Engineering Development Group

EzCheese v6.2
User's Guide

Rev. A
12 Apr 2013

Classified By: 2259322
Derived From: COL S-06
Reason: 1.4 (c)
Declassify on: 20350629

Change Log

Doc Rev	Doc Date	Rev By	Change Description	REFERENCE	AUTHORITY / Approval Date
New	04-12-13	XXY	New		

Table of Contents

1. (U) Scope

(U) This document establishes the User Guide for EzCheese v6.2.

1.1 (U) System Overview and Description

(S) COG/HTD and COG/NOD have requested enhancements to the existing EZCheese application that runs from a flash drive to drop a payload, perform a system survey, and run a configurable file collection. As in version 5.1.1 the link file creation GUI, Mac-n-Cheese, has been separated from the survey configuration GUI. The link files for version 6.2 have been upgraded from EnviousArtist to Giraffe. Additionally, link files can be created for windows XP, Vista, or 7 on either 32 or 64 bit machines from any of the operating systems. EZCheese 6.2 also includes the option to deploy multiple payloads with individual blacklists. Unlink previous versions the survey/ file collection executable is not restricted to running from removable media.

(S) Flash drives are configured with the EZCheese application prior to deployment. Once on target, the user browses to a specific folder on the thumb drive which will trigger the Giraffe exploit and launch the EzCheese collection. The tool will run for few minutes and will write all data back to the thumb drive, buried in the folder structure, in an encrypted and compressed format.

1.2 (U) Assumptions and Constraints

(S) In order for the survey tool to run, the user must use Windows Explorer to display a link file crafted for the current OS. This will trigger the Giraffe exploit which will load a dynamically linked library (DLL). If the target is not running any programs in the configured process blacklist, and it is not running a blacklisted OS/ServicePack, it will start the EzCheese survey program. On Windows XP, this exploit will only run once per machine such that if the user browses to that directory again, nothing will happen. On Windows Vista, the dll will load every time the user browses to the folder containing the link. No old survey data will be overwritten and data from additional surveys can be collected and stored in individual folders.

2. (U) Applicable Documents

(S) The following documents pertain to this tool. In the event of a conflict between the documents referenced below, the contents of this document will be considered binding.

- EzCheese v6.2 User Guide_Rev A_2012-04-12.doc (S//NF)
- EzCheese v6.2 TDR_Rev New_2013-04-12.ppt (S//NF)

3. (U) System Description

3.1 (U) Technical References

3.2 (U) System Concepts and Capabilities

- (S) The Giraffe exploit relies on the user inserting a USB flash drive into the target machine and browsing to a specific folder using Windows Explorer. When the specially crafted link files are rendered on the screen, a DLL file they specify will be loaded.
- (S) EzCheese relies on a minimum of three files to be added to the operational drive:
    - the Giraffe link(s) (.lnk files) to load a DLL file
    - the DLL file that is invoked by the link, that launches an executable
    - the configured executable payload to perform the survey

  Nine files are required to target all 32- and 64-bit OS combinations. The number of files required on the thumb drive can be determined using this chart:

Link(s)	Dll(s)	Executable
32-bit WinXP		
32-bit Vista	32-bit dll (if any 32-bit links)	
32-bit Win7		
		32-bit executable (for any config)
64-bit WinXP		
64-bit Vista	64-bit dll (if any 64-bit links)	
64-bit Win7		

- (S) Two different utilities are used for configuration: **EzConfigUltimate** configures the executable, and **Man-n-Cheese** creates and configures the links and Dlls.
- **NOTE:** To re-run the tool on the same machine you **MUST** kill the explorer.exe process and restart it.

3.3 Prerequisites

- (S) The target system must be running a 32-bit or 64-bit version of Windows XP, Windows Vista, or Windows 7.

4. (U) Operation

4.1 (U) Installation and Setup

1. (S) The EzConfigUltimate v6.2 GUI configures various parameters of the operational files written to the flash drive. Various environment variables (such

as %temp% or %appdata%) can be used in collection and output fields. Additionally, where output is being written, additional variables are recognized that can be used to direct multiple surveys and collections to unique locations:

a. %GUID% - a unique id string, changed for every launch
b. %ft% - a hex string derived from the current time
c. %st% - a readable time/date string
d. %drive% - the drive letter of the flash drive (Ex: F:\)

2. (S) The EzCheese tool is configured to work with one specific thumb drive based on its unique drive serial number. If the directory structure is copied to another drive the tool will not run. In order to install the tool on another drive, the user must configure a new installation.

4.2 (U) Preparing for an Operation - Initiating a Session

4.2.1 (U) Initial Setup

(S) The following instructions provide information on how to configure the EzCheese tool in Station by a TOO. There are two separate configuration tools:

1. EzConfigUltimate.exe, which configures the single multi-platform survey executable.
2. Mac-n-Cheese.exe, which creates the links and configures the Dll files to launch the configured survey.

Configuring the survey with EzConfigUltimate:

(U) Double-click on EZConfigUltimate.exe. The following user interface will appear:

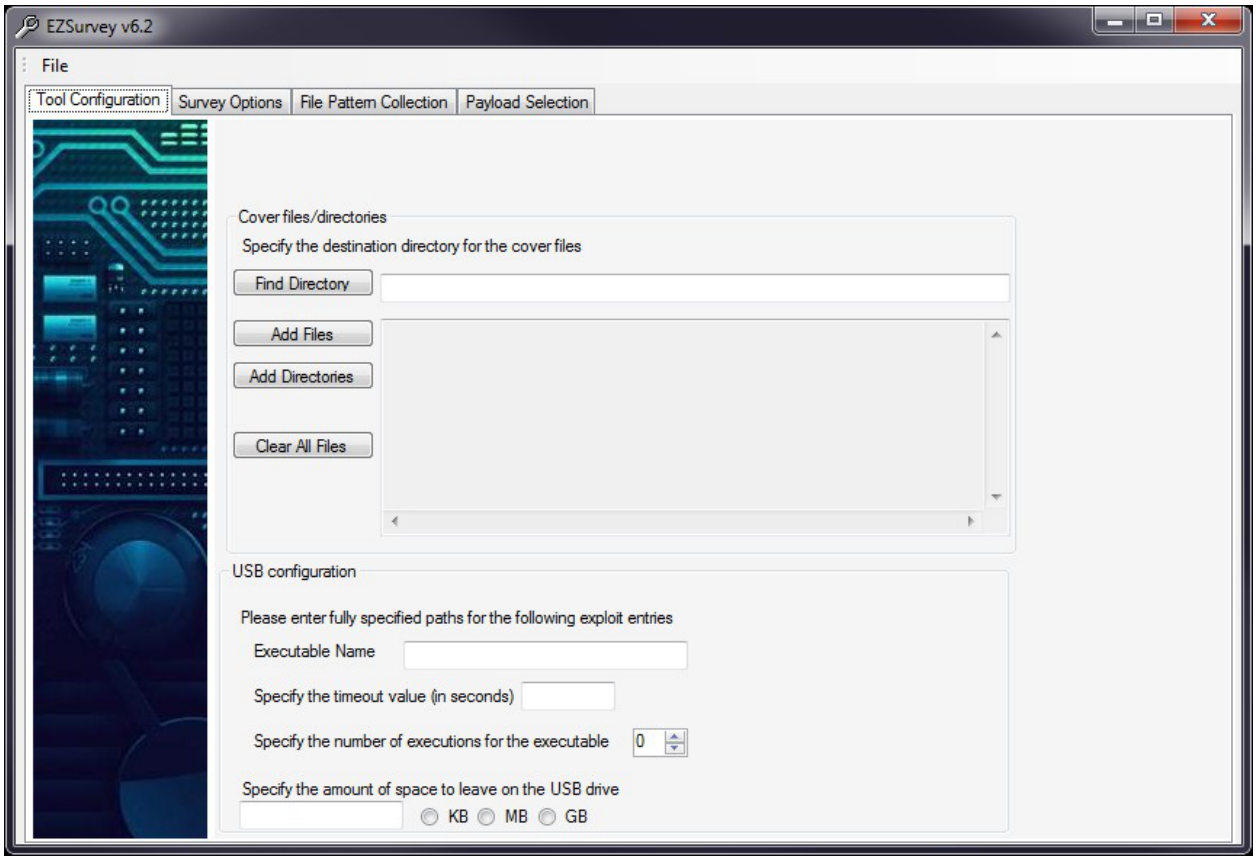

Figure 1: (S) EZSurvey v6.2 - Tool Configuration Tab

(S) The user interface is arranged with four tabs: Tool Configuration, Survey Options, File Pattern Collection and Payload Selection. Each tab offers various options to the user configuring the tool for an operation.

(S) The first tab is the Tool Configuration tab. This page contains a message indicating the current operating system. It notifies the user that this tool must be configured for use on the same operating system as indicated on the screen.

(S) The next section allows for the selection of specific cover files and/or directories to be added to the USB drive. Using this method to copy the cover files to the flash drive prevents the need to browse the drive with Windows after configuration (which sometimes resulted in activation of the tool on the configuration machine when links were present on the drive). The file names specified here are relative to the configuration machine. The “find directory” field should include the target flash drive letter.

(S) The final section allows the user to configure specific options regarding the tool itself. The user must specify the location of the executable, relative to the configuration machine, where the survey executable will be created on the flash drive. Please note that the user must enter a full path to the file on the flash drive, and the drive letter should refer to the target flash drive’s letter as mounted on the configuration machine. Additionally, the executable should have an appropriate extension (.exe). The user may

also specify the amount of space to leave on the drive, the timeout value - a time when the application will terminate upon execution on target.

(S) A new feature for v6.2 is the execution counter. This feature creates a counter at the end of the file. Each time the dll created by Mac-n-Cheese launches the EZCheese dll the counter is decremented.

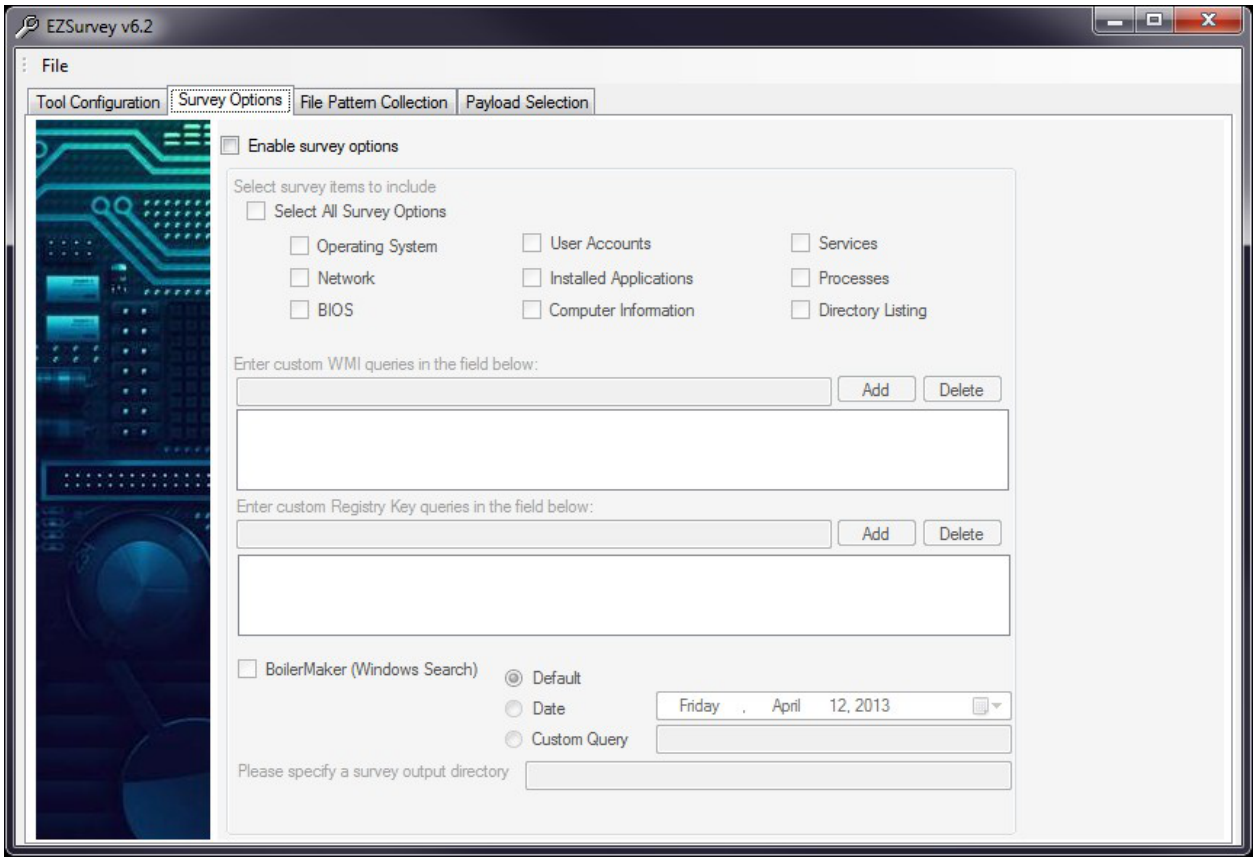

Figure 2: (S) Survey Options Tab

(S) The next tab is for Survey Options (Figure 2). Clicking the Enable survey options checkbox will enable the screen. Now the user can select specific survey options to run on the target. The first section is a set of canned Windows Management Instrumentation queries. The user may also enter custom queries to run against the target for both WMI and against Registry Keys. The last section allows the user to run file system surveys based on Windows Search - as the tool Boilermaker does. Please note that this will only work on Windows Vista and higher - it is disabled for earlier versions of Windows.

(S) The final field is for the user to specify the survey output directory on the flash drive. The survey output directory will be the location where the collection program will save the survey information. If the output directory is intended for the USB drive, begin the path with a backslash or with %drive%. For example: \surveyOutput or %drive

%\surveyOutput. **Note: If a drive letter is included, the application will attempt to write the survey results to the exact path provided - it will not adjust to the drive letter of the USB drive on the target machine.**

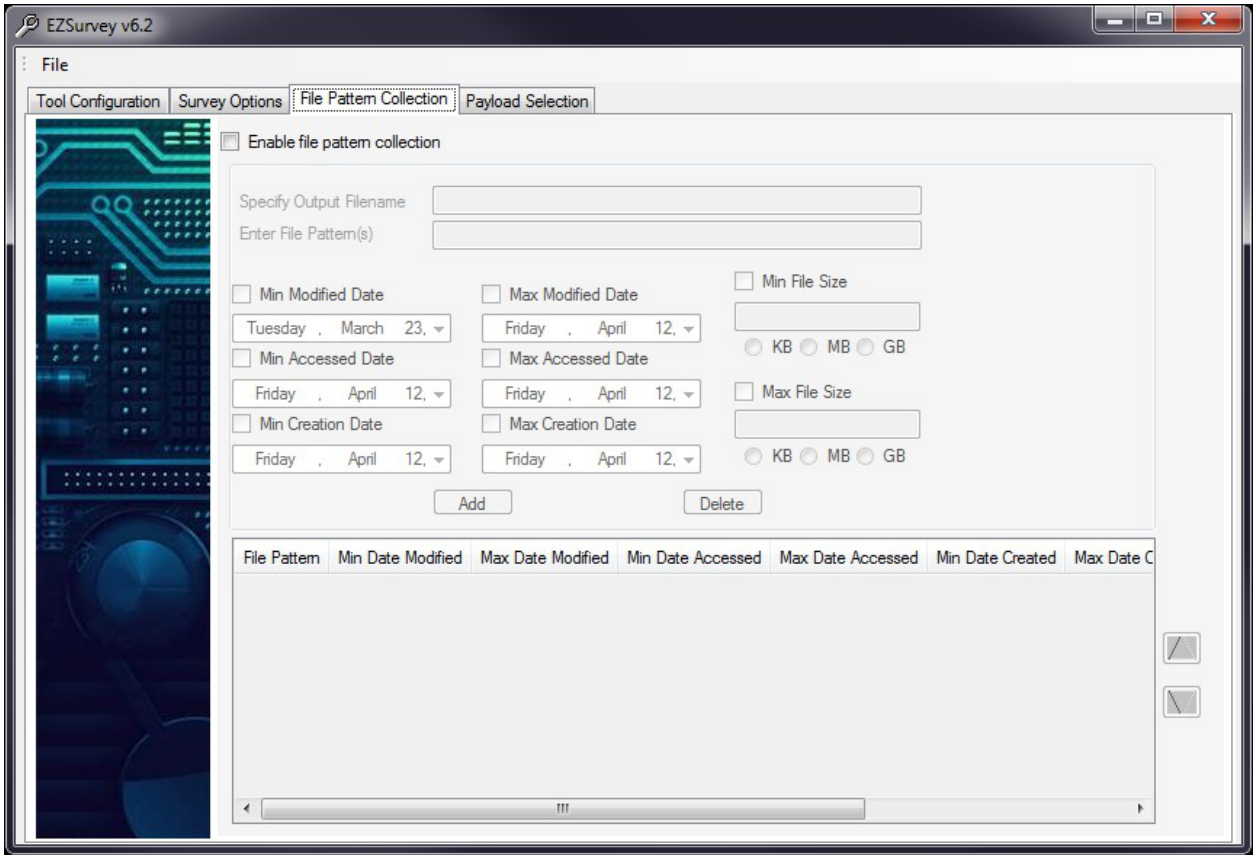

Figure 3: (S) File Pattern Collection Tab

(S) The third tab allows for configurable File Pattern Collection (see figure 3). Again, the user must check the Enable file pattern collection check box to enable the screen. For each file pattern entered, collection criteria is created and saved as a row in the collection priorities table. Wildcards and environment variables may be used in the file pattern field. For example, a file pattern of ***.doc** will collect all Microsoft Word docs off of all fixed drives in the system. A file pattern of **C:*.doc** will collect all Microsoft Word docs off of the C drive. Note that 2007 Office docs have an **x** on the extension, so to include all 2007 Word docs search with **C:*.docx or C:*.doc***. To search for specific files, enter the entire path to the file: **C:\Program Files\sample.txt**.

(S) To enable the date controls and the min/max file size fields, the appropriate check boxes must be selected. Also for each file pattern, an output filename must be specified. This should be the full path to the file on the USB drive, minus the drive letter (i.e. it should always start with a backslash such as "**\output\outputFile.dat"** or it should use the %drive% substitution such as **"%drive%\output\outputFile.dat"**).

(S) Once collection criteria are set, click the **Add Row** button. This will add a row to the table on the lower part of the screen. To add additional file patterns with different collection criteria, change the entries in the Collection Criteria area of the screen, and then click **Add Row** again to add a new entry to the table.

(S) Entries may be moved up and down within the table by clicking on the row of interest to move (it will be highlighted once it is selected), and then clicking the **Up** and **Down** buttons until the row is in the desired position. Note that collection will occur based on the priority of entries in the table, with the highest priority collection set starting at the top. Each collection set will run individually. The top entry in the file collection table is collected during the directory list. Once the directory list finishes, second collection set have been saved, it will move to the next row of the table and so on, until the USB drive is filled to the limit.

(S) To delete a row in the table, click on a row, (again it will be highlighted when selected), and then hit the **Delete Row** button. **Figure 3** highlights an example.

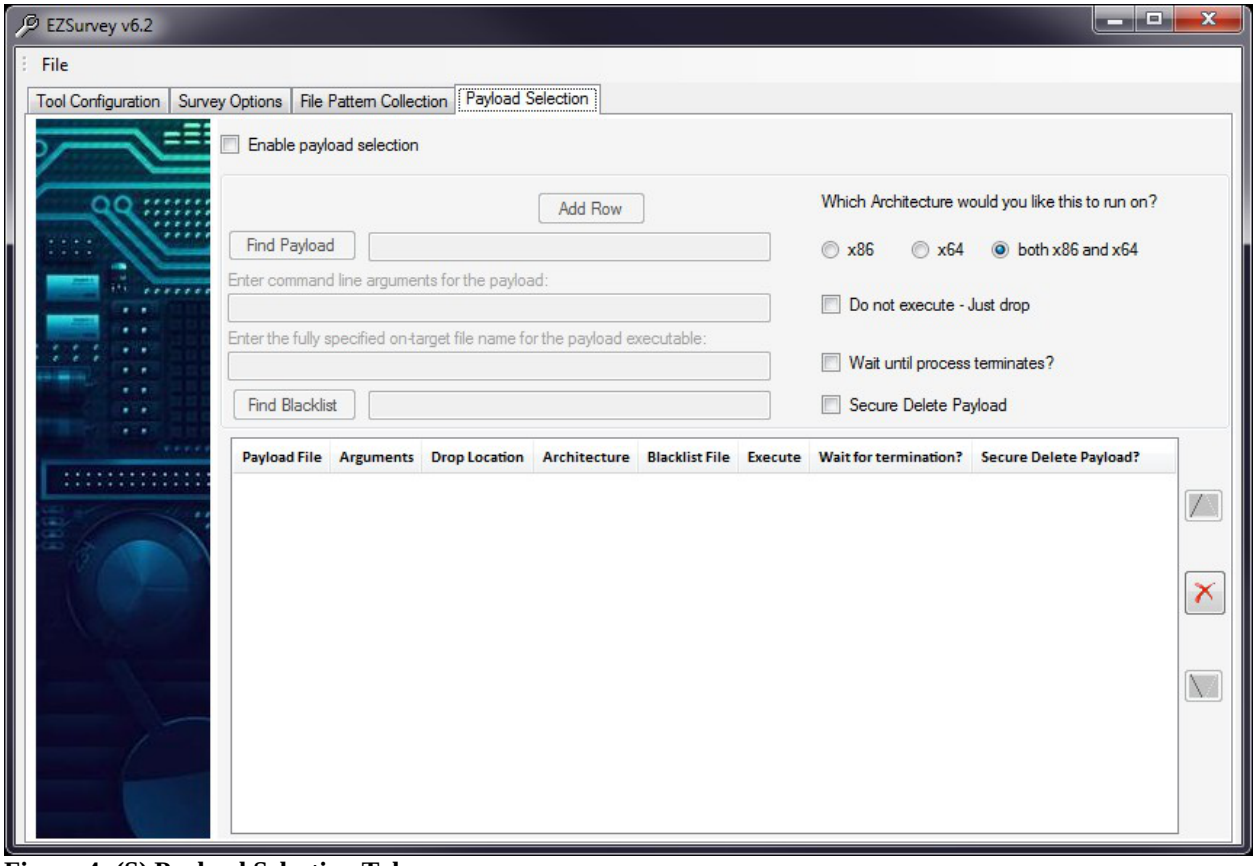

Figure 4: (S) Payload Selection Tab

(S) The final tab, Payload Selection, allows the user to specify payloads to drop on the target machine: See **Figure 4**.

(S) The first step to add a payload is to click the “Add Row” button. This button adds a row to the table at the bottom of the screen. Each payload entry can be modified by selecting an entry in the payload table. After selecting a payload in the table all the values will be loaded into the fields on the top half of the screen. Modifications will be automatically updated in the table.

(S) To select a payload click on the **Find Payload** button. A folder dialog will appear. Simply browse to the location of the payload file on the configuration machine, and then click **Open**. The path to the payload may also be manually entered in the text box located to the right of the **Find Payload** button. To use a file already located on the target system, leave the Payload field blank.

(S) Any arguments used when launching the payload should be entered in the **Payload Arguments** text field. For example, if ipconfig is used as a payload it takes command line arguments such as **/all**. So at the command line a user would type:

ipconfig /all

(S) To include command line arguments using the EZSurvey v6.2 GUI, only the arguments are needed, so the user would enter only **/all** in the **Payload Arguments** text field. Arguments now support using command line variables and the built in EZCheese variables that can be found in the appendix.

(S) Only one path is needed on the target machine: the fully qualified path to the location where EzCheese should drop the payload. This filename refers to the location relative to the target machine where the payload will be written and launched. Environment variables, such as %temp% and %appdata% will be expanded on the target machine. The payload can be written to, then launched from, the flash drive using the %drive% variable described below. If you specify a file that is already located on the target computer, EZCheese can just run that file in place.

(S) Optionally, click on the “Find Blacklist” button to select the text file containing any processes that you want to check for before executing the payload. The blacklist processes should be in a text file with one process per line. A blacklist could look like:

Avp.exe
AntiLogger.exe

(S) EZSurvey 6.2 allows for individual blacklists per payload. These blacklists only impact the execution of the payload they are associated with. Other payloads can still run and the survey / file collection will still execute.

(S) If you are selecting a payload that is architecture dependent you can use the radio buttons on the top right to specify on which architecture you want the payload to run.

(S) To have a file drop to disk but not run, simply click the box “Do not execute – Just drop”.

(S) If the payload(s) you are dropping need to wait before moving on to the next executable click the box next to “Wait until process terminates?”.

(S) EZCheese has the option to “securely” delete a payload. If you click the “secure delete payload” box the payload will be overwritten with zeroes three passes and the filename will also be overwritten with random characters three times. Additionally, Secure delete requires the “Wait until process terminates” box to be checked so that the process has full access to the file.

(S) Click on “Add” after all the parameters have been entered. This adds a row to the Payload Table. You can continue adding payloads with arguments and blacklists using the previous steps.

Configuring the link(s) and Dll(s) with Mac-n-Cheese.

(S) Important: Close *all* explorer windows displaying any contents of the target thumb drive. This will prevent inadvertent launch of the tool on the configuration system. Use dir /a from a command prompt to view.

(S) Launch the Mac-n-Cheese executable. A tabbed configuration tool appears as in figure 5 below. The Load Config and Save Config buttons allow a user to create or load an XML file specifying a full configuration. When all fields are complete, the Create Link(s) button writes the link(s) and Dll(s) to launch a specified payload.

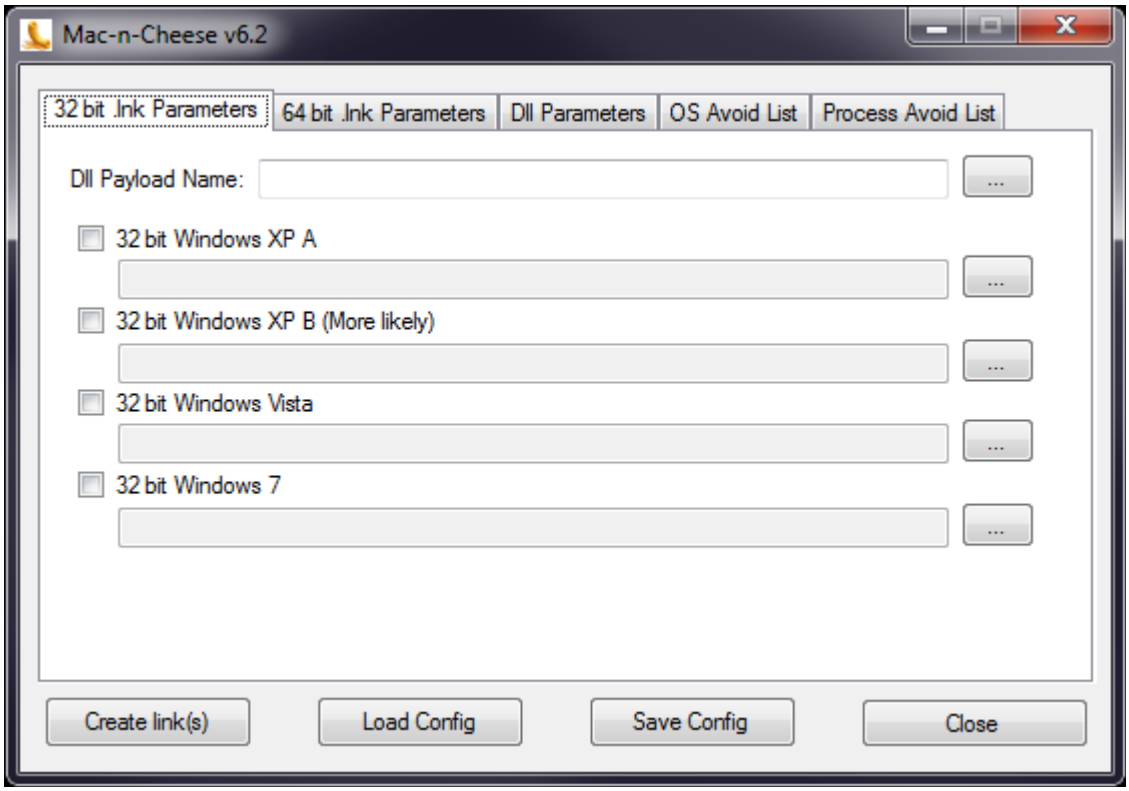

Figure 5: (S) Link Parameters tab

(S) The first two tabs in Mac-n-Cheese are used to create the Giraffe Link files. The first tab is for 32-bit execution and the 2nd tab is for 64-bit execution. Different link files need to be created for the different OS architectures.

(S) In each tab you will need to specify the name of the dll that will get loaded on exploitation and the name of the link files that you want created. You can manually enter data in the text boxes or use the "…" buttons on the right side of the screen to create the file names. To specify a link file name you must first click the check box to the left of that OS. Note, to increase the likelihood of execution on Windows XP, two different link files need to be created. If you do not want the additional link file, Windows XP B is the more likely link file to gain execution.

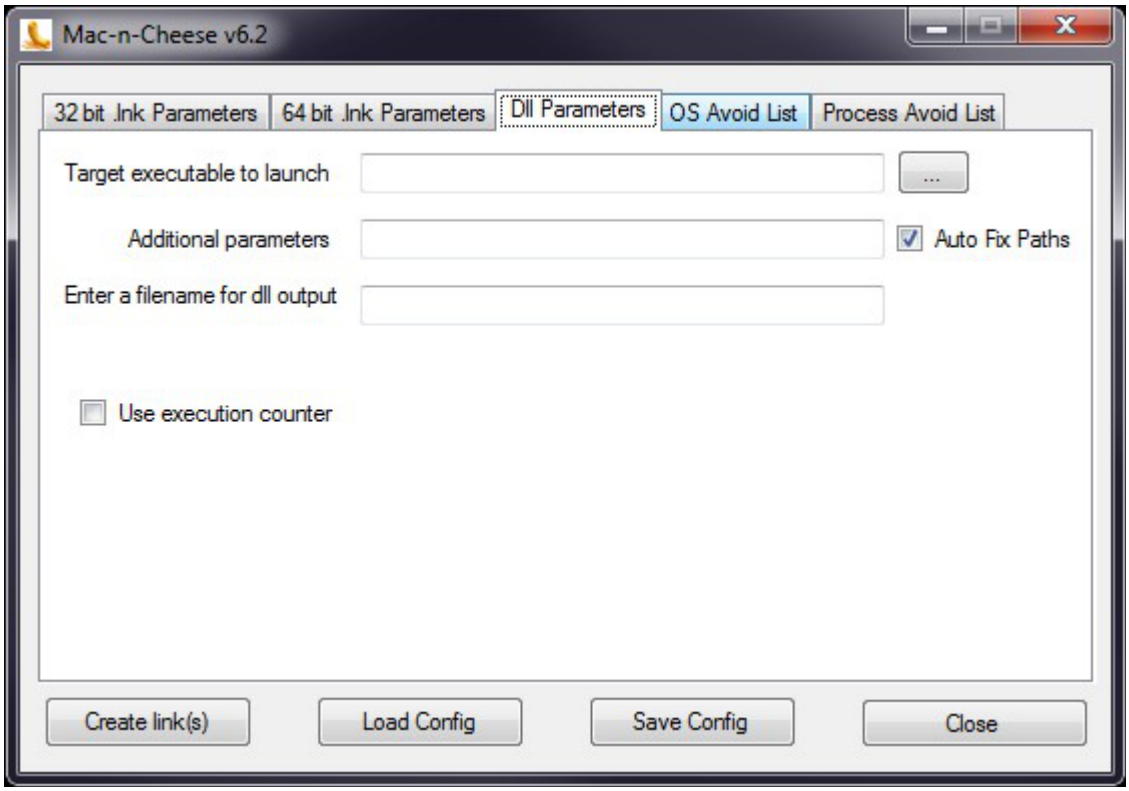

Figure 6: (S) Dll Parameters tab

(S) The Dll Parameters tab sets the file name of the payload executable to launch. Click on the button to the right of the "Target executable to launch" box. Browse to and select the executable that you want launched. In the next box, "Additional parameters", you can specify arguments to pass to the executable.

The "Auto Fix Paths" box is used to make the executable path relative to the drive the link file containing the link file. You will generally want to keep this box checked.

(S) Mac-n-Cheese has the option to have the dll create a file with a process list and OS version. Specify the location where you want the file to be created. It will be created system and hidden in that location. Make sure the location is on the usb drive.

(S) A new option for v6.2 is the "execution counter". If you check this option then you can use the execution counter option in EZCheese. In EZSurvey GUI main screen you can specify how many times the executable should be launched by the Dll.

(S) If no processes or OS / Service Pack combinations are to be avoided, the configuration may be complete at this point.

(S) It is a good idea to save the configuration file on the configuration machine or another non-operational drive for easy reference.

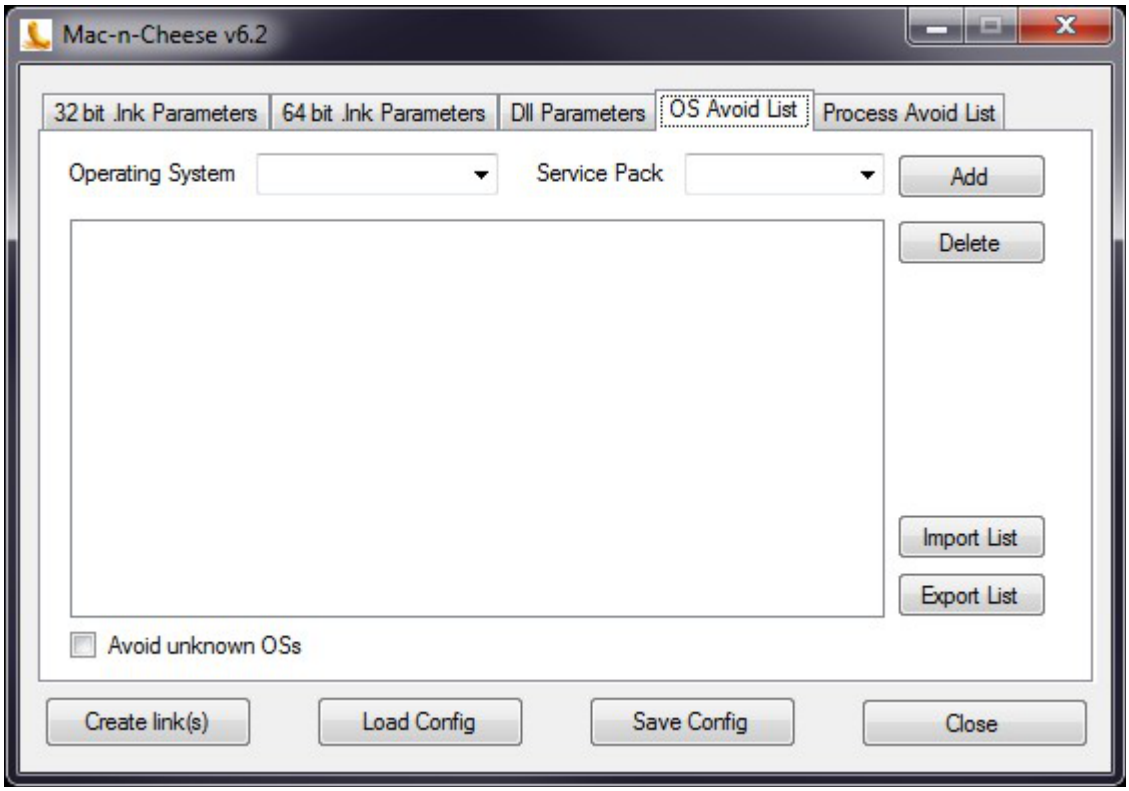

Figure 7: (S) OS Avoid List tab

(S) The next tab is the "OS Avoid List". If the payload executable is known to have issues with specific OS or Service Pack combinations, they can be specified here. For example, if the payload will not work with Windows 7 Service Pack 1, select Windows 7 from the Operating System drop-down, then Service Pack 1 from the Service Pack drop-down, then click the Add button.

(S) If the payload should not be launched on future versions of windows, click the "Avoid unknown OSs" checkbox.

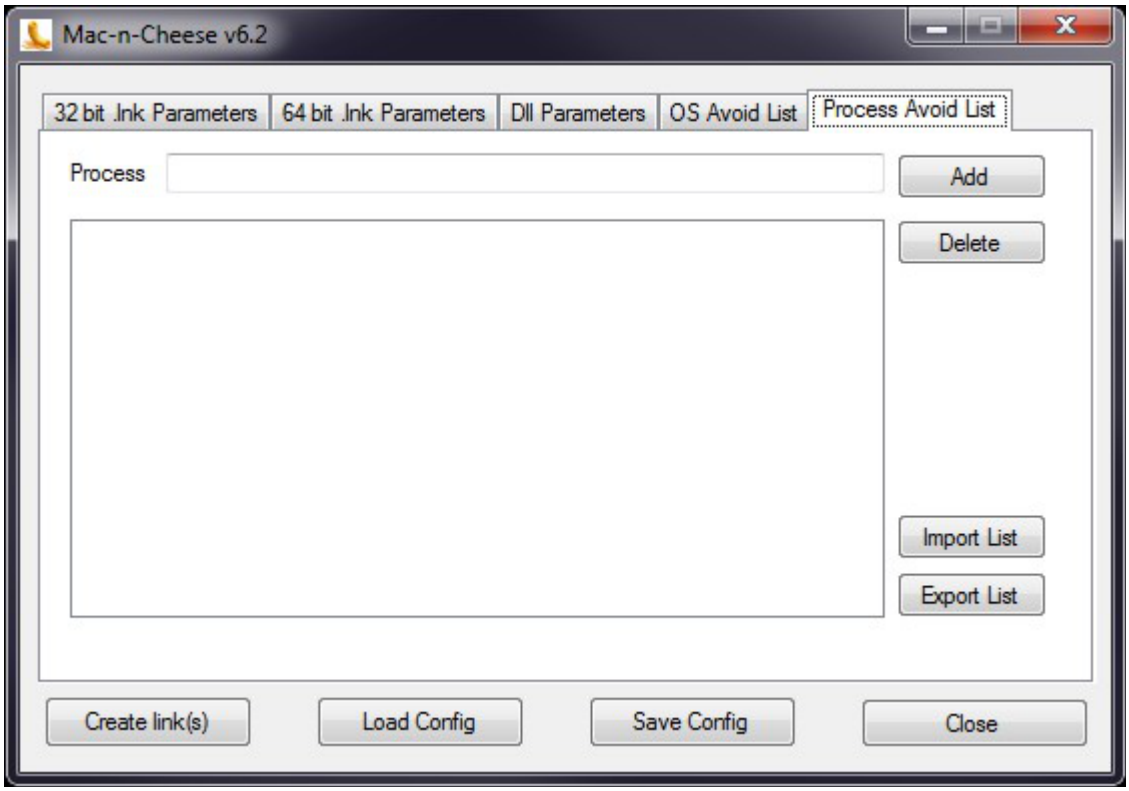

Figure 8: (S) Process Avoid List tab

(S) If the payload executable is known to alert specific AVs or known to be incompatible with certain executables, add the process names to avoid in this tab. For example, if Kaspersky Internet Suite causes alerts when the payload is launched, type avp.exe into the edit box and click the Add button.

(S) This process avoid list will stop the dll from executing the file specified in the "Dll Parameters" tab. If you specified a dll output file the dll will still output the OS and process information to that file so you can see that the dll was loaded and aborted because of a process.

(S) For large lists of processes to avoid, the Import List and Export List buttons can simplify the configuration process.

(S) When configuration is complete, click the Create link(s) button to write the links and Dlls to the specified drive.

4.2.2 (U) Additional Notes

(S) Shortcut variables may also be used in the path names for the target entries and the file patterns. For example, %temp%\dir1\dir2\payload.exe would be expanded as a payload executable directory. Three additional environment variables are expanded if entered on the GUI for the "Survey output directory" and the "Specify output file" fields, as follows:

- %drive% - adds the drive flash drive letter to the filepath (e.g. “G:\”)
- %GUID% - adds a GUID in the filepath
- %ft% - adds the filetime to the filepath
- %st% - adds the systemtime to the filepath

(S) So an example entry would be:

- \Windows\System32\%GUID%

(S) The GUI now allows for a user to save and/or load configuration files. The user must simply navigate to the file menu and select either "Load Configuration" or "Save Configuration" based on the action desired. The file menu also allows for individual tabs to be cleared, if necessary.

4.2.3 (U) Application Configuration

(S) Once all desired collection sets are in the table, and the exploit parameters are set, the user must navigate to the file menu, then select **Configure Exploit** for EZConfigUltimate or **Create Link(s)** for Mac-n-Cheese, to configure the tool. The application now forces the user to save a configuration file before proceeding. Once configured, the tool will copy all cover files, the exe, dll, and link to the appropriate locations on the flash drive.

4.3 (S) Initiating a Session on the Target System

(S) The following steps should be taken to activate the EzCheese tool on a target system:

1. (S) Insert the USB drive into the target system.

2. (S) Open Windows Explorer (some systems will do this automatically upon thumb drive insertion), browse to the USB drive, and then browse to the folder containing the link(s) on the drive. Other than drive activity, there will be no reliable indication that the collection has begun or that the payload has been dropped on the target.

(S) IMPORTANT: The collection process may take several minutes. If the drive is removed from the system before the collection completes, some survey/collection data may not be written to the thumb drive. The user should allow the tool to complete the survey/collection and stop activity to the thumb drive. There is no other visible indication that the process is finished.

4.4 (U) Stopping and Suspending Work

(S) The EzCheese tool cannot be stopped once it is initiated. If the drive is removed while the tool is still running, it will terminate gracefully but only complete a partial collection.

4.5 (U) Contingencies and Alternate States and Modes of Operation

(S) If the link file is removed from the drive, the tool will not execute. Removing this file is a way to disarm the drive if desired.

(S) **Note:** remove the link(s) using a command prompt (for example, type: `del h:\docs\thumbs.lnk`) Browsing to the link in explorer will trigger the tool to collect on the local computer.

4.6 (U) Assistance and Problem Reporting

(S) Please contact EDG/AED/OSB for assistance.

5. (U) Additional Operational Procedures

5.1 (U) Post Processing

(S) The following guidelines should be used to post process any survey/collection results from the EzCheese tool:

1. (S) Plug the target thumb drive into an appropriately classified, controlled computer. Note the letter assigned to the drive.

2. (S) From a command line prompt, copy the CheeseProcessor.exe to the directory where the processed data should be written.

3. (S) Run the CheeseProcessor.exe and specify the full path to the survey data directory (e.g. **CheeseProcessor.exe f:\apps\cache\www\0000**). The collected files are processed and written to the current directory.

4. (S) Run the CheeseProcessor.exe and specify the full path to a specific file to extract the files collected there (e.g. **CheeseProcessor.exe f:\apps\cache\html.cache)**. The files that met specific criteria (established during the configuration phase) are processed and written to a directory within the current directory named CollectedFiles.

5. (S) To post-process the dll output file, run **CheeseProcessor.exe –o *surveyfile***. This will create a file “BasicSurvey.txt” in the same directory as CheeseProcessor.exe.

(S) The collected data will be extracted to the current directory. The following directories and files will be created:

- Directory Listing.txt
- SysInfo.txt
- Arp Table.txt
- Routing Table.txt
- IP config.txt
- CollectedFiles*

- Firefox information:
    - FirefoxBookmarks*

  - bookmarks.html
  - cookies.txt
  - places.sqlite
  - Firefox Cookies.txt
  - Firefox History.txt

- Internet Explorer information:
  - IECookies*
  - IEFavorites*
  - IE History.txt

6. (U) System Backup and Restore

(S) A normal system restore recovery does not reset the OS sufficiently to run EzCheese a second time-- the Windows XP OS activates the link only once. To activate the link again, either 1) rename or copy the link or 2) kill the explorer.exe process and restart it, *then reboot*.

(U) Appendix A: System Footprint

(S) The following files are added to the operational flash drive:

File	Size	MD5 Hash
Exe file	varies	varies
Dll file	varies	varies
Link file	varies	varies

Note: Due to configurability, the size and MD5 hash of any configured file will vary.

(U) Appendix B: PSP Findings

(S) For full PSP findings, please consult the IV&V slides that were delivered with EZCheese 6.1 (Phase 2). Here is a brief summary:

BitDefender: **Alerts will pop up!** On Windows XP, Vista, and 7 32-bit and 64-bit an **ALERT** popped up immediately upon inserting the USB drive on both low and high settings.

Avast! Internet Security: **Alerts will pop up!** On Windows XP, Vista, and 7 32-bit and 64 bit the execution of an .exe file from a USB drive triggers a pop up. If you know your target is running Avast! you can use EZCheese 6.1b which mitigates this pop up.

Kaspersky Internet Security 2012: On Windows XP, Vista, and 7 Kasperksy logged behavior of EZCheese at both low and high settings.

ESET Smart Security: On Windows XP 32-bit not all survey information was collected, possibly due to ESET protecting information or blocking the survey process.

Trend Micro Titanium Internet Security: On Windows XP 32-bit at high settings the payload was not deployed.

Norton Internet Security: On high settings an entry is recorded in the log file.

(U) Appendix B: Artifacts Left Behind

(S) After executing EZCheese there will be information left behind in memory. This includes the name of executables, paths to those executables, and the name and path of link files.