ID: 385340
Sample Name: Payment Advice Note from 02.04.2021 to 608761.exe
Cookbook: default.jbs
Time: 10:56:16
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

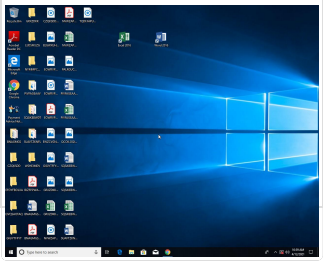
Analysis Report Payment Advice Note from 02.04.2021 t…

Overview

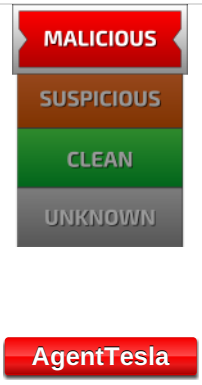
General Information

Sample Name:	Payment Advice Note from 02.04.2021 to 608761.exe
Analysis ID:	385340
MD5:	65e28f2d01fc1d2..
SHA1:	80314bd15640f1f..
SHA256:	12b9e3e3878aed..
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection



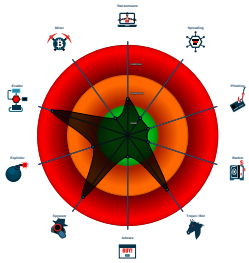
AgentTesla

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- Payment Advice Note from 02.04.2021 to 608761.exe (PID: 6088 cmdline: 'C:\Users\user\Desktop\Payment Advice Note from 02.04.2021 to 608761.exe' MD5: 65E28F2D01FC1D21E9D6632B85CE197C)
  - Payment Advice Note from 02.04.2021 to 608761.exe (PID: 1064 cmdline: C:\Users\user\Desktop\Payment Advice Note from 02.04.2021 to 608761.exe MD5: 65E28F2D01FC1D21E9D6632B85CE197C)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "jackie@ascobahkk.comxXlyWel0smtp.ascobahkk.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.221029733.00000000043B3000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.476337979.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.220556345.00000000032F1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000002.480501378.0000000002DC1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.480501378.0000000002DC1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 4 entries

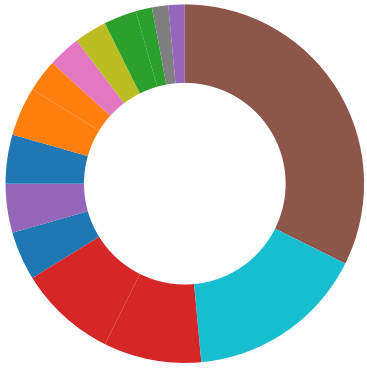
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Payment Advice Note from 02.04.2021 to 608761.exe.4455738.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.Payment Advice Note from 02.04.2021 to 608761.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Payment Advice Note from 02.04.2021 to 608761.exe.4455738.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Yara detected AntiVM3

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)

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

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 browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

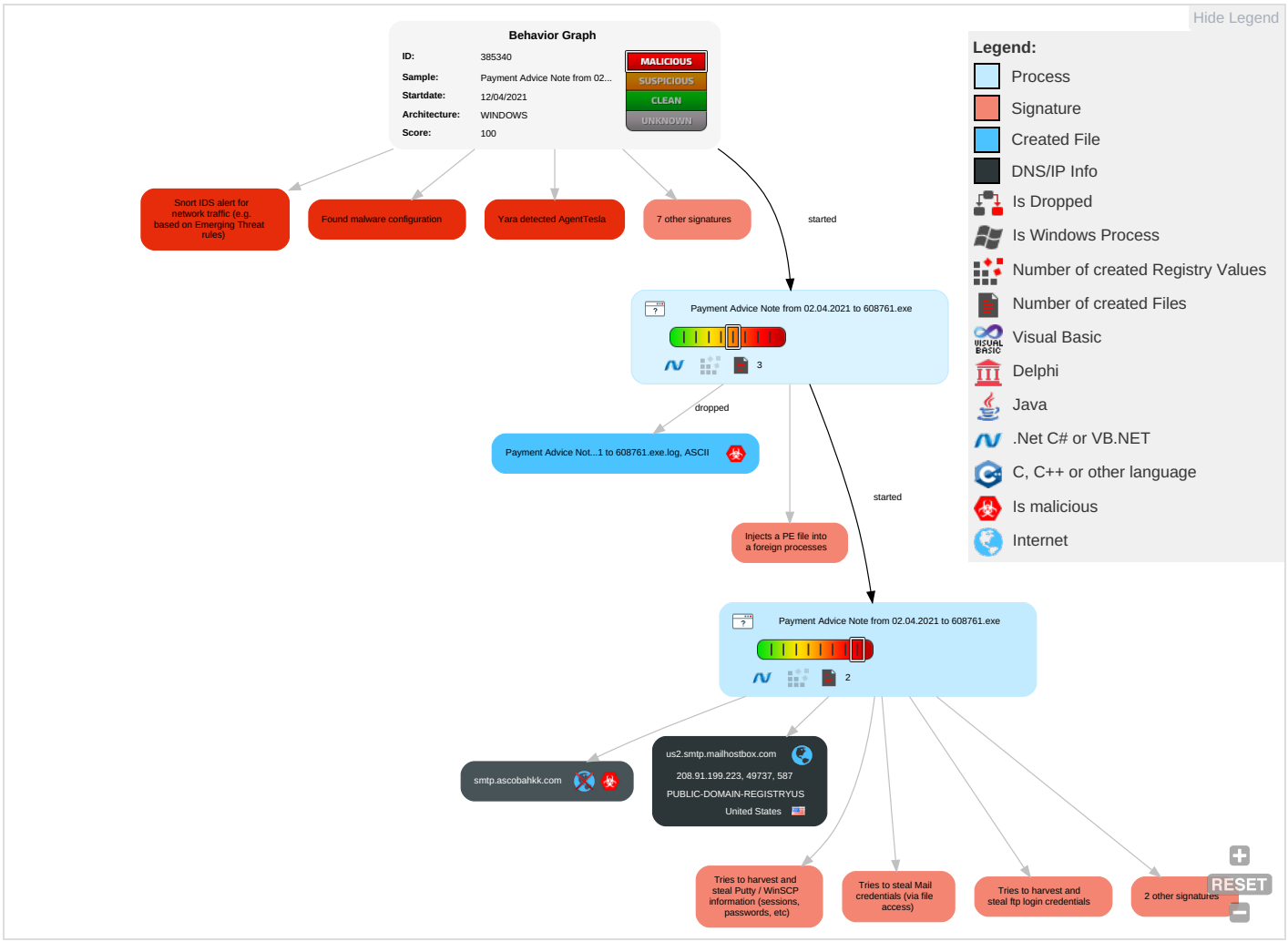
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encry Chan
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1 1 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth	Non-S Port
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Credentials in Registry 1	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Appli Layer Proto
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Appli Layer Proto
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallba Chan
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multit Comr
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comr Used

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 Note from 02.04.2021 to 608761.exe	12%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Payment Advice Note from 02.04.2021 to 608761.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.Payment Advice Note from 02.04.2021 to 608761.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		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	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://smtp.ascobahkk.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%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://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	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://TpBEZpmhMLGhKCamPG.org	0%	Avira URL Cloud	safe	
http://tzGfKE.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high
smtp.ascobahkk.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Payment Advice Note from 02.04.2021 to 608761.exe, 00000002.00000002.480501378.0000000002DC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	Payment Advice Note from 02.04.2021 to 608761.exe, 00000002.00000002.480501378.0000000002DC1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.ascobahkk.com	Payment Advice Note from 02.04.2021 to 608761.exe, 00000002.00000002.482832070.0000000003079000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://us2.smtp.mailhostbox.com	Payment Advice Note from 02.04.2021 to 608761.exe, 00000002.00000002.482832070.0000000003079000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Payment Advice Note from 02.04.2021 to 608761.exe, 00000002.00000002.480501378.0000000002DC1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Payment Advice Note from 02.04.2021 to 608761.exe, 00000001.00000002.220578954.0000000003310000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Payment Advice Note from 02.04.2021 to 608761.exe, 00000001.00000002.221029733.00000000043B3000.00000004.00000001.sdmp, Payment Advice Note from 02.04.2021 to 608761.exe, 00000002.00000002.476337979.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Payment Advice Note from 02.04.2021 to 608761.exe, 00000001.00000002.220556345.00000000032F1000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://TpBEZpmhMLGhKCamPG.org	Payment Advice Note from 02.04.2021 to 608761.exe, 00000002.00000002.480501378.0000000002DC1000.00000004.00000001.sdmp, Payment Advice Note from 02.04.2021 to 608761.exe, 00000002.00000002.483013632.000000003085000.00000004.00000001.sdmp, Payment Advice Note from 02.04.2021 to 608761.exe, 00000002.00000003.431612776.0000000000FB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://tzGfKE.com	Payment Advice Note from 02.04.2021 to 608761.exe, 00000002.00000002.480501378.0000000002DC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.223	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385340
Start date:	12.04.2021
Start time:	10:56:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Advice Note from 02.04.2021 to 608761.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.8%) • Quality average: 45.7% • Quality standard deviation: 30.2%
HCA Information:	• Successful, ratio: 98% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 52.147.198.201, 52.255.188.83, 104.42.151.234, 20.82.210.154, 23.57.80.111, 13.88.21.125, 92.122.213.247, 92.122.213.194, 8.248.117.254, 8.248.131.254, 67.26.137.254, 67.26.139.254, 67.27.158.254, 20.54.26.129, 40.88.32.150, 168.61.161.212 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:57:09	API Interceptor	816x Sleep call for process: Payment Advice Note from 02.04.2021 to 608761.exe modified

Time	Type	Description

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	AD1-2001028L.exe	Get hash	malicious	Browse	
	AD1-2001028L (2).exe	Get hash	malicious	Browse	
	Swift Copy#947026.exe	Get hash	malicious	Browse	
	Order Enquiry 200234.exe	Get hash	malicious	Browse	
	New Order Quotation.exe	Get hash	malicious	Browse	
	Image0001.exe	Get hash	malicious	Browse	
	Invoice.exe	Get hash	malicious	Browse	
	April New Order.exe	Get hash	malicious	Browse	
	Inv-254345.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	$$$.exe	Get hash	malicious	Browse	
	FF&E Items.exe	Get hash	malicious	Browse	
	Order_AH874.exe	Get hash	malicious	Browse	
	Purchase Order #07916813.exe	Get hash	malicious	Browse	
	AWB # 2205280630.jpg.exe	Get hash	malicious	Browse	
	Purchase Order 03-25-2021.exe	Get hash	malicious	Browse	
	Quotation 400026.exe	Get hash	malicious	Browse	
	378753687654345678345602.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	e0xd7qhFaMk3Dpx.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAGO FACTURA V-8680.exe	Get hash	malicious	Browse	• 208.91.198.143
	usd 420232.exe	Get hash	malicious	Browse	• 208.91.199.225
	P037725600.exe	Get hash	malicious	Browse	• 208.91.199.225
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.225
	NEW ORDER.exe	Get hash	malicious	Browse	• 208.91.198.143
	TRANSFERENCIA AL EXTERIOR U810295.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAYMENT SWIFT COPY MT103.exe	Get hash	malicious	Browse	• 208.91.198.143
	UPDATED SOA.exe	Get hash	malicious	Browse	• 208.91.199.224
	BANK PAYMENT.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	IMG_00000000001.PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	New Order PO#121012020_____PDF_____.exe	Get hash	malicious	Browse	• 208.91.198.143
	swift Copy.xls.exe	Get hash	malicious	Browse	• 208.91.199.225
	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV TBN.uslfze.exe	Get hash	malicious	Browse	• 208.91.199.224
	purchase order.exe	Get hash	malicious	Browse	• 208.91.199.223
	AD1-2001028L.exe	Get hash	malicious	Browse	• 208.91.199.225
	AD1-2001028L (2).exe	Get hash	malicious	Browse	• 208.91.199.223

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Dubai REGA 2021UAE.exe	Get hash	malicious	Browse	• 208.91.199.135
	e0xd7qhFaMk3Dpx.exe	Get hash	malicious	Browse	• 208.91.198.143
	Dridex.xls	Get hash	malicious	Browse	• 208.91.199.159
	documents-351331057.xlsm	Get hash	malicious	Browse	• 162.251.80.27

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	documents-351331057.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	DUBAI UAEGH092021.exe	Get hash	malicious	Browse	• 208.91.199.135
	PAGO FACTURA V-8680.exe	Get hash	malicious	Browse	• 208.91.198.143
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	usd 420232.exe	Get hash	malicious	Browse	• 208.91.199.225
	P037725600.exe	Get hash	malicious	Browse	• 208.91.199.225
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	NEW ORDER.exe	Get hash	malicious	Browse	• 208.91.198.143
	TRANSFERENCIA AL EXTERIOR U810295.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAYMENT SWIFT COPY MT103.exe	Get hash	malicious	Browse	• 208.91.198.143
	UPDATED SOA.exe	Get hash	malicious	Browse	• 208.91.199.224
	BANK PAYMENT.exe	Get hash	malicious	Browse	• 208.91.199.224
	document-1245492889.xls	Get hash	malicious	Browse	• 5.100.155.169
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Advice Note from 02.04.2021 to 608761.exe.log

Process:	C:\Users\user\Desktop\Payment Advice Note from 02.04.2021 to 608761.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.4508402175934

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Payment Advice Note from 02.04.2021 to 608761.exe
File size:	765440
MD5:	65e28f2d01fc1d21e9d6632b85ce197c
SHA1:	80314bd15640f1fa2219d984f8dfbf57e31c2305
SHA256:	12b9e3e3878aed00a346cfbe1cbcfe58d52af8a7b27a0420ef91d3b8395ffb19
SHA512:	6e4db02d9a4af0e3e118f7ef9e758a698870c5023632e9f84fab7fda85db4e3b782e60fd29aed0cd7c447b9dc08f1f7169562127b3b10bbd7de6431a5b60ba00
SSDEEP:	12288:SBt33BHKdWi+br+5uX1VOtROblyhi54hrevdmBIg11:SLnls+v+6VOtR0PiqSYBIg11
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....zf`.....P.....F.... ... .@.. .....@.....

File Icon

Icon Hash:	09e4a4dececc63680

Static PE Info

General

Entrypoint:	0x4b1f46
Entrypoint Section:	.text
Digitally signed:	false
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:	0x60667A9F [Fri Apr 2 01:59:59 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb1ef4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb2000	0xa8b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xaff4c	0xb0000	False	0.732181895863	data	7.60186559741	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb2000	0xa8b4	0xaa00	False	0.302205882353	data	3.60229082529	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb2100	0x94a8	data		
RT_GROUP_ICON	0xbb5b8	0x14	data		
RT_VERSION	0xbb5dc	0x378	data		
RT_MANIFEST	0xbb964	0xf4c	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

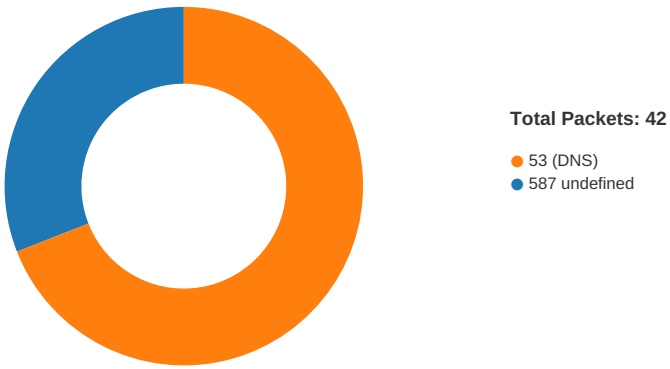
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	(c) Ubisoft
Assembly Version	4.1.0.2
InternalName	ReturnMessage.exe
FileVersion	4.1.0.2
CompanyName	Ubisoft
LegalTrademarks	Ubisoft Connect
Comments	
ProductName	Ubisoft Game Launcher
ProductVersion	4.1.0.2
FileDescription	Ubisoft Game Launcher
OriginalFilename	ReturnMessage.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-10:58:56.977144	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49737	587	192.168.2.3	208.91.199.223

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:58:55.112742901 CEST	49737	587	192.168.2.3	208.91.199.223
Apr 12, 2021 10:58:55.284945011 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:55.285125017 CEST	49737	587	192.168.2.3	208.91.199.223
Apr 12, 2021 10:58:55.925510883 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:55.926039934 CEST	49737	587	192.168.2.3	208.91.199.223
Apr 12, 2021 10:58:56.091690063 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:56.091717958 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:56.094475985 CEST	49737	587	192.168.2.3	208.91.199.223
Apr 12, 2021 10:58:56.263942957 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:56.264977932 CEST	49737	587	192.168.2.3	208.91.199.223
Apr 12, 2021 10:58:56.433099031 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:56.434525013 CEST	49737	587	192.168.2.3	208.91.199.223
Apr 12, 2021 10:58:56.600677013 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:56.601398945 CEST	49737	587	192.168.2.3	208.91.199.223
Apr 12, 2021 10:58:56.801235914 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:56.801776886 CEST	49737	587	192.168.2.3	208.91.199.223

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:58:56.970885038 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:56.977144003 CEST	49737	587	192.168.2.3	208.91.199.223
Apr 12, 2021 10:58:56.977442980 CEST	49737	587	192.168.2.3	208.91.199.223
Apr 12, 2021 10:58:56.977602959 CEST	49737	587	192.168.2.3	208.91.199.223
Apr 12, 2021 10:58:56.977766037 CEST	49737	587	192.168.2.3	208.91.199.223
Apr 12, 2021 10:58:57.142786026 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:57.143593073 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:57.238548994 CEST	587	49737	208.91.199.223	192.168.2.3
Apr 12, 2021 10:58:57.278672934 CEST	49737	587	192.168.2.3	208.91.199.223

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:56:59.183449030 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:12.003546000 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:12.052460909 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:14.965512991 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:15.014177084 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:15.853039980 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:15.904565096 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:29.757240057 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:29.814264059 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:30.551348925 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:30.609112024 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:31.991564989 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:32.049195051 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:33.064308882 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:33.116137981 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:33.814610004 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:33.863590002 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:34.206150055 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:34.254992962 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:34.502823114 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:34.563544989 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:35.324554920 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:35.373497963 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:36.496972084 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:36.556931973 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:50.276333094 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:50.334959984 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:54.640559912 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:54.692504883 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:55.349205971 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:55.398257971 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:56.450181961 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:56.501727104 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:57.204210043 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:57.274502039 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 10:57:57.569654942 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:57:57.618537903 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 10:58:10.774117947 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:58:10.823090076 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 10:58:15.225090027 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:58:15.284106016 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 10:58:30.278692007 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:58:30.327559948 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 10:58:31.477926970 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:58:31.535423994 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 10:58:32.375191927 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:58:32.423952103 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 10:58:46.279635906 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:58:46.331204891 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 10:58:47.853208065 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:58:47.921875954 CEST	53	57762	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:58:54.468168020 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:58:54.668865919 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 10:58:54.692765951 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:58:54.969451904 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 10:59:02.283458948 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:59:02.344305038 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 10:59:03.315958023 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:59:03.365974903 CEST	53	58987	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 10:58:54.468168020 CEST	192.168.2.3	8.8.8.8	0xda06	Standard query (0)	smtp.ascobahkk.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:58:54.692765951 CEST	192.168.2.3	8.8.8.8	0x1bc5	Standard query (0)	smtp.ascobahkk.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 10:58:54.668865919 CEST	8.8.8.8	192.168.2.3	0xda06	No error (0)	smtp.ascobahkk.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:58:54.668865919 CEST	8.8.8.8	192.168.2.3	0xda06	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Apr 12, 2021 10:58:54.668865919 CEST	8.8.8.8	192.168.2.3	0xda06	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Apr 12, 2021 10:58:54.668865919 CEST	8.8.8.8	192.168.2.3	0xda06	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Apr 12, 2021 10:58:54.668865919 CEST	8.8.8.8	192.168.2.3	0xda06	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Apr 12, 2021 10:58:54.969451904 CEST	8.8.8.8	192.168.2.3	0x1bc5	No error (0)	smtp.ascobahkk.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:58:54.969451904 CEST	8.8.8.8	192.168.2.3	0x1bc5	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Apr 12, 2021 10:58:54.969451904 CEST	8.8.8.8	192.168.2.3	0x1bc5	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Apr 12, 2021 10:58:54.969451904 CEST	8.8.8.8	192.168.2.3	0x1bc5	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Apr 12, 2021 10:58:54.969451904 CEST	8.8.8.8	192.168.2.3	0x1bc5	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

SMTP Packets

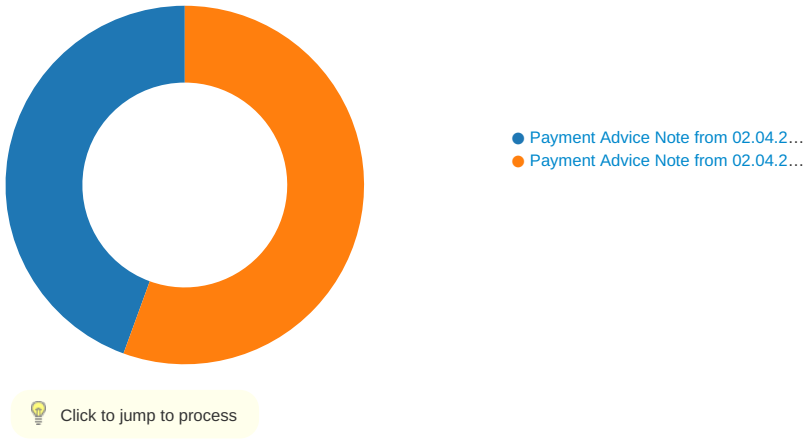
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 10:58:55.925510883 CEST	587	49737	208.91.199.223	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Apr 12, 2021 10:58:55.926039934 CEST	49737	587	192.168.2.3	208.91.199.223	EHLO 258555
Apr 12, 2021 10:58:56.091717958 CEST	587	49737	208.91.199.223	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Apr 12, 2021 10:58:56.094475985 CEST	49737	587	192.168.2.3	208.91.199.223	AUTH login amFja2llQGFzY29iYWhray5jb20=
Apr 12, 2021 10:58:56.263942957 CEST	587	49737	208.91.199.223	192.168.2.3	334 UGFzc3dvcmQ6
Apr 12, 2021 10:58:56.433099031 CEST	587	49737	208.91.199.223	192.168.2.3	235 2.7.0 Authentication successful
Apr 12, 2021 10:58:56.434525013 CEST	49737	587	192.168.2.3	208.91.199.223	MAIL FROM:<jackie@ascobahkk.com>
Apr 12, 2021 10:58:56.600677013 CEST	587	49737	208.91.199.223	192.168.2.3	250 2.1.0 Ok
Apr 12, 2021 10:58:56.601398945 CEST	49737	587	192.168.2.3	208.91.199.223	RCPT TO:<jackie@ascobahkk.com>

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 10:58:56.801235914 CEST	587	49737	208.91.199.223	192.168.2.3	250 2.1.5 Ok
Apr 12, 2021 10:58:56.801776886 CEST	49737	587	192.168.2.3	208.91.199.223	DATA
Apr 12, 2021 10:58:56.970885038 CEST	587	49737	208.91.199.223	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Apr 12, 2021 10:58:56.977766037 CEST	49737	587	192.168.2.3	208.91.199.223	.
Apr 12, 2021 10:58:57.238548994 CEST	587	49737	208.91.199.223	192.168.2.3	250 2.0.0 Ok: queued as B3289D7823

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Payment Advice Note from 02.04.2021 to 608761.exe PID: 6088
Parent PID: 5672

General

Start time:	10:57:07
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Payment Advice Note from 02.04.2021 to 608761.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment Advice Note from 02.04.2021 to 608761.exe'
Imagebase:	0xfc0000
File size:	765440 bytes
MD5 hash:	65E28F2D01FC1D21E9D6632B85CE197C
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: 00000001.00000002.221029733.00000000043B3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.220556345.00000000032F1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Advice Note from 02.04.2021 to 608761.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E35C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Advice Note from 02.04.2021 to 608761.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E35C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E025705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E02CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF803DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE91B4F	ReadFile

Analysis Process: Payment Advice Note from 02.04.2021 to 608761.exe PID: 1064
Parent PID: 6088

General

Start time:	10:57:10
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Payment Advice Note from 02.04.2021 to 608761.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Payment Advice Note from 02.04.2021 to 608761.exe
Imagebase:	0x9f0000
File size:	765440 bytes
MD5 hash:	65E28F2D01FC1D21E9D6632B85CE197C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.476337979.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.480501378.0000000002DC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.480501378.0000000002DC1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E025705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E02CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF803DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CE91B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CE91B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c4d46b61-cbd4-4a83-b8c0-2fcdb90b4f2d	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CE91B4F	ReadFile

Disassembly

Code Analysis