ID: 458946
Sample Name: Inv 0110617985
PO Wartsila quantiparts B.V..exe
Cookbook: default.jbs
Time: 22:20:22
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

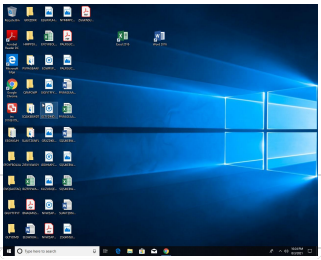
Windows Analysis Report Inv 0110617985 PO Wartsila q…

Overview

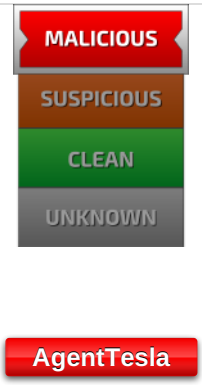
General Information

Sample Name:	Inv 0110617985 PO Wartsila quantiparts B.V..exe
Analysis ID:	458946
MD5:	5c9c7f90ae087c4..
SHA1:	15a76b5c5d5ee6..
SHA256:	2e4901e09f9e7e7.
Tags:	exe null
Infos:	

Most interesting Screenshot:



Detection

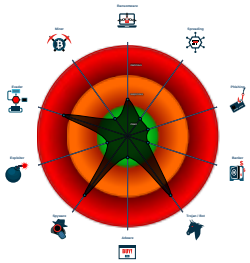


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fil…

Classification



Process Tree

- **System is w10x64**
- Inv 0110617985 PO Wartsila quantiparts B.V..exe (PID: 1236 cmdline: 'C:\Users\user\Desktop\Inv 0110617985 PO Wartsila quantiparts B.V..exe' MD5: 5C9C7F90AE087C40601F5D6BD85CADB7)
  - Inv 0110617985 PO Wartsila quantiparts B.V..exe (PID: 4472 cmdline: C:\Users\user\Desktop\Inv 0110617985 PO Wartsila quantiparts B.V..exe MD5: 5C9C7F90AE087C40601F5D6BD85CADB7)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "samy@cairoshippinginternational.com",
  "Password": "NermoSamy@2006+",
  "Host": "mail.cairoshippinginternational.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.483047618.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.483047618.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000002.485981746.000000000321000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.485981746.000000000321000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: Inv 0110617985 PO Wartsila quantiparts B.V..exe PID: 4472	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.Inv 0110617985 PO Wartsila quantiparts B.V..exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.Inv 0110617985 PO Wartsila quantiparts B.V..exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

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

Malware Analysis System Evasion:

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

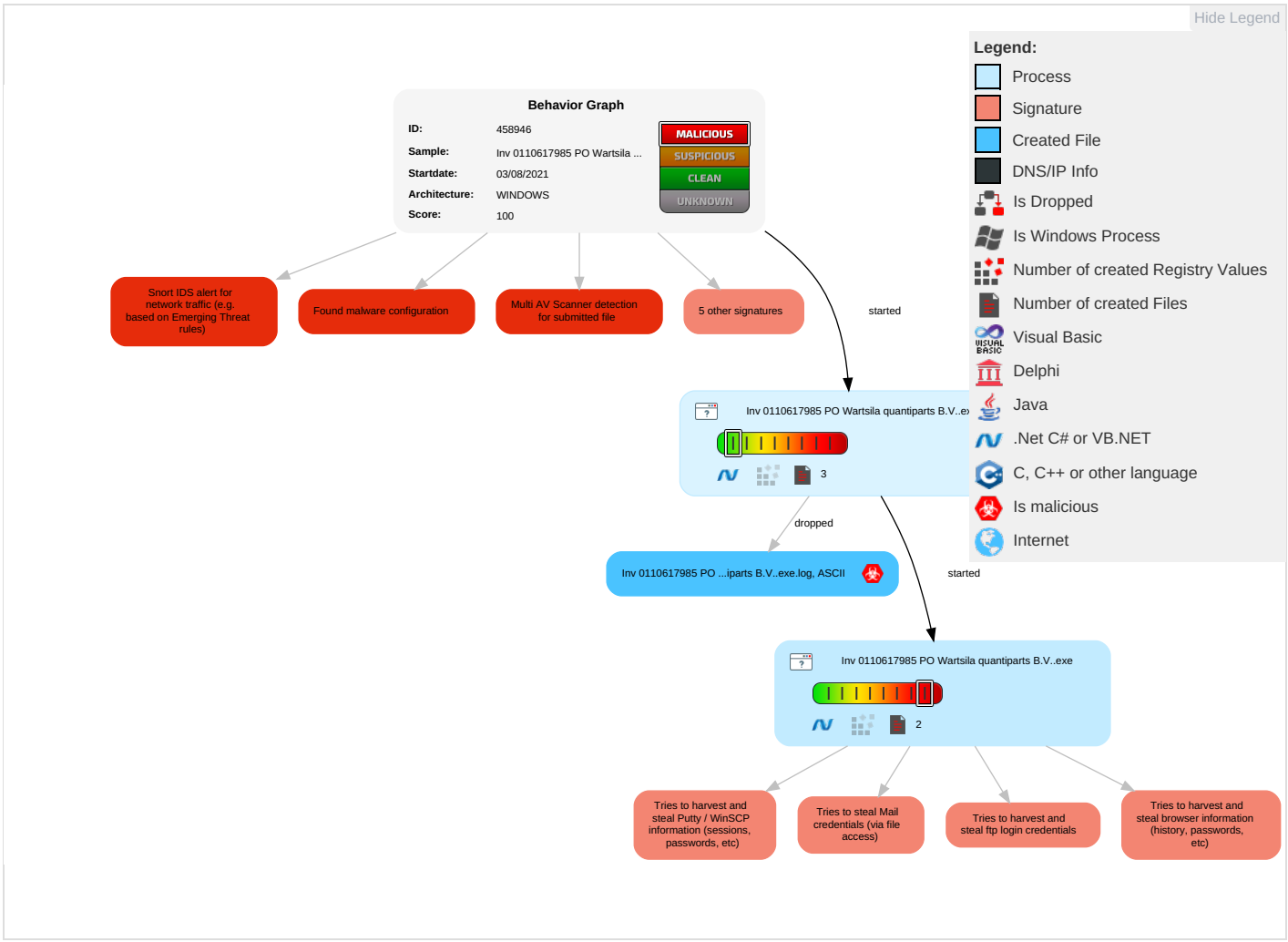
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E Ir N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	E R C
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 Local System 2	Automated Exfiltration	Steganography	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Clipboard Data 1	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	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 3	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S

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
Inv 0110617985 PO Wartsila quantiparts B.V..exe	71%	Virustotal		Browse
Inv 0110617985 PO Wartsila quantiparts B.V..exe	49%	Metadefender		Browse
Inv 0110617985 PO Wartsila quantiparts B.V..exe	86%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Inv 0110617985 PO Wartsila quantiparts B.V..exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.Inv 0110617985 PO Wartsila quantiparts B.V..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://https://2ldxNK2U0Dyorw0.org	0%	Avira URL Cloud	safe	
http://kgXKqA.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:	458946
Start date:	03.08.2021
Start time:	22:20:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Inv 0110617985 PO Wartsila quantiparts B.V..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:	24
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@0/0
EGA Information:	Failed
HDC Information:	Failed

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
22:22:29	API Interceptor	585x Sleep call for process: Inv 0110617985 PO Wartsila quantiparts B.V..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\Inv 0110617985 PO Wartsila quantiparts B.V..exe.log	
Process:	C:\Users\user\Desktop\Inv 0110617985 PO Wartsila quantiparts B.V..exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Inv 0110617985 PO Wartsila quantiparts B.V..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):	7.565991695094325
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:	Inv 0110617985 PO Wartsila quantiparts B.V..exe
File size:	1315328
MD5:	5c9c7f90ae087c40601f5d6bd85cadb7
SHA1:	15a76b5c5d5ee677f33b76a8371054821c6f6522
SHA256:	2e4901e09f9e7e72b65f301113d5bb075576e02fee03eb8414a986a1cca63cbb
SHA512:	79b82f4867e04356cd8717dee05b993814832d01ebf4f02ec6ec6227e9517a8cdfb960d7a1001f933c37b545fc2e03cb60210ecfc04aed5e19f60e2c3c35395d
SSDEEP:	24576:1sXS/d3NKzksHks2y8jf4HVy9YvHHaWTojUylbD8N6ZNuZ:bKaw1QWTZbIN6ZNu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....I.a.....P.....%... ...@....@.. .....@.....

File Icon

Icon Hash:	d8b4e6c6d8d8f2dc

Static PE Info

General

Entrypoint:	0x5125ba
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:	0x61024914 [Thu Jul 29 06:22:12 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1105c0	0x110600	False	0.868828698658	data	7.71885600168	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x114000	0x307a8	0x30800	False	0.404905968106	data	5.84479226844	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x146000	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

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Inv 0110617985 PO Wartsila quantiparts B.V..exe PID: 1236 Parent PID: 5544

General

Start time:	22:22:09
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Inv 0110617985 PO Wartsila quantiparts B.V..exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Inv 0110617985 PO Wartsila quantiparts B.V..exe'
Imagebase:	0xd00000
File size:	1315328 bytes
MD5 hash:	5C9C7F90AE087C40601F5D6BD85CADB7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Inv 0110617985 PO Wartsila quantiparts B.V..exe PID: 4472 Parent PID: 1236

General

Start time:	22:22:29
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Inv 0110617985 PO Wartsila quantiparts B.V..exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Inv 0110617985 PO Wartsila quantiparts B.V..exe
Imagebase:	0xe20000
File size:	1315328 bytes
MD5 hash:	5C9C7F90AE087C40601F5D6BD85CADB7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.483047618.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.483047618.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.485981746.0000000003211000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.485981746.0000000003211000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis