MALICIOUS

Classifications: Backdoor | Keylogger | Injector

Threat Names: Gen:Variant.Razy.854557

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
Sample Name	**Nure Setup 0.2.1.exe**
ID	#334078
MD5	e1476603c8671d988432c22e3988e238
SHA1	60db15cb48cd6c63073f2d067f75a1d091c21843
SHA256	34de8177caa508681d06648ddecd62c2edc7206830e683d6f0cc1cc3d5e28603
File Size	114593.48 KB
Report Created	2021-03-31 19:45 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (27 rules, 76 matches)

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the dropped file C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra\win32\nure-helper.exe as "Gen:Variant.Razy.854557".			
4/5	Injection	Writes into the memory of another running process	1	Injector
	• (Process #3) nure.exe modifies memory of (process #5) cmd.exe.			
3/5	Discovery	Reads network configuration	2	-
	• (Process #3) nure.exe reads the current network configuration through the host.conf file. • (Process #10) nure.exe reads the current network configuration through the host.conf file.			
3/5	Hide Tracks	Hides data in extended file attributes	1	-
	• (Process #4) nure.exe sets extended file attributes for "\Device\ConDrv\Connect" to possibly hide the file.			
2/5	Anti Analysis	Tries to detect debugger	2	-
	• (Process #3) nure.exe tries to detect a debugger via API "IsDebuggerPresent". • (Process #3) nure.exe tries to detect a debugger via API "CheckRemoteDebuggerPresent".			
2/5	Defense Evasion	Sends control codes to connected devices	1	-
	• (Process #3) nure.exe controls device "\\.\USB#ROOT_HUB20#4&32CF2352&0#{F18A0E88-C30C-11D0-8815-00A0C906BED8}" through API DeviceIOControl.			
2/5	Discovery	Reads network adapter information	2	-
	• (Process #3) nure.exe reads the network adapters' addresses by API. • (Process #10) nure.exe reads the network adapters' addresses by API.			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #7) nure-helper.exe tries to detect "wine" by calling GetProcAddress() on "wine_get_version".			
2/5	Anti Analysis	Delays execution	2	-
	• (Process #3) nure.exe has a thread which sleeps more than 5 minutes. • (Process #7) nure-helper.exe has a thread which sleeps more than 5 minutes.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	9	-
	• (Process #4) nure.exe makes a direct system call to "NtOpenFile". • (Process #4) nure.exe makes a direct system call to "NtMapViewOfSection". • (Process #4) nure.exe makes a direct system call to "NtQueryAttributesFile". • (Process #4) nure.exe makes a direct system call to "NtOpenThreadToken". • (Process #4) nure.exe makes a direct system call to "NtOpenProcessToken". • (Process #4) nure.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #4) nure.exe makes a direct system call to "NtCreateFile". • (Process #4) nure.exe makes a direct system call to "NtSetInformationThread". • (Process #4) nure.exe makes a direct system call to "NtSetInformationFile".			
2/5	Network Connection	Sets up server that accepts incoming connections	3	Backdoor

• (Process #7) nure-helper.exe starts a TCP server listening on port 49713.
• (Process #7) nure-helper.exe starts a TCP server listening on port 49715.
• (Process #7) nure-helper.exe starts a TCP server listening on port 49716.

1/5	Mutex	Creates mutex	2	-

• (Process #1) nure setup 0.2.1.exe creates mutex with name "f245fb50-b1fe-521e-8ee2-704cd498cf77".
• (Process #3) nure.exe creates mutex with name "Local\AtomProcessSingletonStartup!".

1/5	Discovery	Enumerates running processes	2	-

• (Process #1) nure setup 0.2.1.exe enumerates running processes.
• (Process #3) nure.exe enumerates running processes.

1/5	Privilege Escalation	Enables process privilege	1	-

• (Process #1) nure setup 0.2.1.exe enables process privilege "SeSecurityPrivilege".

1/5	Hide Tracks	Creates process with hidden window	3	-

• (Process #3) nure.exe starts (process #4) nure.exe with a hidden window.
• (Process #3) nure.exe starts (process #5) cmd.exe with a hidden window.
• (Process #7) nure-helper.exe starts (process #8) cmd.exe with a hidden window.

1/5	Obfuscation	Reads from memory of another process	1	-

• (Process #3) nure.exe reads from (process #4) nure.exe.

1/5	Obfuscation	Creates a page with write and execute permissions	2	-

• (Process #3) nure.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.
• (Process #3) nure.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").

1/5	Discovery	Reads system data	1	-

• (Process #7) nure-helper.exe reads the cryptographic machine GUID from registry.

1/5	Input Capture	Monitors keyboard input	1	Keylogger

• (Process #3) nure.exe frequently reads the state of a keyboard key by API.

1/5	Obfuscation	Resolves API functions dynamically	6	-

• (Process #1) nure setup 0.2.1.exe resolves 51 API functions by name.
• (Process #3) nure.exe resolves 327 API functions by name.
• (Process #7) nure-helper.exe resolves 73 API functions by name.
• (Process #4) nure.exe resolves 380 API functions by name.
• (Process #10) nure.exe resolves 85 API functions by name.
• (Process #11) nure.exe resolves 83 API functions by name.

1/5	Execution	Drops binary file	1	-

• Drops file C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\MacOS\terminal-notifier.

1/5	Execution	Drops PE file	20	-

• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra\win32\nure-helper.exe".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\System.dll".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\StdUtils.dll".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\SpiderBanner.dll".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\nsProcess.dll".
• Drops file C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\nsis7z.dll.
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\d3dcompiler_47.dll".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\ffmpeg.dll".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\libEGL.dll".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\libGLESv2.dll".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\Nure.exe".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\notifu\notifu.exe".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\notifu\notifu64.exe".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\snoreToast\SnoreToast.exe".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\elevate.exe".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\swiftshader\libEGL.dll".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\swiftshader\libGLESv2.dll".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\vk_swiftshader.dll".
• (Process #1) nure setup 0.2.1.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\vulkan-1.dll".
• Drops file C:\Users\RDhJ0CNFevzX\AppData\Local\nure-updater\installer.exe.

1/5	Execution	Executes dropped PE file	3	-

• Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra\win32\nure-helper.exe".
• Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\Nure.exe".
• Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\nure-updater\installer.exe".

1/5	System Modification	Creates an unusually large number of files	1	-

• (Process #1) nure setup 0.2.1.exe creates an above average number of files.

1/5	Network Connection	All network connection attempts failed	1	-

• Host "193.38.55.46" is unavailable.

1/5	Network Connection	Connects to remote host	4	-

• (Process #7) nure-helper.exe accepts an incoming TCP connection from host "193.38.55.46:3000".
• (Process #7) nure-helper.exe accepts an incoming TCP connection from host "193.38.55.46:3001".
• (Process #7) nure-helper.exe opens an outgoing TCP connection to host "193.38.55.46:3000".
• (Process #7) nure-helper.exe opens an outgoing TCP connection to host "193.38.55.46:3001".

1/5	Network Connection	Tries to connect using an uncommon port	2	-

• (Process #7) nure-helper.exe tries to connect to TCP port 3000 at 193.38.55.46.
• (Process #7) nure-helper.exe tries to connect to TCP port 3001 at 193.38.55.46.

-	Trusted	Known clean file	100	-

• File "C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\System.dll" is a known clean file.
• File "C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\StdUtils.dll" is a known clean file.
• File "C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\SpiderBanner.dll" is a known clean file.
• File "C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\nsProcess.dll" is a known clean file.
• File "C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\nsis7z.dll" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\chrome_100_percent.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\chrome_200_percent.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\LICENSE.electron.txt" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\LICENSES.chromium.html" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\am.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ar.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\bg.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\bn.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ca.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\cs.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\da.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\de.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\el.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\en-GB.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\en-US.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\es-419.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\es.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\et.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fa.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fi.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fil.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fr.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\gu.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\he.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hi.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hr.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hu.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\id.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\it.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ja.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\kn.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ko.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\lt.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\lv.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ml.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\mr.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ms.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\nb.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\nl.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pl.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pt-BR.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pt-PT.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ro.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ru.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sk.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sl.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sr.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sv.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sw.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ta.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\te.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\th.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\tr.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\uk.pak" is a known clean file.
• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\vi.pak" is a known clean file.

Remarks

Max Binlog Size Reached (0x02000046): The maximum binlog size was reached. The analysis was terminated prematurely.

Anti Virus Error (0x0060000E): Some of the analysis artifacts were not scanned by Built-in AV due to an error. Check the logs or contact support for further information.

Anti-Sleep Triggered (0x0200000E): The overall sleep time of all monitored processes was truncated from "1 day, 9 hours, 15 minutes, 48 seconds" to "12 minutes, 10 seconds" to reveal dormant functionality.

Mitre ATT&CK Matrix

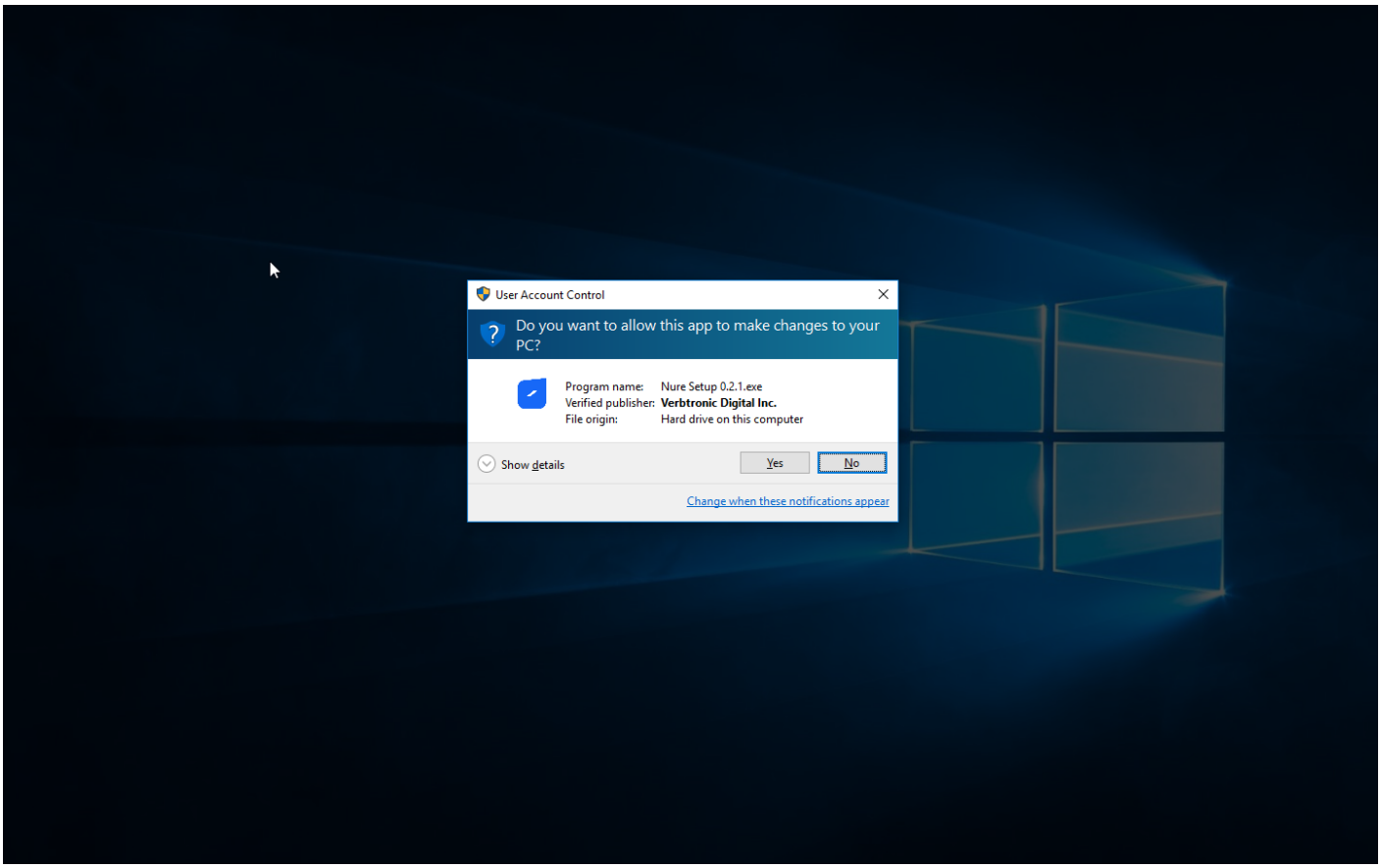
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
-	-	-	-	-	-	#T1057 Process Discovery	-	-	-	-	-
-	-	-	-	-	-	#T1016 System Network Configuration Discovery	-	-	-	-	-
-	-	-	-	#T1143 Hidden Window	-	-	-	-	-	-	-
-	-	-	-	#T1045 Software Packing	-	-	-	-	-	-	-
-	-	-	-	#T1497 Virtualization /Sandbox Evasion	-	#T1497 Virtualization /Sandbox Evasion	-	-	-	-	-
-	-	-	-	-	-	#T1082 System Information Discovery	-	-	-	-	-
-	-	-	-	-	-	#T1012 Query Registry	-	-	-	-	-
-	-	-	-	#T1096 NTFS File Attributes	-	-	-	-	-	-	-
-	-	-	-	-	#T1056 Input Capture	-	-	#T1056 Input Capture	-	-	-
-	-	-	-	-	-	-	-	-	#T1065 Uncommonly Used Port	-	-

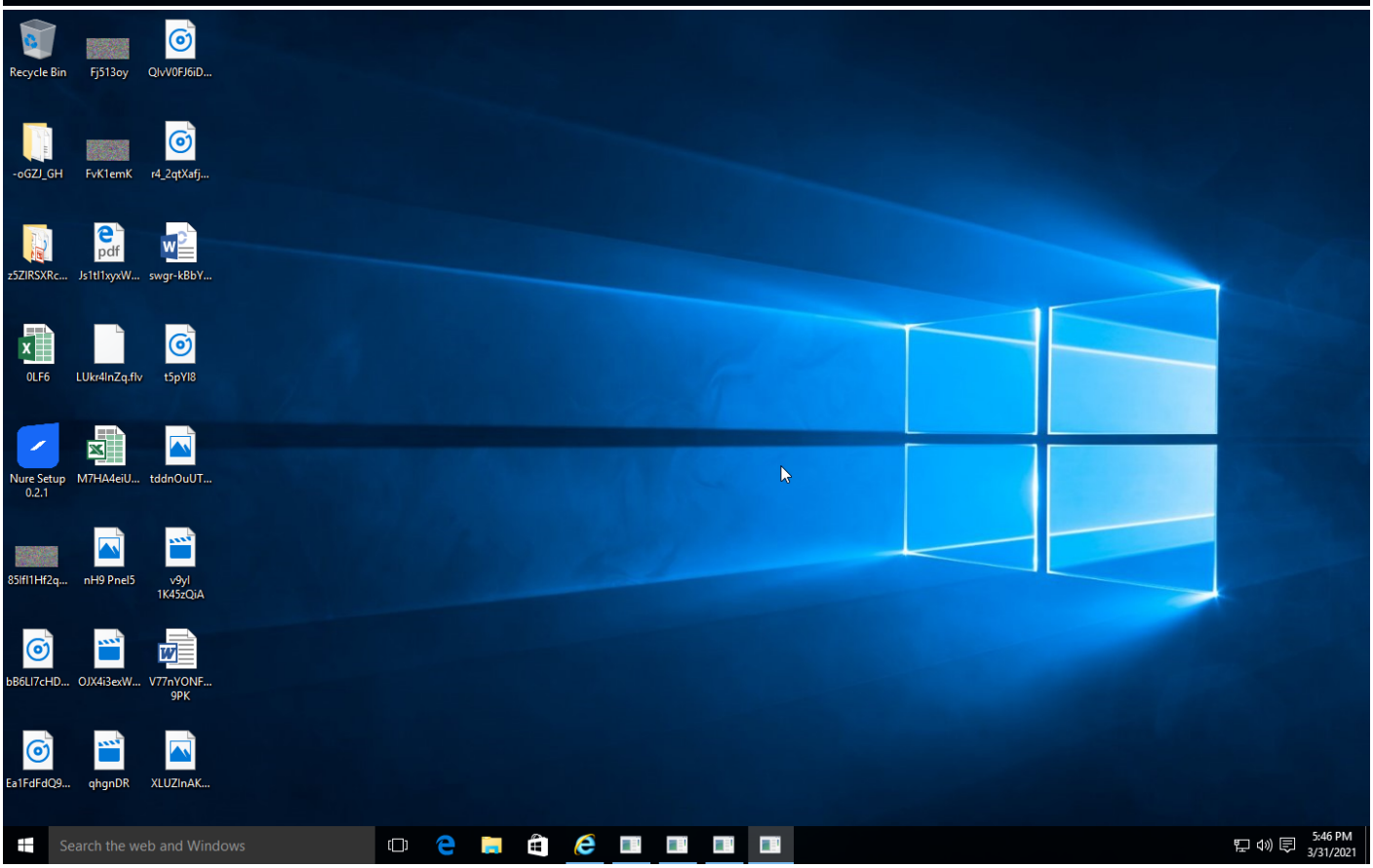
Sample Information

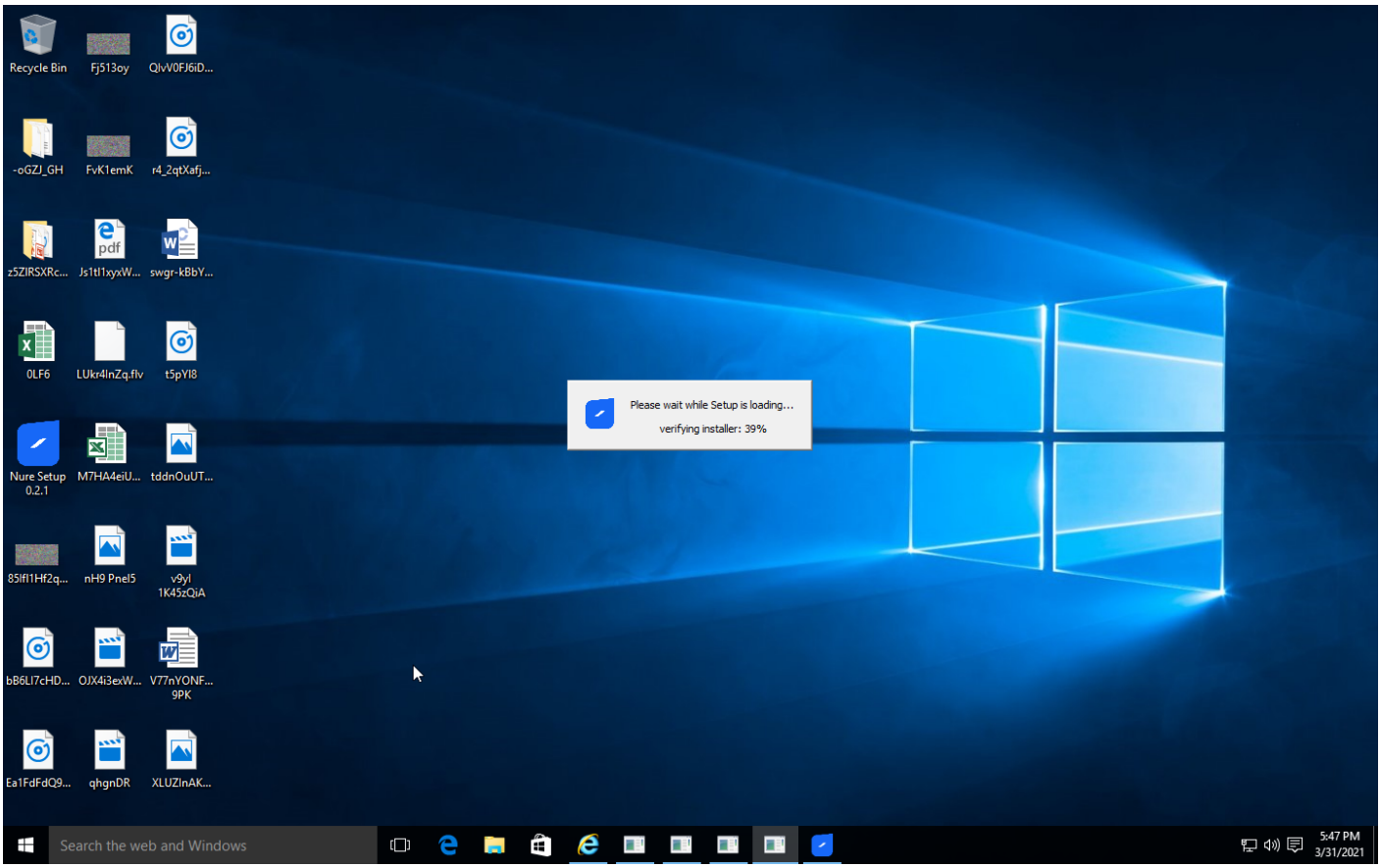
ID	1004853
MD5	e1476603c8671d988432c22e3988e238
SHA1	60db15cb48cd6c63073f2d067f75a1d091c21843
SHA256	34de8177caa508681d06648ddecd62c2edc7206830e683d6f0cc1cc3d5e28603
SSDeep	3145728:APwxKCODEtVyuqG29HQBiLINBbcW+SsXecroU5:rKCttVy7GI6+5r3
ImpHash	b34f154ec913d2d2c435cbd644e91687
Filename	Nure Setup 0.2.1.exe
File Size	114593.48 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

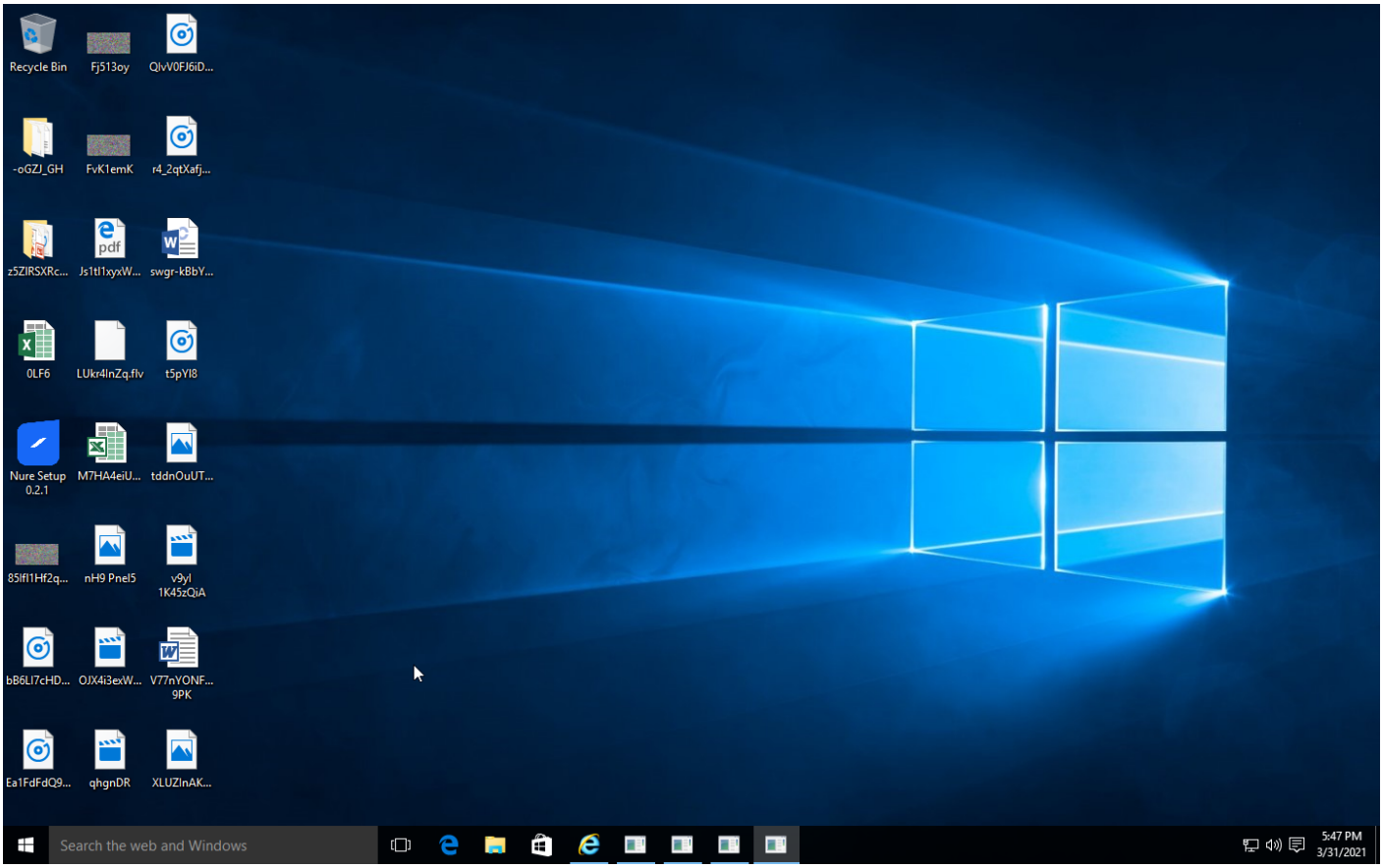
Analysis Information

Creation Time	2021-03-31 19:45 (UTC+2)
Analysis Duration	00:03:40
Termination Reason	Maximum binlog size reached
Number of Monitored Processes	9
Execution Successfull	False
Reputation Analysis Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


User Account Control
Do you want to allow this app to make changes to your PC?
Program name: Nure Setup 0.2.1.exe
Verified publisher: Verbtronic Digital Inc.
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
Fj513oy
QlvV0FJ6iD...
-oGZJ_GH
FvK1emK
r4_2qtXafj...
z5ZIRSXRc...
Js1tf1xyxW...
swgr-kBbY...
0LF6
LUkr4lnZq.flv
t5pYI8
Nure Setup 0.2.1
M7HA4eiU...
tddnOuUT...
85lf11Hf2q...
nH9 PneI5
v9yl 1K45zQiA
bB6LI7cHD...
OJX4i3exW...
V77nYONF... 9PK
Ea1FdFdQ9...
qhgnDR
XLUZlnAK...
Search the web and Windows
5:46 PM
3/31/2021





Screenshots trunkated.

NETWORK

General

0 bytes total sent

0 bytes total received

2 ports 3000, 3001

1 contacted IP addresses

213 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes recivied

DNS Requests

-

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://code.google.com/p/angleproject/				0 bytes	N/A
GET	http://lcamtuf.coredump.cx/afl/				0 bytes	N/A
GET	http://source.android.com				0 bytes	N/A
GET	http://developer.android.com/tools/extras/support-library.html				0 bytes	N/A
GET	http://developer.android.com/sdk/index.html				0 bytes	N/A
GET	http://webkit.org				0 bytes	N/A
GET	http://software.blackmagicdesign.com/DeckLink/v10.7/Blackmagic_DeckLink_SDK_10.7.zip				0 bytes	N/A
GET	http://www.chromium.org/blink				0 bytes	N/A
GET	http://www.daemonology.net/bsdiff/				0 bytes	N/A
GET	http://lxr.mozilla.org/mozilla/source/toolkit/mozapps/update/src/updater/				0 bytes	N/A

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://code.google.com/p/google-axs-chrome/				0 bytes	N/A
GET	http://github.com/google/closure-compiler				0 bytes	N/A
GET	http://caminobrowser.org/				0 bytes	N/A
GET	http://r8.googlesource.com/r8				0 bytes	N/A
GET	http://www.opensource.apple.com/				0 bytes	N/A
GET	http://code.google.com/p/data-race-test/wiki/DynamicAnnotations				0 bytes	N/A
GET	http://www.netlib.org/fdlibm/				0 bytes	N/A
GET	http://ffmpeg.org/				0 bytes	N/A
GET	http://findbugs.sourceforge.net/				0 bytes	N/A
GET	http://downloads.xiph.org/releases/flac/flac-1.3.1.tar.xz				0 bytes	N/A
GET	http://www.freetype.org/				0 bytes	N/A
GET	http://android-gifview.googlecode.com/svn/!svn/bc/8/trunk/				0 bytes	N/A
GET	http://code.google.com/p/google-jstemplate/				0 bytes	N/A
GET	http://harfbuzz.org				0 bytes	N/A
GET	http://hunspell.sourceforge.net/				0 bytes	N/A
GET	http://www.ijg.org				0 bytes	N/A
GET	http://developer.mozilla.org/en-US/docs/Accessibility/AT-APIs				0 bytes	N/A
GET	http://code.google.com/p/atinject/				0 bytes	N/A
GET	http://jinja.pocoo.org/				0 bytes	N/A
GET	http://www.khronos.org/registry				0 bytes	N/A
GET	http://ltp.sourceforge.net/coverage/lcov.php				0 bytes	N/A
GET	http://brltty.app				0 bytes	N/A
GET	http://libcxx.llvm.org/				0 bytes	N/A
GET	http://libcxxabi.llvm.org/				0 bytes	N/A
GET	http://libevent.org/				0 bytes	N/A
GET	http://llvm.org/docs/LibFuzzer.html				0 bytes	N/A
GET	http://libpng.org/				0 bytes	N/A

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.freedesktop.org/wiki/Software/systemd/				0 bytes	N/A
GET	http://libusb.org				0 bytes	N/A
GET	http://www.webmproject.org				0 bytes	N/A
GET	http://xmlsoft.org				0 bytes	N/A
GET	http://xmlsoft.org/XSLT				0 bytes	N/A
GET	http://code.google.com/p/libyuv/				0 bytes	N/A
GET	http://www.logilab.org/				0 bytes	N/A
GET	http://www.7-zip.org/sdk.html				0 bytes	N/A
GET	http://www.mesa3d.org/				0 bytes	N/A
GET	http://www.mozilla.org/projects/nspr/				0 bytes	N/A
GET	http://www.mozilla.org/projects/security/pki/nss/				0 bytes	N/A
GET	ftp://sourceware.org/pub/newlib/newlib-2.0.0.tar.gz				0 bytes	N/A
GET	http://cgit.freedesktop.org/~aplattner/nvidia-settings/				0 bytes	N/A
GET	http://cristal.univ-lille.fr/~casiez/1euro/				0 bytes	N/A
GET	http://www.openh264.org/				0 bytes	N/A
GET	http://www.azillionmonkeys.com/qed/hash.html				0 bytes	N/A
GET	http://code.google.com/p/pdfium/				0 bytes	N/A
GET	http://www.dabeaz.com/ply/ply-3.11.tar.gz				0 bytes	N/A
GET	http://www.polymer-project.org				0 bytes	N/A
GET	http://www.pylint.org/				0 bytes	N/A
GET	http://schema.org/version/6.0/schema.jsonld				0 bytes	N/A
GET	http://code.google.com/p/smhasher/				0 bytes	N/A
GET	http://google.github.io/snappy/				0 bytes	N/A
GET	http://devel.freebsoft.org/speechd				0 bytes	N/A
GET	http://www.strongtalk.org/				0 bytes	N/A
GET	http://www.suitable.com/tools/smslib.html				0 bytes	N/A
GET	http://gperftools.googlecode.com/				0 bytes	N/A
GET	http://www.chromium.org				0 bytes	N/A

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.linux-usb.org/usb-ids.html				0 bytes	N/A
GET	http://trevp.net/tlslite/				0 bytes	N/A
GET	http://mxr.mozilla.org/comm-central/source/mozilla/netwerk/base/src/nsURLParsers.cpp				0 bytes	N/A
GET	http://github.com/sctplab/usrsctp				0 bytes	N/A
GET	http://git.linuxtv.org/v4l-utils.git				0 bytes	N/A
GET	http://code.google.com/p/v8				0 bytes	N/A
GET	http://valgrind.org				0 bytes	N/A
GET	http://webkit.org/				0 bytes	N/A
GET	http://www.webmproject.org/code/				0 bytes	N/A
GET	http://developers.google.com/speed/webp				0 bytes	N/A
GET	http://www.webrtc.org				0 bytes	N/A
GET	http://freedesktop.org				0 bytes	N/A
GET	http://www.freedesktop.org/wiki/Software/xdg-user-dirs				0 bytes	N/A
GET	http://tukaani.org/xz/				0 bytes	N/A
GET	http://zlib.net/				0 bytes	N/A
GET	https://github.com/abseil/abseil-cpp				0 bytes	N/A
GET	https://raw.githubusercontent.com/GoogleChrome/accessibility-developer-tools/master/dist/js/axs_testing.js				0 bytes	N/A
GET	https://developer.android.com/jetpack/androidx				0 bytes	N/A
GET	https://aomedia.googlesource.com/aom/				0 bytes	N/A
GET	https://developer.android.com/topic/libraries/architecture/index.html				0 bytes	N/A
GET	https://android.googlesource.com/platform/bionic/+/master/libc/				0 bytes	N/A
GET	https://chromium.googlesource.com/chromium/src.git/+/master/third_party/android_crazy_linker/				0 bytes	N/A
GET	https://developer.android.com/reference/android/util/FloatProperty.html				0 bytes	N/A

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://maven.google.com/androidx/multidex/multidex/2.0.0/multidex-2.0.0.aar				0 bytes	N/A
GET	https://android.googlesource.com/platform/frameworks/support				0 bytes	N/A
GET	https://android.googlesource.com/platform/packages/apps/Settings/				0 bytes	N/A
GET	https://android.googlesource.com/platform/frameworks/base				0 bytes	N/A
GET	https://github.com/google-ar/arcore-android-sdk				0 bytes	N/A
GET	https://developers.google.com/ar/develop/java/enable-arcore#dependencies				0 bytes	N/A
GET	https://github.com/dequelabs/axe-core/				0 bytes	N/A
GET	https://boringssl.googlesource.com/boringssl				0 bytes	N/A
GET	https://github.com/liblouis/liblouis				0 bytes	N/A
GET	https://chromium.googlesource.com/breakpad/breakpad				0 bytes	N/A
GET	https://github.com/google/brotli				0 bytes	N/A
GET	https://github.com/rianhunter/zxcvbn-cpp				0 bytes	N/A
GET	https://github.com/google/cityhash				0 bytes	N/A
GET	https://github.com/google/compact_enc_det				0 bytes	N/A
GET	https://github.com/google/cld3				0 bytes	N/A
GET	https://crashpad.chromium.org/				0 bytes	N/A
GET	https://github.com/google/crc32c				0 bytes	N/A
GET	https://github.com/d3/d3				0 bytes	N/A
GET	https://github.com/google/dagger				0 bytes	N/A
GET	https://code.videolan.org/videolan/dav1d				0 bytes	N/A
GET	https://dawn.googlesource.com/dawn				0 bytes	N/A
GET	https://github.com/y-256/libdivsufsort				0 bytes	N/A
GET	https://github.com/chromium/dom-distiller				0 bytes	N/A
GET	https://github.com/googlei18n/emoji-segmenter				0 bytes	N/A

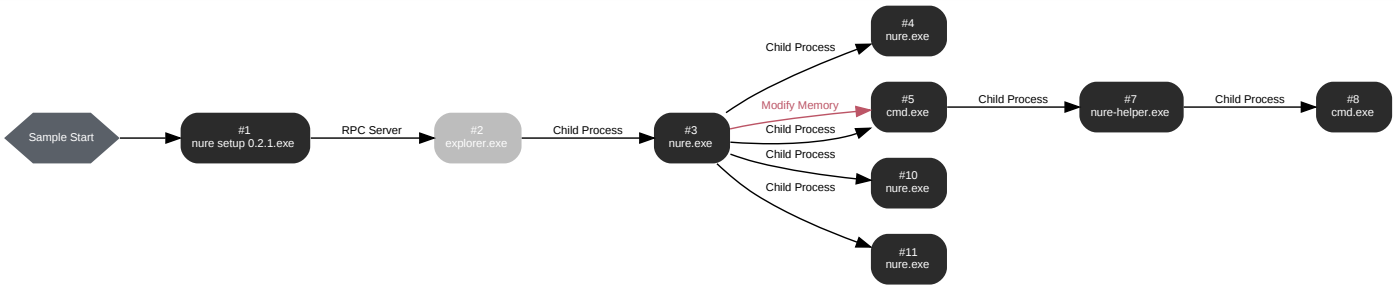
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://source.android.com/				0 bytes	N/A
GET	https://github.com/libexpat/libexpat				0 bytes	N/A
GET	https://github.com/mit-plv/fiat-crypto				0 bytes	N/A
GET	https://github.com/GPUOpen-Effects/FidelityFX-SPD				0 bytes	N/A
GET	https://github.com/google/flatbuffers				0 bytes	N/A
GET	https://fusejs.io				0 bytes	N/A
GET	https://github.com/google/closure-library				0 bytes	N/A
GET	https://github.com/google/double-conversion				0 bytes	N/A
GET	https://github.com/google/ink				0 bytes	N/A
GET	https://github.com/googlei18n/google-input-tools.git				0 bytes	N/A
GET	https://github.com/google/google-toolbox-for-mac				0 bytes	N/A
GET	https://pki.goog/roots.pem				0 bytes	N/A
GET	https://github.com/google/glog				0 bytes	N/A
GET	https://github.com/grpc/grpc				0 bytes	N/A
GET	https://github.com/google/guava				0 bytes	N/A
GET	https://github.com/googlevr/gvr-android-sdk				0 bytes	N/A
GET	https://github.com/Microsoft/webauthn/				0 bytes	N/A
GET	https://android.googlesource.com/platform/external/hyphenation-patterns/				0 bytes	N/A
GET	https://github.com/LinuxA11y/IAccessible2				0 bytes	N/A
GET	https://github.com/unicode-org/icu				0 bytes	N/A
GET	https://chromium.googlesource.com/deps/inspector_protocol/				0 bytes	N/A
GET	https://github.com/googlei18n/libphonenumber/				0 bytes	N/A
GET	https://github.com/google/j2objc/				0 bytes	N/A
GET	https://github.com/open-source-parsers/jsoncpp				0 bytes	N/A
GET	https://github.com/KhronosGroup/glslang				0 bytes	N/A
GET	https://github.com/google/leveldb.git				0 bytes	N/A

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://github.com/googlei18n/libaddressinput				0 bytes	N/A
GET	https://github.com/AOMediaCodec/libavif				0 bytes	N/A
GET	https://skia.googlesource.com/libgifcodec/				0 bytes	N/A
GET	https://chromium.googlesource.com/chromiumos/platform2/libipp				0 bytes	N/A
GET	https://chromium.googlesource.com/external/webrtc				0 bytes	N/A
GET	https://github.com/libjpeg-turbo/libjpeg-turbo/				0 bytes	N/A
GET	https://github.com/google/libprotobuf-mutator				0 bytes	N/A
GET	https://git.gnome.org/browse/libsecret/				0 bytes	N/A
GET	https://github.com/cisco/libsrtp				0 bytes	N/A
GET	https://llvm.org/svn/llvm-project/libunwind/trunk/				0 bytes	N/A
GET	https://github.com/airbnb/lottie-web				0 bytes	N/A
GET	https://github.com/material-components/material-components-android				0 bytes	N/A

Reduced dataset

BEHAVIOR

Process Graph



Process #1: nure setup 0.2.1.exe

ID	1
Filename	c:\users\rdhj0cnfevzx\desktop\nure setup 0.2.1.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\Nure Setup 0.2.1.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 80618, Reason: Analysis Target
Unmonitor End Time	End Time: 205386, Reason: Terminated
Monitor Duration	124.77s
Return Code	0
PID	2368
Parent PID	2104
Bitness	32 Bit

Dropped Files (236)

Filename	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\System.dll	12.00 KB	3eb38ae99653a7dbc724132ee240f6e5c4af4bfe7c01d31d23faf373f9f2eaca	✕
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\StdUtils.dll	100.00 KB	b72e9013a6204e9f01076dc38dabbf30870d44dfc66962adbf73619d4331601e	✕
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\SpiderBanner.dll	9.00 KB	996a259e53ca18b89ec36d038c40148957c978c0fd600a268497d4c92f882a93	✕
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\nsProcess.dll	4.50 KB	30c6c3dd3cc7fcea6e6081ce821adc7b2888542dae30bf00e881c0a105eb4d11	✕
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\app-64.7z	10240.00 KB	ba487d51c0656b9324c2a0c05c6088668a6c9981e4cf173279e09367d0511fcc	✕
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\nsis7z.dll	424.00 KB	b393f05e8ff919ef071181050e1873c9a776e1a0ae8329aefff7007d0cadf592	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\chrome_100_percent.pak	121.46 KB	5ae14147992a92548bcad76867dd88cdfcdb69d951c8720920cce6fb135e3189	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\chrome_200_percent.pak	181.51 KB	dd8146b2ee289e4d54a4a0f1fd3b2f61b979c6a2baaba96a406d96c3f4fdb33b	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\icudtl.dat	10240.00 KB	4a33fabd88f3bc0f2bd32a70f5e99efea5b1ccebe9bef0291a28e6bd6006537d	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\LICENSE.electron.txt	1.04 KB	c44607a865e7a6db05552baa0ef71f9887d96acd00d123854b44996bc27c0e33	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\LICENSES.chromium.html	4605.23 KB	03f1d245e6a2facca9edbdaad108169e0765dd9101875bc2d123797994b9e80f	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\am.pak	142.12 KB	e9c78c2410d5c81e0cd5d122462e852143eea15ca69cd01b85322cede1e10806	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ar.pak	144.86 KB	1cdef40ba8343e7f826c2020906915efaac5e56f543cd2ed6ebf704882525d8c	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\bg.pak	154.55 KB	1bb8c5ce9215d42ba9ceec52f86fbff46df668ce48ff56bd1cbe96adadf4922c	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\bn.pak	203.77 KB	f7d704207cb3340f1ace2f2e5af031e816bb86e4bf3f665907d837d094bba37a	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ca.pak	99.35 KB	14e99f4d94868a454f40ee8e0f62d056e0abb303caf6e184a9a61bdec18ac271	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\cs.pak	101.63 KB	9651b8f3304c70d96dcca76cfffad90ce8afcab6231ffd8e4e9beade3d510841	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\da.pak	92.82 KB	1d1a3e38ddf282969bca2a5d893b3db4a0aed10b53eab37bb2dad7d2d18c94de	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\de.pak	98.95 KB	e71f4320553f65cfd0356a4b30f3aec2eec7b4fd327866d528917b9909cfa761	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\el.pak	172.39 KB	a3431d3ac720f871c33d7e522cf506b2fa8ea1872bac02a4b4b427a6d063af38	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\en-GB.pak	82.33 KB	c4fdfa9c6f30ad657bf12ccb95f70542a0fade45d8490259a4507629f4b33299	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\en-US.pak	83.06 KB	d1d3f892be16329c79f9a8ee8c5fa1c9fb46d17edfeb56a3d9407f9d7587a0de	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\es-419.pak	97.18 KB	64df687bbb37bcd92e609f7e3bf950ee5629b693ff8636607285f5753b1bdaae	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\es.pak	99.39 KB	eb22282dbf211f64142ef4dfac2c1d811d65decd617c4a3d1c892967dc72ac07	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\et.pak	88.94 KB	b3baf825f9b237565260ba2935fe9acf2ae381e3bfc6fbf837dbfe6fb83314b5	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fa.pak	138.70 KB	8ea08e9874892edefcbdc55c393dc00fe451f3c7f29b57d7105377349eb4bfc4	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fi.pak	91.43 KB	bfc24d41ea8e362bb1a18c11860d2217fc100b1a422cf54629c7d0c6640d5ed7	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fil.pak	101.16 KB	75d473ffd351a828bd7854067ad986908efefdfb75800650587b8bef09f9ff2a	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fr.pak	107.33 KB	b387afb8c8ae3c3ce90728fb7eb39a39ec789c6e7bfe4dbd2b5d49e72434db1f	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\gu.pak	194.66 KB	a49597e67fcf93448c89e07f9cc3519b3b1b77505bc30adf3f25c250718eec0c	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\he.pak	122.21 KB	7420e94f19bd61f33950e120f29c9783305f218d089f0a7d3ea3451655cdda1f	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hi.pak	201.34 KB	acc53ca41a9a04a57c1f18fea58cc4329b8add0ded37f9f7d7a73584a910d6c9	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hr.pak	96.83 KB	e55d011ac0cc50d33bf22d43a9c5a6b59f5c31bd2884789efee124929be9a7fa	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hu.pak	103.95 KB	030cbf833a350946959afa0d2b699512c0b715ff7b38b613bcd16b15282b940a	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\id.pak	89.06 KB	d12d87d003bda037b411daab09d1698671f8284e4297ffc08b0558749df6495b	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\it.pak	96.68 KB	266f501703d3899000d5eb60d55ccc8f59f186e862a4a9a34910e81699ea289e	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ja.pak	116.93 KB	4d0910d196b6b5652e3e5d677ddb048b8dae1ec974593484df2838093c96fed7	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\kn.pak	223.73 KB	f25c8b41249c8f54224702795644c80bb5a7eaaeb6f0af5b6a1048960a27c827	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ko.pak	98.60 KB	99addd110ae7ba9fb37daf5c32ad2815172840764da0c71d0304dc9562951d61	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\lt.pak	105.47 KB	9124dc353864cf6570580ae3afa0a7f09f5e3d32a61e71a64ff4cf824ad4fb29	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\lv.pak	104.35 KB	6861e9a4e8a9f2493f0103afa0f860c280478a64293a6de883ba9cb6a45776f6	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ml.pak	235.08 KB	cc9fd4f2d44df646c6117465f820ad390efbc9cb64eb4ff898a50cdfef8f324c	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\mr.pak	191.24 KB	5f1ffe801f3701434a73d3ad3d04e9fcb6238f0f3b14e9325413910799954543	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ms.pak	91.24 KB	f4f6362d9963b7d244e29e85c7ecda552ff7756621f6efc9f3b6f12940896a81	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\nb.pak	90.02 KB	efc934122d4232276f9f2317e5906517bd91ec2a6d76995fe8aae04eff866a50	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\nl.pak	93.89 KB	4669c10a7fcc8a150a641e73320547ed1b966a92fe78041a860ce4892f79b0cd	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pl.pak	101.95 KB	ce84676f37bf97078b3d087d913a874d3c092f76b729f43d3e9553d3c9754f03	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pt-BR.pak	96.49 KB	7cca8f6ee8b2a19c8ea53b3a2bb2af4ebbb2b8612caba87f581938e7d6aa9f18	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pt-PT.pak	97.23 KB	7f0b86e4f6391e48fd045c8b967a1ad33d9c54f5a6ceda98d800c254dd2ec059	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ro.pak	99.54 KB	60859215a025b95a1ac06333a66d14e1698b28ae31451c999e8adc072401a86a	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ru.pak	157.89 KB	5c93984215f69bc6c7a1430fedbdc619ee6ccc9e491354e3541fdc8ed1947f8b	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sk.pak	103.32 KB	4a09c8f22d1fe71cdfd0149599c59ec3059cd35f7dc8f33f22f967a237f7def1	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sl.pak	98.77 KB	1ed9fc4abb8bef48e0fd5e10a107fb456dcb0c7a275bb789cb0728cfadfdcc42	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sr.pak	148.22 KB	362a50ec28da0af4c6b8e282ad64d45298b939a03883de22c5a33adfa919bc74	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sv.pak	89.98 KB	cfe9ad173d516a3e1855f00f53fcb20a53ade93fef6256e909b0f0da12723cc2	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sw.pak	91.43 KB	26fbb15e26f5a4c44bc0e86326fbff28686c771edd11bda6bfea178364299eaa	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ta.pak	230.33 KB	2363b6a8cce7868830915303dc2825351e7ea9dfd98568e448cd8b71c7ceef90	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\te.pak	213.26 KB	c9f427a4efa5d9835432e3a190e26d684c18c26e13fcda1b7e73d6a7527cfd4f	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\th.pak	183.14 KB	301966a229a09b37e5b2bf12c89522a33144c977411099b81502261c4ca554ad	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\tr.pak	94.80 KB	81694a8258624f82dfbe0af43aa0ce5fdf1304c25a2f6735b972a2a29beb8e15	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\uk.pak	158.48 KB	27d3c996804b4f4c106f12becdaeeb1ce65df53abe12658574852ab7b6643bc1	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\vi.pak	111.74 KB	7f94586012c85732d23b05dbdde2c497326d5fcab87de83aafa3594b614dbd36	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\zh-CN.pak	83.32 KB	44a9dd0a830ce2feeb81523cce7fae8a0a553f05921b34d34c7826d50ac3a1b7	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\zh-TW.pak	83.48 KB	268041a1a95dd540cf7e92a01802b65df8c8d1c80726007da1bb8a9cba6e5414	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources.pak	4898.19 KB	7b953443e3cd54a0a4775528b52fbfe5ebecbc2c71731600ed0999d227969506	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app-update.yml	146 bytes	93ea2cedd1ea49a5dc6eab0c97c422b642edf48cd0b5e65efb8ef865d2628c4d	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar	10240.00 KB	70a861b0a9ac7a34e2338bf24140471684df6ed7d4e8df2019ddd054c625df32	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\dist\index.min.js	34.09 KB	9ea8667cf8d736e27222e589901f95b6749ab9f09cb339bb4b90fd180700f937	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\dist\index.min.js.LICENSE.txt	133 bytes	bf7901cd6cf0fb3d64522c548e8adb561f245de169307f31eca2b5f9c46dde0e	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\example.js	250 bytes	9980e1f206d33d936779cb9d9cc4b499195ebe9d9177724822369f51ffe63013	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\LICENSE	1.04 KB	f71842df80e1cd78d057d41f4f027d8f38755f500f8993f973922ba1bdb1bed8	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\package.json	673 bytes	c362572d0b77ae7c9686c326b475930a7a353c145def38a3ab8029e432a7bce3	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\base-table.json	10.35 KB	a5644d406081ed410f4d6a103972f4e849e092ea673d507769ae1f74f1cc0028	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\constants.js	268 bytes	3c406a345cd43f5a765679668c41101c73bbf1d9be4db2117134e51755af7194	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\index.js	2.80 KB	31a73ecac682c9e11284d1f0a3e808b37a683aa31af2f5b6660017e3b0aa586b	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\int-table.js	284 bytes	6a77cb6cb5219a932bf97f90152b18d3f90c0f1c518a1388d2fefc82208f6359	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\print.js	284 bytes	d9971e3545106957ae0fd9447d2bf39761ad573a2409dc7f1b0a3d7e892acd1c	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\util.js	720 bytes	d16dcaa40f95ed96fc9ef7175600152880335a8960ae2ad4b7072081d40dbdfe	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\varint-table.js	354 bytes	4ee737eee2cce9e65b4425978748d5fefa71c2ac7c3bc9d92fa0d17a6727c828	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\tools\update-table.js	753 bytes	afe42d63569c6829912ab2fb29efa19f29b5cc231d1545c5e1607cdddfcb27f7	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.js	74.88 KB	cff46d23d1b89ab25cd8e1f82d9f01449f0ea2d5d1ad877f446663748df6dc18	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.js.map	82.81 KB	519ed5be2ef4d28d9f8da43c907f03ac27479a94026824e1e29085c15bce0273	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.min.js	33.73 KB	fafb34cdfa41d9dbb5e8007027d37f07ec60bdd7be2574d2c86338193f46068c	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.min.js.map	107.11 KB	015427fe24191037d48e45804a702b0e007c110e6503ca0e6a6721cb32241d00	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\package.json	649 bytes	8fdfef8c3a3dab093d1ac84622accaccb76709b32e02361f44272087299c9f3c	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src\base-table.json	9.82 KB	543a6614d6afd218760a5aa18c1a2adb76511cb2ae783f0e2cafbe76c0d1598c	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src\index.js	2.76 KB	2872182c7dc0bfbee35e65c0b4e5e0c2f1e4a9d77135dc72fdf8b847ac5ee0f9	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src\util.js	683 bytes	8d4123d7dddfbb1c4902734c0e54c366afce71780bb027f1eaa70df7b9ce32be	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\.prettierrc	46 bytes	3ddf7961125a3524f7b06e696cc578259f87f57584b8d69b461873dc13910bf0	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\index.js	1.60 KB	e85060c605820a1acd5fd5aa8b149d4fcd5bef5e498a80392a7a1b68cac43d62	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\lib\checkGrowl.js	536 bytes	6d8fdba983f2589ac744b68437918c63e679a962c4e06007b4f81cb089fdb103	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\lib\utils.js	12.30 KB	97aad0d16fb442b7f7f4262bb7e27d6dc9fc41060ad5d876c36878e4bb011bf2	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\LICENSE	1.04 KB	c5f00acfdb0120b3fafa9869ece941c0a095253770f652927da96352b502df90	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\notifiers\balloon.js	4.27 KB	0d2f65f5bee22e3ef06e3bdfad02dc476e18fc65a7c2572c29f943a1001c5d0c	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\notifiers\growl.js	1.78 KB	33e91460fca7d54f27d7d8d569ecffa6444e03624881e74cb490174093069bbb	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\notifiers\notificationcenter.js	2.45 KB	b4724a9422d5d15d7148ac08a3f299f06443b55a65ed2b5f87a6f4d88f9a122c	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\notifiers\notifysend.js	2.14 KB	6bd1e4987a4cab694503737d1e1f19b9f62af695e85a4e30b8a868313429bdce	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\notifiers\toaster.js	2.44 KB	cd945dd67095b22d9302396bb716ac654c3a79bc336cee486e27fc446ad49041	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\package.json	1.26 KB	adfb2a4b27233cf273b7c68fff2803d79ae10d38601a9d867bed9d2eb857ea9d	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Info.plist	1.77 KB	24a13344667a084f692b2103741f4d4ed8bacf5a53e2abe508f10423c5d6b27f	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\MacOS\terminal-notifier	85.63 KB	2588f4ae2118396419767c388cf2b0a9a5e0cb53ce5d05a07c00f68a97a50215	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\PkgInfo	8 bytes	82502191c9484b04d685374f9879a0066069c49b8acae7a04b01d38d07e8eca0	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Resources\en.lproj\Credits.rtf	436 bytes	b4386fe1cef65cd91e6c8ecc065d117089083f91b7cadbf0c3e5eae20e8b9640	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Resources\en.lproj\InfoPlist.strings	92 bytes	39cf2ee07b7b333e7c179d0bf4d798a5b72af6a4e584f51e642703bbfa4fc828	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Resources\en.lproj\MainMenu.nib	25.19 KB	66a2378cee667b39af5a92676f20f2db13dcf73cf2d23d2a30ef140cdb71f1ad	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Resources\Terminal.icns	360.73 KB	ccfc0f457dbbed2b164a9f708e1a0000fad8f896b0d5332b376e2b748f3ff525	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\snoreToast\LICENSE	7.47 KB	ea8af5e789cb2d4e9b10bce3874982ade163b749b6bfbdb32e2df21c4d106de1	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\terminal-notifier-LICENSE	1.26 KB	77a2769c8dc103f8051ccabab083c18e4cfbd26ba51589f26278c94dee997e56	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\.svgo.yml	1.42 KB	168cc89c100ef9cf95c3ae81f16badcbf607b289a3de0dec9fcfb387ff4c4f4b	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\bin\svgo	55 bytes	e6a786bf92347f485cc9c0641b8710afe2b3e65947c2b292f46ff3a4ce39a0e2	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\css-tools.js	6.44 KB	940ec165700a82e5cf8caf847f6f4853d4beb50ea01ea14999df8a9a669e8648	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo.js	2.58 KB	3f242b971d909eb7e806591cc410b665a9aec897ff30eac9c9d913ad76e46fc7	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\coa.js	18.49 KB	33b7d6a10da711fea14d42d70fa32d61ec48ba725b9abd3d0e57f02868249237	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\config.js	5.99 KB	2ab9c99b50782420c8eb6ab915b8d883016b26aa18db54c73ee41fdc02755e19	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\css-class-list.js	3.18 KB	35d6b21efdf077532af6a1a22b7448dc053b47561b69bcd290210db1ba1fbc47	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\css-select-adapter.js	1.50 KB	aceb6bda2465b65fac984e291a3fd842f06cb64b13dd261b737c0e3c12634548	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\css-style-declaration.js	8.02 KB	0640e9b4b150751d266a61cd8f3f39bd7e51538bc0d0d307dd62395c4166f1e8	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\js2svg.js	7.78 KB	d4ae62eff5227f574ec5a72b130ed2b1ca49c13f8bb54ffe28ea41e7c9cd2da6	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\jsAPI.js	8.95 KB	4f2b487896fc022ebda148d57cfc07722652e0f23d7dc1bbe31623d904f850bf	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\plugins.js	2.10 KB	08e6a754152cfcd81f3af1c6c62e1ad32fa76c1a4726037a7c5b0802c8c6d715	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\svg2js.js	4.43 KB	e5f00eb2a1ceaff6bf57d55f6587fcb7d8afbf53e9fc9ff722ab8e0902a52085	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\tools.js	3.75 KB	cc7028a1dc0123aa13a7a05c9893f4196d04393d3c0eaaf03c1b1b9675950ddd	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\LICENSE	3.49 KB	7b20556d33022fb8475af038919caedecd3d5072db9b336e738390208decaf1e	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\Makefile	524 bytes	710a4a77e6e63fa206a58ff9aee8b9577193db543beda9ca667b1ba7e117ddac	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\package.json	1.18 KB	e8afcef3529ea1c2843c6f2b87d179a2e0c0f6dd40c40b08ba23a5a2fa2666be	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\addAttributesToSVGElement.js	2.02 KB	f3b8014445e6f0cbd27f5945b6ded6062036992a5f281cfe4cc017fee600c47b	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\addClassesToSVGElement.js	1.07 KB	2c03b0d95b48a0ce9b084e82950a6e20dc26cea4f8986183faf0d531ad7a1958	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\cleanupAttrs.js	1.28 KB	9ef0f0d3190ca2f47d166beea59e62e70bd5cc08a4320415598e1af3fa8ee7af	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\cleanupEnableBackground.js	2.25 KB	51c05f8a3e2db6c94e7d9004ba13c23c19361f6ecadd6031a99eaaf0f51036ef	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\cleanupIDs.js	6.58 KB	5e50a7293c635a364c6f1de665ef01a941f9824f0d7df3168fc0f7ff0c2889ea	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\cleanupListOfValues.js	3.52 KB	0ff4e6d679235700ca3b4162fa572db8b12ef3809f38ce23f0105dfd87cb8da4	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\cleanupNumericValues.js	2.50 KB	56adcbee59f4bfdcdf1decb4ae4b2bdda7423acad24e8bc87e5fcc2452b3a26c	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\collapseGroups.js	2.92 KB	e58b50938ca85c26da430a73d614a81006198a35cbef1b031a5d32aa5474b968	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertColors.js	3.58 KB	05f885bdf572ce5c83731aaa47a650913360cda07c3fb3f1d0d8c66b8e1b89dc	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertEllipseToCircle.js	895 bytes	9c89a343297860ab804295614a788aaf9711c3ab6867c54143398f97c6b5e47c	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertPathData.js	30.16 KB	5ca6a349da130fea38f571b5cd6351d5da69c2d7d997e837f6ba5e39955224c4	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertShapeToPath.js	4.39 KB	6f01d924ed540e990c92f1dd7c0e6603443f5ca6dedd34d81bf742f5ff08efe7	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertStyleToAttrs.js	4.10 KB	ef74471cb20352cddbdce7cb395a3595ab98e81904b06db66b37104f52eb0c51	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertTransform.js	10.62 KB	8643aea0bdc9da1d212f732d4b822bcf360ea60ad2bf9927d5ba2b95c1c85f24	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\inlineStyles.js	7.70 KB	387060c09953a1a566b88e6c18df376433a02a1082d1decac3c1db28f1092fc2	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\mergePaths.js	2.08 KB	85df51ed543025cf7228c07cd6d872c48a7552744aa9cca7b7ac3a05a2467981	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\minifyStyles.js	3.97 KB	d8ada72c15d4d8b48152d5b63c19b15fe9697c6a9251e3432ecd408905c152f9	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\moveElemsAttrsToGroup.js	3.31 KB	09cc62c0fd49d94af79b115a02ed1061e3df78a44031fddd24ad327854908de4	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\moveGroupAttrsToElems.js	1.81 KB	2afe183c1debcf134b87a1c8825a04916541a5cb5011251c910a1cd57667ccf0	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\prefixIds.js	5.41 KB	6262052097fc0fc77f25c1b73bf329d54cdc62f25c4bd72bbef69895fc502370	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\removeAttributesBySelector.js	1.87 KB	73b405c018d768962d2903061be50bc33cd6dea72980db054d6f18bed8c7427f	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\removeAttrs.js	4.06 KB	5f91280acabf49187c60f9061d9e4d496d6d8a9aae445465175a6b70369e7dc8	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\removeComments.js	508 bytes	9dcfaea9fe169527a1c101ae86d3df0ee97dae75d8d0814d62fba2c8147380ea	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\removeDesc.js	767 bytes	234a1abd1fcfbac2dc4a3d4ea4878d491359b853a1125aed1b8f503229d28006	✕
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\removeDimensions.js	1.30 KB	071130a0b12267c954f0cb585af5ed1b7865a8a34a96023e80743ae49dabd44a	✕

Reduced dataset

Host Behavior

Type	Count
System	455
Module	751
File	7127
Window	25
Mutex	1
Registry	29
Process	110
Environment	1
User	1
-	31
COM	5

Process #2: explorer.exe

ID	2
Filename	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192942, Reason: RPC Server
Unmonitor End Time	End Time: 303008, Reason: Terminated by Timeout
Monitor Duration	110.07s
Return Code	Unknown
PID	2104
Parent PID	18446744073709551615
Bitness	64 Bit

Process #3: nure.exe

ID	3
Filename	c:\users\rdhj0cnfevzx\appdata\local\programs\nure\nure.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\Nure.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\
Monitor Start Time	Start Time: 206457, Reason: Child Process
Unmonitor End Time	End Time: 303008, Reason: Terminated by Timeout
Monitor Duration	96.55s
Return Code	Unknown
PID	1748
Parent PID	2104
Bitness	64 Bit

Host Behavior

Type	Count
Module	909
File	334
System	623
Environment	843
-	102
Registry	116
Process	224
-	29
Window	19
Mutex	87
-	8
COM	22
-	573
User	5
-	86
-	1
Keyboard	467

Process #4: nure.exe

ID	4
Filename	c:\users\rdhj0cnfevzx\appdata\local\programs\nure\nure.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\Nure.exe" --type=gpu-process --field-trial-handle=1540,14212168910224858381,438... ...AAAAAAAAAAAAUAAAAQAAAAAAAAAAAAAAAGAAAAEAAAAAAAAAABAAAABQAAABAAAAAAAAAAAQAAAAYAAAA= --mojo-platform-channel-handle=1556 /prefetch:2
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\
Monitor Start Time	Start Time: 236570, Reason: Child Process
Unmonitor End Time	End Time: 303008, Reason: Terminated by Timeout
Monitor Duration	66.44s
Return Code	Unknown
PID	4196
Parent PID	1748
Bitness	64 Bit

Host Behavior

Type	Count
File	360
Module	1798
System	25
Environment	19
-	83
Registry	6
-	9
COM	1

Process #5: cmd.exe

ID	5
Filename	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /d /s /c ""C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra\win32\nure-helper.exe""
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\
Monitor Start Time	Start Time: 239064, Reason: Child Process
Unmonitor End Time	End Time: 303008, Reason: Terminated by Timeout
Monitor Duration	63.94s
Return Code	Unknown
PID	3224
Parent PID	1748
Bitness	64 Bit

Injection Information (1)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#3: c:\users\rdhj0cnfevzx\appdata\local\programs\nure\nure.exe	0xc40	0x7ff8463f53a0(140704307172256)	0x10	✓	1

Host Behavior

Type	Count
Module	8
Registry	17
File	6
Environment	14
System	1
Process	1

Process #7: nure-helper.exe

ID	7
Filename	c:\users\rdhj0cnfevzx\appdata\local\programs\nure\resources\extra\win32\nure-helper.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra\win32\nure-helper.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\
Monitor Start Time	Start Time: 240317, Reason: Child Process
Unmonitor End Time	End Time: 303008, Reason: Terminated by Timeout
Monitor Duration	62.69s
Return Code	Unknown
PID	4488
Parent PID	3224
Bitness	64 Bit

Host Behavior

Type	Count
Module	100
System	14
Environment	16
-	10
File	404
Process	1
User	1
-	1
-	8
Registry	9

Network Behavior

Type	Count
TCP	3

Process #8: cmd.exe

ID	8
Filename	c:\windows\system32\cmd.exe
Command Line	cmd ver
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\
Monitor Start Time	Start Time: 244502, Reason: Child Process
Unmonitor End Time	End Time: 249750, Reason: Terminated
Monitor Duration	5.25s
Return Code	0
PID	4568
Parent PID	4488
Bitness	64 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	70
Environment	10
System	2

Process #10: nure.exe

ID	10
Filename	c:\users\rdhj0cnfevzx\appdata\local\programs\nure\nure.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\Nure.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --fiel... ...Cookies,SpareRendererForSitePerProcess --lang=en-US --service-sandbox-type=network --mojo-platform-channel-handle=1704 /prefetch:8
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\
Monitor Start Time	Start Time: 258262, Reason: Child Process
Unmonitor End Time	End Time: 303008, Reason: Terminated by Timeout
Monitor Duration	44.75s
Return Code	Unknown
PID	3712
Parent PID	1748
Bitness	64 Bit

Host Behavior

Type	Count
Module	222
File	194
System	17
Environment	15
-	26
Registry	26
-	9

Process #11: nure.exe

ID	11
Filename	c:\users\rdhj0cnfevzx\appdata\local\programs\nure\nure.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\Nure.exe" --type=renderer --field-trial-handle=1540,14212168910224858381,438351... ...-frame-before-activation --renderer-client-id=4 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=2052 /prefetch:1
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\
Monitor Start Time	Start Time: 259781, Reason: Child Process
Unmonitor End Time	End Time: 303008, Reason: Terminated by Timeout
Monitor Duration	43.23s
Return Code	Unknown
PID	4740
Parent PID	1748
Bitness	64 Bit

Dropped Files (1)

Filename	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✕

Host Behavior

Type	Count
Module	238
File	363
System	15
Environment	15
-	54
Registry	3
-	14

ARTIFACTS

File

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
b15241b99e501f131299333437ff457a87b53d39eebf10d3eea6a1810c6f242e	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra\win32\nure-helper.exe, C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra\win32/nure-helper.exe	Dropped File	5781.00 KB	application/vnd.microsoft.portable-executable	Create, Read, Write, Access	MALICIOUS
34de8177caa508681d06648ddecd62c2edc7206830e683d6f0cc1cc3d5e28603	C:\Users\RDhJ0CNFevzX\Desktop\Nure Setup 0.2.1.exe	Sample File	114593.48 KB	application/vnd.microsoft.portable-executable	Read, Access	MALICIOUS
9fef8a418523835124f7a23ab77eb48ef6f357627aed217bcacdf72579f0e005	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\Nure.exe	Dropped File	10240.00 KB	application/vnd.microsoft.portable-executable	Create, Write, Access	MALICIOUS
3eb38ae99653a7dbc724132ee240f6e5c4af4bfe7c01d31d23faf373f9f2eaca	C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\System.dll	Dropped File	12.00 KB	application/vnd.microsoft.portable-executable	Create, Delete, Write, Access	CLEAN
b72e9013a6204e9f01076dc38dabbf30870d44dfc66962adbf73619d4331601e	C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\StdUtils.dll	Dropped File	100.00 KB	application/vnd.microsoft.portable-executable	Create, Delete, Write, Access	CLEAN
996a259e53ca18b89ec36d038c40148957c978c0fd600a268497d4c92f882a93	C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\SpiderBanner.dll	Dropped File	9.00 KB	application/vnd.microsoft.portable-executable	Create, Delete, Write, Access	CLEAN
30c6c3dd3cc7fcea6e6081ce821adc7b2888542dae30bf00e881c0a105eb4d11	C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\nsProcess.dll	Dropped File	4.50 KB	application/vnd.microsoft.portable-executable	Create, Delete, Write, Access	CLEAN
ba487d51c0656b9324c2a0c05c6088668a6c9981e4cf173279e09367d0511fcc	C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\app-64.7z	Dropped File	10240.00 KB	application/x-7z-compressed	Delete, Read, Access, Create, Write	CLEAN
b393f05e8ff919ef071181050e1873c9a776e1a0ae8329aefff7007d0cadf592	C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\nsis7z.dll	Dropped File	424.00 KB	application/vnd.microsoft.portable-executable	Delete, Access	CLEAN
5ae14147992a92548bcad76867dd88cdfcdb69d951c8720920cce6fb135e3189	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\chrome_100_percent.pak	Dropped File	121.46 KB	application/octet-stream	Create, Write, Access	CLEAN
dd8146b2ee289e4d54a4a0f1fd3b2f61b979c6a2baaba96a406d96c3f4fdb33b	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\chrome_200_percent.pak	Dropped File	181.51 KB	application/octet-stream	Create, Write, Access	CLEAN
4a33fabd88f3bc0f2bd32a70f5e99efea5b1ccebe9bef0291a28e6bd6006537d	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\icudtl.dat	Dropped File	10240.00 KB	application/octet-stream	Create, Write, Access	CLEAN
c44607a865e7a6db05552baa0ef71f9887d96acd00d123854b44996bc27c0e33	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\LICENSE.electron.txt	Dropped File	1.04 KB	text/plain	Create, Write, Access	CLEAN
03f1d245e6a2facca9edbdaad108169e0765dd9101875bc2d123797994b9e80f	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\LICENSES.chromium.html	Dropped File	4605.23 KB	text/html	Create, Write, Access	CLEAN
e9c78c2410d5c81e0cd5d122462e852143eea15ca69cd01b85322cede1e10806	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\am.pak	Dropped File	142.12 KB	application/octet-stream	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
1cdef40ba8343e7f826c2020906915efaac5e56f543cd2ed6ebf704882525d8c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ar.pak	Dropped File	144.86 KB	application/octet-stream	Create, Write, Access	CLEAN
1bb8c5ce9215d42ba9ceec52f86fbff46df668ce48ff56bd1cbe96adadf4922c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\bg.pak	Dropped File	154.55 KB	application/octet-stream	Create, Write, Access	CLEAN
f7d704207cb3340f1ace2f2e5af031e816bb86e4bf3f665907d837d094bba37a	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\bn.pak	Dropped File	203.77 KB	application/octet-stream	Create, Write, Access	CLEAN
14e99f4d94868a454f40ee8e0f62d056e0abb303caf6e184a9a61bdec18ac271	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ca.pak	Dropped File	99.35 KB	application/octet-stream	Create, Write, Access	CLEAN
9651b8f3304c70d96dcca76cfffad90ce8afcab6231ffd8e4e9beade3d510841	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\cs.pak	Dropped File	101.63 KB	application/octet-stream	Create, Write, Access	CLEAN
1d1a3e38ddf282969bca2a5d893b3db4a0aed10b53eab37bb2dad7d2d18c94de	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\da.pak	Dropped File	92.82 KB	application/octet-stream	Create, Write, Access	CLEAN
e71f4320553f65cfd0356a4b30f3aec2eec7b4fd327866d528917b9909cfa761	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\de.pak	Dropped File	98.95 KB	application/octet-stream	Create, Write, Access	CLEAN
a3431d3ac720f871c33d7e522cf506b2fa8ea1872bac02a4b4b427a6d063af38	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\el.pak	Dropped File	172.39 KB	application/octet-stream	Create, Write, Access	CLEAN
c4fdfa9c6f30ad657bf12ccb95f70542a0fade45d8490259a4507629f4b33299	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\en-GB.pak	Dropped File	82.33 KB	application/octet-stream	Create, Write, Access	CLEAN
d1d3f892be16329c79f9a8ee8c5fa1c9fb46d17edfeb56a3d9407f9d7587a0de	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\en-US.pak	Dropped File	83.06 KB	application/octet-stream	Create, Write, Access	CLEAN
64df687bbb37bcd92e609f7e3bf950ee5629b693ff8636607285f5753b1bdaae	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\es-419.pak	Dropped File	97.18 KB	application/octet-stream	Create, Write, Access	CLEAN
eb22282dbf211f64142ef4dfac2c1d811d65decd617c4a3d1c892967dc72ac07	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\es.pak	Dropped File	99.39 KB	application/octet-stream	Create, Write, Access	CLEAN
b3baf825f9b237565260ba2935fe9acf2ae381e3bfc6fbf837dbfe6fb83314b5	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\et.pak	Dropped File	88.94 KB	application/octet-stream	Create, Write, Access	CLEAN
8ea08e9874892edefcbdc55c393dc00fe451f3c7f29b57d7105377349eb4bfc4	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fa.pak	Dropped File	138.70 KB	application/octet-stream	Create, Write, Access	CLEAN
bfc24d41ea8e362bb1a18c11860d2217fc100b1a422cf54629c7d0c6640d5ed7	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fi.pak	Dropped File	91.43 KB	application/octet-stream	Create, Write, Access	CLEAN
75d473ffd351a828bd7854067ad986908efefdfb75800650587b8bef09f9ff2a	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fil.pak	Dropped File	101.16 KB	application/octet-stream	Create, Write, Access	CLEAN
b387afb8c8ae3c3ce90728fb7eb39a39ec789c6e7bfe4dbd2b5d49e72434db1f	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fr.pak	Dropped File	107.33 KB	application/octet-stream	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
a49597e67fcf93448c89e07f9cc3519b3b1b77505bc30adf3f25c250718eec0c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\gu.pak	Dropped File	194.66 KB	application/octet-stream	Create, Write, Access	CLEAN
7420e94f19bd61f33950e120f29c9783305f218d089f0a7d3ea3451655cdda1f	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\he.pak	Dropped File	122.21 KB	application/octet-stream	Create, Write, Access	CLEAN
acc53ca41a9a04a57c1f18fea58cc4329b8add0ded37f9f7d7a73584a910d6c9	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hi.pak	Dropped File	201.34 KB	application/octet-stream	Create, Write, Access	CLEAN
e55d011ac0cc50d33bf22d43a9c5a6b59f5c31bd2884789efee124929be9a7fa	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hr.pak	Dropped File	96.83 KB	application/octet-stream	Create, Write, Access	CLEAN
030cbf833a350946959afa0d2b699512c0b715ff7b38b613bcd16b15282b940a	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hu.pak	Dropped File	103.95 KB	application/octet-stream	Create, Write, Access	CLEAN
d12d87d003bda037b411daab09d1698671f8284e4297ffc08b0558749df6495b	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\id.pak	Dropped File	89.06 KB	application/octet-stream	Create, Write, Access	CLEAN
266f501703d3899000d5eb60d55ccc8f59f186e862a4a9a34910e81699ea289e	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\it.pak	Dropped File	96.68 KB	application/octet-stream	Create, Write, Access	CLEAN
4d0910d196b6b5652e3e5d677ddb048b8dae1ec974593484df2838093c96fed7	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ja.pak	Dropped File	116.93 KB	application/octet-stream	Create, Write, Access	CLEAN
f25c8b41249c8f54224702795644c80bb5a7eaaeb6f0af5b6a1048960a27c827	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\kn.pak	Dropped File	223.73 KB	application/octet-stream	Create, Write, Access	CLEAN
99addd110ae7ba9fb37daf5c32ad2815172840764da0c71d0304dc9562951d61	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ko.pak	Dropped File	98.60 KB	application/octet-stream	Create, Write, Access	CLEAN
9124dc353864cf6570580ae3afa0a7f09f5e3d32a61e71a64ff4cf824ad4fb29	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\lt.pak	Dropped File	105.47 KB	application/octet-stream	Create, Write, Access	CLEAN
6861e9a4e8a9f2493f0103afa0f860c280478a64293a6de883ba9cb6a45776f6	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\lv.pak	Dropped File	104.35 KB	application/octet-stream	Create, Write, Access	CLEAN
cc9fd4f2d44df646c6117465f820ad390efbc9cb64eb4ff898a50cdfef8f324c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ml.pak	Dropped File	235.08 KB	application/octet-stream	Create, Write, Access	CLEAN
5f1ffe801f3701434a73d3ad3d04e9fcb6238f0f3b14e9325413910799954543	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\mr.pak	Dropped File	191.24 KB	application/octet-stream	Create, Write, Access	CLEAN
f4f6362d9963b7d244e29e85c7ecda552ff7756621f6efc9f3b6f12940896a81	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ms.pak	Dropped File	91.24 KB	application/octet-stream	Create, Write, Access	CLEAN
efc934122d4232276f9f2317e5906517bd91ec2a6d76995fe8aae04eff866a50	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\nb.pak	Dropped File	90.02 KB	application/octet-stream	Create, Write, Access	CLEAN
4669c10a7fcc8a150a641e73320547ed1b966a92fe78041a860ce4892f79b0cd	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\nl.pak	Dropped File	93.89 KB	application/octet-stream	Create, Write, Access	CLEAN
ce84676f37bf97078b3d087d913a874d3c092f76b729f43d3e9553d3c9754f03	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pl.pak	Dropped File	101.95 KB	application/octet-stream	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
7cca8f6ee8b2a19c8ea53b3a2bb2af4ebbb2b8612caba87f581938e7d6aa9f18	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pt-BR.pak	Dropped File	96.49 KB	application/octet-stream	Create, Write, Access	CLEAN
7f0b86e4f6391e48fd045c8b967a1ad33d9c54f5a6ceda98d800c254dd2ec059	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pt-PT.pak	Dropped File	97.23 KB	application/octet-stream	Create, Write, Access	CLEAN
60859215a025b95a1ac06333a66d14e1698b28ae31451c999e8adc072401a86a	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ro.pak	Dropped File	99.54 KB	application/octet-stream	Create, Write, Access	CLEAN
5c93984215f69bc6c7a1430fedbdc619ee6ccc9e491354e3541fdc8ed1947f8b	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ru.pak	Dropped File	157.89 KB	application/octet-stream	Create, Write, Access	CLEAN
4a09c8f22d1fe71cdfd0149599c59ec3059cd35f7dc8f33f22f967a237f7def1	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sk.pak	Dropped File	103.32 KB	application/octet-stream	Create, Write, Access	CLEAN
1ed9fc4abb8bef48e0fd5e10a107fb456dcb0c7a275bb789cb0728cfadfdcc42	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sl.pak	Dropped File	98.77 KB	application/octet-stream	Create, Write, Access	CLEAN
362a50ec28da0af4c6b8e282ad64d45298b939a03883de22c5a33adfa919bc74	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sr.pak	Dropped File	148.22 KB	application/octet-stream	Create, Write, Access	CLEAN
cfe9ad173d516a3e1855f00f53fcb20a53ade93fef6256e909b0f0da12723cc2	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sv.pak	Dropped File	89.98 KB	application/octet-stream	Create, Write, Access	CLEAN
26fbb15e26f5a4c44bc0e86326fbff28686c771edd11bda6bfea178364299eaa	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sw.pak	Dropped File	91.43 KB	application/octet-stream	Create, Write, Access	CLEAN
2363b6a8cce7868830915303dc2825351e7ea9dfd98568e448cd8b71c7ceef90	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ta.pak	Dropped File	230.33 KB	application/octet-stream	Create, Write, Access	CLEAN
c9f427a4efa5d9835432e3a190e26d684c18c26e13fcda1b7e73d6a7527cfd4f	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\te.pak	Dropped File	213.26 KB	application/octet-stream	Create, Write, Access	CLEAN
301966a229a09b37e5b2bf12c89522a33144c977411099b81502261c4ca554ad	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\th.pak	Dropped File	183.14 KB	application/octet-stream	Create, Write, Access	CLEAN
81694a8258624f82dfbe0af43aa0ce5fdf1304c25a2f6735b972a2a29beb8e15	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\tr.pak	Dropped File	94.80 KB	application/octet-stream	Create, Write, Access	CLEAN
27d3c996804b4f4c106f12becdaeeb1ce65df53abe126585748 52ab7b6643bc1	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\uk.pak	Dropped File	158.48 KB	application/octet-stream	Create, Write, Access	CLEAN
7f94586012c85732d23b05dbdde2c497326d5fcab87de83aafa3594b614dbd36	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\vi.pak	Dropped File	111.74 KB	application/octet-stream	Create, Write, Access	CLEAN
44a9dd0a830ce2feeb81523cce7fae8a0a553f05921b34d34c7826d50ac3a1b7	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\zh-CN.pak	Dropped File	83.32 KB	application/octet-stream	Create, Write, Access	CLEAN
268041a1a95dd540cf7e92a01802b65df8c8d1c80726007da1bb8a9cba6e5414	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\zh-TW.pak	Dropped File	83.48 KB	application/octet-stream	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
7b953443e3cd54a0a4775528b52fbfe5ebecbc2c71731600ed0999d227969506	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources.pak	Dropped File	4898.19 KB	application/octet-stream	Create, Write, Access	CLEAN
93ea2cedd1ea49a5dc6eab0c97c422b642edf48cd0b5e65efb8ef865d2628c4d	\\?\C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app-update.yml, C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app-update.yml	Dropped File	146 bytes	text/plain	Create, Read, Write, Access	CLEAN
70a861b0a9ac7a34e2338bf24140471684df6ed7d4e8df2019ddd054c625df32	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar, \\?\C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar	Dropped File	10240.00 KB	application/octet-stream	Create, Write, Access	CLEAN
9ea8667cf8d736e27222e589901f95b6749ab9f09cb339bb4b90fd180700f937	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\dist\index.min.js	Dropped File	34.09 KB	text/plain	Create, Write, Access	CLEAN
bf7901cd6cf0fb3d64522c548e8adb561f245de169307f31eca2b5f9c46dde0e	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\dist\index...t, C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.min.js.LICENSE	Dropped File	133 bytes	text/plain	Create, Write, Access	CLEAN
9980e1f206d33d936779cb9d9cc4b499195ebe9d91777248223 69f51ffe63013	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\example.js, C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\example.js	Dropped File	250 bytes	text/plain	Create, Write, Access	CLEAN
f71842df80e1cd78d057d41f4f027d8f38755f500f8993f973922ba1bdb1bed8	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\LICENSE, C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\LICENSE	Dropped File	1.04 KB	text/plain	Create, Write, Access	CLEAN
c362572d0b77ae7c9686c326b475930a7a353c145def38a3ab8029e432a7bce3	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\package.json	Dropped File	673 bytes	text/plain	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
a5644d406081ed410f4d6a103972f4e849e092ea673d507769ae1f74f1cc0028	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\base-table.json	Dropped File	10.35 KB	text/plain	Create, Write, Access	CLEAN
3c406a345cd43f5a765679668c41101c73bbf1d9be4db2117134e51755af7194	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src\constants.js, C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\constants.js	Dropped File	268 bytes	text/plain	Create, Write, Access	CLEAN
31a73ecac682c9e11284d1f0a3e808b37a683aa31af2f5b6660017e3b0aa586b	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\index.js	Dropped File	2.80 KB	text/plain	Create, Write, Access	CLEAN
6a77cb6cb5219a932bf97f90152b18d3f90c0f1c518a1388d2fefc82208f6359	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\int-table.js, C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src\int-table.js	Dropped File	284 bytes	text/plain	Create, Write, Access	CLEAN
d9971e3545106957ae0fd9447d2bf39761ad573a2409dc7f1b0a3d7e892acd1c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src\print.js, C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\print.js	Dropped File	284 bytes	text/plain	Create, Write, Access	CLEAN
d16dcaa40f95ed96fc9ef7175600152880335a8960ae2ad4b7072081d40dbdfe	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\util.js	Dropped File	720 bytes	text/plain	Create, Write, Access	CLEAN
4ee737eee2cce9e65b4425978748d5fefa71c2ac7c3bc9d92fa0d17a6727c828	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\varint...\...able.js, C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src\varint-table.js	Dropped File	354 bytes	text/plain	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
afe42d63569c6829912ab2fb29efa19f29b5cc231d1545c5e1607cdddfcb27f7	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\tools\update-table.js, C:\Us...\hJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\tools\update-table.js	Dropped File	753 bytes	text/plain	Create, Write, Access	CLEAN
cff46d23d1b89ab25cd8e1f82d9f01449f0ea2d5d1ad877f446663748df6dc18	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.js	Dropped File	74.88 KB	text/plain	Create, Write, Access	CLEAN
519ed5be2ef4d28d9f8da43c907f03ac27479a94026824e1e29085c15bce0273	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.js.map	Dropped File	82.81 KB	text/plain	Create, Write, Access	CLEAN
fafb34cdfa41d9dbb5e80707027d37f07ec60bdd7be2574d2c86338193f46068c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.min.js	Dropped File	33.73 KB	text/plain	Create, Write, Access	CLEAN
015427fe24191037d48e45804a702b0e007c110e6503ca0e6a6721cb32241d00	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.min.js.map	Dropped File	107.11 KB	text/plain	Create, Write, Access	CLEAN
8fdfef8c3a3dab093d1ac84622accaccb76709b32e02361f44272087299c9f3c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\package.json	Dropped File	649 bytes	text/plain	Create, Write, Access	CLEAN
543a6614d6afd218760a5aa18c1a2adb76511cb2ae783f0e2cafbe76c0d1598c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src\base-table.json	Dropped File	9.82 KB	text/plain	Create, Write, Access	CLEAN
2872182c7dc0bfbee35e65c0b4e5e0c2f1e4a9d77135dc72fdf8b847ac5ee0f9	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src\index.js	Dropped File	2.76 KB	text/plain	Create, Write, Access	CLEAN
8d4123d7dddfbb1c4902734c0e54c366afce71780bb027f1eaa70df7b9ce32be	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src\util.js	Dropped File	683 bytes	text/plain	Create, Write, Access	CLEAN
3ddf7961125a3524f7b06e696cc578259f87f57584b8d69b461873dc13910bf0	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\.prettierrc	Dropped File	46 bytes	text/plain	Create, Write, Access	CLEAN
e85060c605820a1acd5fd5aa8b149d4fcd5bef5e498a80392a7a1b68cac43d62	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\index.js	Dropped File	1.60 KB	text/plain	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
6d8fdba983f2589ac744b68437918c63e679a962c4e06007b4f81cb089fdb103	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\lib\checkGrowl.js	Dropped File	536 bytes	text/plain	Create, Write, Access	CLEAN
97aad0d16fb442b7f7f4262bb7e27d6dc9fc41060ad5d876c36878e4bb011bf2	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\lib\utils.js	Dropped File	12.30 KB	text/plain	Create, Write, Access	CLEAN
c5f00acfdb0120b3fafa9869ece941c0a095253770f652927da96352b502df90	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\LICENSE	Dropped File	1.04 KB	text/plain	Create, Write, Access	CLEAN
0d2f65f5bee22e3ef06e3bdfad02dc476e18fc65a7c2572c29f943a1001c5d0c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\notifiers\balloon.js	Dropped File	4.27 KB	text/plain	Create, Write, Access	CLEAN
33e91460fca7d54f27d7d8d569ecffa6444e03624881e74cb490174093069bbb	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\notifiers\growl.js	Dropped File	1.78 KB	text/plain	Create, Write, Access	CLEAN
b4724a9422d5d15d7148ac08a3f299f06443b55a65ed2b5f87a6f4d88f9a122c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\notifiers\notificationcenter.js	Dropped File	2.45 KB	text/plain	Create, Write, Access	CLEAN
6bd1e4987a4cab694503737d1e1f19b9f62af695e85a4e30b8a8683134229bdce	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\notifiers\notifysend.js	Dropped File	2.14 KB	text/plain	Create, Write, Access	CLEAN
cd945dd67095b22d9302396bb716ac654c3a79bc336cee486e27fc446ad49041	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\notifiers\toaster.js	Dropped File	2.44 KB	text/plain	Create, Write, Access	CLEAN
adfb2a4b27233cf273b7c68fff2803d79ae10d38601a9d867bed9d2eb857ea9d	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\package.json	Dropped File	1.26 KB	text/plain	Create, Write, Access	CLEAN
24a13344667a084f692b2103741f4d4ed8bacf5a53e2abe508f10423c5d6b27f	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Info.plist	Dropped File	1.77 KB	text/xml	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
2588f4ae2118396419767c388cf2b0a9a5e0cb53ce5d05a07c00f68a97a50215	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\MacOS\terminal-notifier	Dropped File	85.63 KB	application/x-mach-binary	Create, Write, Access	CLEAN
82502191c9484b04d685374f9879a0066069c49b8acae7a04b01d38d07e8eca0	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\PkgInfo	Dropped File	8 bytes	text/plain	Create, Write, Access	CLEAN
b4386fe1cef65cd91e6c8ecc065d117089083f91b7cadbf0c3e5eae20e8b9640	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Resources\en.lproj\Credits.rtf	Dropped File	436 bytes	text/rtf	Create, Write, Access	CLEAN
39cf2ee07b7b333e7c179d0bf4d798a5b72af6a4e584f51e642703bbfa4fc828	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Resources\en.lproj\InfoPlist.strings	Dropped File	92 bytes	text/plain	Create, Write, Access	CLEAN
66a2378cee667b39af5a92676f20f2db13dcf73cf2d23d2a30ef140cdb71f1ad	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Resources\en.lproj\MainMenu.nib	Dropped File	25.19 KB	application/octet-stream	Create, Write, Access	CLEAN
ccfc0f457dbbed2b164a9f708e1a0000fad8f896b0d5332b376e2b748f3ff525	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Resources\Terminal.icns	Dropped File	360.73 KB	image/x-icns	Create, Write, Access	CLEAN
ea8af5e789cb2d4e9b10bce3874982ade163b749b6bfbdb32e2df21c4d106de1	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\snoreToast\LICENSE	Dropped File	7.47 KB	text/plain	Create, Write, Access	CLEAN
77a2769c8dc103f8051ccabab083c18e4cfbd26ba51589f26278c94dee997e56	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\terminal-notifier-LICENSE	Dropped File	1.26 KB	text/plain	Create, Write, Access	CLEAN
168cc89c100ef9cf95c3ae81f16badcbf607b289a3de0dec9fcfb387ff4c4f4b	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\.svgo.yml	Dropped File	1.42 KB	text/plain	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
e6a786bf92347f485cc9c0641b8710afe2b3e65947c2b292f46ff3a4ce39a0e2	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\bin\svgo	Dropped File	55 bytes	text/plain	Create, Write, Access	CLEAN
940ec165700a82e5cf8caf847f6f4853d4beb50ea01ea14999df8a9a669e8648	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\css-tools.js	Dropped File	6.44 KB	text/plain	Create, Write, Access	CLEAN
3f242b971d909eb7e806591cc410b665a9aec897ff30eac9c9d913ad76e46fc7	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo.js	Dropped File	2.58 KB	text/plain	Create, Write, Access	CLEAN
33b7d6a10da711fea14d42d70fa32d61ec48ba725b9abd3d0e57f02868249237	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\coa.js	Dropped File	18.49 KB	text/plain	Create, Write, Access	CLEAN
2ab9c99b50782420c8eb6ab915b8d883016b26aa18db54c73ee41fdc02755e19	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\config.js	Dropped File	5.99 KB	text/plain	Create, Write, Access	CLEAN
35d6b21efdf077532af6a1a22b7448dc053b47561b69bcd290210db1ba1fbc47	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\css-class-list.js	Dropped File	3.18 KB	text/plain	Create, Write, Access	CLEAN
aceb6bda2465b65fac984e291a3fd842f06cb64b13dd261b737c0e3c12634548	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\css-select-adapter.js	Dropped File	1.50 KB	text/plain	Create, Write, Access	CLEAN
0640e9b4b150751d266a61cd8f3f39bd7e51538bc0d0d307dd62395c4166f1e8	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\css-style-declaration.js	Dropped File	8.02 KB	text/plain	Create, Write, Access	CLEAN
d4ae62eff5227f574ec5a72b130ed2b1ca49c13f8bb54ffe28ea41e7c9cd2da6	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\js2svg.js	Dropped File	7.78 KB	text/plain	Create, Write, Access	CLEAN
4f2b487896fc022ebda148d57cfc07722652e0f23d7dc1bbe31623d904f850bf	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\jsAPI.js	Dropped File	8.95 KB	text/plain	Create, Write, Access	CLEAN
08e6a754152cfcd81f3af1c6c62e1ad32fa76c1a4726037a7c5b0802c8c6d715	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\plugins.js	Dropped File	2.10 KB	text/plain	Create, Write, Access	CLEAN
e5f00eb2a1ceaff6bf57d55f6587fcb7d8afbf53e9fc9ff722ab8e0902a52085	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\svg2js.js	Dropped File	4.43 KB	text/plain	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
cc7028a1dc0123aa13a7a05c9893f4196d04393d3c0eaaf03c1b1b9675950ddd	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo\tools.js	Dropped File	3.75 KB	text/plain	Create, Write, Access	CLEAN
7b20556d33022fb8475af038919caedecd3d5072db9b336e738390208decaf1e	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\LICENSE	Dropped File	3.49 KB	text/plain	Create, Write, Access	CLEAN
710a4a77e6e63fa206a58ff9aee8b9577193db543beda9ca667b1ba7e117ddac	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\Makefile	Dropped File	524 bytes	text/plain	Create, Write, Access	CLEAN
e8afcef3529ea1c2843c6f2b87d179a2e0c0f6dd40c40b08ba23a5a2fa2666be	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\package.json	Dropped File	1.18 KB	text/plain	Create, Write, Access	CLEAN
f3b8014445e6f0cbd27f5945b6ded6062036992a5f281cfe4cc017fee600c47b	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\addAttributesToSVGElement.js	Dropped File	2.02 KB	text/plain	Create, Write, Access	CLEAN
2c03b0d95b48a0ce9b084e82950a6e20dc26cea4f8986183faf0d531ad7a1958	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\addClassesToSVGElement.js	Dropped File	1.07 KB	text/plain	Create, Write, Access	CLEAN
9ef0f0d3190ca2f47d166beea59e62e70bd5cc08a4320415598e1af3fa8ee7af	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\cleanupAttrs.js	Dropped File	1.28 KB	text/plain	Create, Write, Access	CLEAN
51c05f8a3e2db6c94e7d9004ba13c23c19361f6ecadd6031a99eaaf0f51036ef	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\cleanupEnableBackground.js	Dropped File	2.25 KB	text/plain	Create, Write, Access	CLEAN
5e50a7293c635a364c6f1de665ef01a941f9824f0d7df3168fc0f7ff0c2889ea	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\cleanupIDs.js	Dropped File	6.58 KB	text/html	Create, Write, Access	CLEAN
0ff4e6d679235700ca3b4162fa572db8b12ef3809f38ce23f0105dfd87cb8da4	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\cleanupListOfValues.js	Dropped File	3.52 KB	text/plain	Create, Write, Access	CLEAN
56adcbee59f4bfdcdf1decb4ae4b2bdda7423acad24e8bc87e5fcc2452b3a26c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\cleanupNumericValues.js	Dropped File	2.50 KB	text/plain	Create, Write, Access	CLEAN
e58b50938ca85c26da430a73d614a81006198a35cbef1b031a5d32aa5474b968	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\collapseGroups.js	Dropped File	2.92 KB	text/plain	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
05f885bdf572ce5c83731aaa47a650913360cda07c3fb3f1d0d8c66b8e1b89dc	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertColors.js	Dropped File	3.58 KB	text/plain	Create, Write, Access	CLEAN
9c89a343297860ab804295614a788aaf9711c3ab6867c54143398f97c6b5e47c	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertEllipseToCircle.js	Dropped File	895 bytes	text/plain	Create, Write, Access	CLEAN
5ca6a349da130fea38f571b5cd6351d5da69c2d7d997e837f6ba5e39955224c4	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertPathData.js	Dropped File	30.16 KB	text/plain	Create, Write, Access	CLEAN
6f01d924ed540e990c92f1dd7c0e6603443f5ca6dedd34d81bf742f5ff08efe7	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertShapeToPath.js	Dropped File	4.39 KB	text/plain	Create, Write, Access	CLEAN
ef74471cb20352cddbdce7cb395a3595ab98e81904b06db66b37104f52eb0c51	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertStyleToAttrs.js	Dropped File	4.10 KB	text/plain	Create, Write, Access	CLEAN
8643aea0bdc9da1d212f732d4b822bcf360ea60ad2bf9927d5ba2b95c1c85f24	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\convertTransform.js	Dropped File	10.62 KB	text/plain	Create, Write, Access	CLEAN
387060c09953a1a566b88e6c18df376433a02a1082d1decac3c1db28f1092fc2	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\inlineStyles.js	Dropped File	7.70 KB	text/plain	Create, Write, Access	CLEAN
85df51ed543025cf7228c07cd6d872c48a7552744aa9cca7b7ac3a05a2467981	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\mergePaths.js	Dropped File	2.08 KB	text/plain	Create, Write, Access	CLEAN
d8ada72c15d4d8b48152d5b63c19b15fe9697c6a9251e3432ecd408905c152f9	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\minifyStyles.js	Dropped File	3.97 KB	text/html	Create, Write, Access	CLEAN
09cc62c0fd49d94af79b115a02ed1061e3df78a44031fddd24ad327854908de4	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\moveElemsAttrsToGroup.js	Dropped File	3.31 KB	text/plain	Create, Write, Access	CLEAN
2afe183c1debcf134b87a1c8825a04916541a5cb5011251c910a1cd57667ccf0	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\moveGroupAttrsToElems.js	Dropped File	1.81 KB	text/plain	Create, Write, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
6262052097fc0fc77f25c1b73bf329d54cdc62f25c4bd72bbef69895fc502370	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\prefixIds.js	Dropped File	5.41 KB	text/plain	Create, Write, Access	CLEAN
73b405c018d768962d2903061be50bc33cd6dea72980db054d6f18bed8c7427f	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\removeAttributesBySelector.js	Dropped File	1.87 KB	text/plain	Create, Write, Access	CLEAN
5f91280acabf49187c60f9061d9e4d496d6d8a9aae445465175a6b70369e7dc8	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins\removeAttrs.js	Dropped File	4.06 KB	text/plain	Create, Write, Access	CLEAN

Reduced dataset

Filename

Filename	Category	Operations	Verdict
C:\Users\RDHJ0C~1\AppData\Local\Temp\	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsq2A2E.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Nure Setup 0.2.1.exe	Dropped File, Sample File	Read, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\System.dll	Dropped File	Create, Delete, Write, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\StdUtils.dll	Dropped File	Create, Delete, Write, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\SpiderBanner.dll	Dropped File	Create, Delete, Write, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\nsProcess.dll	Dropped File	Create, Delete, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure	Accessed File	Create, Access	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDHJ0C~1\AppData\Local\Temp\nss3D97.tmp\app-64.7z	Dropped File	Delete, Read, Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\dist	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\tools	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\tools	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\lib	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\notifiers	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor	Accessed File	Create, Access	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\MacOS	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Resources	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\mac.noindex\terminal-notifier.app\Contents\Resources\en.lproj	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\notifu	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\node-notifier\vendor\snoreToast	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\bin	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\lib\svgo	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\svgo\plugins	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\terser	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\terser\bin	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\terser\dist	Accessed File	Create, Access	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\terser\tools	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\uglify-js	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\uglify-js\bin	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\uglify-js\lib	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\uglify-js\tools	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\webpack	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\webpack\node_modules	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\webpack\node_modules\terser	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\webpack\node_modules\terser\bin	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\webpack\node_modules\terser\dist	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\webpack\node_modules\terser\tools	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra\win32	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\swiftshader	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\chrome_100_percent.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\chrome_200_percent.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\icudtl.dat	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\LICENSE.electron.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\LICENSES.chromium.html	Dropped File	Create, Write, Access	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\am.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ar.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\bg.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\bn.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ca.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\cs.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\da.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\de.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\el.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\en-GB.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\en-US.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\es-419.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\es.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\et.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fa.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fi.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fil.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\fr.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\gu.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\he.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hi.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hr.pak	Dropped File	Create, Write, Access	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\hu.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\id.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\it.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ja.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\kn.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ko.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\lt.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\lv.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ml.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\mr.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ms.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\nb.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\nl.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pl.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pt-BR.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\pt-PT.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ro.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ru.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sk.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sl.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sr.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sv.pak	Dropped File	Create, Write, Access	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\sw.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\ta.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\te.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\th.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\tr.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\uk.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\vi.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\zh-CN.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\locales\zh-TW.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources.pak	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app-update.yml	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\dist\index.min.js	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\dist\index.min.js.LICENSE.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\example.js	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\LICENSE	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\package.json	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\base-table.json	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\constants.js	Dropped File	Create, Write, Access	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\index.js	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\int-table.js	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\print.js	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\util.js	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\src\varint-table.js	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\cids\node_modules\multicodec\tools\update-table.js	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.js	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.js.map	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.min.js	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.min.js.LICENSE	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\dist\index.min.js.map	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\example.js	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\LICENSE	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\package.json	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\app.asar.unpacked\node_modules\multicodec\src\base-table.json	Dropped File	Create, Write, Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://github.com/abseil/abseil-cpp				GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://raw.githubusercontent.com/GoogleChrome/accessibility-developer-tools/master/dist/js/axs_testing.js				GET	CLEAN
https://developer.android.com/jetpack/androidx				GET	CLEAN
https://aomedia.googlesource.com/aom/				GET	CLEAN
http://code.google.com/p/angleproject/				GET	CLEAN
http://lcamtuf.coredump.cx/afl/				GET	CLEAN
http://source.android.com				GET	CLEAN
https://developer.android.com/topic/libraries/architecture/index.html				GET	CLEAN
https://android.googlesource.com/platform/bionic/+/master/libc/				GET	CLEAN
https://chromium.googlesource.com/chromium/src.git/+/master/third_party/android_crazy_linker/				GET	CLEAN
https://developer.android.com/reference/android/util/FloatProperty.html				GET	CLEAN
http://developer.android.com/tools/extras/support-library.html				GET	CLEAN
https://maven.google.com/androidx/multidex/multidex/2.0.0/multidex-2.0.0.aar				GET	CLEAN
https://android.googlesource.com/platform/frameworks/support				GET	CLEAN
https://android.googlesource.com/platform/packages/apps/Settings/				GET	CLEAN
http://developer.android.com/sdk/index.html				GET	CLEAN
https://android.googlesource.com/platform/frameworks/base				GET	CLEAN
http://webkit.org				GET	CLEAN
https://github.com/google-ar/arcore-android-sdk				GET	CLEAN
https://developers.google.com/ar/develop/java/enable-arcore#dependencies				GET	CLEAN
https://github.com/dequelabs/axe-core/				GET	CLEAN
http://software.blackmagicdesign.com/DeckLink/v10.7/Blackmagic_DeckLink_SDK_10.7.zip				GET	CLEAN
http://www.chromium.org/blink				GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://boringssl.googlesource.com/boringssl				GET	CLEAN
https://github.com/liblouis/liblouis				GET	CLEAN
https://chromium.googlesource.com/breakpad/breakpad				GET	CLEAN
https://github.com/google/brotli				GET	CLEAN
http://www.daemonology.net/bsdiff/				GET	CLEAN
http://lxr.mozilla.org/mozilla/source/toolkit/mozapps/update/src/updater/				GET	CLEAN
https://github.com/rianhunter/zxcvbn-cpp				GET	CLEAN
http://code.google.com/p/google-axs-chrome/				GET	CLEAN
https://github.com/google/cityhash				GET	CLEAN
http://github.com/google/closure-compiler				GET	CLEAN
http://caminobrowser.org				GET	CLEAN
https://github.com/google/compact_enc_det				GET	CLEAN
https://github.com/google/cld3				GET	CLEAN
https://crashpad.chromium.org				GET	CLEAN
https://github.com/google/crc32c				GET	CLEAN
https://github.com/d3/d3				GET	CLEAN
http://r8.googlesource.com/r8				GET	CLEAN
https://github.com/google/dagger				GET	CLEAN
http://www.opensource.apple.com				GET	CLEAN
https://code.videolan.org/videolan/dav1d				GET	CLEAN
https://dawn.googlesource.com/dawn				GET	CLEAN
https://github.com/y-256/libdivsufsort				GET	CLEAN
https://github.com/chromium/dom-distiller				GET	CLEAN
http://code.google.com/p/data-race-test/wiki/DynamicAnnotations				GET	CLEAN
https://github.com/googlei18n/emoji-segmenter				GET	CLEAN
https://source.android.com				GET	CLEAN
https://github.com/libexpat/libexpat				GET	CLEAN
http://www.netlib.org/fdlibm/				GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://ffmpeg.org				GET	CLEAN
https://github.com/mit-plv/fiat-crypto				GET	CLEAN
https://github.com/GPUOpen-Effects/FidelityFX-SPD				GET	CLEAN
http://findbugs.sourceforge.net				GET	CLEAN
http://downloads.xiph.org/releases/flac/flac-1.3.1.tar.xz				GET	CLEAN
https://github.com/google/flatbuffers				GET	CLEAN
http://www.freetype.org				GET	CLEAN
https://fusejs.io				GET	CLEAN
http://android-gifview.googlecode.com/svn/!svn/bc/8/trunk/				GET	CLEAN
https://github.com/google/closure-library				GET	CLEAN
https://github.com/google/double-conversion				GET	CLEAN
https://github.com/google/ink				GET	CLEAN
https://github.com/googlei18n/google-input-tools.git				GET	CLEAN
https://github.com/google/google-toolbox-for-mac				GET	CLEAN
https://pki.goog/roots.pem				GET	CLEAN
https://github.com/google/glog				GET	CLEAN
http://code.google.com/p/google-jstemplate/				GET	CLEAN
https://github.com/grpc/grpc				GET	CLEAN
https://github.com/google/guava				GET	CLEAN
https://github.com/googlevr/gvr-android-sdk				GET	CLEAN
http://harfbuzz.org				GET	CLEAN
https://github.com/Microsoft/webauthn/				GET	CLEAN
http://hunspell.sourceforge.net				GET	CLEAN
https://android.googlesource.com/platform/external/hyphenation-patterns/				GET	CLEAN
https://github.com/LinuxA11y/IAccessible2				GET	CLEAN
http://www.ijg.org				GET	CLEAN
https://github.com/unicode-org/icu				GET	CLEAN
https://chromium.googlesource.com/deps/inspector_protocol/				GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://github.com/googlei18n/libphonenumber/				GET	CLEAN
http://developer.mozilla.org/en-US/docs/Accessibility/AT-APIs				GET	CLEAN
https://github.com/google/j2objc/				GET	CLEAN
http://code.google.com/p/atinject/				GET	CLEAN
http://jinja.pocoo.org				GET	CLEAN
https://github.com/open-source-parsers/jsoncpp				GET	CLEAN
http://www.khronos.org/registry				GET	CLEAN
https://github.com/KhronosGroup/glslang				GET	CLEAN
http://ltp.sourceforge.net/coverage/lcov.php				GET	CLEAN
https://github.com/google/leveldb.git				GET	CLEAN
https://github.com/googlei18n/libaddressinput				GET	CLEAN
https://github.com/AOMediaCodec/libavif				GET	CLEAN
http://brltty.app				GET	CLEAN
http://libcxx.llvm.org				GET	CLEAN
http://libcxxabi.llvm.org				GET	CLEAN
http://libevent.org				GET	CLEAN
http://llvm.org/docs/LibFuzzer.html				GET	CLEAN
https://skia.googlesource.com/libgifcodec/				GET	CLEAN
https://chromium.googlesource.com/chromiumos/platform2/libipp				GET	CLEAN
https://chromium.googlesource.com/external/webrtc				GET	CLEAN
https://github.com/libjpeg-turbo/libjpeg-turbo/				GET	CLEAN
http://libpng.org				GET	CLEAN
https://github.com/google/libprotobuf-mutator				GET	CLEAN
https://git.gnome.org/browse/libsecret/				GET	CLEAN
https://github.com/cisco/libsrtp				GET	CLEAN
http://www.freedesktop.org/wiki/Software/systemd/				GET	CLEAN
https://llvm.org/svn/llvm-project/libunwind/trunk/				GET	CLEAN
http://libusb.org				GET	CLEAN
http://www.webmproject.org				GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://xmlsoft.org				GET	CLEAN
http://xmlsoft.org/XSLT				GET	CLEAN
http://code.google.com/p/libyuv/				GET	CLEAN
http://www.logilab.org				GET	CLEAN
https://github.com/airbnb/lottie-web				GET	CLEAN
http://www.7-zip.org/sdk.html				GET	CLEAN
https://github.com/material-components/material-components-android				GET	CLEAN
https://github.com/material-components/material-components-ios				GET	CLEAN
https://github.com/google/material-design-icons				GET	CLEAN
https://github.com/material-foundation/material-font-disk-loader-ios				GET	CLEAN
https://github.com/material-foundation/material-internationalization-ios				GET	CLEAN
https://github.com/material-foundation/material-roboto-font-loader-ios				GET	CLEAN
https://github.com/material-foundation/material-sprited-animation-view-ios				GET	CLEAN
https://github.com/material-foundation/material-text-accessibility-ios				GET	CLEAN
https://android.googlesource.com/platform/development/+/b356564/samples/Support4Demos/src/com/example/android/supportv4/media/MediaController.java				GET	CLEAN
https://android.googlesource.com/platform/cts/+/master/tests/tests/provider/src/android/provider/cts/MediaStoreUtils.java				GET	CLEAN
http://www.mesa3d.org				GET	CLEAN
https://chromium.googlesource.com/chromiumos/platform/minigbm				GET	CLEAN
https://github.com/client9/stringencoders				GET	CLEAN
https://github.com/material-motion/motion-animator-objc				GET	CLEAN
https://github.com/material-motion/motion-interchange-objc				GET	CLEAN
https://github.com/material-motion/motion-transitioning-objc				GET	CLEAN
https://dxr.mozilla.org/mozilla-central/source/security/manager/				GET	CLEAN
https://github.com/google/nearby-connections				GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.mozilla.org/projects/nspr/				GET	CLEAN
https://www.nasm.us				GET	CLEAN
http://www.mozilla.org/projects/security/pki/nss/				GET	CLEAN
ftp://sourceware.org/pub/newlib/newlib-2.0.0.tar.gz				GET	CLEAN
http://cgit.freedesktop.org/~aplattner/nvidia-settings/				GET	CLEAN
https://developer.oculus.com/downloads/package/oculus-sdk-for-windows/				GET	CLEAN
http://cristal.univ-lille.fr/~casiez/1euro/				GET	CLEAN
https://chromium.googlesource.com/openscreen				GET	CLEAN
https://opencv.org/releases/				GET	CLEAN
http://www.openh264.org				GET	CLEAN
https://git.xiph.org/?p=opus.git				GET	CLEAN
https://github.com/khaledhosny/ots.git				GET	CLEAN
http://www.azillionmonkeys.com/qed/hash.html				GET	CLEAN
http://code.google.com/p/pdfium/				GET	CLEAN
https://android.googlesource.com/platform/external/perfetto/				GET	CLEAN
https://bitbucket.org/jpommier/pffft/				GET	CLEAN
https://developer.android.com/guide/app-bundle/playcore				GET	CLEAN
https://developers.google.com/android/guides/setup				GET	CLEAN

Reduced dataset

Domain

Domain	IP Address	Country	Protocols	Verdict
github.com			HTTPS, HTTP	CLEAN
raw.githubusercontent.com			HTTPS	CLEAN
developer.android.com			HTTPS, HTTP	CLEAN
aomedia.googlesource.com			HTTPS	CLEAN
code.google.com			HTTP	CLEAN
lcamtuf.coredump.cx			HTTP	CLEAN
source.android.com			HTTPS, HTTP	CLEAN
android.googlesource.com			HTTPS	CLEAN
chromium.googlesource.com			HTTPS	CLEAN

Domain	IP Address	Country	Protocols	Verdict
maven.google.com			HTTPS	CLEAN
webkit.org			HTTP	CLEAN
developers.google.com			HTTPS, HTTP	CLEAN
software.blackmagicdesign.com			HTTP	CLEAN
www.chromium.org			HTTP	CLEAN
boringssl.googlesource.com			HTTPS	CLEAN
www.daemonology.net			HTTP	CLEAN
lxr.mozilla.org			HTTP	CLEAN
caminobrowser.org			HTTP	CLEAN
crashpad.chromium.org			HTTPS	CLEAN
r8.googlesource.com			HTTP	CLEAN
www.opensource.apple.com			HTTP	CLEAN
code.videolan.org			HTTPS	CLEAN
dawn.googlesource.com			HTTPS	CLEAN
www.netlib.org			HTTP	CLEAN
ffmpeg.org			HTTP	CLEAN
findbugs.sourceforge.net			HTTP	CLEAN
downloads.xiph.org			HTTP	CLEAN
www.freetype.org			HTTP	CLEAN
fusejs.io			HTTPS	CLEAN
android-gifview.googlecode.com			HTTP	CLEAN
pki.goog			HTTPS	CLEAN
harfbuzz.org			HTTP	CLEAN
hunspell.sourceforge.net			HTTP	CLEAN
www.ijg.org			HTTP	CLEAN
developer.mozilla.org			HTTP	CLEAN
jinja.pocoo.org			HTTP	CLEAN
www.khronos.org			HTTP	CLEAN
ltp.sourceforge.net			HTTP	CLEAN
brltty.app			HTTP	CLEAN
libcxx.llvm.org			HTTP	CLEAN
libcxxabi.llvm.org			HTTP	CLEAN
libevent.org			HTTP	CLEAN
llvm.org			HTTPS, HTTP	CLEAN
skia.googlesource.com			HTTPS	CLEAN
libpng.org			HTTP	CLEAN

Domain	IP Address	Country	Protocols	Verdict
git.gnome.org			HTTPS	CLEAN
www.freedesktop.org			HTTP	CLEAN
libusb.org			HTTP	CLEAN
www.webmproject.org			HTTP	CLEAN
xmlsoft.org			HTTP	CLEAN
www.logilab.org			HTTP	CLEAN
www.7-zip.org			HTTP	CLEAN
www.mesa3d.org			HTTP	CLEAN
dxr.mozilla.org			HTTPS	CLEAN
www.mozilla.org			HTTP	CLEAN
www.nasm.us			HTTPS	CLEAN
sourceware.org			HTTP	CLEAN
cgit.freedesktop.org			HTTP	CLEAN
developer.oculus.com			HTTPS	CLEAN
cristal.univ-lille.fr			HTTP	CLEAN
opencv.org			HTTPS	CLEAN
www.openh264.org			HTTP	CLEAN
git.xiph.org			HTTPS	CLEAN
www.azillionmonkeys.com			HTTP	CLEAN
bitbucket.org			HTTPS	CLEAN
www.dabeaz.com			HTTP	CLEAN
www.polymer-project.org			HTTP	CLEAN
www.pylint.org			HTTP	CLEAN
quiche.googlesource.com			HTTPS	CLEAN
schema.org			HTTP	CLEAN
skia.org			HTTPS	CLEAN
google.github.io			HTTP	CLEAN
devel.freebsoft.org			HTTP	CLEAN
sqlite.org			HTTPS	CLEAN
www.strongtalk.org			HTTP	CLEAN
www.suitable.com			HTTP	CLEAN
swiftshader.googlesource.com			HTTPS	CLEAN
gperftools.googlecode.com			HTTP	CLEAN
pagure.io			HTTPS	CLEAN
www.linux-usb.org			HTTP	CLEAN
trevp.net			HTTP	CLEAN

Domain	IP Address	Country	Protocols	Verdict
mxr.mozilla.org			HTTP	CLEAN
git.linuxtv.org			HTTP	CLEAN
valgrind.org			HTTP	CLEAN
www.webrtc.org			HTTP	CLEAN
gitlab.freedesktop.org			HTTPS	CLEAN
sourceforge.net			HTTPS, HTTP	CLEAN
freedesktop.org			HTTP	CLEAN
tukaani.org			HTTP	CLEAN
zlib.net			HTTP	CLEAN
svg.github.io			HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
193.38.55.46		Netherlands	TCP	CLEAN

Email

-

Email Address

-

Mutex

Name	Operations	Parent Process Name	Verdict
f245fb50-b1fe-521e-8ee2-704cd498cf77	access	nure setup 0.2.1.exe	CLEAN
Local\AtomProcessSingletonStartup!	access	nure.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\f245fb50-b1fe-521e-8ee2-704cd498cf77	create, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\f245fb50-b1fe-521e-8ee2-704cd498cf77	create, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\f245fb50-b1fe-521e-8ee2-704cd498cf77\InstallLocation	write, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\f245fb50-b1fe-521e-8ee2-704cd498cf77\KeepShortcuts	write, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\f245fb50-b1fe-521e-8ee2-704cd498cf77\ShortcutName	write, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\f245fb50-b1fe-521e-8ee2-704cd498cf77\DisplayName	write, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\f245fb50-b1fe-521e-8ee2-704cd498cf77\UninstallString	write, access	nure setup 0.2.1.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{f245fb50-b1fe-521e-8ee2-704cd498cf77}\QuietUninstallString	write, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{f245fb50-b1fe-521e-8ee2-704cd498cf77}\DisplayVersion	write, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{f245fb50-b1fe-521e-8ee2-704cd498cf77}\DisplayIcon	write, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{f245fb50-b1fe-521e-8ee2-704cd498cf77}\Publisher	write, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{f245fb50-b1fe-521e-8ee2-704cd498cf77}\NoModify	write, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{f245fb50-b1fe-521e-8ee2-704cd498cf77}\NoRepair	write, access	nure setup 0.2.1.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{f245fb50-b1fe-521e-8ee2-704cd498cf77}\EstimatedSize	write, access	nure setup 0.2.1.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\UBR	read, access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ReleaseId	read, access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	nure.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	create, access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings	create, access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	create, access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\System\DNSClient	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SearchList	read, access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Domain	read, access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\UseDomainNameDevolution	read, access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel	read, access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\UseDomainNameDevolution	read, access	nure.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DomainNameDevolutionLevel	read, access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\DnsPolicyConfig	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\DnsConnections	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\DnsConnectionsProxies	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Avalon.Graphics\DISPLAY1	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Avalon.Graphics\DISPLAY1\PixelStructure	read, access	nure.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Themes\Personalize	access	nure.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Themes\Personalize\AppsUseLightTheme	read, access	nure.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\PriorityControl	access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\PriorityControl\ConvertibleSlateMode	read, access	nure.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	nure-helper.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	nure-helper.exe	CLEAN
HKEY_LOCAL_MACHINE	access	nure.exe	CLEAN
HKEY_CLASSES_ROOT	access	nure.exe	CLEAN
HKEY_USERS	access	nure.exe	CLEAN

Process

Process Name	Commandline	Verdict
nure.exe	"C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\Nure.exe"	MALICIOUS
nure-helper.exe	"C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra\win32\nure-helper.exe"	MALICIOUS
nure.exe	"C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\Nure.exe" --type=gpu-process --field-trial-handle=1540,14212168910224858381,438... ...AAAAAAAAAAAAUAAAAQAAAAAAAAAAAAAAAGAAAAEAAAAAAAAAABAAAABQAAABAAAAAAAAAAAAQAAAAYAAAA= --mojo-platform-channel-handle=1556 /prefetch:2	SUSPICIOUS
nure.exe	"C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\Nure.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --fiel... ...Cookies,SpareRendererForSitePerProcess --lang=en-US --service-sandbox-type=network --mojo-platform-channel-handle=1704 /prefetch:8	SUSPICIOUS
nure setup 0.2.1.exe	"C:\Users\RDhJ0CNFevzX\Desktop\Nure Setup 0.2.1.exe"	CLEAN
explorer.exe	C:\Windows\Explorer.EXE	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /d /s /c ""C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra\win32\nure-helper.exe""	CLEAN
cmd.exe	cmd ver	CLEAN
nure.exe	"C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\Nure.exe" --type=renderer --field-trial-handle=1540,14212168910224858381,438351... ...-frame-before-activation --renderer-client-id=4 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=2052 /prefetch:1	CLEAN

YARA / AV

Antivirus (1)

File Type	Threat Name	Filename	Verdict
DROPPED	Gen:Variant.Razy.854557	C:\Users\RDhJ0CNFevzX\AppData\Local\Programs\Nure\resources\extra\win32\nure-helper.exe	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Analyzer Information

Analyzer Version	4.1.1
Dynamic Engine Version	4.1.1 / 02/08/2021 15:19
Static Engine Version	1.6.0
Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (November 12, 2020)
Built-in AV Database Update Release Date	2021-03-31 14:29:22+00:00
VTI Ruleset Version	3.8
YARA Built-in Ruleset Version	1.5
Analysis Report Layout Version	10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed