Project 2

Alex Wyner

10/16/2022

Project 3-4

I was not able to complete the installation of the keylogger without compromising the security of my computer at several steps throughout the process. Initially upon downloading the software without installing or launching anything, it was flagged as malware and I was required to whitelist it through Windows antivirus. After attempting to install it on a virtual machine, the processes belonging to the software were flagged and killed by the antivirus. At this point I stopped whitelisting and forcing the software through the antivirus. This demonstrates that this software is very likely known malware and therefore its signature was known and automatically flagged by Windows Defender.

Project 4-1

Screenshots attached

29) No step 29

Reflection:

Microsoft appears to be more upfront and provide more information about their vulnerabilities than Apple based off of this exercise. In my opinion, it is far better to be honest and open about any security vulnerabilities your software may have because it is better to risk looking bad by admitting you have vulnerabilities than to have your clients discover your software has vulnerabilities when a malicious actor exploits them and compromises their network.

Project 5-2

Screenshots attached

14) The hardware information is accurate, although it should be noted that it reflects the hardware information according to the resources I allocated to that virtual machine, for example the reporte number of cores is 4 while the computer hosting the virtual machine actually has 8 and 4 were dedicated to the VM.

I don't think this is worded strongly enough. I personally would include the precise location of the computer, as we should have that provided to us by the location feature, and threaten legal action if the device is not returned.

21) It would definitely be helpful to take screenshots to see what they are up to on the device, and it would certainly be helpful to have a picture of whoever is using the device to give to police to track down the individual.

23) It can be sufficient information to begin to locate the device. It would likely not be an immediate process, however, because the location information is not very accurate and is off by several miles in my case. However, if brought to police it is possible to request information about the IP address from the ISP it belongs to and potentially figure out the physical address that that IP address belongs to.

Reflection: While this software has many useful and interesting features, it must be noted that these features only work if the device is powered on and connect to the Internet. This means that in order to circumvent this software, all a thief needs to do is take the computer offline and either sell it, passing it on to someone else, or wipe the computer clean and install a fresh operating system. As far as I can tell, there is no way for the software to persist if the storage of the device is wiped clean and a fresh OS is installed.

Project 5-3

Screenshots attached

Project 5-4

Screenshots attached

There isn't a Norton Antivirus app anymore

6) Only app by Norton is a VPN, not antivirus

7) No Norton app

8) Considering the Norton Antivirus app no longer exists I would not consider using it for my android device.

18) Compared to desktop antimalware I would say these apps were fairly easy to install and configure. However, they tend to have less features and capabilities than desktop software.

Reflection: While these apps were fairly straightforward to install and configure, my main concern would be ensuring the legitimacy of the software being downloaded. There is no way to validate checksums, and there are plenty of apps on the Google Play store that are malicious and are designed to either look legitimate or mimic real companies or organizations. It is especially dangerous to download a malicious app to your mobile device because it can lead to compromising your physical location, access to your microphone of your phone, the camera of your phone, text history, and other sensitive information.