

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 3322, Task ID: 795

Task ID:	795
Risk Level:	8
Date Processed:	2016-05-18 10:39:04 (UTC)
Processing Time:	29.55 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\0f31e2adf1807f61e5d6989596ebfb36.exe"
Sample ID:	3322
Type:	basic
Owner:	admin
Label:	0f31e2adf1807f61e5d6989596ebfb36
Date Added:	2016-05-18 10:30:50 (UTC)
File Type:	PE32:win32:gui
File Size:	403680 bytes
MD5:	0f31e2adf1807f61e5d6989596ebfb36
SHA256:	463ad234a346831c72a1e5c1a0ea1d410820651860165d642b04d72a74ba6066
Description:	None

## Pattern Matching Results

6	Modifies registry autorun entries
2	PE: Nonstandard section
8	Modifies Applnit_DLLs registry value

## Static Events

Anomaly:	PE: No DOS stub
Anomaly:	PE: Contains one or more non-standard sections

## Process/Thread Events

Creates process:	C:\windows\temp\0f31e2adf1807f61e5d6989596ebfb36.exe
["C:\windows\temp\0f31e2adf1807f61e5d6989596ebfb36.exe" ]	
Creates process:	C:\PROGRA~3\Mozilla\qnouina.exe [C:\PROGRA~3\Mozilla\qnouina.exe - zbgmkin]
Terminates process:	C:\Windows\Temp\0f31e2adf1807f61e5d6989596ebfb36.exe
Terminates process:	C:\PROGRA~3\Mozilla\qnouina.exe

## Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\DBWinMutex

## File System Events

Creates:	C:\ProgramData\Mozilla
Creates:	C:\ProgramData\Mozilla\qnouina.exe
Creates:	C:\ProgramData\Mozilla\
Creates:	C:\ProgramData\Mozilla\talpxfj.dll
Opens:	C:\Windows\Prefetch\0F31E2ADF1807F61E5D6989596EBF-FAB1374B.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\0f31e2adf1807f61e5d6989596ebfb36.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb

Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\msasn1.dll
Opens:	C:\Windows\SysWOW64\crypt32.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\nsi.dll
Opens:	C:\Windows\SysWOW64\ws2_32.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\Windows\SysWOW64\dwmmapi.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\
Opens:	C:\Windows\SysWOW64\clbcatq.dll
Opens:	C:\Windows\SysWOW64\taskschd.dll
Opens:	C:\Windows\SysWOW64\xmlite.dll
Opens:	C:\ProgramData\Mozilla\qnouina.exe
Writes to:	C:\ProgramData\Mozilla\qnouina.exe
Writes to:	C:\ProgramData\Mozilla\talpxfj.dll
Reads from:	C:\Windows\Fonts\StaticCache.dat
Reads from:	C:\Windows\Temp\0f31e2adf1807f61e5d6989596ebfb36.exe

## Windows Registry Events

---

Opens key:	HKLM\software\microsoft\wow64
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:	
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers	
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\language
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key:	HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key:	HKLM\software\policies\microsoft\mui\settings
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop\languageconfiguration
Opens key:	HKCU\control panel\desktop
Opens key:	HKCU\control panel\desktop\muicached
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:	HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key:	HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:	HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation	
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file

execution options  
     Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\dlloptions  
     Opens key: HKLM\  
     Opens key: HKLM\system\currentcontrolset\services\crypt32  
     Opens key: HKLM\software\wow6432node\microsoft\windows  
 nt\currentversion\gre\_initialize  
     Opens key: HKLM\software\wow6432node\microsoft\windows  
 nt\currentversion\compatibility32  
     Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime  
 compatibility  
     Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows  
     Opens key: HKLM\system\currentcontrolset\control\lsa\lspolicy  
     Opens key: HKLM\system\currentcontrolset\control\lsa  
     Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration  
     Opens key: HKLM\software\wow6432node\microsoft\ole  
     Opens key: HKLM\software\wow6432node\microsoft\ole\tracing  
     Opens key: HKLM\software\microsoft\ole\tracing  
     Opens key: HKLM\software\wow6432node\microsoft\oleaut  
     Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr  
     Opens key: HKLM\software\policies\microsoft\sqmclient\windows  
     Opens key: HKLM\software\microsoft\sqmclient\windows  
     Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation  
     Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
     Opens key: HKLM\system\currentcontrolset\control\session manager  
     Opens key: HKLM\system\currentcontrolset\control\nls\locale  
     Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts  
     Opens key: HKLM\system\currentcontrolset\control\nls\language groups  
     Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink  
     Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\datastore\_v1.0  
     Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\surrogatefallback  
     Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\surrogatefallback\segoe ui  
     Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\shell folders  
     Opens key: HKLM\software\microsoft\cryptography  
     Opens key: HKLM\software\wow6432node\microsoft\rpc  
     Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername  
     Opens key: HKLM\system\setup  
     Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc  
     Opens key: HKLM\software\policies\microsoft\windows nt\rpc  
     Opens key: HKCU\software\classes\  
     Opens key: HKCU\software\classes\appid\0f31e2adf1807f61e5d6989596ebfb36.exe  
     Opens key: HKCR\appid\0f31e2adf1807f61e5d6989596ebfb36.exe  
     Opens key: HKLM\software\microsoft\com3  
     Opens key: HKLM\software\microsoft\windowsruntime\clsid  
     Opens key: HKLM\software\microsoft\windowsruntime\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}  
     Opens key: HKCR\activatableclasses\clsid  
     Opens key: HKCR\activatableclasses\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}  
     Opens key: HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}  
     Opens key: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}  
     Opens key: HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas  
     Opens key: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas  
     Opens key: HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32  
     Opens key: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler32  
 Opens key: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler32  
 Opens key: HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler  
 Opens key: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler  
 Opens key: HKU\.\default\software\policies\microsoft\windows\safer\codeidentifiers  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize  
 Opens key: HKU\.\default\control  
 panel\desktop\muicached\machinelanguageconfiguration  
 Opens key: HKU\.\default\software\policies\microsoft\control panel\desktop  
 Opens key: HKU\.\default\control panel\desktop\languageconfiguration  
 Opens key: HKU\.\default\control panel\desktop  
 Opens key: HKU\.\default\control panel\desktop\muicached  
 Opens key: HKU\.\default\software\microsoft\windows nt\currentversion\appcompatflags  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options  
 Opens key: HKLM\software\microsoft\ole  
 Opens key: HKU\.\default\control panel\international  
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]  
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]  
 Queries value:  
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]  
 Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]  
 Queries value:  
 HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]  
 Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]  
 Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[alternatecodepage]  
 Queries value: HKCU\control panel\desktop[preferreduilanguages]  
 Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]  
 Queries value:  
 HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]  
 Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]  
 Queries value: HKCU\software\microsoft\windows  
 nt\currentversion\appcompatflags[showdebuginfo]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\dllnsoptions[usefilter]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\dllnsoptions[0f31e2adf1807f61e5d6989596ebfb36.exe]  
 Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\gre\_initialize[disablemetafiles]  
 Queries value: HKLM\software\wow6432node\microsoft\windows  
 nt\currentversion\compatibility32[0f31e2adf1807f61e5d6989596ebfb36]  
 Queries value: HKLM\software\wow6432node\microsoft\windows  
 nt\currentversion\windows[loadappinit\_dlls]  
 Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]  
 Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]  
 Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
 Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]  
 Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]  
 Queries value: HKLM\software\wow6432node\microsoft\windows\windows error  
 reporting\wmr[disable]  
 Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]  
 Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]  
 Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]  
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]  
 Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]  
 Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]  
 Queries value: HKLM\software\microsoft\windows

```

nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\shell folders[common appdata]
  Queries value: HKLM\software\microsoft\cryptography[machineguid]
  Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value: HKLM\system\setup[oobeinprogress]
  Queries value: HKLM\system\setup\systemsetupinprogress]
  Queries value: HKLM\software\microsoft\rpc[idletimerwindow]
  Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value: HKLM\software\microsoft\com3[com+enabled]
  Queries value: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}[]
  Queries value: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32[inprocserver32]
  Queries value: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32[]
  Queries value: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32[threadingmodel]
  Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value: HKU\.\default\control panel\desktop[preferreduilanguages]
  Queries value: HKU\.\default\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllinoptions[qnouina.exe]
  Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[qnouina]
  Queries value: HKU\.\default\control panel\international[surrencyoverride]
  Value changes: HKLM\software\wow6432node\microsoft\windows

```

nt\currentversion\windows[appinit\_dlls]

Value changes: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\windows[loadappinit\_dlls]