

# Virtual Analyzer Report



## Submission Context

Logged	2021-01-24 20:18:12
Submitter	Manual Submission
Type	GZIP archive

## Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	TrojanSpy.Win32.AVEMARIA.AASM		
Exploited vulnerabilities	-		
Analyzed objects	GZIP archive	1 - DHL Tracking receipt.gz	65D2935EFCa27E3235D5B8D139A9BEDBF048D804
	Windows 32-bit EXE file	1.1 - DHL Tracking receipt.exe	95E6673E5391E2BD6C1F084C4EC2436A64D68F48

## Analysis Environments

	Win2012_Office
Anti-security, self-preservation	✓
Autostart or other system reconfiguration	
Deception, social engineering	
File drop, download, sharing, or replication	
Hijack, redirection, or data theft	✓
Malformed, defective, or with known malware trails	✓
Process, service, or memory object change	✓
Rootkit, cloaking	
Suspicious network or messaging activity	

## Win2012\_Office

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TrojanSpy.Win32.AVEMARIA.AASM
Exploited vulnerabilities	-
Network connection	No network

### Object 1 - DHL Tracking receipt.gz (GZIP archive)

File name	DHL Tracking receipt.gz
File type	GZIP archive
SHA-1	65D2935EFCa27E3235D5B8D139A9BEDBF048D804
SHA-256	81D860BBE409BFF8E22C71D33C856013ED70E080240B79709EEA7A35D57A26C7
MD5	2E4DD3DDA2245041BF3B5A8F98A62B83
Size	376685 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

### Object 1.1 - DHL Tracking receipt.exe (Windows 32-bit EXE file)

File name	DHL Tracking receipt.exe
File type	Windows 32-bit EXE file
SHA-1	95E6673E5391E2BD6C1F084C4EC2436A64D68F48
SHA-256	045C0E5635C5639593D56F6B5A33C54B011A55AC121DA44EA80CADD894ADF5B6
MD5	E47F96576C73B11A58BC50DF5CB44FBB
Size	439808 byte(s)

Risk Level	High risk
Detection	TrojanSpy.Win32.AVEMARIA.AASM
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Hijack, redirection, or data theft (5) Malformed, defective, or with known malware trails (1) Process, service, or memory object change (3)

## Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics	
Execution	Windows Management Instrumentation	<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3, 4, 5
	Execution through API	<div><div></div><div></div><div></div></div> Characteristics:	1
Defense Evasion	Software Packing	<div><div></div><div></div><div></div></div> Characteristics:	1
Discovery	System Information Discovery	<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3, 4, 5

© ATT&CK™ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (1)

Characteristic	Significance	Details
Uses suspicious packer	<div><div></div><div></div><div></div></div>	File Name: %WorkingDir%\DHL Tracking receipt.exe Packer: UNKNOWN

▼ Hijack, redirection, or data theft (5)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2784 Info: Obtains processorID from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2784 Info: Obtains __PATH from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2784 Info: Obtains __GENUS from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2784 Info: Obtains __CLASS from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2784 Info: Obtains SerialNumber from API result

▼ Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as known malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: TrojanSpy.Win32.AVEMARIA.AASM Engine Version: 12.500.1004 Malware Pattern Version: 16.495.92

▼ Process, service, or memory object change (3)

Characteristic	Significance	Details
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2784 Image Path: %WorkingDir%\DHL Tracking receipt.exe
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2712 Image Path: %WorkingDir%\DHL Tracking receipt.exe Shell Command: "%WorkingDir%\DHL Tracking receipt.exe"
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2712 Injected API: SetThreadContext Target Process ID: 2784 Target Image Path: %WorkingDir%\DHL Tracking receipt.exe

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
go.microsoft.com	-	53	-	No risk	-	DHL Tracking receipt.exe
www.bing.com	-	53	-	No risk	-	DHL Tracking receipt.exe
clients2.google.com	-	53	-	No risk	-	DHL Tracking receipt.exe

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	95E6673E5391E2BD6C1F084C4EC2436A64D68F48	High

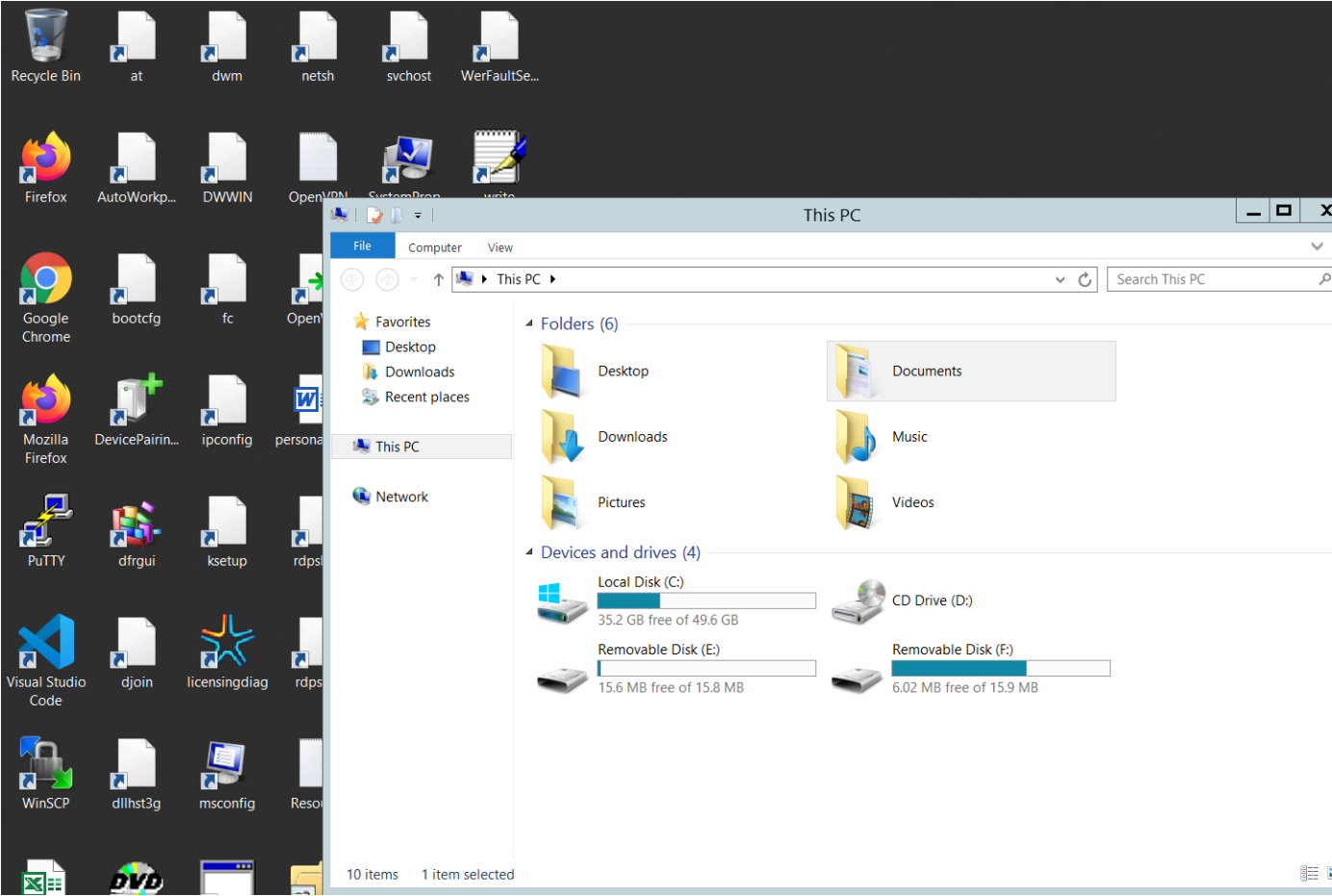
▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TrojanSpy.Win32.AVEMARIA.AASM Engine Version: 12.500.1004 Malware Pattern Version: 16.495.92		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\DHL Tracking receipt.exe Packer: UNKNOWN		
Call Process API	API Name: CreateProcessW Args: ( %WorkingDir%\DHL Tracking receipt.exe, "%WorkingDir%\DHL Tracking receipt.exe", , , , CREATE_SUSPENDED, , , , Process:2784:%WorkingDir%\DHL Tracking receipt.exe ) Return: 1		2712
Detection	Threat Characteristic: Creates process Process ID: 2712 Image Path: %WorkingDir%\DHL Tracking receipt.exe Shell Command: "%WorkingDir%\DHL Tracking receipt.exe"		

















Call Thread API	API Name: SetThreadContext Args: ( Process Name:2784:%WorkingDir%DHL Tracking receipt.exe ) Return: 1		2712
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2712 Injected API: SetThreadContext Target Process ID: 2784 Target Image Path: %WorkingDir%DHL Tracking receipt.exe		
Detection	Threat Characteristic: Creates process Process ID: 2784 Image Path: %WorkingDir%DHL Tracking receipt.exe		
Call System API	API Name: CryptExportKey Args: ( 4be938, 0, 6, 0, 0, 36be60 ) Return: 1	2712	2784
Call WMI API	API Name: IWbemLevel1Login::NTLMLLogin Args: ( \\.\root\cimv2, en-US,en, 0, 542da60, 5c7eb64 ) Return: 0	2712	2784
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( \\.\root\cimv2, NULL, NULL, NULL, 0, NULL, 0, 5c7eb64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_BaseBoard::Get Args: ( SerialNumber, 0, NIUIX0SX0LPX8F, 8, 0 ) Return: 0	2712	2784
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2784 Info: Obtains SerialNumber from API result		
Call WMI API	API Name: IWbemLevel1Login::NTLMLLogin Args: ( \\.\root\cimv2, en-US,en, 0, 542cee0, 36eef8 ) Return: 0	2712	2784
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( \\.\root\cimv2, NULL, NULL, , 80, , 0, 36eef8 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_Processor::Get Args: ( __PATH, 0, \\Win-Lena\ROOT\cimv2:Win32_Processor, 8, 64 ) Return: 0	2712	2784
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2784 Info: Obtains __PATH from API result		
Call WMI API	API Name: Win32_Processor::Get Args: ( __CLASS, 0, Win32_Processor, 8, 64 ) Return: 0	2712	2784
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2784 Info: Obtains __CLASS from API result		
Call WMI API	API Name: Win32_Processor::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2784 Info: Obtains __GENUS from API result		
Call WMI API	API Name: Win32_Processor::Get Args: ( __PATH, 0, \\Win-Lena\root\cimv2:Win32_Processor.DeviceID="CPU0", 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_Processor::Get Args: ( processorID, 0, 1, 8, 32 ) Return: 0	2712	2784
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2784 Info: Obtains processorID from API result		
Call WMI API	API Name: Win32_Processor::Get Args: ( processorID, 0, 1, 8, 32 ) Return: 0	2712	2784
Call WMI API	API Name: IWbemLevel1Login::NTLMLLogin Args: ( \\.\root\cimv2, en-US,en, 0, 542cee0, 36eef8 ) Return: 0	2712	2784
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( \\.\root\cimv2, NULL, NULL, , 80, , 0, 36eef8 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\ROOT\cimv2:Win32_NetworkAdapterConfiguration, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __CLASS, 0, Win32_NetworkAdapterConfiguration, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=0, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=1, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=2, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=3, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=4, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=5, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=6, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=7, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784

Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\\root\\cimv2:Win32_NetworkAdapterConfiguration.Index=8, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\\root\\cimv2:Win32_NetworkAdapterConfiguration.Index=9, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\\root\\cimv2:Win32_NetworkAdapterConfiguration.Index=10, 8, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, -1, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, -1, 11, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( MacAddress, 0, 9C:DA:3E:35:D2:E3, 8, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( MacAddress, 0, 9C:DA:3E:35:D2:E3, 8, 0 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	2712	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\Win-Lena\\root\\cimv2:Win32_NetworkAdapterConfiguration.Index=11, 8, 64 ) Return: 0	2712	2784

▼ Screenshot



Process Graph Legend

Node		Notable Threat Characteristics	
	Submitted sample		Anti-security, self-preservation
	Root process		Autostart or other system reconfiguration
	Child process		Deception, social engineering
	Direct event		File drop, download, sharing, or replication
	Indirect event		Hijack, redirection, or data theft
	Created		Malformed, defective, or with known malware traits
	Event actions		Process, service, or memory object change
			Rootkit, cloaking
			Suspicious network or messaging activity