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