Foundstone *Riffle* Forensic Tool
Quick Start Guide

I. Introduction

Foundstone's *Riffle* is an efficient and versatile forensic artifact collection tool designed to identify Windows hosts that have been compromised by malware or cyber attacks. It is a Win32 command application that runs on Windows XP and all Windows O/S' released since including 64-bit systems. *Riffle* is controlled by a standard INI file, riffle.ini. The application will not run without an INI file. (Be sure to read the *Riffle – FAQ* document for more information.)

II. Configuration

Riffle is a stand-alone application that is designed to run once on a Windows workstation. It has no other dependencies other than the required INI file. *Riffle* does not require an installer or a server. It is not an agent. When executed, Riffle collects a series of forensic artifacts from a host, archives them into a 7zip file, and delivers the archive file to an FTP site, SMB share, or email address.

Riffle will perform the below operations, depending on the settings in the INI file:

Riffle Artifact Collection Capabilities
• Extracts a live $MFT using sector-level disk reads.
• Extract the Registry hives (SYSTEM, SECURITY, APPLICATION, and SAM)
• Extracts the contents of the Windows Prefetch folder on workstations.
• Extracts NTUser.dat files of all user profiles.
• Extract Windows event logs.
• Extracts the Hosts file.
• Executes *a*t and *schtasks* and saves output to determine scheduled tasks.
• Executes *netstat –ano* and saves output to determine network connections.
• Executes *tasklist -fo csv -v* to determine running processes with PID's.
• Executes *tasklist -fo csv /svc* to determine what services are running under a task.
• Executes *ipconfig /displaydns* and saves output to determine DNS activity.
• Executes *ipconfig* and saves output to determine network configuration.
• Extracts McAfee A/V log files including On-Access and Access Protection logs.
• Extracts contents of McAfee A/V Quarantine folder.
• Extracts Internet history from Internet Explorer and Mozilla FireFox.

In addition, *Riffle* carries within its own payload, useful tools to do additional artifact collection.

Riffle Third-Party Tools
• SysInternals® *PSLogList* is used to extract live event logs including the conversion of the logs to a csv file containing textual context of the events obtained from the host.*
• SysInternals® *Autorunsc* console tool is used to identify start-up applications, services and drivers. This versatile tool also hashes all of the startup binaries it detects.*
• *md5deep* is used to hash files on the %SYSTEMDRIVE%. This proven workhorse is a very efficient and powerful hashing tool. If hashing is enabled in the INI file, by default, *Riffle* will hash all files in the user profile folder (Documents and Settings, or Users) and the entire Window folder. You can also hash all the files on the system volume if desired.

* Client must agree to abide by Microsoft's end-user license agreement (EULA).

You can tell Riffle how much, or how little, data you would like to collect off a host by enabling or disabling features in the INI file (riffle.ini). The INI file is a standard settings file you have probably seen many times before. The sample INI file provided is well documented.

There are 11 sections in the INI file. They are shown in the below table.

Riffle INI Sections
[APPLICATION] Section
[FILESYSTEM] Section
[REG] Section
[LOGS] Section
[NETWORK] Section
[HASHES]] Section
[PROCESSES] Section
[AUTORUNS] Section
[SCHEDULER] Section
[INTERNET] Section
[SMBSHARE] Section
[SMTP] Section

Each section has entries that enable/disable artifact collection functions or provide configuration information.

[APPLICATION] SECTION

The application section contains configuration information relative to the *Riffle* application.

Value	Setting	Notes
working_dir	Configurable	"\\temp\\riffle” is Default. (Must have two \’s)
archive_dir	Configurable	“\\ is Default (Root) (Must have two \’s)
Stdout	1 = Enabled 0=Disabled	Enables output to stdout. Default = Disabled
Debug	1 = Enabled 0=Disabled	Enables debug logging. Default = Disabled
encrypt_archive	1 = Enabled 0=Disabled	Encrypt archive file. Default = Disabled
delete_folders	1 = Enabled 0=Disabled	Delete working folders. Default = Enabled
delete_archive	1 = Enabled 0=Disabled	Delete archive after delivery. Default = Disabled

[FILESYSTEM] SECTION

The filesystem section contains configuration information relative to filesystem artifacts.

Value	Setting	Notes
$MFT	1 = Enabled 0=Disabled	Collect $MFT ff %SYSVOL%. Default = Enabled
Prefetch	1 = Enabled 0=Disabled	Collect Prefetch folder. Default = Enabled
Ntuser	1 = Enabled 0=Disabled	Collect all NTUser.dat files. Default = Disabled

[REG] SECTION

The reg section contains configuration information relative to Registry hives.

Value	Setting	Notes
Enabled	1 = Enabled 0=Disabled	Collect REG Hives. Default = Enabled

[LOGS] SECTION

The logs section contains configuration information relative to log file artifacts.

Value	Setting	Notes
evt_logs	1 = Enabled 0=Disabled	Collect Event logs. Default = Enabled
evt-logs_txt	1 = Enabled 0=Disabled	Convert event logs to text. Default = Disabled
av_logs	1 = Enabled 0=Disabled	Collect McAfee A/V logs. Default = Enabled
Quarantine	1 = Enabled 0=Disabled	Collect McAfee Quarantine folder. Default=Disabled

[NETWORK] SECTION

The network section contains configuration information relative to networking artifacts.

Value	Setting	Notes
Netstat	1 = Enabled 0=Disabled	Collect netstat info. Default = Enabled
Dnscache	1 = Enabled 0=Disabled	Collect DNSCache info. Default = Enabled
Hosts	1 = Enabled 0=Disabled	Collect hosts file. Default = Enabled
Ipconfig	1 = Enabled 0=Disabled	Collect ipconfig info. Default = Enabled

[HASHES] SECTION

The hashes section contains configuration information relative to hashing the filesystem.

Value	Setting	Notes
Hashfiles	1 = Enabled 0=Disabled	Enable hashing. Default = Disabled
hash_all	1 = Enabled 0=Disabled	Hash entire %SYSVOL%. Default = Disabled

Note: If hashing is enabled and hash_all is disabled, only the user profile folder (Document and Settings or Users) and the entire Windows folder will be hashed. If both settings are enabled, the entire system volume will be hashed. It takes time to hash, so be sure the client understands the implication of this task.

[PROCESSES] SECTION

The processes section contains configuration information relative to process artifacts.

Value	Setting	Notes
tasklist	1 = Enabled 0=Disabled	Enable tasklist collection. Default = Enabled

[AUTORUNS] SECTION

The autoruns section contains configuration information relative to running Autorunsc.

Value	Setting	Notes
enabled	1 = Enabled 0=Disabled	Enable Autorunsc collection. Default = Enabled

[SCHEDULER] SECTION

The scheduler section contains configuration information relative to scheduled task artifacts.

Value	Setting	Notes
at	1 = Enabled 0=Disabled	Collect *at* output. Default = Enabled
schtasks	1 = Enabled 0=Disabled	Collect *schtasks* output. Default = Enabled

[INTERNET] SECTION

The Internet section contains configuration information relative to browser history.

Value	Setting	Notes
iehistory	1 = Enabled 0=Disabled	Collect IE browser history. Default = Enabled
foxhistory	1 = Enabled 0=Disabled	Collect FireFox browser history. Default = Enabled

[FTP] SECTION

The ftp section contains configuration information for FTP delivery of the artifact file.

Value	Setting	Notes
Enabled	1 = Enabled 0=Disabled	Enables FTP. Default = Disabled
Ftpserver	Configurable	URL or IP address of FTP server.
Ftpdir	Configurable	chdir command to execute at login
Ftpuser	Configurable	FTP user name
Ftppwd	Configurable	FTP user password

Note: Currently, Riffle only supports standard FTP. It is suggested that you enable encryption of the *Riffle* archive file if you are going to use FTP as a delivery method.

[SMBSHARE] SECTION

The smbshare section contains configuration information for SMB share delivery of the artifact file.

Value	Setting	Notes
enabled=0	1 = Enabled 0=Disabled	Enables SMBShare delivery. Default = Disabled
smbshare=""	Configurable	URL or IP address of SMB share.
smbuser=""	Configurable	SMB share user name
smbpwd=""	Configurable	SMB share user password

Note: *Riffle* uses the standard *net share* command to map the SMB share. The *smbshare* value must be properly escaped. An example of a valid *smbshare* values are listed below:

smbshare="\\\\Servername\\somefolder"
smbshare="\\\\10.10.4.210\\somefolder"

The *smbuser* value must also be properly escaped as shown below:

smbuser="Somedomain\\someusername"

[SMTP] SECTION

The smtp section contains configuration information for SMTP delivery of logs and/or artifact file.

Value	Setting	Notes
enabled	1 = Enabled 0=Disabled	Enables SMTP delivery. Default = Disabled
smtp_logonly	1 = Enabled 0=Disabled	Determines if only the log file is sent via E-Mail.
smtp_server	Configurable	SMTP server name or IP address.
smtp_port	Configurable	SMTP port.
smtp_user	1 = Enabled 0=Disabled	SMTP login user name.
smtp_pwd	Configurable	SMTP user password.
smtp_from	Configurable	SMTP from address. Default = riffle@foundstone.com
smtp_to	Configurable	Send To: E-Mail address

Note: *Riffle* will E-Mail an artifact file if it is 5MB in size or less. If you are going to send artifact files via E-Mail it is highly encouraged you enable encryption of the archive file.

III. Implementation

Implementation of *Riffle* is simple. You will need a mechanism to deploy *Riffle.exe* and *Riffle.ini* to a host and execute Riffle with local administrator or system privileges. Most users place the two files on the root folder of the system volume and run it from there.

Depending on the client, you have several deployment mechanisms available to you. The most common method is leveraging a deployment tool that is already in place. This includes Microsoft's SMS, Altiris, BigFix, and other enterprise support tools. The two *Riffle* files can be deployed as a package. It is suggested that you thoroughly test the settings in the INI file prior to deployment.

A second method for deployment is to have the client create a login script via a group policy in Active Directory. This is also a very effective method of deployment. The only drawback is that you have to wait until the user logs in to start the artifact collection.

Finally, there are manual deployment methods you can use. SysInternal's PsExec and a free tool named xCmd.exe can be scripted to do the deployment. We are working on creating an ePO package to do the deployment. This should prove very popular with the one caveat that ePO can only deploy the tool to hosts it has under management.

Once Riffle is deployed and you have collected the artifact files, you can move on to the second phase of malware/APT detection. This involves the extracting of the collected artifacts and loading them into a Foundstone malware correlation database. Refer to the associated methodology documentation for more information.