tiger Report

Case Overview

Hello world

Case Acquisition

ahjgsd

Case Findings

hagjdfuqh

Case Conclusion

"Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Artifacts

process_list

comment: asd
name: Idle
physical_offset: 44446144
pid: 0
object_id: 16
active_threads: 0
marked: disabled
ppid: 0

comment: temp
name: svchost.exe
physical_offset: 2107906864
pid: 1156
object_id: 17
active_threads: 0
marked: disabled
ppid: 440

comment: temp
name: SearchIndexer.
physical_offset: 2133860448
pid: 1792
object_id: 42
active_threads: 0
marked: disabled
ppid: 440

service_list

comment: temp
display_name: Remote Procedure Call (RPC)
name: RpcSs
physical_offset: 156575264
object_id: 50
start: SERVICE_AUTO_START
state: SERVICE_RUNNING
marked: disabled
type: SERVICE_WIN32_SHARE_PROCESS

registry_list

comment: temp
name: HKEY_LOCAL_MACHINE
physical_offset: 142495760
marked: disabled
object_id: 3
file_path: /SystemRoot/System32/Config/SAM

kernel_list

comment: tcp
name: monitor.sys
physical_offset: 94305536
marked: disabled
object_id: 124
file_path: /SystemRoot/system32/DRIVERS/monitor.sys

network_list

comment: udp
physical_offset: 2107902624
marked: disabled

```
object_id: 608
local_address: 0:0:0:0:0:1
protocol_version: UDPv6
port: 61588


comment: tcp
physical_offset: 2111054464
marked: disabled
object_id: 613
local_address: 0:0:0:0:0:0
protocol_version: TCPv6
port: 5357
```