ID: 653502
Sample Name: purchase order.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:38:23
Date: 28/06/2022
Version: 35.0.0 Citrine

Table of Contents

Copyright Joe Security LLC 2022

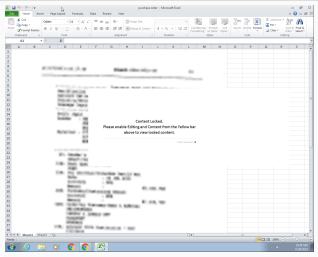
Windows Analysis Report

purchase order.xlsx

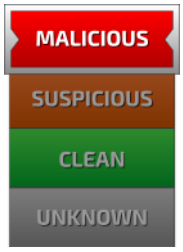
Overview

General Information

Sample Name:	purchase order.xlsx
Analysis ID:	653502
MD5:	a8930c1fcd80e9…
SHA1:	0cbf04bf7fc8522…
SHA256:	c02ff7b4d28a259..
Tags:	VelvetSweatshop xlsx
Infos:	



Detection

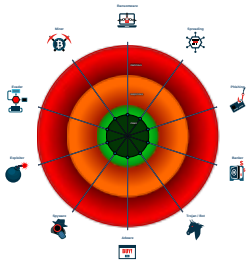


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince v…
- Multi AV Scanner detection for subm…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2664 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Copyright Joe Security LLC 2022

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

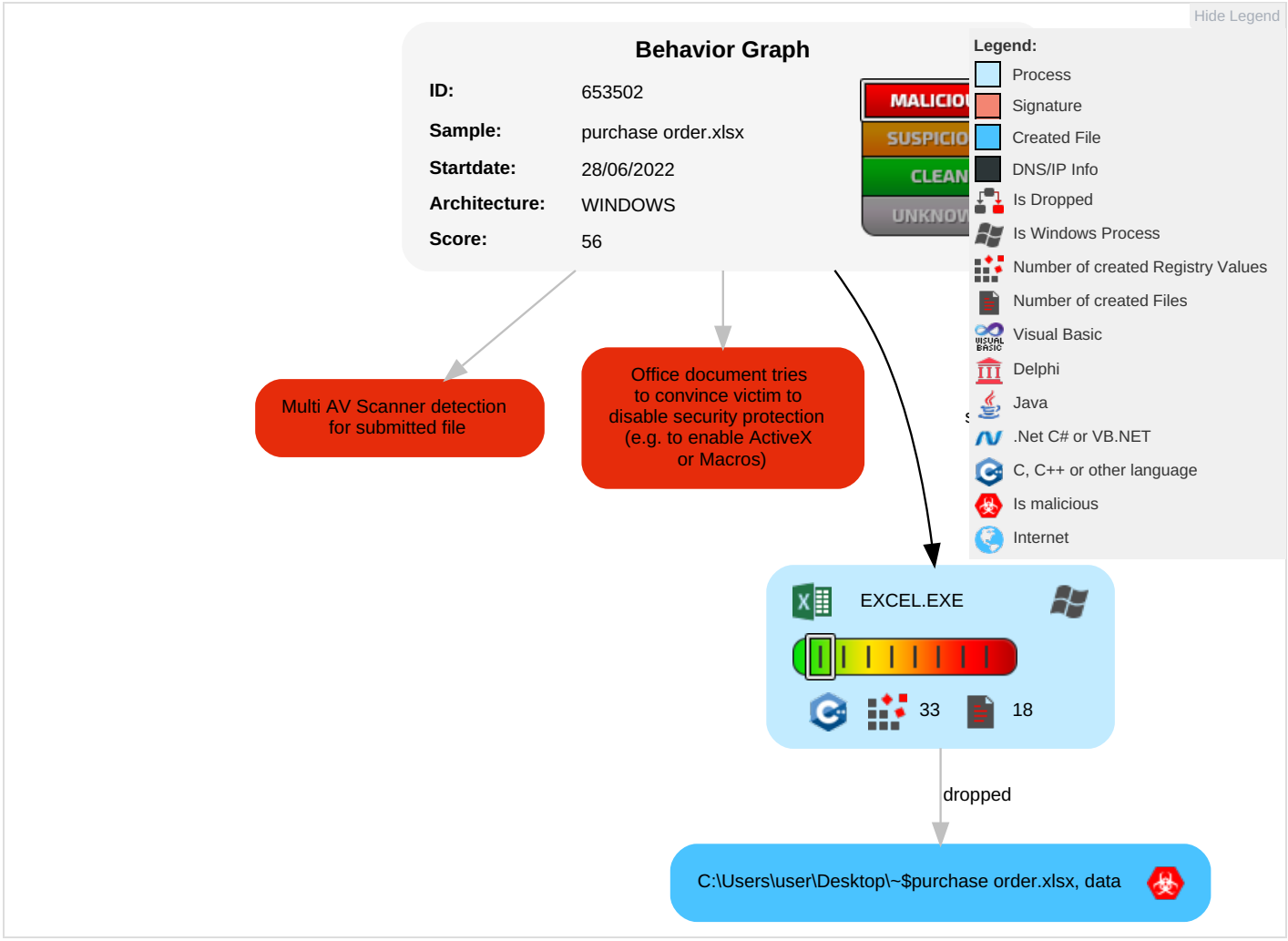
System Summary

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

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

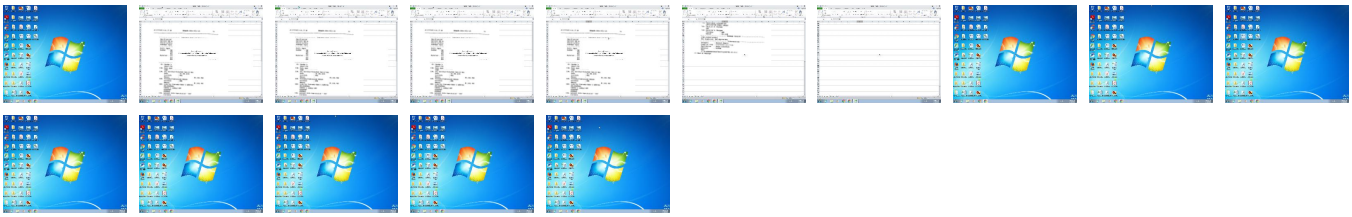
Behavior Graph

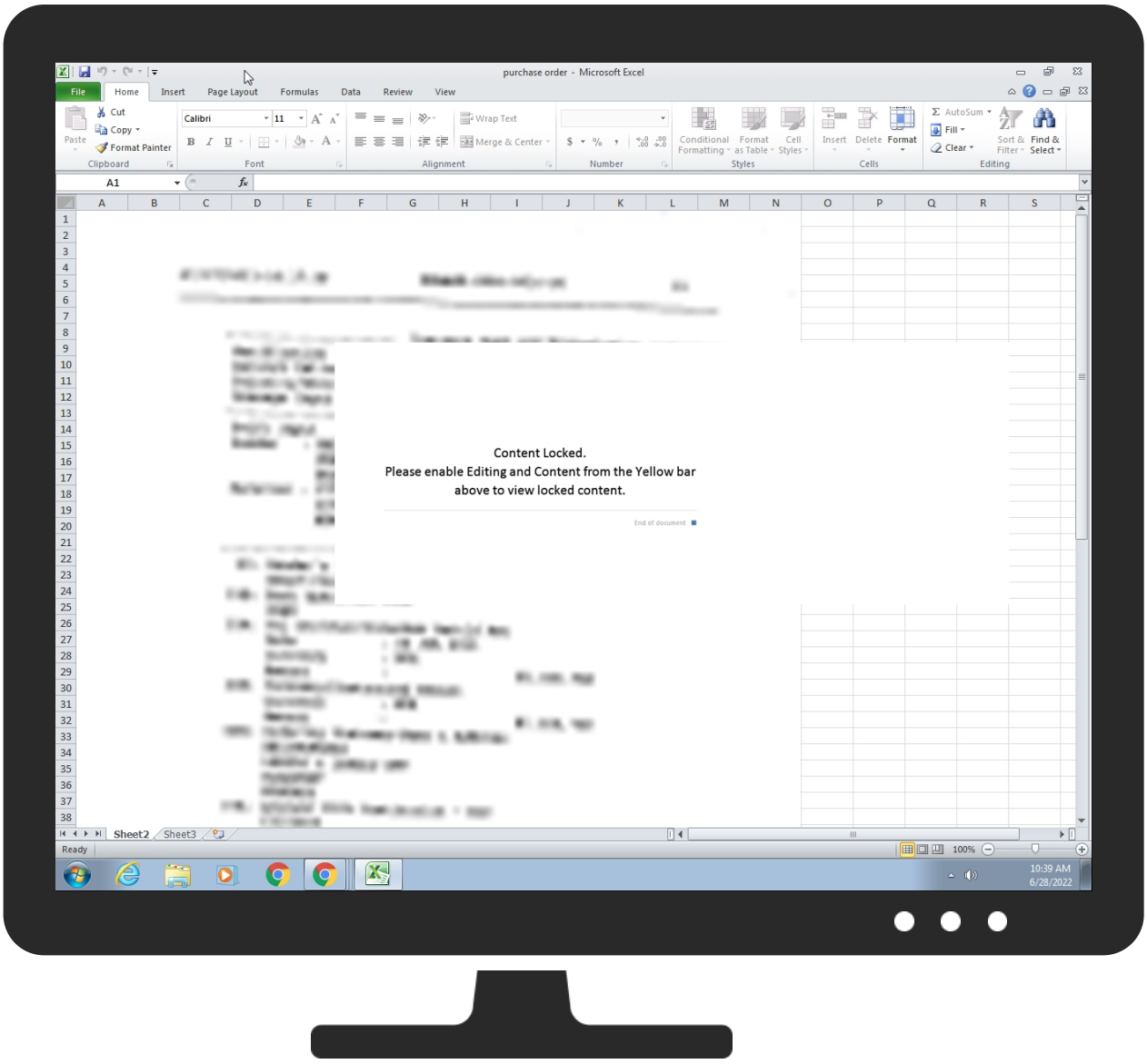


Screenshots

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
purchase order.xlsx	17%	ReversingLabs	Document-Office.Exploit.CVE-2017-0199	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	653502
Start date and time: 28/06/202210:38:23	2022-06-28 10:38:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	purchase order.xlsx
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:	2
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:	mal56.winXLSX@1/9@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xlsx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\43629BF8.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	498420
Entropy (8bit):	0.641121533751757
Encrypted:	false
SSDEEP:	384:jXXwBkNWZ3cJuUvmWnTG+W4DH8ddxzsFfW3:DXwBkNWZ3cjvmWa+VDO
MD5:	B6B2AE798B3758B49D802640BD39AF32
SHA1:	656AC44B76A94412C192609FBE730B73B238C3A9
SHA-256:	6E281E82686640834CECC8BAECB83C1AEB68114A45299115D5B590E7C51E9332
SHA-512:	375A29D725F6FD007BEE3C126165635DC89D16CAAB1FB0D5AD5AA87A1332E51EB55153D6216A954EA77E3B2DA11C35DAB2D428AAB7014B9813035964090F7D 8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....l.....2.....m>..C... EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....[$...(....f.[.@.. %.....H.....,...RQ(}.....$Q(}..... ...ld.[..... .....d.[.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....8...X.....8.[.....dv.. ....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....2.....L.....P... ...6...F....F...F..EMF+*@..$..... .....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4A9EED13.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	344
Entropy (8bit):	2.446884075910387
Encrypted:	false
SSDEEP:	6:YDRX/5OQHzqEkNslqg6lnW6kK0XgtjuYVz2tYVzfvt8J:Y1ROo6ClqgOnVp0NYVxVjw
MD5:	00022229E61960C6F67FEA5ABD7CC7BF
SHA1:	95550373818BBB679D2388324C94A949CFFF90D5
SHA-256:	CA521CE8E4A2C824905F74E45089E94D008E3E346439ECB9146AAD551C609A0F

SHA-512:	CE17174A7CD5F6063151FF025F50C2DB959421A529B45358750C6722E10FBD1E073970AD1809D03E86BF58AA9752EEA286907EF53630321D50146EA6FEBDF8F4
Malicious:	false
Reputation:	low
Preview:	....I..... EMF....X.....8...X.....?.....F...X...L...GDIC.....#s....4.....8.....8.....%.....%.....0.....K.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\527F7CC6.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 187, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	16424
Entropy (8bit):	7.9810223666914055
Encrypted:	false
SSDEEP:	384:rGO9ao+FvCVT/82OoZJh+5thcR6zPOkCpVP9o+axwZFl+v:6Olyc8cNpVlKoW
MD5:	86212DE909C5057FF80D28C6BCDA1B97
SHA1:	7B4846994D2A926D32AE44464802C8862D0D89AD
SHA-256:	B796FFD015039600D93F191B42361B22A940F84BAADA5E4E7A9BD62829458BD0
SHA-512:	DE7F37E3BF5A8E07BB5E323EA9A767CEE3856925DA332A4858C5D44A1B9635D9660BFE809BE6F6A8CCCB4EA3CD578CBE395A7B25AC30A89476353B898A585F4B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....&.....[iCCPICC Profile..x..Xy8U]._.....LNfB.."2.C..q...q...R...TR.SH"c2.HH.YI.I.....z.o.....[.u.....}.{....>|pp....H .-...v..X.1.....&.{h.....,....0.([...[o.'_l#K..\..L.;...P.C3.a..@R0.....(.m.[Sp.)....P.....0."Z[j....{.....K..w....@.J..%.@=.cu..Pwx....#.=... ....`..0/..L.u.Wa,L9.x.G@#.*p....s.Z.*.....oN....D..p..,w.....5.....nggI..-.....\..o.h.p.#....7.u.....N.%...2....H.d?..:.*..D.O.G.N.....Ff..h.r.....{QPZ.[.R.K\W...~.(..C.8..r%..g...h.....##..j.G..K4...j.....sO..^.~.....F..=&C..f3....4V.."6.m.NX.9..8.:F;.;'.Lu..z...v...Y.U...3.....x.`.D.N..G|..O...9|!b)r-.:M...#.{...Y...s...P._w..R._..M..I.../.....22.<.:..=K.:.....^..zW*G?.-/.^V~.....B."....%..>ea.....*..7V5T..T.>....$.!..3.F.&./._5?|q..U...m.eI..+.W.....G.=4=U.n}L}.....O.....Z.CG.G.G.^[.a~.7...|.a.....]?.}h.:5.....O..&f.?.}Q...../_....._...k...U-.....9.....,_..A.P).(b.y....F.R....yK;G.....v.....g...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F15EBB99.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 187, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	16424
Entropy (8bit):	7.9810223666914055
Encrypted:	false
SSDEEP:	384:rGO9ao+FvCVT/82OoZJh+5thcR6zPOkCpVP9o+axwZFl+v:6Olyc8cNpVlKoW
MD5:	86212DE909C5057FF80D28C6BCDA1B97
SHA1:	7B4846994D2A926D32AE44464802C8862D0D89AD
SHA-256:	B796FFD015039600D93F191B42361B22A940F84BAADA5E4E7A9BD62829458BD0
SHA-512:	DE7F37E3BF5A8E07BB5E323EA9A767CEE3856925DA332A4858C5D44A1B9635D9660BFE809BE6F6A8CCCB4EA3CD578CBE395A7B25AC30A89476353B898A585F4B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....&.....[iCCPICC Profile..x..Xy8U]._.....LNfB.."2.C..q...q...R...TR.SH"c2.HH.YI.I.....z.o.....[.u.....}.{....>|pp....H .-...v..X.1.....&.{h.....,....0.([...[o.'_l#K..\..L.;...P.C3.a..@R0.....(.m.[Sp.)....P.....0."Z[j....{.....K..w....@.J..%.@=.cu..Pwx....#.=... ....`..0/..L.u.Wa,L9.x.G@#.*p....s.Z.*.....oN....D..p..,w.....5.....nggI..-.....\..o.h.p.#....7.u.....N.%...2....H.d?..:.*..D.O.G.N.....Ff..h.r.....{QPZ.[.R.K\W...~.(..C.8..r%..g...h.....##..j.G..K4...j.....sO..^.~.....F..=&C..f3....4V.."6.m.NX.9..8.:F;.;'.Lu..z...v...Y.U...3.....x.`.D.N..G|..O...9|!b)r-.:M...#.{...Y...s...P._w..R._..M..I.../.....22.<.:..=K.:.....^..zW*G?.-/.^V~.....B."....%..>ea.....*..7V5T..T.>....$.!..3.F.&./._5?|q..U...m.eI..+.W.....G.=4=U.n}L}.....O.....Z.CG.G.G.^[.a~.7...|.a.....]?.}h.:5.....O..&f.?.}Q...../_....._...k...U-.....9.....,_..A.P).(b.y....F.R....yK;G.....v.....g...

C:\Users\user\AppData\Local\Temp\~DF077F770245D24E55.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	72696
Entropy (8bit):	7.868306503118196
Encrypted:	false
SSDEEP:	1536:eZfD+2fBiNR+vgt1ru46raHpu8KBZo5ujmBonFLT1J:eZyVhTWupIrocjmBoFz
MD5:	A8930C1FCD80E9965AE26446AFB717F6
SHA1:	0CBF04BF7FC8522AB983F0246357FA70A85EE56B
SHA-256:	C02FF7B4D28A259D37A659A6951DBA4EE574562EF5FC3B3A0135640C0370DEE2
SHA-512:	EAD35C97BFCCB344ED5837E82E1F648E518C52A1C6C67BD6511E018B4DC2D1364AE1F6B7DDAD69F02E58AA417402327AC3E36F175220C2C6F72FC01D4758B77F
Malicious:	false

Reputation:	low
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DF14B34C0311447876.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFEA544448D310CFF4.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFFF7070C2B802BAB2.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\Desktop\~$purchase order.xlsx

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:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.868306503118196
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	purchase order.xlsx
File size:	72696
MD5:	a8930c1fcd80e9965ae26446afb717f6
SHA1:	0cbf04bf7fc8522ab983f0246357fa70a85ee56b
SHA256:	c02ff7b4d28a259d37a659a6951dba4ee574562ef5fc3b3a0135640c0370dee2
SHA512:	ead35c97bfccb344ed5837e82e1f648e518c52a1c6c67bd6511e018b4dc2d1364ae1f6b7ddad69f02e58aa417402327ac3e36f175220c2c6f72fc01d4758b77f
SSDEEP:	1536:eZfD+2fBiNR+vgt1ru46raHpu8KBZo5ujmBonFLT1J:eZyVhTWupIrocjmBoFz
TLSH:	2C63D08237AB691BCC12093CD51142471E780F5869A8697BACC9B30F487D7CFED53AAD
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: EXCEL.EXE PID: **2664**, Parent PID: **576**

General

Target ID:	0
Start time:	10:39:16

Start date:	28/06/2022
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:	0x13fe90000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$purchase order.xlsx	0	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	user	success or wait	1	140067879	WriteFile
C:\Users\user\Desktop\~$purchase order.xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	1400678D3	WriteFile
C:\Users\user\Desktop\~$purchase order.xlsx	0	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	user	success or wait	1	140067879	WriteFile
C:\Users\user\Desktop\~$purchase order.xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	1400678D3	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E390648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	~%)	binary	7E 25 29 00 68 0A 00 00 02 00 00 00 00 00 00 00 52 00 00 00 01 00 00 00 28 00 00 00 1E 00 00 00 70 00 75 00 72 00 63 00 68 00 61 00 73 00 65 00 20 00 6F 00 72 00 64 00 65 00 72 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 75 00 72 00 63 00 68 00 61 00 73 00 65 00 20 00 6F 00 72 00 64 00 65 00 72 00 00 00	success or wait	1	6E390648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly