ID: 755822
Sample Name: ACP-2210825ORDER.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:11:40
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

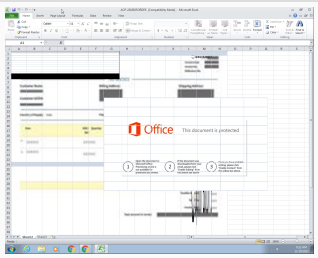
Windows Analysis Report

ACP-2210825ORDER.xls

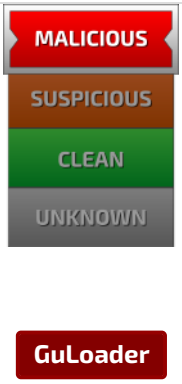
Overview

General Information

Sample Name:	ACP-2210825ORDER.xls
Analysis ID:	755822
MD5:	6c84860292e2a4..
SHA1:	7061c26320bf88..
SHA256:	cadae8bf6a2bcf1..
Tags:	xls
Infos:	



Detection



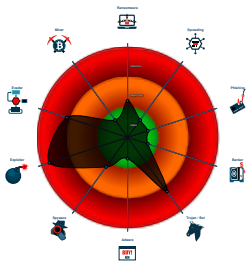
GuLoader

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

Signatures

- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Office document tries to convince v…
- Antivirus / Scanner detection for sub…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Yara detected GuLoader
- Office equation editor starts process…
- Shellcode detected
- Office equation editor drops PE file
- Tries to detect virtualization through…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1036 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1168 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1136 cmdline: "C:\Users\Public\vbc.exe" MD5: 7081C4822CF1C7572DD82822B8F27C49)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.1187007837.00000000030C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Antivirus detection for dropped file

Exploits

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

Office equation editor establishes network connection

Software Vulnerabilities

Shellcode detected

System Summary

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

Office equation editor drops PE file

Data Obfuscation

Yara detected GuLoader

Boot Survival

Drops PE files to the user root directory

Malware Analysis System Evasion

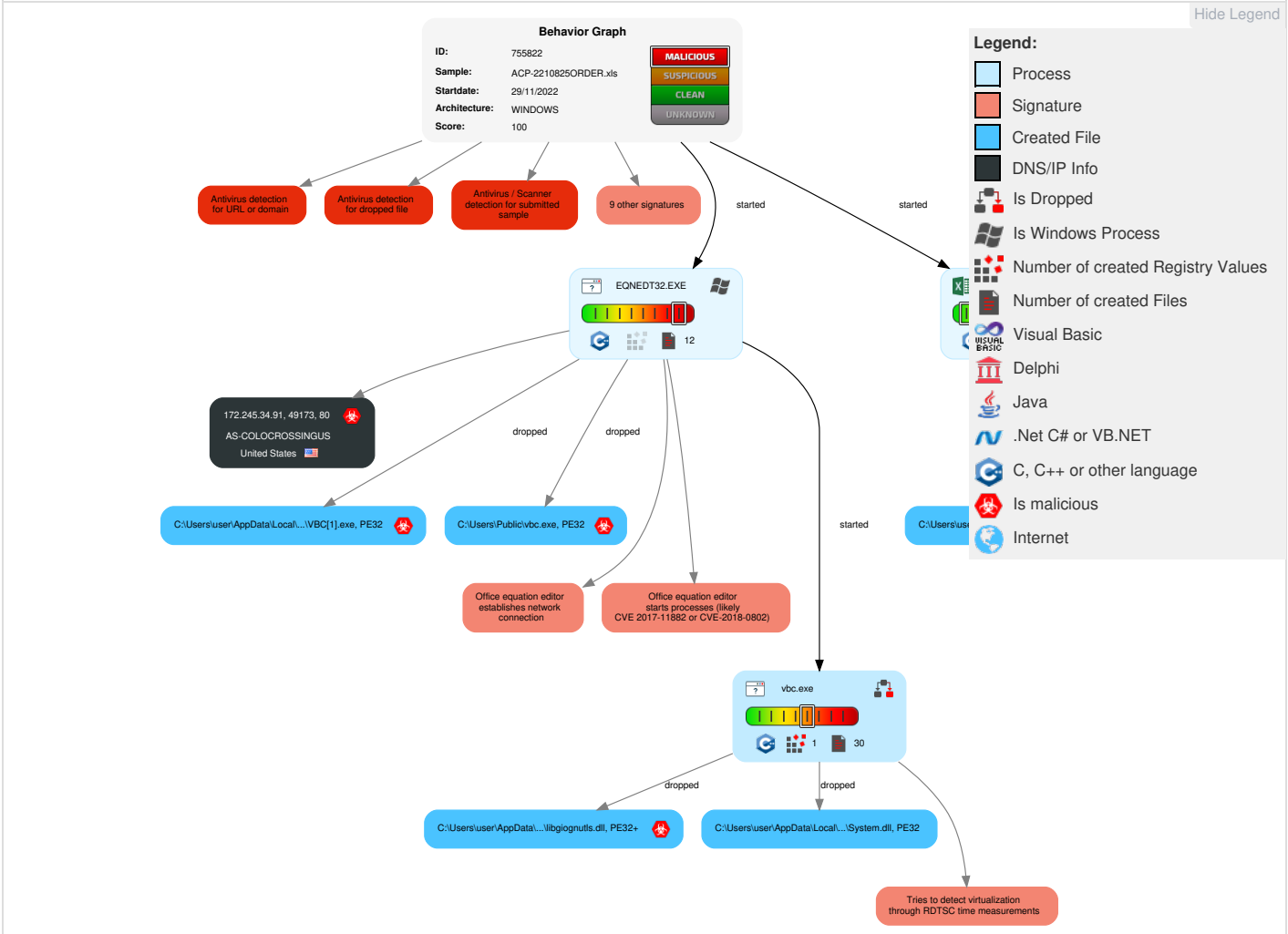
Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Scripting	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 1 1 Masquerading	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Disable or Modify Tools	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	3 3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 2 Exploitation for Client Execution	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 Virtualization/Sandbox Evasion	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Access Token Manipulation	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Process Injection	LSA Secrets	1 5 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Scripting	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

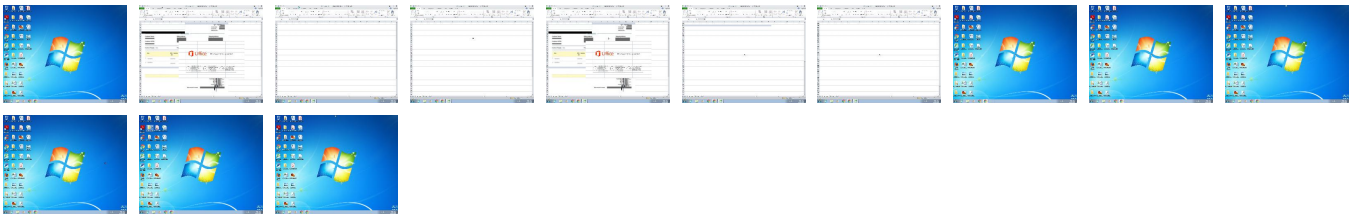
Behavior Graph

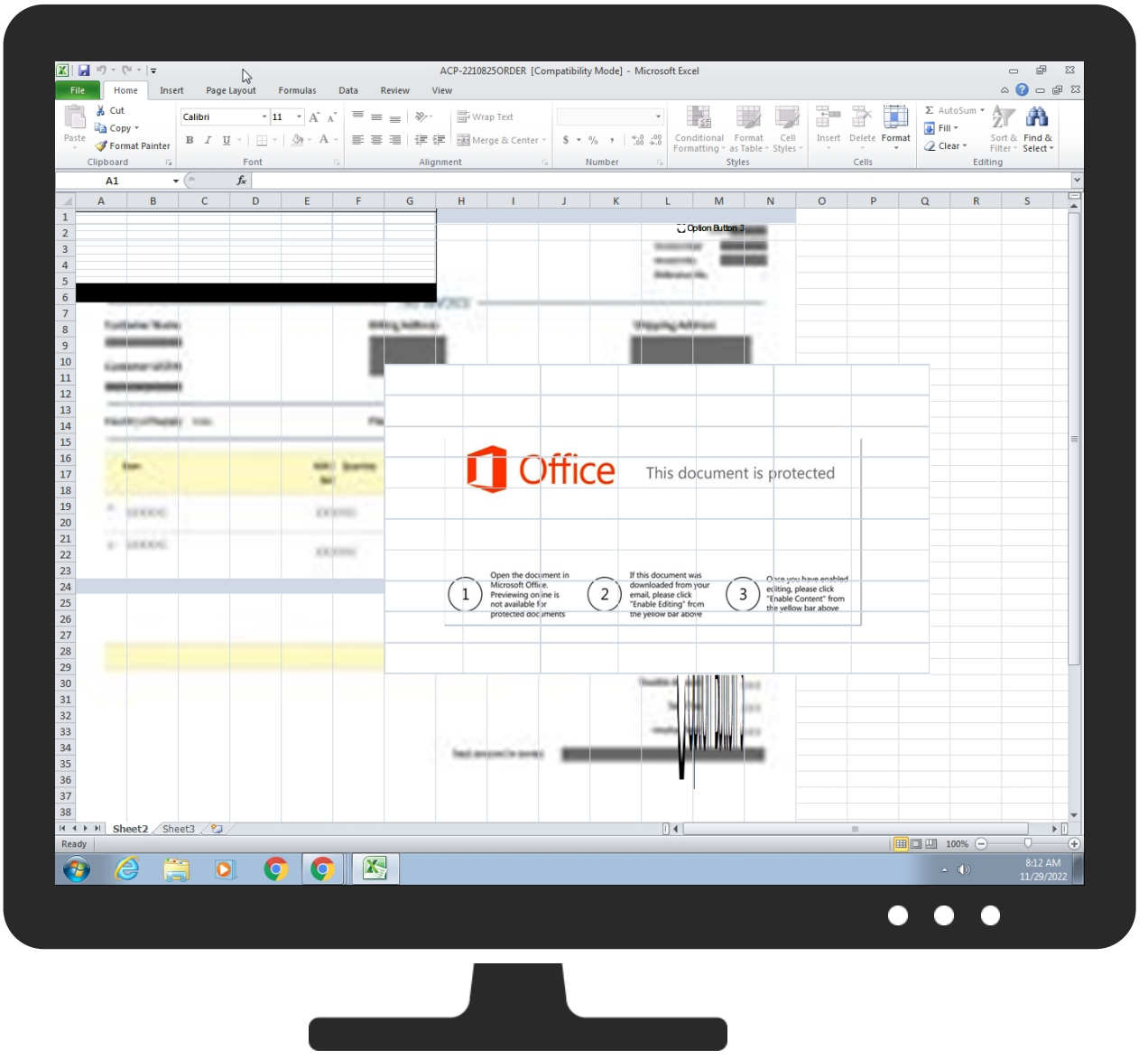


Screenshots

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
ACP-2210825ORDER.xls	27%	Virustotal		Browse
ACP-2210825ORDER.xls	100%	Avira	EXP/CVE-2017-11882.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF688530565CAD41F4.TMP	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Temp\nsp5B93.tmp\System.dll	2%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\libgiognutls.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://172.245.34.91/5643/VBC.exej	0%	Avira URL Cloud	safe	
http://172.245.34.91/5643/VBC.exel	0%	Avira URL Cloud	safe	
http://172.245.34.91/5643/VBC.exehhC:	0%	Avira URL Cloud	safe	
http://172.245.34.91/5643/VBC.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

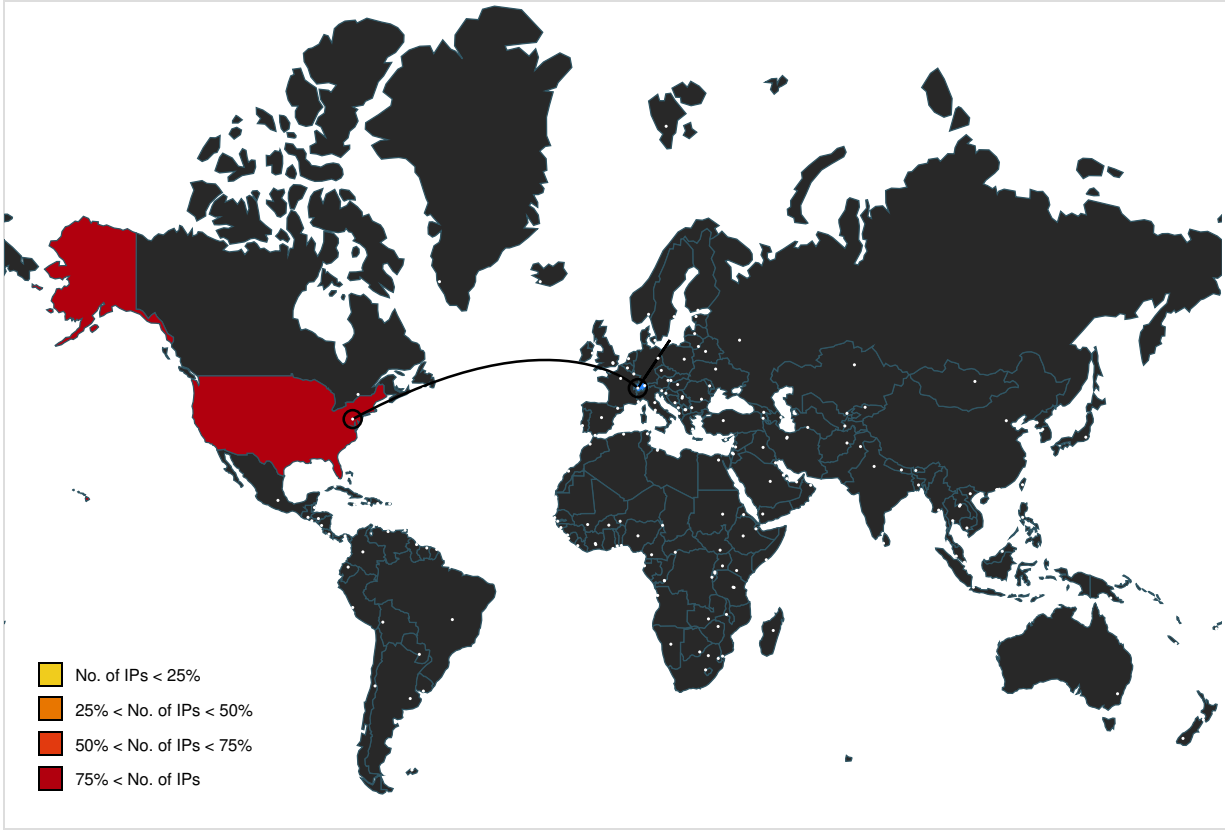
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://172.245.34.91/5643/VBC.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://172.245.34.91/5643/VBC.exej	EQNEDT32.EXE, 00000002.00000002.97364630.0000000003540000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://172.245.34.91/5643/VBC.exel	EQNEDT32.EXE, 00000002.00000002.97339312.000000000065F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	vbc.exe, 00000005.00000000.972752433.000000000040A000.00000008.00000001.01000000.00000004.sdmp, vbc.exe, 00000005.00000002.1185344377.000000000040A000.00000004.00000001.01000000.00000004.sdmp, vbc.exe.2.dr, VBC[1].exe.2.dr	false		high
http://172.245.34.91/5643/VBC.exehhC:	EQNEDT32.EXE, 00000002.00000002.97339312.000000000065F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.245.34.91	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755822
Start date and time:	2022-11-29 08:11:40 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ACP-2210825ORDER.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@4/20@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.8% (good quality ratio 84.3%) • Quality average: 87.7% • Quality standard deviation: 21.4%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Report size getting too big, too many NtOpenKeyEx 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
08:12:45	API Interceptor	102x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	477800
Entropy (8bit):	7.505402259729816
Encrypted:	false
SSDEEP:	12288:Lz772qgvq2nLm4W2RPLKb+nFzlQ3Ja8TA:gXnS4W2RPLKm/of
MD5:	7081C4822CF1C7572DD82822B8F27C49
SHA1:	4EE3B6C423B1C9EBF5BEFBC73D1EEF0C576CF026

SHA-256:	B5330F82F3C5C3F223AE9DECD3EBDCD74D1A13D95B1C42BD7B2DE4E6C6CB0083
SHA-512:	6E3377E6A47518F2267CD38646E2CEC576D41FD8A67C8C2590F43BF353C0B1F322FC229E70BC98E9C7DFAA1A11CF872A0C8E2C15A31EE90EF1C4E65EAC98E 3A
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..P...P...P..*_...P...P..OP..*_...P..s...P...V...P..Rich.P.....PE ..L...8.MX.....b...*.....J4.....@.....p.....@.....h.....5..X.....tex t....a.....b..... ..`.rdata.....f.....@..@.data...8.....z.....@....ndata...0.....rsrc...h.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F090A1F.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	4056
Entropy (8bit):	1.929653848333741
Encrypted:	false
SSDEEP:	12:YB1uOUvJqRENEtEtEdEdEdEO6Mcs/vs9/09v89fE9vM9/U9Lzlm97z9m9Lz1m9bO:Y7uTvJqRiGGWWWRKqurbkdBvae
MD5:	4A103FC1809C8EA381D2ACB5380EF4F6
SHA1:	6C81D37798C4D78C64E7D3EF7EB2ACB317C9FF67
SHA-256:	1AB8F5ABD845FFD0C61A61BB09BFCF20569B80B4496BCCB58C623753CF40485C
SHA-512:	77DA8AB022505D77F89749E97628CAF4DD8414251CB673598ACBA8F7D30D1889037FAB30094A6CE7DC47293697A6BEF28B92364D00129B59D2FC3711C82650F5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....l.....0.....C'..... EMF.....8...X.....?.....F...,... ...EMF+.@.....x...x...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....".....l.....".....l.....".....l.....1.....".....l..... .....1.....".....l.....1.....".....l.....1.....".....l.....1.....".....l..... .....1.....'.....%.....&.....%.....6.....0.....%.....L...d...../.....0. .....!...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2A84DD94.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	17500
Entropy (8bit):	2.2677225081522296
Encrypted:	false
SSDEEP:	96:uRiEE000XyDcvSRiGGWWWRNN/ECl0jp2iGGWWWZmCl8bo+BvWbkmIg:d0stoE4
MD5:	5A977E68E4AD913CC2A9FC917F1CA510
SHA1:	D68C009CC5EE57A931D1BB1D062294F319C03183
SHA-256:	82CAABC053EAB9A6F6A826A3FEA7EC1D834A053268B516E8CB81B5B0B161FD73
SHA-512:	71C40805CE1E750B1158356834D9EA8902B4D5A1BDA91A11DBB154FE1480FCDC4C51C8E6E82C985D8F563777B2F21775A23DA5E0794843EC88E6F6419516997
Malicious:	false
Reputation:	low
Preview:	....l.....`...0.....uN..p... EMF....\D.....8...X.....?.....F...,... ...EMF+.@.....x...x...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....".....l.....".....l.....a...1..."....l..... .....a...1..."....l.....a...1..."....l.....a...1..."....l.....a...1..."....l..... .....a...1..'.....%.....&.....%.....6.....`.....%.....L...d...../.....`. .....!...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2C485423.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	17500
Entropy (8bit):	2.2677225081522296
Encrypted:	false
SSDEEP:	96:uRiEE000XyDcvSRiGGWWWRNN/ECl0jp2iGGWWWZmCl8bo+BvWbkmIg:d0stoE4
MD5:	5A977E68E4AD913CC2A9FC917F1CA510
SHA1:	D68C009CC5EE57A931D1BB1D062294F319C03183
SHA-256:	82CAABC053EAB9A6F6A826A3FEA7EC1D834A053268B516E8CB81B5B0B161FD73
SHA-512:	71C40805CE1E750B1158356834D9EA8902B4D5A1BDA91A11DBB154FE1480FCDC4C51C8E6E82C985D8F563777B2F21775A23DA5E0794843EC88E6F6419516997

Malicious:	false
Reputation:	low
Preview:	....l..........`...0..........uN..p... EMF....\D.....8...X.....?.....F...,... ...EMF+.@.....x...x...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....".....l.....".....l.....".....l.....a...1..."....l..... .....a...1..."....l.....a...1..."....l.....a...1..."....l.....a...1..."....l..... .....a...1..'.....%.....&.....%.....6.....`.....%.....L...d....._.....`. .....l...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\489D37C8.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	17500
Entropy (8bit):	2.2754571047715912
Encrypted:	false
SSDEEP:	96:uRiEE000XyDcvSRiGGWWWRNN/uf2iGGWWWZmCI8bUaBvWbkmIg:d0EUI4
MD5:	38A09794AE082E08EA4F8B6E517F4814
SHA1:	8B7DF3EE701A7E43BBD9A1AC03A7C342FDB4F2B5
SHA-256:	22A5F86B243A131E89E06FF0FA824A09369D1878DC1F1C4E3527FFDDBEFF70F3
SHA-512:	2BF53BB29C684C2D54ADEA3D1877A31DF011A9B58EDCF54FCE697291BEC9056591BB3BDE95DC05BC1A3474A721B2889E4312903479782823F0606BD32B4243E 5
Malicious:	false
Reputation:	low
Preview:	....l..........`...0..........uN..p... EMF....\D.....8...X.....?.....F...,... ...EMF+.@.....x...x...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....".....l.....".....l.....".....l.....a...1..."....l..... .....a...1..."....l.....a...1..."....l.....a...1..."....l.....a...1..."....l..... .....a...1..'.....%.....&.....%.....6.....`.....%.....L...d....._.....`. .....l...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4A546E2A.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	4056
Entropy (8bit):	1.929653848333741
Encrypted:	false
SSDEEP:	12:YB1uOUvJqRENEtEtEdEdEdEO6Mcs/vs9/09v89fE9vM9/U9Lzlm97z9m9Lz1m9bO:Y7uTvJqRiGGWWWRKqurbkdBvae
MD5:	4A103FC1809C8EA381D2ACB5380EF4F6
SHA1:	6C81D37798C4D78C64E7D3EF7EB2ACB317C9FF67
SHA-256:	1AB8F5ABD845FFD0C61A61BB09BFCF20569B80B4496BCCB58C623753CF40485C
SHA-512:	77DA8AB022505D77F89749E97628CAF4DD8414251CB673598ACBA8F7D30D1889037FAB30094A6CE7DC47293697A6BEF28B92364D00129B59D2FC3711C82650F5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....l.....0.....C'..... EMF.....8...X.....?.....F...,... ...EMF+.@.....x...x...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....".....l.....".....l.....".....l.....1.....".....l..... .....1.....".....l.....1.....".....l.....1.....".....l.....1.....".....l..... .....1.....'.....%.....&.....%.....6.....0.....%.....L...d...../.....0. .....l...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\628281DB.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	321644
Entropy (8bit):	2.239527826723405
Encrypted:	false
SSDEEP:	768:2DONBmwaWFloY6jKV8g5d1KnK1LXMpaCnwSOybdY0p:mONIwaWFlajKpk6LXMpVTT
MD5:	35F7C4CEEC52F37D0B0881CCC3A7612D
SHA1:	3FC1E0B485071C1725703E6CB1029485B895765F
SHA-256:	17918DE803C9609AB1D8BF011FC75835E43FF490299D7D67EAB7F550E1FC0968
SHA-512:	ACE05DA7132DEEBF169C45D3C726B34B8DEE745F00109ABED41B6A6A4D6AE2DD1010AAD7C4FC08DA96335C33D4B6D7A49A24E2621812D15D6FEA584CEE34 56B
Malicious:	false

Preview:	....l.....m.....J..sK.. EMF....l...8.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....{.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....x$....._..f.x.@..%...._..._.....l._..._. RQ.Rl._.d._....._.P._.$Q.Rl.\_.d.\_. ...Id.xd.\_.l.\_. .....d.x.....@1.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....,_....x..y.._..._..8.x.....dv.....% .....%.....%.....!.....{.....".....%.....%.....%.....T...T.....@.E.@....n.....L.....{.....P... ...6...F..... .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\95D0DCC2.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	17500
Entropy (8bit):	2.2724443756862973
Encrypted:	false
SSDEEP:	96:uRiEE000XyDcvSRiGGWWWRNN/aP2iGGWWWZmCI8bMGBvWbkmIg:d0kMc4
MD5:	831E92F84F915D931EE02260D16AC145
SHA1:	51C81E34BEBE02A91EA7DA9F275E9EFD72547D01
SHA-256:	C4CAD71039044EFBE493BD54FD3A00FB9C35FF9CC8BA47F668490A3803378594
SHA-512:	E85B4B468A2E9F76CCAD6CFFEC6478138046B0F335C6409D7F0849A4755D4C57477FE587624AD8EF418AA829B79183C975EF2858B3052022686BC812DC974C78
Malicious:	false
Preview:	....l.....`...0.....uN..p... EMF....\D.....8...X.....?.....F...,... ...EMF+.@.....x...x...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....".....l.....".....l.....".....l.....a...1..".....l..... .....a...1..".....l.....a...1..".....l.....a...1..".....l.....a...1..".....l..... .....a...1..'.....%.....&.....%.....6.....`.....%.....L...d....._.....`. .....!...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9BAF1916.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	321644
Entropy (8bit):	2.239527826723405
Encrypted:	false
SSDEEP:	768:2DONBmwaWFloY6jKV8g5d1KnK1LXMpaCnwSOybdY0p:mONIwaWFlajKpk6LXMpVTT
MD5:	35F7C4CEEC52F37D0B0881CCC3A7612D
SHA1:	3FC1E0B485071C1725703E6CB1029485B895765F
SHA-256:	17918DE803C9609AB1D8BF011FC75835E43FF490299D7D67EAB7F550E1FC0968
SHA-512:	ACE05DA7132DEEBF169C45D3C726B34B8DEE745F00109ABED41B6A6A4D6AE2DD1010AAD7C4FC08DA96335C33D4B6D7A49A24E2621812D15D6FEA584CEE34 56B
Malicious:	false
Preview:	....l.....m.....J..sK.. EMF....l...8.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....{.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....x$....._..f.x.@..%...._..._.....l._..._. RQ.Rl._.d._....._.P._.$Q.Rl.\_.d.\_. ...Id.xd.\_.l.\_. .....d.x.....@1.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....,_....x..y.._..._..8.x.....dv.....% .....%.....%.....!.....{.....".....%.....%.....%.....T...T.....@.E.@....n.....L.....{.....P... ...6...F..... .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BC7C3885.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	17500
Entropy (8bit):	2.2754571047715912
Encrypted:	false
SSDEEP:	96:uRiEE000XyDcvSRiGGWWWRNN/uf2iGGWWWZmCI8bUaBvWbkmIg:d0EUI4
MD5:	38A09794AE082E08EA4F8B6E517F4814
SHA1:	8B7DF3EE701A7E43BBD9A1AC03A7C342FDB4F2B5
SHA-256:	22A5F86B243A131E89E06FF0FA824A09369D1878DC1F1C4E3527FFDDBEFF70F3
SHA-512:	2BF53BB29C684C2D54ADEA3D1877A31DF011A9B58EDCF54FCE697291BEC9056591BB3BDE95DC05BC1A3474A721B2889E4312903479782823F0606BD32B4243E 5
Malicious:	false
Preview:	....l.....`...0.....uN..p... EMF....\D.....8...X.....?.....F...,... ...EMF+.@.....x...x...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....".....l.....".....l.....".....l.....a...1..".....l..... .....a...1..".....l.....a...1..".....l.....a...1..".....l.....a...1..".....l..... .....a...1..'.....%.....&.....%.....6.....`.....%.....L...d....._.....`. .....!...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C6BD8529.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	17500
Entropy (8bit):	2.2724443756862973
Encrypted:	false
SSDEEP:	96:uRiEE000XyDcvSRiGGWWWRNN/aP2iGGWWWZmCI8bMGBvWbkmIg:d0kMc4
MD5:	831E92F84F915D931EE02260D16AC145
SHA1:	51C81E34BEBE02A91EA7DA9F275E9EFD72547D01
SHA-256:	C4CAD71039044EFBE493BD54FD3A00FB9C35FF9CC8BA47F668490A3803378594
SHA-512:	E85B4B468A2E9F76CCAD6CFFEC6478138046B0F335C6409D7F0849A4755D4C57477FE587624AD8EF418AA829B79183C975EF2858B3052022686BC812DC974C78
Malicious:	false
Preview:	....l.....`...0.....uN..p... EMF....\D.....8...X.....?.....F...,.. ...EMF+.@.....x...x...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....".....l.....".....l.....".....l.....a...1..".....l..... .....a...1..".....l.....a...1..".....l.....a...1..".....l.....a...1..".....l..... .....a...1..'.....%.....&.....%.....6.....`.....%.....L...d....._.....`. .....l...

C:\Users\user\AppData\Local\Temp\nsp5B93.tmp\System.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11776
Entropy (8bit):	5.656065698421856
Encrypted:	false
SSDEEP:	192:eY24sihno00Wfl97nH6T2enXwWobpWBTU4VtHT7dmN35Ol+Sl:E8Qll975eXqlWBrz7YLOl+
MD5:	17ED1C86BD67E78ADE4712BE48A7D2BD
SHA1:	1CC9FE86D6D6030B4DAE45ECDDCE5907991C01A0
SHA-256:	BD046E6497B304E4EA4AB102CAB2B1F94CE09BDE0EEBBA4C59942A732679E4EB
SHA-512:	0CBED521E7D6D1F85977B3F7D3CA7AC34E1B5495B69FD8C7BFA1A846BAF53B0ECD06FE1AD02A3599082FFACAF8C71A3BB4E32DEC05F8E24859D736B828092CD5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....MX.. .....l..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..b....P.....*.....@..B.....

C:\Users\user\AppData\Local\Temp\~DF15E3E53C3844A1B8.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF357B58C09F937A89.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512

Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF688530565CAD41F4.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Tue Nov 29 05:27:07 2022, Security: 1
Category:	dropped
Size (bytes):	1130496
Entropy (8bit):	7.090671625727551
Encrypted:	false
SSDEEP:	24576:mLsr5XXXXXXXXXXXUXXXXXXXSXXXXXXXXzmZr5XXXXXXXXXXXXUXXXXXXXSXXXd:Ch
MD5:	0E013B64C85479178FE144D0F1AB7C4B
SHA1:	D05316B326B2DA075C00246DE6E3CBFB8B255A96
SHA-256:	CAB79276FB8419A70BAAC774C9DB91D16ED1DADF5F5624C4148E7F1975FDFF94
SHA-512:	34699E3C80C5F5E95C876D5794E05701C1726E04A46AF9976CB6415551688B97F39DFC78556F4F7A0588B4E24111663F7BAC1D188E80F256BAE5821BAFCCE5B0
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	.....>.....m...n...\...]...^.....n.....p..... .....H..... .....i...Z..... ...!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DFEB3257B002629434.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Obeyeo.Bib

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	178824
Entropy (8bit):	6.515135274289935
Encrypted:	false
SSDEEP:	1536:Aqnh3ZWvlivpBh2LolEVEF+F2MVQ454gp3cHE6xBiP29vpAX5D57DwVaDXW:RkYzh2Lol/FdUJNfPgk5DVDUd
MD5:	52F571D999E9DD5B6ABFFE0CC9BF8DF3
SHA1:	67743CD31368EA4C7C350C5071A6B1D8A5AF400B
SHA-256:	7CC58916DBEADFF389E9375FD1F8973DB606156E953F309C55C40384E54765E3

SHA-512:	0BA04B8CDA196099229824B65348B71483D50377D10660AF8CD70A10919A310D88DDBA80D1F595524F71764BB2A765C87B9E5E2276391B11A272A52E3BBA7C11
Malicious:	false
Preview:	...6.{..N..p2...H.=L.]....I..b.0..2).v..X..~..q..nm.9..$h....YZ..}..V.u..E.a(M.....q.....@9.n.`7.....z.N...<...&..h..\.....&.h@p.....%.~5._b..b.....B(....:.4.....t.S0..J..0.h.&. .H.t.gV.&..y.,J.3...m..\.....~n..L.AnI.....C.a.7w^!9.D.]J.....p...C8..Hn.....14.|.. ...k.....9.....@%.....S..d.>.*I.9.@.....I.....,4G.I.}..e....<.....]...wj.Z.^...j.Fv.#..9n.c{.`..4U...,Q... v.g.t)..o...g.....E.}..9...1....Wbl..JT%8..m[x.a.u.7.i).....1+..$l@...x$.~.....6q.BE.x..7...n.n..gOZ.V.7..6.a!.c....`.vGm)..."L#~..E.....tV.....DjX.....Z.>..Z.).c.....D7}d.v.. . .%...v.fH.....Cw..x.^.....b\ct....Y.*.g.b...1*cR..%6F'.....Q-.....GH....L!?1...<.^Rf.G.H[O.<.Ke.....R..._e..1..s.....y.~..x!...Tl.... .a .;..KG.]%:."%.O..X.S..b..t.o{.....#..9...b. .J.e..w...<~b.....5.....XC....Z....E.zE.g.k.X.^.=.W)...>.'K.h<.C\././.7.d.....~./.a~.Yc.....4...{....d..m."...v.....v".....iY....9..ka.....M...m.})....Y..f..-..4..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\Urokkeligheden.Ord114

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	119298
Entropy (8bit):	**7.998253263209972**
Encrypted:	**true**
SSDEEP:	1536:6JcdhM4/003cKP7zr9UE0q19q9MUxJ0O1mwVrLSft3KeDQMjE4le/l1NUYeECfZm:LdhM4/Fpb/1Ca2LEt9DQMA4lGVUh14B
MD5:	251C92F85825E5BBBE4D7624FC7F4AE4
SHA1:	BF396458B8D37DCC5880B29A7482A4896828C35F
SHA-256:	20694D441EEAB696B6D6AE5B7785BB0CAD19E1708EF49C28737CAD1805B49CDC
SHA-512:	5730DF53CE6DE9791F81287EA340ECDECEF1B99B80DC7501F9739083AF5D66543795E82C19388522580A43B8553FEAA2D5C0B419502BC7325E34F1862BBD44D
Malicious:	false
Preview:	...Ct.m.j\i...G..@k.....D.....W.S.CE.P'.O....9l....4Y%\.R...%..'.D.o.%9h.....vP.h0...E_..1.}.....{...).h....F.r..Im....D..{..dF4.@F..=.....G..&..... v47.L..V..%.$x..rK..ue=. w.)..+b...$.m.Gj..@x.3...14J...#"....G| v8@Y2.R..v..."j...~.,..<..}...&H9F..v..=....>;.....HF..c...~..'c.f.p0"...>Q\./."...n..t.....$^.Z.c....h(.df.B..`,..#.?s.8..k'.B.t.....<3..s..h- ).Q..\R.O.C=.c.<S..b(..Q#.....r...j..z...U.vU.>..C...@...G-..7=.....".mu52.[...`Bf}0q.V.IF.\|(.pMo...^L.I.@.#[bH...1..I.I.Mi..iB..(N"$e.....r..9....1z.2..P.G*H..p....sE..O.cR.I.Z.H /.u_.Z+"Rk.M.g..q....Z..{0...*g....;....t..QF2.oA.v{....h.....TIN...r.. O.u..P...(........G.....+kk%9W.b.I.Q.....Gy9^~./..Q8..lo]$.5.....4. };.....80....ze.^I....WL.b....!..0.N.{Q...'..... I..dnP....7.p..aB.w.Z.v]R.../r.C6(q.C...%...n....2@..0$.X.;CW.1...5...s#.]..x[h..T./.>.(...dJ...q?._.I....K...1'....9.).n1#..5:&.S3^........Z.Z.0.c._.'.....r;bw.P.....K.^.....(....'..4.?....N....#.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\libgiognutls.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	131991
Entropy (8bit):	5.8780987492725405
Encrypted:	false
SSDEEP:	1536:v6J1cdTEl2OzvUtevCuoCW9fPr+vo9F5J7YWv3vbRnBycYWOGWSeaGymtYWOGWSS:VdW2OLgNCwXKSH8WPvVBjA+KE8S5
MD5:	10D998CF80B4437C2979B25EBCBE16D1
SHA1:	79C99DD2ABB99253E41C5E40DAB29522F93345BB
SHA-256:	A0A87BC30F4B39D7B642841A10208CE5286C6CA712B28B9D921E1EA6F547AEE6
SHA-512:	44863645B48815C3C248111F86440E3A0C515AF61B5A17D15B5A6C7304277F76056BCEB6C579E7824E11ADCA4DB3E385FA8019D602C40FA527E725C09B6AA523
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....&"...%.....P.....@.....g}.. ..`... .....IE.....0..... i..(.....text...X.....`..`.data..... .....@. ...rdata...A...0...B.....@..@.pdata.....R.....@..@.xdata..X.....`.....@..@.bss....p.....edata.....n.....@..@.idata.. IE.....F...p.....@....CRT....X.....@....tls..... .....@....reloc.....0.....@..B..... .....

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	477800
Entropy (8bit):	7.505402259729816
Encrypted:	false
SSDEEP:	12288:Lz772qgvq2nLm4W2RPLKb+nFzIQ3Ja8TA:gXnS4W2RPLKm/of
MD5:	7081C4822CF1C7572DD82822B8F27C49
SHA1:	4EE3B6C423B1C9EBF5BEFBC73D1EEF0C576CF026
SHA-256:	B5330F82F3C5C3F223AE9DECD3EBDCD74D1A13D95B1C42BD7B2DE4E6C6CB0083
SHA-512:	6E3377E6A47518F2267CD38646E2CEC576D41FD8A67C8C2590F43BF353C0B1F322FC229E70BC98E9C7DFAA1A11CF872A0C8E2C15A31EE90EF1C4E65EAC98EE 3A

Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..P...P...P..*_...P...P..OP..*_...P..s...P...V...P..Rich.P.....PE ..L...8.MX.....b...*.....J4.....@.....p.....@.....h.....5..X.....text ...a.....b..... ..`.rdata.....f.....@..@.data...8.....z.....@....ndata...0.....rsrc...h.....@..@..... ....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Tue Nov 29 05:27:07 2022, Security: 1
Entropy (8bit):	7.090542873047565
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	ACP-2210825ORDER.xls
File size:	1130496
MD5:	6c84860292e2a4d210396b7012be9b8a
SHA1:	7061c26320bf8836b55ac660860fa0937ae8f48e
SHA256:	cadae8bf6a2bcf1ee630695a250a481d22d0b6d409832f60070b118dfc3bca75
SHA512:	dbeb30f6ec918e82c13ed2aea4f14eeba7a38252fda3ebba49b63b0840a529b026cb36c40927b69d95970fe83c0b09c957a5b918d124eff97bfeaf3cda77a426
SSDEEP:	24576:XLsr5XXXXXXXXXXXUXXXXXXXSXXXXXXXXpmSr5XXXXXXXXXXXXUXXXXXXXSXXXZ:sh
TLSH:	1135BE347893CE36D9A586347BA6D5B103037C733E548A5722C3732E1AF334265D6EAA
File Content Preview:	.....>.....m...n...\...]...^.....n.....p.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "ACP-2210825ORDER.xls"

Indicators

Has Summary Info:	
Application Name:	Microsoft Excel
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Summary

Code Page:	1252
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2022-11-29 05:27:07
Creating Application:	
Security:	1

Document Summary	
Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	786432

Streams with VBA	
VBA File Name: Sheet1.cls, Stream Size: 977	
General	
Stream Path:	MBD017EF321/_VBA_PROJECT_CUR/VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	977
Data ASCII:	. . . . .] . . . # . . . . . x . . . . . M E . . . . . (. . . . . S L . . . . S . . . . . S . . . . . < . . . . . N . 0 . { . . 0 . 0 . 2 . 0 . 8 . 2 . 0 . - .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 5d c7 15 f4 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: Sheet2.cls, Stream Size: 977	
General	
Stream Path:	MBD017EF321/_VBA_PROJECT_CUR/VBA/Sheet2
VBA File Name:	Sheet2.cls
Stream Size:	977
Data ASCII:	. . . . .] & g . . # . . . . . x . . . . . M E . . . . . (. . . . . S L . . . . S . . . . . S . . . . . < . . . . . N . 0 . 0 . 0 . 2 . 0 . 8 . 2 . 0 . -
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 5d c7 26 67 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: Sheet3.cls, Stream Size: 977	
General	
Stream Path:	MBD017EF321/_VBA_PROJECT_CUR/VBA/Sheet3
VBA File Name:	Sheet3.cls
Stream Size:	977
Data ASCII:	. . . . .] . . . . # . . . . . x . . . . . M E . . . . . (. . . . . S L . . . . S . . . . . S . . . . . < . . . . . N . 0 . { 0 . 0 . 2 . 0 . 8 . 2 . 0 . -
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 5d c7 1e 0d 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 985	
General	
Stream Path:	MBD017EF321/_VBA_PROJECT_CUR/VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls

Stream Size:	985
Data ASCII:	. . . . .] K . . # . . . . . x . . . . . M E . . . . . (. . . . . S L . . . . S . . . . . S . . . . . < . . . . . N . 0 . { . . 0 . 0 . 2 . 0 . 8 . 1 . 9 . - .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 5d c7 d5 4b 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: Sheet1.cls, Stream Size: 977	
General	
Stream Path:	MBD017EF322/_VBA_PROJECT_CUR/VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	977
Data ASCII:	. . . . .] . . . # . . . . . x . . . . . M E . . . . . (. . . . . S L . . . . S . . . . . S . . . . . < . . . . . N . 0 . { . . 0 . 0 . 2 . 0 . 8 . 2 . 0 . - .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 5d c7 15 f4 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: Sheet2.cls, Stream Size: 977	
General	
Stream Path:	MBD017EF322/_VBA_PROJECT_CUR/VBA/Sheet2
VBA File Name:	Sheet2.cls
Stream Size:	977
Data ASCII:	. . . . .] & g . . # . . . . . x . . . . . M E . . . . . (. . . . . S L . . . . S . . . . . S . . . . . < . . . . . N . 0 . 0 . 0 . 2 . 0 . 8 . 2 . 0 . -
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 5d c7 26 67 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: Sheet3.cls, Stream Size: 977	
General	
Stream Path:	MBD017EF322/_VBA_PROJECT_CUR/VBA/Sheet3
VBA File Name:	Sheet3.cls
Stream Size:	977
Data ASCII:	. . . . .] . . . . # . . . . . x . . . . . M E . . . . . (. . . . . S L . . . . S . . . . . S . . . . . < . . . . . N . 0 . { . 0 . 0 . 2 . 0 . 8 . 2 . 0 . -
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 5d c7 1e 0d 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 985
General

Stream Path:	MBD017EF322/_VBA_PROJECT_CUR/VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	985
Data ASCII:	. . . . .] K . . # . . . . . x . . . . . M E . . . . . (. . . . . S L . . . . S . . . . . S . . . . . < . . . . . N . 0 . { . . 0 . 0 . 2 . 0 . 8 . 1 . 9 . - .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 5d c7 d5 4b 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.25248375192737
Base64 Encoded:	True
Data ASCII:	. . . . F & . . . M i c r o s o f t O f f i c e E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . 9 q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 26 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 244

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	244
Entropy:	2.889430592781307
Base64 Encoded:	False
Data ASCII:	. . . . . + , 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . S h e e t 1 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . W o r k s h e e t s . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 c4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 a1 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 200

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	200
Entropy:	3.268293668191049
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . + ' 0 . . . . . @ . . . . . H . . . . . T . . . . . ` . . . . . x . . . . . M i c r o s o f t E x c e l . @ . . . . | . # . @ . . . . 8 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: MBD017EF320/\x1CompObj, File Type: data, Stream Size: 99

General	
Stream Path:	MBD017EF320/\x1CompObj
File Type:	data
Stream Size:	99
Entropy:	3.631242196770981
Base64 Encoded:	False
Data ASCII:	. . . . . ! . . . M i c r o s o f t O f f i c e E x c e l W o r k s h e e t . . . . . E x c e l M L 1 2 . . . . . 9 q . . . . .

General	
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 57 6f 72 6b 73 68 65 65 74 00 0a 00 00 00 45 78 63 65 6c 4d 4c 31 32 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD017EF320/Package, File Type: Microsoft Excel 2007+, Stream Size: 11564

General	
Stream Path:	MBD017EF320/Package
File Type:	Microsoft Excel 2007+
Stream Size:	11564
Entropy:	7.132901381496351
Base64 Encoded:	True
Data ASCII:	P K . . . . ! . . o . . . L . . . . . . [C o n t e n t _ T y p e s] . x m l . (. . . .
Data Raw:	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 a2 c8 b4 f4 6f 01 00 00 4c 05 00 00 13 00 cb 01 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 c7 01 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

Stream Path: MBD017EF321/\x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	MBD017EF321/\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.25248375192737
Base64 Encoded:	True
Data ASCII:	. . . . F & . . . M i c r o s o f t O f f i c e E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . 9 q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 26 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD017EF321/\x5DocumentSummaryInformation, File Type: data, Stream Size: 244

General	
Stream Path:	MBD017EF321/\x5DocumentSummaryInformation
File Type:	data
Stream Size:	244
Entropy:	2.889430592781307
Base64 Encoded:	False
Data ASCII:	. . . . + , 0 . . . . H . . . . P . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . S h e e t 1 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . W o r k s h e e t s . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 c4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 a1 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: MBD017EF321/\x5SummaryInformation, File Type: dBase III DBT, version number 0, next free block index 65534, 1st item "\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\371\371\371\372\372\372\370\370\370\362\362\362\352\352\352\336\ Stream Size: 120200

General	
Stream Path:	MBD017EF321/\x5SummaryInformation
File Type:	dBase III DBT, version number 0, next free block index 65534, 1st item "\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\371\371\371\372\372\372\370\370\370\362\362\362\352\352\352\336\336\336\3 21\321\321\325\325\325\332\332\332\336\336\336\340\340\340\340\340\340\337\337\337\335\335\335\336\336\336\336\336\336\336\336\336\335\335 335\334\334\334\332\332\332\327\327\327\326\326\326\325\325\325\325\325\325\324\324\324\324\324\324\323\323\323\324\324\324\330\330\330\33 4\334\334\335\335\335\334\334\334\331\331\331\324\324\324\316\316\316\322\322\322\327\327\327"
Stream Size:	120200
Entropy:	4.560418312417174
Base64 Encoded:	True
Data ASCII:	. . . . O h . . . + ' 0 . . . X . . . . H . . . . P . . . . \\ . . . . h . . . . M i c r o s o f t E x c e l . @ . . . . | . # . @ . . . . G . . . . Z . . . . O . . . . ! . . . . c . . . . - . . . . ! . . . c . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 58 d5 01 00 08 00 00 00 01 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 08 00 00 00 5c 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 11 00 00 00 a0 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: MBD017EF321/MBD017ED236/\x1CompObj, File Type: data, Stream Size: 99

General	
Stream Path:	MBD017EF321/MBD017ED236/\x1CompObj

General	
File Type:	data
Stream Size:	99
Entropy:	3.631242196770981
Base64 Encoded:	False
Data ASCII:	......................!...Microsoft Office Excel Worksheet.....ExcelML12.....9q............
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 57 6f 72 6b 73 68 65 65 74 00 0a 00 00 00 45 78 63 65 6c 4d 4c 31 32 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD017EF321/MBD017ED236/Package, File Type: Microsoft Excel 2007+, Stream Size: 7880	
General	
Stream Path:	MBD017EF321/MBD017ED236/Package
File Type:	Microsoft Excel 2007+
Stream Size:	7880
Entropy:	6.5489983015138815
Base64 Encoded:	True
Data ASCII:	PK..........!.XV.`..........[Content_Types].xml .(..
Data Raw:	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 58 56 c6 8f 60 01 00 00 18 05 00 00 13 00 da 01 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 d6 01 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

Stream Path: MBD017EF321/Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 151951	
General	
Stream Path:	MBD017EF321/Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	151951
Entropy:	7.683490359133683
Base64 Encoded:	True
Data ASCII:	..............................\\.p.... B....a........=...............ThisWorkbook..=....l.9P.8.......X.@....
Data Raw:	09 08 10 00 00 06 05 00 a9 1f cd 07 c1 00 01 00 06 04 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 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 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

Stream Path: MBD017EF321/_VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 520	
General	
Stream Path:	MBD017EF321/_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	520
Entropy:	5.18674908320575
Base64 Encoded:	True
Data ASCII:	ID="{E603BE49-3BE4-49D7-957C-E16AB764E9E7}"..Document=ThisWorkbook/&H00000000..Document=Sheet1/&H00000000..Document=Sheet2/&H00000000..Document=Sheet3/&H00000000..Name="VBAProject"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="222024CA14CE14CE1
Data Raw:	49 44 3d 22 7b 45 36 30 33 42 45 34 39 2d 33 42 45 34 2d 34 39 44 37 2d 39 35 37 43 2d 45 31 36 41 42 37 36 34 45 39 45 37 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 32 2f 26 48 30 30 30

Stream Path: MBD017EF321/_VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 104	
General	
Stream Path:	MBD017EF321/_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	104
Entropy:	3.0488640812019017
Base64 Encoded:	False
Data ASCII:	ThisWorkbook.T.h.i.s.W.o.r.k.b.o.o.k...Sheet1.S.h.e.e.t.1...Sheet2.S.h.e.e.t.2...Sheet3.S.h.e.e.t.3.....
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 53 68 65 65 74 31 00 53 00 68 00 65 00 65 00 74 00 31 00 00 00 53 68 65 65 74 32 00 53 00 68 00 65 00 65 00 74 00 32 00 00 00 53 68 65 65 74 33 00 53 00 68 00 65 00 65 00 74 00 33 00 00 00 00 00

Stream Path: MBD017EF321/_VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2615

General	
Stream Path:	MBD017EF321/_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2615
Entropy:	3.966034925838034
Base64 Encoded:	False
Data ASCII:	a . . . . . @ . . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 0 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 6 . \\ . V . B . E . 6 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F . o . r .
Data Raw:	cc 61 85 00 00 01 00 ff 09 40 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 30 00 23 00

Stream Path: MBD017EF321/_VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 553	
General	
Stream Path:	MBD017EF321/_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	553
Entropy:	6.393413723460345
Base64 Encoded:	True
Data ASCII:	. % . . . . . 0 * . . . . p . . H . . . . d . . . . . V B A P r o j e c t . . 4 . . @ . . j . . . = ... r . . . . . e . . . . J < . . . . . r s t d o l e > . . . s . t . d . o . l . e . . . h . % . ^ . . * \\ G { 0 0 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ S y s W O W 6 4 \\ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . E O f f D i c E O . f . i . c E . . E . 2 D F 8 D 0 4 C . - 5 B F A - 1 0 1 B - B D E 5 E A A C 4 . 2 E .
Data Raw:	01 25 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 bc bb 86 65 0c 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Stream Path: MBD017EF322/\x1CompObj, File Type: data, Stream Size: 114	
General	
Stream Path:	MBD017EF322/\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.25248375192737
Base64 Encoded:	True
Data ASCII:	. . . . F & . . . M i c r o s o f t O f f i c e E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . 9 q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 26 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD017EF322/\x5DocumentSummaryInformation, File Type: data, Stream Size: 244	
General	
Stream Path:	MBD017EF322/\x5DocumentSummaryInformation
File Type:	data
Stream Size:	244
Entropy:	2.889430592781307
Base64 Encoded:	False
Data ASCII:	. . . . . + , 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . S h e e t 1 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . W o r k s h e e t s . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 c4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 a1 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: MBD017EF322/\x5SummaryInformation, File Type: dBase III DBT, version number 0, next free block index 65534, 1st item "\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\371\371\371\372\372\372\370\370\370\362\362\362\352\352\352\336\ Stream Size: 120200	
General	
Stream Path:	MBD017EF322/\x5SummaryInformation
File Type:	dBase III DBT, version number 0, next free block index 65534, 1st item "\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\371\371\371\372\372\372\370\370\370\362\362\362\352\352\352\336\336\336\3 21\321\321\325\325\325\332\332\332\336\336\336\340\340\340\340\340\340\337\337\337\335\335\335\336\336\336\336\336\336\336\336\336\335\335\ 335\334\334\334\332\332\332\327\327\327\326\326\326\325\325\325\325\325\325\324\324\324\324\324\324\323\323\323\324\324\324\330\330\330\33 4\334\334\335\335\335\334\334\334\331\331\331\324\324\324\316\316\316\322\322\322\327\327\327"
Stream Size:	120200
Entropy:	4.560271435258422
Base64 Encoded:	True

General	
Data ASCII:	. . . . O h . . . + ' 0 . . . X . . . . H . . . . P . . . . \\ . . . . h . . . . M i c r o s o f t E x c e l . @ . . . . | . # . @ . . . . G . . . . Z . . . . O . . . . ! . . . . c . . . . - . . . . ! . . . c . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 58 d5 01 00 08 00 00 00 01 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 08 00 00 00 5c 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 11 00 00 00 a0 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: MBD017EF322/MBD017ED236/\x1CompObj, File Type: data, Stream Size: 99	
General	
Stream Path:	MBD017EF322/MBD017ED236/\x1CompObj
File Type:	data
Stream Size:	99
Entropy:	3.631242196770981
Base64 Encoded:	False
Data ASCII:	. . . . ! . . . M i c r o s o f t O f f i c e E x c e l W o r k s h e e t . . . . . E x c e l M L 1 2 . . . . . 9 q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 57 6f 72 6b 73 68 65 65 74 00 0a 00 00 00 45 78 63 65 6c 4d 4c 31 32 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD017EF322/MBD017ED236/Package, File Type: Microsoft Excel 2007+, Stream Size: 7880	
General	
Stream Path:	MBD017EF322/MBD017ED236/Package
File Type:	Microsoft Excel 2007+
Stream Size:	7880
Entropy:	6.5489983015138815
Base64 Encoded:	True
Data ASCII:	P K . . . . ! . X V . ` . . . . [C o n t e n t _ T y p e s] . x m l . (. . . .
Data Raw:	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 58 56 c6 8f 60 01 00 00 18 05 00 00 13 00 da 01 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 d6 01 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

Stream Path: MBD017EF322/Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 151951	
General	
Stream Path:	MBD017EF322/Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	151951
Entropy:	7.683500296443008
Base64 Encoded:	True
Data ASCII:	. . . . \\ . p . . . . B . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... I . 9 P . 8 . . . . X . @ . . . .
Data Raw:	09 08 10 00 00 06 05 00 a9 1f cd 07 c1 00 01 00 06 04 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 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 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

Stream Path: MBD017EF322/_VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 524	
General	
Stream Path:	MBD017EF322/_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	524
Entropy:	5.18268582383174
Base64 Encoded:	True
Data ASCII:	I D = " { E 6 0 3 B E 4 9 - 3 B E 4 - 4 9 D 7 - 9 5 7 C - E 1 6 A B 7 6 4 E 9 E 7 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 1 / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 2 / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 3 / & H 0 0 0 0 0 0 0 0 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " F E F C F 8 9 E 0 8 A 6 A 0 A A A
Data Raw:	49 44 3d 22 7b 45 36 30 33 42 45 34 39 2d 33 42 45 34 2d 34 39 44 37 2d 39 35 37 43 2d 45 31 36 41 42 37 36 34 45 39 45 37 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 32 2f 26 48 30 30 30

Stream Path: MBD017EF322/_VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 104	
General	
Stream Path:	MBD017EF322/_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	104

General	
Entropy:	3.0488640812019017
Base64 Encoded:	False
Data ASCII:	T h i s W o r k b o o k . T . h . i . s . W . o . r . k . b . o . o . k . . . S h e e t 1 . S . h . e . e . t . 1 . . . S h e e t 2 . S . h . e . e . t . 2 . . . S h e e t 3 . S . h . e . e . t . 3 . . . . .
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 53 68 65 65 74 31 00 53 00 68 00 65 00 65 00 74 00 31 00 00 00 53 68 65 65 74 32 00 53 00 68 00 65 00 65 00 74 00 32 00 00 00 53 68 65 65 74 33 00 53 00 68 00 65 00 65 00 74 00 33 00 00 00 00 00

Stream Path: MBD017EF322/_VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2615	
General	
Stream Path:	MBD017EF322/_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2615
Entropy:	3.966034925838034
Base64 Encoded:	False
Data ASCII:	a . . . . . @ . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 0 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 2 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 6 . \ \ . V . B . E . 6 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F . o . r .
Data Raw:	cc 61 85 00 00 01 00 ff 09 40 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 30 00 23 00

Stream Path: MBD017EF322/_VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 553	
General	
Stream Path:	MBD017EF322/_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	553
Entropy:	6.393413723460345
Base64 Encoded:	True
Data ASCII:	. % . . . . . 0 * . . . . p . . H . . . . d . . . . . V B A P r o j e c t . . 4 . . @ . . j . . . = ... r . . . . . e . . . . J < . . . . . r s t d o l e > . . . s . t . d . o . l . e . . . h . % . ^ . . * \ \ G { 0 0 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s W O W 6 4 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . E O f f D i c E O . f . i . c E . . E . 2 D F 8 D 0 4 C . - 5 B F A - 1 0 1 B - B D E 5 E A A C 4 . 2 E .
Data Raw:	01 25 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 bc bb 86 65 0c 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Stream Path: MBD017EF323/\x1CompObj, File Type: data, Stream Size: 114	
General	
Stream Path:	MBD017EF323/\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.25248375192737
Base64 Encoded:	True
Data ASCII:	. . . . F & . . . M i c r o s o f t O f f i c e E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . 9 q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 26 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD017EF323/\x5DocumentSummaryInformation, File Type: data, Stream Size: 244	
General	
Stream Path:	MBD017EF323/\x5DocumentSummaryInformation
File Type:	data
Stream Size:	244
Entropy:	2.889430592781307
Base64 Encoded:	False
Data ASCII:	. . . . . + , 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . S h e e t 1 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . W o r k s h e e t s . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 c4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 a1 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: MBD017EF323/\x5SummaryInformation, File Type: dBase III DBT, version number 0, next free block index 65534, 1st item "\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\371\371\371\372\372\372\370\370\370\362\362\362\352\352\352\336\ Stream Size: 120200

General	
Stream Path:	MBD017EF323/\x5SummaryInformation
File Type:	dBase III DBT, version number 0, next free block index 65534, 1st item "\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\370\371\371\371\372\372\372\370\370\370\362\362\362\352\352\352\336\336\336\321\321\321\325\325\325\332\332\332\336\336\336\340\340\340\340\340\340\337\337\337\335\335\335\336\336\336\336\336\336\336\336\336\335\335\335\334\334\334\332\332\332\327\327\327\326\326\326\325\325\325\325\325\325\324\324\324\324\324\324\323\323\323\324\324\324\330\330\330\334\334\334\335\335\335\334\334\334\331\331\331\324\324\324\316\316\316\322\322\322\327\327\327"
Stream Size:	120200
Entropy:	4.560400140271791
Base64 Encoded:	True
Data ASCII:	. . . . O h . . . + ' 0 . . . X . . . . H . . . . P . . . . \\ . . . . h . . . . M i c r o s o f t E x c e l . @ . . . . | . # . @ . . . . G . . . . Z . . . . O . . . . ! . . . . c . . . . - . . . . ! . . . c . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 58 d5 01 00 08 00 00 00 01 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 08 00 00 00 5c 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 11 00 00 00 a0 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: MBD017EF323/MBD017ED236/\x1CompObj, File Type: data, Stream Size: 99	
General	
Stream Path:	MBD017EF323/MBD017ED236/\x1CompObj
File Type:	data
Stream Size:	99
Entropy:	3.631242196770981
Base64 Encoded:	False
Data ASCII:	. . . . ! . . . M i c r o s o f t O f f i c e E x c e l W o r k s h e e t . . . . . E x c e l M L 1 2 . . . . . 9 q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 57 6f 72 6b 73 68 65 65 74 00 0a 00 00 00 45 78 63 65 6c 4d 4c 31 32 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD017EF323/MBD017ED236/Package, File Type: Microsoft Excel 2007+, Stream Size: 7880	
General	
Stream Path:	MBD017EF323/MBD017ED236/Package
File Type:	Microsoft Excel 2007+
Stream Size:	7880
Entropy:	6.5489983015138815
Base64 Encoded:	True
Data ASCII:	P K . . . . ! . X V . ` . . . . [C o n t e n t _ T y p e s] . x m l . (. . . .
Data Raw:	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 58 56 c6 8f 60 01 00 00 18 05 00 00 13 00 da 01 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 d6 01 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

Stream Path: MBD017EF323/Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 151951	
General	
Stream Path:	MBD017EF323/Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	151951
Entropy:	7.6835052184911135
Base64 Encoded:	True
Data ASCII:	. . . . \\ . p . . . . B . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... I . 9 P . 8 . . . . X . @ . . . .
Data Raw:	09 08 10 00 00 06 05 00 a9 1f cd 07 c1 00 01 00 06 04 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 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 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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 08:13:05.353737116 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.475182056 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.475337982 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.476435900 CET	49173	80	192.168.2.22	172.245.34.91

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 08:13:05.603394032 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.603449106 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.603480101 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.603504896 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.603518009 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.603530884 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.603550911 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.603557110 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.603560925 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.603580952 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.603585005 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.603604078 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.603611946 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.603638887 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.603666067 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.603737116 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.616553068 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.724899054 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.724945068 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.724972010 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.724997997 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725025892 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725059986 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725080013 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725087881 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725087881 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725099087 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725119114 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725126982 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725126982 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725140095 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725147009 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725158930 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725177050 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725186110 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725204945 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725205898 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725219011 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725231886 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725249052 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725260019 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725286961 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725311995 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725338936 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725342035 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725342035 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725363970 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725342035 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725392103 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.725393057 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725393057 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725429058 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.725440979 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.726560116 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847157955 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847219944 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847260952 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847296000 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847332001 CET	80	49173	172.245.34.91	192.168.2.22

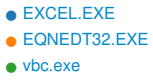
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 08:13:05.847367048 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847400904 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847434998 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847464085 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847466946 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847464085 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847500086 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847515106 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847531080 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847532034 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847558975 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847564936 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847580910 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847582102 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847601891 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847629070 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847657919 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847687006 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847687006 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847702980 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847719908 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847731113 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847749949 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847762108 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847774982 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847790003 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847795963 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847807884 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847819090 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847841978 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847865105 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847867012 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847891092 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847896099 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847913027 CET	49173	80	192.168.2.22	172.245.34.91
Nov 29, 2022 08:13:05.847913980 CET	80	49173	172.245.34.91	192.168.2.22
Nov 29, 2022 08:13:05.847929001 CET	49173	80	192.168.2.22	172.245.34.91

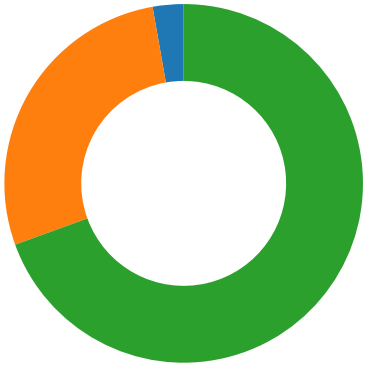
HTTP Request Dependency Graph

- 172.245.34.91

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1036, Parent PID: 576

General

Target ID:	0
Start time:	08:12:24
Start date:	29/11/2022
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:	0x13f8d0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	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\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E2D0648	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	f|+	binary	66 7C 2B 00 0C 04 00 00 02 00 00 00 00 00 00 00 58 00 00 00 01 00 00 00 2A 00 00 00 22 00 00 00 61 00 63 00 70 00 2D 00 32 00 32 00 31 00 30 00 38 00 32 00 35 00 6F 00 72 00 64 00 65 00 72 00 2E 00 78 00 6C 00 73 00 00 00 61 00 63 00 70 00 2D 00 32 00 32 00 31 00 30 00 38 00 32 00 35 00 6F 00 72 00 64 00 65 00 72 00 00 00	success or wait	1	6E2D0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: 1168, Parent PID: 576

General

Target ID:	2
Start time:	08:12:45
Start date:	29/11/2022
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	35406D3	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	35406D3	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	35406D3	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	35406D3	URLDownloadToFileW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	35406D3	URLDownloadToFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	35406D3	URLDownloadToFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	35406D3	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	35406D3	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	35406D3	URLDownloadToFileW
C:\Users\Public\vbc.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	35406D3	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\VBC[1].exe	0	694	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 31 fd fd 50 fd fd fd 50 fd fd fd 50 fd fd 2a 5f fd fd fd 50 fd fd fd 50 fd fd fd 4f 50 fd fd 2a 5f fd fd fd 50 fd bd 73 fd fd fd 50 fd fd 2e 56 fd fd fd 50 fd fd 52 69 63 68 fd 50 fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 38 fd 4d 58 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 62 00 00 00 2a 02 00 00 08 00 00 4a 34 00 00 00 10 00 00 00 fd 00 00 00 00 40	MZ@!L!This program cannot be run in DOS mode.$1PPP*_PPOP*_Ps P.VPRichPPEL8MXb*J4@	success or wait	1	35406D3	URLDownloadToFileW

<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\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\VBC[1].exe</td><td>694</td><td>8192</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td></td><td>success or wait</td><td>1</td><td>35406D3</td><td>URLDownloadToFileW</td></tr>
<tr><td>C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\VBC[1].exe</td><td>8886</td><td>1072</td><td>6a 6f fd 35 40 fd 42 00 fd 15 fd fd 40 00 6a 05 50 fd 0e 41 00 fd 15 68 fd 40 00 5e fd fd 55 fd fd fd 2c 02 00 00 53 56 33 fd 57 fd 5d fd fd 5d fd fd 15 fd fd 40 00 fd 00 fd 43 00 68 00 04 00 00 05 fd 03 00 00 56 53 fd 4c fd 42 00 fd 15 fd fd 40 00 6a 03 68 00 00 00 fd 56 fd fd 2e 00 00 fd fd fd fd fd fd 3d 18 fd 40 00 75 0a fd fd fd 40 00 fd 45 02 00 00 56 fd 00 68 43 00 56 fd fd 32 00 00 56 fd fd 2c 00 00 50 68 00 fd 43 00 fd fd 32 00 00 53 57 fd 15 fd fd 40 00 3b e3 fd fd 41 00 fd fd 0f fd fd 00 00 00 fd 54 fd 42 00 fd fd fd fd 1b fd 25 00 7e 00 00 05 00 02 00 00 3b fd 7c 02 fd fd 57 68 fd 41 00 fd 63 04 00 00 fd fd 0f fd 57 01 00 00 39 1d 54 fd 42 00 75 7e 6a 1c fd 45 fd 68 fd 41 00 50 fd fd 2d 00 00 fd 45 29 fd fd fd fd 75 71 fd 7d</td><td>jo5@B@jPAh@^U,SV3W]]@ChVSLB@jhV.=@u@EVhCV2V,PhC2SW@;ATB%~;|WhAcW9TBu~jEhAP-Euq}</td><td>success or wait</td><td>1</td><td>35406D3</td><td>URLDownloadToFileW</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	0	9958	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 31 fd fd 50 fd fd fd 50 fd fd fd 50 fd fd 2a 5f fd fd fd 50 fd fd fd 50 fd fd 4f 50 fd fd 2a 5f fd fd fd 50 fd bd 73 fd fd fd 50 fd fd 2e 56 fd fd fd 50 fd fd 52 69 63 68 fd 50 fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 38 fd 4d 58 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 62 00 00 00 2a 02 00 00 08 00 00 4a 34 00 00 00 10 00 00 00 fd 00 00 00 00 40	MZ@!L!This program cannot be run in DOS mode.$1PPP*_PPOP*_Ps P.VPRichPPEL8MXb*J4@	success or wait	1	35406D3	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\VBC[1].exe	13430	8192	fd 5b 02 00 00 fd 76 28 68 1a fd fd fd 57 fd 4d 02 00 00 6a 03 57 fd 15 6c fd 40 00 39 2d 22 42 00 fd 44 24 2c 74 08 66 fd fd fd fd fd fd 04 fd c3 fd 08 51 50 fd 15 68 fd 40 00 fd fd 25 00 01 00 00 50 fd 74 24 30 fd 15 18 fd 40 00 fd c3 fd 02 50 fd 28 02 00 00 fd fd 04 53 fd 35 fd 16 42 00 fd 15 18 fd 40 00 3b fd 74 03 55 fd 02 6a 01 68 60 fd 00 00 55 57 fd 15 fd fd 40 00 50 fd 15 fd fd 40 00 fd 1d 20 fd 40 00 6a 01 55 68 fd 00 00 00 fd 74 24 38 fd fd 39 2d 22 42 00 74 13 55 6a 02 68 01 04 00 00 57 fd fd fd 35 fd 16 42 00 fd 06 fd 35 24 37 42 00 fd fd 01 00 00 fd 28 37 42 00 68 40 fd 42 00 53 fd fd 20 00 00 fd 76 18 53 fd fd 20 00 00 fd 04 45 28 37 42 00 50 fd fd 20 00 00 53 57 fd 15 60 fd 40 00 55 fd 76 08 fd 1b fd fd fd fd fd 0f fd fd fd fd	[v(hWMjWl@9-BD$,tfQPh@%Pt$0@P(S5B@;tUjh`UW@P@@jUht$89-BtUjh W5B5$7B(7Bh@BS vSE(7BP SW`@Uv	success or wait	61	35406D3	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	9958	28292	fd 00 40 00 00 2b 05 fd 41 00 3b fd 7f 02 fd fd fd 4e 41 00 57 56 fd fd 00 00 00 00 fd fd 0f fd fd 00 00 00 01 3d fd 41 00 fd 35 60 fd 40 00 fd 3d 64 fd 40 00 39 1d 50 fd 42 00 74 29 39 1d fd 42 00 75 21 fd fd fd 41 00 53 2b 05 0e 41 00 2b 44 24 18 03 05 40 fd 40 00 fd 0e 41 00 fd fd fd fd 59 fd 48 fd 40 00 fd 2d 68 fd 40 00 fd 05 6c fd 40 00 00 fd 00 00 fd fd 33 00 00 fd fd 7c 6a fd 35 68 fd 40 00 2b fd 74 21 56 55 fd 35 1c fd 40 00 fd 16 2b 00 00 fd fd 74 4b 01 35 40 fd 40 00 39 1d 64 fd 40 00 75 fd fd 0c 39 1d 64 fd 40 00 75 37 3b fd 74 33 fd 0e 41 00 fd fd 2b 0d 40 fd 40 00 03 4c 24 14 fd fd 0f fd 25 fd fd fd 53 53 50 fd 35 1c fd 40 00 fd 15 48 fd 40 00 fd 0e fd fd fd fd 13 6a fd fd 02 6a fd 58 fd 0a 6a 01 fd 51 fd fd fd 59 33 fd	@+A;NAWV=A5`@=d@9PBt)9Bu!AS+A+D$@@AYH@-h@l@3\|j5h@+t!VU5@+tK5@@9d@u9d@u7;t3A+@@L$%SSP5@H@jjXjQY3	success or wait	8	35406D3	URLDownloadToFileW
C:\Users\Public\vbc.exe	388042	89758	3a 17 7c fd fd 3c fd 74 75 fd 6f fd 69 3a 01 4d fd fd 33 70 fd 2f fd 22 fd 59 fd fd 0d 25 fd 78 fd 0d 0b fd 68 d6 fd fd 14 fd fd fd 25 fd 09 2b 21 f8 67 fd 10 fd fd 64 fd 5a fd 4f 0a fd fd 48 62 7b fd 0c fd fd fd 43 0b fd 5d 78 47 fd fd 58 fd 17 4d 54 fd 37 fd fd fd 65 75 68 fd 51 fd 63 fd 63 fd fd 79 45 fd 60 fd 30 fd 54 fd 67 fd 78 fd 7a 66 fd fd 76 2a fd 27 7d fd fd 17 fd 16 fd fd fd 11 fd 32 47 10 fd 61 69 fd 04 fd 24 fd 02 fd fd fd fd df 51 fd fd 27 fd 51 31 fd 23 3c fd 61 34 fd 36 04 fd fd 5f 6a 72 fd 03 fd fd 5e 56 fd 3f 0d 16 fd fd fd fd 73 37 fd fd fd fd 34 fd 02 14 fd fd fd 6c fd cc fd 2a fd 15 fd fd 6b 7d fd 71 fd 06 fd 03 2c fd 0c fd 2f fd 1c fd 35 62 11 fd 17 27 35 44 fd 32 42 28 6e fd fd fd 08 08 fd fd 46 10	:|<tuoi:M3p/"Y%xh%+!gdZOHb{C]xGXMT7euhQcyE`0Tgxzfv*'}2Gi$Q'Q1#<a46_jr^V?s7l*k}q,/5b'5D2B(nF	success or wait	1	35406D3	URLDownloadToFileW

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: 1136, Parent PID: 1168

General

Target ID:	5
Start time:	08:12:50
Start date:	29/11/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	477800 bytes
MD5 hash:	7081C4822CF1C7572DD82822B8F27C49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000002.1187007837.00000000030C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsf59CD.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsf59CE.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Obeyeo.Bib	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\K noglemarvsundersgelsen	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\K noglemarvsundersgelsen\Armoniac	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\K noglemarvsundersgelsen\Armoniac\libgiognutls.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\K noglemarvsundersgelsen\Armonia c\Urokkeligheden.Ord114	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Temp\nsp5B93.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsp5B93.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405889	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsp5B93.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Temp\nsp5B93.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	3	405E13	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsp5B93.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	19411	405E13	CreateFileW
C:\Users\user\AppData\Local\Temp\nsp5B93.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	6	405E13	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsp5B93.tmp	success or wait	1	405A32	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	405EB3	WriteFile
unknown	43561	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	21	405EB3	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Obeyeo.Bib	0	16384	fd fd fd 36 fd 7b fd 3b 4e 9a fd 70 32 fd fd fd 48 fd 3d 4c fd 5d fd 5e fd 0f 08 fd 6c fd fd 62 fd 30 fd fd 32 29 0e 76 fd fd 58 1b fd 7e fd 16 71 fd fd 6e 6d fd 39 07 2e 24 68 fd 01 7f fd 59 5a 04 fd 7d fd fd 56 ea 75 fd fd 45 fd 61 28 4d fd fd fd fd c7 fd e5 fd fd 1f 71 14 fd fd fd 02 fd 40 39 32 6e fd 60 37 fd fd fd 15 fd fd 7a 0e 4e fd fd 7f 3c fd 19 fd 26 17 07 68 fd fd 5c fd 15 fd fd 7f 26 fd 68 40 70 fd fd fd 1c 0e 25 fd 7e 35 fd 5f 62 10 fd 62 fd fd fd fd 10 05 fd bf 42 28 7f fd fd fd 3a fd 34 fd fd 0e fd fd fd 74 fd 53 30 fd 0e 4a fd 1b 30 13 68 fd 26 fd b5 48 1c 74 fd 67 56 fd 26 fd fd 79 fd 2c 4a 2e 33 fd fd fd 6d 0c fd 5c fd fd 0b fd fd 00 1c 7e 6e fd 0a 4c fd 41 6e 49 fd fd 1a fd fd 43 fd 61 fd 37 77 5e	6{Np2H=L]lb02)vX~qnm9.$hYZ}VuEa(Mq@9n`7zN<&h\&h@p%~5_bbB(:4tS0J0h&HtgV&y,J.3m\~nLAnICa7w^	success or wait	11	405EB3	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\libgiognutls.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 00 00 00 00 00 fd 01 00 fd 01 00 00 fd 00 26 22 0b 02 02 25 00 0a 01 00 00 fd 01 00 00 04 00 00 50 13 00 00 00 10 00 00 00 00 fd fd 02 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 40 02 00 00 04 00 00 67 7d 02 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd&"%P@g}`	success or wait	9	405EB3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\Urokkeligheden.Ord114	0	16384	fd fd fd 43 74 fd 6d 17 6a 5c 69 fd fd 12 47 fd fd 40 6b fd fd fd 1e fd fd 44 11 fd df fd fd 57 fd 53 fd 43 45 fd 50 27 fd 4f fd fd 02 fd 39 6c fd 46 fd fd 34 59 25 5c fd 52 fd fd 14 25 17 fd 27 fd 44 fd 6f fd 25 39 68 fd fd fd fd 12 fd fd fd 76 50 08 68 30 2e fd fd 45 5f fd fd 31 00 7d fd fd 3d fd e2 fd fd fd fd fd fd fd 85 fd 0b 7b fd 06 fd 29 fd 68 fd fd fd fd 46 fd 72 fd fd 6c 6d 0d fd 01 1f 44 0a 14 7b fd fd 64 46 34 fd 40 46 fd fd 3d 07 19 fd 11 fd 47 fd fd 26 fd fd 10 15 fd fd fd 20 76 34 37 fd 4c 53 18 56 00 fd 25 fd 24 78 07 fd 72 4b fd 11 75 65 3d 1d 77 fd 29 fd fd 2b 62 fd fd 1d 24 fd 6d fd 47 6a fd fd 40 78 fd 33 fd 08 15 31 34 4a 17 03 fd 23 22 fd 13 11 fd 47 7c 20 76 38 40 59 32 fd 52 fd fd 76 fd fd 22	Ctmj\iG@kDWSCEP'O9l4Y%\R%'Do%9hvPh0.E_1}{)hFrlmD{dF4@F=G& v47LV%$xrKue=w)+b$mGj@x314J#"G| v8@Y2Rv"	success or wait	8	405EB3	WriteFile
C:\Users\user\AppData\Local\Temp\nsp5B93.tmp\System.dll	0	11776	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 31 fd fd fd 75 fd 75 fd 75 fd fd bd 73 fd 75 fd 61 b3 76 fd fd 72 fd 21 4c fd 71 fd 16 16 fd 74 b3 4a b8 fd 74 fd 52 69 63 68 75 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 1a fd 4d 58 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 20 00	MZ@!L!This program cannot be run in DOS mode.$1uuusuar!qttRichuPELMX!	success or wait	1	405EB3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	400	405E84	ReadFile
C:\Users\Public\vbc.exe	unknown	16384	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf59CE.tmp	unknown	4	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf59CE.tmp	unknown	26442	success or wait	1	403269	ReadFile
C:\Users\user\AppData\Local\Temp\nsf59CE.tmp	unknown	4	success or wait	3	405E84	ReadFile
C:\Users\Public\vbc.exe	unknown	16384	success or wait	16	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf59CE.tmp	unknown	16384	success or wait	28	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf59CE.tmp	unknown	4	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf59CE.tmp	unknown	4	success or wait	2	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf59CE.tmp	unknown	4	success or wait	19411	405E84	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\Urokkeligheden.Ord114	unknown	2	success or wait	318	4026D2	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Obeyeo.Bib	unknown	1052672	success or wait	1	10002965	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Spaan	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Spaan\Pushfully	success or wait	1	40242E	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Spaan\Pushfully	Trials101	binary	FF C0 52 EF	success or wait	1	40248E	RegSetValueExW

Disassembly

No disassembly