ID: 502625
Sample Name: Purchase Order PO5351.exe
Cookbook: default.jbs
Time: 07:26:11
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

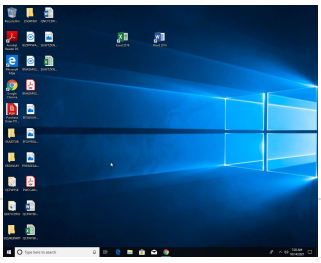
Windows Analysis Report Purchase Order PO5351.exe

Overview

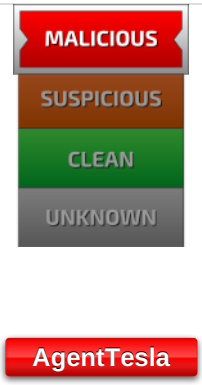
General Information

Sample Name:	Purchase Order PO5351.exe
Analysis ID:	502625
MD5:	583ae888adbd5a..
SHA1:	02fe0acb2796c2b..
SHA256:	e2ef34d6833b50a.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



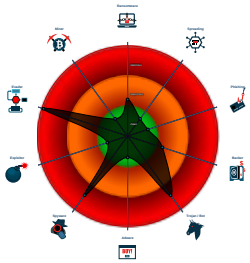
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Yara detected AgentTesla
- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Initial sample is a PE file and has a …
- Detected potential unwanted applica…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Machine Learning detection for samp…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- Purchase Order PO5351.exe (PID: 492 cmdline: 'C:\Users\user\Desktop\Purchase Order PO5351.exe' MD5: 583AE888ADBD5A79D055FBD414CC403B)
  - Purchase Order PO5351.exe (PID: 5504 cmdline: 'C:\Users\user\Desktop\Purchase Order PO5351.exe' MD5: 583AE888ADBD5A79D055FBD414CC403B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "newwork1@appalliser.com",
  "Password": "!%RvA^hkLSn&",
  "Host": "mail.appalliser.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.551186931.000000000481 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.551186931.000000000481 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000001.291805615.000000000041 4000.00000040.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000001.291805615.000000000041 4000.00000040.00020000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.550696214.000000000334 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.Purchase Order PO5351.exe.415058.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.Purchase Order PO5351.exe.415058.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.2.Purchase Order PO5351.exe.3345530.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.Purchase Order PO5351.exe.3345530.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.2.Purchase Order PO5351.exe.3345530.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 31 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Detected unpacking (creates a PE file in dynamic memory)

System Summary:

Initial sample is a PE file and has a suspicious name

Detected potential unwanted application

.NET source code contains very large array initializations

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

Malware Analysis System Evasion:

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to harvest and steal browser information (history, passwords, etc)

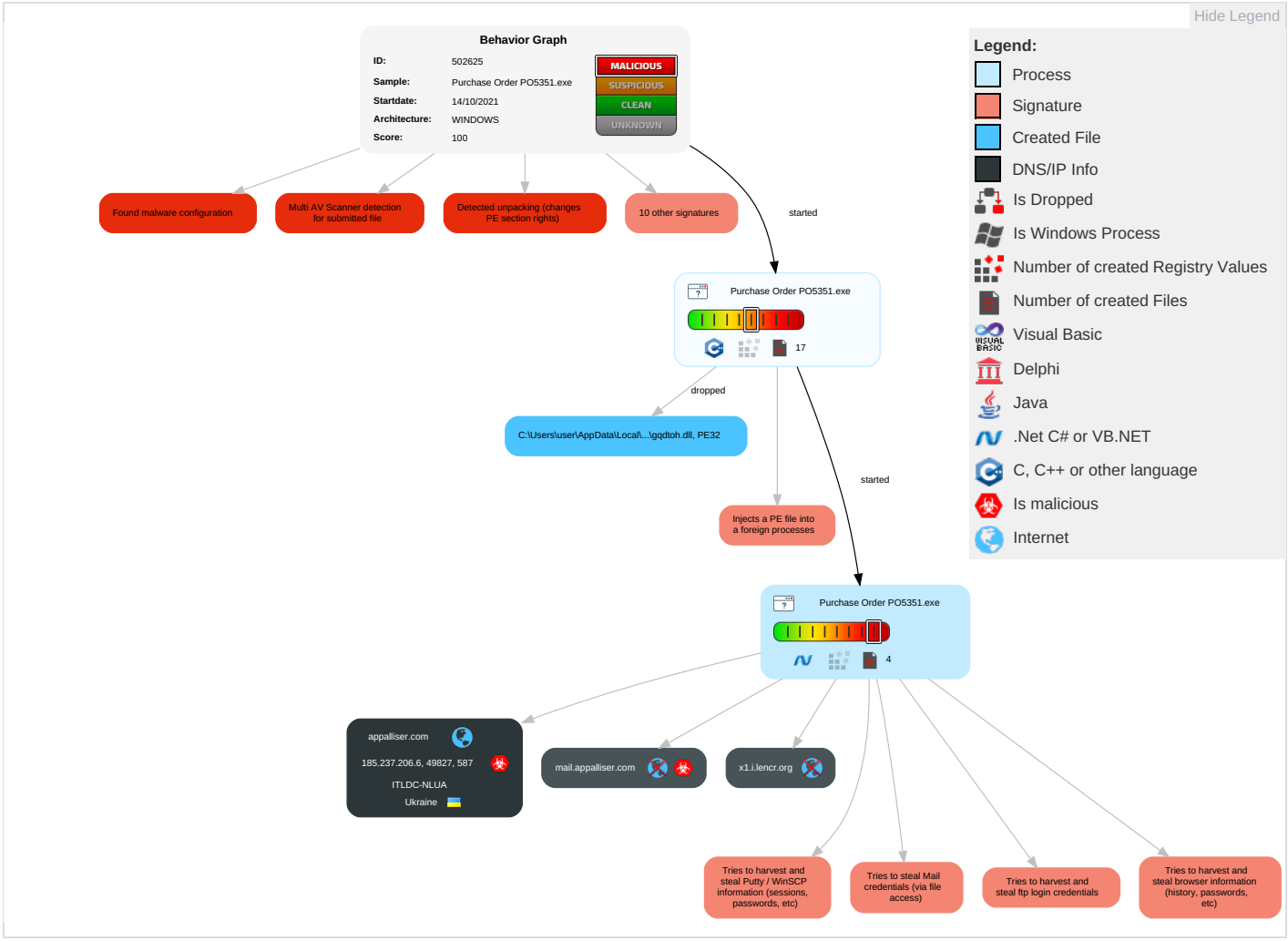
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	System Information Discovery 1 2 7	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3 1	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Virtualization/Sandbox Evasion 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

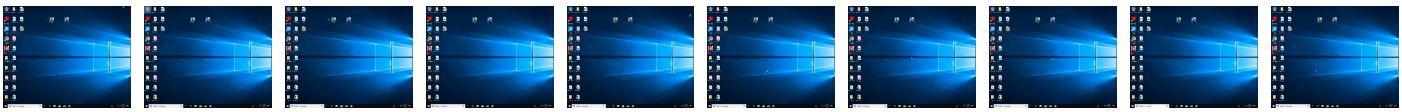
Behavior Graph



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 PO5351.exe	27%	ReversingLabs	Win32.Trojan.AgentTesla	
Purchase Order PO5351.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.Purchase Order PO5351.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.1.Purchase Order PO5351.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.Purchase Order PO5351.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.Purchase Order PO5351.exe.4810000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.Purchase Order PO5351.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.Purchase Order PO5351.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://m5KdogWJECP9WFOWfNf.org	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://crl.veris	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://JydZpq.com	0%	Avira URL Cloud	safe	
http://https://dii.lencr.org/	0%	Avira URL Cloud	safe	
http://mail.appalliser.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://appalliser.com	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
appalliser.com	185.237.206.6	true	true		unknown
x1.i.lencr.org	unknown	unknown	false		unknown
mail.appalliser.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.237.206.6	appalliser.com	Ukraine		21100	ITLDC-NLUA	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502625
Start date:	14.10.2021
Start time:	07:26:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order PO5351.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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.spyw.evad.winEXE@3/5@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.1% (good quality ratio 13.2%) • Quality average: 79.6% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 82% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:27:17	API Interceptor	817x Sleep call for process: Purchase Order PO5351.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.237.206.6	Purchase Order.exe	Get hash	malicious	Browse	
	cBPH5n4T38.exe	Get hash	malicious	Browse	
	L6F6m2L2Ll.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ITLDC-NLUA	Purchase Order.exe	Get hash	malicious	Browse	• 185.237.206.6
	cBPH5n4T38.exe	Get hash	malicious	Browse	• 185.237.206.6
	yj1ZBFihuK.exe	Get hash	malicious	Browse	• 185.51.246.132
	L6F6m2L2Ll.exe	Get hash	malicious	Browse	• 185.237.206.6
	IfNKmms6qs.exe	Get hash	malicious	Browse	• 195.123.220.96
	RSDka7Gji5	Get hash	malicious	Browse	• 5.34.180.211
	k3dBuYbiCS	Get hash	malicious	Browse	• 5.34.180.235
	88ADABCBDAF29FCCC7DA2F88D9FF0363E3315583A421D.exe	Get hash	malicious	Browse	• 91.235.129.177
	visual-studio.exe	Get hash	malicious	Browse	• 185.14.28.246
	install.apk	Get hash	malicious	Browse	• 217.12.201.177
	Downloader39.apk	Get hash	malicious	Browse	• 217.12.201.177
	Download.apk	Get hash	malicious	Browse	• 217.12.201.177
	eAjAn18mbk.exe	Get hash	malicious	Browse	• 91.235.129.250
	6x2arY3565.exe	Get hash	malicious	Browse	• 91.235.129.250
	173f5bc0bdb61d4dfcb99400b4620b6cb9ad0838836e2.exe	Get hash	malicious	Browse	• 91.235.129.250
	d9EUyMpJpx.exe	Get hash	malicious	Browse	• 91.235.129.250

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jrmUDTByys.exe	Get hash	malicious	Browse	• 91.235.129.250
	sCBiepj0Jg.exe	Get hash	malicious	Browse	• 91.235.129.112
	fXQSFpOUX2.exe	Get hash	malicious	Browse	• 195.54.162.52
	8ppXPyEzVO.exe	Get hash	malicious	Browse	• 195.54.162.52

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\2D85F72862B55C4EADD9E66E06947F3D	
Process:	C:\Users\user\Desktop\Purchase Order PO5351.exe
File Type:	data
Category:	dropped
Size (bytes):	1391
Entropy (8bit):	7.705940075877404
Encrypted:	false
SSDEEP:	24:ooVdTH2NMU+I3E0Ulcrgdaf3sWrATrnkC4EmCUkmGMkfQo1fSZotWzD1:ooVguI3Kcx8WIzNeCUkJMmSuMX1
MD5:	0CD2F9E0DA1773E9ED864DA5E370E74E
SHA1:	CABD2A79A1076A31F21D253635CB039D4329A5E8
SHA-256:	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6
SHA-512:	3B40F27E828323F5B91F8909883A78A21C86551761F27B38029FAAEC14AF5B7AA96FB9F9CC93EE201B5EB1D0FEF17B290747E8B839D2E49A8F36C5EBF3C7C910
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..k0..S.....@.YDc.c...0...*.H.....0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10...150604110438Z..350604110438Z0O1.0...U... .US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10.."0...*.H.....0.....$s..7.+W(.....8..n<.W.x.u...jn..O(..h.lD...c...k....1.!~.3<.H..y.....!.K...qiJffl.~<p. .)".....K...~....G.|.H#S.8.O.o...IW..t../.8.{.p!.u.0<.....c...O..K~.....w...{J.L.%.p..)..S$.....J.?..aQ.....cq...o[...\4ylv.;.by.../&.....6....7..6u...r.....l....*.A..v.....5/(.l....dwn G7..Y^h..r...A)>Y>.&.$...Z.L@.F.....:Qn.;.}r...xY.>Qx...../..>{J.Ks.....P.|C.t..t.....0.[q6....00\H..;..}`...).....A.....|.;F.H*..v.v..j.=...8.d..+..(.....B.".'].y...p..N..:..'Qn..d.3CO.....B0 @0...U.....0...U.....0....0...U.....y.Y.{....s.....X..n0...*.H.....U.X....P.....i ').au\.n...i/..VK..s.Y.!.~.Lq...`.9....!V..P.Y...Y.....b.E.f..|o..;....'...}~.."....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2D85F72862B55C4EADD9E66E06947F3D	
Process:	C:\Users\user\Desktop\Purchase Order PO5351.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	2.7594548283587708
Encrypted:	false
SSDEEP:	3:kkFklgbEvfllXlE/zMc/lljNNX8RolJuRdyo1dlUKlGXJlDdt:kK5ok1/l3NMa8Rdy+UKcXP
MD5:	5F3C33F91C2F962BF5FA0D280584412E
SHA1:	0BD2C8EB615D8EEC101ED6D8517D29EC53802537
SHA-256:	12B1E1A221F5D6877700117BCA8E62521A01C45FBE84523D1F39416953C789BF
SHA-512:	D7D2E13AD367FC97D47214A4C304A360840BC7886F37AF4592A18F471D47316B6486E50810F49E051B56366B3FB3B0DE3E8C65DE337C1E73E89DC69608714FB0
Malicious:	false
Reputation:	low
Preview:	p..... ....."...(..... .....~...{.....o...h.t.t.p.:.//.x.1...i...l.e.n.c.r...o.r.g./...".5.a.6.2.8.1.5.c.-.5.6.f."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\Purchase Order PO5351.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.40614825999367
Encrypted:	false
SSDEEP:	6:kKx8EMl/s8gFN+SkQlPlEGYRMY9z+4KlDA3RUeOlEfcTt:5W/Y2kPlE99SNxAhUefit
MD5:	1BBD1E1AA8D8C39ACDA50880D6710C45
SHA1:	C60321BDB330D8818735A893375F22BC438A94D8

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
SHA-256:	EE58BDDD88137D1F719E2A6C888202FBF2EABC57217C6625FB139F7293530AB4
SHA-512:	45620FCB54597857963015FBB3D0FDD46AC4E59D18E815FC98CF94D2E6711309FD06883AFD225E5707676945A8A32B27C3398F5ABD4467F03274F35E0DDCAA32
Malicious:	false
Reputation:	low
Preview:	p..... .....m.G#...(.....5..... .....^.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."0.a.a.8.a.1.5.e.a.6.d.7.1.:.0."...

C:\Users\user\AppData\Local\Temp\7qxl8ve37ylrx	
Process:	C:\Users\user\Desktop\Purchase Order PO5351.exe
File Type:	data
Category:	dropped
Size (bytes):	292863
Entropy (8bit):	7.961452658152969
Encrypted:	false
SSDEEP:	6144:LGSgzB/hb/7+23m406iCGMFEDu7JumazHCjbfO:LGdVVD+23HK/OED8cujjO
MD5:	8A370FB10ECBA8A64914D4E12B0772AF
SHA1:	C313F3E635FFA7A4A64CD4E15C0A9330D7353528
SHA-256:	AE42F2FDFC9DA6EAA2D92F2581122CA1525552E8A219BE8434D8C01838A1E368
SHA-512:	0BF128F3880B90AA60799E948CD5E6A325EA9C96464754905A9220A46A1CC16CBA1CA9A22FFD8ABB34CB529B7996D5C93EE846A0AED48545E61F88D7190EDA0F
Malicious:	false
Reputation:	low
Preview:	.[+....n.s6.Ot.....Bl..V.$I..3_.{..(S..=9.....#.....j..Y.1...~.]Q.../....{.....8...7.G.2..3<.:....DA.....c3...G.d(.}.....9...5`.,.x^\.....E..0p.....z..M...X.^u@\...$....,A8..{..< =.....j.a...T.e.jx.....J}...ju..P...l5.....nv.6.....c'.}...B...V.$..&.J...(...=9..q.....#.....q..m..Z].P7..$..\..H...3....PO.rA.I..._~..7.s...x...Ec3...G.=....{..p._f.....gw....@...}3 .....4y....O...!.#.i.A'|..>"*.^V..@...E).#.\.Pj<)S.?>.g]..l#..^.8]N`I.(....3.....[.P...l5..2....n~.6.....s....1.B...V.$I..3_.{..9.].C.....h#..W...Q...R.q.Ym..Z...7....m.H.pj....PO..r1.....~..7.s.t.....2OZ/.G.'....q..zG.f.H1..a.w.im.@...k}3..+....4yt.I.O.r...x.@.I'|..>"*.^V..@..&E).#.\....)y.?>.g]..l#..x.8.L`I.(....3.....[.P...l5.....n.s6.....s.....B...V.$I..3_.{..(S..=9.....#.....R.q.Ym..Z..P7.....\..H.....I.PO.r1.I....~..7.s.t.x...Ec3...G.=....{..zX.f.....a.w.im.@...}3 .....4y....O....P..@.A'|..>"*.^V..@...E).#.\....)y.?>.g]..l#..x.8.L`I

C:\Users\user\AppData\Local\Temp\nsk73A9.tmp\gqdtoh.dll	
Process:	C:\Users\user\Desktop\Purchase Order PO5351.exe
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	6.32837076682099
Encrypted:	false
SSDEEP:	384:RDreFw05DTFqdzQs+L5awDnZFf6KX2Y+jA4M99OvC5M8vslmSzM2g:SwgFqxw5agnT2t4WvCbvGmSzM
MD5:	5A58F937DF449DE296B78BFF64CDD730
SHA1:	A62509AA4D31DDB12A3DC881FB029D575B77484D
SHA-256:	59080307E0CFB01FE407D6F08347F540F3F0B42764B46C65C6571FF186ACE7C7
SHA-512:	BDCAFA07ACE4802845FD06BF203A4C393F211635E3A8F2B7FD2AF3DF0667318F90B7DB2563CA2838A510D72253D3B8F797D7491BA9FA1AD632D3DC274FA81D07
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D1...../2....E.....[.....[.....[.....[.....Rich.....PE..L....yga.....!.....2...*.....P.....^....@.....U..H....W.....U.....P..8.....text....0.....2..... ..`.rdata.....P.....6.....@..@.data...0...`.....D.....@....rsrc.....\.....@..B.reloc.....^.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.653315782399445
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Purchase Order PO5351.exe
File size:	364231
MD5:	583ae888adbd5a79d055fbd414cc403b

General

SHA1:	02fe0acb2796c2be544cee6cde690071e3cbfced
SHA256:	e2ef34d6833b50a6bb0c28e94c5f1f0c7454d13b41c14b5b5a8de2a84f8a8771
SHA512:	6d584518b741a225f887d8bacc621ae0461b3ada7781fdba51a2cdcd717c3869bafc9d06da88c22b3530341032676057c5747afb3be9187844bb3f2293f37060
SSDEEP:	6144:uBlL/HheqzZxjy75LlbajiuZL75W4MTHkoPq7Cp2pskLhukZAd7isYL4jtaA2oQq:suKrj4LlbajiuZ/c4M7XusgACAd7ivz2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich.QF.....PE..L...e:.V.....\.....0.....p....@

File Icon

Icon Hash:	0d19392929312d35

Static PE Info

General

Entrypoint:	0x4030fb
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x56FF3A65 [Sat Apr 2 03:20:05 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	b76363e9cb88bf9390860da8e50999d2

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert Assured ID Code Signing CA-1, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 1/13/2020 4:00:00 PM 1/20/2021 4:00:00 AM
Subject Chain	• CN=Tencent Technology(Shenzhen) Company Limited, O=Tencent Technology(Shenzhen) Company Limited, L=Shenzhen, S=Guangdong, C=CN
Version:	3
Thumbprint MD5:	0B0EC13829CB3DF95419600B93128938
Thumbprint SHA-1:	F293EED3FF3D548262CDDC43DCE58CFC7F763622
Thumbprint SHA-256:	3B72D7A1799B268BCF7BEAA29AD853A7C82E3D8F1EBAF7D3A5B0E5597ED12BA4
Serial:	01EA62E443CB2250C870FF6BB13BA98E

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5aeb	0x5c00	False	0.665123980978	data	6.42230569414	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1196	0x1200	False	0.458984375	data	5.20291736659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b038	0x600	False	0.432291666667	data	4.0475118296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0x10f20	0x11000	False	0.306310317096	data	4.93888725895	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 07:28:47.837179899 CEST	192.168.2.3	8.8.8.8	0xbd07	Standard query (0)	mail.appalliser.com	A (IP address)	IN (0x0001)
Oct 14, 2021 07:28:47.958342075 CEST	192.168.2.3	8.8.8.8	0x50fe	Standard query (0)	mail.appalliser.com	A (IP address)	IN (0x0001)
Oct 14, 2021 07:28:50.094244957 CEST	192.168.2.3	8.8.8.8	0x381e	Standard query (0)	x1.i.lencr.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 14, 2021 07:28:47.926345110 CEST	8.8.8.8	192.168.2.3	0xbd07	No error (0)	mail.appalliser.com	appalliser.com		CNAME (Canonical name)	IN (0x0001)
Oct 14, 2021 07:28:47.926345110 CEST	8.8.8.8	192.168.2.3	0xbd07	No error (0)	appalliser.com		185.237.206.6	A (IP address)	IN (0x0001)
Oct 14, 2021 07:28:47.993088007 CEST	8.8.8.8	192.168.2.3	0x50fe	No error (0)	mail.appalliser.com	appalliser.com		CNAME (Canonical name)	IN (0x0001)
Oct 14, 2021 07:28:47.993088007 CEST	8.8.8.8	192.168.2.3	0x50fe	No error (0)	appalliser.com		185.237.206.6	A (IP address)	IN (0x0001)
Oct 14, 2021 07:28:50.115859032 CEST	8.8.8.8	192.168.2.3	0x381e	No error (0)	x1.i.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Oct 14, 2021 07:28:48.190017939 CEST	587	49827	185.237.206.6	192.168.2.3	220-cp7nl.hyperhost.ua ESMTP Exim 4.94.2 #2 Thu, 14 Oct 2021 08:28:48 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Oct 14, 2021 07:28:48.190541983 CEST	49827	587	192.168.2.3	185.237.206.6	EHLO 494126
Oct 14, 2021 07:28:48.214942932 CEST	587	49827	185.237.206.6	192.168.2.3	250-cp7nl.hyperhost.ua Hello 494126 [102.129.143.33] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Oct 14, 2021 07:28:48.215382099 CEST	49827	587	192.168.2.3	185.237.206.6	STARTTLS
Oct 14, 2021 07:28:48.241825104 CEST	587	49827	185.237.206.6	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Purchase Order PO5351.exe PID: 492 Parent PID: 4760

General

Start time:	07:27:03
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\Purchase Order PO5351.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order PO5351.exe'
Imagebase:	0x400000
File size:	364231 bytes
MD5 hash:	583AE888ADBD5A79D055FBD414CC403B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.293225806.00000000023A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.293225806.00000000023A0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Purchase Order PO5351.exe PID: 5504 Parent PID: 492

General

Start time:	07:27:04
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\Purchase Order PO5351.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order PO5351.exe'
Imagebase:	0x400000
File size:	364231 bytes
MD5 hash:	583AE888ADBD5A79D055FBD414CC403B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.551186931.0000000004812000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.551186931.0000000004812000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000001.291805615.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000001.291805615.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.550696214.0000000003341000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.550696214.0000000003341000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.548389108.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.548389108.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.550919665.00000000047C0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.550919665.00000000047C0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.548716786.00000000004CB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.548716786.00000000004CB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.550115709.0000000002341000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.550115709.0000000002341000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

File Created

File Read

Disassembly

Code Analysis