

SECRET//NOFORN



Dumbo v2.0

User Guide

7 April 2015

CL BY: 2428190
REASON: 1.5(c)
DECL: X1; 17 June 2028
DRV: COL 1-82

SECRET//NOFORN

Table of Changes

Date	Change Description	Authority

(U) Table of Contents

1.0 (U) Introduction.....1
 1.1 (U) Requirement.....1
 1.2 (U) Purpose.....1
2.0 (U) System Overview.....1
3.0 (U) Getting Started.....2
 3.1 (U) Pre-deployment.....2
 3.2 (U) Deployment.....2
 3.3 (U) Additional Notes.....2
 3.4 (U) Sample Output.....3

Dumbo User Guide

1.0 (U) Introduction

(S) Dumbo runs on a target to which we have physical access, attempts to disable all network adapters, suspends any processes using a camera recording device, and attempts to corrupt any files to which those processes were actively writing.

1.1 (U) Requirement

(S) The Intelligence Community has identified the need (requirement # 2015-0150) for a capability to suspend processes utilizing webcams and corrupt any video recordings that could compromise a PAG deployment.

1.2 (U) Purpose

(S) This User Guide describes how to use Dumbo v2.0.

2.0 (U) System Overview

(S) The tool is meant to be executed on a target machine directly from a USB thumb drive. The application will require being run as SYSTEM. The tool will output details on disabling the network adapters, suspending processes using any camera devices, and corrupting those processes' associated files that have write-permission. The output will also be logged in a file called "log.txt" in the same folder as the tool's execution.

(S) Note, although the tool attempts to disable all Bluetooth adapters, it does not explicitly check for the success of the operation. The tool will, however, report the success or failure of disabling network adapters.

Runner.exe: Main executable for Dumbo v2.0. Takes no parameters, and should be run from a SYSTEM cmd.exe shell.

scanner.sys: Driver necessary for tool to run correctly on Windows XP 32 bit. Driver will automatically be installed and removed, if necessary. Driver must be named "scanner.sys" and located in the same folder as Runner.exe to be installed correctly. Driver is not needed, and will not be installed, on any operating system other than Windows XP 32 bit.

3.0 (U) Getting Started

3.1 (U) Pre-deployment

(S) Note that the tool requires being run as SYSTEM, and should be executed from a SYSTEM level cmd.exe shell. The tool will prevent itself from being run outside of such conditions and produce output such as seen below in the “Sample Output” section.

(S) Windows XP 64 bit is not supported. If run on Windows XP 64, the tool will not attempt to do any of its features, and will display a warning for 5 seconds before exiting. An example of this can be seen in a screenshot below in the “Sample Output” section

(S) The tool requires that the user be logged in. This is achieved by blacklisting the “LogonUI.exe” process that exists when a locked screen is present.

3.2 (U) Deployment

- (S) Run the tool from a SYSTEM level cmd.exe shell
- (S) The tool prompts for an exit timer once all of its steps are completed. The exit timer will not begin until the thumb drive the tool is run from is ejected. If the drive is ejected before the user manually inputs an exit time, the time is assumed to be 7 minutes.
- (S) The tool will clear and hide window once drive is ejected
- (S) The tool stores a text file back to the USB drive of all actions undertaken

3.3 (U) Additional Notes

(S) Dumbo works by discovering which processes have access to the physical camera device and uses that information to corrupt video files. In some instances, programs emulate a camera input to other programs; such is the case with Fujitsu’s YouCam.exe. When this occurs, YouCam.exe will have control of the actual webcam, and feed input to other processes that record images to files as needed. In this scenario, Dumbo will suspend YouCam.exe but will not be able to detect the other processes to which YouCam.exe is feeding images. Although the camera will not be able to record additional frames, Dumbo will not be able to corrupt files that were written to prior, as it is unaware of the processes writing the video files. If the operator sees a process using the camera device, but Dumbo detects no files being written, the operator should manually search for video files.

(S) In some instances, video recording software has the ability to detect it is not responding, and will restart itself; such is the case with iSpy.exe. When Dumbo detects a process using a camera device, it also claims control of the device. If the recording software were to restart itself, it would no longer be able to access the camera until Dumbo exits. In the case of iSpy, although the program may restart, it will be unable to record any additional frames; it will appear as if it was unable to access the camera, due to it already being in use.

3.4 (U) Sample Output

(S) Below is a sample output of a target running Windows XP 32 bit while actively recording a video called from a recording software called “iSpy”. The screenshot was taken with the exit time entered as 5 minutes and is awaiting drive ejection. This represents a successful execution of the tool.

[SECRET]

```

C:\WINDOWS\system32\cmd.exe - Runner.exe

E:\>Runner.exe
=====
Started: 2015-04-02 21:16:06 UTC

Tool is running as SYSTEM <GOOD>
All network adapters have been disabled <GOOD>

Imaging Devices Found: 1 <INFO>
Device Name: USB Video Device
Object Name: \Device\00000082

Loaded driver necessary for XP <GOOD>

Processes Using Imaging Device: 1 <INFO>
C:\Program Files\iSpy\iSpy\iSpy.exe
Suspended: TRUE <GOOD>

Files with Write-Access Found: 2 <INFO>
C:\DOCUME~1\Owner\LOCALS~1\Temp\Perflib_Perfdata_29c.dat <BAD>
C:\Documents and Settings\Owner\Application Data\iSpy\WebServerRoot\Media\video\
BZXZU\1_2015-04-02_16-15-21.mp4 <BAD>

Corrupted: Perflib_Perfdata_29c.dat <GOOD>
Corrupted: 1_2015-04-02_16-15-21.mp4 <GOOD>

Unloaded driver successfully <GOOD>

Exit time in minutes (default is 7): 5
The window will disappear when drive is removed.
You will have 5 minutes to exit once drive is removed.
Network will reconnect and processes will be resumed thereafter.

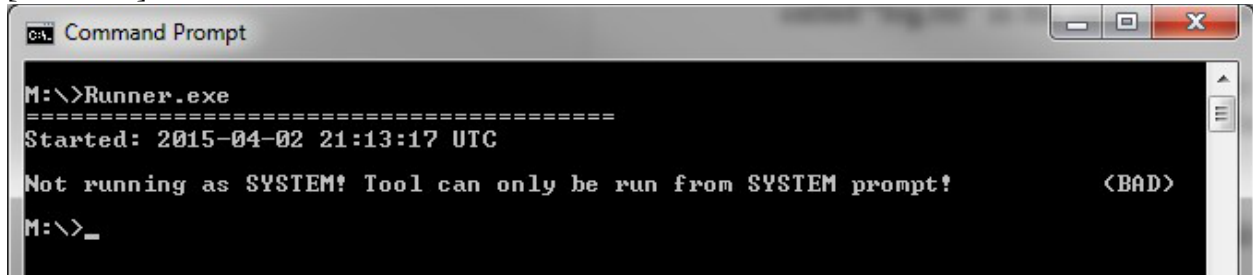
```

[SECRET]

(S) All output above, with the exception of the last statements related to exit time, would also be stored in “log.txt”.

(S) The tool requires that it be run as SYSTEM to execute. If a user attempts to run the tool outside of a SYSTEM cmd shell, the following message will appear. The process will sleep for 5 seconds to allow the user to read before exiting. The following output is the result of a user attempting to simply double-click the executable from Windows 7.

[SECRET]

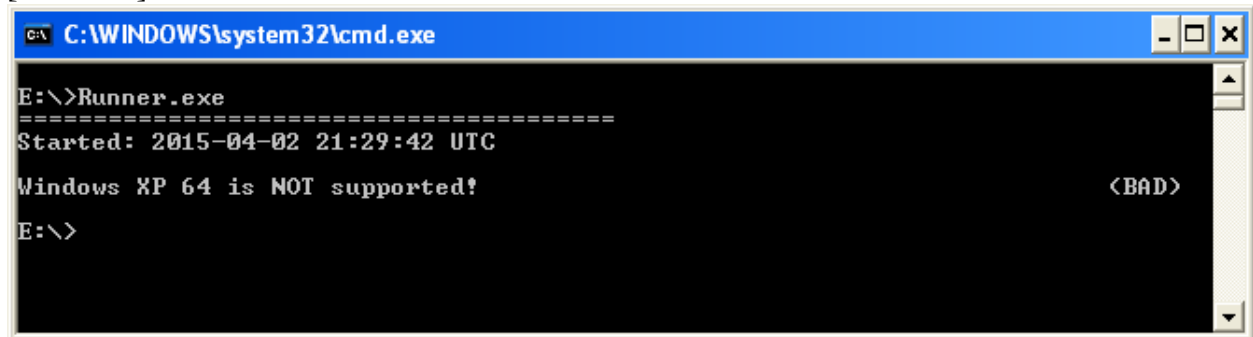


```
Command Prompt
M:\>Runner.exe
=====
Started: 2015-04-02 21:13:17 UTC
Not running as SYSTEM! Tool can only be run from SYSTEM prompt!    <BAD>
M:\>_
```

[SECRET]

(S) Windows XP 64bit is not a supported operating system. If a user attempts to run Dumbo on this operating system, the following message will appear and wait 5 seconds before exiting.

[SECRET]



```
C:\WINDOWS\system32\cmd.exe
E:\>Runner.exe
=====
Started: 2015-04-02 21:29:42 UTC
Windows XP 64 is NOT supported!    <BAD>
E:\>
```

[SECRET]