win764wannacry Report

## Case Overview

Wannacry infected memory

## Case Acquisition

Test Report

## Case Findings

Found various suspicious processes and its artifacts

## Case Conclusion

The connections made by the processes were to the malicious sites

## Artifacts

### process\_list

comment: Suspicious  
 name: @WanaDecryptor  
 physical\_offset: 2110197856  
 pid: 304  
 marked: disabled  
 object\_id: 20  
 unlinked: No  
 ppid: 2668

comment: Random text name  
 name: ed01ebfbc9eb5b  
 physical\_offset: 2140283360  
 pid: 2668  
 marked: disabled  
 object\_id: 40  
 unlinked: No  
 ppid: 1488

comment: Another decryptor  
 name: @WanaDecryptor  
 physical\_offset: 2141180000  
 pid: 1456  
 marked: disabled  
 object\_id: 42  
 unlinked: No  
 ppid: 2668

### dll\_object\_list

comment: Dll of processes  
 name: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe  
 physical\_offset: 966618208  
 pid: 2668  
 marked: disabled  
 object\_id: 1228  
 load\_count: 65535  
 dll\_base: 2082914304  
 size\_of\_image: 3514368  
 full\_dll\_name: C:/Users/Sagar/Downloads/WannaCry/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

comment: Dll of process  
 name: ntdll.dll  
 physical\_offset: 966618448  
 pid: 2668  
 marked: disabled  
 object\_id: 1229  
 load\_count: 65535  
 dll\_base: 715448320  
 size\_of\_image: 1740800  
 full\_dll\_name: C:/Windows/SYSTEM32/ntdll.dll

comment: Dll of process  
 name: wow64.dll  
 physical\_offset: 867009280  
 pid: 2668  
 marked: disabled  
 object\_id: 1230  
 load\_count: 3  
 dll\_base: 2003447808  
 size\_of\_image: 258048  
 full\_dll\_name: C:/Windows/SYSTEM32/wow64.dll

comment: Dll of process  
 name: wow64win.dll  
 physical\_offset: 867008848  
 pid: 2668  
 marked: disabled  
 object\_id: 1231  
 load\_count: 1  
 dll\_base: 1996636160  
 size\_of\_image: 376832  
 full\_dll\_name: C:/Windows/SYSTEM32/wow64win.dll

comment: Dll of process  
 name: wow64cpu.dll  
 physical\_offset: 867010240  
 pid: 2668  
 marked: disabled  
 object\_id: 1232  
 load\_count: 1  
 dll\_base: 2013417472  
 size\_of\_image: 32768  
 full\_dll\_name: C:/Windows/SYSTEM32/wow64cpu.dll

### phandle\_list

comment: Mutex used by suspicious processes  
 name: MsWinZonesCacheCounterMutexA  
 pid: 2668  
 physical\_offset: 2145322816  
 marked: disabled  
 object\_id: 15046  
 type: Mutant

comment: Mutex used by suspicious processes  
 name: MsWinZonesCacheCounterMutexA0  
 pid: 2668  
 physical\_offset: 2139573376  
 marked: disabled  
 object\_id: 15048  
 type: Mutant

### service\_list

### registry\_list

### kernel\_list

### network\_list

comment: Connections of the process  
 object\_id: 16949  
 pid: 1456  
 physical\_offset: 2140174592  
 foreign\_address: 104.32.6.2:0  
 marked: disabled  
 local\_address: 120.32.6.2:0  
 protocol\_version: TCPv4  
 owner\_process: @WanaDecryptor  
 port: 0

comment: Connections of the process  
 object\_id: 16951  
 pid: 304  
 physical\_offset: 2140218864  
 foreign\_address: 104.16.167.3:0  
 marked: disabled  
 local\_address: 120.16.167.3:0  
 protocol\_version: TCPv4  
 owner\_process: @WanaDecryptor  
 port: 0