PROCESS

ICO	SUMMARY
	Parent Process
	Spawned Process
	Process is listening on a port (server)
	Process is trying to communicate but no response
	Process is communicating

VIRUS

MALWARE
Oct 26, 2017

Process rundll32.exe [1784]

- cmd.exe, 3400, null
- cmd.exe, 2808, null
- cmd.exe, 2904, null
- E80D.tmp, 1600, null ← Spawned a .tmp file
- 10.0.0.0 **445**
- 172.16.177.0 **445**
- 10.0.0.0 **139**
- 172.16.177.0 **139**
- 10.0.0.1 **445**
- 172.16.177.1 **445**
- 10.0.0.1 **139**
- 172.16.177.1 **139**
- 10.0.0.3 **445**
- 10.0.0.2 **80**
- 10.0.0.3 **139**
- 172.16.177.145 **80**
- 172.16.177.2 **139**
- 172.16.177.2 **80**
- 10.0.0.4 **445**
- 172.16.177.3 **445**
- 10.0.0.4 **139**
- 172.16.177.3 **139**

RUNNING A SCAN.
ORANGE = Connection not established
GREEN = Connection was established and machine was alive

- 10.0.0.5 **445**
- 172.16.177.4 **445**
- 10.0.0.5 **139**
- 172.16.177.4 **139**
- 10.0.0.6 **445**
- 172.16.177.5 **445**
- 10.0.0.6 **139**
- 172.16.177.5 **139**
- 10.0.0.7 **445**
- 172.16.177.6 **445**
- 10.0.0.7 **139**
- 172.16.177.6 **139**
- 10.0.0.8 **445**
- 172.16.177.7 **445**
- 10.0.0.8 **139**
- 172.16.177.7 **139**
- 10.0.0.9 **445**
- 172.16.177.8 **445**
- 10.0.0.9 **139**
- 172.16.177.8 **139**
- 10.0.0.10 **445**
- 172.16.177.9 **445**
- 10.0.0.10 **139**
- 172.16.177.9 **139**
- 172.16.177.10 **445**
- 10.0.0.11 **139**
- 172.16.177.10 **139**
- 10.0.0.12 **445**
- 172.16.177.11 **445**
- 10.0.0.12 **139**
- 172.16.177.11 **139**
- 10.0.0.13 **445**
- 172.16.177.12 **445**
- 10.0.0.13 **139**
- 172.16.177.12 **139**
- 10.0.0.14 **445**

- 172.16.177.13 **445**
- 10.0.0.14 **139**
- 172.16.177.13 **139**
- 10.0.0.15 **445**
- 172.16.177.14 **445**
- 10.0.0.15 **139**
- 172.16.177.14 **139**
- 10.0.0.16 **445**
- 172.16.177.15 **445**
- 10.0.0.16 **139**
- 172.16.177.15 **139**
- 10.0.0.17 **445**
- 172.16.177.16 **445**
- 10.0.0.17 **139**
- 172.16.177.16 **139**
- 10.0.0.18 **445**
- 172.16.177.17 **445**
- 10.0.0.18 **139**
- 172.16.177.17 **139**
- 10.0.0.19 **445**
- 172.16.177.18 **445**
- 10.0.0.19 **139**
- 172.16.177.18 **139**
- 10.0.0.20 **445**
- 172.16.177.19 **445**
- 10.0.0.20 **139**
- 172.16.177.19 **139**
- 10.0.0.21 **445**
- 172.16.177.20 **445**
- 10.0.0.21 **139**
- 172.16.177.20 **139**
- 10.0.0.22 **445**
- 172.16.177.21 **445**
- 10.0.0.22 **139**
- 172.16.177.21 **139**
- 10.0.0.23 **445**

- 172.16.177.22 **445**
- 10.0.0.23 **139**
- 172.16.177.22 **139**
- 10.0.0.24 **445**
- 172.16.177.23 **445**
- 10.0.0.24 **139**
- 172.16.177.23 **139**
- 10.0.0.25 **445**
- 172.16.177.24 **445**
- 10.0.0.25 **139**
- 172.16.177.24 **139**
- 10.0.0.26 **445**
- 172.16.177.25 **445**
- 10.0.0.26 **139**
- 172.16.177.25 **139**
- 10.0.0.27 **445**
- 172.16.177.26 **445**
- 10.0.0.27 **139**
- 172.16.177.26 **139**
- 10.0.0.28 **445**
- 172.16.177.27 **445**
- 10.0.0.28 **139**
- 172.16.177.27 **139**
- 10.0.0.29 **445**
- 172.16.177.28 **445**
- 10.0.0.29 **139**
- 172.16.177.28 **139**
- 10.0.0.30 **445**
- 172.16.177.29 **445**
- 10.0.0.30 **139**
- 172.16.177.29 **139**
- 10.0.0.31 **445**
- 172.16.177.30 **445**
- 10.0.0.31 **139**
- 172.16.177.30 **139**
- 10.0.0.32 **445**

- 172.16.177.31 **445**
- 10.0.0.32 **139**
- 172.16.177.31 **139**
- 10.0.0.33 **445**
- 172.16.177.32 **445**
- 10.0.0.33 **139**
- 172.16.177.32 **139**
- 10.0.0.34 **445**
- 172.16.177.33 **445**
- 10.0.0.34 **139**
- 172.16.177.33 **139**
- 10.0.0.35 **445**
- 172.16.177.34 **445**
- 10.0.0.35 **139**
- 172.16.177.34 **139**
- 10.0.0.36 **445**
- 172.16.177.35 **445**
- 10.0.0.36 **139**
- 172.16.177.35 **139**
- 10.0.0.37 **445**
- 172.16.177.36 **445**
- 10.0.0.37 **139**
- 172.16.177.36 **139**
- 10.0.0.38 **445**
- 172.16.177.37 **445**
- 10.0.0.38 **139**
- 172.16.177.37 **139**
- 10.0.0.39 **445**
- 172.16.177.38 **445**
- 10.0.0.39 **139**
- 172.16.177.38 **139**
- 10.0.0.40 **445**
- 172.16.177.39 **445**
- 10.0.0.40 **139**
- 172.16.177.39 **139**
- 10.0.0.41 **445**

- 172.16.177.40 **445**
- 10.0.0.41 **139**
- 172.16.177.40 **139**
- 10.0.0.42 **445**
- 172.16.177.41 **445**
- 10.0.0.42 **139**
- 172.16.177.41 **139**
- 10.0.0.43 **445**
- 172.16.177.42 **445**
- 10.0.0.43 **139**
- 172.16.177.42 **139**
- 10.0.0.44 **445**
- 172.16.177.43 **445**
- 10.0.0.44 **139**
- 172.16.177.43 **139**
- 10.0.0.45 **445**
- 172.16.177.44 **445**
- 10.0.0.45 **139**
- 172.16.177.44 **139**
- 10.0.0.46 **445**
- 172.16.177.45 **445**
- 10.0.0.46 **139**
- 172.16.177.45 **139**
- 10.0.0.47 **445**
- 172.16.177.46 **445**
- 10.0.0.47 **139**
- 172.16.177.46 **139**
- 10.0.0.48 **445**
- 172.16.177.47 **445**
- 10.0.0.48 **139**
- 172.16.177.47 **139**
- 10.0.0.49 **445**
- 172.16.177.48 **445**
- 10.0.0.49 **139**
- 172.16.177.48 **139**
- 10.0.0.50 **445**

- 172.16.177.49 **445**
- 10.0.0.50 **139**
- 172.16.177.49 **139**
- 10.0.0.51 **445**
- 172.16.177.50 **445**
- 10.0.0.51 **139**
- 172.16.177.50 **139**
- 10.0.0.52 **445**
- 172.16.177.51 **445**
- 10.0.0.52 **139**
- 172.16.177.51 **139**
- 10.0.0.53 **445**
- 172.16.177.52 **445**
- 10.0.0.53 **139**
- 172.16.177.52 **139**
- 10.0.0.54 **445**
- 172.16.177.53 **445**
- 10.0.0.54 **139**
- 172.16.177.53 **139**
- 10.0.0.55 **445**
- 172.16.177.54 **445**
- 10.0.0.55 **139**
- 172.16.177.54 **139**
- 10.0.0.56 **445**
- 172.16.177.55 **445**
- 10.0.0.56 **139**
- 172.16.177.55 **139**
- 10.0.0.57 **445**
- 172.16.177.56 **445**
- 10.0.0.57 **139**
- 172.16.177.56 **139**
- 10.0.0.58 **445**
- 172.16.177.57 **445**
- 10.0.0.58 **139**
- 172.16.177.57 **139**
- 10.0.0.59 **445**

- 172.16.177.58 **445**
- 10.0.0.59 **139**
- 172.16.177.58 **139**
- 10.0.0.60 **445**
- 172.16.177.59 **445**
- 10.0.0.60 **139**
- 172.16.177.59 **139**
- 10.0.0.61 **445**
- 172.16.177.60 **445**
- 10.0.0.61 **139**
- 172.16.177.60 **139**
- 10.0.0.62 **445**
- 172.16.177.61 **445**
- 10.0.0.62 **139**
- 172.16.177.61 **139**
- 10.0.0.63 **445**
- 172.16.177.62 **445**
- 10.0.0.63 **139**
- 172.16.177.62 **139**
- 10.0.0.64 **445**
- 172.16.177.63 **445**

Process cmd.exe [3400]

- schtasks.exe, 3296, null

Scheduled a task

Process conhost.exe [2348]

Process schtasks.exe [3296]

Process cmd.exe [2808]

- schtasks.exe, 2596, null

Process conhost.exe [3632]

Process schtasks.exe [2596]

Process cmd.exe [2904]

Process conhost.exe [3460]

Process E80D.tmp [1600]

Process conhost.exe [3572]

Process cmd.exe [3656]

- schtasks.exe, 4028, C:\Windows\SysWOW64\schtasks.exe

Process schtasks.exe [4028]

- **Process dllhost.exe [2980]**
- **Process cmd.exe [828]**
- **Process conhost.exe [3636]**
- **Process cmd.exe [3496]**
- **Process cmd.exe [1712]**
    - schtasks.exe, 2548, C:\Windows\SysWOW64\schtasks.exe
- **Process schtasks.exe [2548]**