ID: 433165
Sample Name: document-447482460.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:04:48
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

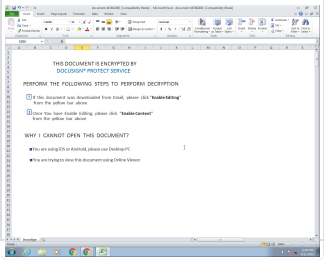
Analysis Report document-447482460.xls

Overview

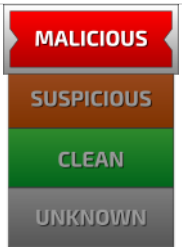
General Information

Sample Name:	document-447482460.xls
Analysis ID:	433165
MD5:	c956ee532ca353..
SHA1:	f99efeea7c2ca81..
SHA256:	8c00f6935288672.
Infos:	

Most interesting Screenshot:



Detection



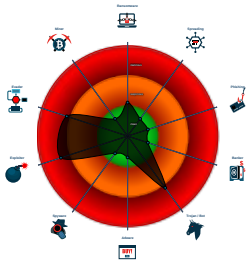
Hidden Macro 4.0

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Outdated Microsoft Office dropper d…
- Sigma detected: Microsoft Office Pr…
- Yara detected hidden Macro 4.0 in E…
- Document contains embedded VBA …
- Potential document exploit detected…
- Tries to resolve domain names, but …

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2436 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2580 cmdline: rundll32 ..\nxckew.wle,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
document-447482460.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x11d56:$e1: Enable Editing • 0x11dcb:$e2: Enable Content
document-447482460.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x134a2:$s1: Excel • 0x144fd:$s1: Excel • 0x37b4:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-447482460.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

Copyright Joe Security LLC 2021

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Outdated Microsoft Office dropper detected

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

HIPS / PFW / Operating System Protection Evasion:

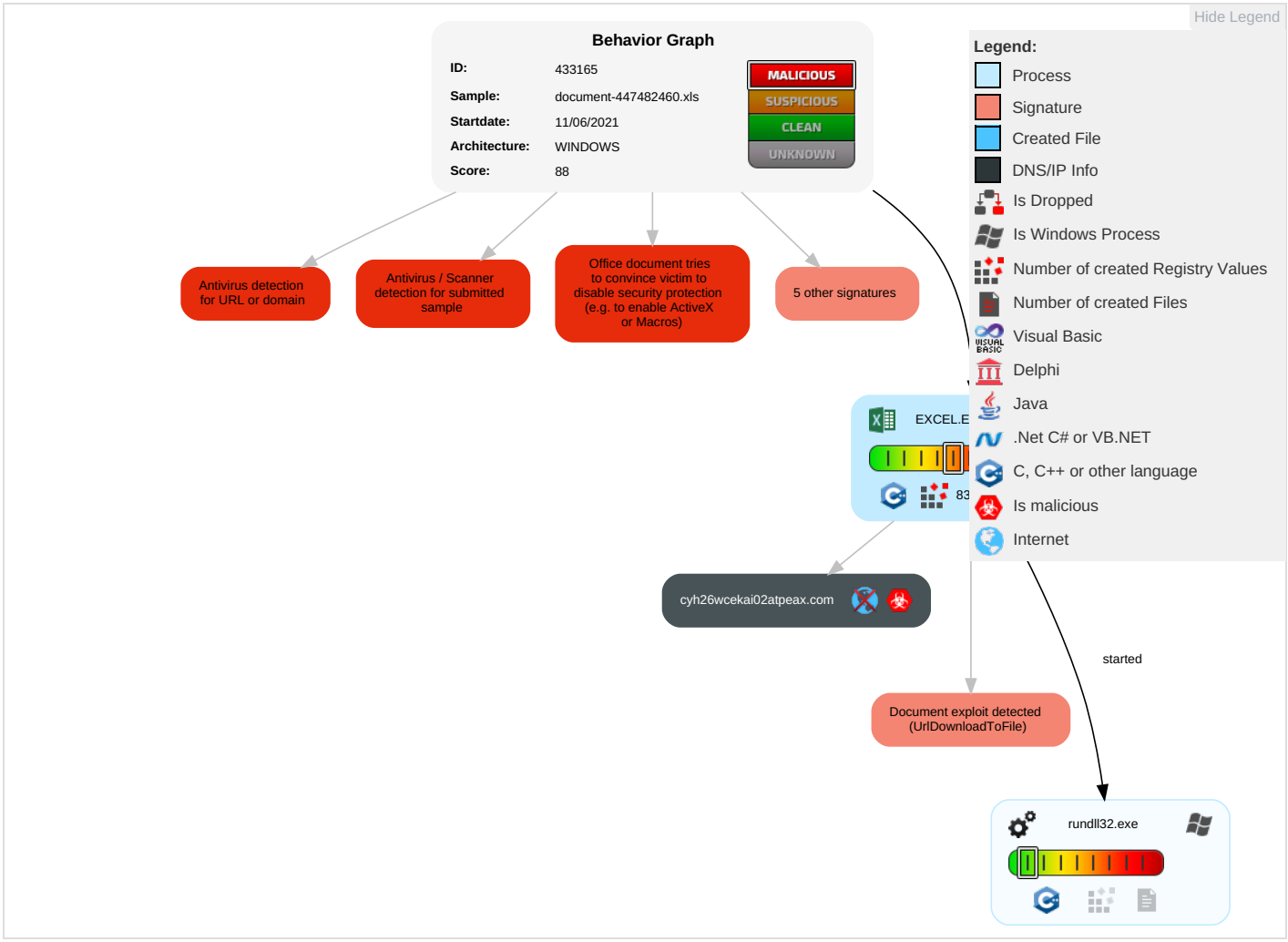
Yara detected hidden Macro 4.0 in Excel

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	I
Valid Accounts	Scripting 1 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 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S F
Default Accounts	Exploitation for Client Execution 2 1	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	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	Steganography	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 E F
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A F o

Copyright Joe Security LLC 2021

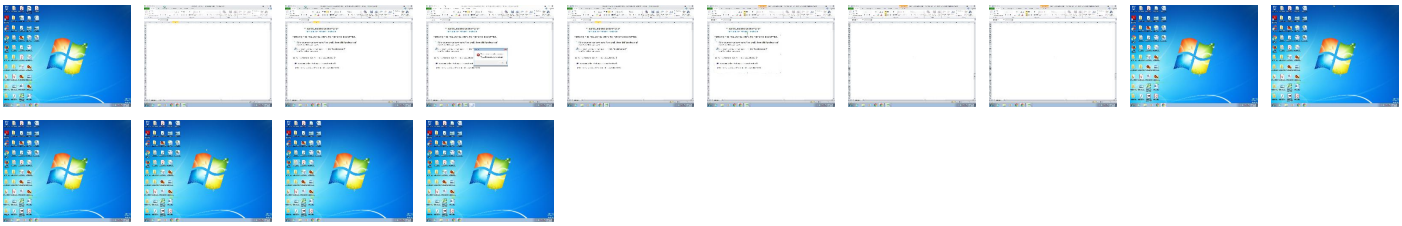
Behavior Graph

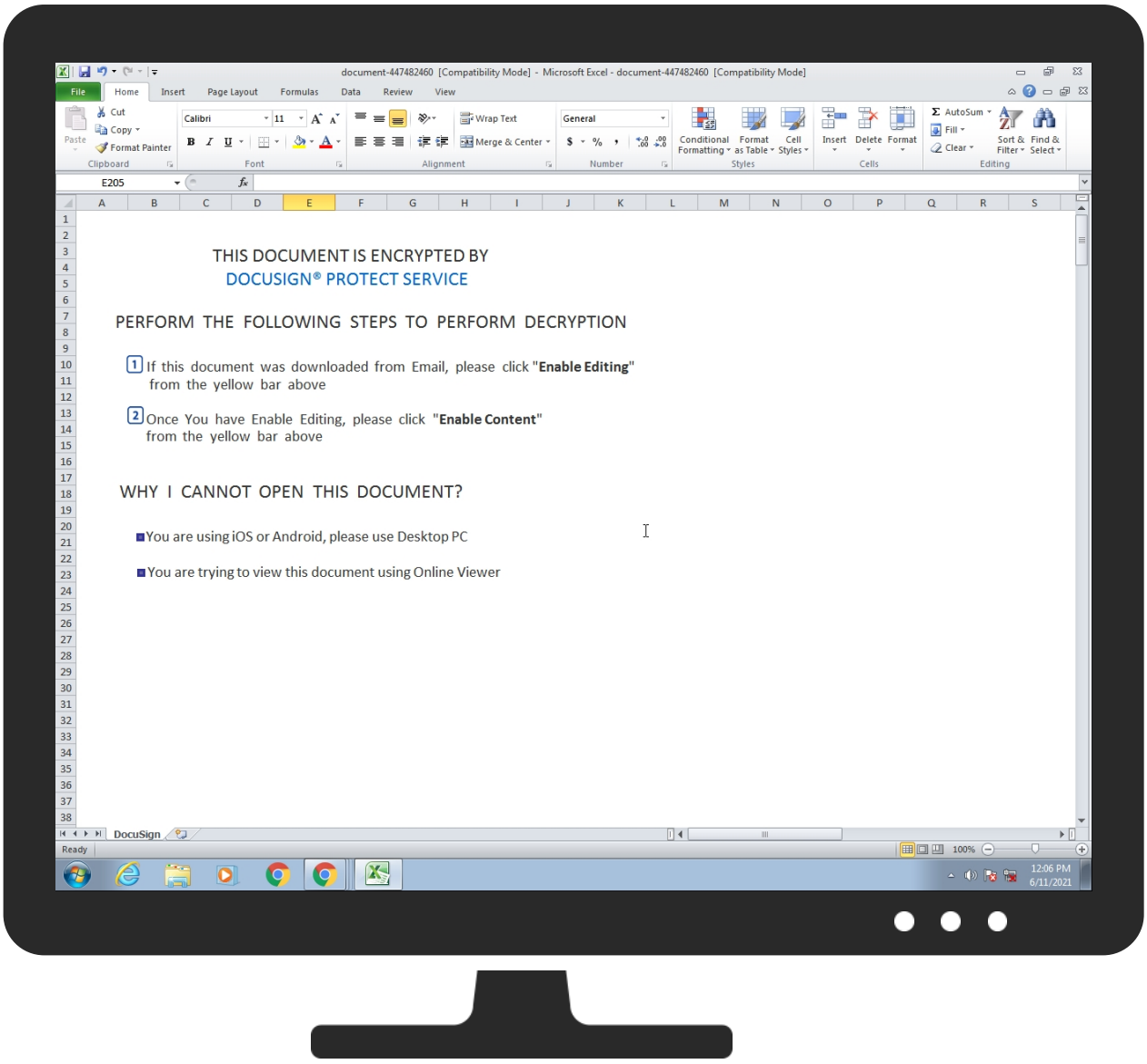


Screenshots

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
document-447482460.xls	100%	Avira	XF/Agent.B2	

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://cyh26wcekai02atpeax.com/fera/frid.gif	100%	Avira URL Cloud	malware	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cyh26wcekai02atpeax.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433165
Start date:	11.06.2021
Start time:	12:04:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-447482460.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.troj.expl.evad.winXLS@3/5@4/0
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: .xls • 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

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\050F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	62922
Entropy (8bit):	7.6710168506352945
Encrypted:	false
SSDEEP:	1536:cnHzWfiqrMMz9Sw3xNhVsSAc2frW2Z1lwASJYZ:cnTWfiqLTnjsSAc2frW2XlyS
MD5:	4473FEFA6A9F351C07873106B8C938AB
SHA1:	62F7E2A76DEE3CB5FD401E614CB4E073A02FD9AA
SHA-256:	705BC9FE56692290560E62CF1A7095F8B8BD42D71EB7CF3DA267D6B43C31AEDE
SHA-512:	69B142DFB1CAA3F8BA944E5D81CC74F018E393C5B15DD982DC1B894C76BD410DFB5AC84ABF3F3741895983F92834D6819803E77C3ABB08AE43347C14E698F8F
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C....I?.&..an.0.....#.z."..G.5.#D.....J..e.....X.I8%.w.- .Z|.4.....[...s...+.....|."..... .Zt./g..\z...:e.....x0.....:V]...R-.6..u~...n.!B0Z.D...S{.j.Zi....Kf..... Y...c.....|C3. ..D...B.c._..7.....^..p.i..VP..~.Km..O>.....$...5l$...o....8.4@kB.g.G...y..x.....n.$.x.G.=...3.63...,r..!...../..o..L..5.gN.#.R.E.u..xvg7.{...)[....>.M.Ja.uO'.....iV.F...x...<.....AL... wh...4.N..._/...m^^g.....PK.....!..%b.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Fri Jun 11 18:05:52 2021, atime=Fri Jun 11 18:05:52 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	867

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Entropy (8bit):	4.481517628504972
Encrypted:	false
SSDEEP:	12:85QbKhSLgXg/XAlCPCHaXEKB8VXB/XG44X+WnicvbTfbDtZ3YilMMEpxRljKw6Tg:85YKe/XT0K6VX34YeHDDv3q+rNru/
MD5:	EAB077F882847D1BE9A8D21F4CC94485
SHA1:	9E890ACC89741D7DD297EBB7332E94B02305993D
SHA-256:	A706417477CEB3D58BC3DDF87B86A6095A2339129786667 36CB5B9302A2B12A1
SHA-512:	CA6B9E1A2A24AF4A2DFA0163FDE76203E84DDF1F11C4EAFD14AF54881015D0F4EF680E83ECBD37BACE4CCFD4E649C967652CF53B17FDE7BA93A42E17BF966A97
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G...bX..^...bX..^...@.....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\..#.....\\377142\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.....377142.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-447482460.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 14:08:19 2020, mtime=Fri Jun 11 18:05:52 2021, atime=Fri Jun 11 18:05:52 2021, length=88576, window=hide
Category:	dropped
Size (bytes):	2108
Entropy (8bit):	4.539833983921728
Encrypted:	false
SSDEEP:	48:8b/XT0ZVXbgNMN+Qh2b/XT0ZVXbgNMN+Q/:8b/XuVXb/+Qh2b/XuVXb/+Q/
MD5:	FA5D7C43CCEBB912344C53A3B80EDAB2
SHA1:	C317B4BA1F571CE5BCA12A2FE18A8AF2B49A7687
SHA-256:	64A95B43BD8BD5FE9A9AD44F607B24AB2C468AFC4596DB88B52F3A94DB3906C1
SHA-512:	5F9DB72318FC4FAA63AA0DB6B8781299A72659031723FC7512D13CC5053E610301AD7A938C91709F0F2547695D10B00D23FBB3B81523B3391DE73DF3176D0D7E
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....\..{...bX..^...Hd..^...Z.....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.....v.2..Z...R.. .DOCUME~1.XLS..Z.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.4.4.7.4.8.2.4.6.0...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\377142\Users.user\Desktop\document-447482460.xls.-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.4.4.7.4.8.2.4.6.0...x.l.s.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....377142.....D_....3N...W..

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):	107
Entropy (8bit):	4.7041366406487235
Encrypted:	false
SSDEEP:	3:oyBVomMY9LRRdzprXCZELRRdzprXCmMY9LRRdzprXCv:dj6Y9LzdqELzdSY9Lzd6
MD5:	BB13025ED62A6FCDE7091729FEB6334B
SHA1:	FEB4612E46438B1EDD8639C21B9E329A9C73D235
SHA-256:	06FC777D7068CDEC783E8D140347BDB24CB737B00FE6195B25BE5B84A2695236
SHA-512:	3805FA3247C49298BA3B8E15A58A928B9A40E714B48C90419711222B939B1537D0547287B3E2B0EE297721CC0D1DFB2D10C11B4E9F9043693A07630863C5D6AA
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-447482460.LNK=0..document-447482460.LNK=0..[xls]..document-447482460.LNK=0..

C:\Users\user\Desktop\160F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	122124
Entropy (8bit):	4.287761039391329
Encrypted:	false
SSDEEP:	3072:ihcKoSsxzNDZLDZjlbR868O8Ku5LXkxEtjPOtioVjDGUU1qfDlaGGx+cL2QqCAH1:KcKoSsxzNDZLDZjlbR868O8Ku5LXkxEC
MD5:	AE66505CC7DCE71E82A33B53148804DE
SHA1:	B473F29DEB964E034E8E6544671ECFCEE528FD22
SHA-256:	003330A6475F686A59077FD1E9C67876CC47FFA0667BBD5272010A8097B73E69

C:\Users\user\Desktop\160F0000	
SHA-512:	47BD64CA95D72BD7052E5FAB0414D02317804EA06641FF923248324A81DCADC11C8D9B4A30ED8AA0AC20D47C6BB162ADAE6FF133211FC646204FCA159B8143 9
Malicious:	false
Reputation:	low
Preview:	........g2.....\.p.... B.....a.....=.....=.....i..9J.8.....X.@.... .....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.... .....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r .i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a .l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Fri Feb 26 09:29:22 2021, Security: 0
Entropy (8bit):	3.4145380978437365
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-447482460.xls
File size:	88576
MD5:	c956ee532ca3530d1f8ffa585e6fe375
SHA1:	f99efeea7c2ca81ffbbd59ee904ae81cf44b3493
SHA256:	8c00f69352886727d9ad19769e77bcfece11f499fb3da89dfb40396ccb06b330
SHA512:	16092ee5da7b51801fa3a002f7ef54e01376a330b4bd2bfb286f2d668402b32acf9cdc139e98193ed73d4148fb7f86e515534d0124aeb63f85162ddff72cb861
SSDEEP:	1536:tIcKoSsxz1PDZLDZjlbR868O8KWc03Y7uDphYHceXVhca+fMHLtyeGx2zZ8dIOil:tIcKoSsxzNDZLDZjlbR868O8KWc03Y7D
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-447482460.xls"

Indicators

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

Summary

Summary

Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-26 09:29:22
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

Macro 4.0 Code

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/11/21-12:05:59.991593	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
06/11/21-12:06:01.008111	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
06/11/21-12:06:03.025969	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8

Network Port Distribution

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 12:05:54.909857035 CEST	192.168.2.22	8.8.8.8	0x8c10	Standard query (0)	cyh26wceka i02atpeax.com	A (IP address)	IN (0x0001)
Jun 11, 2021 12:05:55.921636105 CEST	192.168.2.22	8.8.8.8	0x8c10	Standard query (0)	cyh26wceka i02atpeax.com	A (IP address)	IN (0x0001)
Jun 11, 2021 12:05:56.936053038 CEST	192.168.2.22	8.8.8.8	0x8c10	Standard query (0)	cyh26wceka i02atpeax.com	A (IP address)	IN (0x0001)
Jun 11, 2021 12:05:58.948674917 CEST	192.168.2.22	8.8.8.8	0x8c10	Standard query (0)	cyh26wceka i02atpeax.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 12:05:58.979480982 CEST	8.8.8.8	192.168.2.22	0x8c10	Server failure (2)	cyh26wceka i02atpeax.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 12:05:59.990859985 CEST	8.8.8.8	192.168.2.22	0x8c10	Server failure (2)	cyh26wceka i02atpeax.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 12:06:01.005148888 CEST	8.8.8.8	192.168.2.22	0x8c10	Server failure (2)	cyh26wceka i02atpeax.com	none	none	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 12:06:03.025798082 CEST	8.8.8.8	192.168.2.22	0x8c10	Server failure (2)	cyh26wceka i02atpeax.com	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2436 Parent PID: 584

General

Start time:	12:05:49
Start date:	11/06/2021
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:	0x13ff30000
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: 2580 Parent PID: 2436

General

Start time:	12:05:57
Start date:	11/06/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\nxckew.wle,DllRegisterServer
Imagebase:	0xff6a0000
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021