BIZCOMMUNITY

Are your passwords being stored securely?

The use of malware designed to harvest consumers' digital data - known as password stealers - has seen a significant rise in 2019. According to Kaspersky's data, the number of users, targeted by the stealers, peaked from less than 600,000 in the first half of 2018 to over 940,000 during the same period in 2019.

Source: pixabay.com

Password Stealing Ware (PSW) is a major weapon in the cybercriminals' toolkit to sabotage users' privacy. This malicious type of software grabs data directly from users' web browsers using various methods. Quite often, this information is sensitive and includes access details for online accounts as well as financial information – like saved passwords, autofill data and saved payment card details.

In addition, some families of this type of malware are designed to steal browser cookies, user files from a specific location (for example, a user's desktop) as well as app files, such as messenger services.

Over the past six months, Kaspersky has detected high levels of activity by the stealers in Europe and Asia. Most frequently, the malware has targeted users in Russia, India, Brazil, Germany and the USA.

One of the most widely spread Stealer Trojans was multifunctional Azorult, detected on the computers of more than 25% of all users who encountered Trojan-PSW type malware in the examined period.

“Modern consumers are increasingly active online and understandably rely on the internet to carry out many tasks in their daily lives. This fills their digital profiles with more and more data and details and makes them a lucrative target for criminals as they could be monetised in numerous ways afterwards. By securely storing passwords and credentials, consumers can use their favourite online services in confidence that their information will not be put at risk. This should be also supported by the installation of a security solution as one can never be too careful,” notes Alexander Eremin, a security researcher at Kaspersky.

Steps to stay secure

Kaspersky recommends that consumers follow this advice to ensure their passwords and other credentials remain secure:

- Do not share passwords or personal information with friends or family as they could unwittingly make them vulnerable to malware. Do not post them on forums or social media channels.
- Always install updates and product patches to ensure protection from the latest malware and threats.
- Start using reliable security solutions that is designed to securely store passwords and personal information, including passports, driver's licenses and bank cards.