Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-01-24 20:21:58
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	Trojan.Win32.MALREP.THAADBA		
Exploited vulnerabilities	-		
Analyzed objects	GZIP archive	1 - quote 2021.gz	C82CC2381DCDFEB609582972DC827620A0213BDC
	Windows 32-bit EXE file	1.1 - quote 2021.exe	FCDCBB14DFC3734017B78883DEC9BB14DCA04B56

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	Trojan.Win32.MALREP.THAADBA
Exploited vulnerabilities	-
Network connection	No network

Object 1 - quote 2021.gz (GZIP archive)

File name	quote 2021.gz
File type	GZIP archive
SHA-1	C82CC2381DCDFEB609582972DC827620A0213BDC
SHA-256	C47E0E5ED39F8985B77829071B9D06EB14EADAA0C25B0B6CC45BCC0C2491397A
MD5	624832629A637E269526FE224B20E3A7
Size	509865 byte(s)

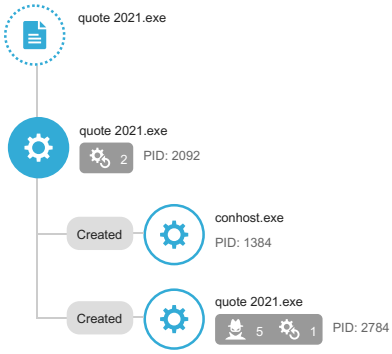
Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Object 1.1 - quote 2021.exe (Windows 32-bit EXE file)

File name	quote 2021.exe
File type	Windows 32-bit EXE file
SHA-1	FCDCBB14DFC3734017B78883DEC9BB14DCA04B56
SHA-256	AD52D6434817F1D79C061DB7DEEEE5E5A6911DB99B057340CC8089C9A2C87587
MD5	59FCC2B396BA1CE5BF5BAD893B11106B
Size	665600 byte(s)

Risk Level	High risk
Detection	Trojan.Win32.MALREP.THAADBA
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (2) Hijack, redirection, or data theft (10) Malformed, defective, or with known malware traits (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	Characteristics: 1, 2, 3, 4, 5
	Execution through API	Characteristics: 1
Defense Evasion	Software Packing	Characteristics: 1
Discovery	System Information Discovery	Characteristics: 1, 2, 3, 4, 5
Collection	Data from Local System	Characteristics: 1, 2, 3, 4, 5

Notable Threat Characteristics

Anti-security, self-preservation (1)

Characteristic	Significance	Details
Uses suspicious packer		File Name: %WorkingDir%\quote 2021.exe Packer: UNKNOWN

Autostart or other system reconfiguration (2)

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions		Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE

Hijack, redirection, or data theft (10)

Characteristic	Significance	Details
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\key3.db
Accesses decoy file		%APPDATA%\Mozilla\Firefox\profiles.ini
Accesses decoy file		%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data
Accesses decoy file		%APPDATA%\COMODO\ICEDRAGON\PROFILES.INI
Accesses decoy file		%APPDATA%\FILEZILLA\RECENTSERVERS.XML
Executes commands or uses API to obtain system information		Process ID: 2784 Info: Obtains processorID from API result
Executes commands or uses API to obtain system information		Process ID: 2784 Info: Obtains __PATH from API result
Executes commands or uses API to obtain system information		Process ID: 2784 Info: Obtains __GENUS from API result
Executes commands or uses API to obtain system information		Process ID: 2784 Info: Obtains __CLASS from API result
Executes commands or uses API to obtain system information		Process ID: 2784 Info: Obtains SerialNumber from API result

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

Characteristic	Significance	Details
Detected as known malware		Source: ATSE Detection Name: Trojan.Win32.MALREP.THAADBA Engine Version: 12.500.1004 Malware Pattern Version: 16.495.92

Process, service, or memory object change (3)

Characteristic	Significance	Details
Creates process		Process ID: 2784 Image Path: %WorkingDir%\quote 2021.exe
Creates process		Process ID: 2092 Image Path: %WorkingDir%\quote 2021.exe Shell Command: "%WorkingDir%\quote 2021.exe"
Resides in memory to evade detection		Injecting Process ID: 2092 Injected API: SetThreadContext Target Process ID: 2784 Target Image Path: %WorkingDir%\quote 2021.exe

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
self.events.data.microsoft.com	-	53	-	No risk	-	quote 2021.exe
update.googleapis.com	-	53	-	No risk	-	quote 2021.exe
go.microsoft.com	-	53	-	No risk	-	quote 2021.exe
www.bing.com	-	53	-	No risk	-	quote 2021.exe
clients2.google.com	-	53	-	No risk	-	quote 2021.exe

Suspicious Objects

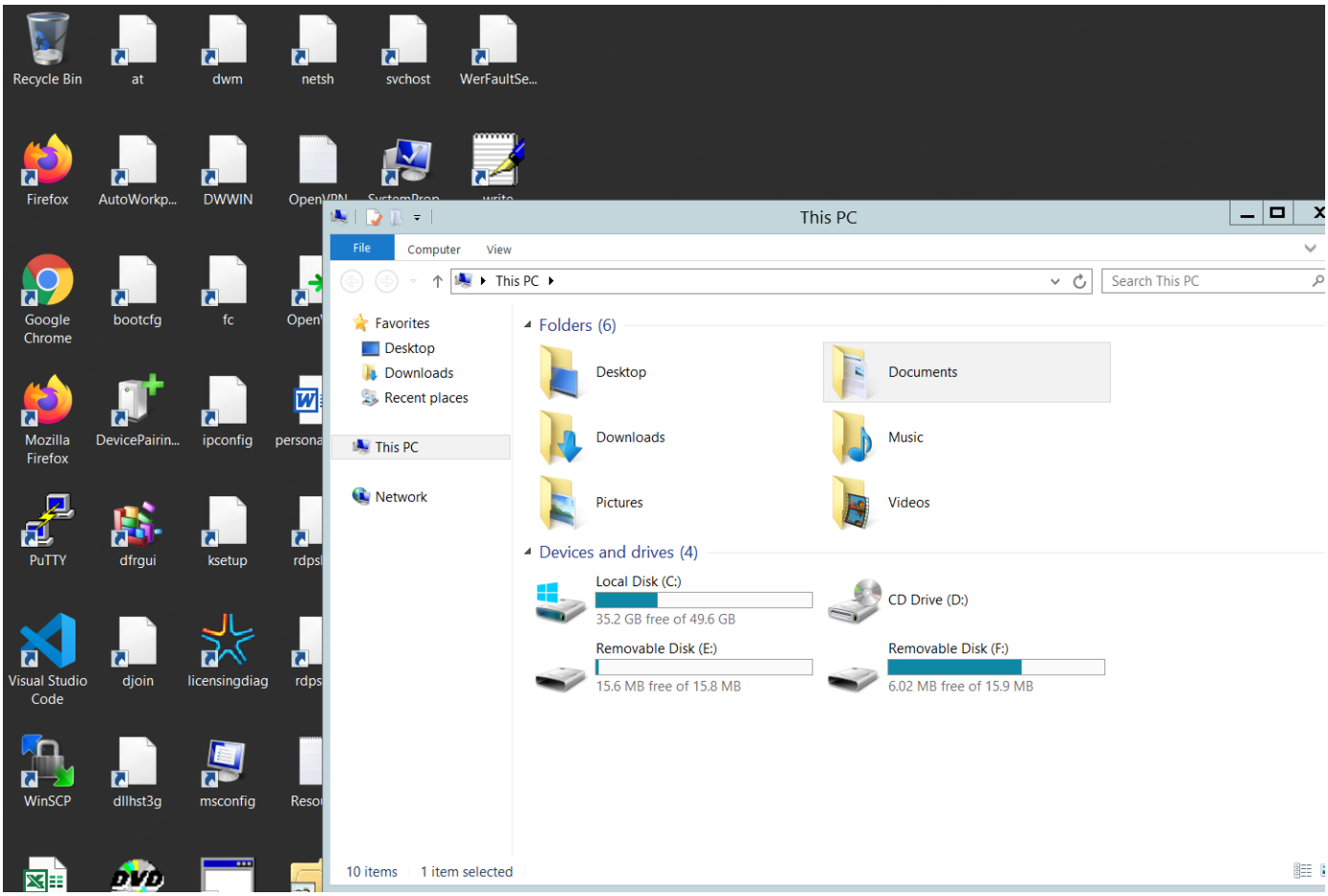
Type	Object	Risk Level
File (SHA1)	FCDCBB14DFC3734017B78883DEC9BB14DCA04B56	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.Win32.MALREP.THAADBA Engine Version: 12.500.1004 Malware Pattern Version: 16.495.92		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\quote 2021.exe Packer: UNKNOWN		
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\quote 2021.exe, "%WorkingDir%\quote 2021.exe", , , , CREATE_SUSPENDED, , , , Process:2784:%WorkingDir%\quote 2021.exe) Return: 1		2092
Detection	Threat Characteristic: Creates process Process ID: 2092 Image Path: %WorkingDir%\quote 2021.exe Shell Command: "%WorkingDir%\quote 2021.exe"		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2784:%WorkingDir%\quote 2021.exe) Return: 1		2092
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2092 Injected API: SetThreadContext Target Process ID: 2784 Target Image Path: %WorkingDir%\quote 2021.exe		
Detection	Threat Characteristic: Creates process Process ID: 2784 Image Path: %WorkingDir%\quote 2021.exe		
Call System API	API Name: CryptExportKey Args: (4ef138, 0, 6, 0, 0, 2abe90) Return: 1	2092	2784
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 53b2598, 5c1f064) Return: 0	2092	2784
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, NULL, 0, NULL, 0, 5c1f064) Return: 0	2092	2784
Call WMI API	API Name: Win32_BaseBoard::Get Args: (SerialNumber, 0, NIUIX0SX0LPX8F, 8, 0) Return: 0	2092	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::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 53b2c18, 2aef28) Return: 0	2092	2784
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, , 80, , 0, 2aef28) Return: 0	2092	2784
Call WMI API	API Name: Win32_Processor::Get Args: (__PATH, 0, \\Win-Lena\ROOT\cimv2:Win32_Processor, 8, 64) Return: 0	2092	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	2092	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	2092	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	2092	2784
Call WMI API	API Name: Win32_Processor::Get Args: (processorID, 0, 1, 8, 32) Return: 0	2092	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	2092	2784
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 53b1e98, 2aef28) Return: 0	2092	2784
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, , 80, , 0, 2aef28) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\ROOT\cimv2:Win32_NetworkAdapterConfiguration, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__CLASS, 0, Win32_NetworkAdapterConfiguration, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=0, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=1, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=2, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=3, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784

Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=4, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=5, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=6, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=7, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=8, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, 0, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=9, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=10, 8, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, -1, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (IPEnabled, 0, -1, 11, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (MacAddress, 0, 9C:DA:3E:35:D2:E3, 8, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (MacAddress, 0, 9C:DA:3E:35:D2:E3, 8, 0) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__GENUS, 0, 2, 3, 64) Return: 0	2092	2784
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: (__PATH, 0, \\Win-Lena\root\cimv2:Win32_NetworkAdapterConfiguration.Index=11, 8, 64) Return: 0	2092	2784
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\FILEZILLA\RECENTSERVERS.XML		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	2092	2784
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	2092	2784
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Call Service API	API Name: OpenServiceW Args: (54135e0, VaultSvc, 14) Return: 5413540	2092	2784
Call Service API	API Name: StartServiceW Args: (5413540, 0, 0) Return: 1	2092	2784
Call Service API	API Name: StartServiceW Args: (5413540, 0, 0) Return: 1	2092	2784
Call System API	API Name: CLSIDFromProgIDEx Args: (WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8}) Return: 0	2092	2784
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\COMODO\ICEDRAGON\PROFILES.INI		
Call System API	API Name: CLSIDFromProgIDEx Args: (WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8}) Return: 0	2092	2784
Call System API	API Name: CLSIDFromProgIDEx Args: (WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8}) Return: 0	2092	2784
Call System API	API Name: CLSIDFromProgIDEx Args: (WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8}) Return: 0	2092	2784
Call System API	API Name: CLSIDFromProgIDEx Args: (WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8}) Return: 0	2092	2784
Detection	Threat Characteristic: Accesses decoy file %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data		
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini		
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\xldumgeb.default\key3.db		

▼ 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