Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 138, Task ID: 550

Task ID:	550
Risk Level:	7
Date Processed:	2016-04-28 13:01:58 (UTC)
Processing Time:	2.99 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9b4316a022e8ffa53c35fafab8f7753b.exe"

Sample ID:	138
Type:	basic
Owner:	admin
Label:	9b4316a022e8ffa53c35fafab8f7753b
Date Added:	2016-04-28 12:45:04 (UTC)
File Type:	PE32:win32:gui
File Size:	305192 bytes
MD5:	9b4316a022e8ffa53c35fafab8f7753b
SHA256:	ff81ac1ada501179e980e72ae0459d6be9d6987581d867e79039f84ad8ebda54
Description:	None

Pattern Matching Results

5	PE: Contains compressed section
5	Packer: UPX
4	Checks whether debugger is present
2	PE: Nonstandard section
7	Signed by adware producer [Adware, PUA]
7	Creates known events: Amonetize 2

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process:	C:\windows\temp\9b4316a022e8ffa53c35fafab8f7753b.exe ["C:\windows\temp\9b4316a022e8ffa53c35fafab8f7753b.exe"]
Terminates process:	C:\Windows\Temp\9b4316a022e8ffa53c35fafab8f7753b.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\AmInst__Runing_1
Creates event:	\Sessions\1\BaseNamedObjects\AmiUpdInstallProgress

File System Events

Opens:	C:\Windows\Prefetch\9B4316A022E8FFA53C35FAFAB8F77-1D483179.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\9b4316a022e8ffa53c35fafab8f7753b.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\version.dll
Opens:	C:\Windows\SysWOW64\winhttp.dll

```
  Opens:                  C:\Windows\SysWOW64\sechost.dll
  Opens:                  C:\Windows\SysWOW64\combase.dll
  Opens:                  C:\Windows\SysWOW64\msvcrt.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\advapi32.dll
  Opens:                  C:\Windows\SysWOW64\user32.dll
  Opens:                  C:\Windows\SysWOW64\gdi32.dll
  Opens:                  C:\Windows\SysWOW64\ole32.dll
  Opens:                  C:\Windows\SysWOW64\oleaut32.dll
  Opens:                  C:\Windows\SysWOW64\shlwapi.dll
  Opens:                  C:\Windows\SysWOW64\shell32.dll
  Opens:                  C:\Windows\SysWOW64\imm32.dll
  Opens:                  C:\Windows\SysWOW64\msctf.dll
  Opens:                  C:\Users\Admin\AppData\Local\Temp
  Opens:                  C:\Windows\SysWOW64\uxtheme.dll
  Opens:                  C:\Windows\SysWOW64\clbcatq.dll
  Opens:                  C:\Windows\SysWOW64\IPHLPAPI.DLL
  Opens:                  C:\Windows\SysWOW64\cryptsp.dll
  Opens:                  C:\Windows\SysWOW64\rsaenh.dll
  Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                  C:\Windows\SysWOW64\winnsi.dll
  Opens:                  C:\Windows\SysWOW64\nsi.dll
  Opens:                  C:\Windows\SysWOW64\dhcpcsvc6.dll
  Opens:                  C:\Windows\SysWOW64\ws2_32.dll
  Opens:                  C:\Windows\SysWOW64\dhcpcsvc.dll
```

Windows Registry Events

```
  Opens key:              HKLM\software\microsoft\wow64
  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\system\currentcontrolset\control\session manager
  Opens key:              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:              HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  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\
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  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\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:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:                HKLM\software\wow6432node\microsoft\net framework setup\ndp\v1.1.4322
  Opens key:                HKLM\software\wow6432node\microsoft\net framework setup\ndp\v3.5
  Opens key:                HKCU\software\classes\
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{67bd9eeb-aa06-4329-a940-
d250019300c9}
  Opens key:                HKCR\activatableclasses\clsid
  Opens key:                HKCR\activatableclasses\clsid\{67bd9eeb-aa06-4329-a940-d250019300c9}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{67bd9eeb-aa06-4329-a940-
d250019300c9}
  Opens key:                HKCR\wow6432node\clsid\{67bd9eeb-aa06-4329-a940-d250019300c9}
  Opens key:                HKLM\software\wow6432node\microsoft\net framework setup\ndp\v4\full
  Opens key:                HKCU\software\classes\clsid\{67bd9eeb-aa06-4329-a940-d250019300c9}
  Opens key:                HKCR\clsid\{67bd9eeb-aa06-4329-a940-d250019300c9}
  Opens key:                HKCU\software\classes\activatableclasses\clsid
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{67bd9eeb-aa06-4329-a940-
d250019300c9}
  Opens key:                HKCU\software\classes\appid\9b4316a022e8ffa53c35fafab8f7753b.exe
  Opens key:                HKCR\appid\9b4316a022e8ffa53c35fafab8f7753b.exe
  Opens key:                HKLM\software\wow6432node\microsoft\ole\appcompat
  Opens key:                HKLM\software\microsoft\ole\appcompat
  Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\wow6432node\microsoft\cryptography\offload
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:                HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}
  Opens key:                HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                HKLM\software\wow6432node\microsoft\rpc\extensions
  Opens key:                HKLM\software\microsoft\rpc\extensions
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\winhttp
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a04231f6-42eb-4732-b850-
25b8d56dd1d8}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                HKU\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\connections
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-
08002be10318}\{b5105d63-74c6-4dc1-87b7-55779daa70e9}\connection
  Opens key:                HKLM\software\microsoft\windows nt\currentversion
  Opens key:                HKCU\software\clients\startmenuinternet
  Opens key:                HKLM\software\clients\startmenuinternet
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{0000032a-0000-0000-c000-
000000000046}
  Opens key:                HKCR\activatableclasses\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{0000032a-0000-0000-c000-
000000000046}
  Opens key:                HKCR\wow6432node\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                HKCR\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{0000032a-0000-0000-c000-
000000000046}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{00000338-0000-0000-c000-
000000000046}
  Opens key:                HKCR\activatableclasses\clsid\{00000338-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00000338-0000-0000-c000-
000000000046}
  Opens key:                HKCR\wow6432node\clsid\{00000338-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\clsid\{00000338-0000-0000-c000-000000000046}
  Opens key:                HKCR\clsid\{00000338-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{00000338-0000-0000-c000-
000000000046}
  Opens key:                HKCU\software\classes\wow6432node\interface\{9edc0c90-2b5b-4512-953e-
35767bad5c67}
  Opens key:                HKCR\wow6432node\interface\{9edc0c90-2b5b-4512-953e-35767bad5c67}
  Opens key:                HKCU\software\classes\interface\{9edc0c90-2b5b-4512-953e-35767bad5c67}
  Opens key:                HKCR\interface\{9edc0c90-2b5b-4512-953e-35767bad5c67}
  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\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[9b4316a022e8ffa53c35fafab8f7753b]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:            HKLM\software\microsoft\ole[aggressivemtatesting]
  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\sqmclient\windows[ceipenable]
  Queries value:            HKLM\software\microsoft\rpc[idletimerwindow]
  Queries value:            HKLM\software\wow6432node\microsoft\net framework
setup\ndp\v3.5[install]
  Queries value:            HKLM\software\wow6432node\microsoft\net framework
setup\ndp\v3.5[version]
  Queries value:            HKLM\software\wow6432node\microsoft\net framework setup\ndp\v3.5[sp]
  Queries value:            HKLM\software\microsoft\com3[com+enabled]
  Queries value:            HKLM\software\wow6432node\microsoft\net framework
setup\ndp\v4\full[install]
  Queries value:            HKLM\software\wow6432node\microsoft\net framework
setup\ndp\v4\full[version]
  Queries value:            HKLM\software\wow6432node\microsoft\net framework setup\ndp\v4\full[sp]
  Queries value:            HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
  Queries value:            HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
  Queries value:            HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value:            HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:            HKLM\software\microsoft\cryptography[machineguid]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
  Queries value:            HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32[]
  Queries value:            HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:            HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\winhttp[disablebranchcache]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[searchlist]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enabledhcp]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpdomain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpv6domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpdomain]
   Queries value:             HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:             HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
   Queries value:             HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpnameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpnameserver]
   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\network\{4d36e972-e325-11ce-bfc1-
08002be10318}\{b5105d63-74c6-4dc1-87b7-55779daa70e9}\connection[pnpinstanceid]
   Queries value:             HKLM\software\microsoft\windows nt\currentversion[digitalproductid]
   Queries value:             HKLM\software\microsoft\windows nt\currentversion[digitalproductid4]
   Queries value:             HKLM\software\clients\startmenuinternet[]
```