

Sun City Computer Club

Cyber Security SIG

July 15, 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**

- Where did the Russian criminals go?
Dunno, they ransomware

F

Firefox Version 90 release
Published • Jul 14

John Jenkinson 
 0  0  0



US Presidential Exesecurity Order 9-July-2021
Published • Jul 9

John Jenkinson 
 0  0  0

M

Microsoft emergency patch for PrintNightmare released today July 6
Published • Jul 6

John Jenkinson 
 0  0  0



Microsoft PowerShell PATCH ASAP
Published • Jul 6

John Jenkinson 
 0  2  0

W

Western Digital woes increase
Published • Jul 6

John Jenkinson 
 0  1  0

B

Bad Bad Android Apps!!
Published • Jul 3

John Jenkinson 
 0  0  0

S

Snapchat update on iPhone crashes after latest update
Published • Jun 28

John Jenkinson 
 0  0  0

L

LastPass issues/problems?
Published • Jun 23

John Jenkinson 
 0  0  0

A

Another Optional Windows 10 update from Microsoft June 21, 2021
Published • Jun 22

John Jenkinson 
 0  0  0

A

Apple releases security updates for iOS 12.5.4
Published • Jun 15

John Jenkinson 
 0  0  0

S

Strange occurrence - Microsoft Out of Band update for Windows 10
Published • Jun 12

John Jenkinson 
 0  0  0

C:\Program Files\WindowsApps\Microsoft.PowerShellPreview_7.2.7.0_x64_8wekyb3d8bbwe\pwsh.exe

PowerShell 7.2.0-preview.7
Copyright (c) Microsoft Corporation.

<https://aka.ms/powershell>
Type 'help' to get help.

PS C:\Windows\System32> **\$PSVersionTable**

Name	Value
PSVersion	7.2.0-preview.7
PSEdition	Core
BuildCommitId	7.2.0-preview.7
OS	Microsoft Windows 10.0.19043
Platform	Win32NT
PSCompatibleVersions	{1.0, 2.0, 3.0, 4.0...}
PSRemotingProtocolVersion	2.3
SerializationVersion	1.1.0.1
WSManStackVersion	3.0

Windows PowerShell - powershell

Try the new cross-platform PowerShell <https://aka.ms/pscore6>

S C:\Users\john> **\$PSVersionTable**

Name	Value
SVersion	5.1.19041.1023
SEdition	Desktop
SCompatibleVersions	{1.0, 2.0, 3.0, 4.0...}
BuildVersion	10.0.19041.1023
LRVersion	4.0.30319.42000
SManStackVersion	3.0
SRemotingProtocolVersion	2.3
SerializationVersion	1.1.0.1

S C:\Users\john>

PowerShell

10:25



Open tabs



You don't have any open tabs

+ New tab



Home



Collections



Tabs

- Austin kidnapping Cellular geofencing
- Power Partner event - Thermostat Incentives Opt-out
- Didi ride hailing app banned from China App stores - others to be investigated NYSE stock tumbles
- LinkedIn Tiananmen square interest?
- REvil Kaseya \$70M universal decryptor
- Recover data on Echo devices
- Intuit to share payroll data with Equifax Helpful <-> Harmful
- Facebook fires those who abuse company data
- New England Journal of medicine report electrodes speech area of paralyzed person's brain display words on display screen
- Colorado Consumer Privacy Law (California, Virginia, Colorado)
- Biden "any necessary action"
- Cyber security companies turning away new customers

Current Issues

- Stealth
- Motivated advisory
- Attack friends
- Cameras tell all tales
- Smart speakers – voice purchasing
- Logged in all over all the time
- “I agree”
- I will update my stuff when I get the time

WATCH OUT!



- Firmware
- Watch Out
 - Unusually slow - Why?
 - Windows – Task Manager
 - MAC – Activity Monitor
 - Investigate findings
 - Restart
 - Monitor Internet usage
 - Cable Modem
 - Router
 - Wireless Access Points
 - Neighborhood
 - Pop-ups
 - Crashes
 - Restarts
 - Alerts - Lack thereof

WATCH OUT!!



Video game cheaters



Car has hard drive?



Car has hard drive!

- Windows 365
- Mint Mobile
Name, address, cell phone number, email address, international call details, account number, ...
- Trickbot back - after pentagon takedown
VNC
ISP door-to-door
- SolarWinds yet again Serv-U
- PrintNightmare
Printer driver – Not a printer driver
BUT a highly privileged malware
Point and Print
July 6 patch
Having NoWarningNoElevationOnInstall set to 1 makes your system vulnerable by design
- China government control of 0-day exploit
Discoverer tells government
government decides on repairs, notifications

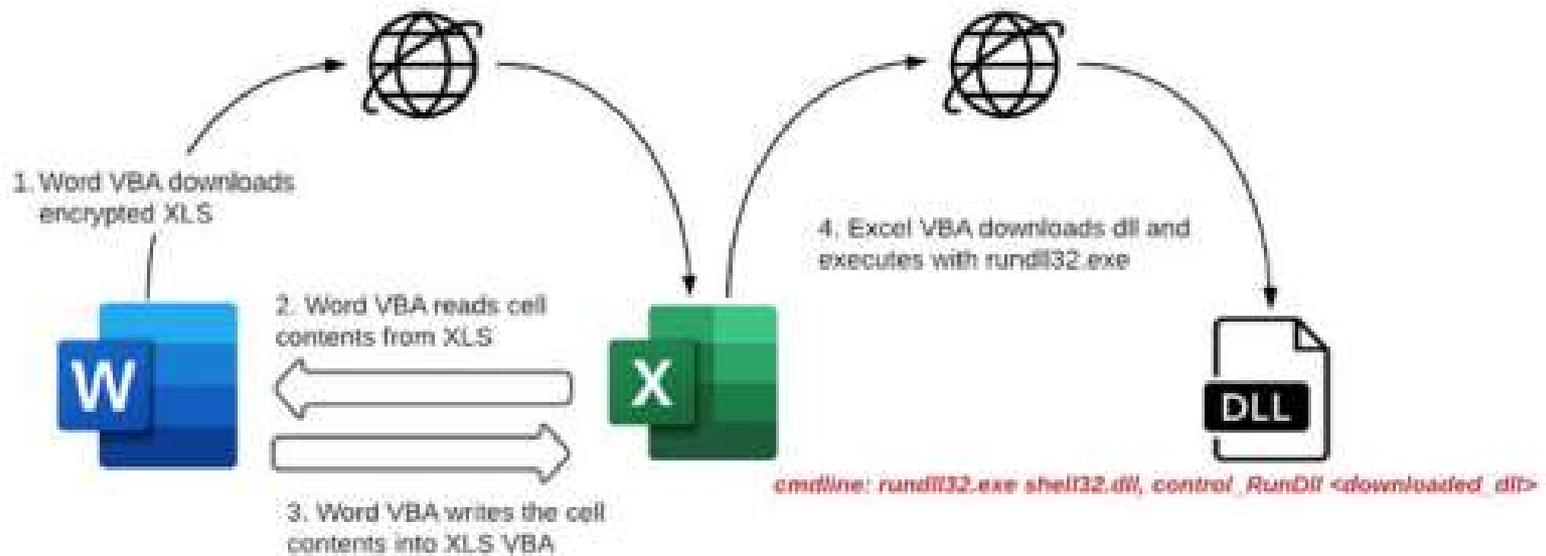
Current Issues

- SolarWinds with a twist
- Managed Service Providers 60
- 1500 MSP clients
- BUT
- Little follow-up
- e.g.
Recon, Backup find & destroy, data exfiltration,

Kaseya

- Windows SIG
 - Office macros
 - Microsoft Patch Tuesday
 - Windows PowerShell
 - Edge exploit to steal cookies
 - Facebook account takeover
 - Office macros – targeting certain financial institutions
- To view or edit this document, please click the 'Enable editing' button on the top bar, and then click 'Enable content'.***
- iOS 0-day compromise fully patched iPhones target government officials via Linked-in messages
 - Yet another Linked-in data breach

Current Issues



Zloader – Banking trojan

- MagSafe battery support
 - BOTH can be charged at same time
- Air quality information for certain countries
- More iOS 14 updates
- Apple Card Family

iOS 14.7

- REvil
- Sodinokibi
- WOW – if only

File Message Help Tell me what you want to do

Ignore Delete Archive Reply Reply All Forward Move OneNote Actions Mark Unread Categorize Follow Up Translate Read Aloud Zoom

Delete Respond Move Tags Editing Speech Zoom

Re: Arrival Notice

NR No Reply [DHL] <info@dhl.com>
To [Redacted]

Reply Reply All Forward ...

at 13.07.2021 3:38

Shipping Invoice Doc.pdf.7z
.7z File



AWB NO: 7253**8341**
ARRIVAL DATE: 12/07/2021

Dear Consignee,

Your parcel has arrived at the office. Our courier was unable to deliver the parcel to you due to wrong address from our customer.

To receive your parcel, please go to our closest office to show this AWB/invoice

please click the attachment to download and print invoice

Note: Document Password is AWB3604

Best Regards,

The DHL Team.



<p>Contact Center</p> <ul style="list-style-type: none"> > DHL Express > DHL Global Forwarding > DHL Freight > DHL Global Mail > DHL Supply Chain 	<p>About Us</p> <ul style="list-style-type: none"> > Partnerships > Company Portrait > Green Solutions > Innovation > Logistics Insights > Center Overview > Corporate Responsibility 	<p>Social Media</p> <ul style="list-style-type: none"> Facebook YouTube 	<p>Fraud Awareness</p> <p>Official Logistics Partner</p>
--	--	--	---

- info@dhl.com

- SPF check fail

Sender Policy Framework

- Image not HTML

Yahoo

Gmail

Suddenlink

- Always display external images - [Learn more](#)
- Ask before displaying external images

Show images in messages

- Always, except in spam folder
- Ask before showing external images

External Images Messages can sometimes contain images that are used to notify the sender that your email address is valid, which may increase the amount of junk mail you receive.

- Block external images when viewing HTML messages. Images received as attachments will be unaffected.
- Do not block external images when viewing HTML messages.

OK Cancel

eMail image handling

<http://stopransomware.gov/>

The screenshot shows the homepage of the Stop Ransomware website. At the top, the URL <https://www.cisa.gov/stopransomware> is visible in the browser's address bar. Below the address bar, there is a navigation bar with the "STOP RANSOMWARE" logo on the left and a search bar on the right. The main content area features three large, colorful panels: "WHAT IS RANSOMWARE?" with a red and black background, "HAVE YOU BEEN HIT BY RANSOMWARE?" with a laptop background, and "AVOID BEING HIT BY RANSOMWARE" with a blue background and a padlock icon. Each panel includes a "LEARN MORE" button. Below these panels, there are four icons representing different sections: "Protection and Response" (lightbulb), "Services" (hand holding gear), "K-12 Resources" (school building), and "Preparation" (star in a circle). At the bottom, a paragraph explains that ransomware is a form of malware that encrypts files and demands ransom for decryption, and that the website is the U.S. Government's official one-stop location for resources.

STOP RANSOMWARE

Search

WHAT IS RANSOMWARE?
LEARN MORE

HAVE YOU BEEN HIT BY RANSOMWARE?
LEARN MORE

AVOID BEING HIT BY RANSOMWARE
LEARN MORE

Protection and Response Services K-12 Resources Preparation

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. This website is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

US Government Stop Ransomware

- Q
- Blockchain based
- NO distributed ledger
- Your data all locked up
- Your data all locked up

SoLVBL Solutions

- 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