Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-03-20 12:45:34
Submitter	Manual Submission
Type	ISO image

Analysis Overview

Overall risk level	Low risk	The object exhibited mildly suspicious characteristics that are most likely benign.	
Detections	Possible_GENISO-6, TROJ_GEN.R002C0DC521		
Exploited vulnerabilities	-		
Analyzed objects	ISO image	1 - EUR_245.000,00.IMG	8BDFEBC464BFF0D80D7E085286305B8E2D6A7444
	Windows 32-bit EXE file	1.1 - EUR_245_.EXE	3AEF098920A566068BDD8FDB54AC80CCCD03E349

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 traits	✓
Process, service, or memory object change	✓
Rootkit, cloaking	
Suspicious network or messaging activity	✓

Win2012_Office

Environment-specific risk level	Low risk The object exhibited mildly suspicious characteristics that are most likely benign.
Detections	Possible_GENISO-6, TROJ_GEN.R002C0DC521
Exploited vulnerabilities	-
Network connection	No network

Object 1 - EUR_245.000,00.IMG (ISO image)

File name	EUR_245.000,00.IMG
File type	ISO image
SHA-1	8BDFEBC464BFF0D80D7E085286305B8E2D6A7444
SHA-256	823BE96D8CADFCCB6D5FD7707F845570286C224FDE3415207998F1137D9B8391
MD5	155E94A98420FC68F6DFC595CAEE994A
Size	1245184 byte(s)

Risk Level	Low risk
Detection	Possible_GENISO-6
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1)

Notable Threat Characteristics

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

Characteristic	Significance	Details
Detected as probable malware	■□□	Source: ATSE Detection Name: Possible_GENISO-6 Engine Version: 12.500.1008 Malware Pattern Version: 16.603.92

Analysis

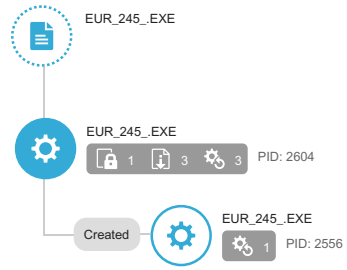
Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: Possible_GENISO-6 Engine Version: 12.500.1008 Malware Pattern Version: 16.603.92		

Object 1.1 - EUR_245_.EXE (Windows 32-bit EXE file)

File name	EUR_245_.EXE
File type	Windows 32-bit EXE file
SHA-1	3AEF098920A566068BDD8FDB54AC80CCCD03E349
SHA-256	1F8649EF7652C22785DC98DB8BCC25F61FB9C209D2F09D00E9FA2EE1FDC03FDE
MD5	BFEF5F44827C90C231863C38FD5A20FF
Size	210453 byte(s)

Risk Level	Low risk
Detection	TROJ_GEN.R002C0DC521
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (2) Autostart or other system reconfiguration (1) File drop, download, sharing, or replication (3) Malformed, defective, or with known malware traits (3) Process, service, or memory object change (4) Suspicious network or messaging activity (2)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1, 2
	Execution through Module Load	Characteristics: 1
Defense Evasion	Software Packing	Characteristics: 1
	File Deletion	Characteristics: 1, 2
Discovery	Process Discovery	Characteristics: 1

Notable Threat Characteristics

Anti-security, self-preservation (2)

Characteristic	Significance	Details
Attempts to detect active running processes		Process ID: 2604 Info: enum processes
Uses suspicious packer		File Name: %WorkingDir%\EUR_245_.EXE Packer: UNKNOWN

Autostart or other system reconfiguration (1)

Characteristic	Significance	Details
Modifies file that can be used to infect systems		%TEMP%\nsf3312.tmp\cuy8ji6yaul6f7b.dll

File drop, download, sharing, or replication (3)

Characteristic	Significance	Details
Drops executable during installation		Dropping Process ID: 2604 File: %TEMP%\nsf3312.tmp\cuy8ji6yaul6f7b.dll Type: VSDT_DLL_W32
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2604 File: %TEMP%\nsf3312.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2604 File: %TEMP%\nsf3311.tmp Type: VSDT_EMPTY

Malformed, defective, or with known malware traits (3)

Characteristic	Significance	Details
Detected as probable malware		Source: ATSE Detection Name: TROJ_GEN.R002C0DC521 Engine Version: 12.500.1008 Malware Pattern Version: 16.603.92
Drops probable malware		Source: ATSE Detection Name: TROJ_GEN.R002C0DC521 File Name: cuy8ji6yaul6f7b.dll SHA1: 4333EC8A274ACB2B335DBF006028FB9B05EA7E60 Engine Version: 12.500.1008 Malware Pattern Version: 16.605.92
Rare executable file		Global Detections: 0

Process, service, or memory object change (4)

Characteristic	Significance	Details
Creates process	■□□	Process ID: 2556 Image Path: %WorkingDir%\EUR_245_.EXE
Creates process	■□□	Process ID: 2604 Image Path: %WorkingDir%\EUR_245_.EXE Shell Command: "%WorkingDir%\EUR_245_.EXE"
Resides in memory to evade detection	■□□	Injecting Process ID: 2604 Injected API: SetThreadContext Target Process ID: 2556 Target Image Path: %WorkingDir%\EUR_245_.EXE
Uses Windows module loader to load dropped DLLs and execute code	■□□	Process ID: 2604 File: %TEMP%\nsf3312.tmp\cuy8ji6yaul6f7b.dll

Suspicious network or messaging activity (2)

Characteristic	Significance	Details
Attempts to connect to suspicious host	■□□	www.grantoutpost.com
Attempts to connect to suspicious host	■□□	www.vaccinn.com

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.grantoutpost.com	-	53	-	-	-	EUR_245_.EXE
go.microsoft.com	-	53	-	No risk	-	EUR_245_.EXE
self.events.data.microsoft.com	-	53	-	No risk	-	EUR_245_.EXE
www.vaccinn.com	-	53	-	-	-	EUR_245_.EXE
www.msftncsi.com	-	53	-	No risk	-	EUR_245_.EXE
www.bing.com	-	53	-	No risk	-	EUR_245_.EXE

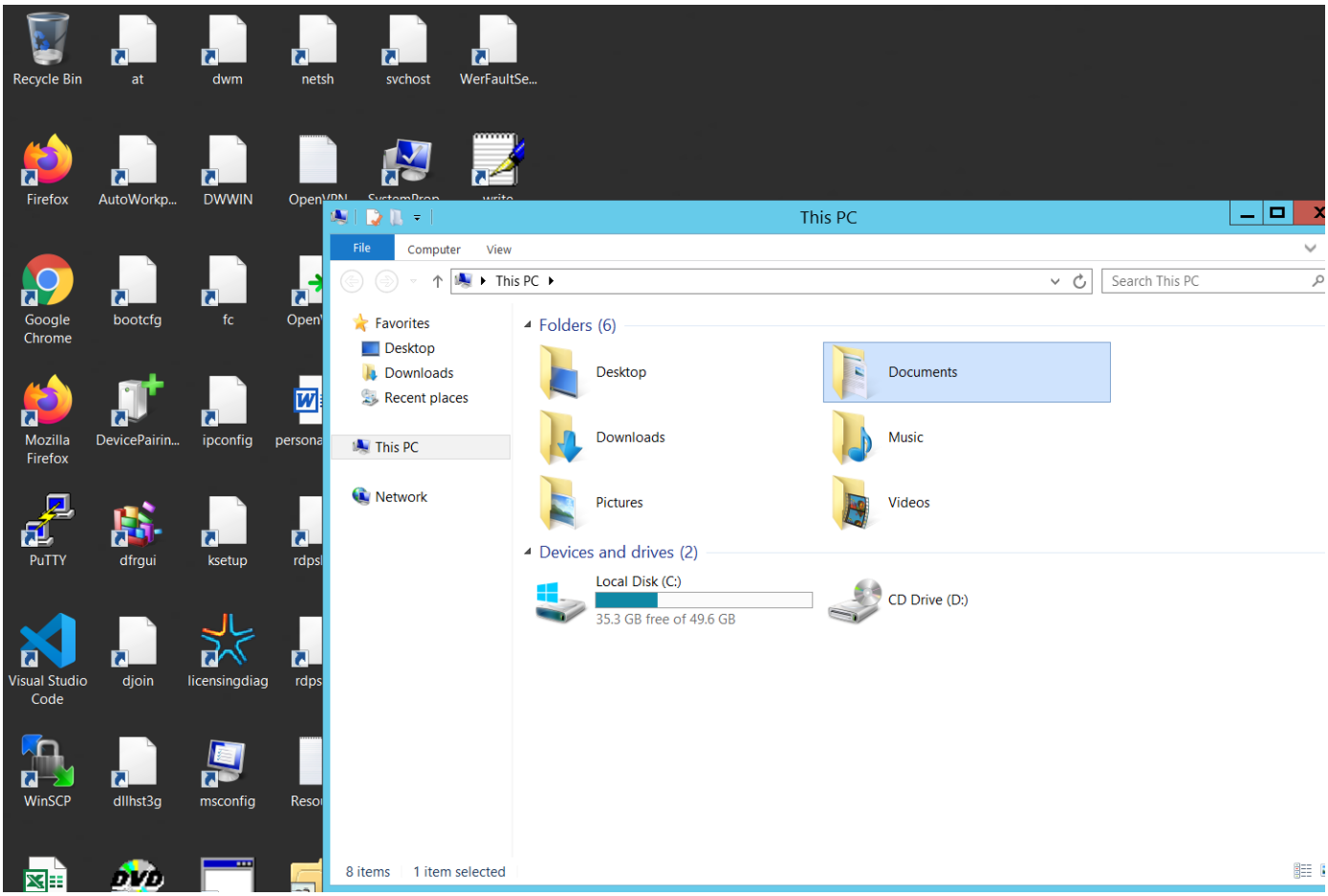
Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
nsf3312.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
cuy8ji6yaul6f7b.dll	Low	TROJ_GEN.R002C0DC521	Drops probable malware	-	175104	4333EC8A274ACB2B335DBF006028FB9B05EA7E60
nsf3311.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host www.grantoutpost.com		
Detection	Threat Characteristic: Attempts to connect to suspicious host www.vaccinn.com		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0DC521 Engine Version: 12.500.1008 Malware Pattern Version: 16.603.92		
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0DC521 File Name: cuy8ji6yaul6f7b.dll SHA1: 4333EC8A274ACB2B335DBF006028FB9B05EA7E60 Engine Version: 12.500.1008 Malware Pattern Version: 16.605.92		
Detection	Threat Characteristic: Rare executable file Global Detections: 0		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\EUR_245_.EXE Packer: UNKNOWN		
Delete File	Path: %TEMP%\nsf3311.tmp Type: VSDT_EMPTY		2604
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2604 File: %TEMP%\nsf3311.tmp Type: VSDT_EMPTY		
Delete File	Path: %TEMP%\nsf3312.tmp Type: VSDT_EMPTY		2604
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2604 File: %TEMP%\nsf3312.tmp Type: VSDT_EMPTY		
Add File	Path: %TEMP%\nsf3312.tmp\cuy8ji6yaul6f7b.dll Type: VSDT_DLL_W32		2604
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2604 File: %TEMP%\nsf3312.tmp\cuy8ji6yaul6f7b.dll Type: VSDT_DLL_W32		
Write File	Path: %TEMP%\nsf3312.tmp\cuy8ji6yaul6f7b.dll Type: VSDT_DLL_W32		2604
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\nsf3312.tmp\cuy8ji6yaul6f7b.dll		
Call System API	API Name: LdrLoadDll Args: (9, 0, %TEMP%\nsf3312.tmp\cuy8ji6yaul6f7b.dll, 10000000) Return: 0		2604
Detection	Threat Characteristic: Uses Windows module loader to load dropped DLLs and execute code Process ID: 2604 File: %TEMP%\nsf3312.tmp\cuy8ji6yaul6f7b.dll		
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 564) Return: 1		2604
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2604 Info: enum processes		
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 564) Return: 1		2604
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 564) Return: 1		2604
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 564) Return: 1		2604
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\EUR_245_.EXE, "%WorkingDir%\EUR_245_.EXE", , , , CREATE_SUSPENDED, , , , Process:2556:%WorkingDir%\EUR_245_.EXE) Return: 1		2604
Detection	Threat Characteristic: Creates process Process ID: 2604 Image Path: %WorkingDir%\EUR_245_.EXE Shell Command: "%WorkingDir%\EUR_245_.EXE"		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2556:%WorkingDir%\EUR_245_.EXE) Return: 1		2604
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2604 Injected API: SetThreadContext Target Process ID: 2556 Target Image Path: %WorkingDir%\EUR_245_.EXE		
Detection	Threat Characteristic: Creates process Process ID: 2556 Image Path: %WorkingDir%\EUR_245_.EXE		

▼ **Screenshot**



Process Graph Legend

Node

- Submitted sample
- Root process
- Child process
- Direct event
- Indirect event
- Created — Event actions

Notable Threat Characteristics

- 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 traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity