ID: 553346
Sample Name:
payment_advice.exe
Cookbook: default.jbs
Time: 18:19:21
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

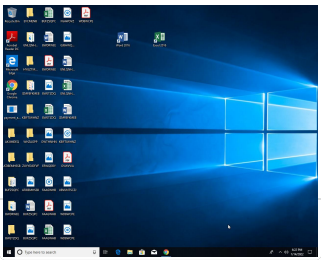
Windows Analysis Report payment_advice.exe

Overview

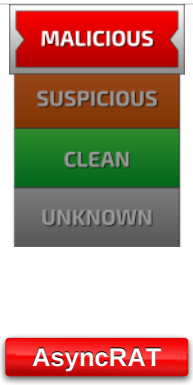
General Information

Sample Name:	payment_advice.exe
Analysis ID:	553346
MD5:	8c111a2fb250966.
SHA1:	1706e12b96c88c..
SHA256:	18dee23d492e67..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



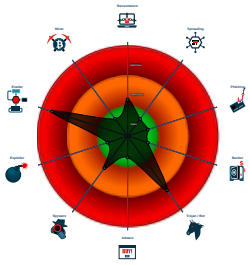
AsyncRAT

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected AsyncRAT
- Sigma detected: Bad Opsec Default…
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- payment_advice.exe (PID: 6548 cmdline: "C:\Users\user\Desktop\payment_advice.exe" MD5: 8C111A2FB2509662DB26B214B72E4E36)
  - RegSvcs.exe (PID: 5580 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 6872 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 4204 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT

```
{
  "Server": "185.222.57.80",
  "Ports": "6275",
  "Version": "0.5.7B",
  "Autorun": "false",
  "Install_Folder": "%AppData%",
  "Install_File": "",
  "AES_key": "QezdxbEnAcR8YRyfVhhUW7fy58KZtsCM",
  "Mutex": "AsyncMutex_6SI8OkPnk",
  "AntiDetection": "false",
  "External_config_on_Pastebin": "null",
  "BDOS": "false",
  "Startup_Delay": "20",
  "HWID": "null",
  "Certificate":
"MIIE8jCCAtqgAwIBAgIQAPsgY74fnNwbIPR6dDIAXTANBgkqhkiG9w0BAQ0FADAaMRgwFgYDVQQDDA9Bc3luY1JBVCBTZXJ2ZXIwIBcNMjIwMTExMTUxMzQ3WhgPOTk5OTEyMzEyMzU5NTlaMBoxGDAWBgNVBAMMD0FzeW5jUkFUIFNlcnZlcjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAImeGbwefUPZlenM9ZLOLyWoIfTUQbvfSf2I4aTtRtrJV0PvNEvbnGLJBVZe2Pl0/07x8Tk2rB11VhT66e/qyj/1GaK2lCocdlZY1ISbbDPiVaENZ3Pd4XFA00Am9axKENbivQzVj9NT8HlT1ymPK1utCLa7IWfmf5SR76DG8iaClYf0QiNFizdty7Bmhnc5ZS9xFI7tWzao+K0Ds7iD0IEQvKPWVAdssV/Y0rDXxcNcYo0iKDU4Qln8Hwgeuqh+ZFSgwwYnbDCfyKHO85s7GCD4MluE6vYBla1guC8SRWvRTIop+edRyivzmQ17cX+9K6W/UcReXkrNe4UEDbSKNzxwp65yTww4B95eJEXiKzrmNpPq1jEs8okWRoPluIKi2SEOMQcUwb6VcNamWQxwnW2WMPswRpcFVedgU0mUTs4AzLhUt8vhf5e3zAs5fYY7G2NtNMUzXgR2AkhbG30dIguSUFxCiyoXL15+Z4aKudbOycqydKoeGghHd9Lgl78N7mjNuM0Ti5YNeHltKbqEb10P5K4ZaSaWQe2FjTTY0/PjTqwUGouJcXg+vG6JYcsfFw4a6n3kivC7AOPYsdvMLuq+D3Rg/wrlo7ZfgzvkZojzjBboBRDbMi57Y8W77i+VEb81VlPwmTcbzP6dFcrfJVmVOgDRW3q96OD9HxfMXQxZAgMBAAGjMjAwMB0GA1UdDgQWBBTaL3HojDpid9l5Z4ww/A0enwsLHzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBDQUAA4ICAQA4PTTl66juqXrGz2R4fBZ1Dy3CfIL590qgWNuzGTkqR2uC54F9gG0bhexUBfK5OZp0ypmQlfRIRw5e6bXXmizGmHXGKdirG4dIiwK2hh/9ENP7D8nafAeIaB935RopQHSR6qXrbm2IiJFJySnfZLCnWADOPq0zy3YlD62JA07DNvEyQKq7v128VkpFPGzCIeFBxcbrLvadpEv71py3DwZJU+FYn2tqFBZPTtVkZcPIlSdG2+f5lp1FlgTZa+p+5pUYrLyH5KI3BZBLpZy29j1/Yy/x5N6eVi7zHNoin4VtMlx8oSKxNfx8C66palvTiw3/Ga9NVyWkvFO43ddgMsdAfJ0CryfKLaK3D9vfd1HgdH6AFB+lHh51ANUeNgRnlngCQ5NZL9PTOBywiHV9aPV1lQPUlbE9SLlmgZfXDzxxHOE+eHR+FpOumMxrEiUAn/x3xRN6jgq1opAJ8dgK1JRx76pC3eXPvyNmz6NPUaVb2oOI+nBDdnAyUWlOY84JrycPi8qt0HbL7FOMhwJKk3wE7zdL32h+bRhef2VediBaEnPI38ZNk6Nn7lYkSifkhOeDTHR2WMoSTNEM+bMpb66/kySmGBEY7f4w0R8190mxufBfIYKeimOunDuRukbKXpNEnmkSPoysVZP9r/KmF0iES7g6FDmfF5ixPsz7B4OS4A==",
  "ServerSignature":
"HIVbYAPWifBLFM1dIsEfxbnVJ30YJJhWw82LHYtKmHEC3g/lAwZSluRjZRWAz1JR169Sn8cJckChtzpnJtaXs6xUOq3xWorDyH9CxmCYqSkPU3OLjEtGBWOhUlAkUyMsAegVguFE9yC3QsL7d9ry54trgH3tAg6a34DzC51v1nMppCNNKptEDh8p2rg8s1IotSV6LVOItcGaHuTjpqfTeXeg/eAL7+fWNw5FMH5j+j5OpNOELl2Y9mbJvjzZ7v7Ff5YXkcEopiyWuEW9eIjuNyOrBU0a9H9MOaSN091fxYLVYDYWVxzt1PbJWRdyLWE00EVdejlfQipA45wZVidw9RxD2O67SVlBO5mm+KQd80ISK1fbp3hZ9hX9OyH//2OwJPiL61w1i5owalTZMVlQ13Gfv1pubixjVVvO7aZwGlmEqWrGDqlyElrefhfni7aWdPIbeBaD1LSv91pHDOTzmrr0nePUF66dkKLcs/BwygcY+XesKJQROtWzWrkFc+jmezq8DIGGCEf+kwq+ZFb1LRxPGOFck8Qr2JS9rqdHbx+Mrmn+sxzk0Ozm9tFUmryKxIMct4fTiT0r6sD/LJyLQZPxH3IHYk36GLpqgOcjGLA3hFtkV41EjGuYNgLkB6ekG++kBHZtstmBNIyfOBmGOhy9BSJ8oAmjYzPP4ivKO7I=",
  "Group": "Default"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.674008993.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000006.00000000.673297148.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000006.00000002.915982123.0000000002961000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000006.00000000.674336932.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000006.00000002.915347249.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.RegSvcs.exe.400000.4.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
6.0.RegSvcs.exe.400000.2.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
6.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
6.0.RegSvcs.exe.400000.3.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
6.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

System Summary:

Initial sample is a PE file and has a suspicious name

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

Data Obfuscation:

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival:

Yara detected AsyncRAT

Malware Analysis System Evasion:

Yara detected AntiVM3

Yara detected AsyncRAT

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

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

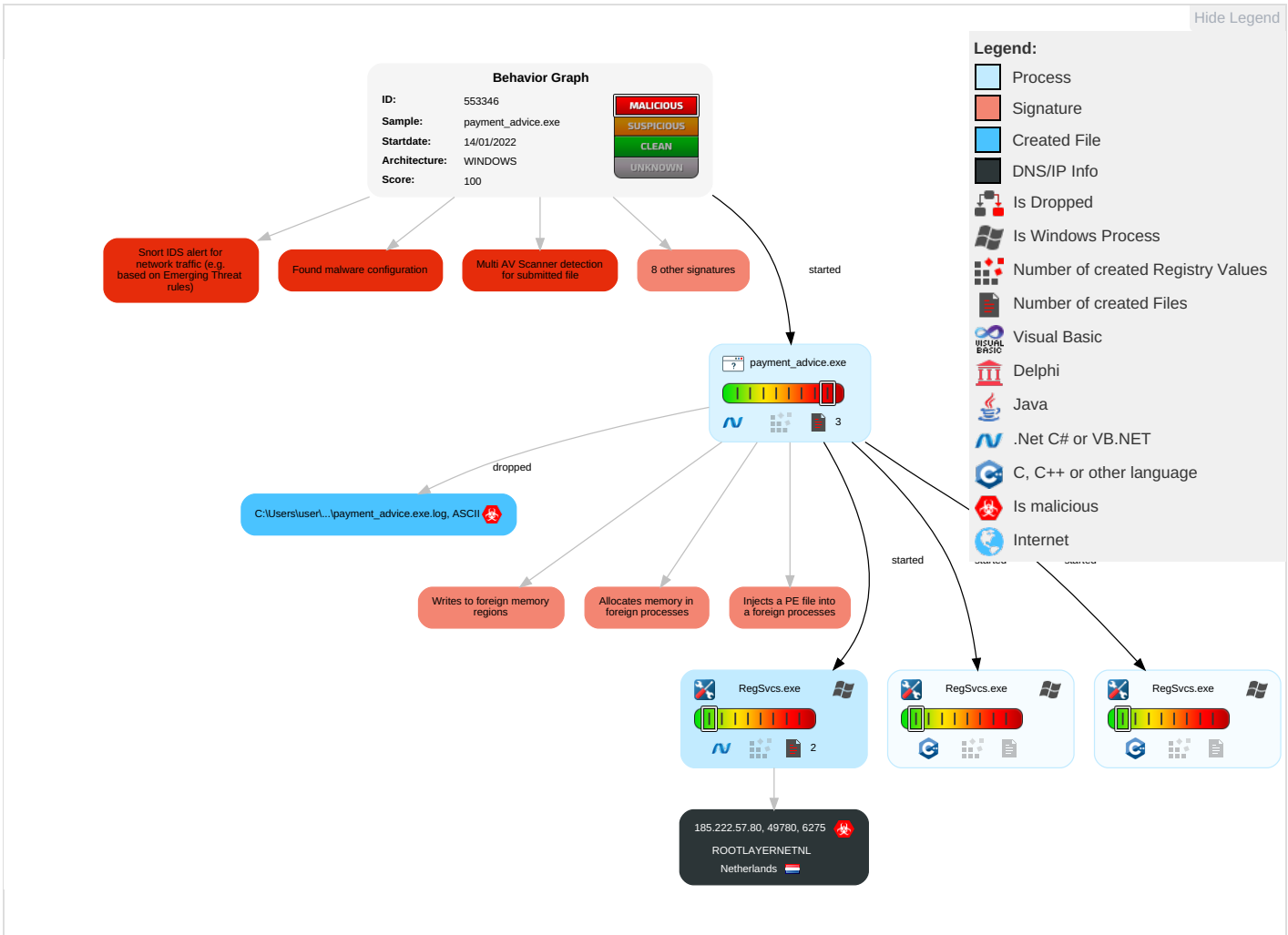
Lowering of HIPS / PFW / Operating System Security Settings:

Yara detected AsyncRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 3 1 2	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesc Insecu Networ Commu
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 1 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

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
payment_advice.exe	24%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.founder.com.cn/cnen	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn.	0%	Virustotal		Browse
http://www.zhongyicts.com.cn.	0%	Avira URL Cloud	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.zhongyicts.com.cnKX	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/==FL	0%	Avira URL Cloud	safe	
http://www.fontbureau.com3	0%	Avira URL Cloud	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.fontbureau.comalic	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.222.57.80	unknown	Netherlands		51447	ROOTLAYERNETNL	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553346
Start date:	14.01.2022
Start time:	18:19:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment_advice.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:	18
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.evad.winEXE@7/3@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 28.7% • Quality standard deviation: 40.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:20:19	API Interceptor	1x Sleep call for process: payment_advice.exe modified
18:20:48	API Interceptor	1x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U...."<ke.....I.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.".Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.".g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....I..H.#...d.Qh..3..fCX....==#..M.I..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.....N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3..._ ..nN]..=..M.o.F.._..z....._...gY..!Z..?l....vp.I.:.d.Z..W.....~...N.._.k...&.....$.....i.F.d.....D!e.....Y..,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c../.;....g&.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1244568012511515
Encrypted:	false
SSDEEP:	6:kKDk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:79kPlE99SNxAhUeYlUSA/t
MD5:	1AD9D3C77987DE50D16FA98A6D04545D
SHA1:	C87624B50174BBAA7748B9902360A3DB8210A7FC
SHA-256:	C055B3399CD39B1D85853DA633FAB0B60D579D3FA65736DB2BD59163040D4F56
SHA-512:	4AD443D435E493D6B30B2B50E577A3D4948FF7922E1973F40CCB907F53F3A5C0AFEB69398C960723680158C233AE0750F1AB40F0D3DFF8366523F39ED1D47D93
Malicious:	false
Reputation:	low
Preview:	p..... .....P.k...(..... ....q.\].....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment_advice.exe.log	
Process:	C:\Users\user\Desktop\payment_advice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment_advice.exe.log	
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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.5940068786416095
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% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	payment_advice.exe
File size:	387584
MD5:	8c111a2fb2509662db26b214b72e4e36
SHA1:	1706e12b96c88c74b1551184770221ae90eded88
SHA256:	18dee23d492e67fd0644205091068422a7322f94f9028a4a85a87505e6003cb8
SHA512:	75f03d45240f22e92f3a6d0133de64ccb7e4d59d0b4eafbc8b44f668e7f3d98580cd486c36aaa110d7ee67b9aa3373b597e427c2c86a54b659e1ad880bc9cb87
SSDEEP:	6144:Dmd5K777777777777N7ErDnTsU9C1w4DZ4OrcY7UyEQ0LtGVvC7RRX:aK777777777777N7EPAUg1w4qgT0LU+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...-G.a.....>.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x45fc3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E1472D [Fri Jan 14 09:49:33 2022 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

General

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	0x5dc44	0x5de00	False	0.625301681092	data	6.61261885246	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x60000	0x614	0x800	False	0.3349609375	data	3.4396261812	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x62000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-18:20:48.001691	TCP	2030673	ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server)	6275	49780	185.222.57.80	192.168.2.4

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: payment_advice.exe PID: 6548 Parent PID: 6588

General

Start time:	18:20:11
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\payment_advice.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\payment_advice.exe"
Imagebase:	0x7e0000
File size:	387584 bytes
MD5 hash:	8C111A2FB2509662DB26B214B72E4E36
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: 00000000.00000002.676199405.0000000002B91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.676199405.0000000002B91000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 5580 Parent PID: 6548

General

Start time:	18:20:20
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x1c0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6872 Parent PID: 6548

General

Start time:	18:20:21
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x50000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 4204 Parent PID: 6548

General

Start time:	18:20:21
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x4a0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000000.674008993.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000000.673297148.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000002.915982123.0000000002961000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000000.674336932.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000002.915347249.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000000.673592493.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis