Scam alert on

Multifunction malware

How the scam works

There is an arms race going on between the criminal hackers constantly releasing new viruses, Trojans, worms and other new forms of malware, and the antivirus companies desperately trying to keep pace with the latest threats. Multifunction malware is designed to evade detection by antivirus software, and to compromise various targets in various ways. In more detail:

1. An incident typically starts with a relatively simple malware component known as a dropper. Its main job is to get itself installed on an infected device, hide, and quietly set up a network link back to the hackers.
2. Through the network, the hackers send the dropper additional and updated malware modules so it can exploit more system security weaknesses, spy on the user through cameras and microphones, record network traffic and keys pressed by the user, capture the user's data, infect other systems *etc*. The sheer variety of modules, along with internal variations, makes it less likely that the antivirus software will identify and block the malware, especially if it hasn't been updated lately … or if it is disabled by the malware (!). The compromised system is known as a bot, part of a botnet.
3. When they are ready, the hackers or their criminal customers command the bots to exploit the users, for example locking them out of their own systems as a way to extort a ransom payment out of them (lock-screen ransomware), stealing their data or attacking/overloading further targets.

Avoid the scam

- The best defense is to avoid being infected in the first place!
- Be wary of unsolicited emails from people you don't know, especially those with attachments or links to websites.
- Steer clear of dubious websites and apps, especially from unofficial webstores.
- Don't load USB sticks, CDs or DVDs that you find or are given: they may be infected.
- Make sure the antivirus software is up to date, and keep up with system security patches.
- Most importantly, keep good offline backups: if your device is badly infected and the data (including local and cloud backups) damaged or destroyed, the only option may be to wipe everything and rebuild the system from scratch, or junk it.

Further information

Browse the intranet *Security Zone* or contact the Help Desk for more.