stark Report

Case Overview

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

Case Acquisition

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

Case Findings

But I must explain to you how all this mistaken idea of denouncing pleasure and praising pain was born and I will give you a complete account of the system, and expound the actual teachings of the great explorer of the truth, the master-builder of human happiness. No one rejects, dislikes, or avoids pleasure itself, because it is pleasure, but because those who do not know how to pursue pleasure rationally encounter consequences that are extremely painful. Nor again is there anyone who loves or pursues or desires to obtain pain of itself, because it is pain, but because occasionally circumstances occur in which toil and pain can procure him some great pleasure. To take a trivial example, which of us ever undertakes laborious physical exercise, except to obtain some advantage from it? But who has any right to find fault with a man who chooses to enjoy a pleasure that has no annoying consequences, or one who avoids a pain that produces no resultant pleasure

Case Conclusion

At vero eos et accusamus et iusto odio dignissimos ducimus qui blanditiis praesentium voluptatum deleniti atque corrupti quos dolores et quas molestias excepturi sint occaecati cupiditate non provident, similique sunt in culpa qui officia deserunt mollitia animi, id est laborum et dolorum fuga. Et harum quidem rerum facilis est et expedita distinctio. Nam libero tempore, cum soluta nobis est eligendi optio cumque nihil impedit

quo minus id quod maxime placeat facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum hic tenetur a sapiente delectus, ut aut reiciendis voluptatibus maiores alias consequatur aut perferendis doloribus asperiores repellat

Artifacts

process_list

comment:

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: Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum hic tenetur a sapiente delectus, ut aut reiciendis voluptatibus maiores alias consequatur aut perferendis doloribus asperiores repellat

name: spoolsv.exe
physical_offset: 2108208736
pid: 1128
object_id: 18
active_threads: 0
marked: disabled
ppid: 440

service_list
comment: tets

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: Sec

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

kernel_list
comment: Good

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

comment: dea

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

network_list
comment: udl

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