(U) Engineering Development Group

(U) Rain Maker 1.0
User's Guide

Rev. A
9 March 2015

Classified By: 2392146
Derived From: COL S-06
Reason: 1.4 (c)
Declassify on: 20350629

(U) Change Log

[Unclassified]

Doc Rev	Doc Date	Rev By	Change Description	REFERENCE	AUTHORITY / Approval Date
New	03/09/15	XX	New		

(U) Table of Contents

1. (U) Scope

(U) This document establishes the User Guide for Rain Maker v1.0.

1.1 (U) System Overview and Description

(S) Rain Maker v1.0 is a collection tool intended to be run from removable media. Version 1.0 specifically is designed for use with portable VLC Player (2.1.5). To trigger collection, the user must open up VLC player on the target machine from the removable media. The removable media can appear as either a fixed or removable drive but must be formatted NTFS. Upon opening VLC player, Rain Maker collects a standard survey of the machine (RoadRunner Survey) and a prioritized file collection. A survey will only be taken on any machine if the last survey of the machine is seven days old or older. The collected data is stored back to Alternate Data Streams off of the root of the volume. For example, if the removable media appears as volume E:\, the data is stored in E:\:$DataIdN. Configuration options allow the user to specify a prioritized list of directories from which to collect files (environment variables can be used), a list of extensions to collect, the percentage of drive space to be left free, and the drive to configure/tie the tool to. Upon configuring a piece of removable media, a public/private key pair is generated (the private key in generated in Implant\Deploy as well as in PostProcessor). **The private key must/must be kept in order to decrypt the returned data.** Also, upon configuring a drive, a "stub" is generated that ties the tool to the drive. The stub, once loaded, decrypts Rain Maker and executes it. This means that if the drive is reformatted or if the portable player is moved to another drive, the actual collection tool will not be decrypted and as a result Rain Maker will not run.

(U) Assumptions and Constraints

(S) We assume that the target places files of interest into the directories we are collecting from. We also assume that the files in the collection directories have the appropriate extensions. It is required that the VLC player be run from the configured removable media. It must run long enough to complete collection. The removable media must be NTFS. VLC player should be exited before unplugging the removable media (a VLC issue).

2. (U) Applicable Documents

(S) The following documents pertain to this tool. In the event of a conflict between the documents referenced below, the contents of this document will be considered binding.

- Rain Maker v1.0 User Guide.doc (S//NF)
- Rain Maker v1.0 TDR Slides.ppt (S//NF)
- User Guide.txt (U)

3. (U) System Description

3.1 (U) System Concepts and Capabilities

- (S) Rain Maker v1.0 does not maintain a presence on the target machine
- (S) Rain Maker v1.0 relies of VLC player for execution
- (S) Rain Maker v1.0 follows the NOD Persistence Specification
- (S) The Rain Maker stub is a DLL hijack of psapi.dll. The external manifest of VLC player is modified to force a Side-by-Side loading of psapi.dll (forcing a DLL hijack where there wasn't one). The stub DLL then uses the volume serial number of the drive it is running from to create an AES key. The key is then used to decrypt Rain Maker v1.0. Once decrypted, Rain Maker v1.0 is memory loaded.
- (S) Upon startup, Rain Maker Stub sets a global mutex allowing only one instance to run at one time.
- (S) Rain Maker will conduct a survey of the machine it is running on if a survey has not been conducted or if the last survey is 7 days old or older.
- (S) A survey hash list is kept to keep track of last survey timestamps for machines that have been surveyed.
- (S) Rain Maker conducts a prioritized file collection (configurable).
- (S) Rain Maker collects files by matching patterns (configurable).
- (S) There is a hard-coded maximum file size of a 100MBs for file collection. This means no files over 100MBs will be collected.
- (S) A file collection hash file is kept. A file is collected if the file name, file size or file modified time differs from all previously collected files.
- (S) Rain Maker v1.0 stores collection in Alternate Data Streams off of the root of the volume it is executing from.

3.2 (U) Prerequisites

- (S) The target system must be running Windows XP, Vista, 7, 8, or 8.1.
- (S) The user of the target computer must execute VLC player from the configured drive.

4. (U) Operation

4.1 (U) Installation and Setup

4.1.1 (S) *Configuration – Rain Maker Configurator*

a. Folder Structure

i. Before trying to configure Rain Maker, first confirm that the Implant folder contains the four required files: RainMaker.dll, RainMakerStub.dll, RainMakerConfigurator.exe, vlc.exe.manifest. You will need to open a command prompt and navigate to this

directory to configure Rain Maker using the RainMakerConfigurator.exe.

b. Deploy Directory
    i. Upon executing the configurator a Deploy folder is generated (as a sub-folder of Implant). Depending upon the options you choose during configuration, up to 5 files will be placed in the Deploy folder. These 5 files include RainMaker_Configured.dll (the configured version generated for this deployment), RainMaker_Configured.dll.enc (the encrypted container containing RainMaker_Configured.dll), RainMakerStub_Configured.dll (the configured stub for this deployment), RainMaker_PubKey.pem and RainMaker_PrivKey.pem (the public and private key generated for this deployment).
c. Target Collection Directories (-t)
    i. A semi-colon delimited list of directories to collect files from. The collection is prioritized in the order they are provided. Environment variables may be supplied as an argument but you must escape all percent signs using a preceding carat (Ex: ^%USERPROFILE^%\Desktop;^%USERPROFILE^%; - In this example files are collected from the Desktop folder and sub-folder before the user's directory). The configuration tool should print out your supplied target collection directories, if environment variables become expanded it means the percent signs were not escaped.
d. Extension/Pattern List (-e)
    i. The extensions and or filename patterns to collect from the target directories. The file extensions are also a semi-colon delimited list. Example: *.doc;*.xls;*.ppt;
e. Disk Free Space (-f)
    i. Percentage of the drive to leave free (0 – 100). If not supplied, the default is 25%. In the default case, this means that if the drive Rain Maker is executing from becomes over 75% full, Rain Maker no longer stores collect.
f. Path To VLC (-vlc)
    i. To infect VLC player for a specific piece of removable media, the configurator needs the path to the VLC executable (vlc.exe) that resides on the removable media. Example: E:\vlc\vlc.exe
g. Relative Path To Encrypted Rain Maker (-r)
    i. This is the relative path from the directory containing vlc.exe where the encrypted container for Rain Maker will reside. Note that these directories are not created by the configurator. Example: plugins\access\customplugins.dat
h. Argument Requirements
    i. When configuring Rain Maker v1.0 you may supply all 5 arguments to generate the configured payloads and infect the media (Recommended). If mistakes are made during configuration,

reinfection (running the configuration tool again) will securely delete prior configurations from the target media and replace them with the new configured payloads. However, if you have executed Rain Maker v1.0, you should reformat the drive before running the configuration tool again. The configuration tool also allows you to run the configuration in stages (more for future use – not recommended). For example, supplying only the target collection list, extension/pattern list, and the relative path to the encrypted container will generate all of the configured payloads without infecting the media. Supplying the path to the VLC player and the relative path to the encrypted container will infect the media with the previously generated payloads. ***NOTE: Always save the private key for your deployment – needed for decryption of data. The private key is stored in both the Deploy and PostProcessor folders.***

5. (U) Post Processing

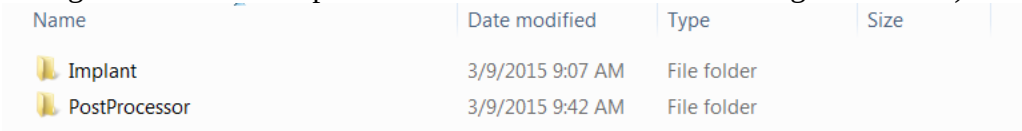
5.1 (U) Post Processor Arguments

- (S) The post processor for Rain Maker v1.0 is a high-side (classified) utility.
- (S) –p: the path to the drive containing collection. Example: -p E:\
- (S) –k: the path to the private key for the deployment (required for decryption). Example: -k RainMaker_PrivKey.pem
- (S) –o (optional): Path to where output files should be placed. If not supplied, results are placed on the user's Desktop in a folder named RainMaker.
- (S) Results are organized by collection date. If a survey was conducted it will appear in the root of the collection date folder. The file collection directory structure is reconstructed.

6. (U) Configuration Example

6.1 (U) Tool Configuration

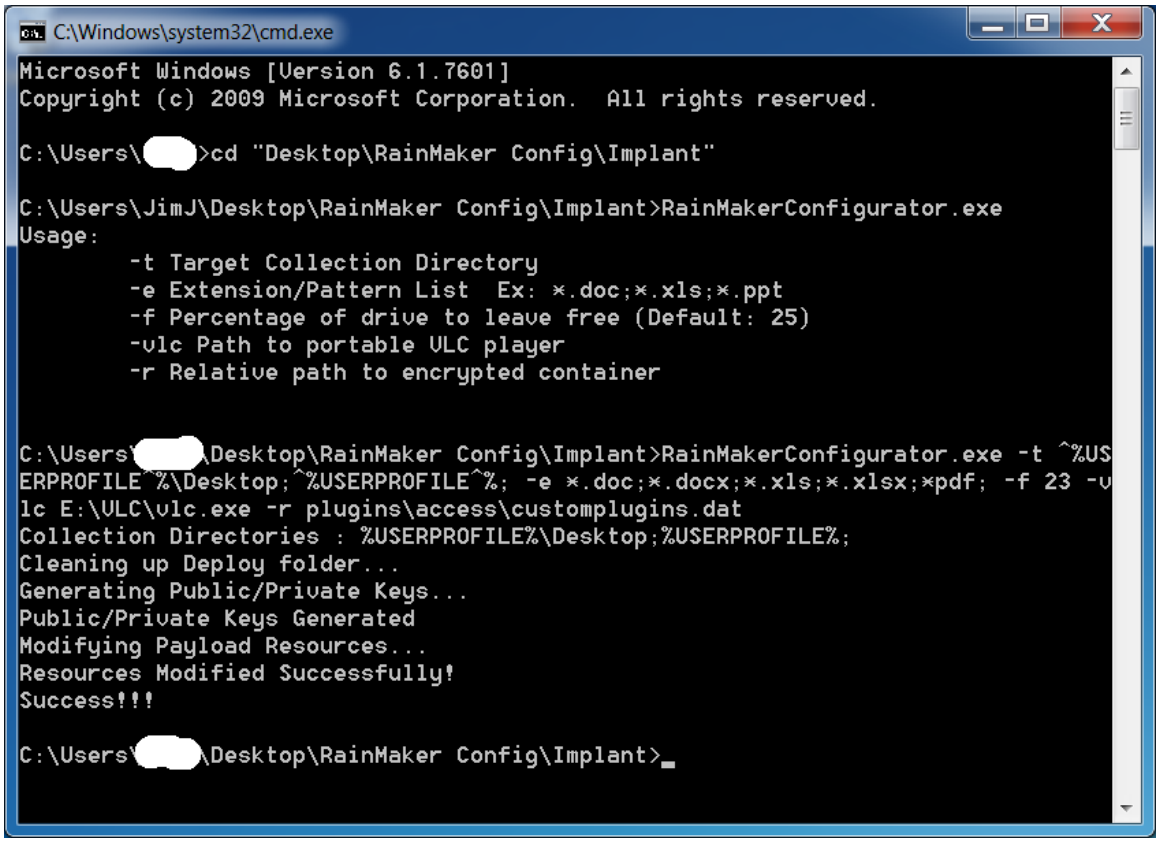
- (S) Folder structure before executing configuration (all files generated by the configuration tool are replaced on each execution of the configuration tool):



Name	Date modified	Type	Size
RainMaker.dll	3/9/2015 9:02 AM	Application extens...	124 KB
RainMakerConfigurator.exe	3/6/2015 1:29 PM	Application	68 KB
RainMakerStub.dll	3/9/2015 9:02 AM	Application extens...	66 KB
vlc.exe.manifest	2/27/2015 7:56 AM	MANIFEST File	1 KB

Name	Date modified	Type	Size
RainMakerPostProcessor.exe	3/6/2015 1:29 PM	Application	69 KB

- (S) Collect files from %USERPROFILE%\Desktop first and then collect from %USERPROFILE%.
- (S) Collect Word Documents, Excel Documents and PDFs.
- (S) Have a minimum of 23% free space on the drive
- (S) Path to the VLC player is E:\VLC\vlc.exe
- (S) Relative path to the encrypted container is plugins\access\customplugins.dat



- (S) Folder structures after configuration:

Name	Date modified	Type	Size
RainMaker_Configured.dll	3/9/2015 9:59 AM	Application extens...	125 KB
RainMaker_Configured.dll.enc	3/9/2015 9:59 AM	ENC File	73 KB
RainMaker_PrivKey.pem	3/9/2015 9:59 AM	PEM File	4 KB
RainMaker_PubKey.pem	3/9/2015 9:59 AM	PEM File	1 KB
RainMakerStub_Configured.dll	3/9/2015 9:59 AM	Application extens...	67 KB

Name	Date modified	Type	Size
RainMaker_PrivKey.pem	3/9/2015 9:59 AM	PEM File	4 KB
RainMakerPostProcessor.exe	3/6/2015 1:29 PM	Application	69 KB

Changed Files:

Name	Date modified	Type	Size
locale	3/6/2015 3:58 PM	File folder	
lua	3/6/2015 3:58 PM	File folder	
plugins	3/9/2015 9:04 AM	File folder	
skins	3/6/2015 3:58 PM	File folder	
AUTHORS.txt	7/23/2014 2:28 AM	Text Document	16 KB
axvlc.dll	7/23/2014 2:29 AM	Application extens...	519 KB
axvlc.dll.manifest	7/23/2014 2:29 AM	MANIFEST File	1 KB
COPYING.txt	7/23/2014 2:28 AM	Text Document	18 KB
libvlc.dll	7/23/2014 2:29 AM	Application extens...	111 KB
libvlc.dll.manifest	7/23/2014 2:28 AM	MANIFEST File	1 KB
libvlccore.dll	7/23/2014 2:30 AM	Application extens...	2,341 KB
NEWS.txt	7/23/2014 2:28 AM	Text Document	143 KB
npvlc.dll	7/23/2014 2:29 AM	Application extens...	369 KB
npvlc.dll.manifest	7/23/2014 2:29 AM	MANIFEST File	1 KB
psapi.dll	7/23/2014 2:28 AM	Application extens...	67 KB
README.txt	7/23/2014 2:28 AM	Text Document	3 KB
THANKS.txt	7/23/2014 2:28 AM	Text Document	6 KB
vlc.exe	7/23/2014 2:29 AM	Application	125 KB
vlc.exe.manifest	7/23/2014 2:28 AM	MANIFEST File	1 KB
vlc.ico	7/23/2014 2:28 AM	Icon	72 KB
vlc-cache-gen.exe	7/23/2014 2:29 AM	Application	113 KB

Name	Date modified	Type	Size
customplugins.dat	7/23/2014 2:28 AM	DAT File	73 KB
libaccess_attachment_plugin.dll	7/23/2014 2:29 AM	Application extens...	14 KB
libaccess_bd_plugin.dll	7/23/2014 2:29 AM	Application extens...	99 KB

6.2 (U)Post Processing

- (S) Supply drive containing collection: E:\
- (S) Supply private key for decryption: RainMaker_PrivKey.pem
- (S) Default output directory