ID: 491993
Sample Name: Revised Proforma Invoice_New order.exe
Cookbook: default.jbs
Time: 08:54:45
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

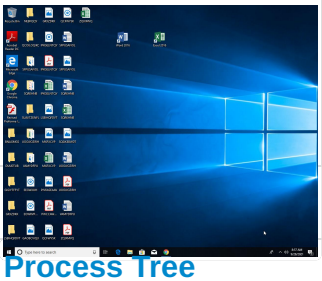
Windows Analysis Report Revised Proforma Invoice_Ne…

Overview

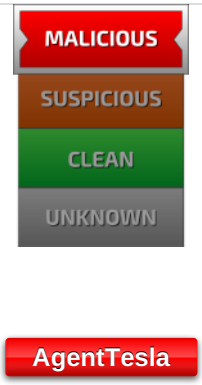
General Information

Sample Name:	Revised Proforma Invoice_New order.exe
Analysis ID:	491993
MD5:	3a391e960ff3639..
SHA1:	8930a2e630f133d.
SHA256:	8842d55ed240f4e.
Tags:	exe Invoice
Infos:	

Most interesting Screenshot:



Detection



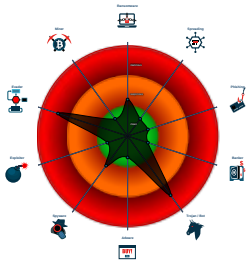
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Multi AV Scanner detection for dropp…
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Queries sensitive network adapter in…
- Queries sensitive BIOS Information …
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- Revised Proforma Invoice_New order.exe (PID: 5956 cmdline: 'C:\Users\user\Desktop\Revised Proforma Invoice_New order.exe' MD5: 3A391E960FF363979A5AC9DC3A95C636)
  - conhost.exe (PID: 6248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6360 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Sleep -s 5 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6004 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Sleep -s 5 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6288 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Sleep -s 5 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Revised Proforma Invoice_New order.exe (PID: 6052 cmdline: C:\Users\user\AppData\Local\Temp\Revised Proforma Invoice_New order.exe MD5: 3A391E960FF363979A5AC9DC3A95C636)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "whitesend@billionv.com",
  "Password": "fgd436-=/eVNM!!@#)mmnb",
  "Host": "s1.20mb.nl"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.927748556.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.927748556.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.805920223.0000000003EED000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.805920223.0000000003EED000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.804939830.0000000002E89000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.Revised Proforma Invoice_New order.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
19.2.Revised Proforma Invoice_New order.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Revised Proforma Invoice_New order.exe.3eed570.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Revised Proforma Invoice_New order.exe.3eed570.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Revised Proforma Invoice_New order.exe.3eed570.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

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

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

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

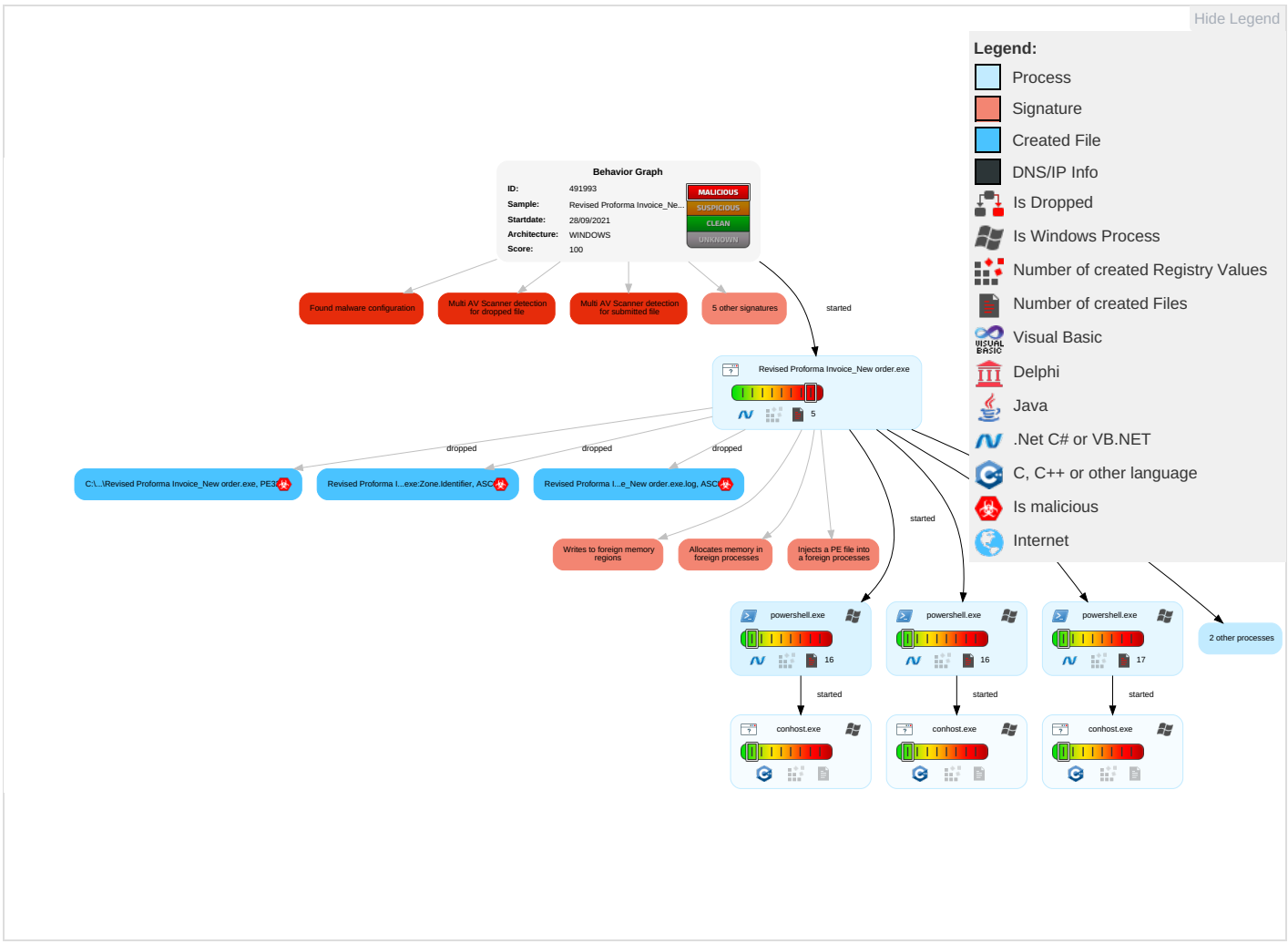
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	I
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 3 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	I I I (
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	I I (
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	I - I
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	I I (
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	, I S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Timestomp 1	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	I A

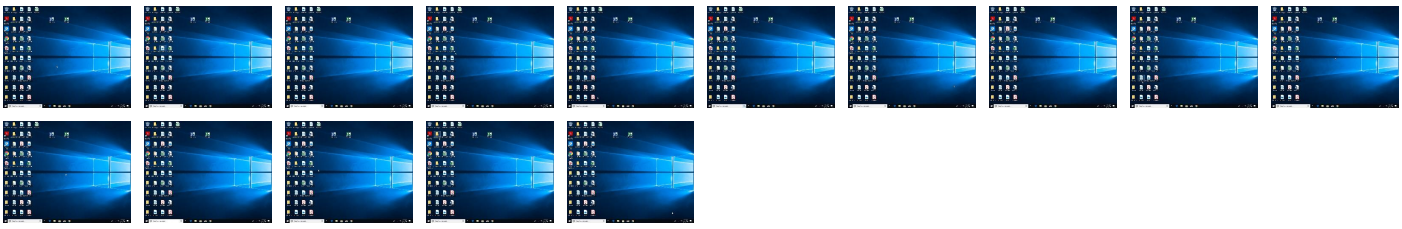
Behavior Graph



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
Revised Proforma Invoice_New order.exe	43%	Virustotal		Browse
Revised Proforma Invoice_New order.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Revised Proforma Invoice_New order.exe	43%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Revised Proforma Invoice_New order.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.2.Revised Proforma Invoice_New order.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	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://AAbVfU.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	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491993
Start date:	28.09.2021
Start time:	08:54:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Revised Proforma Invoice_New order.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.evad.winEXE@13/15@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • 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
08:55:44	API Interceptor	121x Sleep call for process: powershell.exe modified
08:56:57	API Interceptor	372x Sleep call for process: Revised Proforma Invoice_New order.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\Local\Microsoft\CLR_v4.0_32\UsageLogs\Revised Proforma Invoice_New order.exe.log	
Process:	C:\Users\user\Desktop\Revised Proforma Invoice_New order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD D
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	17200
Entropy (8bit):	5.261522518867608
Encrypted:	false
SSDEEP:	384:Qt9/FIFChUbzc9dVTGICercGnuJBuprhOGFaF:UebY9dPCnGuDArhe

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
MD5:	B6FA57F0E1BBBB0682D7622DE3FA2914
SHA1:	FC6B6D183E3EB20081BCCB21B80F25DDA4455A71
SHA-256:	D2C17C3BA5C9F3E7CD9C56E75AD704FD08773CFEAA432EC435851F4F2045E3D9
SHA-512:	A747BAA98EBF051F089989009CEE8038C6C07DCAE3B59A639E862AFD5522AC5D6E86F787A85CAEAAE708FA7497585714CDEE4879A2C9A48FC0BD3ED83CD11 1D
Malicious:	false
Preview:	@...e.....-.u.f.f...E.....~.....@.....D.....fZve...F.....x.)O.....System.Management.AutomationH.....<@.^.L."My...:)..... .Microsoft.PowerShell .ConsoleHost4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\Revised Proforma Invoice_New order.exe	
Process:	C:\Users\user\Desktop\Revised Proforma Invoice_New order.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	636928
Entropy (8bit):	6.580433774088701
Encrypted:	false
SSDEEP:	12288:Wcdn9Pox2engU3L9iCXCQUy+NLBreWNAMg+MMMMMMMMMMuMMMMMMMMMMMMMMMR:WG+9cCStVreKg+MMMMMMMMMMuMMMMMp
MD5:	3A391E960FF363979A5AC9DC3A95C636
SHA1:	8930A2E630F133DFB78E87E06B4F9ECD882A84E1
SHA-256:	8842D55ED240F4ED04D12D227DFD1C65BC20B72BF79FC5E40DAF61D9F3F86D47
SHA-512:	9AD6F160CEF7BA108A88EE963AA224C1766BFB183E7934A88B5A7019788B6874009A4A921F8B853329BE940D08DE74E3DDB0170E69B60152FBD950A5889A5926
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... .....@.. ....@.....\...O.....@..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....".X..... 5.. .....0..c.....-H(....o.....(.....(....&r...p(....o....r...p(....o....r...p(....o....+.r#..p(....(.....(....*..0..s. .....s.....(....(....o.....+.....o.....X....i2..o.....+.....r-..p .....#....o.....&.....&....X....i2..*..*.....?."a.....0..h.....rI..ps.....s ...s!.....o"....o#...,.s$....o...+...o&...+..o'....+..o(...o....(. ....o)...-....,..o*....*.....A..].....s+...%r...po,...%.o

C:\Users\user\AppData\Local\Temp\Revised Proforma Invoice_New order.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Revised Proforma Invoice_New order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1vgntrt1.ztt.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ff5nys0k.j11.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jm0jnll4.eqo.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ngqwsyfo.kwg.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pvgur2kc.vrh.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zbprfsgr.2ta.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\Documents\20210928\PowerShell_transcript.114127.HB6zZtzF.20210928085543.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	937
Entropy (8bit):	5.026199849198843
Encrypted:	false
SSDEEP:	24:BxSALy7vBZUZx2DOXUWMuWHHjeTKKjX4CIym1ZJXbQnxSAZF4:BZUvjUoOSHqDYB1ZsZZC
MD5:	BE395625ABD550D45D1340347F2456F9
SHA1:	E0AB6B4DE16BF293F73ED35E3DC85181A9742435
SHA-256:	5B1C689D2946387FF5A6F68B717B26B5E407DB3BB1FD7B98ACE7BF10CD4FCC96
SHA-512:	A5B9FE0A8558BAA89C5F70FD94BDA7B6BA7C3D99C88BD9EAF08A3CAABAAA40C9DEDB9CB4AF77559AD3A7BE1CF36EBF673606C7E32CB3CAD56694960E427 F7035
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210928085544..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 114127 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Start-Sleep -s 5..Process ID: 6360..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.303 19.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210 928085544..**********..PS>Start-Sleep -s 5..**********..Command start time: 20210928090121..**********..PS>$global:?..True..********** ***********..Windows PowerShell transcript end..End time: 20210928090121..**********..

C:\Users\user\Documents\20210928\PowerShell_transcript.114127.I2K6eNc7.20210928085600.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	937
Entropy (8bit):	5.022561751308841
Encrypted:	false
SSDEEP:	24:BxSAE7vBZUZx2DOXUWMuWcHjeTKKjX4CIym1ZJX+YkmnxSAZF1:BZivjUoOScqDYB1Z07oZZH
MD5:	C787FC2E6CE8E845AED3E1E1B73F5B7F
SHA1:	E7A18ADF3A100C9E039449466766C2679AB13F54
SHA-256:	4B203961D50E0F8040B85FCA4A2648564C5E9012F38DD17D017F316E212A1CAC
SHA-512:	663BAE9B0DF9DF1E2C4C0048FD5482CB720B0623CF7F61A3A81A984FBAFE1C3F05393F48306383BEE4A71471832C3B249977451050CD9FB121580BAF8E614E0E
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210928085601..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 114127 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Start-Sleep -s 5..Process ID: 6288..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.303 19.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210 928085601..**********..PS>Start-Sleep -s 5..**********..Command start time: 20210928090119..**********..PS>$global:?..True..********** ***********..Windows PowerShell transcript end..End time: 20210928090120..**********..

C:\Users\user\Documents\20210928\PowerShell_transcript.114127.syR87O2Z.20210928085551.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	937
Entropy (8bit):	5.0274032551766945
Encrypted:	false
SSDEEP:	24:BxSAJ7vBZUZx2DOXUWMuWfyHjeTKKjX4CIym1ZJXZnxSAZA:BZFvjUoOSfyqDYB1Z3ZZA
MD5:	4CC229CAB135DF0BCC3D34F6EF008DD3
SHA1:	D6625F3A33BF3662B08A19DE79047FBDCE4A8D3A

C:\Users\user\Documents\20210928\PowerShell_transcript.114127.syR87O2Z.20210928085551.txt

SHA-256:	3259462D27B90D29B05AF1A95C3BBEFA1DE5139B941D0E7E4894D716281E7062
SHA-512:	1EC718D8AD201171A967503E0EB21FF3D155F65BBB859BBC5FC2EC278621C6D566B50DFDEF9FC17FE488D5BB9DB4063EB5D26CBFFA29388A8E9FF65625DFFE4
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210928085552..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 114127 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Start-Sleep -s 5..Process ID: 6004..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210928085552..**********..PS>Start-Sleep -s 5..**********..Command start time: 20210928090026..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20210928090026..**********..

Static File Info

General

File type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.580433774088701
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:	Revised Proforma Invoice_New order.exe
File size:	636928
MD5:	3a391e960ff363979a5ac9dc3a95c636
SHA1:	8930a2e630f133dfb78e87e06b4f9ecd882a84e1
SHA256:	8842d55ed240f4ed04d12d227dfd1c65bc20b72bf79fc5e40daf61d9f3f86d47
SHA512:	9ad6f160cef7ba108a88ee963aa224c1766bfb183e7934a88b5a7019788b6874009a4a921f8b853329be940d08de74e3ddb0170e69b60152fbd950a5889a5926
SSDEEP:	12288:Wcdn9Pox2engU3L9iCXCQUy+NLBreWNAMg+MMMMMMMMMMuMMMMMMMMMMMMMMR:WG+9cCStVreKg+MMMMMMMMMMuMMMMMp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... .....0..... ....@.. ..... @.....

File Icon

Icon Hash:	3ce4d6d8ccc4d2cc

Static PE Info

General

Entrypoint:	0x45f3ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xC78687F9 [Wed Jan 29 00:16:57 2076 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

General

Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x5d3b4	0x5d400	False	0.606709743633	data	5.87011026515	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x60000	0x3dff4	0x3e000	False	0.347817697833	data	5.72172062928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Revised Proforma Invoice_New order.exe PID: 5956 Parent PID: 6620

General

Start time:	08:55:40
Start date:	28/09/2021

Path:	C:\Users\user\Desktop\Revised Proforma Invoice_New order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Revised Proforma Invoice_New order.exe'
Imagebase:	0xa40000
File size:	636928 bytes
MD5 hash:	3A391E960FF363979A5AC9DC3A95C636
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: 00000000.00000002.805920223.0000000003EED000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.805920223.0000000003EED000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.804939830.0000000002E89000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.805082375.0000000003E71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.805082375.0000000003E71000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6248 Parent PID: 5956

General

Start time:	08:55:41
Start date:	28/09/2021
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: powershell.exe PID: 6360 Parent PID: 5956

General

Start time:	08:55:42
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Sleep -s 5
Imagebase:	0x1240000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6592 Parent PID: 6360

General

Start time:	08:55:42
Start date:	28/09/2021
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: powershell.exe PID: 6004 Parent PID: 5956

General

Start time:	08:55:50
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Sleep -s 5
Imagebase:	0x1240000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6344 Parent PID: 6004

General

Start time:	08:55:50
Start date:	28/09/2021
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: powershell.exe PID: 6288 Parent PID: 5956

General

Start time:	08:55:59
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Sleep -s 5
Imagebase:	0x1240000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 584 Parent PID: 6288

General

Start time:	08:55:59
Start date:	28/09/2021
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: Revised Proforma Invoice_New order.exe PID: 6052 Parent PID: 5956

General

Start time:	08:56:45
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\Temp\Revised Proforma Invoice_New order.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Revised Proforma Invoice_New order.exe
Imagebase:	0xd80000
File size:	636928 bytes
MD5 hash:	3A391E960FF363979A5AC9DC3A95C636
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: 00000013.00000002.927748556.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000002.927748556.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.928622140.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000002.928622140.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 43%, Virustotal, Browse • Detection: 24%, ReversingLabs

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis