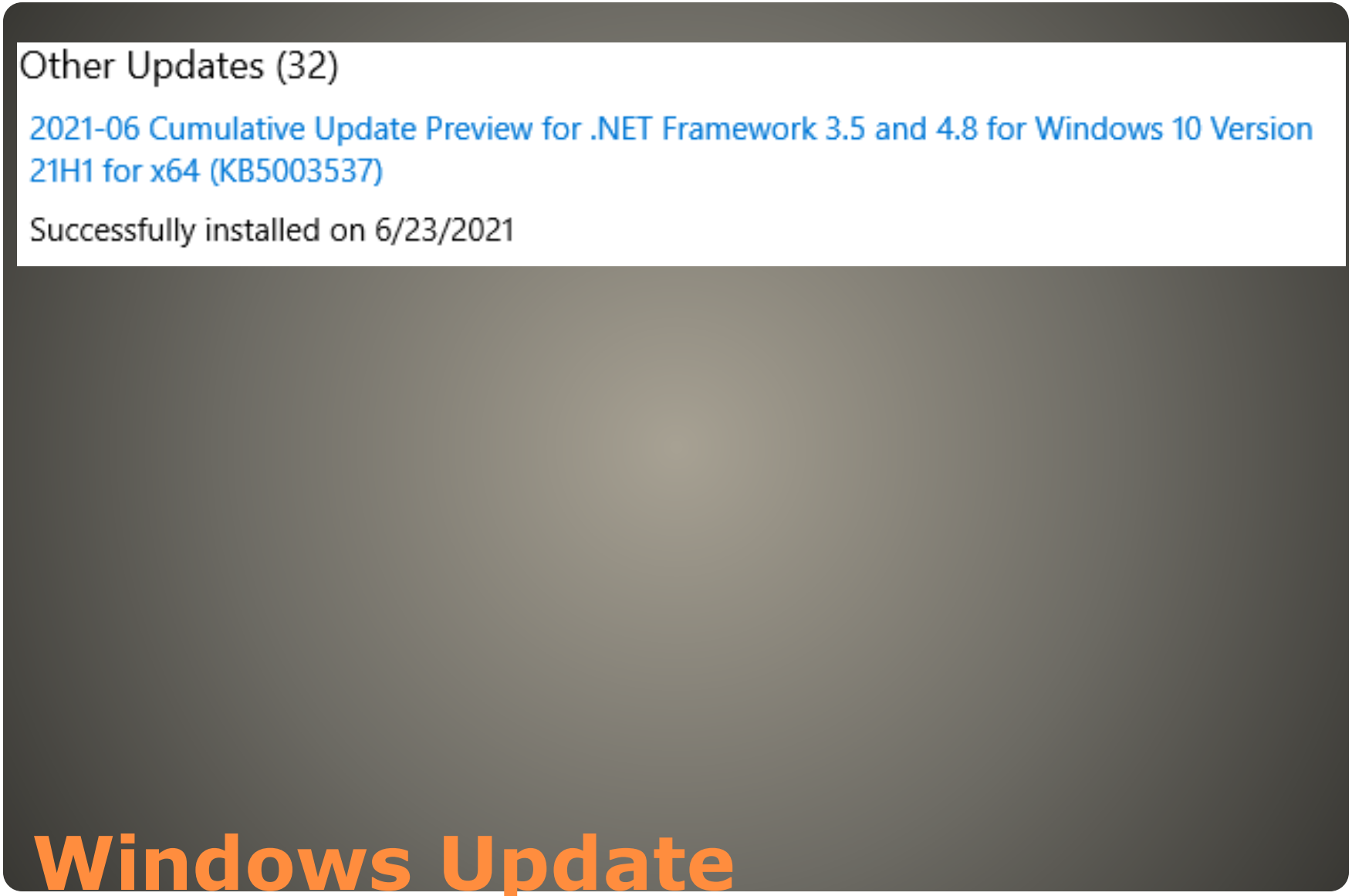


- Remote wipe
- Shoden
- Support ended 6 years ago
- Warring cyber criminals?
- 3-2-1 backup

Western Digital My Book

- “%p%s%s%s%s%n”

Wi-Fi network name to avoid



Windows Update

.NET Framework 3.5 and 4.8

The June 21, 2021 update for Windows 10, version 2004, Windows Server, version 2004, Windows 10, version 20H2, and Windows Server, version 20H2, and Windows Version 21H1 includes cumulative reliability improvements in .NET Framework 3.5 and 4.8. We recommend that you apply this update as part of your regular maintenance routines. Before you install this update, see the Prerequisites and Restart requirement sections.

Quality and reliability improvements

WPF[1]	- Addresses an issue affecting a DataGrid contained in an outer ScrollViewer. - Addresses a crash due to ElementNotAvailableException in a ListView with custom data-item automation peers.
CLR[2]	- When the process is not under high memory pressure it tends to favor doing BGCs over doing full compacting GCs. This is usually desirable but if the app behavior changes dramatically, it could cause much of the fragmentation in older generations (ie, gen2 and LOH) to be unused. You can collect GC ETW events which tell you how much fragmentation there is in gen2 and LOH and verify if you are in this situation.
Winforms	- Addresses an issue in Property Grid control to prevent incorrect data read in some scenarios in 64 bit processes. - Addresses an issue where System.Drawing double frees allocated memory when failing to get printer settings.
ClickOnce	- Addresses a regression introduced in previous updates. We now honor WinTrust policy setting "Ignore timestamp revocation checks" setting when validating timestamps in ClickOnce manifests.

1 Windows Presentation Foundation (WPF)
2 Common Language Runtime (CLR)

- 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