
Security questions

- is it possible to inject meterpreter on the target computer? (do a bit of research) No, my newest version of Windows detected all files. It was only possible to run a file if the AV is disabled, including SmartScreen.

  To successfully spread the malware it needs a custom encoder, best way to write a own one. After execution it's important to include a AV-Evasion a technique in Windows could be using a fileless maleware in combination with LOLBin.

- explain the concept of portfwd and why this is useful for the attacker This can be used to connect to a PORT in the victims network. This is a pivot attack and allows access to normally unaccessible devices from outside.

- explain why it is possible to dump keystrokes from the victim computer The keystroke_start function allocate a 1MB in the memory and run each 30ms a command against all the 256 keys, this is archived by calling the GetAsyncKeyState that gives the state of a key and detect the key if it changes. The shift, control and alt flags are stored in a 16 bit value.

  Unfortunately this don't work with VNC, cause of the GetAsyncKeyState that don't capture the VNC key states.