Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3315, Task ID: 768

Task ID:	768
Risk Level:	9
Date Processed:	2016-05-18 10:35:52 (UTC)
Processing Time:	3.09 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6dc4e4d099b52b843b2c3ab82ba732e1.exe"
Sample ID:	3315
Type:	basic
Owner:	admin
Label:	6dc4e4d099b52b843b2c3ab82ba732e1
Date Added:	2016-05-18 10:30:49 (UTC)
File Type:	PE32:win32:gui
File Size:	40674 bytes
MD5:	6dc4e4d099b52b843b2c3ab82ba732e1
SHA256:	66d07b68175b22c4d776ebf6a8a69ebc0703c494f3c66133554941b03ef1bc2f
Description:	None

Pattern Matching Results

9 Creates malicious mutex

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\WINDOWS\Temp\6dc4e4d099b52b843b2c3ab82ba732e1.exe
["c:\windows\temp\6dc4e4d099b52b843b2c3ab82ba732e1.exe"]
Terminates process: C:\WINDOWS\Temp\6dc4e4d099b52b843b2c3ab82ba732e1.exe

Named Object Events

Creates mutex: \BaseNamedObjects\Worm.P2P.Google
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates: C:\My Downloads
Creates: C:\My Downloads\Xbox.info Crack.exe
Creates: C:\My Downloads\Winzip 8.0 Key Generator.exe
Creates: C:\My Downloads\Mafia ISO - Full Downloader.exe
Creates: C:\My Downloads\Grand Prix 4 Patch.exe
Creates: C:\My Downloads\Winrar 3.2 ISO - Full Downloader.exe
Creates: C:\My Downloads\Critical Point Manga game Full Downloader.exe
Creates: C:\My Downloads\The Eye Of Kraken Patch.exe
Creates: C:\My Downloads\Star Wars II Movie ISO - Full Downloader.exe
Creates: C:\My Downloads\Red Ace Squadron Key Generator.exe
Creates: C:\My Downloads\The Eye Of Kraken Full Downloader.exe
Creates: C:\My Downloads\Internet and Computer Speed Booster Patch.exe
Creates: C:\My Downloads\Star Wars Starfighter Crack.exe
Creates: C:\My Downloads\Microsoft Office XP (English) Full Downloader.exe
Creates: C:\My Downloads\Duke Nukem Manhattan Project Key Generator.exe
Creates: C:\My Downloads\KaZaA Media Desktop v2.5 UNOFFICIAL Key Generator.exe
Creates: C:\My Downloads\The Eye Of Kraken Key Generator.exe
Creates: C:\My Downloads\Dark Age Of Camelot Shrouded Isles Crack.exe
Creates: C:\My Downloads\Half-life ONLINE Full Downloader.exe
Creates: C:\My Downloads\Dweebs 2 Crack.exe

Creates: C:\My Downloads\Battle.net Full Downloader.exe
Creates: C:\My Downloads\Half-life ONLINE Crack.exe
Creates: C:\My Downloads\Unreal Tournament 3 Key Generator.exe
Creates: C:\My Downloads\Free Virus Removal Tool From Symantec Crack.exe
Creates: C:\My Downloads\KaZaA Spyware Remover Patch.exe
Creates: C:\My Downloads\Soldier Of Fortune 2 Patch.exe
Creates: C:\My Downloads\MSN Password Hacker and Stealer Patch.exe
Creates: C:\My Downloads\Deadly Dozen Key Generator.exe
Creates: C:\My Downloads\Quake 4 BETA Full Downloader.exe
Creates: C:\My Downloads\Age of Sail 2 Patch.exe
Creates: C:\My Downloads\Hacking Tool Collection Full Downloader.exe
Creates: C:\My Downloads\LordOfTheRingsr Crack.exe
Creates: C:\My Downloads\Internet and Computer Speed Booster Full Downloader.exe
Creates: C:\My Downloads\Hoyle Card Games 2003 Full Downloader.exe
Creates: C:\My Downloads\Warcraft 3 Full Downloader.exe
Creates: C:\My Downloads\Necromania Trap Of Darkness Key Generator.exe
Creates: C:\My Downloads\Hard Truck 18 Wheels of Steel Full Downloader.exe
Creates: C:\My Downloads\Star Wars Starfighter Patch.exe
Creates: C:\My Downloads\Age Of Empires 2 ISO - Full Downloader.exe
Creates: C:\My Downloads\Soldier Of Fortune 2 ISO - Full Downloader.exe
Creates: C:\My Downloads\Star Wars Starfighter ISO - Full Downloader.exe
Creates: C:\My Downloads\LordOfTheRingsr Patch.exe
Creates: C:\My Downloads\Crazy Taxi Crack.exe
Creates: C:\My Downloads\Red Ace Squadron ISO - Full Downloader.exe
Creates: C:\My Downloads\Gearhead Garage Patch.exe
Creates: C:\My Downloads\Grand Prix 4 Full Downloader.exe
Creates: C:\My Downloads\Half Life Blue Shift Crack.exe
Creates: C:\My Downloads\Squad Battles Eagles Strike Crack.exe
Creates: C:\My Downloads\Tomb Raider 3 Crack.exe
Creates: C:\My Downloads\DSL Modem Uncapper Full Downloader.exe
Creates: C:\My Downloads\Grand Theft Auto 3 Patch.exe
Opens: C:\WINDOWS\Prefetch\6DC4E4D099B52B843B2C3AB82BA73-22E60BF3.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\Temp\6dc4e4d099b52b843b2c3ab82ba732e1.exe
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens: C:\WINDOWS\system32\urlmon.dll.123.Config
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\system32\wininet.dll.123.Manifest
Opens: C:\WINDOWS\system32\wininet.dll.123.Config
Opens: C:\My Downloads
Opens: C:\My Downloads\Xbox.info Crack.exe
Opens: C:\My Downloads\Winzip 8.0 Key Generator.exe
Opens: C:\My Downloads\Mafia ISO - Full Downloader.exe
Opens: C:\My Downloads\Grand Prix 4 Patch.exe
Opens: C:\My Downloads\Winrar 3.2 ISO - Full Downloader.exe
Opens: C:\My Downloads\Critical Point Manga game Full Downloader.exe
Opens: C:\My Downloads\The Eye Of Kraken Patch.exe
Opens: C:\My Downloads\Star Wars II Movie ISO - Full Downloader.exe
Opens: C:\My Downloads\Red Ace Squadron Key Generator.exe
Opens: C:\My Downloads\The Eye Of Kraken Full Downloader.exe
Opens: C:\My Downloads\Internet and Computer Speed Booster Patch.exe
Opens: C:\My Downloads\Star Wars Starfighter Crack.exe
Opens: C:\My Downloads\Microsoft Office XP (English) Full Downloader.exe
Opens: C:\My Downloads\Duke Nukem Manhattan Project Key Generator.exe
Opens: C:\My Downloads\KaZaA Media Desktop v2.5 UNOFFICIAL Key Generator.exe
Opens: C:\My Downloads\The Eye Of Kraken Key Generator.exe
Opens: C:\My Downloads\Dark Age Of Camelot Shrouded Isles Crack.exe

Opens: C:\My Downloads\Half-life ONLINE Full Downloader.exe
Opens: C:\My Downloads\Dweebs 2 Crack.exe
Opens: C:\My Downloads\Battle.net Full Downloader.exe
Opens: C:\My Downloads\Half-life ONLINE Crack.exe
Opens: C:\My Downloads\Unreal Tournament 3 Key Generator.exe
Opens: C:\My Downloads\Free Virus Removal Tool From Symantec Crack.exe
Opens: C:\My Downloads\KaZaA Spyware Remover Patch.exe
Opens: C:\My Downloads\Soldier Of Fortune 2 Patch.exe
Opens: C:\My Downloads\MSN Password Hacker and Stealer Patch.exe
Opens: C:\My Downloads\Deadly Dozen Key Generator.exe
Opens: C:\My Downloads\Quake 4 BETA Full Downloader.exe
Opens: C:\My Downloads\Age of Sail 2 Patch.exe
Opens: C:\My Downloads\Hacking Tool Collection Full Downloader.exe
Opens: C:\My Downloads\LordOfTheRingsr Crack.exe
Opens: C:\My Downloads\Internet and Computer Speed Booster Full Downloader.exe
Opens: C:\My Downloads\Hoyle Card Games 2003 Full Downloader.exe
Opens: C:\My Downloads\Warcraft 3 Full Downloader.exe
Opens: C:\My Downloads\Necromania Trap Of Darkness Key Generator.exe
Opens: C:\My Downloads\Hard Truck 18 Wheels of Steel Full Downloader.exe
Opens: C:\My Downloads\Star Wars Starfighter Patch.exe
Opens: C:\My Downloads\Age Of Empires 2 ISO - Full Downloader.exe
Opens: C:\My Downloads\Soldier Of Fortune 2 ISO - Full Downloader.exe
Opens: C:\My Downloads\Star Wars Starfighter ISO - Full Downloader.exe
Opens: C:\My Downloads\LordOfTheRingsr Patch.exe
Opens: C:\My Downloads\Crazy Taxi Crack.exe
Opens: C:\My Downloads\Red Ace Squadron ISO - Full Downloader.exe
Opens: C:\My Downloads\Gearhead Garage Patch.exe
Opens: C:\My Downloads\Grand Prix 4 Full Downloader.exe
Opens: C:\My Downloads\Half Life Blue Shift Crack.exe
Opens: C:\My Downloads\Squad Battles Eagles Strike Crack.exe
Opens: C:\My Downloads\Tomb Raider 3 Crack.exe
Opens: C:\My Downloads\DSL Modem Uncapper Full Downloader.exe
Opens: C:\My Downloads\Grand Theft Auto 3 Patch.exe
Writes to: C:\My Downloads\Xbox.info Crack.exe
Writes to: C:\My Downloads\Winzip 8.0 Key Generator.exe
Writes to: C:\My Downloads\Mafia ISO - Full Downloader.exe
Writes to: C:\My Downloads\Grand Prix 4 Patch.exe
Writes to: C:\My Downloads\Winrar 3.2 ISO - Full Downloader.exe
Writes to: C:\My Downloads\Critical Point Manga game Full Downloader.exe
Writes to: C:\My Downloads\The Eye Of Kraken Patch.exe
Writes to: C:\My Downloads\Star Wars II Movie ISO - Full Downloader.exe
Writes to: C:\My Downloads\Red Ace Squadron Key Generator.exe
Writes to: C:\My Downloads\The Eye Of Kraken Full Downloader.exe
Writes to: C:\My Downloads\Internet and Computer Speed Booster Patch.exe
Writes to: C:\My Downloads\Star Wars Starfighter Crack.exe
Writes to: C:\My Downloads\Microsoft Office XP (English) Full Downloader.exe
Writes to: C:\My Downloads\Duke Nukem Manhattan Project Key Generator.exe
Writes to: C:\My Downloads\KaZaA Media Desktop v2.5 UNOFFICIAL Key Generator.exe
Writes to: C:\My Downloads\The Eye Of Kraken Key Generator.exe
Writes to: C:\My Downloads\Dark Age Of Camelot Shrouded Isles Crack.exe
Writes to: C:\My Downloads\Half-life ONLINE Full Downloader.exe
Writes to: C:\My Downloads\Dweebs 2 Crack.exe
Writes to: C:\My Downloads\Battle.net Full Downloader.exe
Writes to: C:\My Downloads\Half-life ONLINE Crack.exe
Writes to: C:\My Downloads\Unreal Tournament 3 Key Generator.exe
Writes to: C:\My Downloads\Free Virus Removal Tool From Symantec Crack.exe
Writes to: C:\My Downloads\KaZaA Spyware Remover Patch.exe
Writes to: C:\My Downloads\Soldier Of Fortune 2 Patch.exe
Writes to: C:\My Downloads\MSN Password Hacker and Stealer Patch.exe
Writes to: C:\My Downloads\Deadly Dozen Key Generator.exe
Writes to: C:\My Downloads\Quake 4 BETA Full Downloader.exe
Writes to: C:\My Downloads\Age of Sail 2 Patch.exe
Writes to: C:\My Downloads\Hacking Tool Collection Full Downloader.exe

Writes to: C:\My Downloads\LordOfTheRingsr Crack.exe
Writes to: C:\My Downloads\Internet and Computer Speed Booster Full Downloader.exe
Writes to: C:\My Downloads\Hoyle Card Games 2003 Full Downloader.exe
Writes to: C:\My Downloads\Warcraft 3 Full Downloader.exe
Writes to: C:\My Downloads\Necromania Trap Of Darkness Key Generator.exe
Writes to: C:\My Downloads\Hard Truck 18 Wheels of Steel Full Downloader.exe
Writes to: C:\My Downloads\Star Wars Starfighter Patch.exe
Writes to: C:\My Downloads\Age Of Empires 2 ISO - Full Downloader.exe
Writes to: C:\My Downloads\Soldier Of Fortune 2 ISO - Full Downloader.exe
Writes to: C:\My Downloads\Star Wars Starfighter ISO - Full Downloader.exe
Writes to: C:\My Downloads\LordOfTheRingsr Patch.exe
Writes to: C:\My Downloads\Crazy Taxi Crack.exe
Writes to: C:\My Downloads\Red Ace Squadron ISO - Full Downloader.exe
Writes to: C:\My Downloads\Gearhead Garage Patch.exe
Writes to: C:\My Downloads\Grand Prix 4 Full Downloader.exe
Writes to: C:\My Downloads\Half Life Blue Shift Crack.exe
Writes to: C:\My Downloads\Squad Battles Eagles Strike Crack.exe
Writes to: C:\My Downloads\Tomb Raider 3 Crack.exe
Writes to: C:\My Downloads\DSL Modem Uncapper Full Downloader.exe
Writes to: C:\My Downloads\Grand Theft Auto 3 Patch.exe
Reads from: C:\WINDOWS\Temp\6dc4e4d099b52b843b2c3ab82ba732e1.exe

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\6dc4e4d099b52b843b2c3ab82ba732e1.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\oleaut\userera
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wininet.dll
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\protocols\name-space handler\
Opens key: HKCR\protocols\name-space handler
Opens key: HKCU\software\classes\protocols\name-space handler
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\system\currentcontrolset\control\wmi\security
Opens key: HKLM\software\limewire
Opens key: HKCU\software\shareaza
Opens key: HKCU\software\kazaa

Opens key: HKCU\software\xolox
Opens key: HKLM\software\morpheus
Opens key: HKCU\software\ed2k
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[6dc4e4d099b52b843b2c3ab82ba732e1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[6dc4e4d099b52b843b2c3ab82ba732e1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableallforole32]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[6dc4e4d099b52b843b2c3ab82ba732e1.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-ab78-1084642581fb]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-000000000000]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]