**SillyPutty.exe**

**Static Analysis**

**Hashes:**

MD5: 334A10500FEB0F3444BF2E86AB2E76DA

SHA1: C6A97B63FBD970984B95AE79A2B2AEF5749EE463

SHA256: 0C82E654C09C8FD9FDF4899718EFA37670974C9EEC5A8FC18A167F93CEA6EE83

Virus Total -> recognizes this as a malicious file

**Strings:**

* ShellExecute
* WriteFile
* DeleteFile
* CloseSocket
* Send
* Recv
* MS Shell Dlg
* .Microsoft Visual C++ Runtime Library

**Imports/ API calls:**

* DeleteFileA
* GetCapture
* GetDesktopWindow
* ShellExecuteA
* WriteFile
* GetKeyboardState

**Packed vs Not Packed**:

Virtual Size is much larger than raw size, but malware does not seem to be packed. It still shows many imports and from what I can tell doesn’t leave any clues that a packing program was used other then the large difference in size.

**Architecture**:

* 32-bit executable
* Sat Jul 10 09:51:55 2021 | UTC -> compile time
* 1545216 bytes
* MZx

**Dynamic Analysis:**

Graphical user interface, text, application

Description automatically generated

The window on the left is what we see upon detonation, the right window confirms the malware is compiled with clang meaning it is written in C or C++.

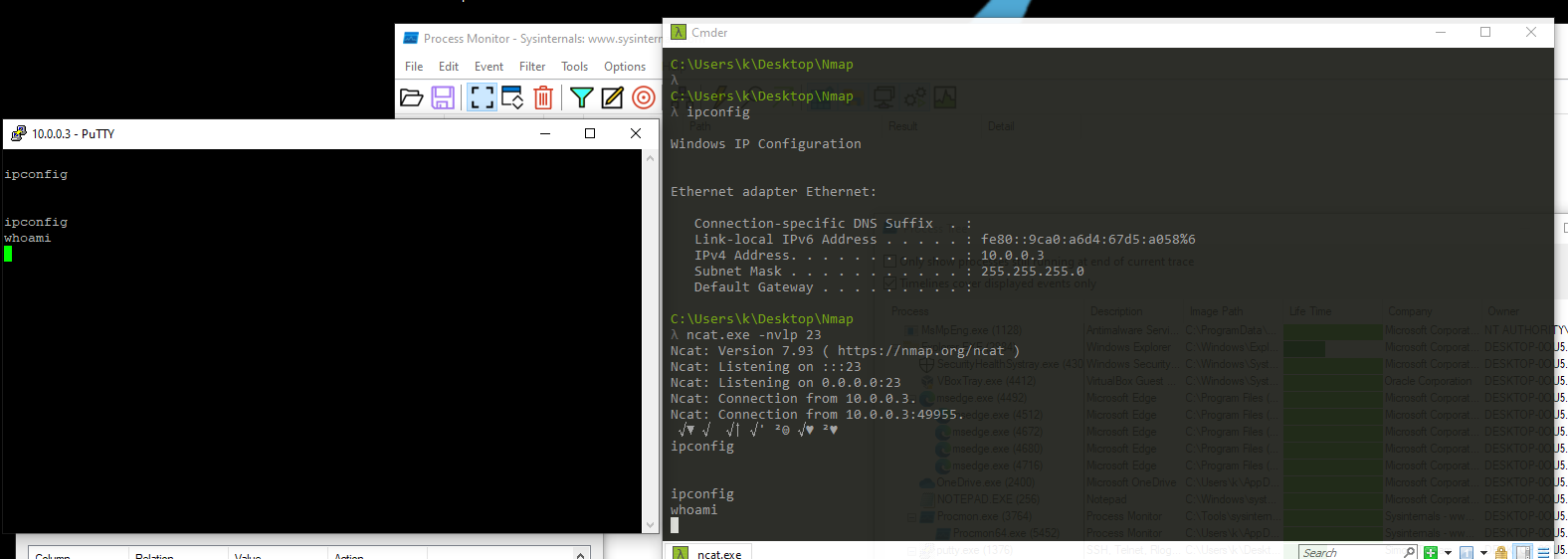
We can also see powershell “flash” open

DNS Query to this domain : destination port is 8443 

Graphical user interface, text, application, email

Description automatically generated

HTTP get request to <http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8f034e717a7d3038>



Putty connected to the netcat listener once supplied with the correct port and listening IP. It seems to be a sort of key logger that records keystrokes typed in the terminal but does not have command execution capabilities.





Different local port depending on configuration in the original putty window

When connected via port 22 and the SSH option on Putty (just a netcat listener on host not actual ssh) putty does not record keys but instead just displays a message

