Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	387
Risk Level:	7
Date Processed:	2016-04-28 12:57:41 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\e55165a67c552497d9d653069eae0a8c.exe"
Sample ID:	97
Type:	basic
Owner:	admin
Label:	e55165a67c552497d9d653069eae0a8c
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	110080 bytes
MD5:	e55165a67c552497d9d653069eae0a8c
SHA256:	e30c0a5cd916b4f9242e6d77470cff238914cd16806422a8c4f422b37976aa6b
Description:	None

Pattern Matching Results

7 YARA score 7

Static Events

YARA rule hit:	KeyLoggerStrings

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\e55165a67c552497d9d653069eae0a8c.exe ["c:\windows\temp\e55165a67c552497d9d653069eae0a8c.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\E55165A67C552497D9D653069EAE0-1B27139F.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\e55165a67c552497d9d653069eae0a8c.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]