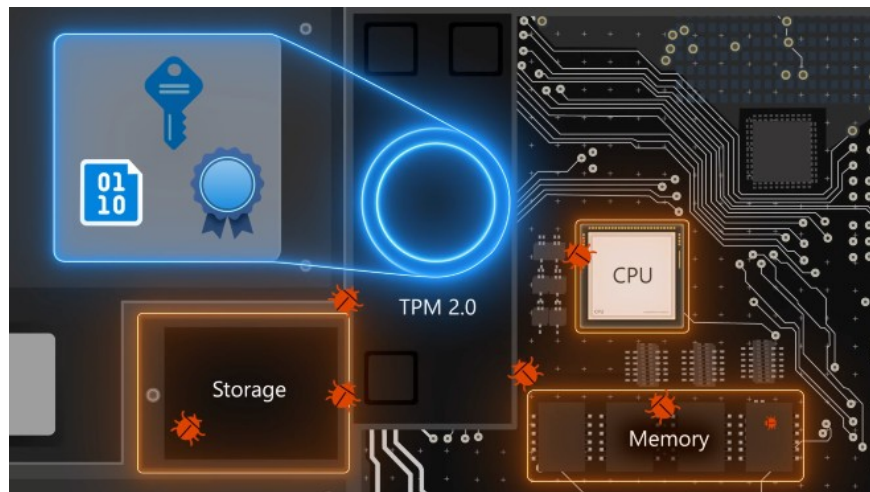


Microsoft proves Windows 10 computers are vulnerable to hacking to advertise Windows 11

Microsoft's newly released Windows 11 is integrated with many security features such as Trusted Platform Module (TPM 2.0), Virtualization-based Security (VBS)... Although these features are available on Windows 10, they are not implemented by default as on Windows 11.

To promote the security of Windows 11, Microsoft invited David Weston, Partner Manager for Enterprise and Operating System Security at Microsoft, to hack straight into Windows 10.

Weston has attacked Windows 10 computers in different ways. Next, he explains why features like TPM 2.0 and VBS are so important in ensuring a safe experience for Windows 11 users.



Playing a hacker, Weston gained control of a device by both remote and direct attacks. He can then steal the victim's data or lock the device for ransom.

At the beginning of the video Weston exploits the Remote Desktop Protocol (RDP) port to gain administrator access. This attack is performed remotely based on the exposed IP of the victim. Once infiltrated, Weston was able to install ransomware on a Windows 10 computer that did not have TPM and Secure Boot enabled.

Weston then bypasses the fingerprint authentication system on a Windows 10 computer that doesn't support VBS. Using a PCILeech, Weston accesses the victim's computer's memory and modifies the biometric code. This allows him to pass the fingerprint check system with ease.

Please see the details of Weston's process of hacking and attacking Windows 10 through the video below:

Once again, I would like to remind you that Microsoft has publicly "drowned" Windows 10 to advertise Windows 11.

You finished reading the article "**Microsoft proves Windows 10 computers are vulnerable to hacking to advertise Windows 11**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
