Engineering Development Group

Emotional Simian v2.2
User Manual

Rev. 1.1
August 30, 2013

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

Change Log

Doc Rev	Doc Date	Rev By	Change Description	Reference	Authority/ Approval Date
DRAFT					
1.1	9/3/13	WB	Clean up		

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

Table of Contents

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

1. Scope

This document establishes the user manual for Emotional Simian v2.2.

1.1 System Overview and Description

Emotional Simian (ES) provides the ability to propagate from a primary host to multiple downstream secondary hosts via USB thumb drives. Emotional Simian can also configure a local thumb drive to execute a configured dll to perform surveys, collect files, and/or install payloads.

1.2 Assumptions and Constraints

The operator needs access to either the targeted thumb drive or the primary host. Additionally, persistence for *ES Server(64).exe* needs to be maintained by the operator.

BitDefender alerts and deletes *ES Server(64).exe* on Windows XP. The DLL can still be deployed to XP BitDefender systems, but operators should not deploy the server to any XP BitDefender system.

Any payloads carried to secondary downstream hosts must be dropped to disk to run.

1.3 Conventions

None.

2. Applicable Documents

The following documents, of the exact issue shown, form a part of this document to the extent specified herein. In the event of a conflict between the documents referenced herein and the contents of this document, the contents of this document will be considered binding. The following documents may be found in the EDG/AED share:

- Emotional Simian V2.2 UserGuide.doc
- Emotional Simian V2.2 TDR.ppt

3. System Description

3.1 Technical References

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

MD5 Values:

Emotional_Simian_Config.exe	199CE7F487C43B3562041BC1D94EDDBF
Emotional_Simian_Config.exe.config	D0089718B62F6E9D91154ACAE007699C
Emotional_Simian_Config.vshost.exe	B4D5137244BB4259A208B815E7C9F7B9
Emotional_Simian_Config.Vshost.exe.config	D0089718B62F6E9D91154ACAE007699C
ES Server.exe	FDB376AAC8F1D3B3891ED49C90CF9770
ES Server64.exe	1CDA0D262661F8561ACD292565DE5AE2
ES Setup. exe	F8A27982E0D8B315CFCEE0F1EF831884
Extract WM Files. exe	1E2092CF75760F96DC5543D233FD7072
Get SN. exe	851AFAFB0EEA7C30F80B20D676BEF84E
Keygen. exe	4305E6275B98A6C22BCA762350615461
Post Processor. exe	D3F1C6CCA9F7CDDFDCBF02F7EF3A0BCF
Whack_Thumbdrive. exe	FF8CF6E59FFBB328C179492D0C391AD8
Dll_Payload.dll	3B90EF9C6BA44B8EE0F0313CA6990614
Dll_Payload64.dll	04F94FE005613B5C0CE13DAFB640D645

3.2 System Concepts and Capabilities

- **Emotional_Simian_Config.exe** – This is the setup GUI used by the user to create the .cfg file to be laid down on the primary host.
- **./Internal/ES Setup.exe** – This tool is called by *Emotional_Simian_Config.exe* and is used to package the .cfg file.
- **./Internal/KeyGen.exe –** This tool is called by *Emotional_Simian_Config.exe* to create a public-private key pair.
- **./Internal/Post Processor.exe** – This tool is used to decompress, decrypt, and piece together any collected files.
- **./Internal/ES Server.exe** – Executable to be laid down on a 32-bit primary host. This tool runs in the background and watches for the insertion of a whitelisted thumb drive. Upon insertion of a whitelisted thumb drive, ES Server will infect the drive with the required files.
- **./Internal/ES Server64.exe** – Executable to be laid down on a 64-bit primary host.
- **./Internal/Extract WM Files.exe** – This tool extracts files stored on the covert storage of the thumb drive.
- **./Internal/Get SN.exe –** This tool can be put on a target to find the serial number of targeted thumb drives (This can also be done by looking at the registry files).
- **./Internal/Dlls/DllPayload64.dll** - The 64-bit version of the Emotional Simian dll payload.

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

- **./Internal/Dlls/DllPayload.dll** – The 32-bit version of Emotional Simian dll payload.
- **./Internal/WhackDrive.exe** – This tool is called by *Emotional_Simian_Config.exe* to weaponize a local thumb drive.

3.3 *Prerequisites*

- The configuration must be executed on a Windows 7 machine.
- Access to the primary host must be gained through other means.
- Access to the thumb drive (if not a remote operation).
- The primary host must be running Windows XP or later.
- Server.exe or Server64.exe must be run with administrative privileges.
- Persistence is to be set up by the operator.

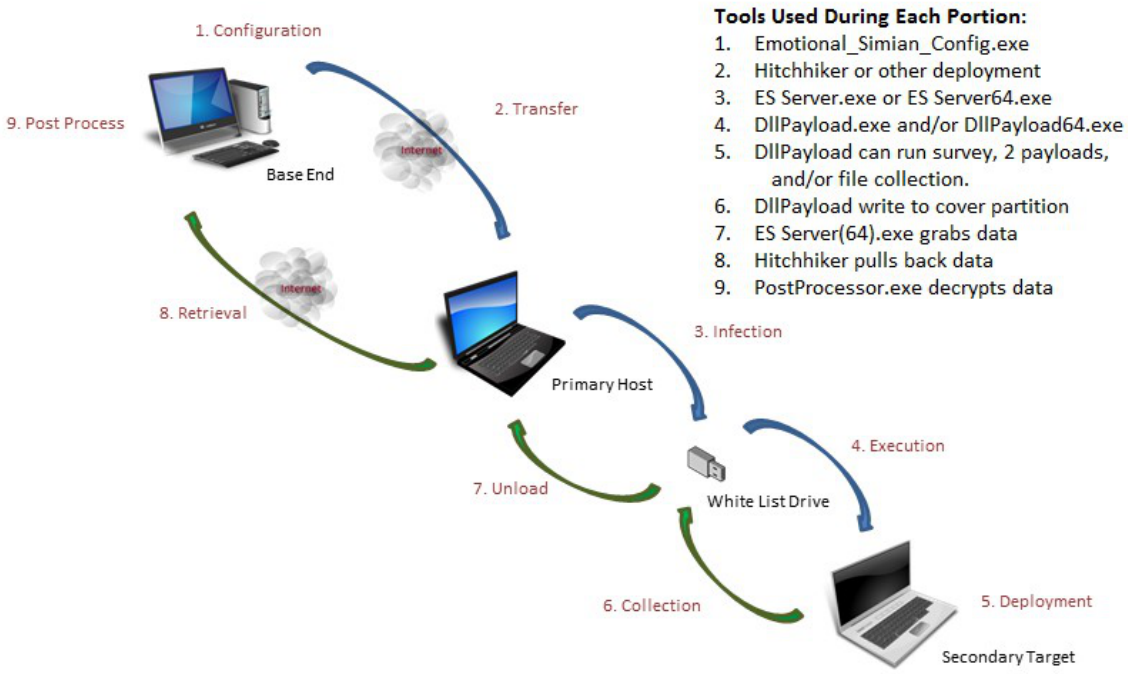
4. Operation

4.1 Quick Overview

The following is a quick overview of the end-to-end process for Emotional Simian and the tools used during each portion of the operation. A more detailed explanation of each step will come later.

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06



1. **Configuration**: Performed by the operator on a Windows 7 machine using *Emotional_Simian_Config.exe*. This tool generates the required .cfg file containing all the payloads and configuration information required for *ES Server(64).exe*.
2. **Transfer**: *ES Server(64).exe* (depending on target bitness) is installed on the primary host with the configuration (.cfg) file via some deployment method. These two files can be placed wherever the operator desires and named whatever the operator desires, but they must be named the same (e.g. clevername.exe and clevername.cfg). *ES Server(64).exe* should then be executed and persistence must be setup by the operator.
3. **Infection**: Upon introduction of a whitelist drive, *ES Server(64).exe* will place the *DllPayload(64).dll* with the appropriate lnk files on the thumb drive (Named whatever the user configured them). The lnk files will cause *DllPayload(64).exe* to run when the user views the lnk file in explorer.
4. **Execution**: If the whitelist drive is introduced to the proper OS for the generated lnk files and viewed in an explorer window, *DllPayload(64).dll* will gain execution. *DllPayload(64).dll* will then launch itself under rundll32.exe, attempt to escalate privileges, and begin to check the configured kill date, master black list, and if the computer had been seen before. Execution will always occur due to the exploit; however, if any of the previous conditions are met then the program will immediately exit.
5. **Deployment:** If the initial requirements are met, ES will attempt to deploy the configured payloads. Each payload has a unique configured decision criteria. The

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

payload can also conduct a survey, or collect files based on the configurations set by *Emotional_Simian_Config.exe*.

6. **Collection:** If *DllPayload(64).dll* does file collection and/or a system survey then the files will be chunked up and written back to the covert partition that exists on the thumb drive.
7. **Unload:** When the thumb drive returns to the primary host, *ES Server(64).exe* will pull any collected files off the covert partition and store them as hidden system files on the Primary Host hard drive (The data is then deleted from the covert partition).
8. **Retrieval:** The operator will then pull the desired files from the Primary Host and place them on the Base End for post processing.
9. **Post Process:** *PostProcess.exe* decrypts, decompresses, and stitches the collected files back together. The recreated files will be dumped into the desired location.

4.2 Configuring Emotional Simian

Emotional_Simian_Config.exe must be run on XP SP3 or later, preferably on Windows 7. *Emotional_Simian_Config.exe* will generate:

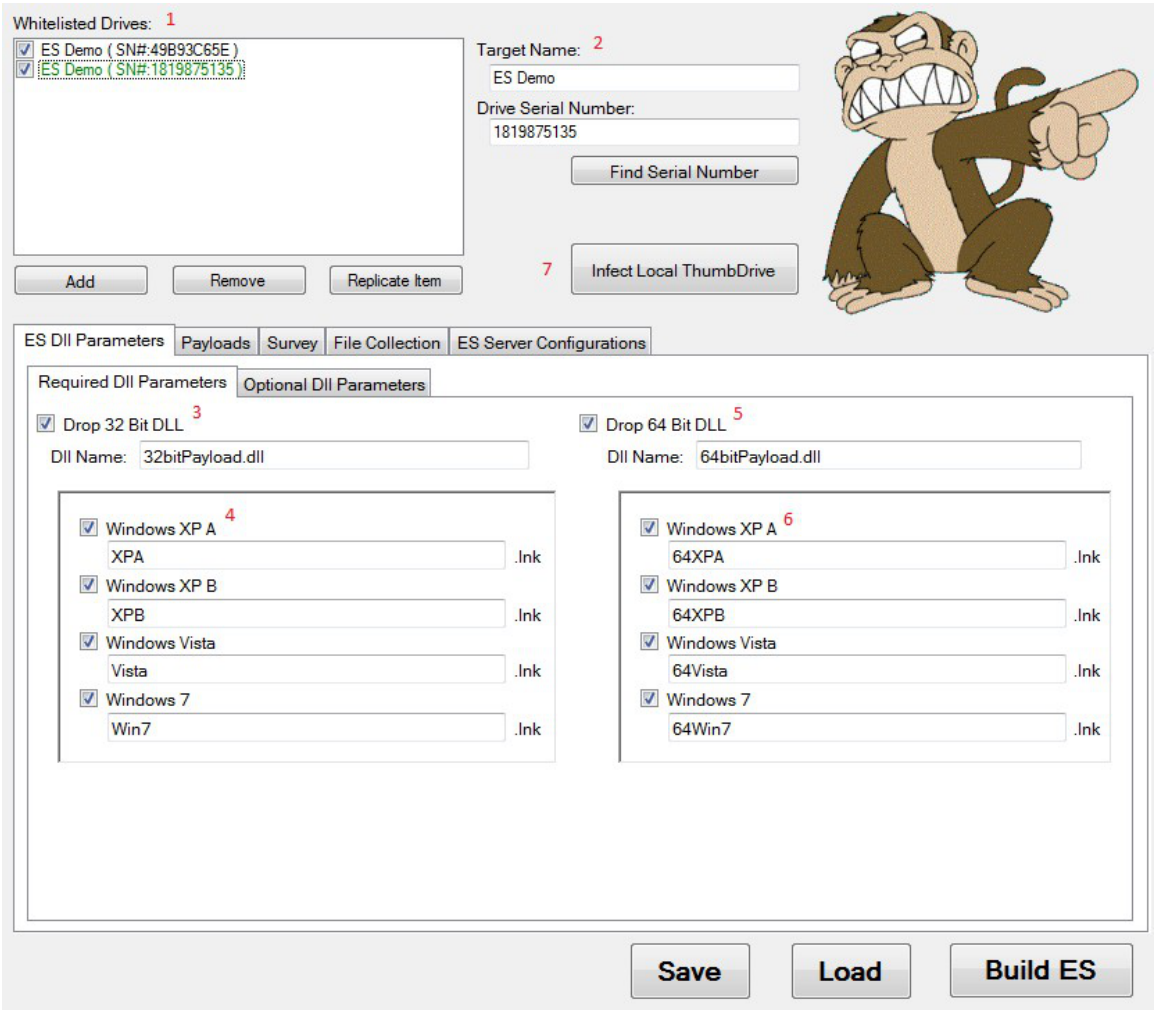
ES Server.exe and ES Server.cfg files to be installed on the Primary Host.
An XML file of all the configurations from the configuration tool along with the public private keys.

NOTE: DO NOT LOSE THE PRIVATE KEY! IF THIS IS LOST, THEN <u>WE WILL BE UNABLE TO DECRYPT ANY COLLECTED FILES</u>.

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

4.2.1 Main Form:



1. **Whitelisted Drives:** This is a list of drives that have been configured for use. If a drive is not checked it will be disabled, but will still be saved in the XML configuration file. The same name with multiple serial numbers is allowed; however, you cannot check them both. In the GUI, note that "checked" and "selected" are two different things: The drive highlighted in green is the one selected; Checked means it will be included in the configurations. **The ES Dll Parameters settings apply only to the selected (green) Whitelisted drive.**
2. **Target Name:** This name is for documentation purposes only, and will not be included in any operational context; it helps the operator keep track of who owns a particular thumb drive. I.e. JQJBADGUY/1 (SN# 889238923484)

SECRET//X1

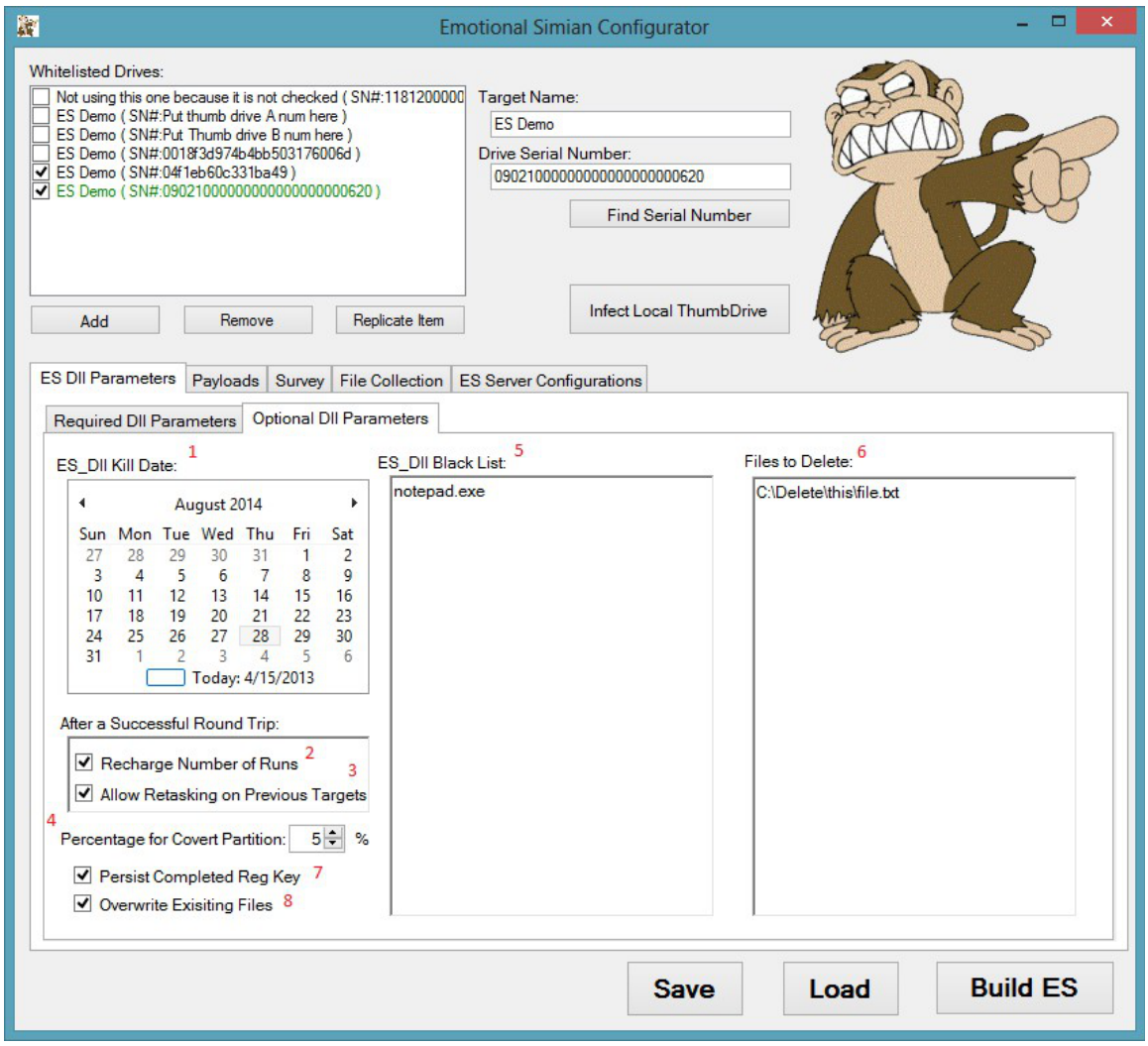
CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

3. **Drop 32 DLL:** This configures the *ES Server(64).exe* to put down a 32 bit DLL on the selected whitelisted thumb drive. Each whitelisted drive can uniquely name the DLLs and lnk files. The only stipulation on the naming conventions is the link files must be named .lnk (already done for you), and the dll must end with an extension (It does not need to be .dll, but it has to have .something).
4. **32 bit lnk files:** These link files are required to execute the ES DLL. If fields are filled out but not checked the information will be saved in the XML file, but not enabled in *ES Setup.exe*.
5. **Drop 64 DLL:** Same functionality as *Drop 32 DLL* for 64 bit DLL files.
6. **64 bit lnk files:** Same functionality as *32 bit lnk files* for 64 bit DLL files.
7. **Infect Local Thumb drive:** This button instantly infects a thumb drive that is plugged into the system instead of running ES Server.exe. First, click the desired 'Whitelisted Drives' configuration and then click this button. *The Pre and Post Build executable/batch scripts will run with this button.*

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

4.2.2 Optional Dll Parameters:



1. **ES_Dll Kill Date:** *DllPayload(64).dll* will exit immediately after exploitation if this date is surpassed. Default is two years into the future.
2. **Recharge Number of Runs:** When the selected whitelisted thumb drive comes back to the Primary Host computer, if checked, *ES Server(64).exe* will put the number of surveys and payload runs back to their original amounts.
3. **Allow Retasking on Previous Targets:** When the selected whitelisted thumb drive infects a secondary host with DllPayload(64).dll, it places a GUID in the Registry under HKLM\Software\ Microsoft\Active Setup or HKLM\Software\ Microsoft\MNU depending upon the **Persist Completed Reg Key** check box. If the selected whitelisted thumb drive has not made it back to the Primary Host

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

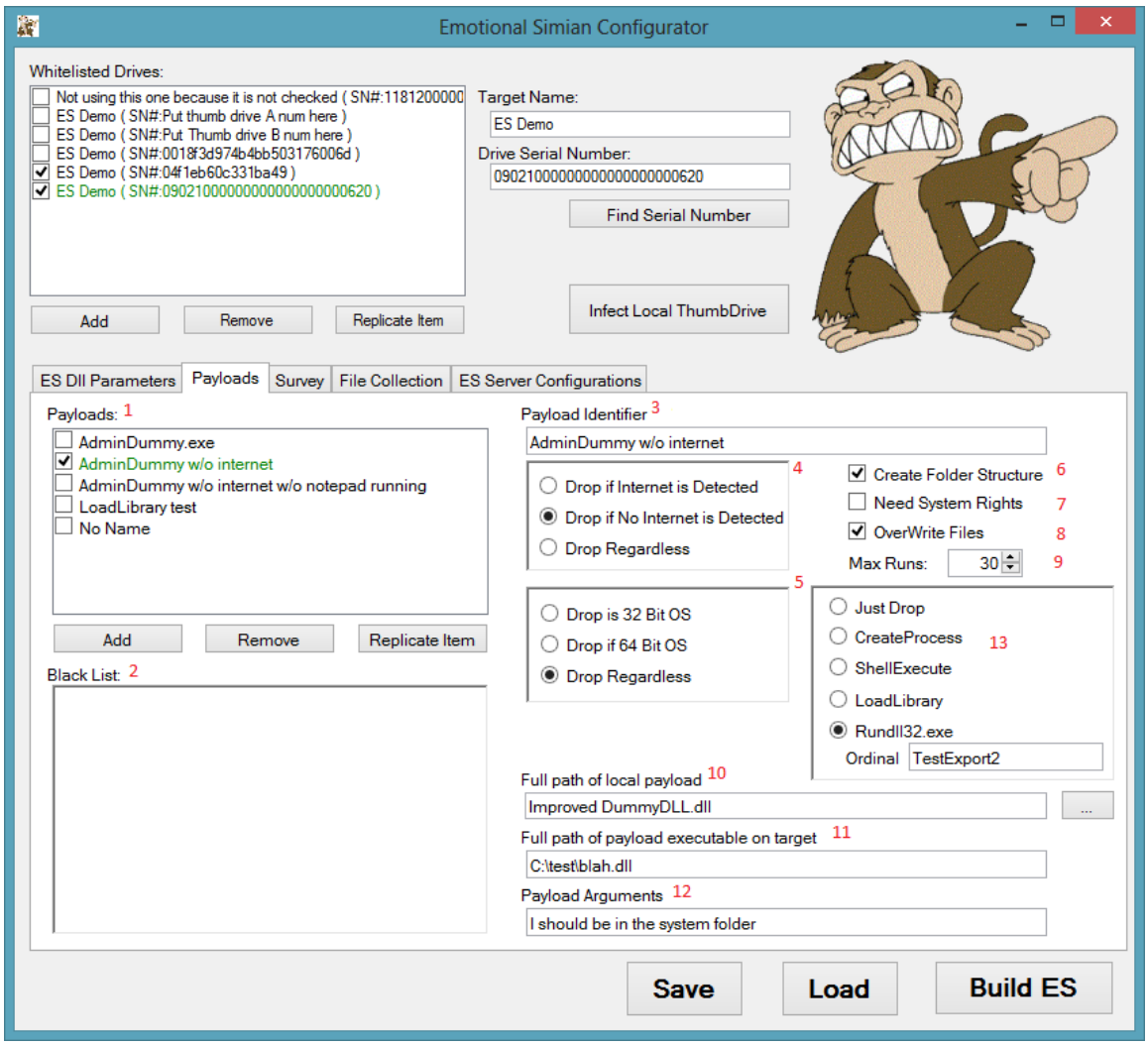
(running *ES Server(64).exe*), it will not trigger on that secondary host a second time. Once the selected whitelisted thumb drive comes back to the Primary Host, if checked, *ES Server(64).exe* will change the GUID located in *DllPayload(64).dll*. This will allow *DllPayload(64).dll* to re-infect secondary hosts.

4. **Percentage for Covert Partition:** This is how much covert storage to allocate on the selected whitelisted thumb drive. *ES Server(64).exe* will attempt to provide what was requested, but if it is not possible then *ES Server(64).exe* will provide the maximum it can without going over the percentage specified. *Taking more than 10% of the drive could be noticeable by the user. (Default is 5%). 0% will configure ES server to not put a covert storage on the drive. 0% does not support collecting surveys or files, but will run payloads.*
5. **ES_Dll Black List:** This is a list of executables where the presence of one will cause DllPayload(64).dll to immediately exit. *Note Black List is an 'or' condition.*
6. **Files to Delete:** The last thing *DllPayload(64).dll* does (post survey, file collection, and/or dropping of the payloads) is the file deletion. *These files have to be absolute paths. If the file is in use, then the file will not be deleted.*
7. **Persist Completed Reg Key:** If this box is not checked, the reg key that indicates the dll has fired will be deleted on reboot. If this box is checked, the reg key will persist on reboot. *The presence of the reg key prevents the secondary host from being infected a second time.*
8. **Overwrite Existing Files:** If this box is checked, and the Dll or lnk files exist on the selected whitelisted thumb drive, they will be overwritten. However, if the files are deleted then they will not be replaced. So, if the Target/Owner of the thumb drive deletes the files, the files will not show up again unless a new configuration file in installed.

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

4.2.3 Payload Tab:



1. **Payloads:** There can be up to ten payloads in this box, but only three payloads may be checked for each thumb drive. The payload highlighted in green is the current selected payload. To create an additional payload, first update the *Payload Identifier* to avoid altering existing payloads.
2. **Black List:** This is a list of executables where the presence of one will cause the payload not to be installed on a secondary host. *Note Black List is an 'or' condition.*
3. **Payload Identifier:** Simple identifier used only in configuration that gives the operator a quick description of the payload associated with each thumb drive.
4. **Drop if No Internet/ Internet:** Self-explanatory.

SECRET//X1

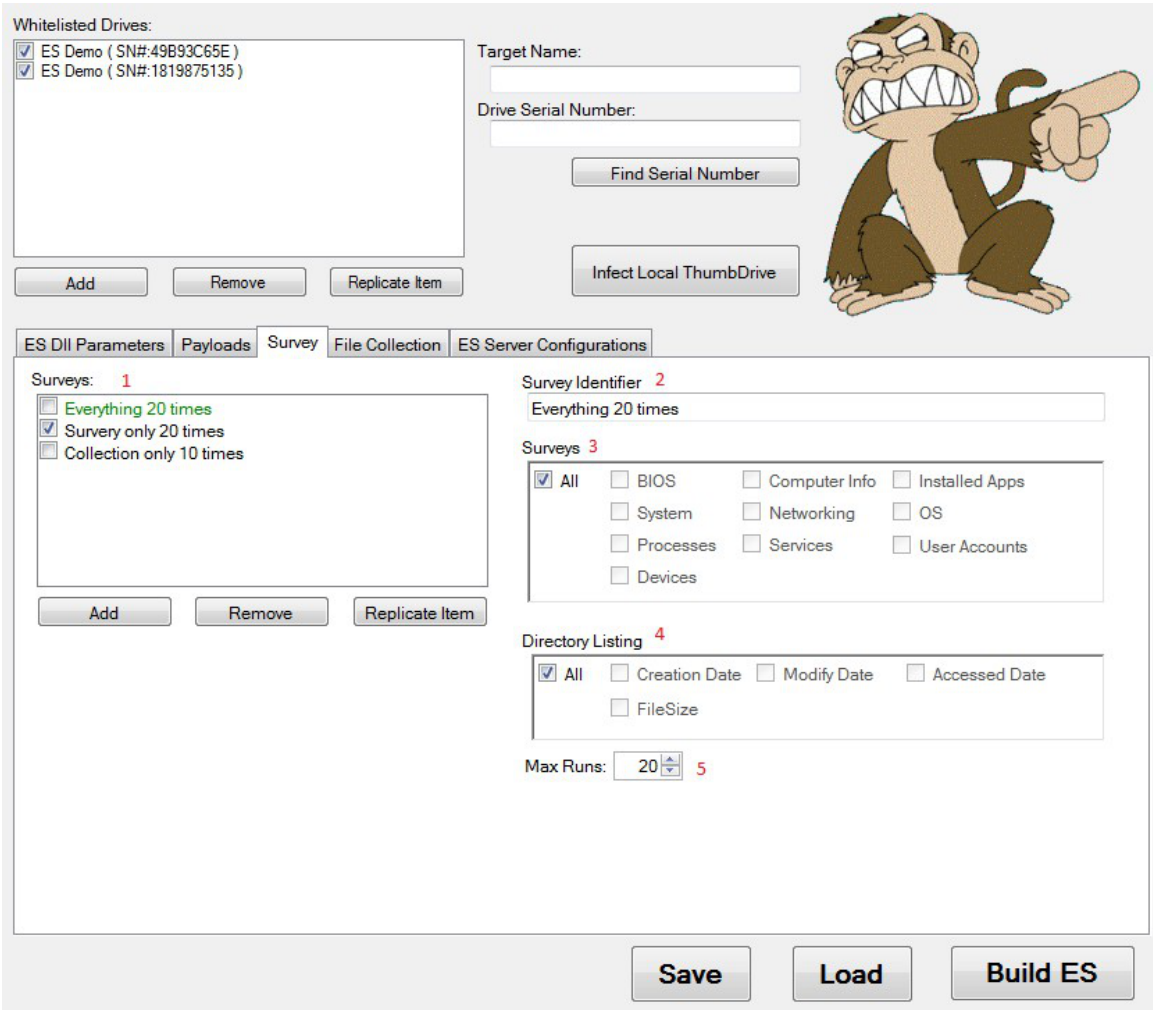
CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

5. **Drop if 32/64 bit:** Self-explanatory.
6. **Create Folder Structure:** If checked, *DllPayload(64).dll* will create the folder structure defined in **Full path of payload executable on target** on the secondary host.
7. **Need System Rights:** Payload needs System (not Admin) rights.
8. **OverWrite Files:** If checked, the payload will replace a file of the same name.
9. **Max Runs:** The max number of times the payload can drop. The number of runs is stored as the creation time of *DllPayload(64)*.dll. If *DllPayload(64)*.dll cannot modify the creation time it will not drop and run the payload. This prevents *DllPayload(64).dll* from working from a CD or write-blocker. *Note: When dropping both 64 bit and 32 bit DLLs, the total includes BOTH.*
10. **Full path of payload executable:** Location and name of the payload.
11. **Full path of payload executable on target:** Path and name of where the payload will be created on the secondary host. Payloads will not be overwritten unless the *OverWrite Files* control is checked. Existing (non over-written) payloads will not be executed.
12. **Payload Arguments:** Arguments that will be fed into the payload at run time.
13. **Run Payload as:** Select how to run the payload.
    Just Drop: Self-explanatory.
    Create Process: Execute .exe payload.
    Shell Execute: Execute .exe payload using a command shell.
    Load Library: Load .dll payload into DllPayload(64) process.
    Rundll32.exe: Run .dll payload as its own process from Rundll32.exe.

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

4.2.4 Survey Tab:

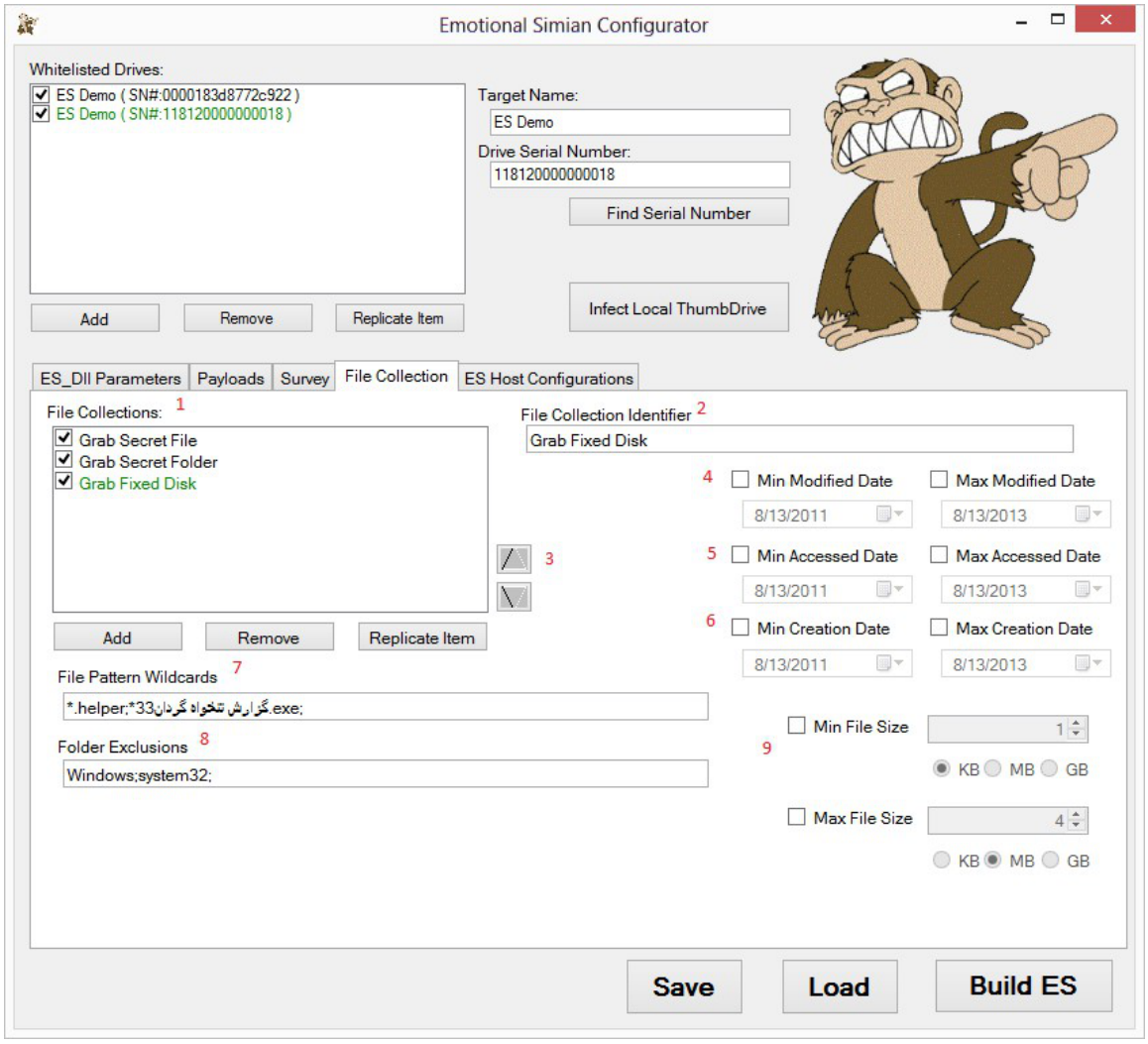


1. **Surveys:** This is the list of surveys that have been created. Only one survey per thumb drive is allowed.
2. **Survey Identifier:** Simple identifier used only in configuration that gives the operator a quick description of the survey associated with each thumb drive.
3. **Survey checkboxes:** The names are intuitive.
4. **Directory Listing:** These boxes select what information about each file is in the directory listing.
5. **Max Runs:** This is the maximum number of times a survey and/or directory listing is run for a *DllPayload(64).dll*.

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

4.2.5 File Collection Tab:



1. **File Collections:** This is the **prioritized** list of file collections that have been created, ten entries maximum. Prioritization is done concurrently, thus if files are found in lower priorities before any higher priorities are found then the first low priority file is collected. The point of this is to guarantee something is always being collected—Priority is essentially trumped if there is no work in the higher priorities. Only checked members will be associated with each Whitelisted drive. *Beware that comparing wildcards to every file on the computer can take up a lot of time; keep file collections to a minimum if time is an issue.*

SECRET//X1

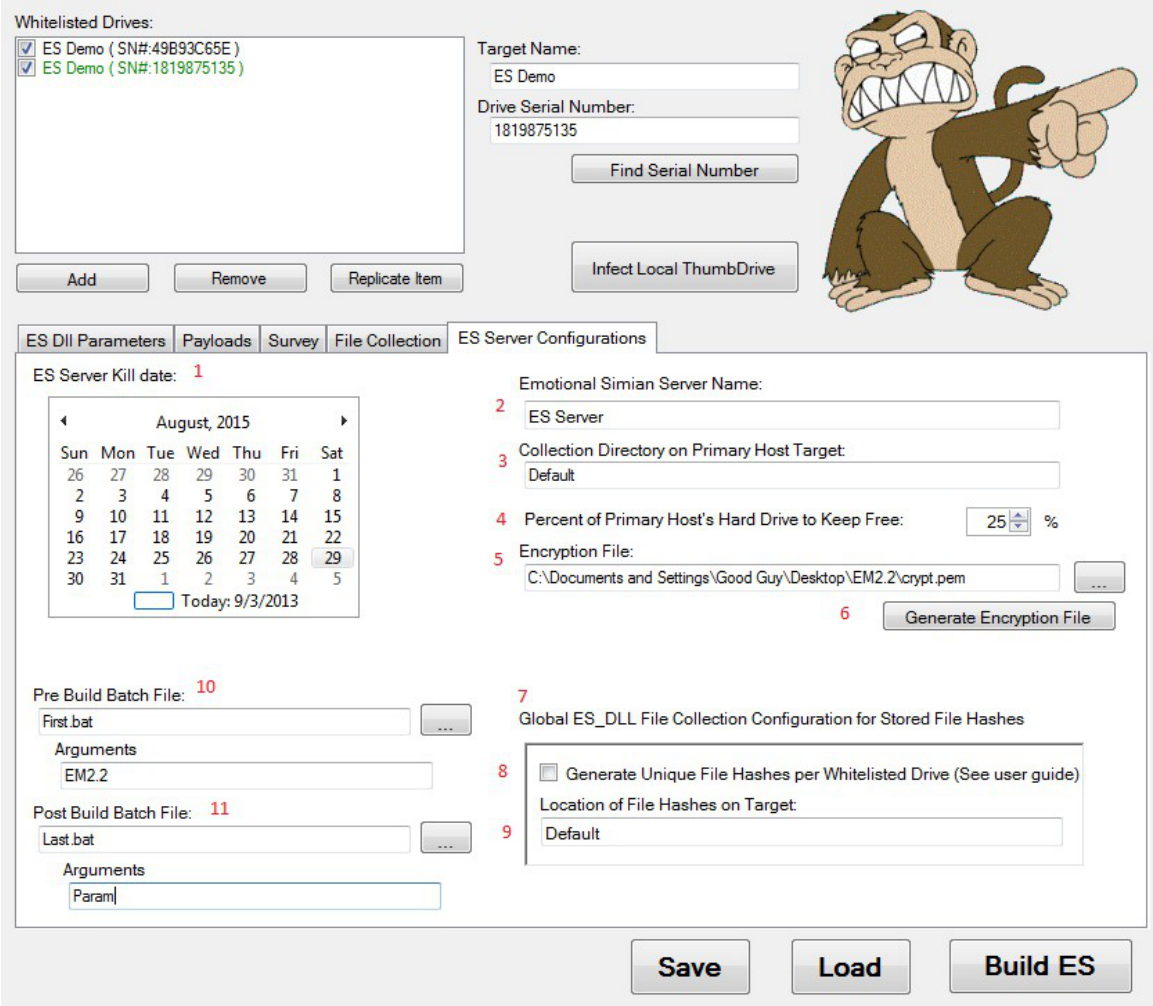
CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

2. **File Collection Identifier:** Simple identifier used only in configuration that gives the operator a quick description of the file collection associated with each thumb drive.
3. **Up / Down Arrows:** Adjust collection priority
4. **Min / Max Modified Date:** If the file exceeds the max, file will not be collected; if the file falls below min, file will not be collected.
5. **Min / Max Accessed Date:** If the file exceeds the max, file will not be collected; if the file falls below min, file will not be collected.
6. **Min / Max Creation Date:** If the file exceeds the max, file will not be collected; if the file falls below min, file will not be collected.
7. **File Pattern Wild Cards:** This is a bit tricky. File wildcards are compared against the entire file path. To collect any file ending with Secret.doc, enter "*Secret.doc;" because
   Secret.doc != c:\user\desktop\Secret.doc, but
   *Secret.doc does equal c:\user\desktop\Secret.doc (and c:\user\desktop\Top Secret.doc). Use *\Secret.doc to specify only files named Secret.doc.
   Each file wild card must be separated by a semi-colon and end with a semi-colon; If collecting only files from the C:\ drive use "c*\secret.doc;". The slash after the * specifies files matching that exact name. "c*Secret.doc;" will collect c:\junkfolder\Not-A-Secret.doc
8. **Folder Exclusion:** These are folders to not collect files from. They must be separated by semi-colons, and end with a semi-colon. Wildcards do not work on these folders, so the name must be entered perfectly (capitalization does not matter). Program Files and Program Files (x86) are two different folders. To exclude all program files enter both:
   Program Files;Program Files (x86);
9. **Min / Max File Size:** If the file exceeds the max, file will not be collected; if the file falls below min, file will not be collected.

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

4.2.6 ES Server Configurations Tab:



1. **ES Server Kill Date:** *ES Server(64).exe* will check this date on initial startup and whenever a thumb drive is inserted.
2. **ES Server Name:** *ES Server(64).exe* will be named this once "Build ES" has been clicked.
3. **Collection Directory on Primary Host Target:** This is the folder to save all collected data in. The default location is right beside *ES Server(64).exe* in a system hidden folder named 0000. The system hidden folder 0000 will always be created in a folder specified e.g. %appdata% will store collected data in %appdata%\0000.
4. **Percent of Primary Host's Hard Drive to Keep Free:** This is to avoid filling up the primary host's hard drive. Percent of drive to keep free.

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

5. **Encryption File:** This is the location of the encryption file on the config system. This file contains the public and private keys necessary for encryption and decryption.
6. **Generate Encryption File:** This is an easy button to create a new pem file. *Warning: Losing this key and the XML config file will cause all data collected to be useless. Old pem files cannot be reproduced. It would be wise to reuse the same pem file for the same ongoing op.*
7. **Global ES_Dll File Collection Configuration for Stored File Hashes:** These global configurations pertain to the *DllPayload(64).dll*.
8. **Generate Unique File Hashes per Whitelisted Drive:** This option specifies whether you want every thumbdrive that executes on target to collect and hash files, or for all of them to use the same hash list. If this box is checked, then every thumbdrive will store its own hash list for files it has collected, thus allowing additional ES drives to collect the same files.

   For example, let's say you configure 5 ES drives to collect all files named Secret.doc. If you check this configuration box, then all 5 ES drives will collect all the Secret.doc files from the target. However, these files are then hashed and subsequent returns to the target will not yield collection of these files again (unless they've changed).

   If you do not check this box, then only the first ES drive will collect all files named Secret.doc. The four other drives and subsequent returns of all five drives to the system will not yield collect of the files again (unless they've changed).
9. **Location of File Hashes on Target:** This is the location of the hash file on the secondary host. The default file location is %appdata %/Microsoft/Internet Explorer/hret.cfg. The hash file will always be named hret.cfg.
10. **Pre Build Batch File:** These fields enable a bat script or executable to run before building an ES Payload.
11. **Post Build Batch File:** These fields enable a bat script or executable to run to clean up the pre build process.

4.3 Deployment to Primary Host

Select "**Build ES**" to create the configuration (*.cfg) and executable (*.exe) files. Try to run the configuration program as Admin because Emotional Simian needs to be at least admin or greater to infect a local thumb drive.

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

32 bit machines use *ES Server.exe*. 64 bit machines use *ES Server64.exe*. Put the appropriate version of *ES Sever(64).exe* on the target Primary Host computer. Both *.cfg files are identical. *ES Sever(64).cfg* has to be the same name as *ES Server(64).exe*.

ES Server(64).exe will load and rename the *.cfg file to *.ini file. A new *.cfg is installed by placing it on the primary host beside *ES Server(64).exe. ES Server(64).exe* does not need to be shut down; just drop the new *.cfg file and wait at most 3 seconds. The old *.ini file will be deleted, and the new *.cfg file will be loaded into *ES Server(64).exe* and renamed to *.ini. The hash list of all infected thumb drives is stored in the *.ini file, so deleting this file will allow *ES Server(64).exe* to infect thumb drives it has already infected.

4.4 Left behind data

4.4.1 Primary Host Data

The following things are left behind or altered by ES Server on the Primary Host:

1. ES_Server.exe -> wherever installed
2. ES_Server.cfg -> wherever installed
3. Collection Folder -> Created after seeing the first thumb drive with collected data, placed where configured (**Collection Directory on Primary Host Target**).

4.4.2 Secondary Host Data

The following files and Reg keys are created by ES Dll Payload on the Secondary Host:

1. Reg Key -> HKCU\Software\Microsoft\Active Setup
    a. Value: Parameters
2. Reg Key If “Persist Completed Reg Key” is checked: HKLM\Software\Microsoft\Active Setup
    a. Value: Some random GUID
3. Reg Key if not persistent: HKLM\Software\Microsoft\MNU
    a. Value: Some random GUID
4. Hash File: Located where configured (**Hash Collection Directory Location on Secondary Target**)
5. Payloads: Wherever they were dropped.

4.5 Retrieval of Collected Files

4.5.1 If a whitelisted drive returns to the Primary Host

1. All data files (Surveys, Directory listings, and/or File collections) will be placed in the folder specified by the **Collection Directory on Primary Host Target** parameter in the configuration program and deleted off the covert storage on the thumb drive.

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06

2. If the **Recharge Number of Runs** check box was selected then all payloads and survey will have their max number of runs reset back to their original amount.
3. If the **Allow Retasking on Previous Targets** check box was selected then a new GUID will be supplied to the *DllPayload(64).dll* allowing that dll to infect secondary hosts previously infected.

Other tools are required to recover collected data from the Primary Host.

4.6 Post Process of Collected Files

Run *Post processor.exe* as Admin with the following arguments:
PostProcessor -d <IN:PEM File> <IN:Folder to decrypt> <OUT:Name of output Folder>

4.7 Additional Software

4.7.1 Keygen.exe:

Keygen.exe produces a Public / Private key pair. The arguments are below:
KenGen.exe <file_to_store_pem.pem>

4.7.2 Extract WM Files.exe

This tool extracts files from the covert storage space on a thumb drive. The arguments are below:
ExtractWMFile.exe <Drive Letter> Optional:<Directory to store files>

If the Directory to store files is not filled out, then the files will be stored in a folder named 1111 right next to the Extract WM Files.exe.

4.7.3 Get SN.exe

This tool finds the serial number of a thumb drive, either on the target or back at station. The arguments are below:
GetSN.exe <Drive Letter>

4.7.4 Whack_Thumbdrive.exe

This tool is used by the GUI to infect a local thumb drive plugged into the computer.
Whack_Thumbdrive.exe <Config.xml> <Drive letter>

SECRET//X1

CL BY: 2397517
REASON: 1.4(c)
DECL: 20361019
DRV: COL S-06