ID: 433217
Sample Name: Quote-TSL-1037174_4810.exe
Cookbook: default.jbs
Time: 13:18:18
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

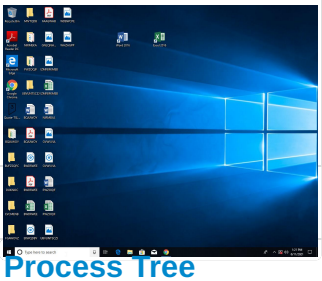
Analysis Report Quote-TSL-1037174_4810.exe

Overview

General Information

Sample Name:	Quote-TSL-1037174_4810.exe
Analysis ID:	433217
MD5:	deb5412f0b0201d.
SHA1:	4086c81e9c51db..
SHA256:	c770d9d870614a..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

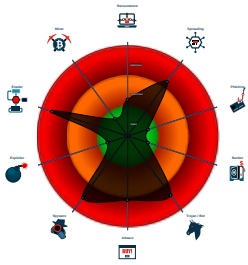
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: MSBuild connects …
- Yara detected AgentTesla
- Yara detected AgentTesla
- .NET source code contains very larg…
- .NET source code references suspic…
- Creates multiple autostart registry ke…
- Hides that the sample has been dow…
- Installs a global keyboard hook
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- Quote-TSL-1037174_4810.exe (PID: 7032 cmdline: 'C:\Users\user\Desktop\Quote-TSL-1037174_4810.exe' MD5: DEB5412F0B0201D045E2007503BBB283)
  - MSBuild.exe (PID: 7088 cmdline: 'C:\Users\user\Desktop\Quote-TSL-1037174_4810.exe' MD5: D621FD77BD585874F9686D3A76462EF1)
- amve.exe (PID: 5912 cmdline: 'C:\Users\user\AppData\Roaming\bnqw\amve.exe' MD5: DEB5412F0B0201D045E2007503BBB283)
  - MSBuild.exe (PID: 6372 cmdline: 'C:\Users\user\AppData\Roaming\bnqw\amve.exe' MD5: D621FD77BD585874F9686D3A76462EF1)
- amve.exe (PID: 6740 cmdline: 'C:\Users\user\AppData\Roaming\bnqw\amve.exe' MD5: DEB5412F0B0201D045E2007503BBB283)
  - MSBuild.exe (PID: 6292 cmdline: 'C:\Users\user\AppData\Roaming\bnqw\amve.exe' MD5: D621FD77BD585874F9686D3A76462EF1)
- NewApp.exe (PID: 2480 cmdline: 'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe' MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 1320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- NewApp.exe (PID: 4088 cmdline: 'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe' MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 2864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "accounts@buynsell.com.pkTZaQ}N$m+6$vmail.buynsell.com.pkmaria@tradzilanilaw.co.za"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.685992308.000000000005C2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.685992308.000000000005C2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.686576879.000000000983000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.686576879.000000000983 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000002.904595118.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.amve.exe.9970000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.amve.exe.9970000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Quote-TSL-1037174_4810.exe.9b10000.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Sigma Overview

Networking:

Sigma detected: MSBuild connects to smtp port

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Boot Survival:

Creates multiple autostart registry keys

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

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

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Maps a DLL or memory area into another process

Modifies the hosts file

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

Yara detected AgentTesla

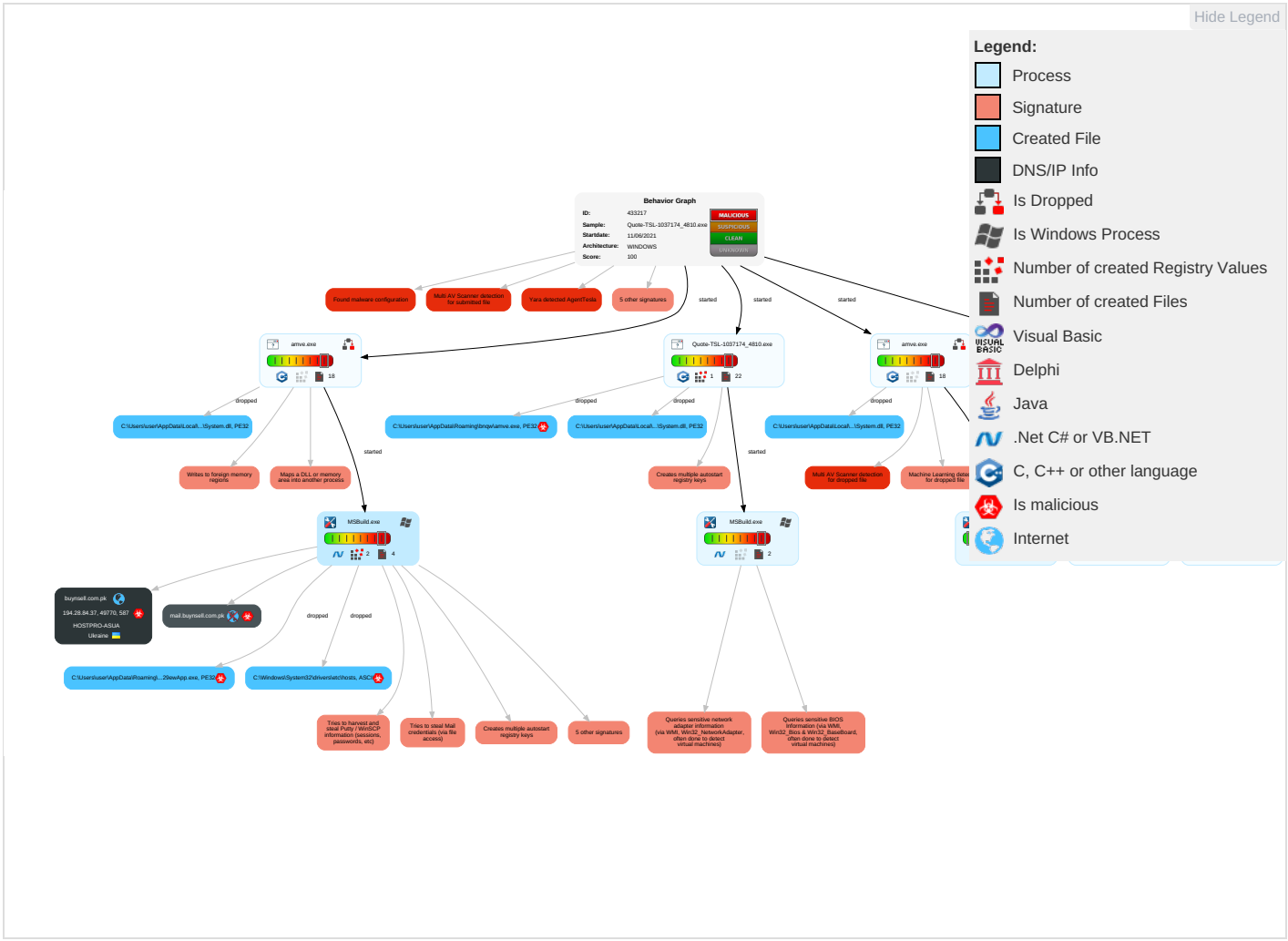
Yara detected AgentTesla

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	Scheduled Task/Job 1	Process Injection 2 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1 1	Registry Run Keys / Startup Folder 1 1	Scheduled Task/Job 1	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 6	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Security Software Discovery 2 2 1	SSH	Clipboard Data 2	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 4 1	DCSync	Virtualization/Sandbox Evasion 1 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 2	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)	Hidden Files and Directories 1	/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/Obfuscate Non-C2 Protocol

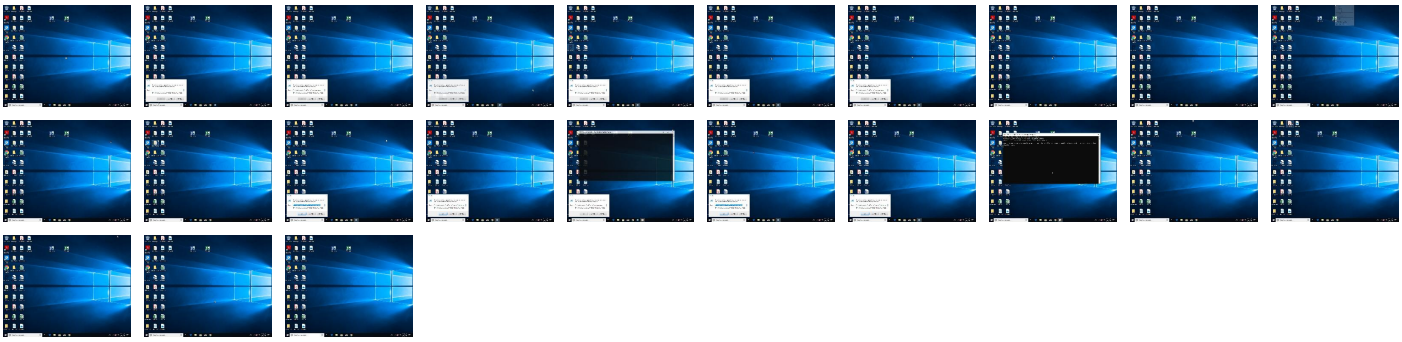
Behavior Graph



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
Quote-TSL-1037174_4810.exe	14%	Metadefender		Browse
Quote-TSL-1037174_4810.exe	59%	ReversingLabs	Win32.Backdoor.Androm	
Quote-TSL-1037174_4810.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\bnqw\amve.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsg8314.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsg8314.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsk5B48.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsk5B48.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nstA2D1.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nstA2D1.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\bnqw\amve.exe	14%	Metadefender		Browse
C:\Users\user\AppData\Roaming\bnqw\amve.exe	59%	ReversingLabs	Win32.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.amve.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
1.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.Quote-TSL-1037174_4810.exe.9950000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.0.amve.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
3.2.amve.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
0.0.Quote-TSL-1037174_4810.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
6.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.amve.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
4.2.MSBuild.exe.5c0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
0.2.Quote-TSL-1037174_4810.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		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://mail.buynsell.com.pk	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://IsXVMb.com	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	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://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://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.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://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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://JMZ6qWBlYHv2.net	0%	Avira URL Cloud	safe	
http://buynsell.com.pk	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0E	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
buynsell.com.pk	194.28.84.37	true	true		unknown
mail.buynsell.com.pk	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.28.84.37	buynsell.com.pk	Ukraine		196645	HOSTPRO-ASUA	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433217
Start date:	11.06.2021
Start time:	13:18:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quote-TSL-1037174_4810.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:	22
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.spre.troj.adwa.spyw.evad.winEXE@13/18@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.9% (good quality ratio 32.8%) • Quality average: 81.5% • Quality standard deviation: 27%
HCA Information:	• Successful, ratio: 90% • 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
13:19:03	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run xmalmtehdauows C:\Users\user\AppData\Roaming\bnqw\amve.exe
13:19:11	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run xmalmtehdauows C:\Users\user\AppData\Roaming\bnqw\amve.exe
13:19:12	API Interceptor	2x Sleep call for process: amve.exe modified
13:19:14	API Interceptor	658x Sleep call for process: MSBuild.exe modified
13:19:49	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run NewApp C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
13:19:57	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
194.28.84.37	DENSCO QUOTE.exe	Get hash	malicious	Browse	
	MESCO TQZ24 QUOTE.exe	Get hash	malicious	Browse	
	TQZ23 DESCO MC.exe	Get hash	malicious	Browse	
	TQZ23 DESCO MC.exe	Get hash	malicious	Browse	
	DENSCO QUOTE.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
HOSTPRO-ASUA	DENSCO QUOTE.exe	Get hash	malicious	Browse	• 194.28.84.37
	MESCO TQZ24 QUOTE.exe	Get hash	malicious	Browse	• 194.28.84.37
	TQZ23 DESCO MC.exe	Get hash	malicious	Browse	• 194.28.84.37
	TQZ23 DESCO MC.exe	Get hash	malicious	Browse	• 194.28.84.37
	DENSCO QUOTE.exe	Get hash	malicious	Browse	• 194.28.84.37
	4Vy2EGhzNF.exe	Get hash	malicious	Browse	• 193.169.188.252
	2020tb3005.doc__.rtf	Get hash	malicious	Browse	• 193.169.188.252
	$RAULIU9.exe	Get hash	malicious	Browse	• 91.239.233.22
	OUTSTANDING_INV_Statement_937931.xls	Get hash	malicious	Browse	• 185.67.1.94
	866-0001E ORDER AND SHIP.doc	Get hash	malicious	Browse	• 193.169.188.252
	866-0001E ORDER AND SHIP.doc	Get hash	malicious	Browse	• 193.169.188.252
	new order list.doc	Get hash	malicious	Browse	• 193.169.188.252
	nX5xMoS3Pn.exe	Get hash	malicious	Browse	• 193.169.188.252
	tryb.doc	Get hash	malicious	Browse	• 193.169.188.252
	Order Specification.exe	Get hash	malicious	Browse	• 185.156.42.252
	rib.exe	Get hash	malicious	Browse	• 91.239.233.22
	http://https://ngor.zlen.com.ua/Restore/Click here to restore message automatically.html	Get hash	malicious	Browse	• 91.239.235.5
	ETD 15-09-2020 (MV.HYUNDAI SUPREME V. 102N_PDF.exe	Get hash	malicious	Browse	• 91.239.235.6
	DHL_Receipt_pdf.exe	Get hash	malicious	Browse	• 91.239.235.6
	ETD 15-09-2020 (MV.HYUNDAI SUPREME V. 102N_PDF.gz.exe	Get hash	malicious	Browse	• 91.239.235.6

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsg8314.tmp\System.dll	SX365783909782021.exe	Get hash	malicious	Browse	
	moq fob order.exe	Get hash	malicious	Browse	
	0900000000000090000.exe	Get hash	malicious	Browse	
	444890321.exe	Get hash	malicious	Browse	
	Packing-List_00930039.exe	Get hash	malicious	Browse	
	2435.exe	Get hash	malicious	Browse	
	INVOICE.exe	Get hash	malicious	Browse	
	Shipment Invoice & Consignment Notification.exe	Get hash	malicious	Browse	
	KY4cmAI0jU.exe	Get hash	malicious	Browse	
	5t2CmTUhKc.exe	Get hash	malicious	Browse	
	8qdfmqz1PN.exe	Get hash	malicious	Browse	
	New Order PO2193570O1.doc	Get hash	malicious	Browse	
	L2.xlsx	Get hash	malicious	Browse	
	Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	
	New Order PO2193570O1.pdf.exe	Get hash	malicious	Browse	
	2320900000000.exe	Get hash	malicious	Browse	
	CshpH9OSkc.exe	Get hash	malicious	Browse	
	5SXTKXCnqS.exe	Get hash	malicious	Browse	
	i6xFULh8J5.exe	Get hash	malicious	Browse	
	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NewApp.exe.log	
Process:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	841
Entropy (8bit):	5.356220854328477
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoIvEE4xDqE4j:MxHKXwYHKhQnoPtHoxHwvEHxDqHj
MD5:	486580834B084C92AE1F3866166C9C34
SHA1:	C8EB7E1CEF55A6C9EB931487E9AA4A2098AACEDF
SHA-256:	65C5B1213E371D449E2A239557A5F250FEA1D3473A1B5C4C5FF7492085F663FB
SHA-512:	2C54B638A52AA87F47CAB50859EFF98F07DA02993A596686B5617BA99E73ABFCD104F0F33209E24AFB32E66B4B8A225D4DB2CC79631540C21E7E8C4573DFD45
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..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..2,"Microsoft.Build.Framework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\5pa4r9ixzaf	
Process:	C:\Users\user\AppData\Roaming\bnqw\amve.exe
File Type:	data
Category:	dropped
Size (bytes):	222208
Entropy (8bit):	**7.999115710953568**
Encrypted:	**true**
SSDEEP:	3072:vaBXEtCG5OYajI1w+Z/rT/uh0uZn1k79bG3E6I4Wwu31L676SM98/1ORmcILLQE7:vsmVGCz9uZn6Z6I4YY8mrPLlQGz
MD5:	C64EDB818138FCBAD02DA4F40AFB504E
SHA1:	E312998ABA653E46AA64AD17EC06B23C123C363A
SHA-256:	10F9B7D302BECDA98408F7A361A7F8DE8ECF2149876D7B2D14C08FD62B7FADB5

C:\Users\user\AppData\Local\Temp\5pa4r9ixzaf	
SHA-512:	F49E83E1DA717D275C85455C797579560F33D1570410BDBD418866F5F6FA8C9C82A6309FE8E06789ABB50F837E5DD4E013205A0FDFA49C57066CE043A8CF0B3
Malicious:	false
Reputation:	low
Preview:	.r.....F...<.&.tt.D.D1=.9....gL.4.....@6..@.B.M..U2=...I....Zh.a..;p..?...T=0./J..B.o..W2...T.....j../7..y...o..s.`....V.pnd...C|....dd.....+0..T.....x...'.....G*.V+.w.`.....,5.G}#..".I..M.".X)..e...Z.I...m.c....O@.d@.....z".|.Kw>....qb??...Qg.D...3../..Abj.@..7p...6_.....|.{..R./...z....G.#.k.O..f.G.L.P.g.n.....9T1.w.kKFM.f....QWI..vfG...d..c.....y...tS..R53=.X..h....$f.....>.p....c.C.d.yx~.q...J..U.`...H[..UU(..r]...u...c.kG.+C.TTq."...._.<.ZD:..Xl.f%.>.b.r..P..4.... .{.b.>.../.....0..t-....$...E.'$^...T"B}<..c...52.%...M.3O..r.....q.....Q..c..<..M..C..OH.....g....;Q.Dd.]}...+d(.Z.L..k..4<.\|.52.F*.n'\..`}.O..6.....:$..@dG..>..g.4..Q... .....K3b\..P...0.c.u;u\'D..Y|.U.l"..Z..S.@.,.Xp...SCp{.....J..SFz..Tp..<..O.".4.R..lf....b'%S.+...I..n.C..$...q..CZ7....Lb%.+.`M....3\.....[..rGv..n...V.an...h[..U.%.a<.TZ.C..xd..e(.....;....C..%*...df7.P...B. j...MB..%}...kZ....V....F,.TF..Sy.7l.....x..KD..GX.yL.$

C:\Users\user\AppData\Local\Temp\fygibjohzelpmv	
Process:	C:\Users\user\AppData\Roaming\bnqw\amve.exe
File Type:	data
Category:	dropped
Size (bytes):	62417
Entropy (8bit):	4.988447505730978
Encrypted:	false
SSDEEP:	1536:INzvOIagVy6DOiz8TlJbvuPt0P63/dXT5KJC2GaNjpmSRGT:INzv3zRDiJCWCvJuC7KjU
MD5:	D966D7333A785DDFF7B56A403AB8388B
SHA1:	130361814DC909C9036E9554B90381265EF37CA7
SHA-256:	32CD0E78D96E6CBF2962685077C0287F5301B5BD788F2F4F4ADAFFF0A05B757E
SHA-512:	B4369E11DC82B7694A7C3941492145EDDA05CCBB52E766D1B0D2FB66BA46C76FACAAEDB4E15121592C8BC51068F79067D34E53073C044DCEC7A006461FD103F
Malicious:	false
Reputation:	low
Preview:	U..."....q....;.....y.....q....;.....3....a....(. ....!...."...s.#...$.$...n.%...5.&....'.....(.....)....*....+.....,.....-...$.....n./...5.0.....1.....2.....3.....4.....5.....6...h.7...$.8...n.9...5.:.....;.....<.....=.....>.....?.....@...'.A...$.B...n.C...5.D.....E.....F.....G.....H.....I.....J.....K...$.L...n.M...5.N.....O...P.P.....Q.....R...S.....T.....U...$.V...n.W...5.X.....Y.....Z.....[.....\.....]....^.....`...n.a...5.b.....c...T.d.....e.....f.....g.....h.....i...$.j...n.k...5.l.....m...R.n.....o.....p.....q.....r...G.s...$.t...n.u...5.v.....w...X.x.....y.....z.....{.....\|...C.}...$.~...n.....5.....V.....h.....$.....n.....5.....\.....I.....$.....n.....5.....

C:\Users\user\AppData\Local\Temp\nsg8313.tmp	
Process:	C:\Users\user\AppData\Roaming\bnqw\amve.exe
File Type:	data
Category:	dropped
Size (bytes):	317921
Entropy (8bit):	7.545162398623952
Encrypted:	false
SSDEEP:	6144:UXAsmVGCz9uZn6Z6I4YY8mrPLlQGcNzvthxuYKbt:XsGGyoJ6kf8meGcNzvtnuYKp
MD5:	EBCC27E483829E2E2E519538BDF71B7E
SHA1:	81FDE871249D5723415F6A5A0B1F7E83788A70E6
SHA-256:	86D71D31A0037F33C03921ADAA1D9ABC3E849E8BB6DD935B783AE5DED46E4EE4
SHA-512:	51339B61CBA1CE0B0F63FEE6C2AE6EFDFE88FBDEB08898F6816115C7E40B174BBCEEE4BF86C8CDED945EA2BE3A29C1D3AA750721D0ACCD643165C6CC25E78332
Malicious:	false
Reputation:	low
Preview:	.T.....,.....T=.....S.....S.....J.....j.....v.....

C:\Users\user\AppData\Local\Temp\nsg8314.tmp\System.dll	
Process:	C:\Users\user\AppData\Roaming\bnqw\amve.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\nsg8314.tmp\System.dll	
Joe Sandbox View:	• Filename: SX365783909782021.exe, Detection: malicious, Browse • Filename: moq fob order.exe, Detection: malicious, Browse • Filename: 0900000000000090000.exe, Detection: malicious, Browse • Filename: 444890321.exe, Detection: malicious, Browse • Filename: Packing-List_00930039.exe, Detection: malicious, Browse • Filename: 2435.exe, Detection: malicious, Browse • Filename: INVOICE.exe, Detection: malicious, Browse • Filename: Shipment Invoice & Consignment Notification.exe, Detection: malicious, Browse • Filename: KY4cmAI0jU.exe, Detection: malicious, Browse • Filename: 5t2CmTUhKc.exe, Detection: malicious, Browse • Filename: 8qdfmqz1PN.exe, Detection: malicious, Browse • Filename: New Order PO2193570O1.doc, Detection: malicious, Browse • Filename: L2.xlsx, Detection: malicious, Browse • Filename: Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx, Detection: malicious, Browse • Filename: New Order PO2193570O1.pdf.exe, Detection: malicious, Browse • Filename: 2320900000000.exe, Detection: malicious, Browse • Filename: CshpH9OSkc.exe, Detection: malicious, Browse • Filename: 5SXTKXCnqS.exe, Detection: malicious, Browse • Filename: i6xFULh8J5.exe, Detection: malicious, Browse • Filename: AWB00028487364 -000487449287.doc, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-D.-D.-D...J.*.D.-E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsk5B47.tmp	
Process:	C:\Users\user\Desktop\Quote-TSL-1037174_4810.exe
File Type:	data
Category:	dropped
Size (bytes):	317921
Entropy (8bit):	7.545162398623952
Encrypted:	false
SSDEEP:	6144:UXAsmVGCz9uZn6Z6I4YY8mrPLlQGcNzvthxuYKbt:XsGGyoJ6kf8meGcNzvtnuYKp
MD5:	EBCC27E483829E2E2E519538BDF71B7E
SHA1:	81FDE871249D5723415F6A5A0B1F7E83788A70E6
SHA-256:	86D71D31A0037F33C03921ADAA1D9ABC3E849E8BB6DD935B783AE5DED46E4EE4
SHA-512:	51339B61CBA1CE0B0F63FEE6C2AE6EFDFE88FBDEB08898F6816115C7E40B174BBCEEE4BF86C8CDED945EA2BE3A29C1D3AA750721D0ACCD643165C6CC25E7 8332
Malicious:	false
Preview:	.T.....,.....T=.....S.....S..... .....J.....j.....v..... ....

C:\Users\user\AppData\Local\Temp\nsk5B48.tmp\System.dll	
Process:	C:\Users\user\Desktop\Quote-TSL-1037174_4810.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-D.-D.-D...J.*.D.-E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nstA2D0.tmp	
Process:	C:\Users\user\AppData\Roaming\bnqw\amve.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\nstA2D0.tmp	
Size (bytes):	317921
Entropy (8bit):	7.545162398623952
Encrypted:	false
SSDEEP:	6144:UXAsmVGCz9uZn6Z6I4YY8mrPLlQGcNzvthxuYKbt:XsGGyoJ6kf8meGcNzvtnuYKp
MD5:	EBCC27E483829E2E2E519538BDF71B7E
SHA1:	81FDE871249D5723415F6A5A0B1F7E83788A70E6
SHA-256:	86D71D31A0037F33C03921ADAA1D9ABC3E849E8BB6DD935B783AE5DED46E4EE4
SHA-512:	51339B61CBA1CE0B0F63FEE6C2AE6EFDFE88FBDEB08898F6816115C7E40B174BBCEEE4BF86C8CDED945EA2BE3A29C1D3AA750721D0ACCD643165C6CC25E78332
Malicious:	false
Preview:	.T.....,.....T=.....S.....S..... .....J.....j.....v..... ....

C:\Users\user\AppData\Local\Temp\nstA2D1.tmp\System.dll	
Process:	C:\Users\user\AppData\Roaming\bnqw\amve.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	261728
Entropy (8bit):	6.1750840449797675
Encrypted:	false
SSDEEP:	3072:Mao0QHGUQWWimj9q/NLpj/WWqvAw2XpFU4rwOe4ubZSif02RFi/x2uv9FeP:boZTTWxxqVpqWVRXfr802biprVu
MD5:	D621FD77BD585874F9686D3A76462EF1
SHA1:	ABCAE05EE61EE6292003AABD8C80583FA49EDDA2
SHA-256:	2CA7CF7146FB8209CF3C6CECB1C5AA154C61E046DC07AFA05E8158F2C0DDE2F6
SHA-512:	2D85A81D708ECC8AF9A1273143C94DA84E632F1E595E22F54B867225105A1D0A44F918F0FAE6F1EB15ECF69D75B6F4616699776A16A2AA8B5282100FD15CA74C
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....".0..|...B.....n.... .....@.. ....`.....O.....>.....`>..... ....H.....text....z... ...|..... ..`.rsrc....>.....@...~.....@..@.relo c.....@..B.....P.....H.....8).....|.....*.{.....*v.(=....r...p({...-..+..}....*....0..%.....(....-..*....(z....&..}.....*.*..... ...0..5.....(....-..*.-.r+..ps>...z.....i(z.....&..}.....*.*.....%.....>....(?...(....*N..(@....oA...(....*:...(B...(....*:...(C...(....**....(....*....0..G.....(.....,.*..(....-...}.....*.r...p(x...&.(v.....}... ...&..}.....*.*.....7.....0..f.....-.r7..ps>...z .....

C:\Users\user\AppData\Roaming\bnqw\amve.exe	
Process:	C:\Users\user\Desktop\Quote-TSL-1037174_4810.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	448961
Entropy (8bit):	6.069011681162613
Encrypted:	false
SSDEEP:	6144:usUlNPJU0e7dkV3ZLFJVsA2mQ7fGUgYCrQOd:sPJU1763Z7VPw7+Ugfxd
MD5:	DEB5412F0B0201D045E2007503BBB283

C:\Users\user\AppData\Roaming\bnqw\amve.exe	
SHA1:	4086C81E9C51DB9E242C604BFA99AD217A45986D
SHA-256:	C770D9D870614A8A39844CD1F564BB823944F8D4D25F7D68F15B1401FB08E4E9
SHA-512:	9310A18A3602D175DD5235AC464CED734AEB1BC5542BC94B45D1BE1B3D8580FB9ACC8FD3834D27025983B87A54DDAACBED9C923E2A79205BFE0CE0AA09E2C F78
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 59%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i..iw..iu..i...i..id..i!..i...i...it..iRichu..i.....PE..L. .....K.....\.....<2.....p....@.....P.....s.....p.....p.....text... ZZ.....\..... ..`.rdata.....p.....`.....@..@.data.....r.....@....ndata.....@.....rsrc...p.....v.....@..@.....

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Preview:	..127.0.0.1

\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	298
Entropy (8bit):	4.943030742860529
Encrypted:	false
SSDEEP:	6:zx3M1tFAbQtU1R30qyMstwYVoRRZBXVN+J0fFdCsq2UTiMdH8stCal+n:zK13l30ZMt9BFN+QdCT2UftCM+
MD5:	6A9888952541A41F033EB114C24DC902
SHA1:	41903D7C8F31013C44572E09D97B9AAFBBCE77E6
SHA-256:	41A61D0084CD7884BEA1DF02ED9213CB8C83F4034F5C8156FC5B06D6A3E133CE
SHA-512:	E6AC898E67B4052375FDDFE9894B26D504A7827917BF3E02772CFF45C3FA7CC5E0EFFDC701D208E0DB89F05E42F195B1EC890F316BEE5CB8239AB45444DAA6 E
Malicious:	false
Preview:	Microsoft (R) Build Engine version 4.7.3056.0..[Microsoft .NET Framework, version 4.0.30319.42000]..Copyright (C) Microsoft Corporation. All rights reserved.....MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.069011681162613
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	Quote-TSL-1037174_4810.exe
File size:	448961
MD5:	deb5412f0b0201d045e2007503bbb283

General

SHA1:	4086c81e9c51db9e242c604bfa99ad217a45986d
SHA256:	c770d9d870614a8a39844cd1f564bb823944f8d4d25f7d68f15b1401fb08e4e9
SHA512:	9310a18a3602d175dd5235ac464ced734aeb1bc5542bc94b45d1be1b3d8580fb9acc8fd3834d27025983b87a54ddaacbed9c923e2a79205bfe0ce0aa09e2cf78
SSDEEP:	6144:usUlNPJU0e7dkV3ZLFJVsA2mQ7fGUgYCrQOd:sPJU1763Z7VPw7+Ugfxd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....

File Icon

Icon Hash:	0000000000000000

Static PE Info

General

Entrypoint:	0x40323c
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:	0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.18162709925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x28e70	0x29000	False	0.0739269721799	data	0.988562741976	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
Jun 11, 2021 13:21:04.146356106 CEST	192.168.2.4	8.8.8.8	0x1834	Standard query (0)	mail.buynsell.com.pk	A (IP address)	IN (0x0001)
Jun 11, 2021 13:21:04.229811907 CEST	192.168.2.4	8.8.8.8	0xc471	Standard query (0)	mail.buynsell.com.pk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 13:21:04.207077026 CEST	8.8.8.8	192.168.2.4	0x1834	No error (0)	mail.buynsell.com.pk	buynsell.com.pk		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 13:21:04.207077026 CEST	8.8.8.8	192.168.2.4	0x1834	No error (0)	buynsell.com.pk		194.28.84.37	A (IP address)	IN (0x0001)
Jun 11, 2021 13:21:04.319475889 CEST	8.8.8.8	192.168.2.4	0xc471	No error (0)	mail.buynsell.com.pk	buynsell.com.pk		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 13:21:04.319475889 CEST	8.8.8.8	192.168.2.4	0xc471	No error (0)	buynsell.com.pk		194.28.84.37	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 13:21:04.716147900 CEST	587	49770	194.28.84.37	192.168.2.4	220-iron.fastbighost.net ESMTP Exim 4.94.2 #2 Fri, 11 Jun 2021 14:21:04 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 11, 2021 13:21:04.716617107 CEST	49770	587	192.168.2.4	194.28.84.37	EHLO 066656
Jun 11, 2021 13:21:04.790772915 CEST	587	49770	194.28.84.37	192.168.2.4	250-iron.fastbighost.net Hello 066656 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 11, 2021 13:21:04.791491032 CEST	49770	587	192.168.2.4	194.28.84.37	STARTTLS
Jun 11, 2021 13:21:04.868208885 CEST	587	49770	194.28.84.37	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Quote-TSL-1037174_4810.exe PID: 7032 Parent PID: 5764

General

Start time:	13:19:01
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Quote-TSL-1037174_4810.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quote-TSL-1037174_4810.exe'
Imagebase:	0x400000
File size:	448961 bytes
MD5 hash:	DEB5412F0B0201D045E2007503BBB283
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: 00000000.00000002.647491799.0000000009B10000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.647491799.0000000009B10000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: MSBuild.exe PID: 7088 Parent PID: 7032

General

Start time:	13:19:02
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quote-TSL-1037174_4810.exe'
Imagebase:	0x980000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 00000001.00000002.671831008.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.671831008.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.674949415.0000000002E21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.674949415.0000000002E21000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Analysis Process: amve.exe PID: 5912 Parent PID: 3424

General

Start time:	13:19:11
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\bnqw\amve.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\bnqw\amve.exe'
Imagebase:	0x400000
File size:	448961 bytes
MD5 hash:	DEB5412F0B0201D045E2007503BBB283
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: 00000003.00000002.675091117.0000000009970000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.675091117.0000000009970000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 14%, Metadefender, Browse • Detection: 59%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: MSBuild.exe PID: 6372 Parent PID: 5912

General

Start time:	13:19:12

Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\bnqw\amve.exe'
Imagebase:	0x1c0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 00000004.00000002.685992308.00000000005C2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.685992308.00000000005C2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.687171582.00000000024C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.687171582.00000000024C1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Analysis Process: amve.exe PID: 6740 Parent PID: 3424

General

Start time:	13:19:19
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\bnqw\amve.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\bnqw\amve.exe'
Imagebase:	0x400000
File size:	448961 bytes
MD5 hash:	DEB5412F0B0201D045E2007503BBB283
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: 00000005.00000002.686576879.0000000009830000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.686576879.0000000009830000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: MSBuild.exe PID: 6292 Parent PID: 6740

General

Start time:	13:19:21
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\bnqw\amve.exe'
Imagebase:	0x790000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 00000006.00000002.904595118.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.904595118.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.906095830.0000000002CF1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: NewApp.exe PID: 2480 Parent PID: 3424

General

Start time:	13:19:57
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe'
Imagebase:	0x120000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 1320 Parent PID: 2480

General

Start time:	13:19:58
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: NewApp.exe PID: 4088 Parent PID: 3424

General

Start time:	13:20:06
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe'
Imagebase:	0xcd0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Written

File Read

Analysis Process: conhost.exe PID: 2864 Parent PID: 4088

General

Start time:	13:20:06
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Disassembly

Code Analysis