Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-03-20 12:49:12
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	VAN_DROPPER.UMXX		
Exploited vulnerabilities	-		
Analyzed objects	ZIP archive	1 - Shipping_Documents_000000000000098000.pdf.zip	EBC200F739C4CC9DB7DEBB15F4E11C6CA1C3CEC0
	MSIL Portable executable	1.1 - Shipping_Documents_000000000000098000.pdf.exe	FB61FD8AA9744F2539981B9D43845F881EA8169E

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	VAN_DROPPER.UMXX
Exploited vulnerabilities	-
Network connection	No network

Object 1 - Shipping_Documents_000000000000098000.pdf.zip (ZIP archive)

File name	Shipping_Documents_000000000000098000.pdf.zip
File type	ZIP archive
SHA-1	EBC200F739C4CC9DB7DEBB15F4E11C6CA1C3CEC0
SHA-256	3A6AA7E3FD4B78A75C97F8300DF6FFEAB91E174A72BBB1B5F301C5D076F97017
MD5	614021A39B7D8CF58CCC3159C4FC021D
Size	569895 byte(s)

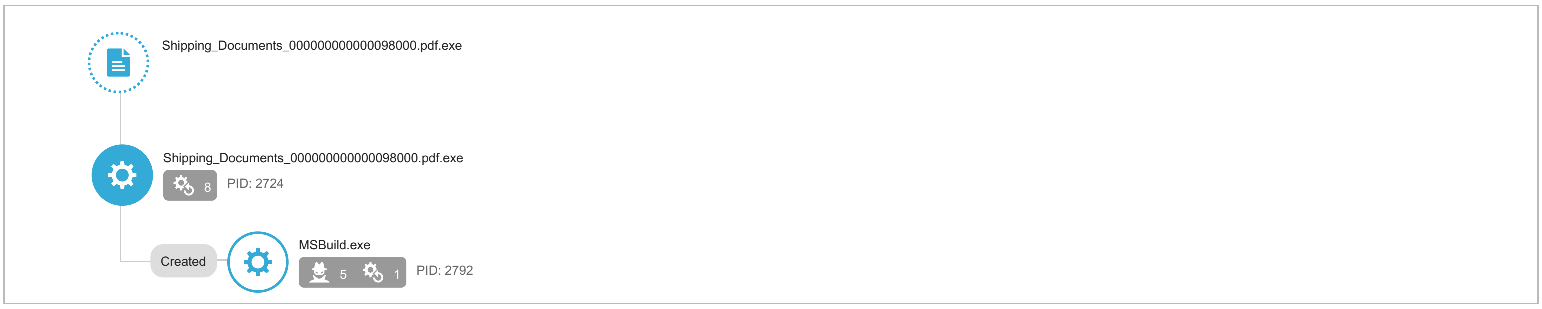
Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Object 1.1 - Shipping_Documents_000000000000098000.pdf.exe (MSIL Portable executable)

File name	Shipping_Documents_000000000000098000.pdf.exe
File type	MSIL Portable executable
SHA-1	FB61FD8AA9744F2539981B9D43845F881EA8169E
SHA-256	AEA1EEAD1914A4BCF7168D97FED9D0027640275ED4029BE99ABC1E16E236124F
MD5	645F4CDF60183443C78E5F8E1405C614
Size	726528 byte(s)

Risk Level	High risk
Detection	VAN_DROPPER.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Hijack, redirection, or data theft (5) Process, service, or memory object change (9)

Process Graph


Shipping_Documents_000000000000098000.pdf.exe
Shipping_Documents_000000000000098000.pdf.exe
8
PID: 2724
Created
MSBuild.exe
5
1
PID: 2792

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
Privilege Escalation	Process Injection	🟥🟥⬜ Characteristics: 1, 2 🟥⬜⬜ Characteristics: 1, 2
Defense Evasion	Software Packing	🟥⬜⬜ Characteristics: 1
	Process Injection	🟥🟥⬜ Characteristics: 1, 2 🟥⬜⬜ Characteristics: 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%\Shipping_Documents_000000000000098000.pdf.exe Packer: UNKNOWN

Hijack, redirection, or data theft (5)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2792 Info: Obtains processorID from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2792 Info: Obtains __PATH from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2792 Info: Obtains __GENUS from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2792 Info: Obtains __CLASS from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2792 Info: Obtains SerialNumber from API result

Process, service, or memory object change (9)

Characteristic	Significance	Details
Creates process in system directory	🟥⬜⬜	Process ID: 2792 Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2724 Injected API: WriteProcessMemory Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2724 Injected API: SetThreadContext Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2724 Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe Injected Address: 0x0
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2724 Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe Injected Content:
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2724 Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe Injected Content: .t.
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 2724 Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe Injected Content: MZ.
Injects memory with dropped files	🟥⬜⬜	Injecting Process ID: 2724 Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe File: MZ.
Converts base64 encoded strings to PE based payloads	🟥⬜⬜	Process ID: 2724 Content: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBT M0hVGhpcyBwcm9ncmFtIGNhbm5v...

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
self.events.data.microsoft.com	-	53	-	No risk	-	Shipping_Documents_000000000000098000.pdf.exe
www.msftncsi.com	-	53	-	No risk	-	Shipping_Documents_000000000000098000.pdf.exe
go.microsoft.com	-	53	-	No risk	-	Shipping_Documents_000000000000098000.pdf.exe
www.bing.com	-	53	-	No risk	-	Shipping_Documents_000000000000098000.pdf.exe

Suspicious Objects

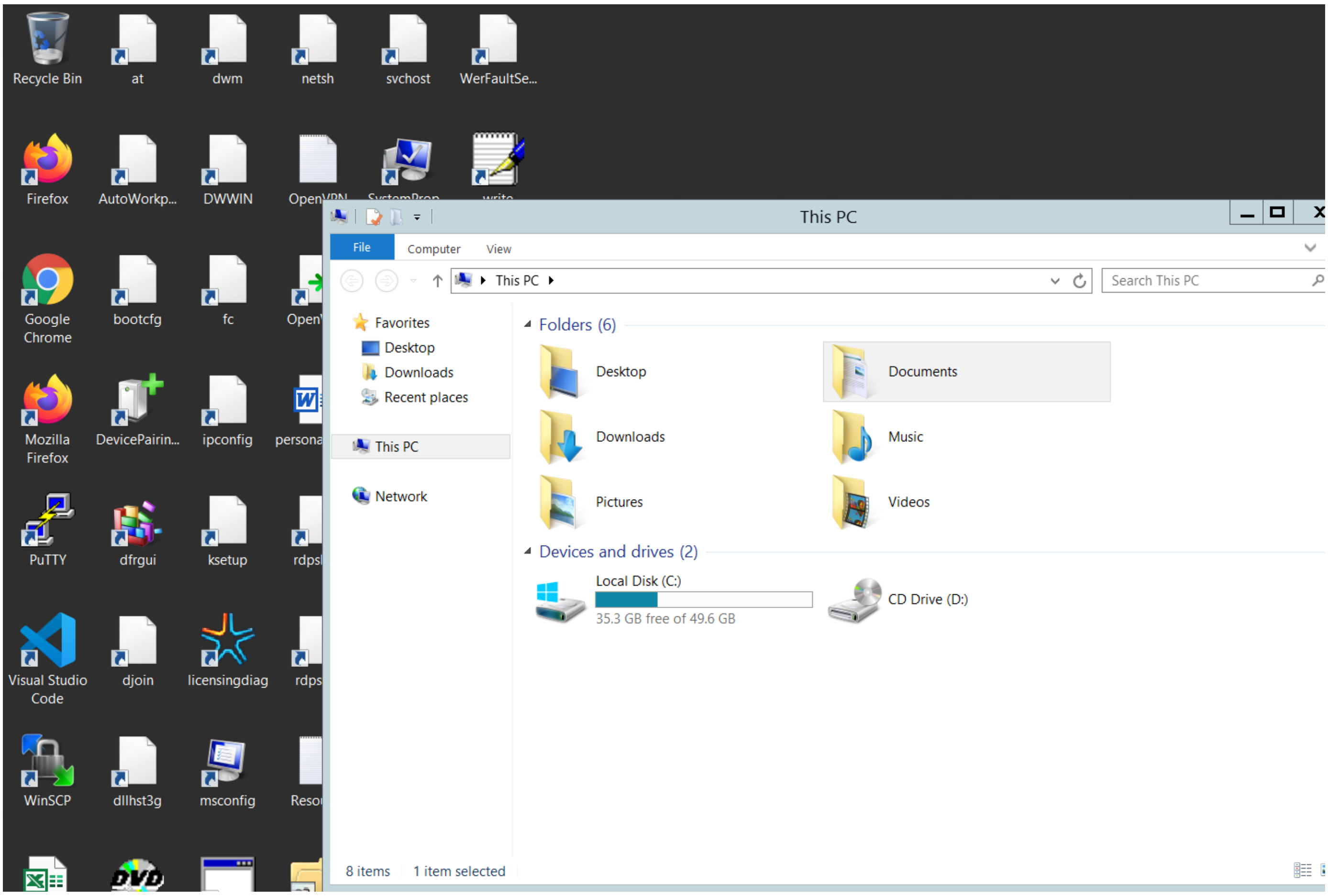
Type	Object	Risk Level
File (SHA1)	FB61FD8AA9744F2539981B9D43845F881EA8169E	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\Shipping_Documents_000000000000098000.pdf.exe Packer: UNKNOWN		
Call System API	API Name: CryptExportKey Args: (7d5600, 0, 6, 0, 0, 4fc050) Return: 1		2724
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 2883960, 8) Return: 0		2724
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 2884000, 8) Return: 0		2724
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 2884040, 8) Return: 0		2724
Call System API	API Name: System.Convert::FromBase64String Args: (TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v...) Return: 4D5A900003000000...		2724
Detection	Threat Characteristic: Converts base64 encoded strings to PE based payloads Process ID: 2724 Content: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v...		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2724
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2724
Call Process API	API Name: CreateProcessW Args: (%windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe, , , , , CREATE_SUSPENDED, , , , Process:2792:%windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe) Return: 1		2724
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2724 Injected API: WriteProcessMemory Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2792:%windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe, 400000, MZ., 512, 4fdc30) Return: 1		2724
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2724 Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2724 Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2792:%windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe, 402000, .t., 218624, 4fdc30) Return: 1		2724
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2724 Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe Injected Content: .t.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2792:%windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe, 438000, , 1024, 4fdc30) Return: 1		2724
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2724 Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2792:%windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe, 43a000, , 512, 4fdc30) Return: 1		2724
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB ff534000 Process:2792:%windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe, ff534008, , 4, 4fdc30) Return: 1		2724
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2724 Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2792:%windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe) Return: 1		2724
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2724 Injected API: SetThreadContext Target Process ID: 2792 Target Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2792,) Return: ?		2724
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2792], ppid[2724) Return: 1		2724
Detection	Threat Characteristic: Creates process in system directory Process ID: 2792 Image Path: %windir%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe		
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 6cf798, 29eb04) Return: 0	2724	2792
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, NULL, 0, NULL, 0, 29eb04) Return: 0	2724	2792
Call WMI API	API Name: Win32_BaseBoard::Get Args: (SerialNumber, 0, NIUIX0SX0LPX8F, 8, 0) Return: 0	2724	2792
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2792 Info: Obtains SerialNumber from API result		
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 6cf598, 5caf688) Return: 0	2724	2792
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, , 80, , 0, 5caf688) Return: 0	2724	2792
Call WMI API	API Name: Win32_Processor::Get Args: (__PATH, 0, \\Win-Lena\ROOT\cimv2:Win32_Processor, 8, 64) Return: 0	2724	2792
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2792 Info: Obtains __PATH from API result		

Call WMI API	API Name: Win32_Processor::Get Args: (__CLASS, 0, Win32_Processor, 8, 64) Return: 0	2724	2792
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2792 Info: Obtains __CLASS from API result		
Call WMI API	API Name: Win32_Processor::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2792 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	2724	2792
Call WMI API	API Name: Win32_Processor::Get Args: (processorID, 0, 1, 8, 32) Return: 0	2724	2792
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2792 Info: Obtains processorID from API result		
Call WMI API	API Name: Win32_Processor::Get Args: (processorID, 0, 1, 8, 32) Return: 0	2724	2792
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 6cf918, 5dff718) Return: 0	2724	2792
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, , 80, , 0, 5dff718) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\ROOT\cimv2:Win32_NetworkAdapterConfiguration, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__CLASS, 0, Win32_NetworkAdapterConfiguration, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=0, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=1, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=2, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=3, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=4, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=5, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=6, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=7, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=8, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=9, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=10, 8, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, -1, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, -1, 11, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (MacAddress, 0, 9C:DA:3E:35:D2:E3, 8, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (MacAddress, 0, 9C:DA:3E:35:D2:E3, 8, 0) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2724	2792
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=11, 8, 64) Return: 0	2724	2792

▼ 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