COMPUTER NEWS from the

Titusville Computer Community

TCC

Titusville, FL

MARCH 2020 Volume 8 NO.3

As found on the web and other sources!

.

Something to look forward too.

Windows 10 Start Menu to be Redesigned

By John Lister on February, 25 2020 in “Infopackets.com”.

Microsoft is reportedly set to ditch "live tiles" from Windows 10. It's part of a planned revamp of the system's Start Menu.

Live tiles originally debuted in Windows Phone 7 and there's a strong argument it's a feature that should have been left to mobile devices. The tile is a square display that shows a specific piece of information such as current weather or a stock price, updated in real time rather than the user having to click on it.

Live Tiles Driven By Mobile

The feature debuted on the PC desktop with Windows 8, which was widely criticized for being designed more for touch screen devices than the traditional mouse and keyboard setup.

In Windows 10 they appear by default in the Start menu, to the right of the more familiar list of options and links to programs. They contain information from Windows apps, the programs that install from the Microsoft store like mobile device apps, rather than the more traditional method of directly installing a program.

Since Microsoft has largely abandoned mobile devices, it's seemingly given up on live tiles and stopped updating the ones powered by its own apps. While tiles for third party apps still have updates, it's questionable how many people find their benefit outweighs the clutter and disruption that the tiles bring.

Start Menu to Get Revamp

Now inside sources report Microsoft will ditch the live tiles in an update later this year or in early 2021 and replace them with static icons. Its part of a revamp of the entire Windows 10 user interface which has already started with some users getting new versions of familiar icons. (Source: windowslatest.com)

In the long run the Start menu is likely to resemble that in Windows 10X, a version of Windows made specifically for foldable devices that can switch between a traditional laptop and a touch screen tablet mode. However, the Windows 10 version will have some differences to reflect the particular needs of desktop users. (Source: techradar.com)

What's Your Opinion?

Do you actively use live tiles in Windows 10? Would you be happy to see them go? What else, if anything, would you change about the Windows 10?

How to Fix: Can't Start Malwarebytes Installer Service

By Dennis Faas on March, 13 2020 in “Infopackets.com”.

Infopackets Reader Marlene T. writes:

“Dear Dennis,

My Windows 10 computer recently upgraded and my desktop icons have gone missing. On top of that, Malwarebytes Antimalware no longer works. When I try to launch Malwarebytes Antimalware, **it freezes at the Malwarebytes logo** and does not progress. I've tried to uninstall Malwarebytes Antimalware but it tells me that it **can't start the malwarebytes installer service**. I'm completely lost! I need your help! "

My response:

I asked Marlene if she would like me to connect to her machine using my remote desktop support service and she agreed.

Below I will discuss my findings.

Related:

- How to Fix: Malwarebytes 'Unable to connect to service' Error
- How to Fix: Malwarebytes MBAMService.exe High CPU Usage

How to Fix: Can't Start Malwarebytes Installer Service

Usually whenever a program stops working or won't launch, the first thing I try is to uninstall the program and reinstall it. If the uninstall doesn't work, reinstalling the program over top of itself usually fixes it.

In this case, it seems that Malwarebytes Antimalware has its own type of installer service, which is also used for uninstalling the program. I suspect it's made this way to prevent other malicious programs from automatically uninstalling its service, and thus infecting the machine. Unfortunately, uninstalling or reinstalling Malwarebytes Antimalware did not fix this issue.

After a bit of research I discovered that there is a Malwarebytes cleaning tool called "**MB Clean**" which is available from the Malwarebytes website. Essentially this program removes all traces of Malwarebytes Antimalware from the system, including registry entries and files. In turn this fixes the broken Malwarebytes Installer Service.

It should be noted that most antivirus programs including McAfee, Kaspersky, and Avast (and others) offer similar tools to completely remove their products from the system, should something go awry and the uninstall / reinstall method does not work.

For the record, the MB Clean program worked successfully and I was able to reinstall Malwarebytes Antimalware on Marlene's PC. When I launched the program, it started up right away.

You can download the MB Clean tool here:

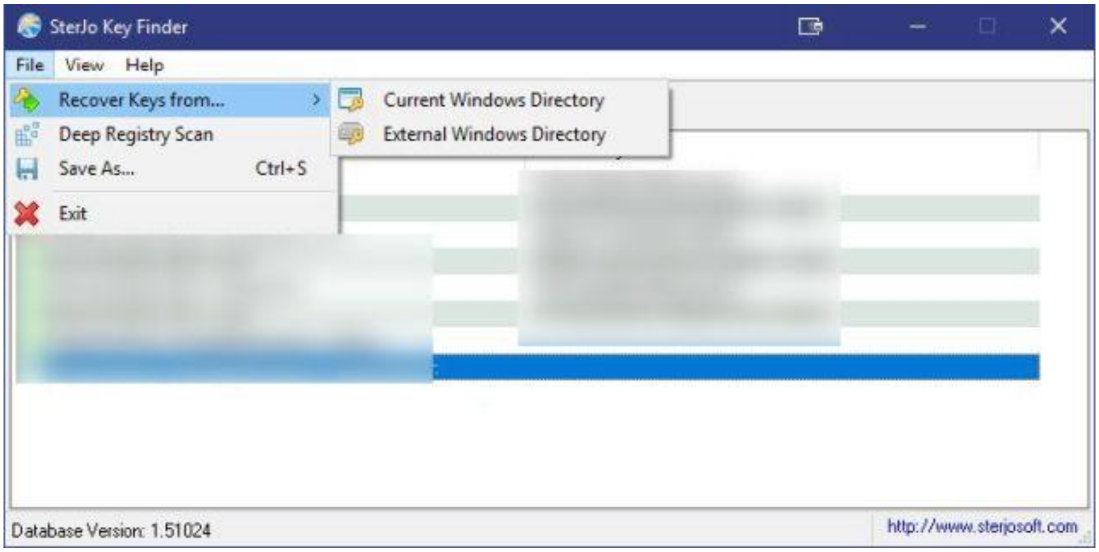
https://downloads.malwarebytes.com/file/mb_clean

Problem solved!

I've lost my product key! Now what shall I do?

Recover Product Keys From Your PC With This Free App

Posted: 11 Mar 2020 on "Gizmo's freeware.com".


SterJo Key Finder
File
View
Help
Recover Keys from...
Deep Registry Scan
Save As...
Ctrl+S
Exit
Current Windows Directory
External Windows Directory
Database Version: 1.51024
http://www.sterjosoft.com

This program quickly scans your PC and finds product keys, serial numbers and registration details for Windows and a large variety of additional software and games. It will scan and display registration information for most Windows versions, most Office versions (Microsoft Office 2013, Office 2010, Office 2007, Office 2003, Office XP, Microsoft Money, Microsoft Works) and programs like Dragon, AutoCAD, Adobe, ACDSee, Corel, O & O, EA and PopCap games, VMWare and more.

SteroJo Key Finder is very easy to use. Download, install and run the program and one click displays all the licenses on your Windows computer. You can copy all the license keys or individual keys and save them as a text file. There are options to recover keys from current or external Windows directories or do a Deep Registry Scan.

Note: since SterJo Key Finder scans your registry to locate registration keys (similar activity to some malware), some anti-virus programs may flag the program as unsafe and some anti-virus programs may identify the authors site as having a PUP or other issue. Double check the result of your anti-virus programs results with other programs or online services, it's not unusual for anti-virus programs to report false positives and some anti-virus programs generate more false positives than others.

SterJo Key Finder runs on Windows 10 32/64 bit, Windows Server 2003, Windows Server 2008, Windows 8 32/64 bit, Windows 7 32/64 bit, Windows Vista 32/64 bit, and Windows XP. There's an installable and a portable version. The installable version is free of malware according to VirusTotal. The installable version has an ad during installation offering the option to download other software - uncheck the box if you aren't interested in the software. ***Read More***

Unsafe VPN Android Apps Threaten Privacy

By John Lister on March, 3 2020 in "Infopackets.com".

Some of the most popular VPN apps for Android are dangerous to use, according to a leading review site. The VPN apps, which are supposed to protect privacy, actually expose users to attacks according to VPN Pro.

A VPN, or virtual private network, is meant to be a way to boost privacy online. It works by re-routing traffic through a middle-man server to make it appear that your IP is in another location. When configured properly, the VPN effectively creates a secure online connection that means even though data is going through the Internet, it can't be read by anyone other than the sender and intended recipient - but there are some major caveats to that and this is only true if the sites and services you're using are all using HTTPS.

Many desktop users use VPNs as a way to disguise their location - for example when accessing sites which block certain users from certain areas, or offer different content such as Netflix.ca and Netflix.com. Others use VPNs as a way to evade monitoring by hostile governments. On mobile devices, however, VPNs are most commonly promoted as a form of "protection" when using public WiFi networks. (Source: norton.com)

Related:

- Explained: Do I need a VPN on a Public Network?
- Explained: VPN vs Proxy; What's the Difference?
- Explained: Do I need a VPN? Are VPNs Safe for Online Banking?

Rogue App Has 100 Million Downloads

VPN Pro says it has found 10 popular Android apps which have critical security bugs. The most popular is SuperVPN Free VPN Client, with 100 million installations from the Google Play store. (Source: vpnpro.com)

Others include:

- TapVPN Free VPN (10 million downloads)
- Best Ultimate VPN - Fast Secure Unlimited VPN (5 million downloads)
- Korea VPN - Plugin for OpenVPN (1 million downloads)
- VPN Unblocker Free unlimited Best Anonymous Secure (1 million downloads)
- Super VPN 2019 USA - Free VPN, Unlock Proxy VPN (50,000 downloads)

The list also includes four apps which have recently been removed from the Google Play store , but may still be widely used:

- Wuma VPN-Pro (Fast & Unlimited & Security)
- VPN Download: Top, Quick & Unblock Sites
- Secure VPN-Fast VPN Free & Unlimited VPN
- Power VPN Free VPN

Man-In-The-Middle Is Malicious

Most of the security problems were similar to that rather spectacular one in SuperVPN. Although it claims to transmit encrypted data, it does so with the decryption key easily readable, which means that the encrypted data can be decrypted.

This effectively allows for a "man-in-the-middle" attack, which in simple terms means an attacker can intercept and redirect data from a VPN to a fake website or service that looks like the intended destination. The attacker will then be able to view all the data being sent to and from the user in a completely stealth manner.

VPN Pro says it can't be certain whether the vulnerabilities are deliberate with the app developers trying to access private data, or if they are just badly designed. However, it does suspect some of the developers have manipulated the Google Play rankings algorithms.

According to VPN Pro, anyone thinking of getting a VPN app should check who is actually behind it, where it's based, and what permissions the app asks for.

What's Your Opinion?

Do you use a VPN? If so, how did you vet it to make sure it was legit? Is it simply too risky to trust free software?

Your Smart House May Be Too Smart!

Flaw in Philips Smart Light Bulbs Exposes Your WiFi Network to Hackers

□February 05, 2020□Mohit Kumar IN “THE HACKER NEWS”.

There are over a hundred potential ways hackers can ruin your life by having access to your WiFi network that's also connected to your computers, smartphones, and other smart devices.

Whether it's about exploiting operating system and software vulnerabilities or manipulating network traffic, every attack relies on the reachability between an attacker and the targeted devices.

In recent years, we have seen how hundreds of widely used smart-but-insecure devices made it easier for remote attackers to sneak into connected networks without breaking WiFi passwords.

In the latest research shared with The Hacker News, Check Point experts today revealed a new high-severity vulnerability affecting **Philips Hue Smart Light Bulbs** that can be exploited over-the-air from over 100 meters away to gain entry into a targeted WiFi network.

The underlying high-severity vulnerability, tracked as **CVE-2020-6007**, resides in the way Philips implemented the Zigbee communication protocol in its smart light bulb, leading to a heap-based buffer overflow issue.

ZigBee is a widely used wireless technology designed to let each device communicate with any other device on the network. The protocol has been built into tens of millions of devices worldwide, including Amazon Echo, Samsung SmartThings, Belkin Emo and more.

"Through this exploitation, a threat actor can infiltrate a home or office's computer network over-the-air, spreading ransomware or spyware, by using nothing but a laptop and an antenna from over 100 meters," the Check Point researchers told The Hacker News.

Check Point also confirmed that the buffer overflow happens on a component called the "bridge" that accepts remote commands sent to the bulb over Zigbee protocol from other devices like a mobile app or Alexa home assistant.

How Does Philips Smart Bulbs Vulnerability Work?

Though researchers choose not to reveal complete technical details or PoC exploit for the flaw at this moment to give affected users enough time to apply patches, they did share a video demonstrating the attack.

As shown in the video, the attack scenario involves:

1. By exploiting a previously discovered bug, an attacker first takes control over the smart bulb.
2. This makes the device 'Unreachable' in the users' control app, tricking them into resetting the bulb and then instructing the control bridge to re-discover the bulb.
3. The bridge discovers the hacker-controlled bulb with updated firmware, and the user adds it back onto their network.
4. The hacker then exploits the ZigBee protocol vulnerabilities to trigger a heap-based buffer overflow on the control bridge, allowing him to install malware on the bridge that's connected to the targeted network.
5. The hacker can use malware to infiltrate the network, eventually leaving millions of other devices connected to the same network at risk of remote hacking.

"Many of us are aware that IoT devices can pose a security risk, but this research shows how even the most mundane, seemingly 'dumb' devices such as lightbulbs can be exploited by hackers and used to take over networks, or plant malware," Yaniv Balmas, Head of Cyber Research at Check Point Research, told The Hacker News.

Check Point responsibly reported these vulnerabilities to Philips and Signify, owner of the Philips Hue brand, in November 2019, who just last month released an updated, patched firmware for the device.

"It's critical that organizations and individuals protect themselves against these possible attacks by updating their devices with the latest patches and separating them from other machines on their networks, to limit the possible spread of malware. In today's complex cyberattack landscape, we cannot afford to overlook the security of anything that is connected to our networks."

If automatic firmware update download feature is not enabled, affected users are recommended to manually install patches and change settings to revive future updates automatically.
Have something to say about this article? Comment below or share it with us on Facebook, Twitter or our LinkedIn Group.

Do You Know Someone Like This?

She's always late. Her ancestors arrived on the Juneflower.
