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

```
comment: asdg
name: spoolsv.exe
physical_offset: 2108208736
pid: 1128
object_id: 18
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


comment: Temp
display_name: Offline Files
name: CscService
physical_offset: 163008640
object_id: 51
start: SERVICE_AUTO_START
state: SERVICE_RUNNING
marked: disabled
type: SERVICE_WIN32_SHARE_PROCESS
```

registry_list

kernel_list

```
comment: Temp
name: TSDDD.dll
physical_offset: 94333264
marked: disabled
object_id: 126
file_path: /SystemRoot/System32/TSDDD.dll
```

comment: Temp
name: lltdio.sys
physical_offset: 2107855200
marked: disabled
object_id: 128
file_path: /SystemRoot/system32/DRIVERS/lltdio.sys

network_list

comment: Udp
physical_offset: 2109824704
object_id: 611
marked: disabled
protocol_version: UDPv4
local_address: 192.168.253.128
port: 1900

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