VALKYRIE COMODO

Summary

File Name: 222.exe

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

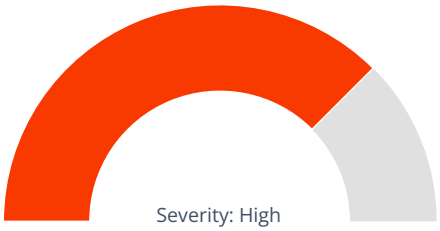
SHA1: 9c1db682706e84bc5c62eb94ba286d040d21bd16

MD5: e470e1efdf057bf0cb67f5f8e7d146f5

MALWARE

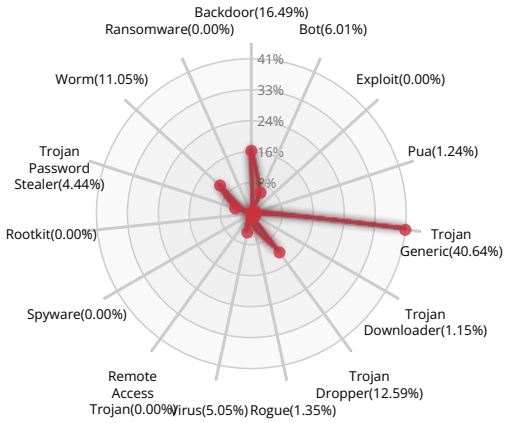
Valkyrie Final Verdict

DETECTION SECTION

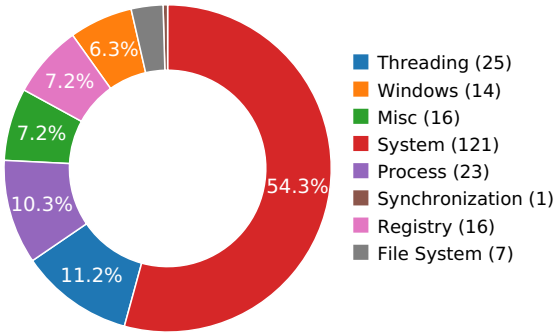


Verdict: Malware

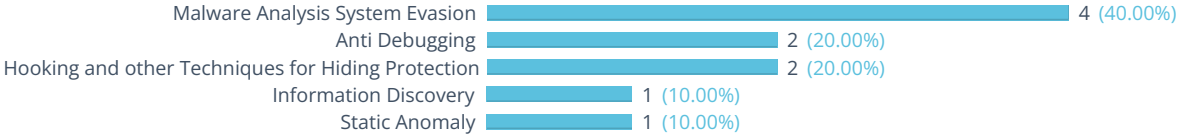
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Expresses interest in specific running processes	Show sources

STATIC ANOMALY

Anomalous binary characteristics	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Detects VirtualBox through the presence of a registry key	Show sources
Checks the version of Bios, possibly for anti-virtualization	Show sources
Detects the presence of Wine emulator via registry key	Show sources
Network activity detected but not expressed in API logs	

ANTI DEBUGGING

Checks for the presence of known devices from debuggers and forensic tools	Show sources
Checks for the presence of known windows from debuggers and forensic tools	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources
The following process appear to have been packed with Themida: 9c1db682706e84bc5c62eb94ba286d040d21bd16.exe	

VALKYRIE COMODO

Behavior Graph

09:00:37 **09:00:37** **09:00:37**

PID 2588

09:00:37	Create Process	The malicious file created a child process as 9c1db682706e84bc5c62eb94ba286d040d21bd16.exe **(PPID 1480)**

09:00:37	NtCreateFile
09:00:37 09:00:37	RegOpenKeyExA **[2 times]**
09:00:37	RegQueryValueExA
09:00:37 09:00:37	FindWindowA **[10 times]**
09:00:37	VirtualProtectEx

Behavior Summary

ACCESSED FILES

\??\SICE
\??\SIWVID
\??\NTICE
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\ntdll.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000\DriverDesc
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\SystemBiosVersion
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\VideoBiosVersion
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

MODIFIED FILES

\??\SICE
\??\SIWVID
\??\NTICE

RESOLVED APIS

kernel32.dll.GetNativeSystemInfo
winmm.dll.timeGetTime
ntdll.dll.NtOpenThread
ntdll.dll.NtQuerySystemInformation
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
ntdll.dll.RtlAllocateHeap

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Wine
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000\DriverDesc
HKEY_LOCAL_MACHINE\Hardware\description\System

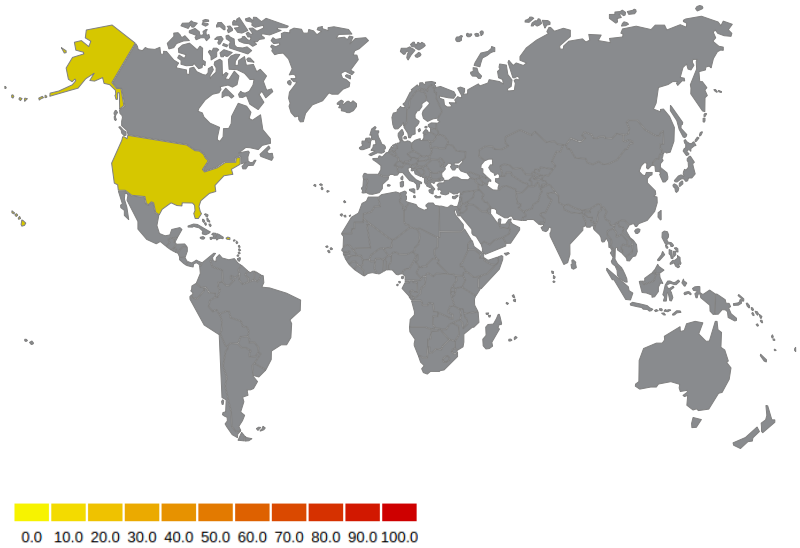
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\SystemBiosVersion
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\VideoBiosVersion
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

READ FILES

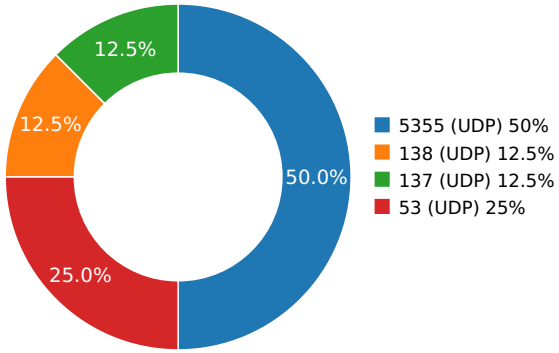
\??\SICE
\??\SIWVID
\??\NTICE
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\ntdll.dll

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
3.00608801842	Sandbox	224.0.0.252	5355
3.01416921616	Sandbox	224.0.0.252	5355
3.0787820816	Sandbox	192.168.56.255	137
5.56357908249	Sandbox	224.0.0.252	5355
8.08627915382	Sandbox	224.0.0.252	5355
9.07877802849	Sandbox	192.168.56.255	138
11.0006351471	Sandbox	8.8.4.4	53
12.0004551411	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:	222.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	9c1db682706e84bc5c62eb94ba286d040d21bd16
MD5:	e470e1efdf057bf0cb67f5f8e7d146f5
First Seen Date:	2024-11-04 18:48:54.302927 (about 18 hours ago)
Number Of Clients Seen:	1
Last Analysis Date:	2024-11-04 18:51:25.630731 (about 18 hours ago)
Human Expert Analysis Date:	2024-11-05 08:38:19.931418 (about 4 hours ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	6
Trid	[]
Compilation Time Stamp	0x6715CDA7 [Mon Oct 21 03:42:31 2024 UTC]
Entry Point	0x715000 (.taggant)
Machine Type	Intel 386 or later - 32Bit
File Size	3030016
Ssdeep	
Sha256	cb15ac6b923950cc436643ca20417973952a9bee1c80d1c0f1bd9c564bd55b0a
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
	0x1000	0x58000	0x27a00	7.97228759374	433805cc7f54e09d19df48c4426b1471
.rsrc	0x59000	0x340	0x400	4.99738997375	914cd139a383496d0085d499d138ef92
.idata	0x5a000	0x1000	0x200	0.999651588151	555a11fa24a077379003c187d9c9d020
qjxzgjzf	0x5b000	0x2b9000	0x2b8600	6.40302521105	fa0724c39c869cac20763fc86cf33fe8
obhbrmkm	0x314000	0x1000	0x400	5.95406882588	495a1b8aa1daeef9588144dfe4a632d5
.taggant	0x315000	0x3000	0x2200	0.790179425507	04f3c5f5a7c155ec6194f491c558003b

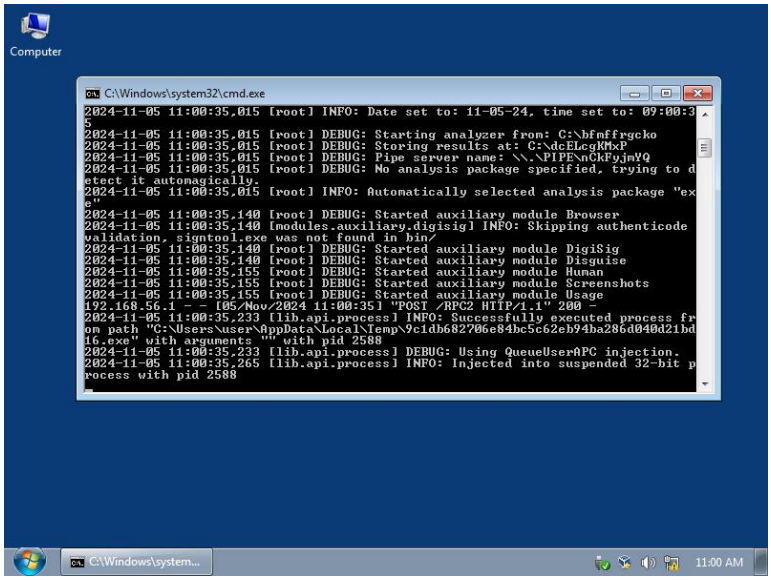
PE Resources

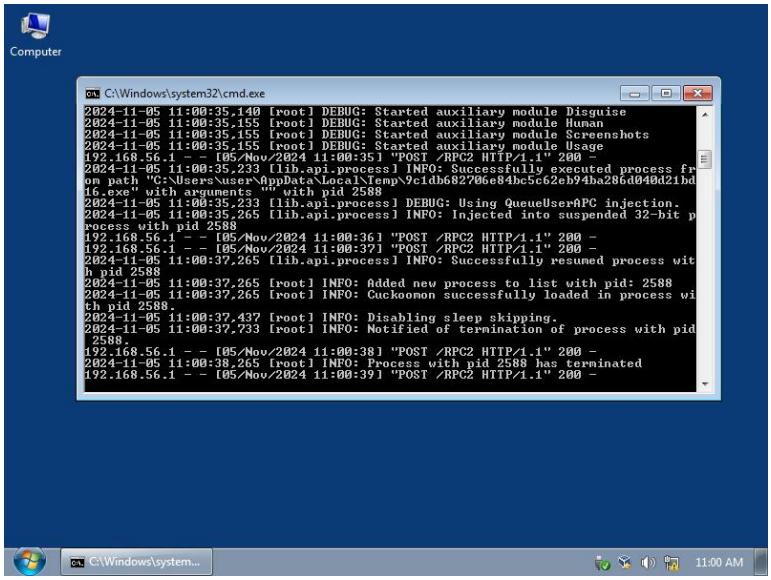
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 364632, u'sha256': u'b3a8ff49e0b32b632b3b99a01c3d191f95a8566664da090bfff4652229fe083e', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 742}

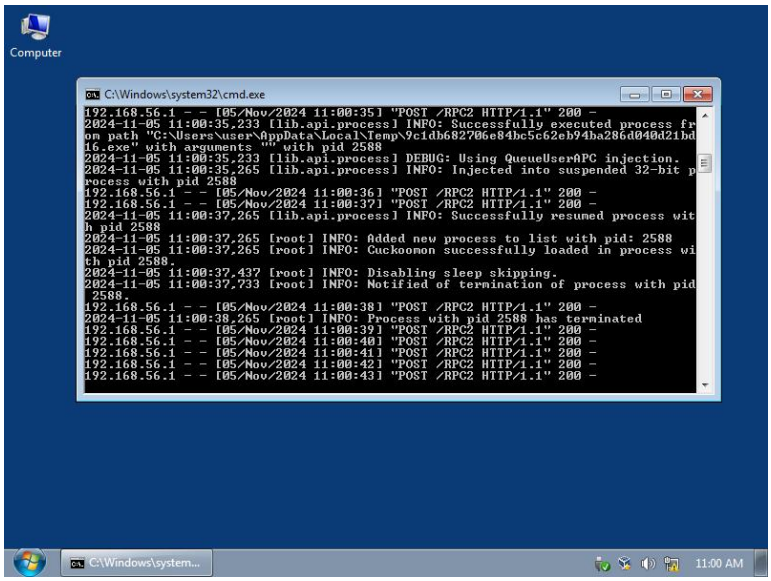
CERTIFICATE VALIDATION

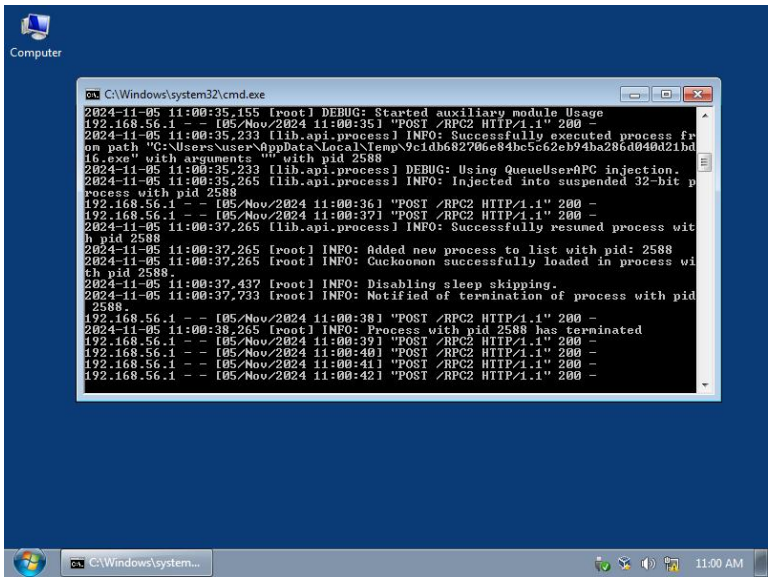
- Certificate Validation is not Applicable ?

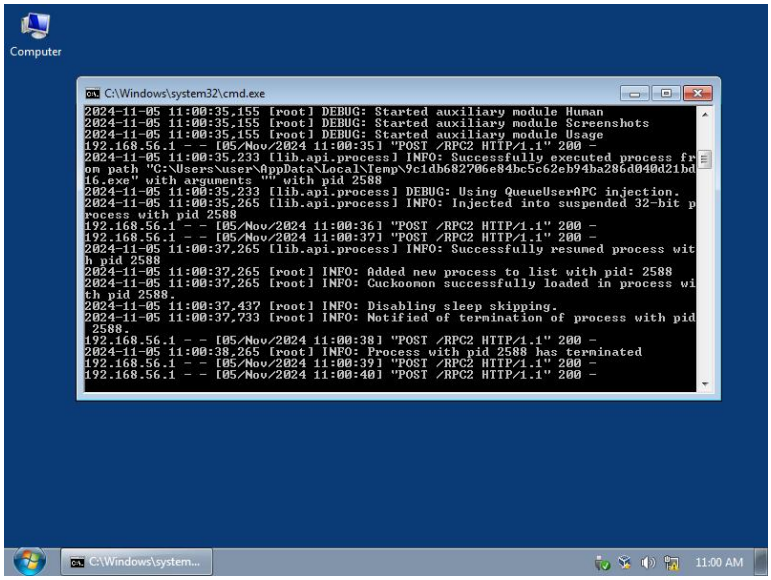
SCREENSHOTS

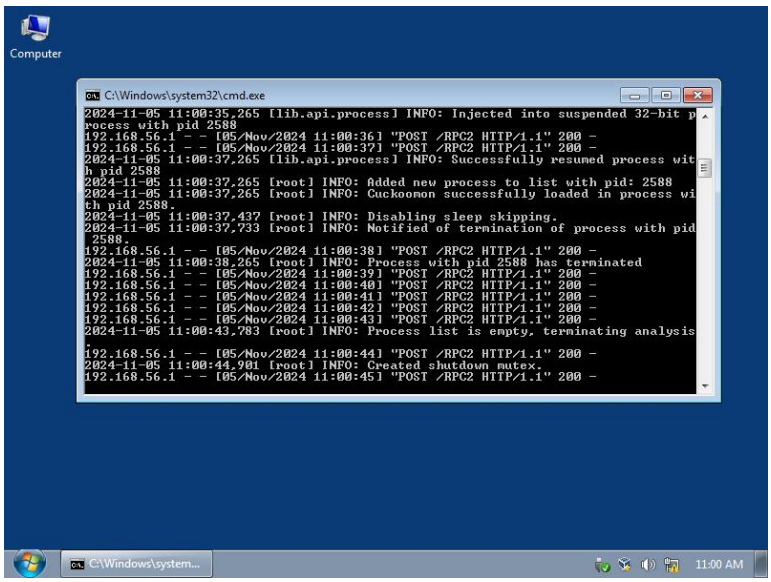


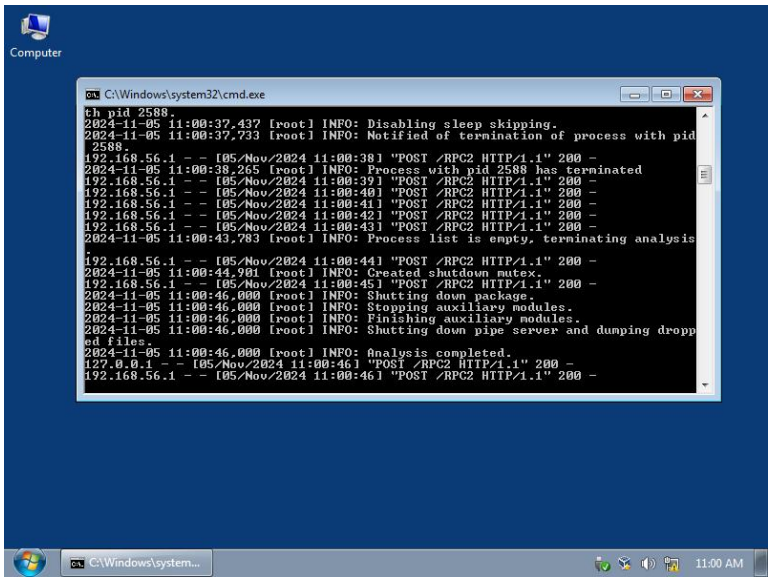


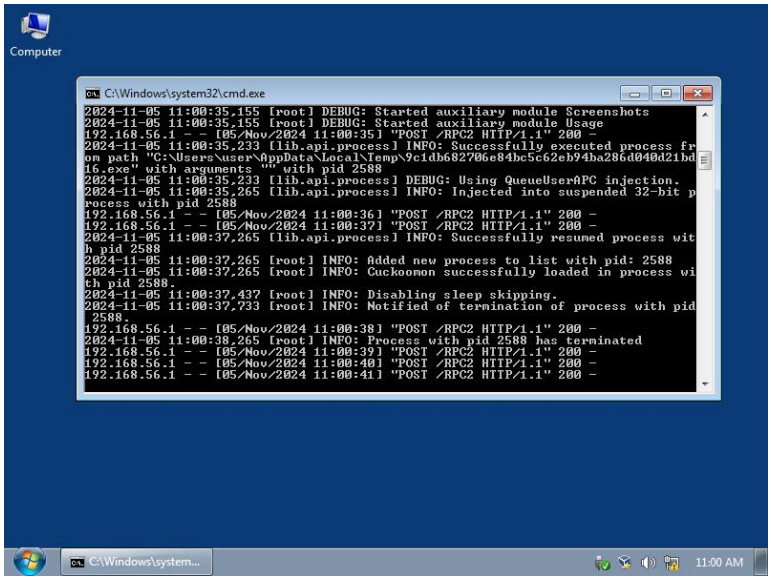


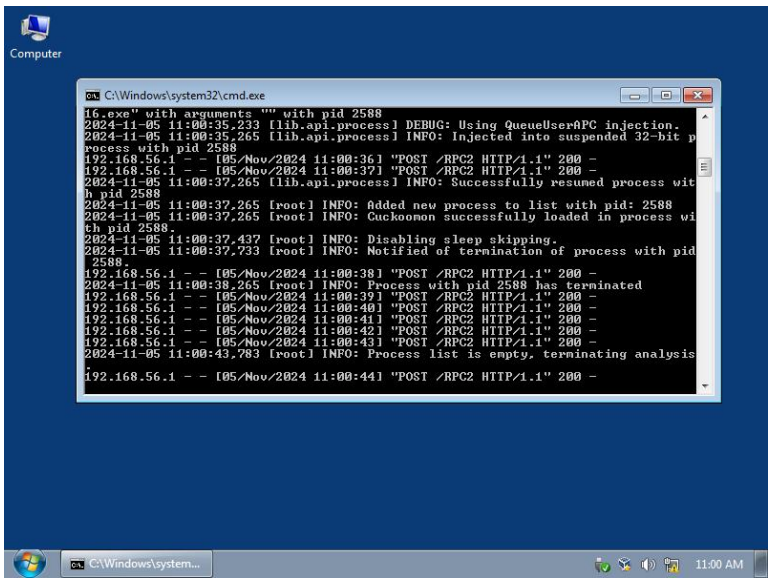

Computer
C:\Windows\system32\cmd.exe
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Usage
192.168.56.1 - - [05/Nov/2024 11:00:35] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:35,233 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\9c1db682706e84bc5c62eb94ba286d040d21bd
16.exe" with arguments "" with pid 2588
2024-11-05 11:00:35,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-05 11:00:35,265 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2588
192.168.56.1 - - [05/Nov/2024 11:00:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:37] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:37,265 [lib.api.process] INFO: Successfully resumed process wit
h pid 2588
2024-11-05 11:00:37,265 [root] INFO: Added new process to list with pid: 2588
2024-11-05 11:00:37,265 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2588.
2024-11-05 11:00:37,437 [root] INFO: Disabling sleep skipping.
2024-11-05 11:00:37,733 [root] INFO: Notified of termination of process with pid
2588.
192.168.56.1 - - [05/Nov/2024 11:00:38] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:38,265 [root] INFO: Process with pid 2588 has terminated
192.168.56.1 - - [05/Nov/2024 11:00:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:42] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:00 AM

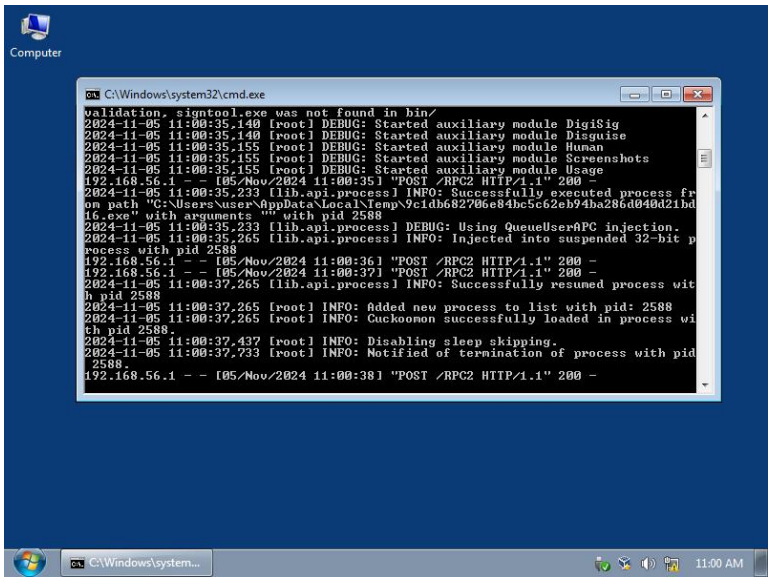

Computer
C:\Windows\system32\cmd.exe
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Human
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Screenshots
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Usage
192.168.56.1 - - [05/Nov/2024 11:00:35] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:35,233 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\9c1db682706e84bc5c62eb94ba286d040d21bd
16.exe" with arguments "" with pid 2588
2024-11-05 11:00:35,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-05 11:00:35,265 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2588
192.168.56.1 - - [05/Nov/2024 11:00:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:37] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:37,265 [lib.api.process] INFO: Successfully resumed process wit
h pid 2588
2024-11-05 11:00:37,265 [root] INFO: Added new process to list with pid: 2588
2024-11-05 11:00:37,265 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2588.
2024-11-05 11:00:37,437 [root] INFO: Disabling sleep skipping.
2024-11-05 11:00:37,733 [root] INFO: Notified of termination of process with pid
2588.
192.168.56.1 - - [05/Nov/2024 11:00:38] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:38,265 [root] INFO: Process with pid 2588 has terminated
192.168.56.1 - - [05/Nov/2024 11:00:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:40] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:00 AM

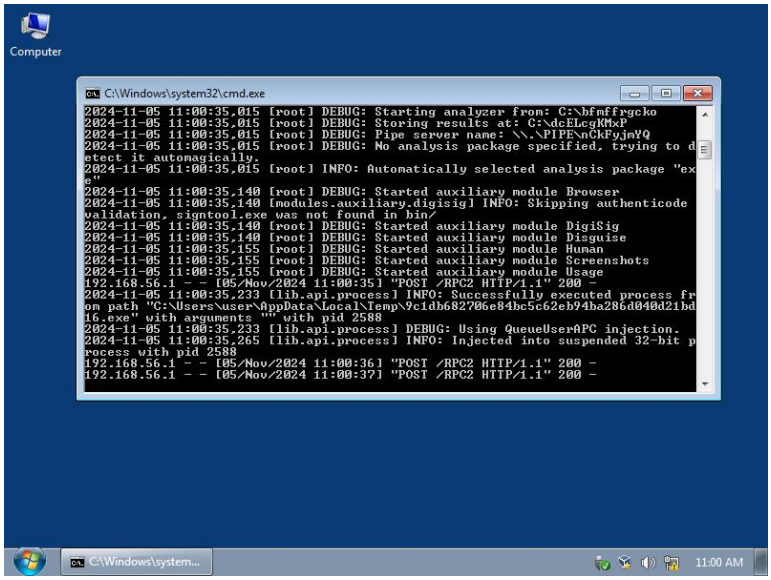

Computer
C:\Windows\system32\cmd.exe
2024-11-05 11:00:35,265 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2588
192.168.56.1 - - [05/Nov/2024 11:00:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:37] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:37,265 [lib.api.process] INFO: Successfully resumed process wit
h pid 2588
2024-11-05 11:00:37,265 [root] INFO: Added new process to list with pid: 2588
2024-11-05 11:00:37,265 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2588.
2024-11-05 11:00:37,437 [root] INFO: Disabling sleep skipping.
2024-11-05 11:00:37,733 [root] INFO: Notified of termination of process with pid
2588.
192.168.56.1 - - [05/Nov/2024 11:00:38] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:38,265 [root] INFO: Process with pid 2588 has terminated
192.168.56.1 - - [05/Nov/2024 11:00:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:43] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:43,783 [root] INFO: Process list is empty, terminating analysis
.
192.168.56.1 - - [05/Nov/2024 11:00:44] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:44,901 [root] INFO: Created shutdown mutex.
192.168.56.1 - - [05/Nov/2024 11:00:45] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:00 AM


Computer
C:\Windows\system32\cmd.exe
th pid 2588.
2024-11-05 11:00:37,437 [root] INFO: Disabling sleep skipping.
2024-11-05 11:00:37,733 [root] INFO: Notified of termination of process with pid
2588.
192.168.56.1 - - [05/Nov/2024 11:00:38] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:38,265 [root] INFO: Process with pid 2588 has terminated
192.168.56.1 - - [05/Nov/2024 11:00:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:43] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:43,783 [root] INFO: Process list is empty, terminating analysis
.
192.168.56.1 - - [05/Nov/2024 11:00:44] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:44,901 [root] INFO: Created shutdown mutex.
192.168.56.1 - - [05/Nov/2024 11:00:45] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:46,000 [root] INFO: Shutting down package.
2024-11-05 11:00:46,000 [root] INFO: Stopping auxiliary modules.
2024-11-05 11:00:46,000 [root] INFO: Finishing auxiliary modules.
2024-11-05 11:00:46,000 [root] INFO: Shutting down pipe server and dumping dropp
ed files.
2024-11-05 11:00:46,000 [root] INFO: Analysis completed.
127.0.0.1 - - [05/Nov/2024 11:00:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:46] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:00 AM


Computer
C:\Windows\system32\cmd.exe
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Screenshots
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Usage
192.168.56.1 - - [05/Nov/2024 11:00:35] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:35,233 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\9c1db682706e84bc5c62eb94ba286d040d21bd
16.exe" with arguments "" with pid 2588
2024-11-05 11:00:35,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-05 11:00:35,265 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2588
192.168.56.1 - - [05/Nov/2024 11:00:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:37] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:37,265 [lib.api.process] INFO: Successfully resumed process wit
h pid 2588
2024-11-05 11:00:37,265 [root] INFO: Added new process to list with pid: 2588
2024-11-05 11:00:37,265 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2588.
2024-11-05 11:00:37,437 [root] INFO: Disabling sleep skipping.
2024-11-05 11:00:37,733 [root] INFO: Notified of termination of process with pid
2588.
192.168.56.1 - - [05/Nov/2024 11:00:38] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:38,265 [root] INFO: Process with pid 2588 has terminated
192.168.56.1 - - [05/Nov/2024 11:00:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:41] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:00 AM


Computer
C:\Windows\system32\cmd.exe
16.exe" with arguments "" with pid 2588
2024-11-05 11:00:35,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-05 11:00:35,265 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2588
192.168.56.1 - - [05/Nov/2024 11:00:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:37] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:37,265 [lib.api.process] INFO: Successfully resumed process wit
h pid 2588
2024-11-05 11:00:37,265 [root] INFO: Added new process to list with pid: 2588
2024-11-05 11:00:37,265 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2588.
2024-11-05 11:00:37,437 [root] INFO: Disabling sleep skipping.
2024-11-05 11:00:37,733 [root] INFO: Notified of termination of process with pid
2588.
192.168.56.1 - - [05/Nov/2024 11:00:38] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:38,265 [root] INFO: Process with pid 2588 has terminated
192.168.56.1 - - [05/Nov/2024 11:00:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:43] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:43,783 [root] INFO: Process list is empty, terminating analysis
.
192.168.56.1 - - [05/Nov/2024 11:00:44] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:00 AM


Computer
C:\Windows\system32\cmd.exe
validation, signtool.exe was not found in bin/
2024-11-05 11:00:35,140 [root] DEBUG: Started auxiliary module DigiSig
2024-11-05 11:00:35,140 [root] DEBUG: Started auxiliary module Disguise
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Human
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Screenshots
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Usage
192.168.56.1 - - [05/Nov/2024 11:00:35] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:35,233 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\9c1db682706e84bc5c62eb94ba286d040d21bd
16.exe" with arguments "" with pid 2588
2024-11-05 11:00:35,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-05 11:00:35,265 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2588
192.168.56.1 - - [05/Nov/2024 11:00:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:37] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:37,265 [lib.api.process] INFO: Successfully resumed process wit
h pid 2588
2024-11-05 11:00:37,265 [root] INFO: Added new process to list with pid: 2588
2024-11-05 11:00:37,265 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2588.
2024-11-05 11:00:37,437 [root] INFO: Disabling sleep skipping.
2024-11-05 11:00:37,733 [root] INFO: Notified of termination of process with pid
2588.
192.168.56.1 - - [05/Nov/2024 11:00:38] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:00 AM


Computer
C:\Windows\system32\cmd.exe
2024-11-05 11:00:35,015 [root] DEBUG: Starting analyzer from: C:\bfmffrgcko
2024-11-05 11:00:35,015 [root] DEBUG: Storing results at: C:\dcELcgKMxP
2024-11-05 11:00:35,015 [root] DEBUG: Pipe server name: \\.\PIPE\uCkFyjmVQ
2024-11-05 11:00:35,015 [root] DEBUG: No analysis package specified, trying to d
etect it automagically.
2024-11-05 11:00:35,015 [root] INFO: Automatically selected analysis package "ex
e"
2024-11-05 11:00:35,140 [root] DEBUG: Started auxiliary module Browser
2024-11-05 11:00:35,140 [modules.auxiliary.digisig] INFO: Skipping authenticode
validation, signtool.exe was not found in bin/
2024-11-05 11:00:35,140 [root] DEBUG: Started auxiliary module DigiSig
2024-11-05 11:00:35,140 [root] DEBUG: Started auxiliary module Disguise
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Human
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Screenshots
2024-11-05 11:00:35,155 [root] DEBUG: Started auxiliary module Usage
192.168.56.1 - - [05/Nov/2024 11:00:35] "POST /RPC2 HTTP/1.1" 200 -
2024-11-05 11:00:35,233 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\9c1db682706e84bc5c62eb94ba286d040d21bd
16.exe" with arguments "" with pid 2588
2024-11-05 11:00:35,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-05 11:00:35,265 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2588
192.168.56.1 - - [05/Nov/2024 11:00:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [05/Nov/2024 11:00:37] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:00 AM