Keeping encryption secure from BitLocker sniffing

DUBAI, UNITED ARAB EMIRATES, February 28, 2024 /EINPresswire.com/ -- Márk Szabó, PR and Security Writer, ESET explains that recently, the YouTube channel stacksmashing uploaded a video on breaking the built-in encryption in Windows, essentially bypassing Windows Disk Encryption on most devices using Microsoft's globally dominant operating system with a cheap $10 tool.

This all in just 43 seconds – record time. And while encryption has often been the poster child for efficient and secure data protection, now it seems like encryption, too, has its holes, despite relying on advanced features such as Trusted Platform Modules (TPM), which are now also required by the newest Windows OS.

But can this security hole be properly navigated? Thankfully, the solution is relatively easy and also does not cost as much as a full data breach would.

Exploring BitLocker sniffing

The method bypassing encryption has been dubbed “BitLocker sniffing,” named after the built-in Windows encryption tool BitLocker. Essentially, data from the TPM is exposed on the bus, and if anything is using the TPM, one can then “sniff” out the data that gets exposed on the bus at some point during the de-encryption process. This can happen on older machines, specifically those whose TPM is not integrated into the CPU.

The exploit on BitLocker relies on the fact that it is not using a password or any other secondary authentication method alongside the TPM. In the case presented in the video, the PC boots automatically with only the TPM providing access to the Disk Encryption Key (also known as Volume Master Key – VMK). While switching on the machine, the BitLocker automatically uses the TPM to decrypt the VMK and boots to Windows login almost immediately. So, the VMK is available in the plain on the bus as the system is booting up.

Simply put, the communication between the TPM and the computer's processor is exposed during startup, meaning that the encryption key can be read by someone snooping on the signal between the TPM and the CPU, which can be done with a cheap tool and some firmware.

This might remind someone familiar with cybersecurity of how in some cases man-in-the-middle attacks can "eavesdrop" on a person's internet connection/Bluetooth/RFID signal while trying to connect to somewhere or something. This occurs because the data stream can become exposed while traveling to a receiver, unless there's some form of additional security involved, like using a VPN while connected to public Wi-Fi, ensuring a protected hidden connection. Basically, adding another security layer on top is required to mask the data transfer.

Is encryption not enough?

This new piece of research is very interesting, especially since using a TPM security module or chip is now a requirement of the Windows 11 OS, which is why many older processors that might not have satisfied the requirement were barred from having the eligibility to install the OS.

The issue is not whether encryption is enough of an incentive for someone to want the newest OS features, but the fact that, so far, it's always been a signal of added security. However, with BitLocker sniffing, it seems like encryption might be just another redundant security function…or is it?

Truthfully, encryption is a necessary – no, a compulsory – security measure for any user that has to ensure their data remains safe and securely stored, limiting potential access opportunities even after a device gets stolen. What's more, as an added security layer, it makes activities that much harder for crooks, as it delays their potential breach time, giving more time to security responders.

Every company security strategy has to include encryption, as this is also required for regulatory compliance and cyber insurance, where the trend sees compulsory standards raised every year.

To answer the headline then: No, encryption is not enough, as multiple security layers are needed for any strategy to work against malicious threats, but it is a necessary component; businesses must include it for better protection. However, encryption does not need to be as it is, a singular security layer, and there are ways to protect it even against BitLocker sniffing.

It's all about the layers

Was it Shrek who described how ogres are layered like onions? Well, like ogres, successful cybersecurity apps and measures are layered too. At ESET, the PROTECT Platform is one example of that, since in and of itself, it contains multiple layers of technologies that protect against threats, be they zero-days that have never seen the light of day or known malware trying its best to avoid detection with newer evasion techniques.

As such, ESET can also guarantee better encryption thanks to a simple thing – a password. It might seem like a simple layer, but it is very powerful, as thanks to its inclusion within ESET Full Disk Encryption (EFDE) and ESET Endpoint Encryption (EEE), it protects against techniques such as BitLocker sniffing, as that technique relies on unprotected communication between a discrete TPM chip and a CPU. Thus, any secondary authentication that happens before the process starts prevents the encryption key from being out in the open.

In normal operation with EFDE and EEE, the user is required to enter their password upon booting up their computer. Essentially, the password is used in conjunction with other data and the TPM encryption to decrypt the VMK. So, without the user's password, the correct VMK cannot be obtained. Yes, at some point the data decrypted by the TPM will be available in the plain; however, this cannot take place without knowing the user's password first.

Powerful encryption, secure systems
In the end, cybersecurity will always need to keep evolving, just as threats do. However, sometimes simple security measures can demonstrate quite an impact.

Passwords have always been the first line of defense against external compromise (as gaining access to a single account can cause a chain reaction), and this will probably continue into the future.

However, a reminder needs to be said – never pick weak passwords, never reuse a single password across all accounts or encryption, and in general, be mindful of cybersecurity. And for businesses in general, consider what level of security is required – as just a single product, or a single additional measure like a strong password for once encryption, can make a difference.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here