VALKYRIE COMODO

Summary

File Name: mainApp.exe

File Type: PE32 executable (console) Intel 80386, for MS Windows

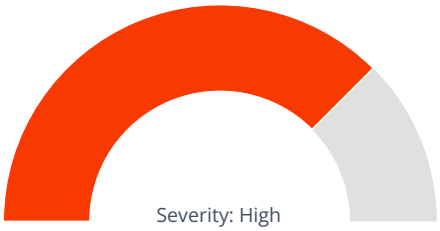
SHA1: e578835b5ba7bc4693b96365522d675e13bd5e75

MD5: a94afcc3efa8c776e49d8d5e559183af

MALWARE

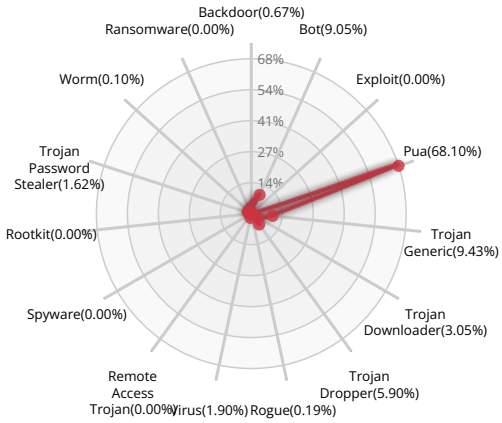
Valkyrie Final Verdict

DETECTION SECTION

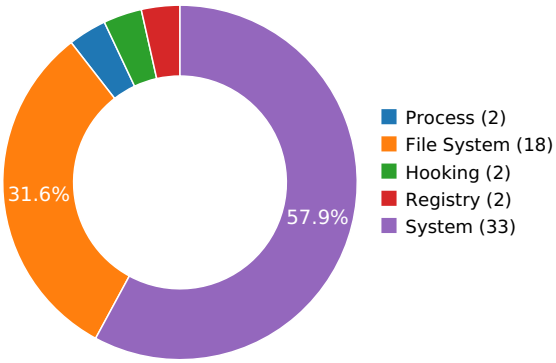


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Malware Analysis System Evasion 1 (100.00%)

VALKYRIE COMODO

Activity Details

MALWARE ANALYSIS SYSTEM EVASION

Network activity detected but not expressed in API logs

VALKYRIE COMODO

Behavior Graph

17:27:49 **17:27:49** **17:27:49**

PID 2652

17:27:49	Create Process	The malicious file created a child process as e578835b5ba7bc4693b96365522d675e13bd5e75.exe **(PPID 1128)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\PSTMESDown\PSTMESDown.dll
C:\Windows\PSTMESDown\PSTMESDown.dll
C:\PSTMESDown\PSTMESDown.dll
C:\ProgramData\Oracle\Java\PSTMESDown\PSTMESDown.dll
C:\Windows\System32\PSTMESDown\PSTMESDown.dll
C:\Windows\System32\WindowsPowerShell\PSTMESDown\PSTMESDown.dll
C:\Program Files\PSTMESDown\PSTMESDown.dll
C:\Program Files (x86)\PSTMESDown\PSTMESDown.dll
C:\Program Files (x86)\Universal Extractor\PSTMESDown\PSTMESDown.dll
C:\Program Files (x86)\Windows Kits\8.1\PSTMESDown\PSTMESDown.dll
C:\Python27\PSTMESDown\PSTMESDown.dll
C:\tools\PSTMESDown\PSTMESDown.dll
C:\tools\IDA_Pro_v6\PSTMESDown\PSTMESDown.dll

RESOLVED APIS

kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.FlsAlloc
kernel32.dll.FlsSetValue
kernel32.dll.FlsGetValue
kernel32.dll.LCMapStringEx
kernel32.dll.AreFileApisANSI
kernel32.dll.CompareStringEx
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.GetDateFormatEx
kernel32.dll.GetLocaleInfoEx
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName
kernel32.dll.LCIDToLocaleName
kernel32.dll.LocaleNameToLCID

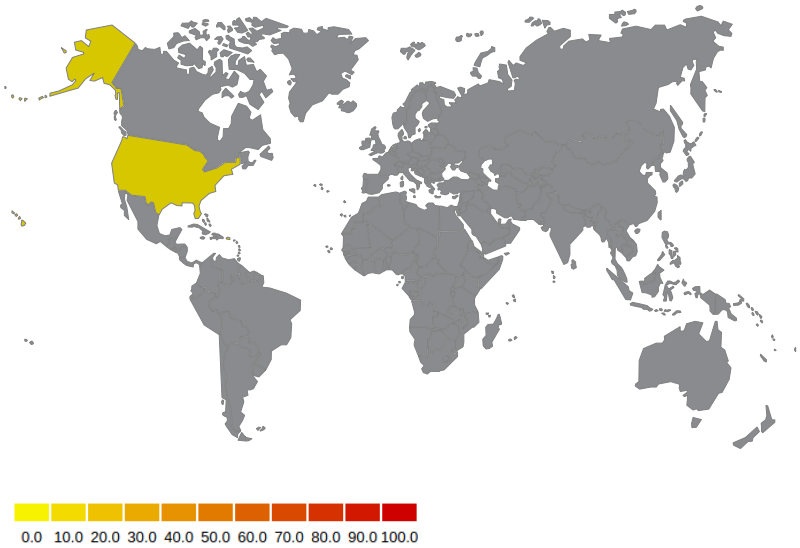
REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize

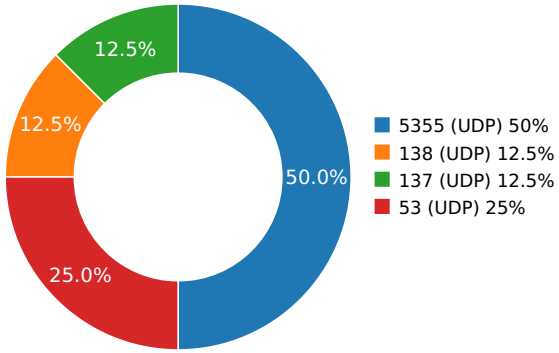
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Google LLC	Malware Process
	8.8.8.8	United States	15169	Google LLC	Malware Process
					Malware Process

DNS QUERIES

Request	Type
5isohu.com	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.00856089592	Sandbox	224.0.0.252	5355
3.01713991165	Sandbox	224.0.0.252	5355
3.07920503616	Sandbox	192.168.56.255	137
5.57933712006	Sandbox	224.0.0.252	5355
8.34408593178	Sandbox	224.0.0.252	5355
9.07898211479	Sandbox	192.168.56.255	138
11.2347149849	Sandbox	8.8.4.4	53
12.2352039814	Sandbox	8.8.8.8	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	mainApp.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
SHA1:	e578835b5ba7bc4693b96365522d675e13bd5e75
MD5:	a94afcc3efa8c776e49d8d5e559183af
First Seen Date:	2024-10-07 14:48:26.320197 (8 days ago)
Number Of Clients Seen:	5
Last Analysis Date:	2024-10-07 22:04:44.835633 (8 days ago)
Human Expert Analysis Date:	2024-10-07 17:22:25.304898 (8 days ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	1
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	4
Trid	[]
Compilation Time Stamp	0x6703F464 [Mon Oct 7 14:47:00 2024 UTC]
Entry Point	0x406230 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	193536
Ssdeep	
Sha256	503140984a1690efeed487f946058e79d537bd6b97b0b95dea97cdef0f56df69
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

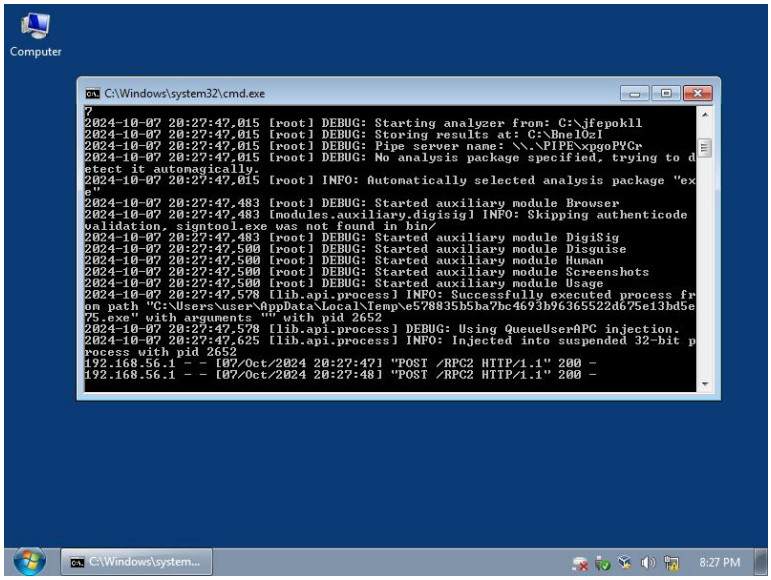
PE Sections

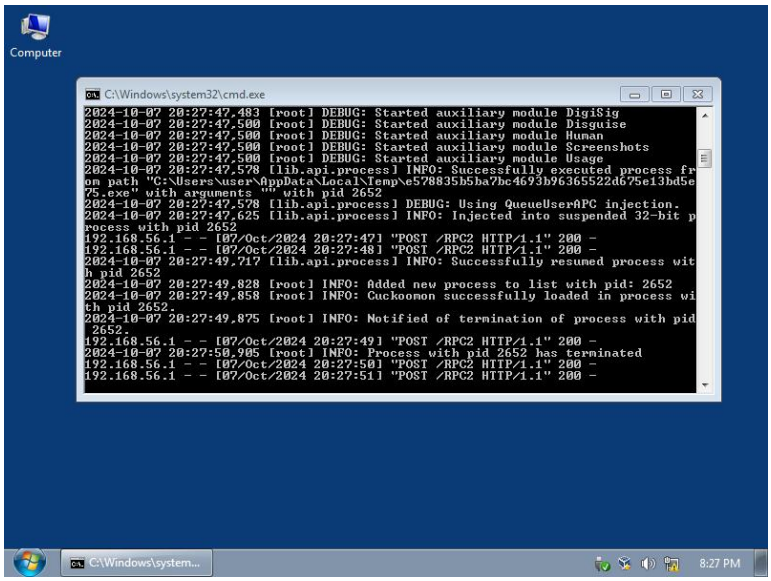
NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x2207a	0x22200	6.59515742841	f3df78e2ac154e788bcef17be3b383c7
.rdata	0x24000	0xa0a8	0xa200	4.96776264586	7c7856a78c9abec5ff75e26eab1be9ef
.data	0x2f000	0x242c	0x1000	2.87831500076	47aee50d6a4643a892b645102ce7a216
.reloc	0x32000	0x1a6c	0x1c00	6.39490171481	dfe67d51d82d31aef9c4e8b45cf3a2ef

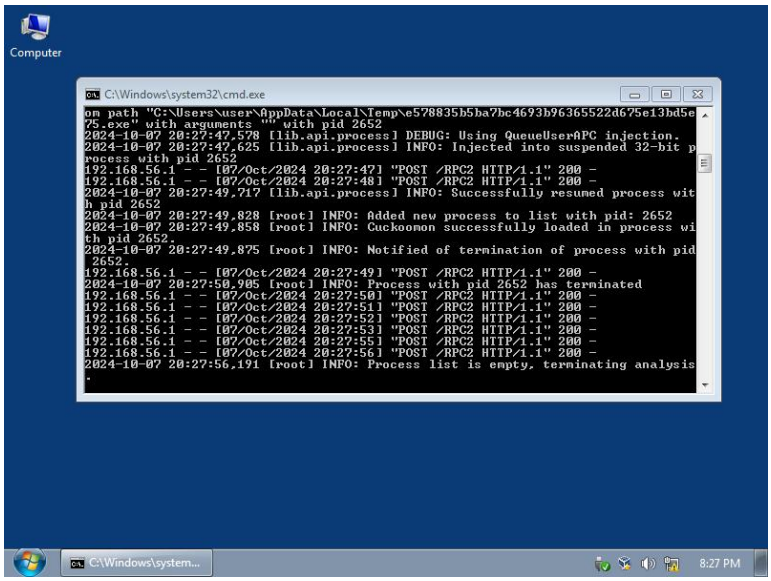
CERTIFICATE VALIDATION

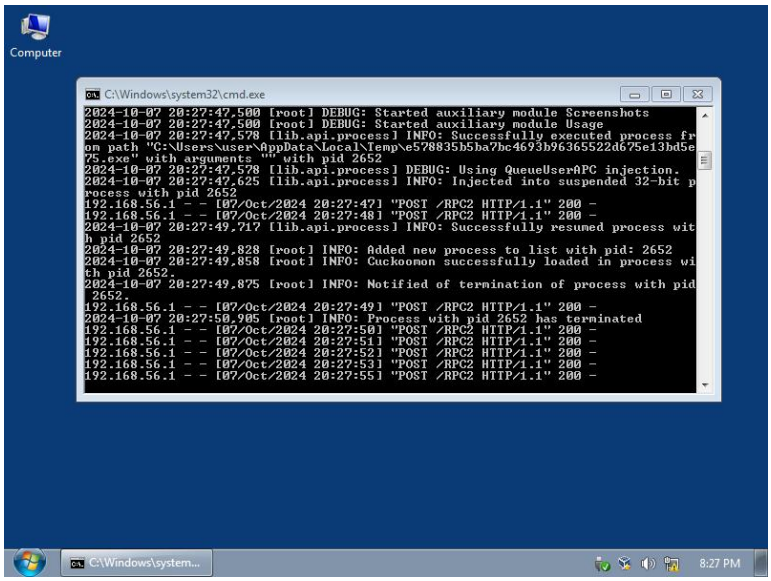
- Certificate Validation is not Applicable ?

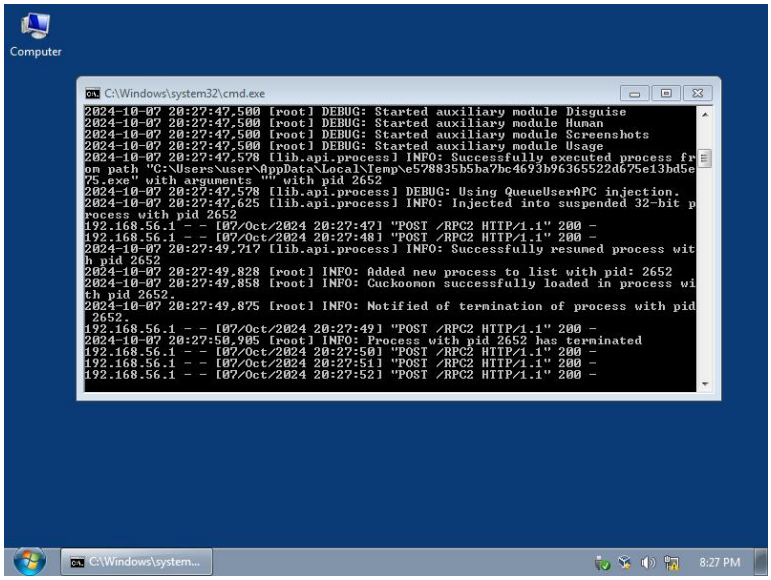
SCREENSHOTS

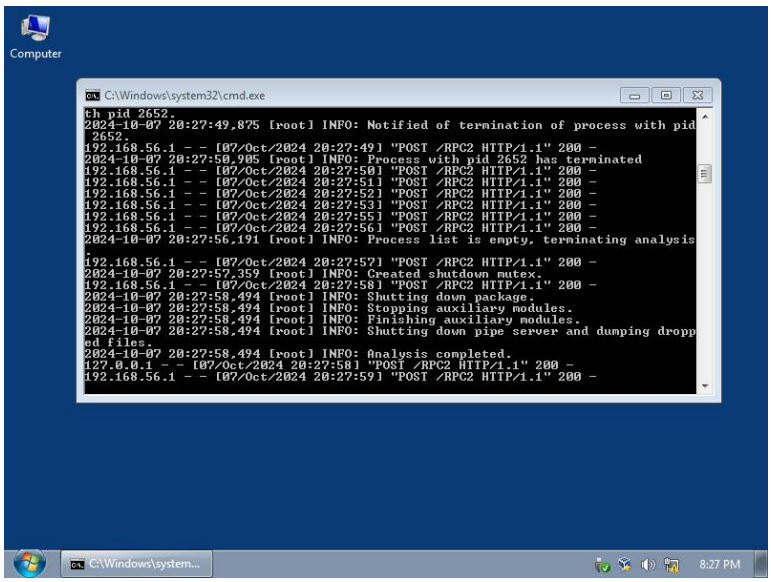

Computer
C:\Windows\system32\cmd.exe
7
2024-10-07 20:27:47,015 [root] DEBUG: Starting analyzer from: C:\jfepokll
2024-10-07 20:27:47,015 [root] DEBUG: Storing results at: C:\BnelOzl
2024-10-07 20:27:47,015 [root] DEBUG: Pipe server name: \\.\PIPE\xpgoPYCr
2024-10-07 20:27:47,015 [root] DEBUG: No analysis package specified, trying to d
etect it automagically.
2024-10-07 20:27:47,015 [root] INFO: Automatically selected analysis package "ex
e"
2024-10-07 20:27:47,483 [root] DEBUG: Started auxiliary module Browser
2024-10-07 20:27:47,483 [modules.auxiliary.digisig] INFO: Skipping authenticode
validation, signtool.exe was not found in bin/
2024-10-07 20:27:47,483 [root] DEBUG: Started auxiliary module DigiSig
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Disguise
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Human
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Screenshots
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Usage
2024-10-07 20:27:47,578 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\e578835b5ba7bc4693b96365522d675e13bd5e
75.exe" with arguments "" with pid 2652
2024-10-07 20:27:47,578 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-10-07 20:27:47,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2652
192.168.56.1 - - [07/Oct/2024 20:27:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:48] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
8:27 PM

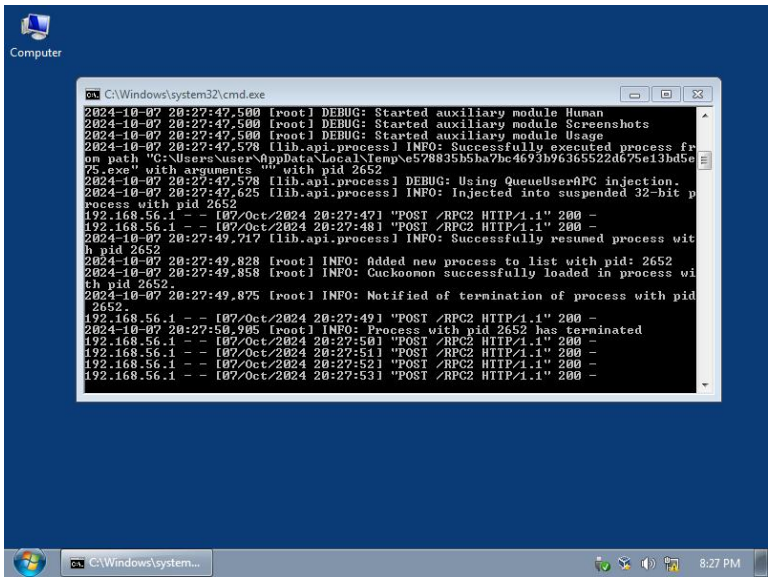

Computer
C:\Windows\system32\cmd.exe
2024-10-07 20:27:47,483 [root] DEBUG: Started auxiliary module DigiSig
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Disguise
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Human
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Screenshots
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Usage
2024-10-07 20:27:47,578 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\e578835b5ba7bc4693b96365522d675e13bd5e
75.exe" with arguments "" with pid 2652
2024-10-07 20:27:47,578 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-10-07 20:27:47,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2652
192.168.56.1 - - [07/Oct/2024 20:27:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:48] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:49,717 [lib.api.process] INFO: Successfully resumed process wit
h pid 2652
2024-10-07 20:27:49,828 [root] INFO: Added new process to list with pid: 2652
2024-10-07 20:27:49,858 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2652.
2024-10-07 20:27:49,875 [root] INFO: Notified of termination of process with pid
2652.
192.168.56.1 - - [07/Oct/2024 20:27:49] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:50,905 [root] INFO: Process with pid 2652 has terminated
192.168.56.1 - - [07/Oct/2024 20:27:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:51] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
8:27 PM

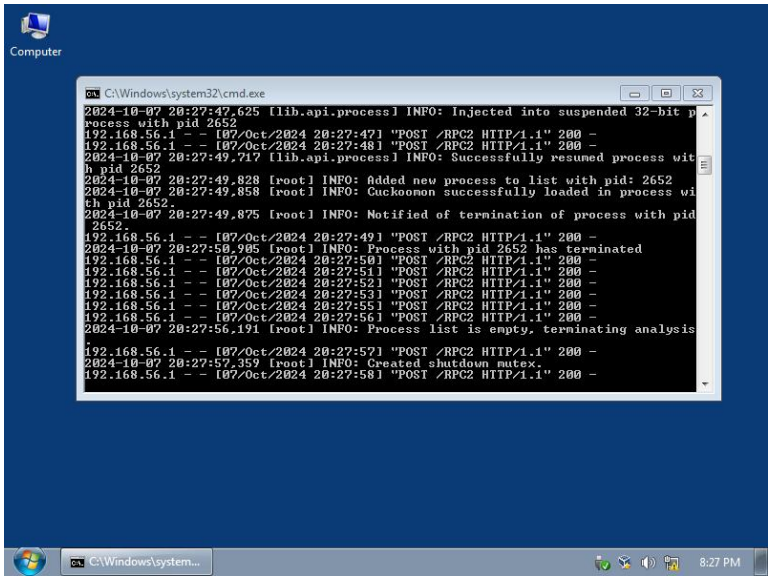

Computer
C:\Windows\system32\cmd.exe
om path "C:\Users\user\AppData\Local\Temp\e578835b5ba7bc4693b96365522d675e13bd5e
75.exe" with arguments "" with pid 2652
2024-10-07 20:27:47,578 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-10-07 20:27:47,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2652
192.168.56.1 - - [07/Oct/2024 20:27:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:48] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:49,717 [lib.api.process] INFO: Successfully resumed process wit
h pid 2652
2024-10-07 20:27:49,828 [root] INFO: Added new process to list with pid: 2652
2024-10-07 20:27:49,858 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2652.
2024-10-07 20:27:49,875 [root] INFO: Notified of termination of process with pid
2652.
192.168.56.1 - - [07/Oct/2024 20:27:49] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:50,905 [root] INFO: Process with pid 2652 has terminated
192.168.56.1 - - [07/Oct/2024 20:27:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:56] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:56,191 [root] INFO: Process list is empty, terminating analysis
.
C:\Windows\system...
8:27 PM

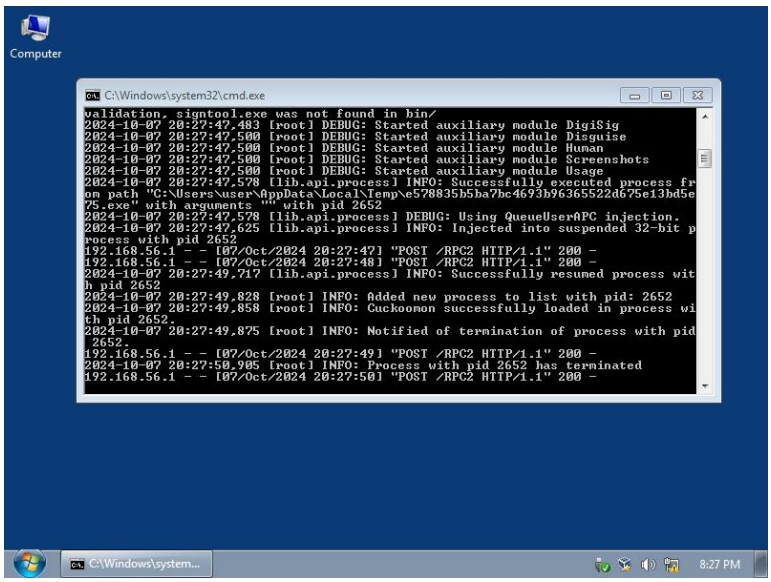

Computer
C:\Windows\system32\cmd.exe
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Screenshots
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Usage
2024-10-07 20:27:47,578 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\e578835b5ba7bc4693b96365522d675e13bd5e
75.exe" with arguments "" with pid 2652
2024-10-07 20:27:47,578 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-10-07 20:27:47,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2652
192.168.56.1 - - [07/Oct/2024 20:27:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:48] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:49,717 [lib.api.process] INFO: Successfully resumed process wit
h pid 2652
2024-10-07 20:27:49,828 [root] INFO: Added new process to list with pid: 2652
2024-10-07 20:27:49,858 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2652.
2024-10-07 20:27:49,875 [root] INFO: Notified of termination of process with pid
2652.
192.168.56.1 - - [07/Oct/2024 20:27:49] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:50,905 [root] INFO: Process with pid 2652 has terminated
192.168.56.1 - - [07/Oct/2024 20:27:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:55] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
8:27 PM

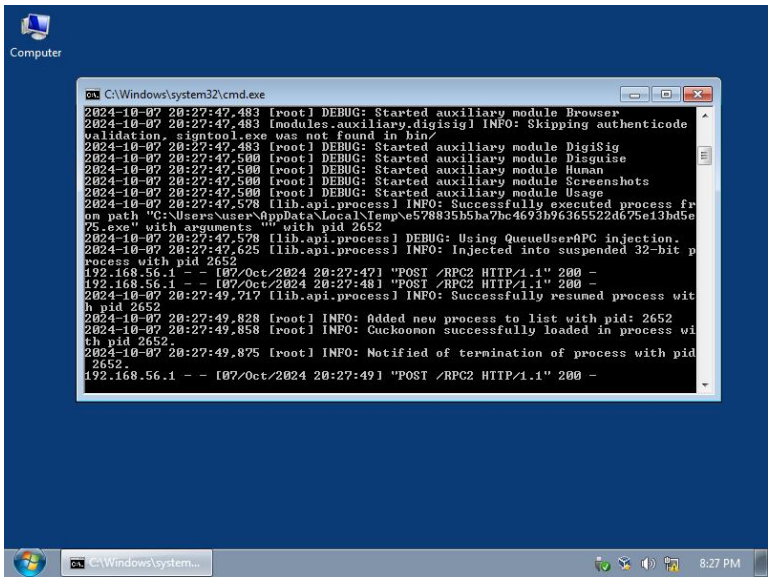

Computer
C:\Windows\system32\cmd.exe
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Disguise
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Human
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Screenshots
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Usage
2024-10-07 20:27:47,578 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\e578835b5ba7bc4693b96365522d675e13bd5e
75.exe" with arguments "" with pid 2652
2024-10-07 20:27:47,578 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-10-07 20:27:47,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2652
192.168.56.1 - - [07/Oct/2024 20:27:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:48] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:49,717 [lib.api.process] INFO: Successfully resumed process wit
h pid 2652
2024-10-07 20:27:49,828 [root] INFO: Added new process to list with pid: 2652
2024-10-07 20:27:49,858 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2652.
2024-10-07 20:27:49,875 [root] INFO: Notified of termination of process with pid
2652.
192.168.56.1 - - [07/Oct/2024 20:27:49] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:50,905 [root] INFO: Process with pid 2652 has terminated
192.168.56.1 - - [07/Oct/2024 20:27:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:52] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
8:27 PM


Computer
C:\Windows\system32\cmd.exe
th pid 2652.
2024-10-07 20:27:49,875 [root] INFO: Notified of termination of process with pid
2652.
192.168.56.1 - - [07/Oct/2024 20:27:49] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:50,905 [root] INFO: Process with pid 2652 has terminated
192.168.56.1 - - [07/Oct/2024 20:27:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:56] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:56,191 [root] INFO: Process list is empty, terminating analysis
.
192.168.56.1 - - [07/Oct/2024 20:27:57] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:57,359 [root] INFO: Created shutdown mutex.
192.168.56.1 - - [07/Oct/2024 20:27:58] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:58,494 [root] INFO: Shutting down package.
2024-10-07 20:27:58,494 [root] INFO: Stopping auxiliary modules.
2024-10-07 20:27:58,494 [root] INFO: Finishing auxiliary modules.
2024-10-07 20:27:58,494 [root] INFO: Shutting down pipe server and dumping dropp
ed files.
2024-10-07 20:27:58,494 [root] INFO: Analysis completed.
127.0.0.1 - - [07/Oct/2024 20:27:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:59] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
8:27 PM


Computer
C:\Windows\system32\cmd.exe
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Human
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Screenshots
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Usage
2024-10-07 20:27:47,578 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\e578835b5ba7bc4693b96365522d675e13bd5e
75.exe" with arguments "" with pid 2652
2024-10-07 20:27:47,578 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-10-07 20:27:47,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2652
192.168.56.1 - - [07/Oct/2024 20:27:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:48] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:49,717 [lib.api.process] INFO: Successfully resumed process wit
h pid 2652
2024-10-07 20:27:49,828 [root] INFO: Added new process to list with pid: 2652
2024-10-07 20:27:49,858 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2652.
2024-10-07 20:27:49,875 [root] INFO: Notified of termination of process with pid
2652.
192.168.56.1 - - [07/Oct/2024 20:27:49] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:50,905 [root] INFO: Process with pid 2652 has terminated
192.168.56.1 - - [07/Oct/2024 20:27:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:53] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
8:27 PM


Computer
C:\Windows\system32\cmd.exe
2024-10-07 20:27:47,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2652
192.168.56.1 - - [07/Oct/2024 20:27:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:48] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:49,717 [lib.api.process] INFO: Successfully resumed process wit
h pid 2652
2024-10-07 20:27:49,828 [root] INFO: Added new process to list with pid: 2652
2024-10-07 20:27:49,858 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2652.
2024-10-07 20:27:49,875 [root] INFO: Notified of termination of process with pid
2652.
192.168.56.1 - - [07/Oct/2024 20:27:49] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:50,905 [root] INFO: Process with pid 2652 has terminated
192.168.56.1 - - [07/Oct/2024 20:27:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:56] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:56,191 [root] INFO: Process list is empty, terminating analysis
.
192.168.56.1 - - [07/Oct/2024 20:27:57] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:57,359 [root] INFO: Created shutdown mutex.
192.168.56.1 - - [07/Oct/2024 20:27:58] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
8:27 PM


Computer
C:\Windows\system32\cmd.exe
validation, signtool.exe was not found in bin/
2024-10-07 20:27:47,483 [root] DEBUG: Started auxiliary module DigiSig
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Disguise
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Human
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Screenshots
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Usage
2024-10-07 20:27:47,578 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\e578835b5ba7bc4693b96365522d675e13bd5e
75.exe" with arguments "" with pid 2652
2024-10-07 20:27:47,578 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-10-07 20:27:47,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2652
192.168.56.1 - - [07/Oct/2024 20:27:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:48] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:49,717 [lib.api.process] INFO: Successfully resumed process wit
h pid 2652
2024-10-07 20:27:49,828 [root] INFO: Added new process to list with pid: 2652
2024-10-07 20:27:49,858 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2652.
2024-10-07 20:27:49,875 [root] INFO: Notified of termination of process with pid
2652.
192.168.56.1 - - [07/Oct/2024 20:27:49] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:50,905 [root] INFO: Process with pid 2652 has terminated
192.168.56.1 - - [07/Oct/2024 20:27:50] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
8:27 PM


Computer
C:\Windows\system32\cmd.exe
2024-10-07 20:27:47,483 [root] DEBUG: Started auxiliary module Browser
2024-10-07 20:27:47,483 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2024-10-07 20:27:47,483 [root] DEBUG: Started auxiliary module DigiSig
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Disguise
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Human
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Screenshots
2024-10-07 20:27:47,500 [root] DEBUG: Started auxiliary module Usage
2024-10-07 20:27:47,578 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\e578035b5ba7bc4693b96365522d675e13bd5e75.exe" with arguments "" with pid 2652
2024-10-07 20:27:47,578 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-10-07 20:27:47,625 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2652
192.168.56.1 - - [07/Oct/2024 20:27:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [07/Oct/2024 20:27:48] "POST /RPC2 HTTP/1.1" 200 -
2024-10-07 20:27:49,717 [lib.api.process] INFO: Successfully resumed process with pid 2652
2024-10-07 20:27:49,828 [root] INFO: Added new process to list with pid: 2652
2024-10-07 20:27:49,858 [root] INFO: Cuckoomon successfully loaded in process with pid 2652.
2024-10-07 20:27:49,875 [root] INFO: Notified of termination of process with pid 2652.
192.168.56.1 - - [07/Oct/2024 20:27:49] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
8:27 PM