ryuzaki Report

Case Overview

A sample case report

Case Acquisition

The RAM image was acquired from VMEM for testing purpose

Case Findings

Nothing to report

Case Conclusion

Sample report concluded

Artifacts

process_list

comment: Sample Process
name: TrustedInstall
physical_offset: 2111638320
pid: 720
object_id: 23
active_threads: 0
marked: disabled
ppid: 440

service_list

comment: Sample Service
display_name: Distributed Link Tracking Client
name: TrkWks
physical_offset: 156352208
object_id: 49
start: SERVICE_AUTO_START
state: SERVICE_RUNNING
marked: disabled
type: SERVICE_WIN32_SHARE_PROCESS

registry_list

comment: Sample Registry Hive
name: HKEY_LOCAL_MACHINE
physical_offset: 44958272

marked: disabled
object_id: 1
file_path: [no name]

kernel_list

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

network_list

comment: Sample Network Connection
pid: 724
physical_offset: 2107714752
object_id: 607
marked: disabled
local_address: 65152:0:55640:35652:22209:54695
protocol_version: UDPv6
owner_process: svchost.exe
port: 1900