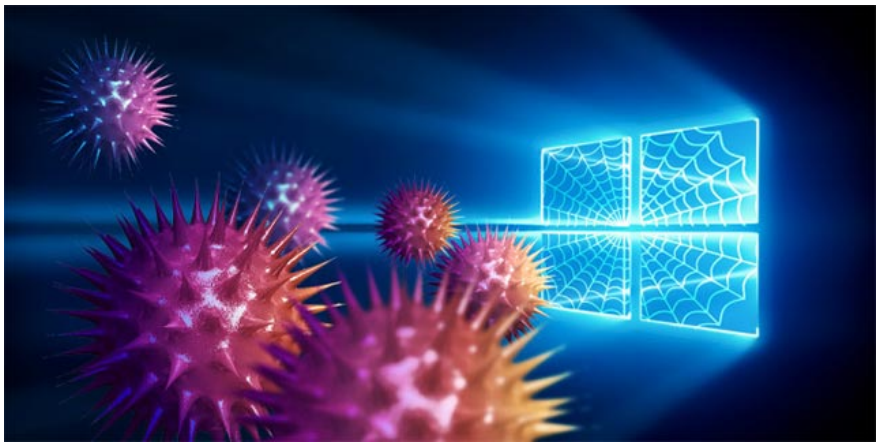
Windows, Android and security intelligence issues

With 4.312 billion users worldwide, ie equivalent to about 55.6% of the global population, the Internet has been and will become a daily 'living space' for most events and activities. human.

With 4.312 billion users worldwide, ie equivalent to about 55.6% of the global population, the Internet has been and will become a daily 'living space' for most events and activities. human. Such activities may be aimed at entertainment, sharing information, transactions, remote computing, communication and many other modern aspects of lifestyle in the 21st century. Besides the popularity of the Internet It is impossible not to mention a very important factor, which is the operating system. According to Statcorer statistics completed in February 2019, among hundreds of operating systems in use worldwide, Android and Windows are the two names with the largest market share with 36.5% and 35.99% respectively. . Meanwhile, these two platforms are also said to possess a lot of serious security holes. That means that 72.49% of computing devices (including smartphones, tablets, laptops, PCs . are generally devices that use the operating system) both by individual users Organizations and businesses are daily accessing the Internet on platforms containing vulnerabilities that are vulnerable to malware attacks.



1. The unsafe 'feature' on UC Browser allows hackers to take control of Android phones remotely

We all know that Windows (formerly MS-DOS) is the preferred target of malware since it was launched as early as the 80s, while Android has also become a 'male ingot'. magnet 'attracting malware (far beyond iOS) since the smartphone market boomed and smartphones became indispensable devices in the lives of billions of people. This is where the responsibilities of both Microsoft (windows) and Google (Android) - the companies responsible for these two operating systems - are verified, especially in the context that these two platforms seem to have moved. The direction becomes an online service, instead of a typical operating system that we used to be familiar with like a Linux desktop. And so the term Threat Intelligence appears, in the context that both companies are still trying to continue to evaluate and improve their operating systems to face the threat. The growing threat of attacks threatens cyber security, abuse and becomes the target of malware authors.

1. What is cybercrime? How to prevent cybercrime?

Both of these operating systems seem to be entering a development phase where security issues are often entrusted more to third parties, the professional anti-virus software vendors are full. But equally 'cunning'. In the first time when these two operating systems have not diverted much to Internet services, both Microsoft and Google seem to be uninterested in studying the intelligence capabilities of security threats to ensure safety. Their operating system as they go beyond the normal development cycle.

This of course changed, because Windows is now equipped with built-in antivirus software by default called Defender, maintained by Microsoft itself through Windows Automatic Updates. The same approach has been taken by Google, as they integrate Google Play Protect as part of the Google Play Store platform. This tool will be directly connected to Google's cloud platform, so updates will be implemented in real time.

1. If using an Android phone, be careful: You may be being tracked without knowing

Microsoft and Google are doing this so that users (and their partner companies / companies) do not need to implement expensive Threat Intelligence processes to secure their own devices. An active approach to security issues will become even more powerful if implemented by code-controlled developers, including operating systems and all system functions. system for related devices. In this regard, only Microsoft and Google

developers, plus some 'collaborators' developers for Android (because Android is an open source operating system) can view the source code and patch the holes. The vulnerability is available on this operating system.

1. Application protection against DFA attacks

In addition, both companies are also authorized by the law to store data entrusted by users in their devices, be it desktops, laptops or smartphones. security and privacy purposes. This is especially true in the case of the European Union, with the new GDPR law being completely changed since May 25, 2018. Thus, it can be seen that it is safe for both Windows and Android is no longer an option for two Microsoft and Google vendors, but it is now legalized. This is also part of why both publishers often offer bonus programs for those who discover security holes on their platforms, because they simply don't have any forces. another on the planet has enough time and knowledge for 'malicious vulnerability hunting' besides professional bug hunters. Currently, the Google Bug Hunter and Microsoft Bug Bounty programs are willing to pay large amounts of money for each vulnerability (depending on the severity) found on their products. Try joining if you are eligible.