ID: 441336
Sample Name:
DEBT_2026004977_03182021.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:43:55
Date: 28/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report DEBT_2026004977_03182021.xlsm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
System Summary: 4
Signature Overview 4
AV Detection: 5
Software Vulnerabilities: 5
Networking: 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 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 14
General 14
File Icon 14
Static OLE Info 14
General 14
OLE File "DEBT_2026004977_03182021.xlsm" 14
Indicators 14
Macro 4.0 Code 14
Network Behavior 14
Network Port Distribution 14
TCP Packets 14
HTTP Request Dependency Graph 14
HTTP Packets 15
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: EXCEL.EXE PID: 2580 Parent PID: 584 15
General 15
File Activities 16
File Created 16
File Deleted 16
File Moved 16
File Written 16
File Read 16
Registry Activities 16
Key Created 16
Key Value Created 16
Analysis Process: rundll32.exe PID: 2352 Parent PID: 2580 16
General 16
File Activities 16
Analysis Process: rundll32.exe PID: 3056 Parent PID: 2580 16

General 16
File Activities 16
Analysis Process: rundll32.exe PID: 2620 Parent PID: 2580 17
General 17
File Activities 17
Disassembly 17
Code Analysis 17

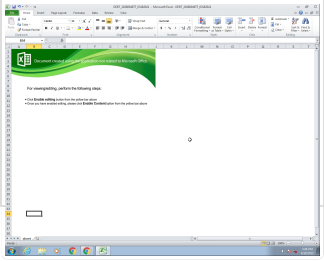
Windows Analysis Report DEBT_2026004977_03182021…

Overview

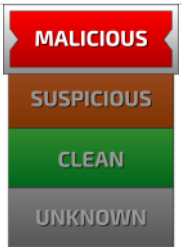
General Information

Sample Name:	DEBT_2026004977_03182021.xlsm
Analysis ID:	441336
MD5:	042b349265bbac..
SHA1:	41b74d0c3b18fdc..
SHA256:	ba1912b685d37e..
Infos:	

Most interesting Screenshot:



Detection



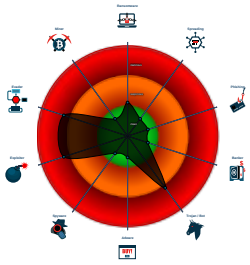
Hidden Macro 4.0

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Yara detected MalDoc1
- Excel documents contains an embe…
- IP address seen in connection with o…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2580 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2352 cmdline: Rundll32 ..\Kiod.hod,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 3056 cmdline: Rundll32 ..\Kiod.hod1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2620 cmdline: Rundll32 ..\Kiod.hod2,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
sharedStrings.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Yara detected MalDoc1

System Summary:

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

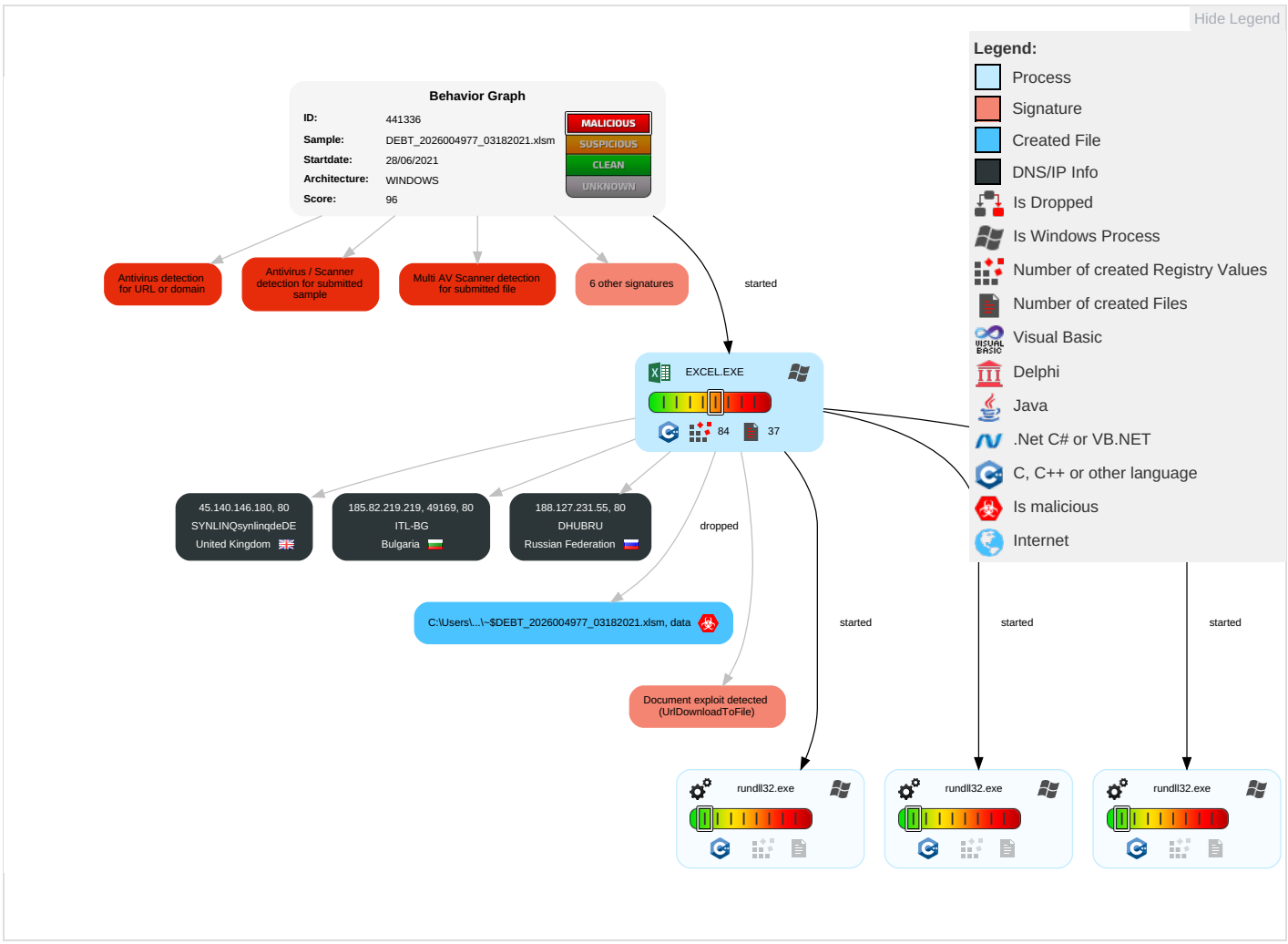
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

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 1	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 2	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 2	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 4	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 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R or

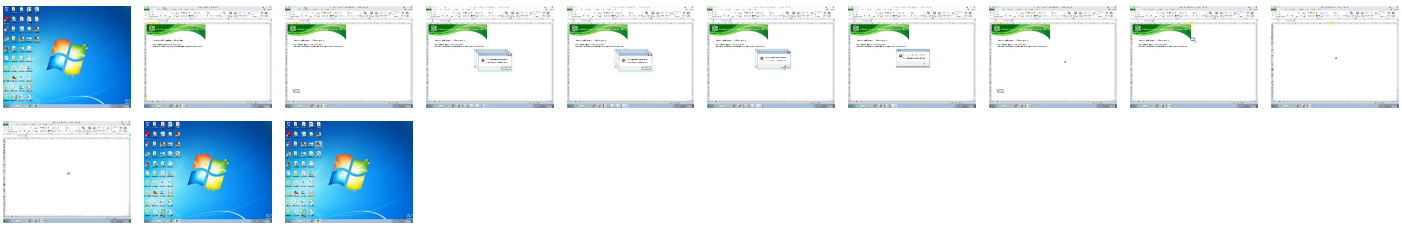
Behavior Graph

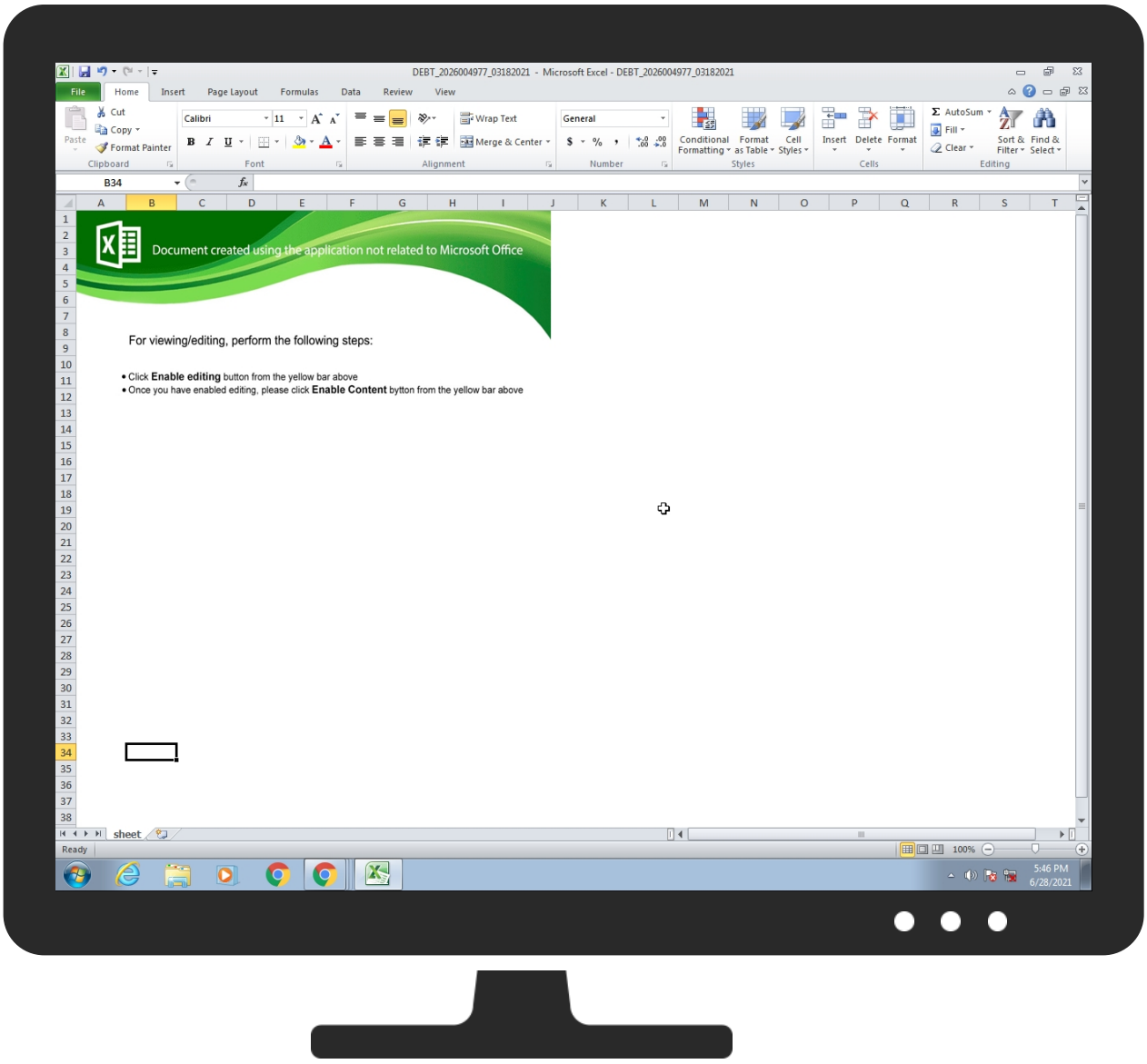


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DEBT_2026004977_03182021.xlsm	56%	Virustotal		Browse
DEBT_2026004977_03182021.xlsm	14%	Metadefender		Browse
DEBT_2026004977_03182021.xlsm	69%	ReversingLabs	Document-Excel.Trojan.TrickBot	
DEBT_2026004977_03182021.xlsm	100%	Avira	EXP/AgentXLM.gpg	

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	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://185.82.219.219/44375.7393215278.dat	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.82.219.219/44375.7393215278.dat	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.140.146.180	unknown	United Kingdom		44486	SYNLINQsynlinqdeDE	false
188.127.231.55	unknown	Russian Federation		56694	DHUBRU	false
185.82.219.219	unknown	Bulgaria		59729	ITL-BG	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	441336
Start date:	28.06.2021
Start time:	17:43:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DEBT_2026004977_03182021.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:	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:	mal96.troj.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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.140.146.180	DEBT_1968116513_03182021.xlsm	Get hash	malicious	Browse	• 45.140.146.180/44287.2826271991.dat
	DEBT_1968116513_03182021.xlsm	Get hash	malicious	Browse	• 45.140.146.180/44287.2769295139.dat
	DEBT_606324840_03182021.xlsm	Get hash	malicious	Browse	• 45.140.146.180/44283.5980373843.dat
	DEBT_606324840_03182021.xlsm	Get hash	malicious	Browse	• 45.140.146.180/44283.5927740741.dat
	DEBT_200373256_03182021.xlsm	Get hash	malicious	Browse	• 45.140.146.180/44273.5569056713.dat
	DEBT_200373256_03182021.xlsm	Get hash	malicious	Browse	• 45.140.146.180/44273.5518829861.dat
188.127.231.55	DEBT_48273645_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55/44273.9677637732.dat
	DEBT_42762980_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55/44273.9653645833.dat
	DEBT_48273645_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55/44273.9629790509.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DEBT_42762980_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55/44273.9601648148.dat
	DEBT_1423690834_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55/44273.79245.dat
	DEBT_1423690834_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55/44273.7872909722.dat
	DEBT_1741141015_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55/44273.7143896991.dat
	DEBT_1484725979_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55/44273.6309172454.dat
	DEBT_1484725979_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55/44273.6248686343.dat
	DEBT_200373256_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55/44273.5569056713.dat
	DEBT_200373256_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55/44273.5518829861.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SYNLINQsynlinqdeDE	ziMPI733fD.exe	Get hash	malicious	Browse	• 45.140.146.253
	o8RYFTZsuU.exe	Get hash	malicious	Browse	• 45.140.146.209
	MrjC4jkPL8.exe	Get hash	malicious	Browse	• 45.140.146.209
	D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe	Get hash	malicious	Browse	• 45.140.147.241
	D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe	Get hash	malicious	Browse	• 45.140.147.241
	TbM6OcUcjT.exe	Get hash	malicious	Browse	• 45.140.147.99
	sdXXFJs5Jq.exe	Get hash	malicious	Browse	• 45.140.147.99
	M1qgqxIZD5.exe	Get hash	malicious	Browse	• 45.140.147.99
	gCCsYyiaIf.exe	Get hash	malicious	Browse	• 45.140.147.99
	AFbK5IqLSC.exe	Get hash	malicious	Browse	• 45.140.147.99
	Bejful1QcQ.exe	Get hash	malicious	Browse	• 45.140.147.99
	1OZycQqlus.exe	Get hash	malicious	Browse	• 45.140.147.99
	k6TgnZE7N6.exe	Get hash	malicious	Browse	• 45.140.147.99
	hILi1CVD4a.exe	Get hash	malicious	Browse	• 45.140.147.99
	nbEmsl0Ep5.exe	Get hash	malicious	Browse	• 45.140.147.99
	R7M6NW416K.exe	Get hash	malicious	Browse	• 45.140.147.99
	HOB5G1yb08.exe	Get hash	malicious	Browse	• 45.140.147.99
	iwp6z0D9Fg.exe	Get hash	malicious	Browse	• 45.140.147.99
	6VLvFftCxz.exe	Get hash	malicious	Browse	• 45.140.147.99
	UzpZjUEotb.exe	Get hash	malicious	Browse	• 45.140.147.99
ITL-BG	0EG8l0QFdv.exe	Get hash	malicious	Browse	• 185.82.217.53
	DEBT_06032021_727093524.xlsm	Get hash	malicious	Browse	• 185.82.216.183
	DEBT_06032021_727093524.xlsm	Get hash	malicious	Browse	• 185.82.216.183
	DEBT_06032021_1841965006.xlsm	Get hash	malicious	Browse	• 185.82.216.183
	DEBT_06032021_1841965006.xlsm	Get hash	malicious	Browse	• 185.82.216.183
	9b5350dd_by_Libranalysis.exe	Get hash	malicious	Browse	• 176.103.62.217
	DEBT_1815748818_03182021.xlsm	Get hash	malicious	Browse	• 185.82.219.219
	DEBT_1815748818_03182021.xlsm	Get hash	malicious	Browse	• 185.82.219.219
	SG1.exe	Get hash	malicious	Browse	• 176.103.62.217
	Debt-Details-503724395-05132021.xlsm	Get hash	malicious	Browse	• 185.82.217.23

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Debt-Details-503724395-05132021.xlsm	Get hash	malicious	Browse	• 185.82.217.23
	KIxSEAenmw.exe	Get hash	malicious	Browse	• 185.82.219.104
	Complaint-1704044493-04302021.xlsm	Get hash	malicious	Browse	• 185.82.219.131
	Complaint-1704044493-04302021.xlsm	Get hash	malicious	Browse	• 185.82.219.131
	Complaint-1290253200-04302021.xlsm	Get hash	malicious	Browse	• 185.82.219.131
	Complaint-1704044493-04302021.xlsm	Get hash	malicious	Browse	• 185.82.219.131
	Complaint-1290253200-04302021.xlsm	Get hash	malicious	Browse	• 185.82.219.131
	Complaint-1290253200-04302021.xlsm	Get hash	malicious	Browse	• 185.82.219.131
	IjckXG93Xw.exe	Get hash	malicious	Browse	• 176.103.62.217
	OD7kxw3BkW.exe	Get hash	malicious	Browse	• 176.103.62.217
DHUBRU	BCFtNdJx3z.exe	Get hash	malicious	Browse	• 185.9.147.62
	DEBT_1815748818_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55
	DEBT_1815748818_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55
	a39c6293_by_Libranalysis.xls	Get hash	malicious	Browse	• 188.127.254.61
	5718536382-05122021.xlsm	Get hash	malicious	Browse	• 188.127.23 1.165
	758850407-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 1.176
	758850407-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 1.176
	758850407-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 1.176
	7310182546-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 1.176
	7310182546-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 1.176
	71235245139-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 1.176
	7310182546-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 1.176
	71235245139-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 1.176
	71235245139-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 1.176
	Contract_858526758.xlsm	Get hash	malicious	Browse	• 188.127.22 7.146
	Contract_858526758.xlsm	Get hash	malicious	Browse	• 188.127.22 7.146
	Overdue-675934828-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 4.138
	Overdue-675934828-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 4.138
	Overdue-675934828-04212021.xlsm	Get hash	malicious	Browse	• 188.127.25 4.138
	Waltons PO- 84635.xls	Get hash	malicious	Browse	• 188.127.254.61

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7A4B8C50.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 1386x1386, frames 3
Category:	dropped
Size (bytes):	171553
Entropy (8bit):	7.651426384659082
Encrypted:	false
SSDEEP:	3072:RXFYiB3kNT+2Jozo1UW8gOvlAsku0Gy3ZsY0OPlaK/LBd:RXFYiB3kNBozoR8gOvljFy3ZIOXP
MD5:	1BE35F6C74B488050049162605294C82
SHA1:	6788B12BD406903C82C3ED6FD46DD8E833612A74

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7A4B8C50.jpeg	
SHA-256:	788C88EB21A724887B5258A8170157BD11FE6A78E0C2C71326E194B6BDF12AC9
SHA-512:	EC53901E929051B186070127AD6B05F1A8E6D25C8216187285AB07B78534DF12649204C81B0A9059ADBDF95AAA92CC3978B68DE60A0DB170EB5C66F74FC8289
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.............C...C...j.j.."..}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?....(.....(...(...(...(...(...(...(...(...(...(...(... (...(..sM.6...j.M...]....<..U{{.....+.n.V...+.....z...;....C..E.......3/L.r3....J.]...[..z-Y...Zw.Lz..eY.!_7...i.S..W`..c.h. .L.8\....h.G..K.n%-.y.m..}..i..i >q..in...@.._.u.^.).m.o.s.J...6.ZI.>zyV..._n.G......

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Temp\1ACE0000</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>188484</td></tr>
<tr><td>Entropy (8bit):</td><td>7.658901379717203</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:YATXFYiB3kNT+2Jozo1UW8gOvlAsku0Gy3ZsY0OPlaK/LBQgB:YATXFYiB3kNBozoR8gOvljFy3ZIOXF</td></tr>
<tr><td>MD5:</td><td>719CF4C7AEF95CBDC3DAD35942D5D1FE</td></tr>
<tr><td>SHA1:</td><td>1C4579FD8230F972FD6FDB04BEA1FD5C0705C9A6</td></tr>
<tr><td>SHA-256:</td><td>49D4FF5754F0FCE1BF2C10D806E10607480EAFF191D47EE4D9B52FC8397D76E1</td></tr>
<tr><td>SHA-512:</td><td>F619F009E22A9452AE47DBDAA3D05B265F5731A1B11C4CA56DEDF599159AA34100DA4DAFF380888B6F0CE13556AB43CAF30F8AB1D964B78757B2C5EE97E594
B</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>...n.0.E.......D'.....E....I?.&..k..a...;...5.K....{..H......"j.Zv..X.Nz.]..._..$...;h....,..?l.`E..[..>q...+......|.".m.x.r-:......K.R...[..J<.T.n....R;V}..Q-.!.-E"...#H.W+-Ay.hI...A(...5M.....R.....<br>.#...tY8....Q..}%..,.`....r..*..^.}.wja...;..7a.^|c.......H....6.LSj.X!..ubi..v/..J$.r.....39...I...Q|O5r..w.T...|.c..O........0m...\..n':D.E.u..O....?..|.(........{...1...&.........1}.}@.."L.....]....4....u .t..
<.\ .S...6/...........PK..........!..#|.....X.......[Content_Types].xml ...(..
....
....</td></tr>
</table>

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\DEBT_2026004977_03182021.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 14:08:13 2020, mtime=Mon Jun 28 23:44:37 2021, atime=Mon Jun 28 23:44:37 2021, length=188484, window=hide
Category:	dropped
Size (bytes):	2178
Entropy (8bit):	4.518526401830706
Encrypted:	false
SSDEEP:	48:8kH/XT3Ikktr6A2Qh2kH/XT3Ikktr6A2Q/:8kH/XLIkk92Qh2kH/XLIkk92Q/
MD5:	F3029A0853DC2BFE43D4375065D99C44
SHA1:	946470D92403DEAF57A368C48E3A5010CCC4A4A5
SHA-256:	B911471017EC3469F8573D29AD9B35C4B2A4968CEC8E61D618C90675C4762C6C
SHA-512:	3EE2D51B0F862E4A94EBB094AD4B85BD26091509C8ACB652C45FBA216BFF7748B255BE0754946204AE6B50AF97E24F2B5BAE1922B81B6F5D4A2FBC640021C69 B
Malicious:	false
Reputation:	low
Preview:	L..................F.... ....0H..{......l.......l..D............................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.N....R.. .DEBT_2~1.XLS..h.......Q.y.Q.y*...8....................D.E.B.T._.2.0.2.6.0.0.4.9.7.7._.0.3.1.8.2.0.2.1...x.l.s.m......................-...8...[............?J......C:\Users\. .#..................\\302494\Users.user\Desktop\DEBT_2026004977_03182021.xlsm.4.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.E.B.T._.2.0.2.6.0.0.4.9.7.7._.0.3.1.8.2.0.2.1...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..

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=Mon Jun 28 23:44:37 2021, atime=Mon Jun 28 23:44:37 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.468852982717485
Encrypted:	false
SSDEEP:	12:85QPLgXg/XAlCPCHaXgzB8IB/ddiUkvX+WnicvbbbDtZ3YilMMEpxRljKPTdJP9O:854/XTwz6IDdivYebDv3q2rNru/
MD5:	92AE07EB4E1468AC1DE7B75803DB7D4A
SHA1:	A17F5354A490AD838391CE772C65F1C37C5B894A
SHA-256:	637AFD1B3EB4EF42D3FEE7A568906D5545D0D2A20CCB773F87DCE461AD79BD44
SHA-512:	153235E7C510F9FF0E22FB705D446AE789A6EBD1E1E8BE8EF5AFE8FFD987ED2E70DC773C3D9F965F0C1BE631311CADAE56422E622FB117CABC74F27C211BE C2

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G.....l.....l...0.....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\..#.....\\302494\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.....302494.....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):	127
Entropy (8bit):	4.61015684972344
Encrypted:	false
SSDEEP:	3:oyBVomxWqiUT/RRXVEAl5DT/RRXVEAlmxWqiUT/RRXVEAlv:djZlbrDlbWlb1
MD5:	D21723E510B78E341C756E99ABD11363
SHA1:	EB6EAA4916A35A49A850AF3DFF7C41C4E8AF9E3D
SHA-256:	20AB3F8F28533ADDE478FD4F3152D6A27DC04C84FD876FEC7F65BCB414668F59
SHA-512:	9B9E807CEEFC53C2878DEB090479802C12D2CD86F6DE797DF4A8F227F47A733E5159EFFBEAB8DC7C1F00AB29266549F9D08423BC0E78A6C91403094AB2F2990B
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..DEBT_2026004977_03182021.LNK=0..DEBT_2026004977_03182021.LNK=0..[misc]..DEBT_2026004977_03182021.LNK=0..[misc]..DEBT_2026004977_03182021.LNK=0..

C:\Users\user\Desktop\DACE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	188484
Entropy (8bit):	7.658901379717203
Encrypted:	false
SSDEEP:	3072:YATXFYiB3kNT+2Jozo1UW8gOvlAsku0Gy3ZsY0OPlaK/LBQgB:YATXFYiB3kNBozoR8gOvljFy3ZIOXF
MD5:	719CF4C7AEF95CBDC3DAD35942D5D1FE
SHA1:	1C4579FD8230F972FD6FDB04BEA1FD5C0705C9A6
SHA-256:	49D4FF5754F0FCE1BF2C10D806E10607480EAFF191D47EE4D9B52FC8397D76E1
SHA-512:	F619F009E22A9452AE47DBDAA3D05B265F5731A1B11C4CA56DEDF599159AA34100DA4DAFF380888B6F0CE13556AB43CAF30F8AB1D964B78757B2C5EE97E594B
Malicious:	false
Reputation:	low
Preview:	...n.0.E.....D'.....E....I?.&..k..a...;...5.K....{..H....."j.Zv..X.Nz.]..._..$...;h....,..?l.`E..[..>q...+.....|.".m.x.r-:.....K.R...[..J<.T.n....R;V}..Q-.!.-E"...#H.W+-Ay.hI...A(...5M.....R.....#...tY8....Q..}%...,`....r..*..^.}.wja...;..7a.^|c.....H....6.LSj.X!..ubi..v/..J$.r.....39...I...Q|O5r..w.T...|.c..O.....0m...\..n':D.E.u..O....?..|.(.....{...1...&.....1}.}@..".L.....]....4....u .t..<.\ .S...6/.....PK.....!..#|.....X.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$DEBT_2026004977_03182021.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**
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):	7.661072420094417
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	DEBT_2026004977_03182021.xlsm
File size:	189006
MD5:	042b349265bbac709ff2cbddb725033b
SHA1:	41b74d0c3b18fdcd17a8ca7ebfd883421f39c993
SHA256:	ba1912b685d37e4db3b8a622fa966a5e2c2f38c56037bfcc2a9f0a6f39872429
SHA512:	59faf72347ac8dde4e263fb3c4e6a063dd4f59159ea55eebfffc6446789afce6ba1a3db8f69916dbe73f5c5c51837ea91e47930b131eb70d962b952ab7d4c131
SSDEEP:	3072:jQXFYiB3kNT+2Jozo1UW8gOvlAsku0Gy3ZsY0OPlaK/LBE:jQXFYiB3kNBozoR8gOvljFy3ZIOX6
File Content Preview:	PK..........!..#|.....X.......[Content_Types].xml ...(..

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "DEBT_2026004977_03182021.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

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 185.82.219.219

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	185.82.219.219	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 28, 2021 17:46:10.333620071 CEST	1	OUT	GET /44375.7393215278.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: 185.82.219.219 Connection: Keep-Alive
Jun 28, 2021 17:46:10.396786928 CEST	1	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.0 (Ubuntu) Date: Mon, 28 Jun 2021 15:46:10 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Content-Encoding: gzip Data Raw: 63 36 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ed 90 b1 0a c2 30 10 86 77 c1 77 38 3b e9 90 a6 85 8e 31 8b 28 38 e8 22 3e 40 62 ce 26 90 26 12 53 b4 6f 6f a2 15 c4 d9 d1 f1 fe fb ee bb e3 98 8e 9d e5 d3 09 d3 28 14 67 d1 44 8b bc a9 1a d8 fb 08 1b df 3b c5 e8 2b 64 f4 89 24 54 7a 35 80 6c 4f de fa b0 2c 6e da 44 2c b2 e2 84 2e 62 e0 4c d7 df 86 94 30 3a b6 f3 ae 04 8d 95 6b 8d bb d3 ba ac 9b b2 82 f9 51 f6 2e f6 8b 4f 96 e6 6d d9 4e df 97 ce 08 01 01 17 a1 94 71 2d 44 0f ca 5c 85 b4 08 bb c3 76 0d c2 29 58 e9 e0 3b 84 73 30 e8 94 1d 00 43 f0 21 4d b4 08 84 64 d7 5f f1 cb 5f 3c 00 85 02 e0 de 44 02 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: c60ww8;1(8">@b&&Soo(gD;+d$Tz5lO,nD,.bL0:kQ.OmNq-D\v)X;s0C!Md__<D0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2580 Parent PID: 584

General

Start time:	17:44:34
Start date:	28/06/2021
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:	0x13f730000
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 — Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 2352 Parent PID: 2580

General

Start time:	17:46:01
Start date:	28/06/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	Rundll32 ..\Kiod.hod,DllRegisterServer
Imagebase:	0xff330000
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 — Show Windows behavior

Analysis Process: rundll32.exe PID: 3056 Parent PID: 2580

General

Start time:	17:46:02
Start date:	28/06/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	Rundll32 ..\Kiod.hod1,DllRegisterServer
Imagebase:	0xff330000
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 — Show Windows behavior

Analysis Process: rundll32.exe PID: 2620 Parent PID: 2580

General

Start time:	17:46:02
Start date:	28/06/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	Rundll32 ..\Kiod.hod2,DllRegisterServer
Imagebase:	0xff330000
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

Show Windows behavior

Disassembly

Code Analysis