SEPIO SYSTEMS WARNS FROM HARDWARE BASED ATTACKS, FOLLOWING A 42% INCREASE IN VULNERABLE DEVICES ATTRIBUTED TO #WFH.

Sepio Systems research team has been examining the effect of #WFH during these past weeks, the data for this analysis was collected from our Sepio Cloud service, which managed large volumes of endpoints with their peripheral devices and accessories.

We found that there was an increase of 42% in the number of devices connected to corporates endpoints, compared with the pre-COVID-19 period. Not only the number of connected devices is important to note, but also the fact that we now see almost three time the number of different device vendors – many of which are no-brand unrecognized cheap devices that are not common in the enterprise environment.

This significant rise is attributed to the fact that employees are connecting their existing home peripheral to their endpoints. From selected inquiries that we have made, we saw cases where the enterprises endpoint was used by other family members for remote schooling or just for fun and games.

Another interesting observation, is the fact that operation hours were significantly extended, so where we once used to see , standard office working hours, has now been stretched as the boundaries between work and leisure hours are sometime mixed together.

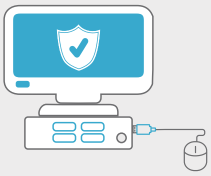
Working from home trends are rising in popularity; 70% of people work remotely at least once a week and over 50% of people work remotely for at least half of the week. Today, COVID-19 is essentially forcing many businesses to make the temporary shift to remote work, meaning more employees are working at home and fewer, if any, are in the office. Working from home means that here are numerous devices connected to the corporate network with a range of manufacturers, and each with different functionalities and capabilities. Although CISOs have started to create longer term security strategies, they sometime fail considering peripherals such as keyboards, mice and USB charging cables, as they are not considered vulnerable devices. However, these devices do pose as a threat to the organization as they have the functionality to both insert and extract, giving them the capacity to cause damage, should they be instructed to do so, even remotely through spoofed wireless connections. These hardware devices can be imbedded with microcomputers, such as the Raspberry Pi, and manipulated to act with malicious intent through payloads. Hence, malware might be installed in the form of trojans, worms or viruses. Other attacks such as man-in-the-middle (MiTM), distributed denial of service (DDoS), keylogging and data breaches can also take place through this attack vector. Moreover, these attacks can be carried out in minutes, if not seconds, and, even after the device has been removed, attackers have remote access to the organization's network allowing them to move laterally through it and gain further access to confidential data.

MAIN FINDINGS

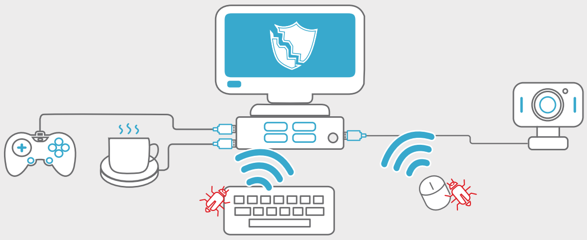
3x Different types of connected devices

42% Number of connected devices

How you used to work...



How you work now...



Your CISOs visibility...