win764wannacry Report

Case Overview

Wannacry infected memory dump.

Case Acquisition

Memory collected from simulation of Wannacry ransomware on Windows 7 virtual machine.

Case Findings

Found the malicious processes and their related objects which are listed in detail below.

Case Conclusion

Attack identified was Wannacry ransomware. The network connections related to the processes were identified and foreign address kelly.torrelays.ovh (148.251.229.164) were found

Report Generation Time

Mon May 14 10:53:02 2018

Artifacts

process_list

----

comment: Possibly malicious

name: @WanaDecryptor
physical_offset: 2110197856
pid: 304
marked: disabled
object_id: 20
unlinked: No
ppid: 2668

----

comment: Spawned by malicious process

name: taskhsvc.exe
physical_offset: 2138738784
pid: 1776
marked: disabled
object_id: 39
unlinked: No
ppid: 304

----

comment: Possibly malicious

name: ed01ebfbc9eb5b
physical_offset: 2140283360
pid: 2668
marked: disabled
object_id: 40
unlinked: No
ppid: 1488

----

dll_object_list

----

phandle_list

----

comment: Handles (Mutants) related to malicious process (Possibly malicious)

name: MsWinZonesCacheCounterMutexA
pid: 2668
physical_offset: 2145322816
marked: disabled
object_id: 15046
type: Mutant

----

comment: Handles (Mutants) related to malicious process (Possibly malicious)

name: MsWinZonesCacheCounterMutexA0
pid: 2668
physical_offset: 2139573376
marked: disabled

object_id: 15048
type: Mutant

----

service_list

----

registry_list

----

kernel_list

----

network_list

----

comment: Network connection related to malicious process (Possibly malicious)

foreign_domain: tor1e1.digitale-gesellschaft.ch
pid: 1776
physical_offset: 2137351808
marked: disabled
object_id: 16941
local_address: 0.0.0.0:11202
protocol_version: TCPv4
owner_process: taskhsvc.exe
foreign_address: 176.10.104.240:64288
port: 11202

----

comment: Network connection related to malicious process (Possibly malicious)

foreign_domain: cpe-104-32-6-2.socal.res.rr.com
pid: 1456
physical_offset: 2140174592
marked: disabled
object_id: 16949
local_address: 120.32.6.2:0
protocol_version: TCPv4
owner_process: @WanaDecryptor
foreign_address: 104.32.6.2:0
port: 0

```
comment: Network connection related to malicious process (Possibly malicious)

foreign_domain: kelly.torrelays.ovh
pid: 1776
physical_offset: 2142753200
marked: disabled
object_id: 16967
local_address: 0.0.0.0:11970
protocol_version: TCPv4
owner_process: taskhsvc.exe
foreign_address: 148.251.229.164:47873
port: 11970
------------------------------------------------------------------------------------------

comment: Network connection related to malicious process (Possibly malicious)

foreign_domain: www.iobit.com
pid: 304
physical_offset: 2142788848
marked: disabled
object_id: 16968
local_address: 0.0.0.0:13250
protocol_version: TCPv4
owner_process: @WanaDecryptor
foreign_address: 127.0.0.1:23075
port: 13250
------------------------------------------------------------------------------------------
```