Engineering Development Group

DarkSeaSkies 1.0
User Requirements Document

Rev. New
26 January 2009

Change Log

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

Table of Contents

1. Scope

The purpose of this User Requirements Document (URD) is to define capabilities that must be met to achieve the users' stated objectives, and to serve as a basis for IV&V testing of DarkSeaSkies 1.0.

1.1 Requirement Overview and Description

COG has a time-sensitive operational need for a porting of the current version of Nightskies to a MacBook Air. Currently this exists for an iPhone (See Requirement 2008-1508). COG has the opportunity to gift a MacBook Air to a target that will be implanted with this tool. The tool will be a beacon/implant that runs in the background of a MacBook Air that provides us with command and control capabilities. The implant will beacon periodically. This beacon must be persistent in the MacBook Air, and must leave a minimal on-disc footprint.

1.2 Current Capability

Nightskies 1.1 exists for the iPhone. Currently NightSkies does not have stealth and persistence capabilities.

1.3 New Capability

Provide persistence (DarkMatter), process, file, and network hiding (SeaPea), and a beacon (NightSkies), integrated onto a MacBook Air with current Mac OSX.

2. Applicable Documents

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

- Nightskies MacBook Air 20081014, November 2008
- DarkSeaSkies CONOP, Rev. 1.0, November 2008
- DarkSeaSkies User Manual, Rev. 1.0, November 2008
- SeaPea URD, Rev. 2.0, November 2008
- NightSkies User Requirements, Rev. 1.2, November 2008

3. Target System Overview

3.1 Operating Environment

The target system is a MacBook Air version 1,1 with firmware version MBA11.0088.B03. The operating system is Mac OSX 10.5.2-10.5.x.

3.2 Operating Constraints

Physical access is required for initial installation of DarkSeaSkies onto the target system. The target system must have at minimum occasional Internet access in order to

communicate with the LP. If DarkSeaSkies is unable to communicate with the LP for a configurable period of time it will delete itself from the system.

4. User Requirements

4.1 Pre-deployment Capability Requirements

Configuration details are required prior to building DarkSeaSkies. Specifically, DarkMatter requires a caution count "Limit" and "Enable Date" as described in *DarkSeaSkies User Manual*. NightSkies has separate configurations which can be found in *NightSkies User Requirements*.

4.2 Deployment Capability Requirements

4.2.1 NightSkies shall support the Macbook Air with OS X 10.5.2 – 10.5.x.

4.2.2 NightSkies shall be compatible with DarkMatter.

4.2.3 DarkMatter shall have the capability to disable itself after a configurable amount of time.

4.2.4 DarkMatter shall have the capability of removing itself and its payload from the EFI.

4.2.5 NightSkies shall be compatible with CP rootkit.

4.2.6 NightSkies shall support the following implant features:

a. Beaconing to a listening post (LP)
b. Command receipt and execution from a LP
c. File transfer to and from the LP
d. Program file execution
e. Delay after browser starts to beacon

4.2.7 The tool shall be packaged manually, according to the parameters provided by COG.

4.3 Post Deployment Capability Requirements

An LP will be required for NightSkies. (REF *NightSkies User Requirements*).

4.4 Security Requirements

None