Engineering Development Group

DarkSeaSkies 1.0
Concept of Operations

Rev. New
26 January 2009

CL BY: 2348366
CL REASON: 1.4(c)
DECL ON: 20331105
DRV FROM: COL S-06

Change Log

Doc Rev	Doc Date	Rev By	Change Description	RFC	Authority/ Approval Date
New	11/05/2008	TWC	Initial Release		

Table of Contents

List of Tables

1. Scope

This document describes the user and system Concept of Operations for DarkSeaSkies 1.0.

1.1 System Overview and Description

DarkSeaSkies is an implant that persists in the EFI firmware of an Apple MacBook Air computer, installs a Mac OSX 10.5 kernel-space implant and executes a user-space implant.

DarkSeaSkies consists of three different tools:

1. ***Dark***Matter: An EFI driver that persists in firmware and installs the other two tools.
2. ***Sea***Pea: A Mac OSX kernel-space implant that executes, and provides stealth and privilege to user-space implants.
3. Night***Skies***: A Mac OSX user-space implant that beacons to a listening post and provides command and control.

This document describes the CONOP of DarkMatter, and that of SeaPea and NightSkies only where they differ from their documented CONOPs. Refer to *SeaPea CONOP* for further information on SeaPea CONOP. Refer to *NightSkies CONOPS* for further information on NightSkies CONOP.

1.2 Assumptions and Constraints

It is assumed that the target system is a MacBook Air version 1,1 with firmware version MBA11.0088.B03 running Mac OSX 10.5.2-10.5.x.

It is assumed that an operator or asset has one-time physical access to the target system and can boot the target system to an external flash drive.

A constraint is that the DarkSeaSkies will not persist in the event of a firmware update.

2. Applicable Documents

The following documents, of the exact issue shown, form a part of this CONOPS to the extent specified herein. In the event of a conflict between the documents referenced herein and the contents of this CONOPS, the contents of this CONOPS will be considered superseding. The following documents may be found within S:\DO\IOC\EDG ALL\EDG AE\Projects\:

- SeaPea CONOP, Rev. 2.0, November 2008
- NightSkies CONOPS, Rev. 1.2, November 2008

3. Mission Overview (Not Applicable)

4. User CONOPS

The DarkSeaSkies User CONOPS is primarily the combined CONOPS of SeaPea and NightSkies, with the following additions.

DarkSeaSkies is installed from a bootable flash drive. The target system is booted while holding down the "option" key until the screen displays a boot drive selection menu. Select the flash drive. Once the DarkSeaSkies installer has started the screen will blank and a ':' will appear in the upper left corner of the screen. On a successful installation a ')' will follow the ':'. On an unsuccessful installation a '(' will follow the ':'.

Once installed, DarkSeaSkies will wait for the configured enable date to begin operation. The configured enable date is saved in the file "enable.time".

Once operational, DarkSeaSkies will examine the following NVRAM variables at each boot to determine the action to take for this boot. All variables have configurable names and randomized GUIDs. Each delivery of DarkSeaSkies has different randomized GUIDs for firmware variables and EFI drivers.

- "Status" indicates the status of the payload from the previous boot. The name of the "Status" variable is saved in the file "status.name" and the GUID in the file "status.guid". It has the following values.
  - '\0' indicates an unknown status, for example the first boot after install
  - '0' indicates that the user-space payload has been dropped
  - '1' is reserved for future use
  - '2' is reserved for future use
  - '3' indicates that the user-space payload executed successfully
  - '4' indicates that the user-space payload encountered an error condition
  - '5' indicates that DarkSeaSkies should uninstall itself and its payload
  - Any other value is equivalent to '5'.
- "Count" maintains a counter used to track the number of cautious boots. A cautious boot is defined fully below. If "Count" does not exist then it is assumed to be zero. The name of the "Count" variable is saved in the file "warning_count.name" and the GUID in the file "warning_count.guid".

"Limit" indicates the value of "Count" at which DarkSeaSkies will uninstall itself and its payload. If "Limit" does not exist then a pre-configured value will be used. The name of the "Limit" variable is saved in the file "warning_threshold.name" and the GUID in the file "warning_threshold.guid".

DarkSeaSkies also determines if a kernel panic occurred. If a panic did occur then the NVRAM variables associated with the panic are deleted so that it is not reported to the operating system.

Based on this input DarkSeaSkies updates "Count" as follows.

- If "Status" indicates success {'2', '3'} and there *was not* a kernel panic

- Caution count NVRAM variable “Count” is set to zero.

- If “Status” indicates success {‘2’, ’3’} and there *was* a kernel panic
  - Increment the caution count NVRAM variable “Count” by one. If the variable “Count” does not exist then it is assumed to be zero.
- If “Status” indicates caution {‘\0’, ’0’, ‘4’} and there *was not* a kernel panic
  - Increment the caution count NVRAM variable “Count” by one. If the variable “Count” does not exist then it is assumed to be zero.
- If “Status” indicates caution {‘\0’, ’0’, ‘4’} and there *was* a kernel panic
  - Increment the caution count NVRAM variable “Count” by two.
- If “Status” indicates and error {‘1’, ‘5’}
  - Set the caution count NVRAM variable “Count” to the value of “Limit”.

Next, “Count” is examined. If “Count” is greater than or equal to “Limit” then DarkSeaSkies and its payload are deleted from the firmware. Otherwise DarkSeaSkies will load, link, and hook the SeaPea kernel implant into the RAM image of the Mac OSX 10.5 operating system. DarkSeaSkies will also write the pre-generated NightSkies configuration to the “Config” NVRAM variable if it does not already exist. The name of the “Config” variable is saved in the file “config.name” and the GUID in the file “config.guid”. Once the root file system becomes writable SeaPea will write the NightSkies tool into a temporary file, execute NightSkies, and secure delete the NightSkies tool.

NightSkies then operates as documented in *NightSkies CONOPS* with the addition that NightSkies must set the “Status” NVRAM variable at each boot appropriate to its status. NightSkies may also read and report the “Count” NVRAM variable to the operator, and allow the operator to set the “Limit” NVRAM variable.

5. System CONOPS (Not Applicable)

6. Notes

6.1 Acronyms/Abbreviations

The Acronyms/Abbreviations used in this document are shown in Table 6.1 -1.

Table 6.1-1 Acronyms/Abbreviations

Acronym/Abbreviation	Term
EFI	Extensible Firmware Interface
NVRAM	Non-Volatile Random Access Memory
GUID	Globally Unique IDentifier

6.2 Definitions

Definitions of common terms used within this document may be found in the Engineering Development Group Program Management Lexicon.

The terms and definitions unique to this As-Built Specification are shown in Table 6.2 -2.

Table 6.2-2 Definition

Term	Definition