ID: 319311
Sample Name: PURCHASE ORDER No-17-11-98543.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:56:19
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

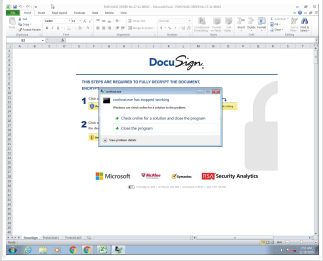
Analysis Report PURCHASE ORDER No-17-11-98543.xls…

Overview

General Information

Sample Name:	PURCHASE ORDER No-17-11-98543.xlsm
Analysis ID:	319311
MD5:	921ac551fe8d88c..
SHA1:	40702dc4f773cfa..
SHA256:	b1660b65514182..
Tags:	xlsm

Most interesting Screenshot:



Detection

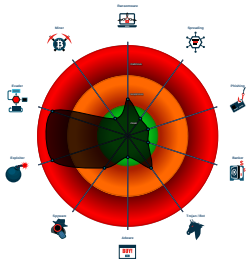
Hidden Macro 4.0

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

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Document exploit detected (creates …
- Document exploit detected (drops P…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Contains functionality to detect slee…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found abnormal large hidden Excel …
- Machine Learning detection for dropp…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1756 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - conhost.exe (PID: 2512 cmdline: 'C:\ETTER\dAneDFma\conhost.exe' MD5: F5ECCDDC7EE3DF74B79DF21D04DD56A1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.2117438541.000000000580000.00000004.00000001.sdmp	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x58de0:$s1: 7++/epp
00000003.00000003.2117438541.000000000580000.00000004.00000001.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x58b70:$xo1: /\x0D\x18\x0B\x0E\x0E\x03MWLR • 0x58c90:$xo1: ?\x1D\x08\x1B\x1E\x1E\x13]G\B
00000003.00000002.2168715128.000000000510000.00000040.00000001.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x599c0:$xo1: /\x0D\x18\x0B\x0E\x0E\x03MWLR • 0x59ae0:$xo1: ?\x1D\x08\x1B\x1E\x1E\x13]G\B
00000003.00000002.2168603978.000000000F8000.00000040.00000001.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x31849:$xo1: /\x0D\x18\x0B\x0E\x0E\x03MWLR • 0x31966:$xo1: ?\x1D\x08\x1B\x1E\x1E\x13]G\B
00000003.00000002.2168630722.000000000400000.00000040.00020000.sdmp	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x5a7e0:$s1: 7++/epp • 0x60160:$s1: http:// • 0x60160:$f1: http://

Click to see the 1 entries

Unpacked PEs

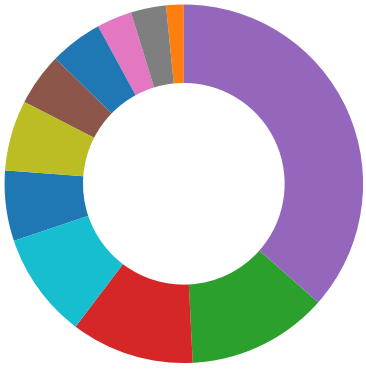
Source	Rule	Description	Author	Strings
3.2.conhost.exe.400000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x58de0:$s1: 7++/epp
3.2.conhost.exe.400000.0.unpack	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x58b70:$xo1: /\x0D\x18\x0B\x0E\x0E\x03MWLR • 0x58c90:$xo1: ?\x1D\x08\x1B\x1E\x1E\x13]G\B
3.2.conhost.exe.400000.0.raw.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x5a7e0:$s1: 7++/epp • 0x60160:$s1: http:// • 0x60160:$f1: http://
3.2.conhost.exe.400000.0.raw.unpack	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x5a570:$xo1: /\x0D\x18\x0B\x0E\x0E\x03MWLR • 0x5a690:$xo1: ?\x1D\x08\x1B\x1E\x1E\x13]G\B
3.3.conhost.exe.580000.0.raw.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x58de0:$s1: 7++/epp
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: System File Execution Location Anomaly

Signature Overview



- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

Found abnormal large hidden Excel 4.0 Macro sheet

Office process drops PE file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

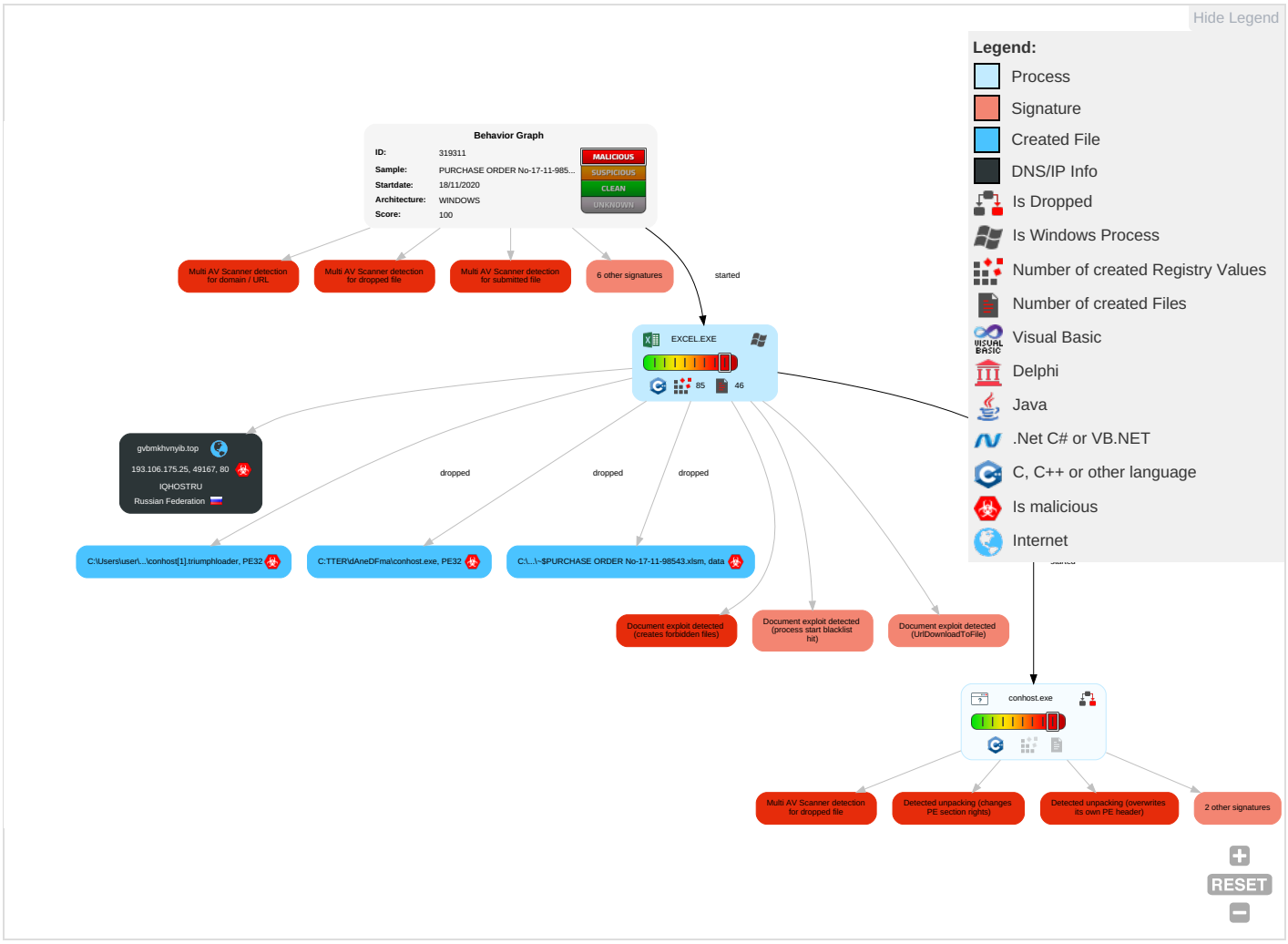
Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 2	Application Shimming 1	Process Injection 1	Masquerading 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scripting 1 1	Boot or Logon Initialization Scripts	Application Shimming 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 4	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	Exploitation for Client Execution 4 3	Logon Script (Windows)	Extra Window Memory Injection 1	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 2 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Extra Window Memory Injection 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Statio

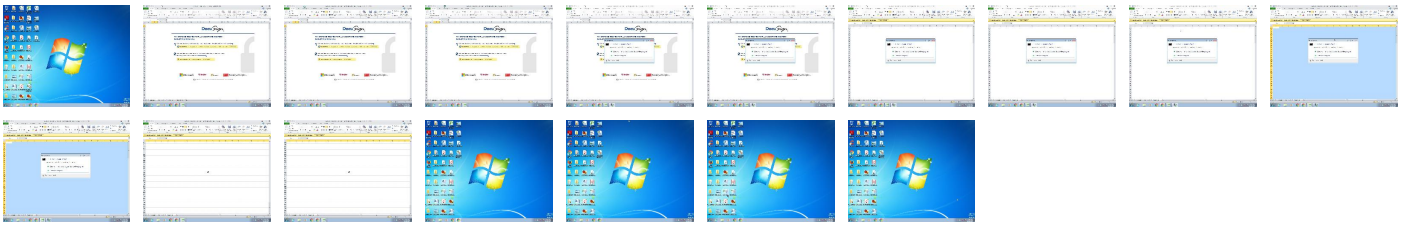
Behavior Graph

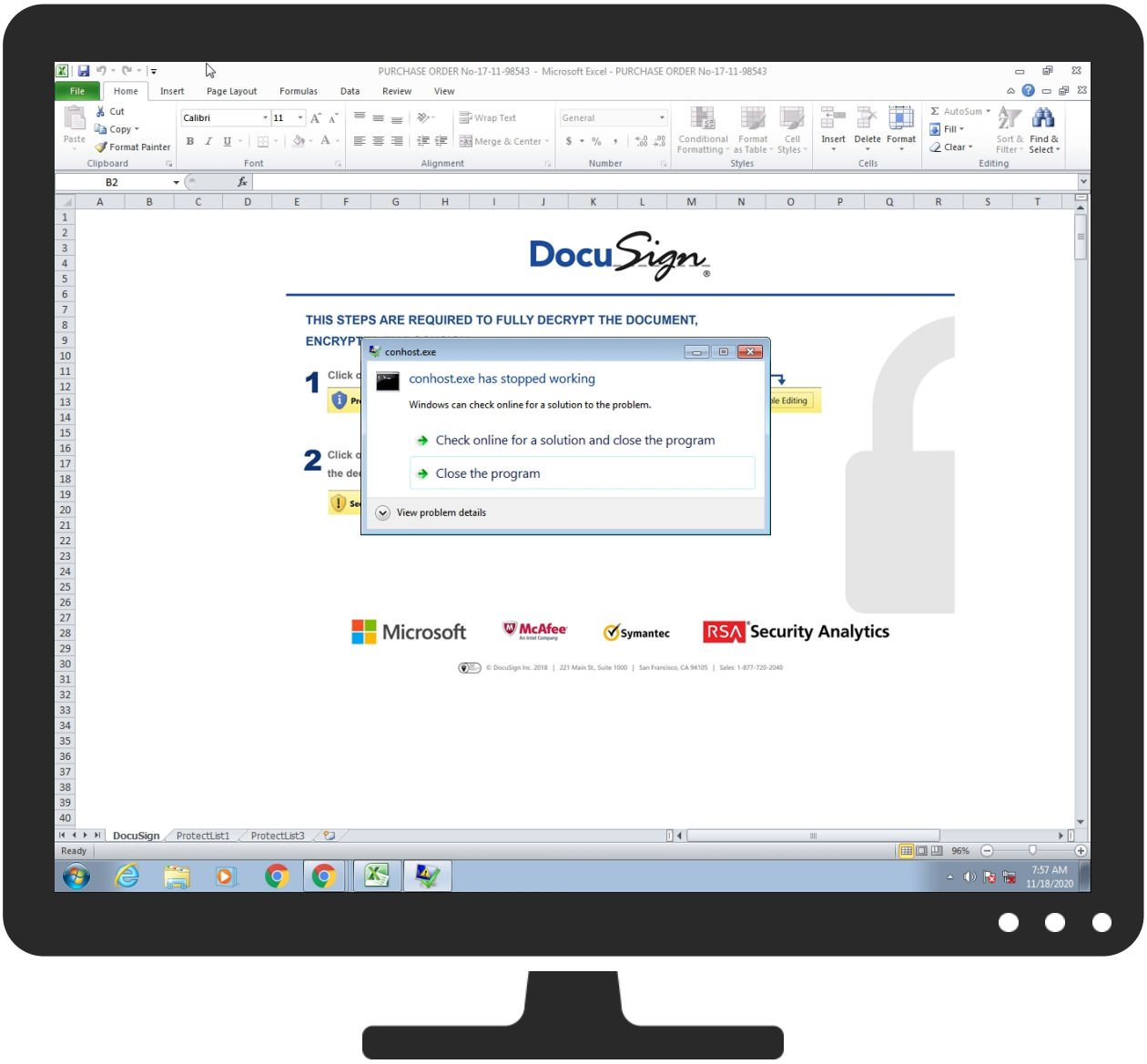


Screenshots

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
PURCHASE ORDER No-17-11-98543.xlsm	9%	Virustotal		Browse
PURCHASE ORDER No-17-11-98543.xlsm	6%	ReversingLabs	Document-Office.Downloader.SLoad	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ETTER\dAneDFma\conhost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\conhost[1].triumphloader	100%	Joe Sandbox ML		
C:\ETTER\dAneDFma\conhost.exe	29%	Virustotal		Browse
C:\ETTER\dAneDFma\conhost.exe	23%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\conhost[1].triumphloader	23%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
gvbmkhvnyib.top	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://gvbmkhvnyib.top/QtuFGobZaW/conhost.triumphloader	7%	Virustotal		Browse
http://gvbmkhvnyib.top/QtuFGobZaW/conhost.triumphloader	0%	Avira URL Cloud	safe	
http://4cnx9s25gsvw.top/syZsNnTNps.vx	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gvbmkhvnyib.top	193.106.175.25	true	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gvbmkhvnyib.top/QtuFGobZaW/conhost.triumphloader	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://4cnx9s25gsvw.top/syZsNnTNps.vx	conhost.exe	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.106.175.25	unknown	Russian Federation		50465	IQHOSTRU	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319311
Start date:	18.11.2020
Start time:	07:56:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PURCHASE ORDER No-17-11-98543.xlsm
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:	7
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.expl.evad.winXLSM@3/10@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.2% (good quality ratio 4.1%) • Quality average: 74.4% • Quality standard deviation: 19.8%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • 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, WerFault.exe, svchost.exe • TCP Packets have been reduced to 100

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IQHOSTRU	VSL- DOCSVtLthwicBDYP6rk- xlsx.exe	Get hash	malicious	Browse	• 193.106.175.134
	COS1102213211.exe	Get hash	malicious	Browse	• 193.106.175.134
	ZT3146457.exe	Get hash	malicious	Browse	• 193.106.175.134
	PO.W424676.exe	Get hash	malicious	Browse	• 193.106.175.134
	KYOCERA.pdf.exe	Get hash	malicious	Browse	• 193.106.175.134
	1pGk0WbLBY.exe	Get hash	malicious	Browse	• 193.106.175.47
	Invoice.exe	Get hash	malicious	Browse	• 193.106.175.47
	remittance confirmation.xlsx	Get hash	malicious	Browse	• 193.106.175.47
	Quotation Complete Overhaul of Main Engine Niigata.exe	Get hash	malicious	Browse	• 193.106.175.47
	fHKvj3Yr9U.exe	Get hash	malicious	Browse	• 193.106.175.47
	Bmxcixs_Signed_.exe	Get hash	malicious	Browse	• 193.106.175.47
	Original Invoice-COAU7226107650.xlsx	Get hash	malicious	Browse	• 193.106.175.47
	yO07G0lvTRQkenm.exe	Get hash	malicious	Browse	• 193.106.175.47
	Mg3eGjc18X.exe	Get hash	malicious	Browse	• 193.106.175.47
	shipment_terms.xlsx	Get hash	malicious	Browse	• 193.106.175.47
	Bank Details.doc.exe	Get hash	malicious	Browse	• 193.106.175.47
	6236463D8973.pdf.exe	Get hash	malicious	Browse	• 193.106.175.47
	SDT_R224e18032356210_XLS.exe	Get hash	malicious	Browse	• 193.106.175.47
	0KtzKZlkMHhoTcu.exe	Get hash	malicious	Browse	• 193.106.175.47
	eWuKwajjuP.exe	Get hash	malicious	Browse	• 193.106.175.47

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ETTER\dAneDFma\conhost.exe

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	297472
Entropy (8bit):	7.789180781231072
Encrypted:	false
SSDEEP:	6144:niLXVcyDs4gQBOJVnl5EIoAxI2ioM+pQDCuaN9T3y3Dw6hjNScK:niLXVKJ93cuYWdT3yzppM1
MD5:	F5ECCDDC7EE3DF74B79DF21D04DD56A1
SHA1:	5E464AEF69763C3FC25BCEADFD8FFF32A405D849
SHA-256:	D893D3B0E8C2FA238A84EEEC1ADB6DEC0853828D314873BE41EE74280541B6D0
SHA-512:	10023265D4AAB08D6CED1B32554754BFA3ED1941F6F92ECB21457CB73AFFBA0FAA8C115E2E2B56ECE9EAAEDB04D82C9EFFDEE65BDE1FF328A8FEB276F9F41578
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 23%
Reputation:	low

C:\ETTER\dAneDFma\conhost.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....rh..rh..rh.. ...rh.. ...rh.. ..rh.....rh..ri.rh.. ...rh.. ...rh.. ...rh.Rich. rh.....PE..L.....P^.....$.....@....@.....,Y..<.....&.....0U.....T..@.....@.... .....text...U#.....$..... ..`.rdata..0"...@...$...(.....@..@.data...XJ...p.....L.....@....tls.....`.....@....rsrc....&.....(...b..... ..@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\conhost[1].triumphloader	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	297472
Entropy (8bit):	7.789180781231072
Encrypted:	false
SSDEEP:	6144:niLXVcyDs4gQBOJVnl5EIoAxI2ioM+pQDCuaN9T3y3Dw6hjNScK:niLXVKJ93cuYWdT3yzppM1
MD5:	F5ECCDDC7EE3DF74B79DF21D04DD56A1
SHA1:	5E464AEF69763C3FC25BCEADFD8FFF32A405D849
SHA-256:	D893D3B0E8C2FA238A84EEEC1ADB6DEC0853828D314873BE41EE74280541B6D0
SHA-512:	10023265D4AAB08D6CED1B32554754BFA3ED1941F6F92ECB21457CB73AFFBA0FAA8C115E2E2B56ECE9EAAEDB04D82C9EFFDEE65BDE1FF328A8FEB276F9F41578
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 23%
Reputation:	low
IE Cache URL:	http://gvbmkhvnyib.top/QtuFGobZaW/conhost.triumphloader
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....rh..rh..rh.. ...rh.. ...rh.. ..rh.....rh..ri.rh.. ...rh.. ...rh.. ...rh.Rich. rh.....PE..L.....P^.....$.....@....@.....,Y..<.....&.....0U.....T..@.....@.... .....text...U#.....$..... ..`.rdata..0"...@...$...(.....@..@.data...XJ...p.....L.....@....tls.....`.....@....rsrc....&.....(...b..... ..@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\71A94C24.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 9 x 6, 8-bit colormap, interlaced
Category:	dropped
Size (bytes):	152
Entropy (8bit):	4.902652329045401
Encrypted:	false
SSDEEP:	3:yionv//thPlzlZRMlp8Lts7CX9/rIREYY2jm6Kpgsyx9yGlvH1p:6v/lhPxpkp8R/BI02j+Odyi9p
MD5:	A2C42F13DD6F6D98613D78C954D8E958
SHA1:	5D6EA91767736E71BB225D9408A21634E959C0EA
SHA-256:	CBA123392EDFD088C8A34FF7DEDFDDD581712E1EC70A30B24E95EBF037C29625
SHA-512:	18F11A9EE85D9EAB340FF27FC1FCEBB1F9F0C945AF110364CE93634251E8EFC07A325F24572B42C2EA12EB60195FD94C70F7644C2698DE4BE70C49AC82B318BF
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....Q.ta....sRGB.....gAMA.....a.....PLTE.....U..~....tRNS...0J....pHYs.....o.d....IDAT.Wc..00...B.....@....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A97335D5.jpg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 2806x1984, frames 3
Category:	dropped
Size (bytes):	157646
Entropy (8bit):	7.675046596886803
Encrypted:	false
SSDEEP:	3072:5G+FN/z4Oy7iR7Dzg8r/vQWtcGu9SovWBGv8ue+fFPrVPSA7QAp0JOs:51huWtcGWSoyGEAfFgCOEs
MD5:	EB37A7A3F548D1174FD2B0A4255B4843
SHA1:	4BB5CA34A1760676800497D3FE65C4A3596BB383
SHA-256:	1EC71CD6171D14F9BC6DA014D98E41AD5117A9CC70C8D921365FB65221F79C53
SHA-512:	87E29834910DD24ED489DF640689BB2B7E9729FFF33A3CC84295E4CF06F0A0AA0536939C019EC381D5DC5E2C530641E14357195BBCB06010F9D3D0CE8D5ED0D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A97335D5.jpg	
Preview:	......JFIF.....'.....'#*" "*#>1++1>H<9<HWNNWmhm.....'.....'#*" "*#>1++1>H<9<HWNNWmhm....."..... ....Wp..O.UmK.....MAK.^..... .....L..W..i.a!.....j./.....#..e.....*-b./.P..M....._".'$.L_@....).Rm.....+...6.\. .....0....W..... {.6&.{..@4.....

C:\Users\user\AppData\Local\Temp\68FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	402957
Entropy (8bit):	7.779201075265673
Encrypted:	false
SSDEEP:	3072:lKvrVXAx/8mQKPVOmvmpmImonVRQMVG+FN/z4Oy7iR7Dzg8r/vQWtcGu9SovWBGt:l+mvmpmImMD1huWtcGWSoyGEAfFgCOEl
MD5:	CE344653150155D9D547D42876AA35A5
SHA1:	BACD23941EAE898AF6A1BDB30A020BF88747B033
SHA-256:	1EAC165A5F9B3BBDC7092053358 75FBCF2E6ED4C0E78E41B5B41C21A45550722
SHA-512:	FCDEE4A12FBEB7EE38E41C646D524590E43407A95943F9D5EB5C98D3C897AFEBBDFEEF92F8A428D4CCBF7C2EB212E5E170CFCB6612260AC9C2BB7EBD0D2769F7
Malicious:	false
Reputation:	low
Preview:	.U.N#1....?.|E3. ..*..<...|@cw2&~.m .{|'dI..F q.....lft.....-;j..B+.Tv...../.(.....~.....F..s.....y.ig...a.=.)L.....\8...:..l4..1<.X]...B...V./.e..)..y.oE.....7.b.z..I.r.:...0...!.k.H.9..o....I..Jbu. !^.If.L.W....M.....g.uC.bl....-<jL{...L.I....@.^...J.t...6...,..n..2....t...M....=....n-...~.K.=.).5...]....A@y.C.o?..c.=:d..,/....2...t;o...o....o..]...CT.j..z.15....=... Qn...5.....PK.....!.L.L..... .....[Content_Types].xml ...(..... ....N

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Nov 18 14:56:49 2020, atime=Wed Nov 18 14:56:49 2020, length=16384, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.4779282422579785
Encrypted:	false
SSDEEP:	12:85QVJLgXg/XAlCPCHaXtB8XzB/UUkh/vX+WnicvbhnbDtZ3YilMMEpxRljKBTdJU:85sj/XTd6jOhXYeNDv3qErNru/
MD5:	163352799BFEEAA2E7ADF3EB03067A17
SHA1:	4E8D4D20F4B0FA986BB362AB09FB984D5A2D0EBE
SHA-256:	DFF13D9964198AD8BB1E83AAF26F4A882BCCAF8B1C355BA22130D163B294D416
SHA-512:	AC5FDDB7A67E02A199BE8C67582028005E8D54CE08DF36D31BFC396C475814FFE868DD90C84E6B33FC4FB8B9C906B7508710EE384F005671CCCA3910A1C41A4
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G.....l.....l....@.....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....rQ....Desktop.d.....QK.XrQ..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1. 7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\992547\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L8C ....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....992547.....D_....3N...W...9r.[.*.....}EkD_....3N...W ...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PURCHASE ORDER No-17-11-98543.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:16 2020, mtime=Wed Nov 18 14:56:49 2020, atime=Wed Nov 18 14:56:49 2020, length=402957, window=hide
Category:	dropped
Size (bytes):	4456
Entropy (8bit):	4.579357809049034
Encrypted:	false
SSDEEP:	96:8O4/XojFkTyT/EQh2O4/XojFkTyT/EQh2O4/XojFkTyT/EQh2O4/XojFkTyT/EQ/:8yjFSQEyjFSQEyjFSQEyjFSQ/
MD5:	B2D166D12A6637FE97494F0087A1FACF
SHA1:	D94EEE9B0CA669F4BC739B752F4A703BA282BD13
SHA-256:	8B4AA8F791979C5B7C2D9ED6275B6F9CB5086D3B63892799C626B4E123950B27
SHA-512:	2356D8F8431A0DCD2B0FC528E35967CEBE96C301D2F0A701A4698E41FED40E14436459EC5911C1D29FB99CA4A01D557E682372FBDD5641810C21B97A2C2724C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PURCHASE ORDER No-17-11-98543.LNK

Preview:

L.................F.... ....{.....l...|..l....&.........................P.O. .:i.....+00.../C:\.................t.1.....QK.X..Users.`.......:..QK.X*..................6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-
.2.1.8.1.3.....L.1......Q.y..user.8......QK.X.Q.y*...&=....U..............A.l.b.u.s.....z.1......Q.y..Desktop.d......QK.X.Q.y*..._=.............:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1
.7.6.9.......2.....rQ.. .PURCHA~1.XLS..r.......Q.y.Q.y*...8....................P.U.R.C.H.A.S.E. .O.R.D.E.R. .N.o.-.1.7.-.1.1.-.9.8.5.4.3...x.l.s.m.....................-...8...[...........?J......C
:\Users\..#..................\\992547\Users.user\Desktop\PURCHASE ORDER No-17-11-98543.xlsm.9.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.U.R.C.H.A.S.E. .O.R.D.E.R. .N.o.-
.1.7.-.1.1.-.9.8.5.4.3...x.l.s.m........:..,.LB.)...Ag..............1SPS.XF.L8C....&.m.m...........-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	306
Entropy (8bit):	4.979468454503797
Encrypted:	false
SSDEEP:	6:dj+lgg3sTOUlgg3sTmlgg3sTOUlgg3sTmlgg3sTOUlgg3sTmlgg3sTq:dOgrTlgrTCgrTlgrTCgrTlgrTCgrTq
MD5:	AA32031DB61362C7645F72B5CF99760F
SHA1:	DB105CCA2EE4332E413D8BF63DB980BE0D2624C1
SHA-256:	3992E9591EB0D63A33F27CDAE69B8C03518D89027A1FA1FC693BBED60E795D96
SHA-512:	A59ADDEEDBA11A288BFCFC1047ABFEF0A98B10AA38EFC9C6B013C6B87FCEFEC202D652625619B14DC67E3D250DB572FBAE0B2818B9270E7C1476831D3D0AE 251
Malicious:	false
Reputation:	low

Preview:

Desktop.LNK=0..[misc]..PURCHASE ORDER No-17-11-98543.LNK=0..PURCHASE ORDER No-17-11-98543.LNK=0..[misc]..PURCHASE ORDER No-17-11-9
8543.LNK=0..PURCHASE ORDER No-17-11-98543.LNK=0..[misc]..PURCHASE ORDER No-17-11-98543.LNK=0..PURCHASE ORDER No-17-11-98543.LNK=0..
[misc]..PURCHASE ORDER No-17-11-98543.LNK=0..

C:\Users\user\Desktop\2AFE0000

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	402957
Entropy (8bit):	7.779201075265673
Encrypted:	false
SSDEEP:	3072:lKvrVXAx/8mQKPVOmvmpmImonVRQMVG+FN/z4Oy7iR7Dzg8r/vQWtcGu9SovWBGt:l+mvmpmImMD1huWtcGWSoyGEAfFgCOEl
MD5:	CE344653150155D9D547D42876AA35A5
SHA1:	BACD23941EAE898AF6A1BDB30A020BF88747B033
SHA-256:	1EAC165A5F9B3BBDC709205335875FBCF2E6ED4C0E78E41B5B41C21A45550722
SHA-512:	FCDEE4A12FBEB7EE38E41C646D524590E43407A95943F9D5EB5C98D3C897AFEBBDFEEF92F8A428D4CCBF7C2EB212E5E170CFCB6612260AC9C2BB7EBD0D27 69F7
Malicious:	false
Reputation:	low

Preview:

.U.N#1....?.|E3. ..*..<...|@cw2&~.m .{l'dI..F q.......lft.....-;j..B+.Tv...../.(...........~.....F..s.....y.ig...a.=.)L.....\8...:..l4..1<.X]...B...V./.e..)..y.oE........7.b.z..I.r.:..0...!.k.H.9..o....I..Jbu.
!^.If.L.W....M.....g.uC.bl....-<jL{...L.I....@.^...J.t...6...,..n..2....t...M....=....n-...~.K.=.).5...]....A@y.C.o?..c.=:d..,./....2...t;o...o....o..]...CT.j..z.15....=... Qn...5.........PK..........!.L.L.....
........[Content_Types].xml ...(..
....
.............................N

C:\Users\user\Desktop\~$PURCHASE ORDER No-17-11-98543.xlsm

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	495
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fj/FFDJw2fV:vBFFGaFFGaFFGS
MD5:	98D7F9B901C91608CD7EA5509662BBCA
SHA1:	F166635CE572B615A1D80076A1AE8DE9220473CF
SHA-256:	F07A8B18E5B50003C42020241E82DDCCFBE254236AF2678C3CEFA4709100F4FE
SHA-512:	5536FD72C18081A1CFB46EB2E311BB257764C53B293E0D4B90F9C6C5EFB00E5A3A28190A2D04F3EE2819CF8DC7EBA7747DC8E8910C8716ACA7BAED0532142D C
Malicious:	**true**
Reputation:	low

Preview:

.user ..A.l.b.u.s. . . . .user ..A.l.b.u.s. . . . .
. . . .user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.772704052855693
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	PURCHASE ORDER No-17-11-98543.xlsm
File size:	401046
MD5:	921ac551fe8d88c2185f39f0e777eabd
SHA1:	40702dc4f773cfa3fcf03c62ec810ba3f5e6b72d
SHA256:	b1660b65514182bf97a767caa264b0500ef14692e69dae6 ddca344591e7e016d
SHA512:	41ca8f90604f42fc4a6685293d349e11e4267a2bbb09986 a9ba4e5aaccf6424386cf877ddf7dfb5898314a388bce02 390537ea7cbe37255f8d3730d050c057aa
SSDEEP:	6144:AESKAVwFGxh1huWtcGWSoyGEAfFgCOExMR:t SKAVwFMtuEcd6GEAfF9x4
File Content Preview:	PK..........!.v.Fa...........docProps/app.xml ...(.................. ....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "PURCHASE ORDER No-17-11-98543.xlsm"

Indicators

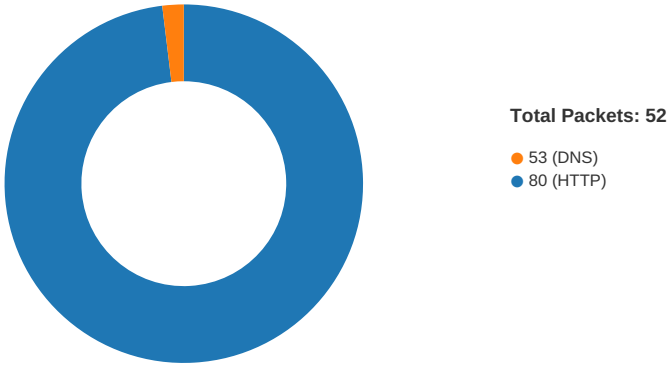
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,s,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 07:57:22.702124119 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.760700941 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.760807991 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.761539936 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.819969893 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.830245018 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.830284119 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.830322981 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.830338001 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.830382109 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.830415964 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.834037066 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.834095001 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.834167004 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.834170103 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.834219933 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.834230900 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.834289074 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.834362984 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.834403992 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.834440947 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.834477901 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.834654093 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.835695982 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.889010906 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.889027119 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.889090061 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.889094114 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.889122963 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.889137030 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.889257908 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.889316082 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.889333963 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.889379025 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.889451027 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.889496088 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.889579058 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.889630079 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.889655113 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.889700890 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.891089916 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.892719030 CET	80	49167	193.106.175.25	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 07:57:22.892774105 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.892829895 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.892855883 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.892894030 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.892968893 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.892992973 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.893013000 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.893090010 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.893150091 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.893174887 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.893232107 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.893290043 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.893347979 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.893373013 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.893455029 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.893526077 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.893585920 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.893651009 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.893654108 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.893717051 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.893781900 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.893857956 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.893861055 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.893913984 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.896778107 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.947757959 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.947827101 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.947845936 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.947926998 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.947952032 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.947954893 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.947993994 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.948029041 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.948065996 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.948134899 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.948178053 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.948230028 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.948272943 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.948359013 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.948404074 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.948508978 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.948559046 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.948582888 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.948622942 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.948703051 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.948745012 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.948831081 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.948873997 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.948945999 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.948988914 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.949076891 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.949155092 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.949194908 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.949265003 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.949304104 CET	80	49167	193.106.175.25	192.168.2.22
Nov 18, 2020 07:57:22.949351072 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.949570894 CET	49167	80	192.168.2.22	193.106.175.25
Nov 18, 2020 07:57:22.951247931 CET	80	49167	193.106.175.25	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 07:57:22.464179039 CET	52197	53	192.168.2.22	8.8.8.8
Nov 18, 2020 07:57:22.688311100 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2020 07:57:22.464179039 CET	192.168.2.22	8.8.8.8	0xfda2	Standard query (0)	gvbmkhvnyib.top	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2020 07:57:22.688311100 CET	8.8.8.8	192.168.2.22	0xfda2	No error (0)	gvbmkhvnyib.top		193.106.175.25	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gvbmkhvnyib.top

HTTP Packets

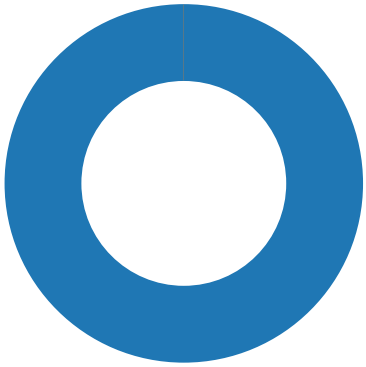
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	193.106.175.25	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 07:57:22.761539936 CET	0	OUT	GET /QtuFGobZaW/conhost.triumphloader HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: gvbmkhvnyib.top Connection: Keep-Alive
Nov 18, 2020 07:57:22.830245018 CET	2	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 18 Nov 2020 06:57:22 GMT Content-Length: 297472 Connection: keep-alive Last-Modified: Wed, 18 Nov 2020 00:57:27 GMT ETag: "48a00-5b457185761f5" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 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 ad 13 06 a2 e9 72 68 f1 e9 72 68 f1 e9 72 68 f1 f7 20 ec f1 cf 72 68 f1 f7 20 fd f1 fa 72 68 f1 f7 20 eb f1 98 72 68 f1 ce b4 13 f1 ec 72 68 f1 e9 72 69 f1 9b 72 68 f1 f7 20 e2 f1 e8 72 68 f1 f7 20 fc f1 e8 72 68 f1 f7 20 f9 f1 e8 72 68 f1 52 69 63 68 e9 72 68 f1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 07 1b 50 5e 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 24 04 00 00 b2 05 00 00 00 00 00 b9 15 00 00 00 10 00 00 00 40 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 0a 00 00 04 00 00 d1 b0 04 00 02 00 00 80 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 2c 59 04 00 3c 00 00 00 00 d0 09 00 c0 26 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 55 04 00 18 00 00 00 e8 54 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 04 00 90 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 55 23 04 00 00 10 00 00 00 24 04 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 30 22 00 00 00 40 04 00 00 24 00 00 00 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 58 4a 05 00 00 70 04 00 00 14 00 00 00 4c 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 6c 73 00 00 00 00 09 00 00 00 00 c0 09 00 00 02 00 00 00 60 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 c0 26 00 00 00 d0 09 00 00 28 00 00 00 62 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6a 0c 68 70 55 44 00 e8 2c 12 00 00 83 65 e4 00 8b 75 08 3b 35 44 ba 49 00 77 22 6a 04 e8 1d 07 00 00 59 83 65 fc 00 56 e8 24 0f 00 00 59 89 45 e4 c7 45 fc fe ff ff ff e8 09 00 00 00 8b 45 e4 e8 38 12 00 00 c3 6a 04 e8 18 06 00 00 59 c3 8b ff 55 8b ec 56 8b 75 08 83 fe e0 0f 87 a1 00 00 00 53 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$rhrhrh rh rh rhrhrirh rh rh rhRichrhPELP^$@@,Y<&0UT@@.textU#$ `.rdata0"@$(@@.dataXJpL@.tls`@.rsrc&(b@@jhpUD,eu;5DIw"jYeV$YEEE8jYUVuS

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1756 Parent PID: 584

General

Start time:	07:56:46
Start date:	18/11/2020
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:	0x13f470000
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\F769.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F7BEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\68FE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$PURCHASE ORDER No-17-11-98543.xlsm	read attributes | delete | syn chronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\2AFE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ETTER\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14019828C	CreateDirectoryA
C:\ETTER\dAneDFma\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14019828C	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14019828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14019828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14019828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14019828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14019828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14019828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14019828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14019828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14019828C	URLDownloadToFileA
C:\ETTER\dAneDFma\conhost.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14019828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F769.tmp	success or wait	1	13FA2B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\68FE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\2AFE0000	C:\Users\user\Desktop\PURCHASE ORDER No-17-11-98543.xlsm	success or wait	1	7FEEAC59AC0	unknown

File Written

<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\Desktop\~$PURCHASE ORDER No-17-11-98543.xlsm</td><td>unknown</td><td>55</td><td>05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20</td><td>.user</td><td>success or wait</td><td>1</td><td>13F6BF526</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\Desktop\~$PURCHASE ORDER No-17-11-98543.xlsm</td><td>unknown</td><td>110</td><td>05 00 41 00 6c 00 62 00 75 00 73 00 20 00</td><td>..A.l.b.u.s. . . . .
. . . .
. . . .</td><td>success or wait</td><td>1</td><td>13F6BF591</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\68FE0000</td><td>569</td><td>425</td><td>c4 55 cb 4e 23 31 10 bc af c4 3f 8c 7c 45 33 0e 20 a1 d5 2a 13 0e 3c 8e 80 04 7c 40 63 77 32 26 7e c9 6d 20 f9 7b 6c 27 64 49 14 12 46 20 71 99 f1 ab ba aa ba e5 f6 f0 6c 66 74 f5 82 81 94 b3 2d 3b 6a 06 ac 42 2b 9c 54 76 d2 b2 87 fb ab fa 2f ab 28 82 95 a0 9d c5 96 cd 91 d8 d9 e8 e0 cf f0 7e ee 91 aa 84 b6 d4 b2 2e 46 ff 8f 73 12 1d 1a a0 c6 79 b4 69 67 ec 82 81 98 a6 61 c2 3d 88 29 4c 90 1f 0f 06 a7 5c 38 1b d1 c6 3a e6 18 6c 34 bc c0 31 3c eb 58 5d ce d2 f2 42 89 b7 13 56 9d 2f ce 65 aa 96 29 93 f1 79 9d 6f 45 04 d4 b4 01 01 ef b5 12 10 93 37 fe 62 e5 86 ae 7a a9 a9 49 c8 72 86 3a e5 e9 30 09 ff 84 21 ef ac 6b fa 48 f0 39 ee c9 6f f7 f2 e4 b1 98 b9 49 f9 0f 4a 62 75 0b 21 5e 83 49 66 f9 4c f3 57 17 a6 8f ce 4d 9b dd bc d9 98 a1 1a 67 02 75 43 1d 62 6c</td><td>.U.N#1....?.|E3. ..*..
<...|@cw2&~.m .{l'dI..F
q.........lft.....-;j..B+.Tv....../.
(.......
.......~........F..s.....y.ig.
....a.=.)L.....\8...:..l4..1<.
X]...B...V./.e..)..y.oE.......
...7.b...z..I.r.:..0...!..k.H.
9..o......I..Jbu.!^.If.L.W....
M.......g.uC.bl</td><td>success or wait</td><td>43</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\68FE0000</td><td>994</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>16</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\68FE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 4c c4 4c 11 ab 01 00 00 ce 06 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK.........!.L.L............ [Content_Types].xml ... (..................................	success or wait	18	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\68FE0000	238778	65536	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 07 c0 0a f6 03 01 22 00 02 11 01 03 11 01 ff c4 00 1d 00 01 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 06 07 05 08 01 03 04 02 09 ff da 00 08 01 01 00 00 00 00 d9 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	......JFIF.................... ....'......'#*'' "*#>1++1>H<9<HWNNW mhm................................'. .....'#*'' "*#>1++1>H<9<HWNNW mhm.............."..............	success or wait	4	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\68FE0000	401722	1235	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 4c c4 4c 11 ab 01 00 00 ce 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e4 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b7 ae d3 c9 30 01 00 00 58 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 48 68 1a 18 6a 02 00 00 36 05 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 7a 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.L.L........... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.....0...X... ....xl/_rels/wor kbook.xml.relsPK..-.........!. Hh..j...6.................z... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$PURCHASE ORDER No-17-11-98543.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F6BF526	WriteFile
C:\Users\user\Desktop\~$PURCHASE ORDER No-17-11-98543.xlsm	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	13F6BF591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\2AFE0000	569	425	c4 55 cb 4e 23 31 10 bc af c4 3f 8c 7c 45 33 0e 20 a1 d5 2a 13 0e 3c 8e 80 04 7c 40 63 77 32 26 7e c9 6d 20 f9 7b 6c 27 64 49 14 12 46 20 71 99 f1 ab ba aa ba e5 f6 f0 6c 66 74 f5 82 81 94 b3 2d 3b 6a 06 ac 42 2b 9c 54 76 d2 b2 87 fb ab fa 2f ab 28 82 95 a0 9d c5 96 cd 91 d8 d9 e8 e0 cf f0 7e ee 91 aa 84 b6 d4 b2 2e 46 ff 8f 73 12 1d 1a a0 c6 79 b4 69 67 ec 82 81 98 a6 61 c2 3d 88 29 4c 90 1f 0f 06 a7 5c 38 1b d1 c6 3a e6 18 6c 34 bc c0 31 3c eb 58 5d ce d2 f2 42 89 b7 13 56 9d 2f ce 65 aa 96 29 93 f1 79 9d 6f 45 04 d4 b4 01 01 ef b5 12 10 93 37 fe 62 e5 86 ae 7a a9 a9 49 c8 72 86 3a e5 e9 30 09 ff 84 21 ef ac 6b fa 48 f0 39 ee c9 6f f7 f2 e4 b1 98 b9 49 f9 0f 4a 62 75 0b 21 5e 83 49 66 f9 4c f3 57 17 a6 8f ce 4d 9b dd bc d9 98 a1 1a 67 02 75 43 1d 62 6c	.U.N#1....?.|E3. ..*.. <...|@cw2&~.m .{l'dI..F q.........lft.....-;j..B+.Tv....../. (....... ....~........F..s.....y.ig. ....a.=.)L.....\8...:..l4..1<. X]...B...V./.e..)..y.oE....... ...7.b...z..I.r.:..0...!..k.H. 9..o......I..Jbu.!^.If.L.W.... M.......g.uC.bl	success or wait	43	7FEEAC59AC0	unknown
C:\Users\user\Desktop\2AFE0000	994	2	03 00	..	success or wait	16	7FEEAC59AC0	unknown
C:\Users\user\Desktop\2AFE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 4c c4 4c 11 ab 01 00 00 ce 06 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.L.L............. [Content_Types].xml ... (...................................	success or wait	18	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\2AFE0000	238778	65536	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 07 c0 0a f6 03 01 22 00 02 11 01 03 11 01 ff c4 00 1d 00 01 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 06 07 05 08 01 03 04 02 09 ff da 00 08 01 01 00 00 00 00 d9 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	......JFIF....................................'......'#*" "*#>1++1>H<9<HWNNW mhm...............................'......'#*" "*#>1++1>H<9<HWNNW mhm............."..	success or wait	4	7FEEAC59AC0	unknown
C:\Users\user\Desktop\2AFE0000	401722	1235	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 4c c4 4c 11 ab 01 00 00 ce 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e4 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b7 ae d3 c9 30 01 00 00 58 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 48 68 1a 18 6a 02 00 00 36 05 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 7a 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.L.L.................................[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.....0...X... ....xl/_rels/wor kbook.xml.relsPK..-.........!. Hh..j...6.................z... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\conhost[1].triumphloader	unknown	808	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 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 ad 13 06 a2 e9 72 68 f1 e9 72 68 f1 e9 72 68 f1 f7 20 ec f1 cf 72 68 f1 f7 20 fd f1 fa 72 68 f1 f7 20 eb f1 98 72 68 f1 ce b4 13 f1 ec 72 68 f1 e9 72 69 f1 9b 72 68 f1 f7 20 e2 f1 e8 72 68 f1 f7 20 fc f1 e8 72 68 f1 f7 20 f9 f1 e8 72 68 f1 52 69 63 68 e9 72 68 f1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 07 1b 50 5e 00 00 00 00 00 00 00 00 e0 00 03	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$............rh..rh..rh.. ...rh.. ...rh.. ...rh......rh..ri. .rh.. ...rh.. ...rh.. ...rh.Ri ch.rh.................PE..L... ..P^...........	success or wait	1	14019828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\conhost[1].triumphloader	unknown	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6a 0c 68 70 55 44 00 e8 2c 12 00 00 83 65 e4 00 8b 75 08 3b 35 44 ba 49 00 77 22 6a 04 e8 1d 07 00 00 59 83 65 fc 00	....j.hpUD..,....e...u.;5D.I .w"j......Y.e..	success or wait	1	14019828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\conhost[1].triumphloader	unknown	195	e9 85 09 00 00 83 8d f8 fb ff ff 01 e9 79 09 00 00 81 8d f8 fb ff ff 80 00 00 00 e9 6a 09 00 00 09 bd f8 fb ff ff e9 5f 09 00 00 66 83 fa 2a 75 2c 83 c3 04 89 9d e4 fb ff ff 8b 5b fc 89 9d d4 fb ff ff 85 db 0f 8d 3f 09 00 00 83 8d f8 fb ff ff 04 f7 9d d4 fb ff ff e9 2d 09 00 00 8b 85 d4 fb ff ff 6b c0 0a 0f b7 ca 8d 44 08 d0 89 85 d4 fb ff ff e9 12 09 00 00 83 a5 f4 fb ff ff 00 e9 06 09 00 00 66 83 fa 2a 75 26 83 c3 04 89 9d e4 fb ff ff 8b 5b fc 89 9d f4 fb ff ff 85 db 0f 8d e6 08 00 00 83 8d f4 fb ff ff ff e9 da 08 00 00 8b 85 f4 fb ff ff 6b c0 0a 0f b7 ca 8d 44 08 d0 89 85 f4	.............y..............j. ...._...f..*u,..........[...........?.................- ....k......D............. ....f..*u&..........[. ....k......D.....	success or wait	1	14019828C	URLDownloadToFileA
C:\ETTER\dAneDFma\conhost.exe	unknown	9195	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 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 ad 13 06 a2 e9 72 68 f1 e9 72 68 f1 e9 72 68 f1 f7 20 ec f1 cf 72 68 f1 f7 20 fd f1 fa 72 68 f1 f7 20 eb f1 98 72 68 f1 ce b4 13 f1 ec 72 68 f1 e9 72 69 f1 9b 72 68 f1 f7 20 e2 f1 e8 72 68 f1 f7 20 fc f1 e8 72 68 f1 f7 20 f9 f1 e8 72 68 f1 52 69 63 68 e9 72 68 f1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 07 1b 50 5e 00 00 00 00 00 00 00 00 e0 00 03	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$............rh..rh..rh.. ...rh.. ...rh.. ...rh......rh..ri. .rh.. ...rh.. ...rh.. ...rh.Ri ch.rh.................PE..L... ..P^...........	success or wait	1	14019828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\conhost[1].triumphloader	unknown	8192	44 00 89 75 e4 eb 2a 8a 46 01 84 c0 74 28 0f b6 3e 0f b6 c0 eb 12 8b 45 e0 8a 80 84 77 44 00 08 44 3b 1d 0f b6 46 01 47 3b f8 76 ea 8b 7d 08 46 46 80 3e 00 75 d1 8b 75 e4 ff 45 e0 83 c6 08 83 7d e0 04 89 75 e4 72 e9 8b c7 89 7b 04 c7 43 08 01 00 00 00 e8 67 fb ff ff 6a 06 89 43 0c 8d 43 10 8d 89 8c 77 44 00 5a 66 8b 31 41 66 89 30 41 40 40 4a 75 f3 8b f3 e8 d7 fb ff ff e9 b7 fe ff ff 80 4c 03 1d 04 40 3b c1 76 f6 46 46 80 7e ff 00 0f 85 34 ff ff ff 8d 43 1e b9 fe 00 00 00 80 08 08 40 49 75 f9 8b 43 04 e8 12 fb ff ff 89 43 0c 89 53 08 eb 03 89 73 08 33 c0 0f b7 c8 8b c1 c1 e1 10 0b c1 8d 7b 10 ab ab ab eb a8 39 35 a0 87 44 00 0f 85 58 fe ff ff 83 c8 ff 8b 4d fc 5f 5e 33 cd 5b e8 51 22 00 00 c9 c3 6a 14 68 18 56 44 00 e8 c6 e3 ff ff 83 4d e0 ff e8 8f 07 00	D..u..*.F...t(..>.....E....wD ..D;...F.G;.v..}.FF.>.u..u..E. ....}...u.r....{..C.....g...j ..C..C....wD.Zf.1Af.0A@@ Ju.... .....L...@;.v.FF.~....4.. ..C.....@Iu..C.....C..S. ...s.3.....{.....95..D ...X.....M._^3.[.Q"....j.h.V D.....M.....	success or wait	39	14019828C	URLDownloadToFileA
C:\ETTER\dAneDFma\conhost.exe	unknown	28098	fb ff ff e9 bf 08 00 00 0f b7 c2 83 f8 49 74 57 83 f8 68 74 46 83 f8 6c 74 18 83 f8 77 0f 85 a4 08 00 00 81 8d f8 fb ff ff 00 08 00 00 e9 95 08 00 00 66 83 3e 6c 75 17 03 f7 81 8d f8 fb ff ff 00 10 00 00 89 b5 c0 fb ff ff e9 78 08 00 00 83 8d f8 fb ff ff 10 e9 6c 08 00 00 83 8d f8 fb ff ff 20 e9 60 08 00 00 0f b7 06 66 83 f8 36 75 1f 66 83 7e 02 34 75 18 83 c6 04 81 8d f8 fb ff ff 00 80 00 00 89 b5 c0 fb ff ff e9 38 08 00 00 66 83 f8 33 75 1f 66 83 7e 02 32 75 18 83 c6 04 81 a5 f8 fb ff ff ff 7f ff ff 89 b5 c0 fb ff ff e9 13 08 00 00 66 83 f8 64 0f 84 09 08 00 00 66 83 f8 69 0f 84 ff 07 00 00 66 83 f8 6f 0f 84 f5 07 00 00 66 83 f8 75 0f 84 eb 07 00 00 66 83 f8 78 0f 84 e1 07 00 00 66 83 f8 58 0f 84 d7 07 00 00 83 a5 a4 fb ff ff 00 8b 85 d0 fb ff ff 52 8d	.....ltW..htF..lt...w. .....f.>lu..... .....x.....l..... .`.....f..6u.f.~.4u.. .....8...f..3u.f .~.2u..... f..d.....f..i.....f..o..... f..u.....f..x.....f..X..... .....R.	success or wait	6	14019828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ETTER\dAneDFma\conhost.exe	unknown	15325	00 0c 00 00 00 09 00 00 00 0c 00 00 00 0a 00 00 00 07 00 00 00 0b 00 00 00 08 00 00 00 0c 00 00 00 16 00 00 00 0d 00 00 00 16 00 00 00 0f 00 00 00 02 00 00 00 10 00 00 00 0d 00 00 00 11 00 00 00 12 00 00 00 12 00 00 00 02 00 00 00 21 00 00 00 0d 00 00 00 35 00 00 00 02 00 00 00 41 00 00 00 0d 00 00 00 43 00 00 00 02 00 00 00 50 00 00 00 11 00 00 00 52 00 00 00 0d 00 00 00 53 00 00 00 0d 00 00 00 57 00 00 00 16 00 00 00 59 00 00 00 0b 00 00 00 6c 00 00 00 0d 00 00 00 6d 00 00 00 20 00 00 00 70 00 00 00 1c 00 00 00 72 00 00 00 09 00 00 00 06 00 00 00 16 00 00 00 80 00 00 00 0a 00 00 00 81 00 00 00 0a 00 00 00 82 00 00 00 09 00 00 00 83 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 91 00 00 00 29 00 00 00 9e 00 00 00 0d 00 00 00 a1 00 00 00 02 00 00 00 a4 00	....!.......5.... ...A.......C.......P.......R.. .....S.......W.......Y.......l ....m... ...p.......r...... ....)......	success or wait	1	14019828C	URLDownloadToFileA
C:\Users\user\Desktop\~$PURCHASE ORDER No-17-11-98543.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F6BF526	WriteFile
C:\Users\user\Desktop\~$PURCHASE ORDER No-17-11-98543.xlsm	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	13F6BF591	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A97335D5.jpg	0	4096	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A97335D5.jpg	0	65536	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\71A94C24.png	0	152	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\PURCHASE ORDER No-17-11-98543.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PURCHASE ORDER No-17-11-98543.xlsm	0	8	pending	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF7A8	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF9E9	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFAC3	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF7A8	EF7A8	binary	04 00 00 00 DC 06 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 AF BC 3C 6C C3 BD D6 01 A8 F7 0E 00 A8 F7 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF9E9	EF9E9	binary	04 00 00 00 DC 06 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 38 6E 92 6C C3 BD D6 01 E9 F9 0E 00 E9 F9 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFAC3	EFAC3	binary	04 00 00 00 DC 06 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 50 00 55 00 52 00 43 00 48 00 41 00 53 00 45 00 20 00 4F 00 52 00 44 00 45 00 52 00 20 00 4E 00 6F 00 2D 00 31 00 37 00 2D 00 31 00 31 00 2D 00 39 00 38 00 35 00 34 00 33 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 7C C1 B3 6C C3 BD D6 01 C3 FA 0E 00 C3 FA 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	{;0	binary	7B 3B 30 00 DC 06 00 00 02 00 00 00 00 00 00 00 8E 00 00 00 01 00 00 00 46 00 00 00 3C 00 00 00 70 00 75 00 72 00 63 00 68 00 61 00 73 00 65 00 20 00 6F 00 72 00 64 00 65 00 72 00 20 00 6E 00 6F 00 2D 00 31 00 37 00 2D 00 31 00 31 00 2D 00 39 00 38 00 35 00 34 00 33 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 70 00 75 00 72 00 63 00 68 00 61 00 73 00 65 00 20 00 6F 00 72 00 64 00 65 00 72 00 20 00 6E 00 6F 00 2D 00 31 00 37 00 2D 00 31 00 31 00 2D 00 39 00 38 00 35 00 34 00 33 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: conhost.exe PID: 2512 Parent PID: 1756

General

Start time:	07:56:50
Start date:	18/11/2020
Path:	C:\ETTER\dAneDFma\conhost.exe
Wow64 process (32bit):	true
Commandline:	'C:\ETTER\dAneDFma\conhost.exe'
Imagebase:	0x400000
File size:	297472 bytes
MD5 hash:	F5ECCDDC7EE3DF74B79DF21D04DD56A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000003.00000003.2117438541.0000000000580000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000003.00000003.2117438541.0000000000580000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000003.00000002.2168715128.0000000000510000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000003.00000002.2168603978.00000000002F8000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000003.00000002.2168630722.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000003.00000002.2168630722.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 29%, Virustotal, Browse • Detection: 23%, ReversingLabs
Reputation:	low

Disassembly

Code Analysis