win764wannacry Report

Case Overview

Wannacry infected memory

Case Acquisition

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/ed01ebfbc9eb5bbea545af4d01bf5f107166184048
0439c6e5babe8e080e41aa.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
marked: disabled
foreign_address: 104.32.6.2:0
protocol_version: TCPv4
local_address: 120.32.6.2:0
owner_process: @WanaDecryptor
port: 0

comment: Connections of the process
object_id: 16951
pid: 304
physical_offset: 2140218864
marked: disabled
foreign_address: 104.16.167.3:0
protocol_version: TCPv4
local_address: 120.16.167.3:0
owner_process: @WanaDecryptor
port: 0