Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-03-20 12:46:52
Submitter	Manual Submission
Type	ZIP archive

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	TROJ_GEN.R06CC0DCE21		
Exploited vulnerabilities	-		
Analyzed objects	ZIP archive	1 - Telex_Invoice_00000000000000000980.zip	FD7D5F5F1391E21B636EF65BF89110B92A6DDF5E
	MSIL Portable executable	1.1 - Telex_Invoice_00000000000000000980.exe	2C9DBDF78703FEFCAA0ADF7F03F8420501ACCDE7

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	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_GEN.R06CC0DCE21
Exploited vulnerabilities	-
Network connection	No network

▼ Object 1 - Telex_Invoice_00000000000000000980.zip (ZIP archive)

File name	Telex_Invoice_00000000000000000980.zip
File type	ZIP archive
SHA-1	FD7D5F5F1391E21B636EF65BF89110B92A6DDF5E
SHA-256	469356A92A1A3815B4ACC5834F5B442BC16413E70C64CDA2384CA785ACCB53B3
MD5	B1A0A7C3777A1F48471873443FFFBAE0
Size	587612 byte(s)

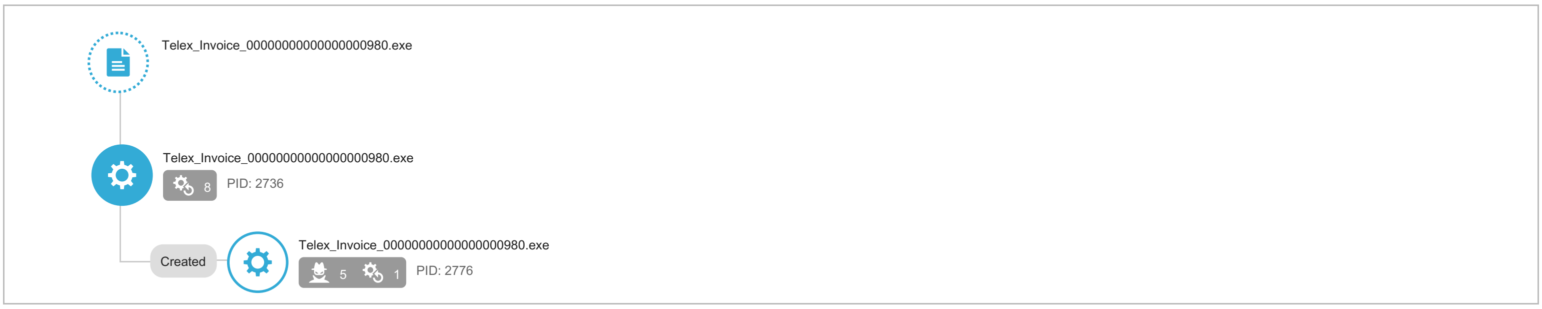
Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

▼ Object 1.1 - Telex_Invoice_00000000000000000980.exe (MSIL Portable executable)

File name	Telex_Invoice_00000000000000000980.exe
File type	MSIL Portable executable
SHA-1	2C9DBDF78703FEFCAA0ADF7F03F8420501ACCDE7
SHA-256	63F0470BBAA42581F6D4C046B3AA72B43AD39A42BB73A83FF5ABEEDB13993537
MD5	1BA3D38261591A93ED9693E1F9E7168E
Size	748032 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.R06CC0DCE21
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Hijack, redirection, or data theft (5) Malformed, defective, or with known malware traits (2) Process, service, or memory object change (9)

Process Graph


Telex_Invoice_00000000000000000980.exe
Telex_Invoice_00000000000000000980.exe
8
PID: 2736
Created
Telex_Invoice_00000000000000000980.exe
5
1
PID: 2776

? Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics		
Execution	Windows Management Instrumentation	🟥⬜⬜	Characteristics:	1, 2, 3, 4, 5
	Execution through API	🟥⬜⬜	Characteristics:	1
Privilege Escalation	Process Injection	🟥🟥⬜ 🟥⬜⬜	Characteristics: Characteristics:	1, 2 1, 2
Defense Evasion	Software Packing	🟥⬜⬜	Characteristics:	1
	Process Injection	🟥🟥⬜ 🟥⬜⬜	Characteristics: Characteristics:	1, 2 1, 2
	Process Hollowing	🟥⬜⬜	Characteristics:	1
Discovery	System Information Discovery	🟥⬜⬜	Characteristics:	1, 2, 3, 4, 5

Notable Threat Characteristics

Anti-security, self-preservation (1)

Characteristic	Significance	Details
Uses suspicious packer	🟥⬜⬜	File Name: %WorkingDir%\Telex_Invoice_00000000000000000980.exe Packer: UNKNOWN

Hijack, redirection, or data theft (5)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2776 Info: Obtains processorID from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2776 Info: Obtains __PATH from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2776 Info: Obtains __GENUS from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2776 Info: Obtains __CLASS from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2776 Info: Obtains SerialNumber from API result

Malformed, defective, or with known malware traits (2)

Characteristic	Significance	Details
Detected as probable malware	🟥⬜⬜	Source: ATSE Detection Name: TROJ_GEN.R06CC0DCE21 Engine Version: 12.500.1008 Malware Pattern Version: 16.605.92
Rare executable file	🟥⬜⬜	Global Detections: 0

Process, service, or memory object change (9)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2776 Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe
Creates process	🟥⬜⬜	Process ID: 2736 Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe Shell Command:
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2736 Injected API: WriteProcessMemory Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2736 Injected API: SetThreadContext Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2736 Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe Injected Address: 0x0
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2736 Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe Injected Content:
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2736 Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe Injected Content: .t.
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 2736 Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe Injected Content: MZ.
Injects memory with dropped files	🟥⬜⬜	Injecting Process ID: 2736 Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe File: MZ.

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
self.events.data.microsoft.com	-	53	-	No risk	-	Telex_Invoice_00000000000000000980.exe
www.msftncsi.com	-	53	-	No risk	-	Telex_Invoice_00000000000000000980.exe
go.microsoft.com	-	53	-	No risk	-	Telex_Invoice_00000000000000000980.exe
www.bing.com	-	53	-	No risk	-	Telex_Invoice_00000000000000000980.exe

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	2C9DBDF78703FEFCAA0ADF7F03F8420501ACCDE7	High

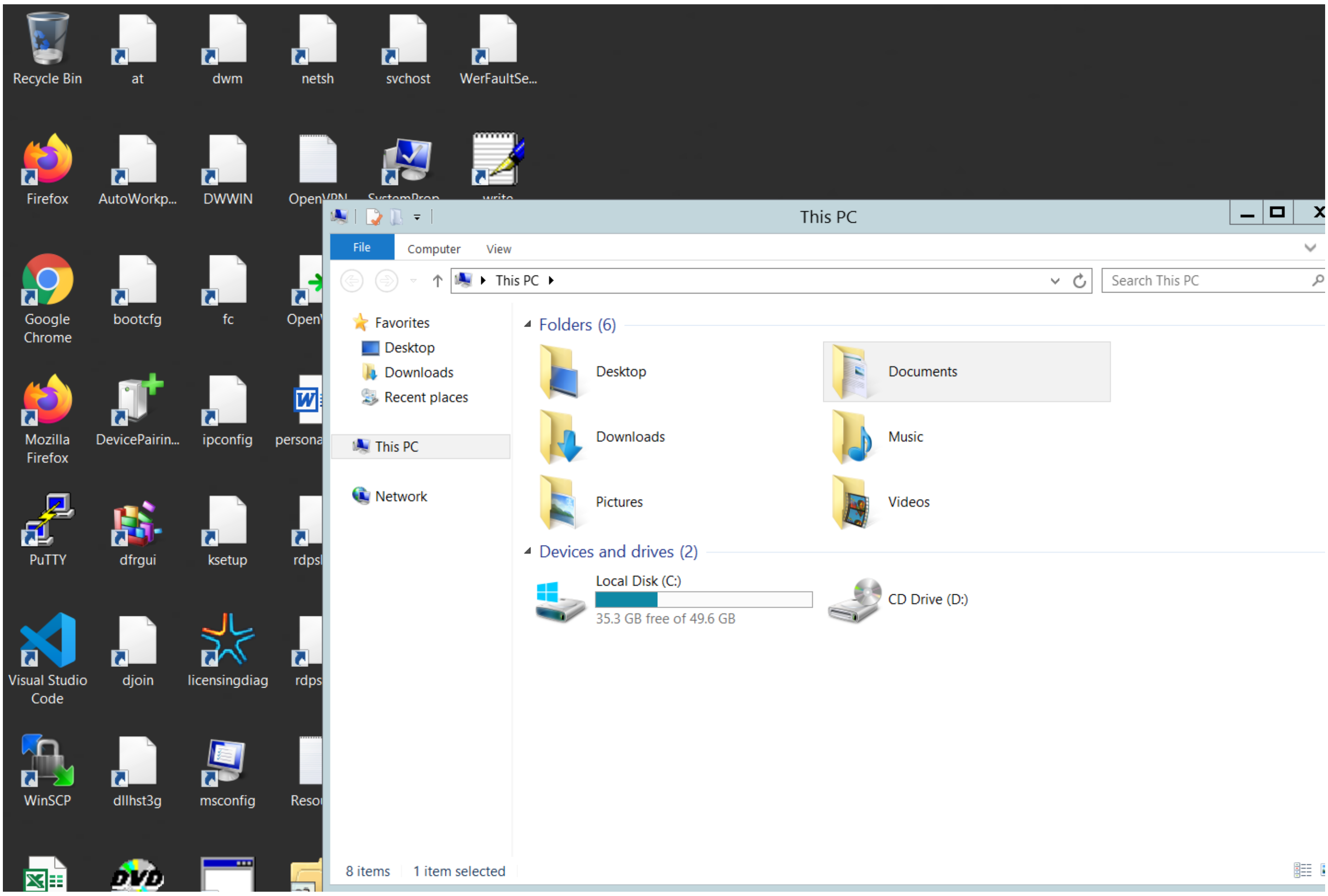
▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R06CC0DCE21 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%\Telex_Invoice_00000000000000000980.exe Packer: UNKNOWN		
Call System API	API Name: CryptExportKey Args: (8e5458, 0, 6, 0, 0, 6dbbd0) Return: 1		2736
Call System API	API Name: System.Convert::FromBase64String Args: (0D8pwTTIN7Fc7EfZx9+lXSMv+U2+4pH3xnPGb/NS22KKGG+JahkcT67oumew/rBDqaxLzz4vRgi0VoI0BNRmrDqWNEEZsHA5pE6/gS6r25zaDStDhwvmyIUDuIoQK5MA...) Return: D03F29C134E537B1...		2736
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2736
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2736
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\Telex_Invoice_00000000000000000980.exe, , , , , CREATE_SUSPENDED, , , , Process:2776:%WorkingDir%\Telex_Invoice_00000000000000000980.exe) Return: 1		2736
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2736 Injected API: WriteProcessMemory Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe		
Detection	Threat Characteristic: Creates process Process ID: 2736 Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2776:%WorkingDir%\Telex_Invoice_00000000000000000980.exe, 400000, MZ., 512, 6dd7a8) Return: 1		2736
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2736 Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2736 Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2776:%WorkingDir%\Telex_Invoice_00000000000000000980.exe, 402000, .t., 218624, 6dd7a8) Return: 1		2736
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2736 Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe Injected Content: .t.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2776:%WorkingDir%\Telex_Invoice_00000000000000000980.exe, 438000, , 1024, 6dd7a8) Return: 1		2736
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2736 Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2776:%WorkingDir%\Telex_Invoice_00000000000000000980.exe, 43a000, , 512, 6dd7a8) Return: 1		2736
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7ed9e000 Process:2776:%WorkingDir%\Telex_Invoice_00000000000000000980.exe, 7ed9e008, , 4, 6dd7a8) Return: 1		2736
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2736 Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2776:%WorkingDir%\Telex_Invoice_00000000000000000980.exe) Return: 1		2736
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2736 Injected API: SetThreadContext Target Process ID: 2776 Target Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2776,) Return: ?		2736
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2776], ppid[2736) Return: 1		2736

Detection	Threat Characteristic: Creates process Process ID: 2776 Image Path: %WorkingDir%\Telex_Invoice_00000000000000000980.exe		
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 5f011d8, edf1a4) Return: 0	2736	2776
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, NULL, 0, NULL, 0, edf1a4) Return: 0	2736	2776
Call WMI API	API Name: Win32_BaseBoard::Get Args: (SerialNumber, 0, NIUIX0SX0LPX8F, 8, 0) Return: 0	2736	2776
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2776 Info: Obtains SerialNumber from API result		
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 5f01758, 68af058) Return: 0	2736	2776
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, , 80, , 0, 68af058) Return: 0	2736	2776
Call WMI API	API Name: Win32_Processor::Get Args: (__PATH, 0, \\Win-Lena\ROOT\cimv2:Win32_Processor, 8, 64) Return: 0	2736	2776
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2776 Info: Obtains __PATH from API result		
Call WMI API	API Name: Win32_Processor::Get Args: (__CLASS, 0, Win32_Processor, 8, 64) Return: 0	2736	2776
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2776 Info: Obtains __CLASS from API result		
Call WMI API	API Name: Win32_Processor::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2776 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	2736	2776
Call WMI API	API Name: Win32_Processor::Get Args: (processorID, 0, 1, 8, 32) Return: 0	2736	2776
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2776 Info: Obtains processorID from API result		
Call WMI API	API Name: Win32_Processor::Get Args: (processorID, 0, 1, 8, 32) Return: 0	2736	2776
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 5f01758, 69ff0d8) Return: 0	2736	2776
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, , 80, , 0, 69ff0d8) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\ROOT\cimv2:Win32_NetworkAdapterConfiguration, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__CLASS, 0, Win32_NetworkAdapterConfiguration, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=0, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=1, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=2, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=3, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=4, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=5, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=6, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=7, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=8, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776

Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=9, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=10, 8, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, -1, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, -1, 11, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (MacAddress, 0, 9C:DA:3E:35:D2:E3, 8, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (MacAddress, 0, 9C:DA:3E:35:D2:E3, 8, 0) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2736	2776
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=11, 8, 64) Return: 0	2736	2776

▼ 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