The Linux subsystem on Windows 10 allows malware to hide without being detected

Microsoft has shown how favorably Linux has been for nearly three years and this love ultimately cost them.

Last year, Microsoft surprised everyone by announcing the launch of Windows Subsystem for Linux (WSL) on Windows 10, allowing the Shell command line to be put on Linux on Windows so users could run native Linux applications right on. Windows without using virtualization tools.

However, Check Point Software Technologies researchers have discovered security issues with WSL, which may allow malware designed for Linux to target Windows computers without being detected by security software. .

Researchers have created a new attack technique called Bashware that takes advantage of the WSL feature on Windows, which is now in beta and ready to be available on Windows 10 Fall Creators Update in October this year.

Bashware cannot be detected by security software

According to researchers at Check Point, Bashware may be abused by malware on Linux because Windows security tools are unable to detect this threat.

This new type of attack allows an attacker to hide the Linux malware from all security tools, including the latest software, malware detection, virus removal, extortion codes .

The reason given is that current security software for Windows is not designed to manage Linux execution processes on Windows OS. 'Existing security tools have yet to adapt to the Linux execution process running on Windows, a hybrid concept that allows Linux and Windows to run concurrently.' 'This could open the door for an attacker to run malicious code and use the functionality provided by WSL to hide themselves from security tools.'

Who is a sinner? Microsoft or security solutions?

To run Linux applications in a standalone environment, Microsoft introduced Pico Processes - a container that allows running binary ELF on Windows. During the test run, researchers can experiment with Bashware attack on 'most existing antivirus and security products' and successfully overcome them.

That's because no software monitors the Pico process, even if Microsoft has provided Pico API, a special application programming interface used by security companies to monitor such processes.

'Bashware does not use any logic or executable errors in WSL. In fact, WSL seems to be very well designed. ' 'What allows Bashware to work is because companies that provide security software are not aware because this technology is quite new.'

Bashware attacks require admin rights, is it more difficult on a PC?

Bashware requires administrative rights to access the target machine, but it is not difficult to capture administrative rights on Windows PC through phishing attacks or theft of login information.

However, these types of attacks are easily detected by security software, causing them to be blocked before Bashware can attack.

Since WSL is not turned off by default, users must turn on 'Development Mode' on their device to use it, the risk is also reduced somewhat.

Current security software cannot detect Bashware

However, researchers at Check Point also said that there is a little known fact that the developer mode can be turned on by editing some Registry Keys, which can be done silently in the background when The attacker has the right.

Bashware attack technique automates the necessary process by silently downloading WSL elements, enabling developer mode, and even downloading and extracting Linux system files from Windows servers and running malware .

No need to write separate malware

The interesting thing about Bashware is that hackers don't need to write their own malicious software for Linux to run through WSL on a Windows machine. That's because Bashware installs software called Wine inside the downloaded Ubuntu environment, then runs the Windows malicious code over it. This malicious code will then launch in Windows as a Pico process, so security software cannot be detected.

400 million computers have potential before Bashware threat

New attack techniques do not use any WSL vulnerabilities because security products do not pay attention to WSL. Because Shell Linux is available on Windows, there may be up to 400 million PCs running Windows affected. Check Point said that its software has been upgraded to combat this type of attack and recommends that other software be updated quickly.