ID: 483875
Sample Name: quotation...exe
Cookbook: default.jbs
Time: 15:32:58
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

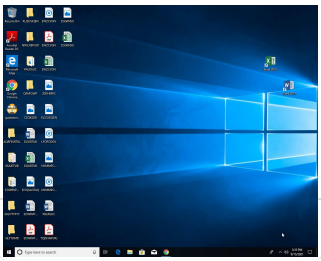
Windows Analysis Report quotation...exe

Overview

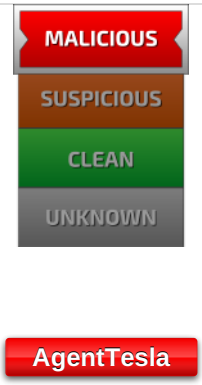
General Information

Sample Name:	quotation...exe
Analysis ID:	483875
MD5:	a0136f82865d2e8.
SHA1:	28162b2798265b..
SHA256:	6c592740621248..
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection

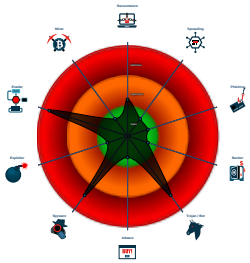


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- quotation...exe (PID: 6048 cmdline: 'C:\Users\user\Desktop\quotation...exe' MD5: A0136F82865D2E88EFA2BC913A75716C)
  - schtasks.exe (PID: 4632 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\pynXGlCh' /XML 'C:\Users\user\AppData\Local\Temp\tmp1BD9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - quotation...exe (PID: 5876 cmdline: C:\Users\user\Desktop\quotation...exe MD5: A0136F82865D2E88EFA2BC913A75716C)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "efiz@glimpse-it.co",
  "Password": "@Mexico1.,",
  "Host": "mail.privateemail.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.511804443.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.511804443.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.270468922.000000000281000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.271683451.0000000003A9B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.271683451.0000000003A9B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.quotation...exe.3909ed0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.quotation...exe.3909ed0.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.quotation...exe.3909ed0.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.quotation...exe.3909ed0.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.2.quotation...exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 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

Multi AV Scanner detection for dropped file

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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)

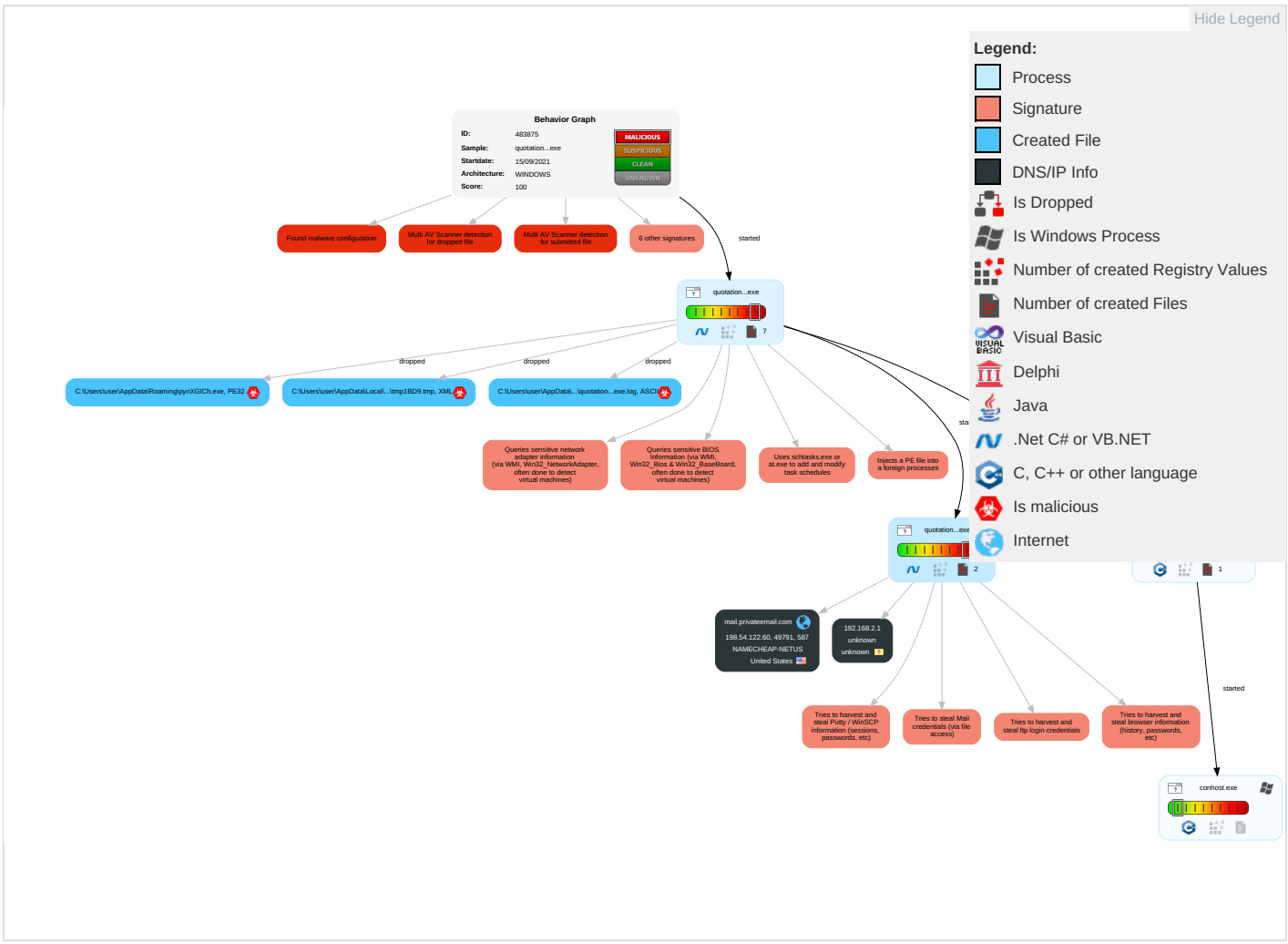
Remote Access Functionality:

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	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	System Information Discovery 1 1 4	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 2	Credentials in Registry 1	Query Registry 1	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 1 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	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	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 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	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

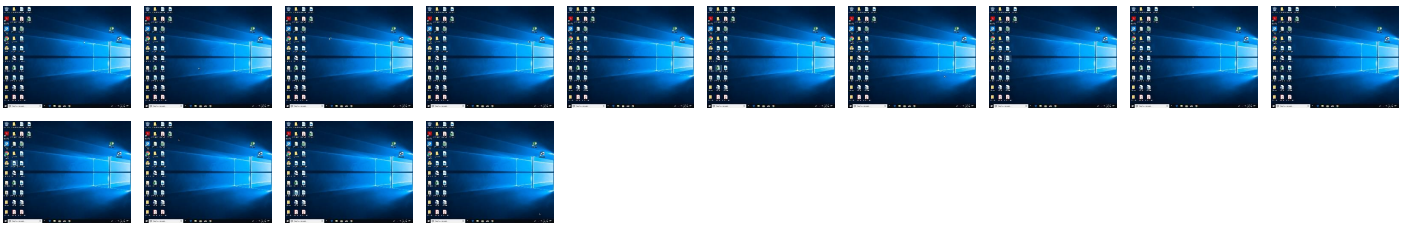
Behavior Graph



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...exe	22%	Virustotal		Browse
quotation...exe	16%	ReversingLabs	ByteCode-MSIL.Trojan.SnakeKeylogger	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\pynXGlCh.exe	22%	Virustotal		Browse
C:\Users\user\AppData\Roaming\pynXGlCh.exe	16%	ReversingLabs	ByteCode-MSIL.Trojan.SnakeKeylogger	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.quotation...exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://kk9JcHjDdoLBIcKJ.com	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	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://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	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://UDgegU.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.privateemail.com	198.54.122.60	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.122.60	mail.privateemail.com	United States		22612	NAMECHEAP-NETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483875
Start date:	15.09.2021
Start time:	15:32:58

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	quotation...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:	28
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@6/4@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.3% (good quality ratio 0.9%) • Quality average: 49.2% • Quality standard deviation: 35.4%
HCA Information:	• Successful, ratio: 86% • 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
15:34:04	API Interceptor	726x Sleep call for process: quotation...exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.122.60	SWE943211.exe	Get hash	malicious	Browse	
	P67mzce6yl.exe	Get hash	malicious	Browse	
	Gu#U00eda de carga.pdf.exe	Get hash	malicious	Browse	
	Pharmaceutical Inquiry.doc	Get hash	malicious	Browse	
	deck.exe	Get hash	malicious	Browse	
	PO0140092021.doc	Get hash	malicious	Browse	
	doc03633420210907151503.doc	Get hash	malicious	Browse	
	fytfireuiwfgdcukyd.doc	Get hash	malicious	Browse	
	quotation 21-138277.doc__.rtf	Get hash	malicious	Browse	
	Pago-20210910.pdf.exe	Get hash	malicious	Browse	
	Cotizaci#U00f3n-09092021.pdf.exe	Get hash	malicious	Browse	
	FVS_6_09_2021_WAZTAT_NAPRWAY.exe	Get hash	malicious	Browse	
	Aplieco_6635.exe	Get hash	malicious	Browse	
	O4Vj9kCSBm.exe	Get hash	malicious	Browse	
	ss_Alum_RFQ.doc	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	
	ASD.exe	Get hash	malicious	Browse	
	HEISCO_1212018.doc	Get hash	malicious	Browse	
	fnbk9UOPUc.exe	Get hash	malicious	Browse	
	Invoice2909818233.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.privateemail.com	SWE943211.exe	Get hash	malicious	Browse	• 198.54.122.60
	P67mzce6yI.exe	Get hash	malicious	Browse	• 198.54.122.60
	Gu#U00eda de carga.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	Pharmaceutical Inquiry.doc	Get hash	malicious	Browse	• 198.54.122.60
	deck.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO0140092021.doc	Get hash	malicious	Browse	• 198.54.122.60
	doc03633420210907151503.doc	Get hash	malicious	Browse	• 198.54.122.60
	fytfireuiwfgdcukyd.doc	Get hash	malicious	Browse	• 198.54.122.60
	quotation 21-138277.doc__.rtf	Get hash	malicious	Browse	• 198.54.122.60
	Pago-20210910.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	Cotizaci#U00f3n-09092021.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	FVS_6_09_2021_WAZTAT_NAPRWAY.exe	Get hash	malicious	Browse	• 198.54.122.60
	Aplieco_6635.exe	Get hash	malicious	Browse	• 198.54.122.60
	O4Vj9kCSBm.exe	Get hash	malicious	Browse	• 198.54.122.60
	ss_Alum_RFQ.doc	Get hash	malicious	Browse	• 198.54.122.60
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 198.54.122.60
	ASD.exe	Get hash	malicious	Browse	• 198.54.122.60
	HEISCO_1212018.doc	Get hash	malicious	Browse	• 198.54.122.60
	fnbk9UOPUc.exe	Get hash	malicious	Browse	• 198.54.122.60
	Invoice2909818233.xlsx	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	DlZa7n6Pjl.exe	Get hash	malicious	Browse	• 185.61.154.7
	SWE943211.exe	Get hash	malicious	Browse	• 198.54.122.60
	Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe	Get hash	malicious	Browse	• 198.54.117.215
	P67mzce6yI.exe	Get hash	malicious	Browse	• 198.54.122.60
	Gu#U00eda de carga.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	debit.xlsx	Get hash	malicious	Browse	• 198.54.117.212
	Pharmaceutical Inquiry.doc	Get hash	malicious	Browse	• 198.54.122.60
	diagram-129.doc	Get hash	malicious	Browse	• 198.54.124.27
	diagram-129.doc	Get hash	malicious	Browse	• 198.54.124.27
	diagram-129.doc	Get hash	malicious	Browse	• 198.54.124.27
	deck.exe	Get hash	malicious	Browse	• 198.54.122.60
	diagram-477.doc	Get hash	malicious	Browse	• 198.54.124.27
	diagram-477.doc	Get hash	malicious	Browse	• 198.54.124.27
	diagram-477.doc	Get hash	malicious	Browse	• 198.54.124.27
	PO0140092021.doc	Get hash	malicious	Browse	• 198.54.122.60
	I210820-0002 D1#U96a8#U6a5f-#U6d77#U95dc#U767c#U7968-R1_pdf.exe	Get hash	malicious	Browse	• 198.54.115.133
	DHL-AWD6909800855.doc	Get hash	malicious	Browse	• 104.219.248.49
	doc03633420210907151503.doc	Get hash	malicious	Browse	• 198.54.122.60
	obizx.exe	Get hash	malicious	Browse	• 104.219.248.49
	fytfireuiwfgdcukyd.doc	Get hash	malicious	Browse	• 198.54.122.60

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\quotation...exe.log	
Process:	C:\Users\user\Desktop\quotation...exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp1BD9.tmp	
Process:	C:\Users\user\Desktop\quotation...exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.17073201951906
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB6tn:cbhC7ZlNQF/rydbz9I3YODOLNdq3W
MD5:	0C2462882F57DA016996EB425672CC4D
SHA1:	677786D1A49CECEFCFE8DAEBFADD0C162D5B7136
SHA-256:	A4DFB7CB88741BDB8B1C31E31AD12B55123EC7AA82A59758FC487C792B7172E4
SHA-512:	031C1117D44A05CB188D13449EADA7DC437B838320BAEE9683D47F8B521A175E7E18BE1907F251B87486136EFDFC49094B33BB552244A0FE7207711B0AF94318
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\pynXGlCh.exe	
Process:	C:\Users\user\Desktop\quotation...exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	699392
Entropy (8bit):	7.458068889779674
Encrypted:	false
SSDEEP:	12288:nYWHCM2K4CXI/yzQs2TaIpI+QRa8t0DCUw6FYB1pja+IA1fhjgzwq5Ysl:nA3CMMIpI+QH+DkKeTTzjgZI
MD5:	A0136F82865D2E88EFA2BC913A75716C
SHA1:	28162B2798265B1406F3C08BFF44F9B0EA50D6C4
SHA-256:	6C5927406212482DF7AD0B2B13010541E7377AE5D392A9CC531D942872DCB22F
SHA-512:	E001D588BDDA99FA742ECB086D26A49444B08D0D429440A0489A6284CED847CA28CE38B6AFDAF474CD212A0B5218C6767B81B3105050A661A6C15CD6BACF263
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 22%, Browse • Antivirus: ReversingLabs, Detection: 16%
Reputation:	low

C:\Users\user\AppData\Roaming\pynXGlCh.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.Aa.....0..<...n.....[... ...`....@.. ..... ..@.....T[..O....`...k..... ....H.....text....;... ...<..... ..`.rsrc....k...`...l...>.....@..@.rel oc.....@..B.....[.....H.....\.....Q...\+.../.....0.....}.....(.....(.....r...p.(....(....o.....{.....(....o.....{....r...p.(....(....o.....{.....(....o.. ....{.....(....o.....{.....(....o....*...0..._.....(.....(.....o.....),....t.....o....r-..p(.....,..o.....+..(....o....(.....+...*..0.....(....o....o ...o!....+..*...0..:.....(.....(.....o.....,r-..p. +....t....o"....+..*...0..:.....(.....(....

C:\Users\user\AppData\Roaming\pynXGlCh.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\quotation...exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.458068889779674
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	quotation...exe
File size:	699392
MD5:	a0136f82865d2e88efa2bc913a75716c
SHA1:	28162b2798265b1406f3c08bff44f9b0ea50d6c4
SHA256:	6c5927406212482df7ad0b2b13010541e7377ae5d392a9cc531d942872dcb22f
SHA512:	e001d588bdda99fa742ecb086d26a49444b08d0d429440a0489a6284ced847ca28ce38b6afdaf474cd212a0b5218c6767b81b3105050a661a6c15cd6bacf26b3
SSDEEP:	12288:nYWHCM2K4CXI/yzQs2TaIpI+QRa8t0DCUw6FYB1pja+IA1fhjgzwq5YsI:nA3CMMIpI+QH+DkKeTTzjgZI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.Aa.....0..<...n.....[... ...`....@.. .....@.....

File Icon

Icon Hash:	f1f0f4d0eecccc71

Static PE Info

General

Entrypoint:	0x4a5ba6
Entrypoint Section:	.text
Digitally signed:	false

General

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61419C27 [Wed Sep 15 07:09:27 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa3bac	0xa3c00	False	0.822355081107	data	7.5296902445	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa6000	0x6b80	0x6c00	False	0.44263599537	data	5.09104510472	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 15:35:54.098917961 CEST	192.168.2.5	8.8.8.8	0x20d9	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 15:35:54.129602909 CEST	8.8.8.8	192.168.2.5	0x20d9	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Sep 15, 2021 15:35:55.347913980 CEST	587	49791	198.54.122.60	192.168.2.5	220 PrivateEmail.com prod Mail Node
Sep 15, 2021 15:35:55.348258018 CEST	49791	587	192.168.2.5	198.54.122.60	EHLO 128757
Sep 15, 2021 15:35:55.520095110 CEST	587	49791	198.54.122.60	192.168.2.5	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Sep 15, 2021 15:35:55.520447969 CEST	49791	587	192.168.2.5	198.54.122.60	STARTTLS
Sep 15, 2021 15:35:55.692142963 CEST	587	49791	198.54.122.60	192.168.2.5	220 Ready to start TLS

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: quotation...exe PID: 6048 Parent PID: 6008

General

Start time:	15:33:55
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\quotation...exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\quotation...exe'
Imagebase:	0x300000
File size:	699392 bytes
MD5 hash:	A0136F82865D2E88EFA2BC913A75716C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.270468922.0000000002841000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.271683451.0000000003A9B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.271683451.0000000003A9B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.271066231.0000000003849000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.271066231.0000000003849000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 4632 Parent PID: 6048

General

Start time:	15:34:07
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\pynXGlCh' /XML 'C:\Users\user\AppData\Local\Temp\tmp1BD9.tmp'
Imagebase:	0x10f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: conhost.exe PID: 5988 Parent PID: 4632

General

Start time:	15:34:07
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: quotation...exe PID: 5876 Parent PID: 6048

General

Start time:	15:34:07
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\quotation...exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\quotation...exe
Imagebase:	0x7ff797770000
File size:	699392 bytes
MD5 hash:	A0136F82865D2E88EFA2BC913A75716C

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: 00000008.00000002.511804443.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.511804443.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.517481719.0000000003111000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.517481719.0000000003111000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis