

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 117, Task ID: 469

Task ID:	469
Risk Level:	1
Date Processed:	2016-04-28 12:59:41 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\97f9d8bd7cc2ebaf184348e0a114d633.exe"
Sample ID:	117
Type:	basic
Owner:	admin
Label:	97f9d8bd7cc2ebaf184348e0a114d633
Date Added:	2016-04-28 12:45:02 (UTC)
File Type:	PE32:win32:gui
File Size:	569358 bytes
MD5:	97f9d8bd7cc2ebaf184348e0a114d633
SHA256:	d9953b0da8f4d8a01d9687997f80c9861b4dd721330fc46725e7731baa7a3bd5
Description:	None

## Pattern Matching Results

## Process/Thread Events

Creates process:	C:\windows\temp\97f9d8bd7cc2ebaf184348e0a114d633.exe
["C:\windows\temp\97f9d8bd7cc2ebaf184348e0a114d633.exe" ]	
Creates process:	C:\Users\Admin\AppData\Local\Temp\Stp71F_TMP.EXE
["C:\Users\Admin\AppData\Local\Temp\Stp71F_TMP.EXE"]	

## Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

## File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\Stp71F.tmp
Creates:	C:\Users\Admin\AppData\Local\Temp\Stp71F_TMP.EXE
Opens:	C:\Windows\Prefetch\97F9D8BD7CC2EBAF184348E0A114D-24A52DBA.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\windows\temp\97f9d8bd7cc2ebaf184348e0a114d633.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af	
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\Temp\97f9d8bd7cc2ebaf184348e0a114d633.exe
Opens:	C:\Users\Admin\AppData\Local\Temp
Opens:	C:\Users\Admin\AppData\Local\Temp\Stp71F.tmp
Opens:	C:\Users\Admin\AppData\Local\Temp\Stp71F_TMP.EXE
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\AppPatch\sysmain.sdb

```

Opens: C:\
Opens: C:\Users
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData
Opens: C:\Users\Admin\AppData\Local
Opens: C:\Users\Admin\AppData\Local\Temp\ui\SwDRM.dll
Opens: C:\Windows\Prefetch\STP71F_TMP.EXE-9D6E46B7.pf
Opens: C:\Windows\SysWOW64\tzres.dll
Opens: C:\Windows\SysWOW64\en-US\tzres.dll.mui
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\Fonts\sserife.fon
Opens: C:\Users\Admin\AppData\Local\Temp\dwmapi.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\Users\Admin\AppData\Local\Temp\Stp71F_TMP.EXE.Local\
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\rpcss.dll
Writes to: C:\Users\Admin\AppData\Local\Temp\Stp71F_TMP.EXE
Reads from: C:\Windows\Temp\97f9d8bd7cc2ebaf184348e0a114d633.exe
Reads from: C:\Users\Admin\AppData\Local\Temp\Stp71F_TMP.EXE
Reads from: C:\Windows\Fonts\StaticCache.dat
Deletes: C:\Users\Admin\AppData\Local\Temp\Stp71F.tmp

```

## Windows Registry Events

---

```

Creates key: HKCU\software\digital river\softwarepassport\mountain stream
software\trekmapgps - annapurna region\0
Creates key: HKCU\software
Creates key: HKCU\software\digital river
Creates key: HKCU\software\digital river\softwarepassport
Creates key: HKCU\software\digital river\softwarepassport\mountain stream software
Creates key: HKCU\software\digital river\softwarepassport\mountain stream
software\trekmapgps - annapurna region
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots

```

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions  
 Opens key: HKLM\  
 Opens key: HKLM\software\wow6432node\microsoft\windows  
 nt\currentversion\diagnostics  
 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\software\microsoft\windows nt\currentversion\image file execution  
 options\stp71f\_tmp.exe  
 Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls  
 Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility  
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat  
 Opens key: HKLM\software\policies\microsoft\windows\appcompat  
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers  
 Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\appcompatflags\custom\stp71f\_tmp.exe  
 Opens key: HKLM\system\currentcontrolset\control\cmf\config  
 Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr  
 Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
 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\ctf\compatibility\stp71f\_tmp.exe  
 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\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}  
 Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}  
 Opens key: HKLM\software\wow6432node\microsoft\ctf\  
 Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\surrogatefallback\ms sans serif  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options[disableusermodecallbackfilter]  
 Queries value: HKLM\system\currentcontrolset\control\session  
 manager[cwdillegalindllsearch]  
 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: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\gre\_initialize[disablemetafiles]  
Queries value: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\compatibility32[97f9d8bd7cc2ebaf184348e0a114d633]  
Queries value: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\windows[loadappinit\_dlls]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell  
folders[cache]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options[disablelocaloverride]  
Queries value: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\compatibility32[stp71f\_tmp]  
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]  
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error  
reporting\wmr[disable]  
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\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\microsoft\ole[pageallocatorusesystemheap]  
Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]

Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]  
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]  
Sets/Creates value: HKCU\software\digital river\softwarepassport\mountain stream  
software\trekmapgps - annapurna region\0[buyurl]