ID: 830400
Sample Name:
rJUSTIFICANTEDEPAGO.exe
Cookbook: default.jbs
Time: 11:19:28
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

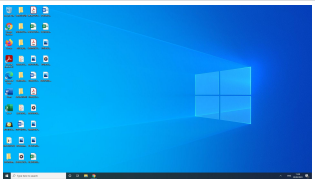
Windows Analysis Report

rJUSTIFICANTEDEPAGO.exe

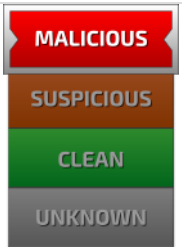
Overview

General Information

Sample Name:	rJUSTIFICANTEDEPAGO.exe
Analysis ID:	830400
MD5:	e542cf9ce8a67..
SHA1:	40161158f7cab..
SHA256:	4e78f6957f4c8...
Infos:	



Detection



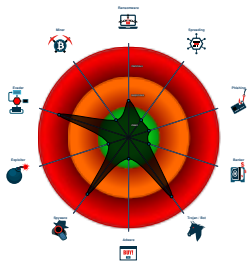
AgentTesla, GuLoader

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Yara detected AgentTesla
- Yara detected GuLoader
- Tries to steal Mail credentials (via fi...
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W...
- Tries to detect Any.run
- Tries to detect sandboxes and other...
- Queries sensitive network adapter in...
- Tries to harvest and steal browser in...
- Queries sensitive BIOS Information...
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64native**
- rJUSTIFICANTEDEPAGO.exe (PID: 4708 cmdline: C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe MD5: E542CF9CE8A67A5B681CC9B0004E0B10)
  - CasPol.exe (PID: 4160 cmdline: C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 8068 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	**http://** https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.6893759617.00000000360C1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.6893759617.00000000360C1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000002.00000002.2804076292.0000000005376000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: CasPol.exe PID: 4160	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: CasPol.exe PID: 4160	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

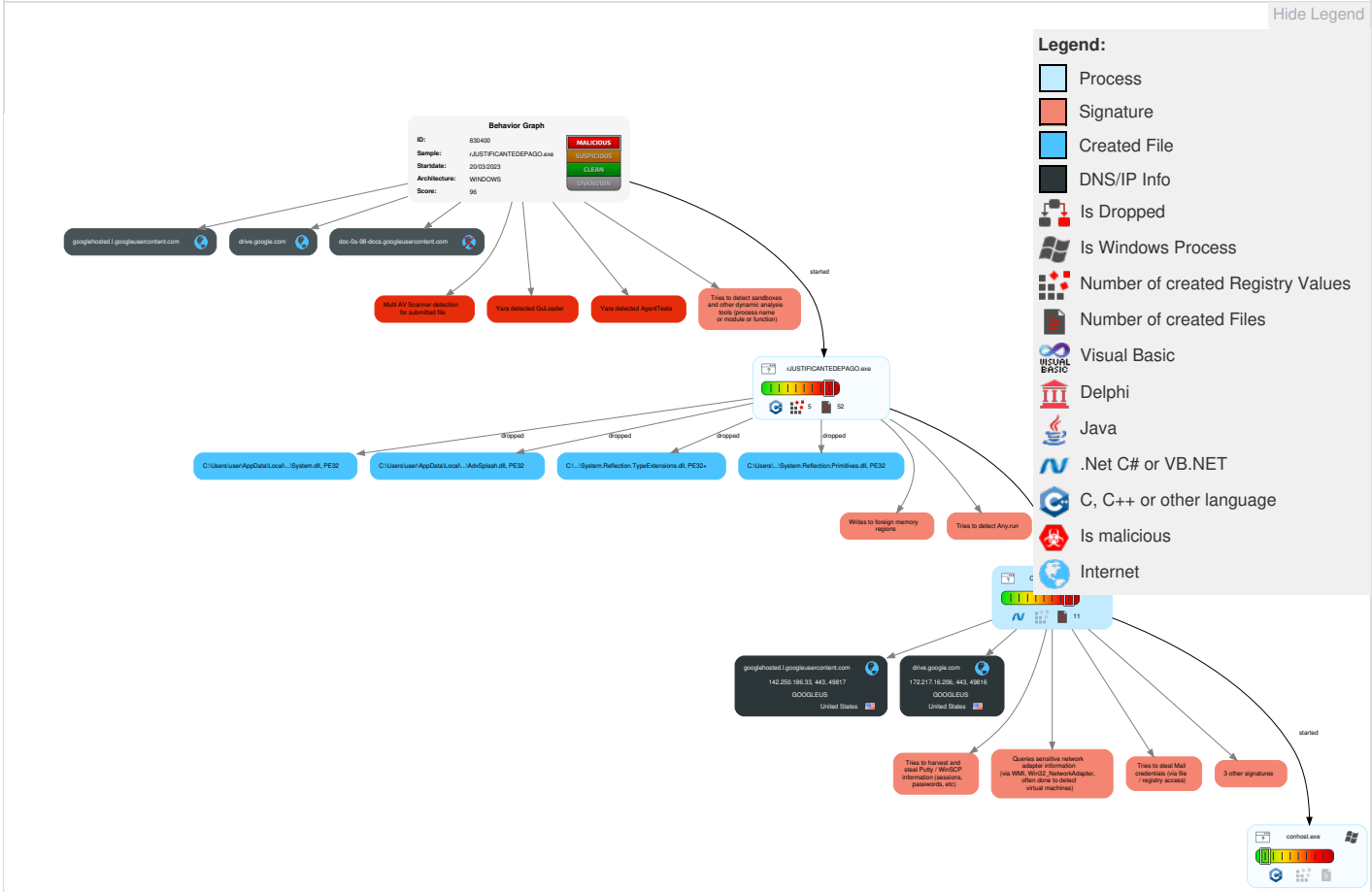
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	1 Windows Service	1 Access Token Manipulation	1 Obfuscated Files or Information	1 Credentials in Registry	1 1 7 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Windows Service	1 Timestomp	Security Account Manager	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 1 Process Injection	1 DLL Side-Loading	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 1 Virtualization/Sandbox Evasion	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Access Token Manipulation	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
rJUSTIFICANTEDEPAGO.exe	22%	Virustotal		Browse
rJUSTIFICANTEDEPAGO.exe	8%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Nonteachable\Bekmpelsesforanstaltninger\Carcinoid2\Efterplaprer\System.Reflection.Primitives.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Nonteachable\Bekmpelsesforanstaltninger\Carcinoid2\Efterplaprer\System.Reflection.Primitives.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Rntgenstraaler\Overholde\Wingdings\System.Reflection.TypeExtensions.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Rntgenstraaler\Overholde\Wingdings\System.Reflection.TypeExtensions.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsz62F8.tmp\AdvSplash.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsz62F8.tmp\AdvSplash.dll	3%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsz62F8.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsz62F8.tmp\System.dll	1%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	172.217.16.206	true	false		high
googlehosted.l.googleusercontent.com	142.250.186.33	true	false		high
doc-0s-98-docs.googleusercontent.com	unknown	unknown	false		high

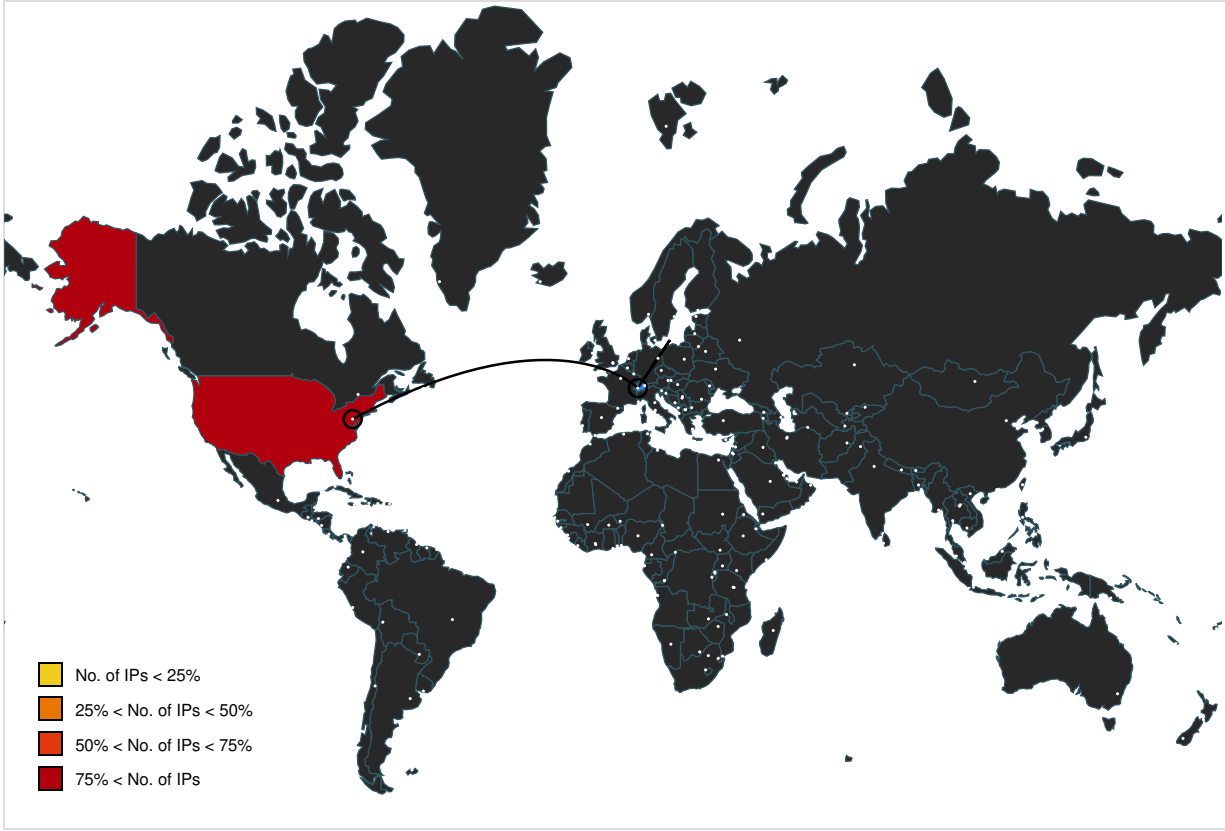
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://doc-0s-98-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/npt87m3l1utm86tkghdjh82fk6qcfges/1679307750000/00651307112604445902/*/1Ll5Auv3nDnZ4O0Qt2f2ZcFUknFi4BgKW?e=download&uuid=ea605c4e-1574-48ab-a781-ae85f09da2da	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/dotnet/runtimeBSJB	rJUSTIFICANTEDEPAGO.exe, 00000002.00000002.2801043131.0000000000789000.00000004.00000001.01000000.00000004.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	rJUSTIFICANTEDEPAGO.exe, 00000002.00000002.2801043131.000000000040A000.00000004.00000001.01000000.00000004.sdmp, rJUSTIFICANTEDEPAGO.exe, 00000002.00000000.1680795427.000000000040A000.00000008.00000001.01000000.00000004.sdmp	false		high
http://https://doc-0s-98-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/npt87m3l	CasPol.exe, 00000007.00000003.2773592501.0000000005510000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000007.00000002.6872352349.00000000054F5000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000007.00000002.6872352349.000000000554E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://doc-0s-98-docs.googleusercontent.com/%%doc-0s-98-docs.googleusercontent.com	CasPol.exe, 00000007.00000002.6872352349.0000000005508000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/dotnet/runtime	rJUSTIFICANTEDEPAGO.exe, 00000002.00000002.2801043131.0000000000789000.00000004.00000001.01000000.00000004.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.16.206	drive.google.com	United States		15169	GOOGLEUS	false
142.250.186.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830400
Start date and time:	2023-03-20 11:19:28 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	rJUSTIFICANTEDEPAGO.exe
Detection:	MAL
Classification:	mal96.troj.spyw.evad.winEXE@4/14@2/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 85.9% (good quality ratio 84.4%) • Quality average: 87% • Quality standard deviation: 21.9%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, audiodg.exe, UserOOBEBroker.exe, RuntimeBroker.exe, ShellExperienceHost.exe, WMIADAP.exe, backgroundTaskHost.exe, MoUsoCoreWorker.exe, svchost.exe, UsoClient.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Biofeedback\Zonar187\Fgtedes\Kisser\battery-level-90-charging-symbolic.svg

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	6689

Entropy (8bit):	5.135211840989561
Encrypted:	false
SSDEEP:	192:VkjcMIy2+X2I2F2C2G2fH7y8cQaVB2nnuy1FQOcQaVv2q22L2k2s:mjcM7u8xaV8nnL1FQOxaVu6
MD5:	C96D0DD361AFC6B812BDDD390B765A26
SHA1:	71081F096719CAA70B9BAEF86FE642635D8E2765
SHA-256:	6690799E5FA3FB0DD6CCE4BAC5AA1607C8A6BB16507854A87520C7DE53052E1B
SHA-512:	7C73BC880A9401C64AB0571957B414180C1B94137C7BC870BA602979E7A990640A37991CB87A40BC7E5942A37FDA25EFC58C759C00F4344BA3D88B9AA64182D
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?>.<svg. xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:cc="http://creativecommons.org/ns#". xmlns :rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#". xmlns:svg="http://www.w3.org/2000/svg". xmlns="http://www.w3.org/2000/svg". width="16". version="1.1". style ="enable-background:new". id="svg7384". height="16.000036">. <metadata. id="metadata90">. <rdf:RDF>. <cc:Work. rdf:about="">. <dc:format>i mage/svg+xml</dc:format>. <dc:type. rdf:resource="http://purl.org/dc/dcmitype/StillImage" />. <dc:title>Gnome Symbolic Icons</dc:title>. <c c:license. rdf:resource="http://creativecommons.org/licenses/by-sa/4.0/" />. </cc:Work>. <cc:License. rdf:about="http://creativecommons.org/li censes/by-sa/4.0/">. <cc:permits. rdf:resource="http://creativecommons.org/ns#Reproduction" />. <cc:permits. rdf:resource="htt

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Nonconcessive\Gennemgaas\Dispend70\colorimeter-colorhug-symbolic .symbolic.png

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	227
Entropy (8bit):	6.604776901672149
Encrypted:	false
SSDEEP:	6:6v/lhPysE9Xj1F/bkqdXujFErL4MImATQZu22F+p:6v/7kR7/bjd8Kgm2Q/2y
MD5:	7843C38CC42C6786B3373F166AF10172
SHA1:	BA0163109D9B641B1312230B3F62E1E10A61AA5E
SHA-256:	E3AF1293F8E8AB5C81300196AF55A7C15D5608291D46A2B86D4255910A7D0E59
SHA-512:	B1D3DF6A0A8CACD729CD9A2FD5AB0F74ED611270FA172CDBEB13D46FA71DD5CC5540A2FBFDB6C3004E652D317C8FAD4EC3AE437DF1C082B629870A33CC6 D34F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...1..P.....#.bae....^.^K/fek+.....X.....gfw....\.D/..b...a.4..$.....H#....o8...}..6.K.....Xc.$ ..'.1.2..vu.../O..>V.....CD....< ....w.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Nonconcessive\Gennemgaas\Dispend70\media-playlist-consecutive-sy mbolic.svg

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1329
Entropy (8bit):	4.950241534342892
Encrypted:	false
SSDEEP:	24:t4Cp/YHyKbRAecFxVrGDT/Gfd8hTdyKbRAecFxVrGDT/bNxNxZrGQ:9YHNtAecFmDT/s8hdNtAecFmDT/j3YQ
MD5:	021A9F00A28C9D496E490AE951E8EF12
SHA1:	F8A6392065D07BAC72E138B0E47A24FFDCCEE74B
SHA-256:	B420561770B77FCB47F69B6198B34B11155535F8A2E907BC4A0998CE74AFD340
SHA-512:	7F4F2D904EA968BF68E35E0D7F1EAE9718234757D1989879996BFB49D9C447F67544CB0E1C441FD6539D58B5F2C6ACA7E9E0208738C235D9AF0C093511760212
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M1.018 7v2H14V7z" style="line-height:normal;font-variant-ligatures:nor mal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align :start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;shape-padding:0;isolation:auto;mix-blend-mode:normal;marker:none" color="#bebebe" font-weight="400" font-family="sans-serif" overflow="visible"/><path d="M11.99 4.99a1 1 0 00-.697 1.717L12.586 8l-1.293 1.293a1 1 0 101.414 1.414L15.414 8l-2.707-2.707a1 1 0 00-.717-.303z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decorati

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Nonconcessive\Gennemgaas\Dispend70\network-offline-symbolic.svg

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1155
Entropy (8bit):	5.154592341044034

Encrypted:	false
SSDEEP:	24:t4CpQyhEXQDWu4AeWrGMyRQJaPahrGDfJcghSvOqlIQX6e4AeWrGMyp:vhjDWu4Ae3M5wSgDDontqe4Ae3MO
MD5:	EFB3C780BC44B346B50B1F0DC6CF6D0F
SHA1:	472B0EDD1C4C3092BC7C4DF934ABE126885B1780
SHA-256:	990859D3B2C830E23EC276BF1D38A38EE1BA3D89BF04CB138107E4CDE31167B5
SHA-512:	5B9C96F146C6A065C89172D02BDE8020876DC9C78859AD2B8B9529C615215F88BA85C2789544F5C5A247C148BB52FE4B5FCA325E7EAC4826D31A0365A0B8BCE E
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M5 7c-.31 0-.615.09-.812.281L.594 11l3.656 3.719c.198.19.44.281.75.281 h1v-1c0-.257-.13-.529-.312-.719L4.406 12H9s1 0 1-1c0 0 0-1-1-1H4.375l1.219-1.281C5.776 8.529 6 8.257 6 8V7z" style="line-height:normal;-inkscape-font-specificat ion:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" color="#000" font-weight="400" font-family="Sans" overflow="visible" op acity=".35"/><path d="M11 11h1.375l1.125 1.094L14.594 11H16v1.469l-1.094 1.062L16 14.594V16h-1.438L13.5 14.937 12.437 16H11v-1.406l1.063-1.063L11 12.47z" style="marker:none" color="#bebebe" overflow="visible"/><path d="M11 9c.31 0 .615-.09.813-.281L15.406 5 11.75 1.281C11.552 1.091 11.31 1 11 1h-1v1c0 .257.13 .529.313.719L11.593 4H7c-.528-.007-1 .472-1 1s.472 1.007 1 1h4.625l-1.219 1.281c-.182.19-.406.462-.406.719v1z" style="line-height:normal;-inkscape-font-specific ation:Sans;text-indent:0;text-align:star

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Nonconcessive\Gennemgaas\Dispend70\network-wireless.png

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	891
Entropy (8bit):	7.745720384539504
Encrypted:	false
SSDEEP:	24:d4qWCHdkXfUZEcO5Mkli416cOQSkye9V+:d4qnHd8Mkli4Dpb6
MD5:	5AF147D26AD399F83825377F04FD56A1
SHA1:	B378A498B0DB8114C794E21D533E80CEBE5DDE04
SHA-256:	6147A091847FCC9D9EDB22E655C4FC9DE6632C76D4252350400FA286F9791109
SHA-512:	EEC16DE49A4698FE4F03F841FBCF045FBBDC9D634EB73ED35DB544B6DB4BC0135CD8E1DF102FD1E8BDE9FC75380948B4C0459685EE2C21858D645B7973759I A6
Malicious:	false
Preview:	.PNG.....IHDR.....a...BIDATx.m.S.%9...$U.Fkl.y].m.6.m.F..5*g;k}.....P.....~u.....M.....M.q.....\|OM>....:?>.X7.U..j.v..?...e....>.Jk.&.{.[=.....t.d.....4.D... V....b..s.L.....Jg,..=V..@.n.....Rqv...._....B.h.;l....A....r.ap....N...1./.O.2.u7#.../.....o..*..O...[..X,<. .....@v.....t...H..Rf..C?q..8.HB.!{K..N.....t..5..1d.+.....).....pL.5.R..=....jC". ...t6.BA.)....xZ..d..^W~yU...ya.....U/...VA.r.....r.U....[".D.).8..iO<..[.....t.e9S...K8!....K..&p..Y2l.....".P8:..v..0....zd.."....O?+^.. =..b....t..K../.....?.?5...c.[.f.nP.P.o....7..k..t.?P(..O >.H~...n..jh.'..]..SC.5M.....'.}.n..'...t..9..c*...Ki...t..1z..N.q...w.w..y..W...K7x.^..p....j...%..3.\|.....x...G.\|~..a.o.N.<.....wK...]..u.....`...(z.B!.?q.b..u..$(.#1..N...b.u...@h...|.w..g.. ..}i....?~.....1~...I..]h.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Nonteachable\Bekmpelsesforanstaltninger\Carcinoid2\Efterplaprer\System.Reflection.Primitives.dll

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14952
Entropy (8bit):	6.599053939997928
Encrypted:	false
SSDEEP:	192:mrlnC6xxk2R5Ws+Wql73WOL8/pCuPHnhWgN7aoWTF6lI+XqnajlkEv:6nbW2R5Ws+Wql7//uPHRN7SIImlqW
MD5:	EDA04E04EBC0EBF7F8BBF30C4DAE6DE3
SHA1:	7BC4D50E6EEC7F04A9272BFEE4E4DB6F278DBE63
SHA-256:	F3E55CB3ADFA93F563B09114D93062E680AB0864C220491458FBE151798B862F
SHA-512:	7027DA3404675596B71394B660E600DA12C0750895F624776362167869760555EE9990699FFC9E4407301FC9437B2F638E2734B8BDEF3C7054990FD5A9C86550
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."!..0.....^+... .....@.. ....`.....+..K....@.....h$...`.....T*..8..... ....H.....text...d.... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....@+.....H..... .....P .....H>.s..X.\...3V...?G../..3q..I.L.....qKy6b..u"HO...JmYQ.....J...*S..".R..=1RY. ....\?.&dM.....@'J.j.:.'.A.../.....I.BSJB.....v4.0.30319.....`.....#~.....#Strings.....#GUID.....#Blob.....3.....3.....@..... .Y.....`.....g...?.g.....g...y.g.....g.....g...`.g...m.g.....

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Rntgenstraaler\Overholde\Wingdings\Preaddition.Bor

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	ASCII text, with very long lines (36518), with no line terminators
Category:	dropped
Size (bytes):	36518
Entropy (8bit):	2.6830744752603626

Encrypted:	false
SSDEEP:	768:xeK/i8OrT1EEEN7NmGmBsb7IxbJhOANjoIi55GP++IssSCDu/2qnSsUHZlI:xeKv2n1OAE/EP9Ka/2lHzl
MD5:	AE738FA62A77E7AC245E166294F62CF4
SHA1:	EB347C2E02E3FBB39D316CEE73ED4B72DCA34C41
SHA-256:	4513093A8A81A33B2704FA5C8D168172A4A561188992D2AE1C93E1AF0611C076
SHA-512:	5B1241A8702E25C84D64CD7B6790852B46FA0848B16056FCFA0035CEAB1AB3448953D3FDF15DE7BB7D0074C7EC7E94748CFEDA625621E3BA5BFB3C4D813C82E2
Malicious:	false
Preview:	000000007E0000000F0F00C2007C009494000000C1000000008600000000000E1E1E1005757570000000000000000D007A7A000000002525250000000029290000008200001717000OFCFC000505050061000000000C500B500AC0077777700D8D8D8000000FE00BC00210000000000930000390078787878780OBEBE0000FE0000EE000075757500ACACAC001E1E0000005C000000000000000D0D0D0D0D0D0D0000005200140008000000004F4F000000006000006B6B6B0017001E006000DA0055550000004A4A000000000014000057575757570003B3B00010000E1E1005757575757005A5A000000A9A9009E005A5A00D7D7D700610000C900000000000D0D0D0D000A4A400007F00000000006A6A0000CA00007B7B00E2008E8E8E00B100D30000BBBBBB00E8000000000077770063636300002600DE00E3E3E3000028001212000000000000007A7A0000CE00EC007676760000005757009F9F00AD00A5A5003D004C4C4C0000003131310000ACACAC0000540000000000000000000000F3F3002929000000000020074000000BA000002000000000A8000000AB00000000004C4C4C4C4C00007E000000000000000000888800D2D2000202020200A3A3A3000000E70000FE000097000086000OC4000000170000005E0000BC00F9000000AA000000FA00A9000083000000C3C3C3007777700

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Rntgenstraaler\Overholde\Wingdings\System.Reflection.TypeExtensions.dll

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32368
Entropy (8bit):	6.393948275188786
Encrypted:	false
SSDEEP:	384:yWweWqlXnYcLpSfX0lawccfNXLWrdzy+A2jc2EPLNtAf/uPHRN7AJ/AlGseC62c:EqlXYcgEAwcc17Wc+bj+PLHuMU/xjx2c
MD5:	F2A123183E106BB1CF19376A8079D171
SHA1:	2B96296BE92D5F2EF7C59A70858AF4CAABC99A9D
SHA-256:	896D4ED138C35ECF19AE432380096562872EAB103F7E352C15D214FD875B337A
SHA-512:	FCA6A89EFB16780A06CD25A55638882970F03E1535180A0E463AF9794184B04EB345CF29B12D4F261094E04A584E9225A7AD36A62631227451059F64A77B3C67
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....[....." .....P..... ..`...@.....@..... .....<.....Z..p$...p.....T.....H.....text....N.....P..... ..`.data.....`.....R..... .....@....reloc.....p.....X.....@..B.....0.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...Z.!...C.o.m.m.e.n.t.s...S.y.s.t.e.m...R.e.f.l.e.c.t.i.o.n...T.y.p.e.E.x.t.e.n.s.i.o.n.s.....L... ..C.o.m.p.a.n.y.N.a.m.e.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...j.!...F.i.l.e.D.e.s.c.r.i.p.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Stereoing\preferences-desktop-font-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	225
Entropy (8bit):	6.596645802250635
Encrypted:	false
SSDEEP:	6:6v/lhPysi5NuhsPwRngRfPq/3+phjSfVsup:6v/7thstJACSNsc
MD5:	F894266AB6A933B2FDA751E6490C319A
SHA1:	2D2D3635198FEEFCB64D1D6B3CDCCDC4EA3DF4B0
SHA-256:	95F533585B4C61936C369557B3B7E397E56545A4C9DB9A5BDDD0E9ABB7A7F7E7
SHA-512:	977ED04753C3CB2B883D03A2A55001F6FCC8617DC3060B6C25AB7E5C691C3F76049E7DEADC7F6567AB7E8DC8492DE2874E8E632CF3EAD7B39ABC8CC98D33142
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..1..@.E...".u.`..#.v.,r.[..1$..]B.@6.,,.e.....fwg...._)9.....y..[n...t.$g..:...P....@k.q.....W.. .PY.$z..x....t..(-~!.0$:P.t.....`..... .Ba..Y.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Stereoing\task-due-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	263
Entropy (8bit):	6.731374842054556
Encrypted:	false

SSDEEP:	6:6v/lhPysw9TXm0RZC/8xhbPgfdSwj4vw29OjuAO4+ZvYNVp:6v/7QVXm0a/8xhbPgfdSBvNYn2ZvYd
MD5:	003B524806C1CA654CAC6ED2EB883E1B
SHA1:	F6F6ACA125DC4DB3B33378404017B5EE7D21D334
SHA-256:	2899E53769FA741E2C0675A2C69D2C246A8F34601BEE58DD66B16261005962A9
SHA-512:	AA905997F9CE39F039E33C4CCA167C0137775D91B4929D918528BA00B92737C448EC46D91A4221644CCC00D1FCAA403AFF83F07276BAB6FD80D4B9E88E652F8
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...K..1.D.....g.e=.x.....[]....Y$J'..`.@.S)R.4.q.D.K....x..%..0>~.;}..^.X....Lt.f!..K.....D.&,.7,..BM..t@..}N..o.?.....Hv.J...(..r.. ..)L...&..dT<..1y...X..X.....q...p..p.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Stereoing\window-close.png

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	337
Entropy (8bit):	7.143668471552015
Encrypted:	false
SSDEEP:	6:6v/lhPWFmX9Ckymx8BZhCjO5QO6MsHqd+K/eBDQeU2oG9xqgjp:6v/7K0omx8yOqVtHH1U2oGR
MD5:	7FBFE5B0A7AD2A67AACFD8481F8DCA01
SHA1:	21BABB6B7EC4746835DB43DC6A69A4AF0EFECA2D
SHA-256:	0B4CD789E087F712F131FACCD754DC461774498DF3CA19B346D461D18A0AE622
SHA-512:	3A8F0D9653301F789A0588E848C40FFC92394461BF70A3421ABC85647F2C115948134FE9E161D055A11D200536356A15677D9C0E645346D27E122001F67FE22B
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx..S.r.P..=7.cw.....W.m...=.....V....I...K.?#@D.0G.....R.rF..^$....p..b..f.<.T.z..... +..3#.v.K...$....pT.j.....[.....r..p....O.2.Y.T.,.....==...9{/..T./....Qa...3%....5...xmkI.7.1..P,g.%y..J..#^.e..I(.%jzI..#../..49...*..?#..I. =~..E.,MN@.....`...../...=.-...1....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Stersfarterne\Svigermdrenes.Hip

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	data
Category:	dropped
Size (bytes):	222555
Entropy (8bit):	7.344342205951728
Encrypted:	false
SSDEEP:	3072:pBmSzQUCQ7eiGVj+oHu80OFKzRem/0qaVnuHyAkwbH4A5ICfxHSdjByvg4T:fmioZd+osLdL/0FuVTjAuypPo
MD5:	1247D9E48508188AEA42C1860C123BDB
SHA1:	B94FAE1C07539802B0D102309BA9B6F2A10C2638
SHA-256:	C6FAD708D2D267FA214B467BA745F085BE0F86DE24F1CBD6DB02F9A168359668
SHA-512:	C2A18EA7DE077087EF70780D10796F338C7FD9764777E33F6AB6B68F32E370DC063AC463A1AF6299A9A50F8410352E5CC9D90F290389D7531F6B4A5666459BFD
Malicious:	false
Preview:	.....;;;.....C.....y.....|||.....6.....ppp.....77.....X.....)))......MM.....;;.....FFFFFF.....RR.....00....;;;;;;.....5.....uu.....).....dd.....t.....L.q.)..y.....++.....5.....**.....L....<.!.....o.....((..AAA.....VVV..WW...xxx..w.....4444..*.....f.....D.....T.....yyy.....!!..jj..bb.ccccc.B...1...;.....V.....g..q.....v....,..xxxx...Z.{.....&...m.....www..$$.....b.M.....$.....YYYY.....bb.....j..iiiii...&.....D.gg.....~.....)))..000.FFFF.n....._.....---.....g.....##.....))).Y.**.....c.....bb.....9.....T.....

C:\Users\user\AppData\Local\Temp\nsz62F8.tmp\AdvSplash.dll

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.496995234059773
Encrypted:	false
SSDEEP:	96:1IUNaXnnXyEIPtXvZhr5RwiULuxDtJ1+wolpE:1Ix3XyEwXvZh1RwnLUDtf+I
MD5:	E8B67A37FB41D54A7EDA453309D45D97
SHA1:	96BE9BF7A988D9CEA06150D57CD1DE19F1FEC19E
SHA-256:	2AD232BCCF4CA06CF13475AF87B510C5788AA790785FD50509BE483AFC0E0BCF
SHA-512:	20EFFAE18EEBB2DF90D3186A281FA9233A97998F226F7ADEAD0784FBC787FEEE419973962F8369D8822C1BBCDFB6E7948D9CA6086C9CF90190C8AB3EC97F4C38
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 3%, Browse

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+.Y.o.7Eo.7Eo.7Eo.6EF.7E..jEf.7E;..Em.7E..3En.7ERicho.7E..... ..PE..L.....uY.....!.....`..... .....P.....`$..E.... ..d.....@..$..... ..... .text..... ..`.rdata..... .....@..@.data.....0.....@....reloc.....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsz62F8.tmp\System.dll

Process:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.659384359264642
Encrypted:	false
SSDEEP:	192:ex24sihno00Wfl97nH6BenXwWobpWBTtvShJ5omi7dJWjOlESlS:h8Qll972eXqlWBFSt273YOlEz
MD5:	8B3830B9DBF87F84DDD3B26645FED3A0
SHA1:	223BEF1F19E644A610A0877D01EADC9E28299509
SHA-256:	F004C568D305CD95EDBD704166FCD2849D395B595DFF814BCC2012693527AC37
SHA-512:	D13CFD98DB5CA8DC9C15723EEE0E7454975078A776BCE26247228BE4603A0217E166058EBADC68090AFE988862B7514CB8CB84DE13B3DE35737412A6F0A8AC3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....uY.. .....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..`....P.....*.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.031249628696672
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	rJUSTIFICANTEDEPAGO.exe
File size:	433352
MD5:	e542cf9ce8a67a5b681cc9b0004e0b10
SHA1:	40161158f7cab76c57b4d95798c74ebc7d612cfe
SHA256:	4e78f6957f4c8c0f56a9b49e139342b1df7b1dc05518d96e776aa687a80f8c58
SHA512:	5cb1f2132c5d85f068ed5fc35229df5f83d711f30748a951bd006569a24df0818aa24effb91d171a895f342b1b9e14ad2df8a2f1124e1ef2c7f8c74a6b9627ce
SSDEEP:	6144:c6bAcJvkzKmPPzS58G93IuZjZz5VWY+LWWwseVp4ZLlbXrvAhM8LjbL7rrraAiGl:z7ubCHICV0LfwqZLlXTqMYvi7
TLSH:	CA94F1227F97E857E4266D78608AEE19AEB0DF249205D317F37139EDE9B53016C2B103
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..l@../OS..@...c>..@..+F...@..Rich.@.....PE..L.....uY.....d....:....

File Icon

Icon Hash:	20c4f8f8e8f0f24c

Static PE Info

General

Entrypoint:	0x403350
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui

Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x59759518 [Mon Jul 24 06:35:04 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	b34f154ec913d2d2c435cbd644e91687

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	E=Baccheion@Train.Ric, OU="Ukampdygtige Ratteners Fllesskolernes ", O=Amerciament, L=Putnam Valley, S=New York, C=US
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 21/12/2022 05:52:29 20/12/2025 05:52:29
Subject Chain	• E=Baccheion@Train.Ric, OU="Ukampdygtige Ratteners Fllesskolernes ", O=Amerciament, L=Putnam Valley, S=New York, C=US
Version:	3
Thumbprint MD5:	9D5FC1EED3EFD5AE85C5FE4E5DE73B01
Thumbprint SHA-1:	5C6F3AFCFAAFE00B47463625067078E82ACF72F1
Thumbprint SHA-256:	29E893BEBBB82AB1F213286EF68814B75D778BAB740B54B6457C756488BE3856
Serial:	53BB1A3E0600B528584097460509366C59C5C7CB

Entrypoint Preview
Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A8A2Ch], eax
je 00007FCB90F077D3h
push ebx
call 00007FCB90F0AA69h
cmp eax, ebx
je 00007FCB90F077C9h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007FCB90F0A9E3h
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FCB90F077ACh
push 0000000Ah

Instruction
call 00007FCB90F0AA3Ch
push 00000008h
call 00007FCB90F0AA35h
push 00000006h
mov dword ptr [007A8A24h], eax
call 00007FCB90F0AA29h
cmp eax, ebx
je 00007FCB90F077D1h
push 0000001Eh
call eax
test eax, eax
je 00007FCB90F077C9h
or byte ptr [007A8A2Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [007A8AF8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0079FEE0h
call dword ptr [00408188h]
push 0040A2C8h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x84fc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3d0000	0x28268	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x67a88	0x2240	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x63c8	0x6400	False	0.6766015625	data	6.504099201068482	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x138e	0x1400	False	0.4509765625	data	5.146454805063938	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39eb38	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x3a9000	0x27000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3d0000	0x28268	0x28400	False	0.3355129076086957	data	4.767250735975199	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3d0310	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x3e0b38	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0x3e9fe0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736	English	United States
RT_ICON	0x3ef468	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x3f3690	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x3f5c38	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x3f6ce0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0x3f7668	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x3f7ad0	0x100	data	English	United States
RT_DIALOG	0x3f7bd0	0xf8	data	English	United States
RT_DIALOG	0x3f7cc8	0xa0	data	English	United States
RT_DIALOG	0x3f7d68	0x60	data	English	United States
RT_GROUP_ICON	0x3f7dc8	0x76	data	English	United States
RT_MANIFEST	0x3f7e40	0x423	XML 1.0 document, ASCII text, with very long lines (1059), with no line terminators	English	United States

Imports

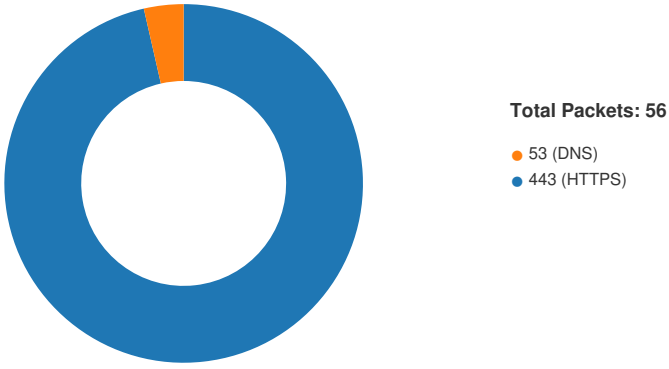
DLL	Import
KERNEL32.dll	SetEnvironmentVariableW, SetFileAttributesW, Sleep, GetTickCount, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, SetCurrentDirectoryW, GetFileAttributesW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, lstrlenW, lstrcpynW, GetDiskFreeSpaceW, ExitProcess, GetShortPathNameW, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, CreateFileW, GetTempFileNameW, WriteFile, lstrcpyA, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, lstrcmpiW, MoveFileW, GetFullPathNameW, SetFileTime, SearchPathW, CompareFileTime, lstrcmpW, CloseHandle, ExpandEnvironmentStringsW, GlobalFree, GlobalLock, GlobalUnlock, GlobalAlloc, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, lstrlenA, MulDiv, MultiByteToWideChar, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW
USER32.dll	GetSystemMenu, SetClassLongW, EnableMenuItem, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, ScreenToClient, GetWindowRect, GetDlgItem, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, GetDC, SetTimer, SetWindowTextW, LoadImageW, SetForegroundWindow, ShowWindow, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, EndPaint, CreateDialogParamW, SendMessageTimeoutW, wsprintfW, PostQuitMessage
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExW, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, SHFileOperationW
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExW, RegOpenKeyExW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, RegEnumValueW, RegDeleteKeyW, RegDeleteValueW, RegCloseKey, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:23:11.148125887 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.148149967 CET	443	49816	172.217.16.206	192.168.11.20
Mar 20, 2023 11:23:11.148309946 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.161170959 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.161183119 CET	443	49816	172.217.16.206	192.168.11.20
Mar 20, 2023 11:23:11.193301916 CET	443	49816	172.217.16.206	192.168.11.20
Mar 20, 2023 11:23:11.193433046 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.193612099 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.194029093 CET	443	49816	172.217.16.206	192.168.11.20
Mar 20, 2023 11:23:11.194288969 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.265213013 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.266252041 CET	443	49816	172.217.16.206	192.168.11.20
Mar 20, 2023 11:23:11.266392946 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.269294024 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.312500000 CET	443	49816	172.217.16.206	192.168.11.20
Mar 20, 2023 11:23:11.548156977 CET	443	49816	172.217.16.206	192.168.11.20
Mar 20, 2023 11:23:11.548352957 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.548438072 CET	443	49816	172.217.16.206	192.168.11.20
Mar 20, 2023 11:23:11.548583984 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.548625946 CET	443	49816	172.217.16.206	192.168.11.20
Mar 20, 2023 11:23:11.548651934 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.548688889 CET	443	49816	172.217.16.206	192.168.11.20
Mar 20, 2023 11:23:11.548733950 CET	443	49816	172.217.16.206	192.168.11.20
Mar 20, 2023 11:23:11.548985958 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.548985958 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.548985958 CET	49816	443	192.168.11.20	172.217.16.206
Mar 20, 2023 11:23:11.641153097 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:11.641195059 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:11.641344070 CET	49817	443	192.168.11.20	142.250.186.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:23:11.641753912 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:11.641777992 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:11.681567907 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:11.681797981 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:11.681797981 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:11.682383060 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:11.682543039 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:11.682563066 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:11.685803890 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:11.685817957 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:11.686108112 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:11.686331034 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:11.686677933 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:11.728390932 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.091964960 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.092227936 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.092228889 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.092359066 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.092581987 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.092612028 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.092665911 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.092758894 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.092834949 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.092834949 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.093034983 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.093281984 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.093947887 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.094284058 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.094346046 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.094567060 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.096529007 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.096740007 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.096829891 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.097059965 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.098711967 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.099062920 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.100601912 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.100784063 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.100878954 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.101051092 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.101166964 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.101330996 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.101402998 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.101568937 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.101603031 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.101632118 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.101773977 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.101773977 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.101876020 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.102026939 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.102076054 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.102236986 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.102243900 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.102284908 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.102389097 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.102389097 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.102442026 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.102590084 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.102626085 CET	443	49817	142.250.186.33	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:23:12.102776051 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.103457928 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.103616953 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.103741884 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.103909969 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.103996038 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.104151964 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.104202986 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.104234934 CET	443	49817	142.250.186.33	192.168.11.20
Mar 20, 2023 11:23:12.104352951 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.104353905 CET	49817	443	192.168.11.20	142.250.186.33
Mar 20, 2023 11:23:12.104458094 CET	443	49817	142.250.186.33	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:23:11.131897926 CET	53658	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:23:11.141695023 CET	53	53658	1.1.1.1	192.168.11.20
Mar 20, 2023 11:23:11.612874031 CET	62382	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:23:11.639658928 CET	53	62382	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 11:23:11.131897926 CET	192.168.11.20	1.1.1.1	0x8c78	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:23:11.612874031 CET	192.168.11.20	1.1.1.1	0x5dc4	Standard query (0)	doc-0s-98-docs.googleusercontent.com	A (IP address)	IN (0x0001)	false

DNS Answers

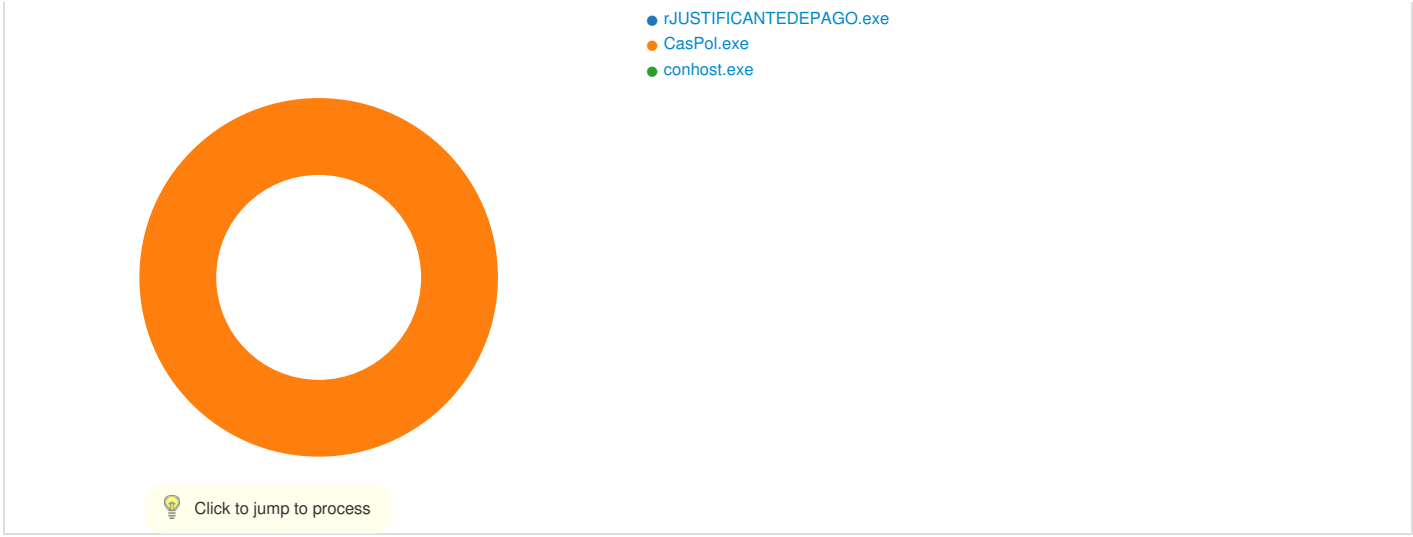
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:23:11.141695023 CET	1.1.1.1	192.168.11.20	0x8c78	No error (0)	drive.google.com		172.217.16.206	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:23:11.639658928 CET	1.1.1.1	192.168.11.20	0x5dc4	No error (0)	doc-0s-98-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:23:11.639658928 CET	1.1.1.1	192.168.11.20	0x5dc4	No error (0)	googlehosted.l.googleusercontent.com		142.250.186.33	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- drive.google.com
- doc-0s-98-docs.googleusercontent.com

Statistics

Behavior



System Behavior

Analysis Process: rJUSTIFICANTEDEPAGO.exe PID: 4708, Parent PID: 4836

General

Target ID:	2
Start time:	11:21:21
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
Imagebase:	0x400000
File size:	433352 bytes
MD5 hash:	E542CF9CE8A67A5B681CC9B0004E0B10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.2804076292.0000000005376000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: **4160**, Parent PID: **4708**

General

Target ID:	7
Start time:	11:23:02
Start date:	20/03/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\rJUSTIFICANTEDEPAGO.exe
Imagebase:	0xaa0000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.6893759617.00000000360C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.6893759617.00000000360C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	232780B	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	232780B	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	232780B	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	232780B	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	232780B	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	232780B	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	73193263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	73193263	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	73193263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	73193263	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	7319099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	7319099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7319099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7319099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	730E62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	7319D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	7319D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7319D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	730E62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	730E62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	730E62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	730E62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7319099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7319099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	720F9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	720F9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	720F9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	720F9B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	730E62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	7319099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	7319099B	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	23	720F9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	720F9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	720F9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	720F9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\7c853485-8994-4511-bd4d-34f894f02b20	unknown	4096	success or wait	2	720F9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\7c853485-8994-4511-bd4d-34f894f02b20	unknown	4096	success or wait	2	720F9B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	720F9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	720F9B71	ReadFile

Analysis Process: conhost.exe PID: **8068**, Parent PID: **4160**

General

Target ID:	8
Start time:	11:23:02
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff78c150000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly