

Southern Districts Computer Users Club Inc.

Supporting inexperienced users with local expertise

Vol.: — 20

No : — 10

October, 2020

SDCUCI NEWS

Contacts: Web Site: — <http://sdcuci.com>
E-mail: — sdcucinc@gmail.com

Newsletter Editor: David Porteous — daibhidhp@aussiebb.com.au

Meetings are held monthly on the third Wednesday at 7.30 pm, in the hall at the rear of St Mary's Catholic Church on the Corner of Bains and Main South Roads, Morphett Vale

Cost \$3.00 per person per meeting. This includes a copy of our Newsletter, plus coffee/tea and supper

Visitors are most welcome

After 3 visits, you are requested to become members

Annual Subscription:
Single — \$20.00
Family — \$30.00

Both Novice and Experienced computer users will be most warmly welcomed



The Brownpaddock Chatter



Photo Editing — Colour Correction

As some of you may know, I am writing the story of my life (currently up to page 47 and I have only just arrived in Australia) so I have 60 odd years still to write about. But I diverge. In the process, I am scanning in a lot of relevant photos for inclusion in due course.



Do you remember the days of the instant photo? You had a special camera (left) and special film and after a lot of noise

the photo you just took is reproduced in

glorious colour. There is one problem. Years later, they

look a bit like that depicted right. Not quite what I wanted as a memory of my life; and, no doubt it would degenerate still further as time progressed. That



particular photo would be about 40 odd years old.



Using Paintshop Pro 2020, I was able to partly bring it back to the original as depicted left. It took a lot of fiddling and about half an hour to get to that. Why the strange dress — well, we were asked to dress in our most outlandish clothes to celebrate the opening of our neighbour across the road's new driveway (he is the one on the left).

It is no use me telling you the technical details because all photo editing programs are different, but in a nut shell it involved mainly brightness and colour modifications, very much on a trial and error basis.



Index

Subject	Issue	Page No.
Boot Process for Windows 10 Described	10/20	04
Brownpaddock's page	10/20	01
Edge in Windows 10 Cannot be Deleted (but see page 5)	10/20	08
Hacking Win 10 Themes can Remotely Control Your PC	10/20	09
Microsoft to Release Subscription-free Standalone Office	10/20	03
Photo Editing — Colour Correction	10/20	02
Uninstall Edge Browser Using PowerShell Command	10/20	05
Validating Windows 10 Product Key	10/20	06

Microsoft to Release Subscription-free Standalone Office

Microsoft has confirmed that a new standalone version of Microsoft Office will be released in the second half of 2021. Chances are that Microsoft will most likely call it **Office 2022**.



The successor to Microsoft Office 2016, Microsoft Office 2019 is the current version of the Office productivity suite. Microsoft made the Office 2019 generally available for Windows 10 and macOS operating systems on September 24, 2018.

Microsoft revealed its plans to release its next standalone version of Microsoft Office at Ignite. In its recent blog post, Microsoft wrote:

“Microsoft Office will also see a new perpetual release for both Windows and Mac, in the second half of 2021.”

Unlike [Microsoft 365](#), the Office 2019 productivity suite is not updated on a constant basis. Both Microsoft Office 2016 and Office 2019 will no longer be supported after 2025.

In addition to the standalone release of Office, Microsoft will also announce upcoming versions of Exchange Server, SharePoint Server, Skype for Business Server, and Project Server in the second half of 2021.

All these products will be accessible to subscribers with a valid subscription license. Subscribers can benefit from support, product updates, security, and time zone patches, among other things.

The next version of Exchange Server will be compatible with in-place upgrades from Exchange Server 2019 for at least two years after the release. It remains to be seen for how long the forthcoming Office will be supported.

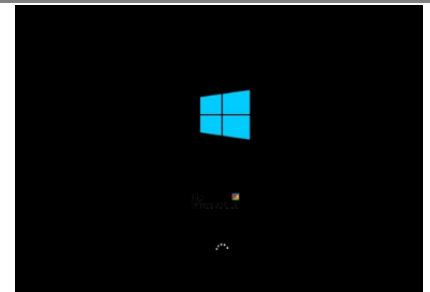
Microsoft has also advised that it will end the support for Office 2010 on PC and Office 2016 on Mac on October 13, this year. Both productivity suites will continue to remain accessible to users. However, after October 13, Microsoft's security updates and bug fixes for Office 2010 on PC and Office 2016 on Mac will cease to exist.

Microsoft will neither make any efforts to prevent Office 2010 and Office 2016 Mac users from accessing Office 365 online services nor enhance nor optimize the existing user experience.

It is early days to know what the new “Office 2021” will include, we shall just have to be patient and await Microsoft's relevant future bulletins.



Boot Process for Windows 10 Described



Have you ever wondered what happens when you push the power button on your computer? Here is how Windows 10 boots and all that goes on in the background. Whilst all we see is a single process, everything happens in steps. The boot process has been designed in such a fashion that if you face any issue with Windows 10 Boot, you will be able to troubleshoot it.

The Windows 10 boot process on BIOS systems comprises four major phases. It starts from the Power On Self-Test, or POST, and ends up loading the Windows OS Loader, the Kernel. This converts input/output requests from software into an instruction set for the Central Processing Unit, the CPU, and Graphics Processing Unit, the GPU. In simple words, it is a layer between the software and the hardware which makes everything possible. Here is a detailed description of the Windows 10 boot process and the list of stages it goes through:

1. PreBoot
2. Windows Boot Manager
3. Windows OS Loader.
4. Windows NT OS Kernel.

During every process, a program is loaded. Depending on whether it uses Legacy BIOS or UEFI*, the file paths and files change.

* *Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a computer's firmware to its operating system (OS). UEFI is expected to soon replace the BIOS.*

Phase	Boot Process	BIOS	UEFI
1	PreBoot	MBR/PBR (Bootstrap Code)	UEFI Firmware
2	Windows Boot Manager	%SystemDrive%\bootmgr	\EFI\Microsoft\Boot\fw.efi
3	Windows OS Loader	%SystemRoot%\system32\winload.exe	%SystemRoot%\system32\winload.efi
4	Windows NT OS Kernel	%SystemRoot%\system32\ntoskrnl.exe	

- 1] **PreBoot:** POST loads firmware settings, checks for a valid disk system, and if the system is good to go for the next phase. If the computer has a valid Master Boot Record (MBR), the boot process moves further and loads Windows Boot Manager.
- 2] **Windows Boot Manager:** This step determines if you have multiple OS installed on your computer. If yes, then it offers a menu with the names of the OSs. When you select the OS, it will load the right program, i.e., Winload.exe to boot you into the correct OS.

(continued on page 4)


(continued from page 3)

3] Windows OS Loader: Like its name, *WinLoad.exe* loads important drivers to kick start the Windows Kernel. The kernel uses the drivers to talk to the hardware and do the rest of the things required for the boot process to continue.

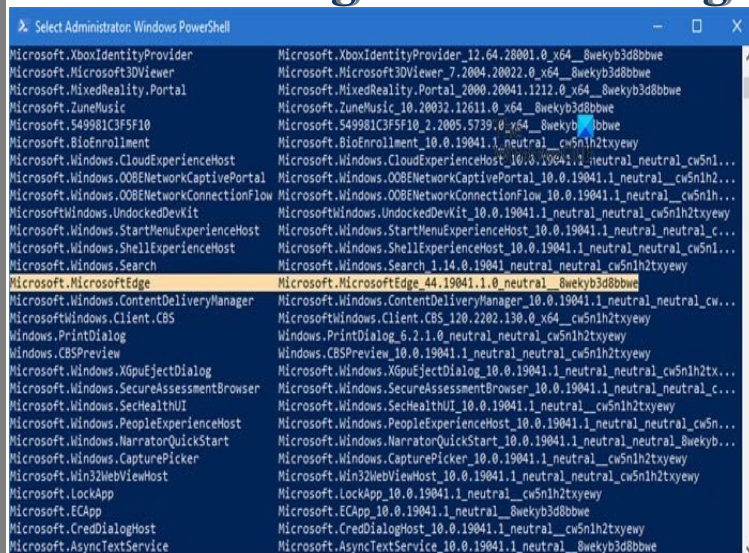
4] Windows NT OS Kernel: This is the last stage that picks up the Registry settings, additional drivers, etc. Once that has been read, control is taken by the system manager process. It loads up the User Interface (UI), the rest of the hardware and software. That is when you finally get to see your Windows 10 Login screen.

When you run Windows 10 on a computer that supports UEFI, Trusted Boot protects your computer from the moment you power it on. When the computer starts, it first finds the operating system bootloader. Computers without Secured Boot simply run whatever bootloader is on the PC's hard drive. When a computer equipped with UEFI starts, it first verifies that the firmware is digitally signed. If Secure Boot is enabled, the firmware examines the bootloader's digital signature to verify that it is intact hasn't been modified.

Lots of things happen even after you log in, but those are all post-boot process scenarios. There is much more to Windows 10 Boot process than explained here – the foregoing are only the basics!

Surprisingly, not too many users know the foregoing—it just happens! 

Uninstall Edge Browser Using PowerShell Command



```
Microsoft.XboxIdentityProvider 12.64.28001.0_x64_8wekyb3d8bbwe
Microsoft.Microsoft3DViewer 7.2004.28022.0_x64_8wekyb3d8bbwe
Microsoft.MixedReality.Portal 2000.28041.1212.0_x64_8wekyb3d8bbwe
Microsoft.ZuneMusic 10.20032.12611.0_x64_8wekyb3d8bbwe
Microsoft.549981C3F5F10 2.2005.5739.0_x64_8wekyb3d8bbwe
Microsoft.BioEnrollment 10.0.19041.1_neutral_cw5nh2txyewy
Microsoft.Windows.CloudExperienceHost 10.0.19041.1_neutral_neutral_cw5nh2txyewy
Microsoft.Windows.008ENetworkCaptivePortal 10.0.19041.1_neutral_cw5nh2txyewy
Microsoft.Windows.008ENetworkConnectionFlow 10.0.19041.1_neutral_cw5nh2txyewy
Microsoft.Windows.UndockedDevKit 10.0.19041.1_neutral_neutral_cw5nh2txyewy
Microsoft.Windows.StartMenuExperienceHost 10.0.19041.1_neutral_neutral_cw5nh2txyewy
Microsoft.Windows.ShellExperienceHost 10.0.19041.1_neutral_neutral_cw5nh2txyewy
Microsoft.Windows.Search 1.14.0.19041_neutral_neutral_cw5nh2txyewy
Microsoft.MicrosoftEdge 44.19041.1_neutral__8wekyb3d8bbwe
Microsoft.Windows.ContentDeliveryManager 10.0.19041.1_neutral_neutral_cw5nh2txyewy
Microsoft.Windows.Client.CBS 120.2202.130.0_x64_cw5nh2txyewy
Windows.PrintDialog 6.2.1.0_neutral_neutral_cw5nh2txyewy
Windows.CBSPreview 10.0.19041.1_neutral_neutral_cw5nh2txyewy
Microsoft.Windows.XGpuEffectDialog 10.0.19041.1_neutral_neutral_cw5nh2txyewy
Microsoft.Windows.SecureAssessmentBrowser 10.0.19041.1_neutral_neutral_cw5nh2txyewy
Microsoft.Windows.SecHealthUI 10.0.19041.1_neutral_cw5nh2txyewy
Microsoft.Windows.PeopleExperienceHost 10.0.19041.1_neutral_neutral_cw5nh2txyewy
Microsoft.Windows.NarratorQuickStart 10.0.19041.1_neutral_neutral_cw5nh2txyewy
Microsoft.Windows.CapturePicker 10.0.19041.1_neutral_cw5nh2txyewy
Microsoft.Windows.WebViewHost 10.0.19041.1_neutral_neutral_cw5nh2txyewy
Microsoft.LockApp 10.0.19041.1_neutral_cw5nh2txyewy
Microsoft.ECApp 10.0.19041.1_neutral__8wekyb3d8bbwe
Microsoft.CredDialogHost 10.0.19041.1_neutral_cw5nh2txyewy
Microsoft.AsyncTextService 10.0.19041.1_neutral__8wekyb3d8bbwe
```

You can use PowerShell Get package command to uninstall apps. Follow the steps as follows: Type PowerShell in the Run (Win+R) prompt and press the Enter key. Execute the following command: `Get-AppxPackage | Select Name, PackageFullName`

- Locate Microsoft Edge and its package name. It should be similar to what is mentioned below.

`Microsoft.MicrosoftEdge`
`Microsoft.MicrosoftEdge_44.18362.449.0_neutral__8wekyb3d8bbwe`

- On the list, locate Microsoft Edge and its package name. It should be similar to what is mentioned on the next page.

(continued on page 6)

(continued from page 5)

Now execute the following command to remove Edge from Windows.

```
Get-AppxPackage -allusers Microsoft.MicrosoftEdge_44.18362.449.0_neutral__8wekyb3d8bbwe | Remove-AppxPackage
```

Once the process is complete, it will uninstall Microsoft Edge from Windows for all the users. If you only want to uninstall for your account, you can skip the *-allusers* switch in the above command.

2] Using Command Prompt

Open an elevated CMD window. Copy and paste the following command and press Enter one by one: `cd C:\Program Files (x86)`

```
\Microsoft\Edge\Application\84.0.522.63\Installer  
setup.exe -uninstall -system-level -verbose-logging  
-force-uninstall
```

Here 84.0.522.63 should be the version number on your PC.

Make sure to remove all the browsing history from Microsoft online account if you do not wish to use it in the future.

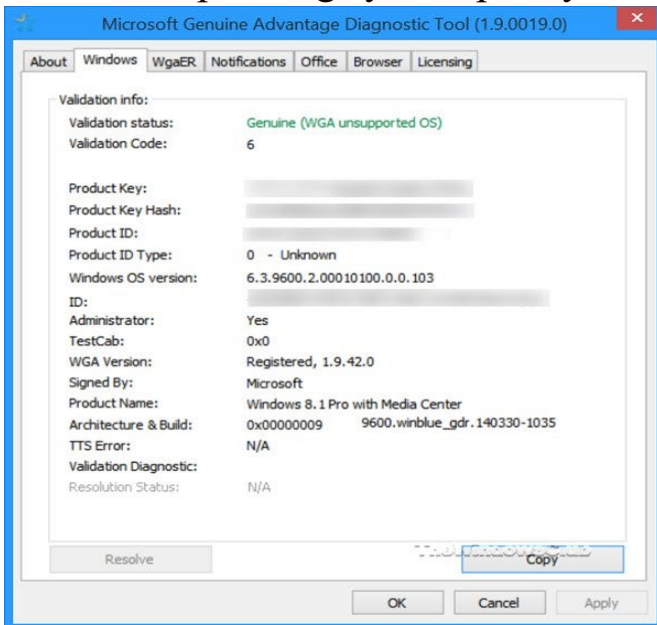


Validating Windows 10 Product Key

Sadly, software piracy is quite common among computer users these days. The Windows operating system is recorded as being illegally used by about 57% (that is more than half) of global users. In 2006, to combat the rate of Windows operating system piracy, Windows introduced Windows Genuine

Advantage.

Prior to Win 10, this feature checked your computer's product keys against thousands of blacklisted ones. If yours was found wanting, the effect would be an occasional change of your wall paper and background every hour. It would also add a notification on your background, to "Activate Windows". Until you use a genuine product key, your computer will be exempted from Windows updates.



Sometimes, users with genuine product keys may also encounter this warning. Some may decide to either remove the Windows Genuine Advantage after it has been installed or bypass the online validation. If you prefer to have the constant Windows check up to stay up-to-date or you wish to find out why your genuine Windows is giving you this error, the Microsoft Genuine Advantage Diagnostic Tool (MGADiag) is the way around. Running the tool

(continued on page 7)

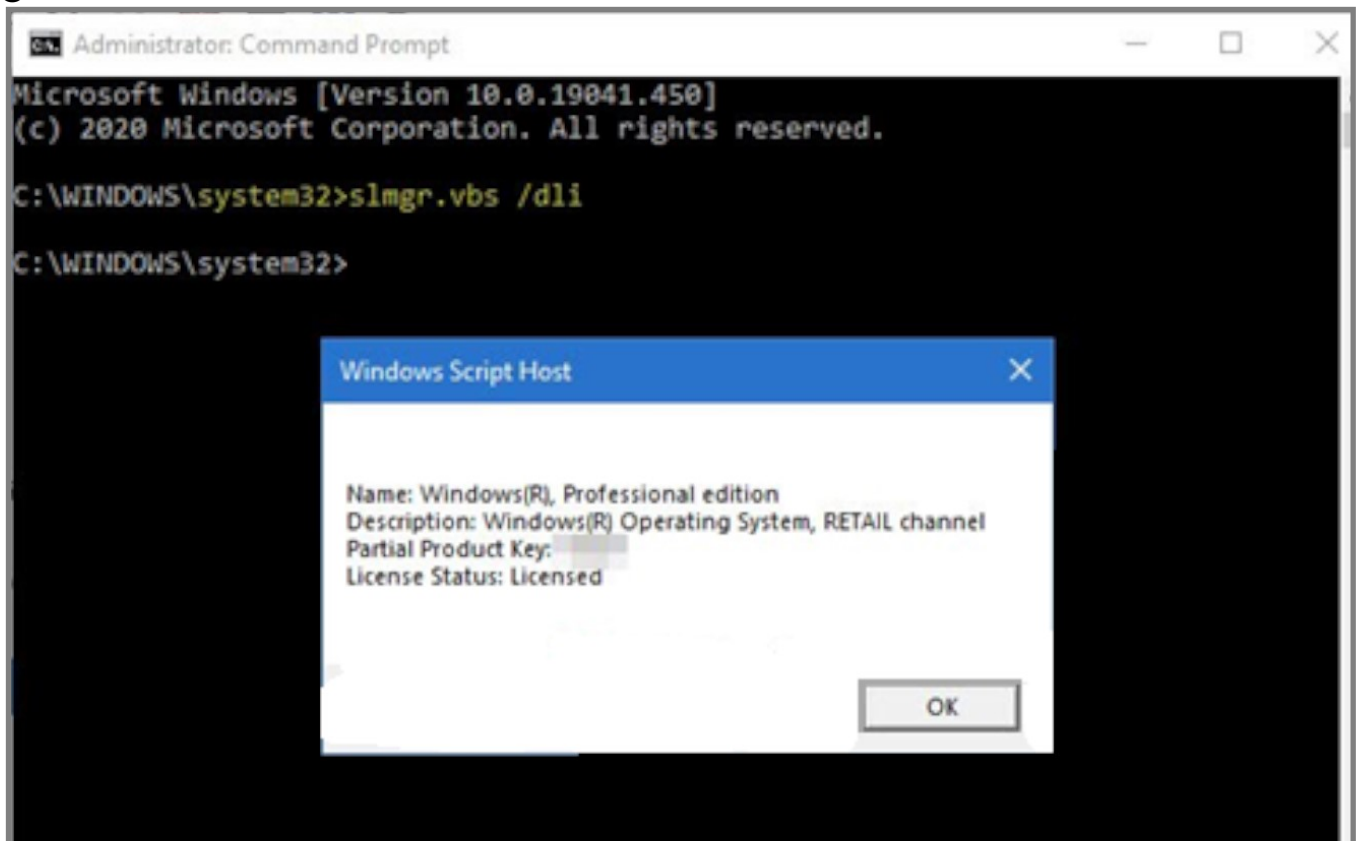
to do a check on your Windows System will give you various pieces of information or clues as to why parts of your system appear to be non-genuine *as reported by the Windows Genuine Advantage Tool*. It also helps in resolving a few issues and (with your permission) sending errors to Windows.

Many users tend to use the MGADiag to confirm if their machines are still in the Grace Period i.e. the amount of free time Microsoft gives illegal Windows users before it sanctions their computers. During this time, Microsoft believes that unlawful users would get hooked, change their minds, and purchase the genuine Windows version. As Bill Gates puts it,

“They’ll get addicted, and then we’ll collect”.

The tool, however, appears to have been deprecated now.

The reason people used MGADiag.exe was to find out if their Windows was genuine; however, it is not built to run on Windows 10



Validating a Windows 10 Product Key

To check if your Win 10 version is genuine, click the “**Win**” key plus the “**R**” key together. Type in “**slmgr.vbs /dli**” then press “**Enter**”. “slmgr” means *Software License Manager*, while “**.vbs**” means *Visual Basic Script*.

In the pop-up window, if you see “*Volume_*” “*activation expiration*” or any text in this line, you will know that your copy of Windows is cracked with an activator software and is not legal. 

Edge in Windows 10 Cannot be Deleted



Microsoft wants to make it absolutely clear that **Windows 10** users will not be able to uninstall the Edge browser, even if they want to. The Redmond-based company has provided the reason why it will not allow Windows 10 users to uninstall Edge from the operating system — Edge is the default web browser on Windows PCs and laptops.

Why Edge can't be uninstalled in Windows 10?

Microsoft will not allow Windows users to uninstall Edge because it will affect their access to the web platform. For instance, when you first install the Windows operating system, you need a web browser application to download other essential apps and software. Plus there are several applications in Windows 10 that require Edge to be installed. Edge has been fully integrated into the operating system — just like Internet Explorer was in earlier times. Microsoft explains. *“Microsoft Edge is the web browser recommended by Microsoft and is the default web browser for Windows. Because Windows supports applications that rely on the web platform, our default web browser is an essential component of our operating system and cannot be uninstalled.”*

Having a pre-installed browser on your system is a good thing since it saves a lot of time and you can connect to the Internet within seconds.

One can argue that Microsoft's logic behind forcing Edge on Windows 10 does not make much sense unless the motive behind doing so is increasing Edge's market share on desktop. Ironically, Microsoft further says: *“Microsoft Edge gives users full control over importing personal data from other browsers. In addition, Windows users can download and install other browsers and change their default browser at any time.”*

There are still ways you can change the default web browser on your PC.

Most recently, Edge has been highly active and competitive with regular updates, features, and performance improvements. It could be argued that Microsoft's Edge is trying hard to replace Google's Chrome a web browser application with the majority of global market share across platforms.



Why not register for

Be Connected

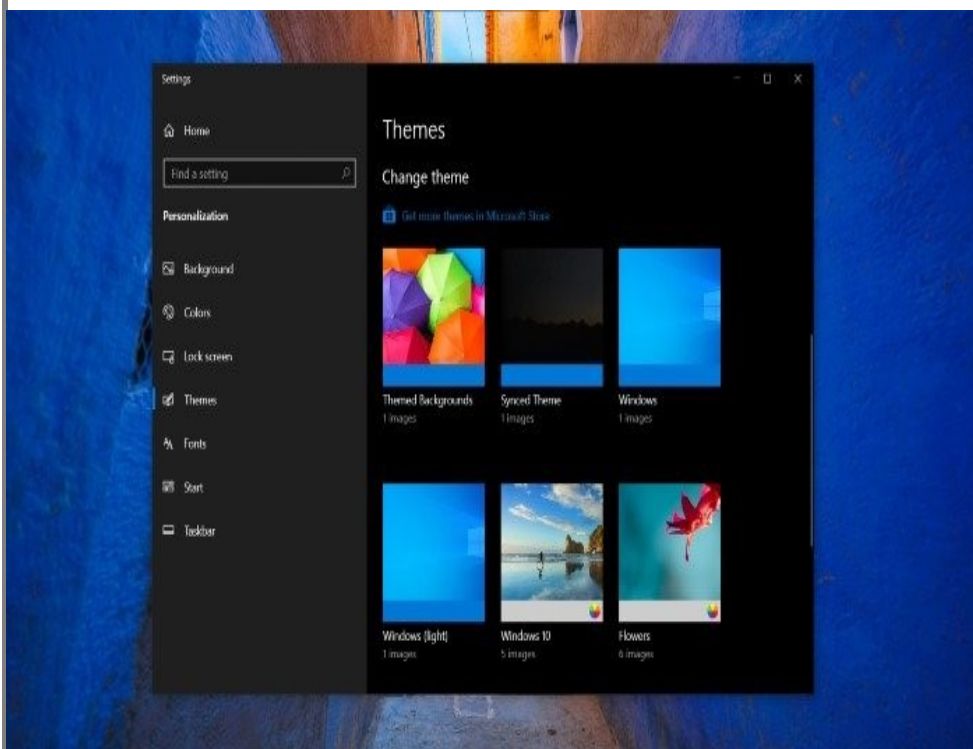
<https://beconnected.esafety.gov.au/>



Hacking Win10 Themes can Remotely Control Your PC

Who doesn't like to customize the default look and feel of their Windows 10 operating system? Windows 10 users can [personalize their computers](#) with a wide variety of [custom themes](#). But something they probably don't know yet is that a new sort of attack may be taking shape.

Windows 10 themes attack could be on the rise



Security researchers believe attackers can exploit Windows 10 themes to steal Windows account credentials, courtesy of “**Pass-the-hash**” attack. First, we must understand what this attack is all about.

Before we can understand the “*pass-the-hash*” attack,

we need to understand what the hash is. When a user logs onto a Windows PC and enters a username and password, the password is never sent over the network. Instead, a hash is derived from the password.

Interestingly, a password hash can uniquely represent the actual plain-text password that can not be mathematically reversed. It also can not reveal what the password is. This hash is known as the Windows NT LAN Manager or NTLM hash.

Windows account credentials and NTLM hash are stored in memory that is managed by a process called Local Security Authority Subsystem Service (LSASS.exe), which allows for a single sign-on, such as when the user needs to access other resources on the network.

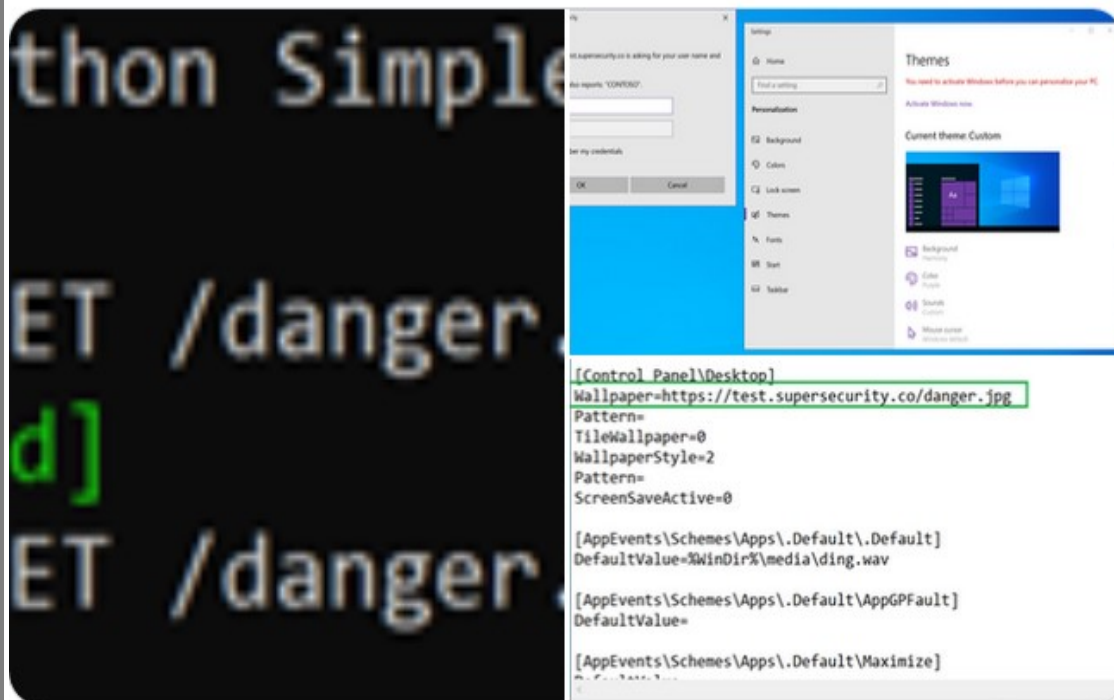
In the “pass-the-hash” attack, attackers can authenticate to a remote server or service by using the underlying NTLM hash of a Windows 10 user's password for authentication and potentially Lateral Movement technique to control Remote Desktop Protocol or RDP servers.

Coming back to attackers potentially abusing Windows 10 themes, a security researcher (@bophos) has revealed how custom themes can help threat actors steal Windows passwords.

(continued on page 10)

The Credential Harvesting Trick

Using a Windows theme file, the Wallpaper key can be configured to point to a remote authority-required http/s resource. When a user activates the theme file (e.g. opens it from a link/attachment), a Windows credibility prompt is displayed to the user.



“Pass-the-Hash” attacks are successful when attackers trick their victims into accessing a Web Distributed Authoring and

Versioning (WebDAV)) or Server Message Block (SMB) location requiring authentication. In a Windows theme file, the wallpaper key can be configured to point to a remote authentication-required HTTP/HTTPS resource.

That “The default handler” loads the “Themes setting dialogue” was discovered a while back, and was reported to the Microsoft Security Resource Centre earlier this year when similar “disclosure” bugs were discovered and patched. This was not patched b/c this is a “feature by design”

“From a defensive perspective, block/re-associate/hunt for “theme”, “themepack”, “desktopthemepackfile” extensions. In browsers, users should be presented with a check before opening. Other CVE vulns have been disclosed in recent years, so it is worth addressing and mitigating”

When a user activates the theme file, a Windows credential prompt is displayed to the user. The wallpaper key is located under the “Control Panel Desktop” section of the .theme file. This technique can help attackers disclose NTLM hash when the key is set to a remote location.

You must set up multi-factor authentication on your Microsoft accounts. Hence, even if the attacker has managed to steal your Windows credentials, your Microsoft account can not be remotely accessed.





At our last member's meeting, I asked a few members what computer platform they were using. Very few were using Windows 10. That makes me wonder how many members actually get anything out of our monthly magazine in which most of my articles relate to that system. I am a firm believer that I

should have tried out any new programs I write about. The downside of that is most relate specifically to Windows 10 or, at least, how Win10 handles them.

It would seem that most members are using either Win 8 or 8.1; a couple are still using Win Vista or Win XP. Now that is getting pretty old but, if that is what suits your needs, then so be it.

Rightly or wrongly, my copy of Win10 is right up to date. I tend to use the Quick Action Tool Bar quite a lot and having just taken delivery of a brand new computer built to my specifications, I needed to adjust Office to the way I like to work. WOW! The "All Commands" option in the Word QAT Bar have increased dramatically; I would guess — almost doubled.

I will try to find something regarding those earlier Windows versions.



Jest a Minute



THIS ~ MONTH's Topic ~
“ANNUAL GENERAL MEETING”
CHAIR: JIM GREENFIELD

— For Your Notes —

Our November Members' Meeting

Cameron Rawlings will join us to ask the question:

“To Use or Not to Use Master Passwords?”

There are advantages of using a master password but also
a possible pit fall or two.



MEETING RULES

We are allowed to use the facilities at the Hall at the rear of St Mary's Catholic Church, on the corner of Bains and Main South Roads, Morphet Vale in return for a small fee plus respect for their property. We ask for your co-operation in respect to the above.

Whilst we have no control over what our members do away from our Club meetings, piracy of copyright material cannot be condoned at our meetings. Please respect copyright laws at all times.



Disclaimer: The information herein is of a general nature. Always do your own research and seek advice before proceeding on information you don't understand.

IT & COMPUTERS

Shop 6, 76 Beach Road
Christies Beach 8186 2736

(Same block as Woolies on Beach Road)

Contact: Jamle or Ash

For all your computing needs
available locally

Need help with your computer?
Looking to purchase a new one?
Need additional peripherals?
Home site visits available !

Looking for excellent customer
and after sales service?

New Computers

Repairs

Virus removal

New software & Upgrades

Peripheral units:

Wireless Keyboard Mouse

Sound Boards & Systems

External & Internal Hard Drives



Tell IT & Computers
you are from
S.D.C.U.C.I.

S.D.C.U.C.I can
recommend the
customer service
offered by
IT&Computers