Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-01-29 23:59:41
Submitter	Manual Submission
Type	RAR 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	RAR archive	1 - BL-0077239753.rar	242EE496B2103D150E2CE0C010D42CCCCB9BE9AE
	MSIL Portable executable	1.1 - BL-0077239753.exe	D6093E89B7E0BB2EC94F10F2AC536DADDE139281

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 - BL-0077239753.rar (RAR archive)

File name	BL-0077239753.rar
File type	RAR archive
SHA-1	242EE496B2103D150E2CE0C010D42CCCCB9BE9AE
SHA-256	E5D9D9B09D77F9F52A538F5C58D5BE3A7A82FEC0152F19A4D533565ADE666E73
MD5	F222005811119175DC78286B82215EBD
Size	455281 byte(s)

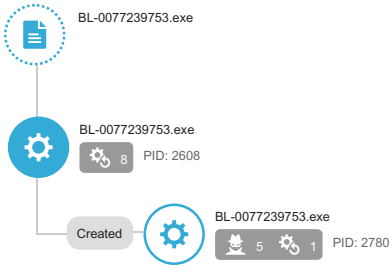
Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Object 1.1 - BL-0077239753.exe (MSIL Portable executable)

File name	BL-0077239753.exe
File type	MSIL Portable executable
SHA-1	D6093E89B7E0BB2EC94F10F2AC536DADDE139281
SHA-256	214F5B950B5D7D816F8E697F5AAAFBF9FDBB598DEDA90D30CBFDE5E5225AD9C1
MD5	3C9DE418F22DBBB95AE5F7AC3022B4DD
Size	557056 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



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: 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%\BL-0077239753.exe Packer: UNKNOWN

Hijack, redirection, or data theft (5)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information		Process ID: 2780 Info: Obtains processorID from API result
Executes commands or uses API to obtain system information		Process ID: 2780 Info: Obtains __PATH from API result
Executes commands or uses API to obtain system information		Process ID: 2780 Info: Obtains __GENUS from API result
Executes commands or uses API to obtain system information		Process ID: 2780 Info: Obtains __CLASS from API result
Executes commands or uses API to obtain system information		Process ID: 2780 Info: Obtains SerialNumber from API result

Process, service, or memory object change (9)

Characteristic	Significance	Details
Creates process		Process ID: 2780 Image Path: %WorkingDir%\BL-0077239753.exe
Creates process		Process ID: 2608 Image Path: %WorkingDir%\BL-0077239753.exe Shell Command:
Resides in memory to evade detection		Injecting Process ID: 2608 Injected API: WriteProcessMemory Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe
Resides in memory to evade detection		Injecting Process ID: 2608 Injected API: SetThreadContext Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe
Resides in memory to evade detection		Injecting Process ID: 2608 Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe Injected Address: 0x0
Resides in memory to evade detection		Injecting Process ID: 2608 Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe Injected Content:
Resides in memory to evade detection		Injecting Process ID: 2608 Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe Injected Content: .u.
Resides in memory to evade detection		Injecting Process ID: 2608 Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe Injected Content: MZ.
Injects memory with dropped files		Injecting Process ID: 2608 Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe File: MZ.

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
self.events.data.microsoft.com	-	53	-	No risk	-	BL-0077239753.exe
www.msftncsi.com	-	53	-	No risk	-	BL-0077239753.exe
go.microsoft.com	-	53	-	No risk	-	BL-0077239753.exe
www.bing.com	-	53	-	No risk	-	BL-0077239753.exe

Suspicious Objects

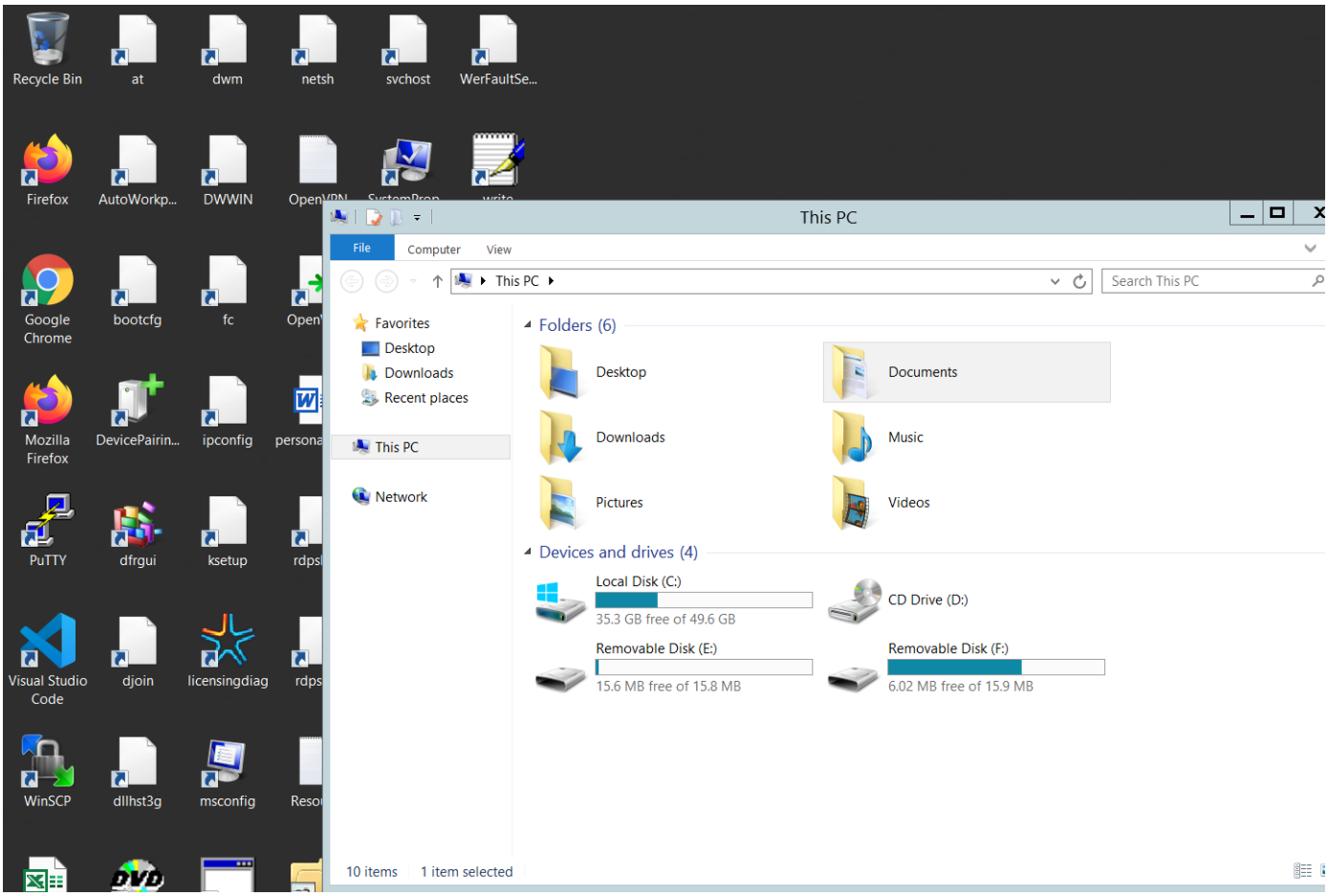
Type	Object	Risk Level
File (SHA1)	D6093E89B7E0BB2EC94F10F2AC536DADDE139281	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\BL-0077239753.exe Packer: UNKNOWN		
Call System API	API Name: CryptExportKey Args: (ae4d30, 0, 6, 0, 0, 9abe20) Return: 1		2608
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0		2608
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\BL-0077239753.exe, , , , , CREATE_SUSPENDED, , , , Process:2780:%WorkingDir%\BL-0077239753.exe) Return: 1		2608
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2608 Injected API: WriteProcessMemory Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe		
Detection	Threat Characteristic: Creates process Process ID: 2608 Image Path: %WorkingDir%\BL-0077239753.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2780:%WorkingDir%\BL-0077239753.exe, 400000, MZ., 512, 9adfac) Return: 1		2608
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2608 Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2608 Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2780:%WorkingDir%\BL-0077239753.exe, 402000, .u., 219136, 9adfac) Return: 1		2608
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2608 Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe Injected Content: .u.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2780:%WorkingDir%\BL-0077239753.exe, 438000, , 1536, 9adfac) Return: 1		2608
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2608 Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2780:%WorkingDir%\BL-0077239753.exe, 43a000, , 512, 9adfac) Return: 1		2608
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7fb1b000 Process:2780:%WorkingDir%\BL-0077239753.exe, 7fb1b008, , 4, 9adfac) Return: 1		2608
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2608 Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2780:%WorkingDir%\BL-0077239753.exe) Return: 1		2608
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2608 Injected API: SetThreadContext Target Process ID: 2780 Target Image Path: %WorkingDir%\BL-0077239753.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2780,) Return: ?		2608
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2780], ppid[2608) Return: 1		2608
Detection	Threat Characteristic: Creates process Process ID: 2780 Image Path: %WorkingDir%\BL-0077239753.exe		
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 542fcb0, 33ea64) Return: 0	2608	2780
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, NULL, 0, NULL, 0, 33ea64) Return: 0	2608	2780
Call WMI API	API Name: Win32_BaseBoard::Get Args: (SerialNumber, 0, NIUIX0SX0LPX8F, 8, 0) Return: 0	2608	2780
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2780 Info: Obtains SerialNumber from API result		
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 542f8b0, 5d4f0d8) Return: 0	2608	2780
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, , 80, , 0, 5d4f0d8) Return: 0	2608	2780
Call WMI API	API Name: Win32_Processor::Get Args: (__PATH, 0, \\Win-Lena\ROOT\cimv2:Win32_Processor, 8, 64) Return: 0	2608	2780
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2780 Info: Obtains __PATH from API result		
Call WMI API	API Name: Win32_Processor::Get Args: (__CLASS, 0, Win32_Processor, 8, 64) Return: 0	2608	2780
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2780 Info: Obtains __CLASS from API result		
Call WMI API	API Name: Win32_Processor::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2780 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	2608	2780
Call WMI API	API Name: Win32_Processor::Get Args: (processorID, 0, 1, 8, 32) Return: 0	2608	2780

Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2780 Info: Obtains processorID from API result		
Call WMI API	API Name: Win32_Processor::Get Args: (processorID, 0, 1, 8, 32) Return: 0	2608	2780
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 54303b0, 5e9f4d8) Return: 0	2608	2780
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, , 80, , 0, 5e9f4d8) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\ROOT\cimv2:Win32_NetworkAdapterConfiguration, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__CLASS, 0, Win32_NetworkAdapterConfiguration, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=0, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=1, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=2, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=3, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=4, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=5, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=6, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=7, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=8, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=9, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=10, 8, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, -1, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, -1, 11, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (MacAddress, 0, 9C:DA:3E:35:D2:E3, 8, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (MacAddress, 0, 9C:DA:3E:35:D2:E3, 8, 0) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2608	2780
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=11, 8, 64) Return: 0	2608	2780

▼ 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