Proposal for Project C

Wednesday, May 13th, 2009

Version 1.4

Prepared by: Greg Hoglund and Keith S. Cosick

CONFIDENTIAL INFORMATION

HBGary, Inc.

3941 Park Drive, Suite 2030

Eldorado Hills, CA 95762

301-652-8885

Table of Contents

Introduction

HBGary empowers customers to counter emerging cyber-threats and the human and organizational factors behind the threat. HBGary provides this proposal to General Dynamics, for 'Project C' which is described below.

1 Solution Summary

General Dynamics has selected HBGary Inc to provide this proposal for development of a software application targeting the Windows XP Operating System that, when executed, loads and enables a covert kernel-mode implant that will exfiltrate a file from disk (or other remotely called commands) over a connected serial port to a remote device. The enabling kernel mode implant will cater to a command and control element via the serial port. The demonstration will utilize an exploit in Outlook as the delivery mechanism for said software application. The subsequently loaded implant will be stable and will not crash the demonstration system. A usermode component will be included as part of the exploitation package that exercises the kernel mode implant for demonstration purposes. The loaded implant will use the connected serial port to remotely enable functions which can be visible on the collection computer connected on the other end of the serial line. The purpose of the demonstration setup is to verify the functionality for the customer and validate that all work has been completed.

Primary Objectives:

- Development of a kernel-mode implant that is clearly able to exfiltrate an on-disk file, opening of the CD tray, blinking of the keyboard lights, opening and deleting a file, and a memory buffer exfiltration over a connected serial line to a collection station. For demonstration, a null modem cable will be used to connect the collection station
- The use of a standard Outlook Exploit as a delivery mechanism for the implant, with the intention being that any suitable exploit could be used for the same.
- As part of the exploit delivery package, a usermode trojan will assist in the loading of the implant, which will clearly demonstrate the full capability of the implant.
- Test set (which will consist of two computers networked together via a null modem cable using HyperTerminal) that can reliably and repeatedly demonstrate the exploit and subsequent implant capability of the system.

2 Implementation Plan

Primary Contact: Bill Thompson
Phone: 650-966-2000 ex. 3143
Cell:
Email: bill.thompson@gd-ais.com
Address:

Secondary Contact: Name
Phone:
Cell:
Email:
Address:

2.1

Project Implementation Plan

- HBGary will begin development of a kernel-mode implant with the ability to exfiltrate an on-disk file, open the CD tray, blink the keyboard lights, open and delete a file, and execute a memory buffer exfiltration over a modem line to a collection station. The enabling kernel mode implant will cater to a command and control element via the serial port, and the rudimentary ICD/API in order to C2 the kernel implant will be developed by HBGary and documented appropriately for GDAIS use. As there are currently no requirements for stealth operation, this implant will be visible on the system if someone with technical knowledge were to investigate. Stability requirements are that this driver is loaded and unloaded without system crash, or blue screen.
- HBGary will perform additional research and development for Direct COM port access for reliability. Currently, this poses a low risk to the project schedule and cost, but there could be additional effort required to ensure reliable COM port access.
- For the purposes of this development effort, a standard Outlook exploit will be utilized as a delivery mechanism for the driver. There are multiple exploits, which would enable functionality; however, HBGary has chosen this as a suitable option based on availability, and to reduce research time resulting in accelerated delivery time to the client.
- As part of the exploit delivery package, a usermode trojan will be developed that will extract driver sys file as a resource, and subsequently load that file. The usermode trojan will only assist in the loading of the implant,
- For functional validation to General Dynamics, a test set (which will consist of two computers networked together via a null modem cable) will be utilized for HBGary to demonstrate successful execution of the trojan, and driver. A successful demonstration will show the use of HyperTerminal actively open (but not in immediate use by the operator) on both laptops while the kernel mode implant is successfully operating. It is understood that character traffic will be present on the laptop not infected with the kernel implant if an exfil command is issued.
  - During this demo, the following functions will be displayed
    a. File exfiltration (given file path)
    b. Open CD tray
    c. Blink keyboard LEDs
    d. Delete a file (given file path)
    e. Open a file (given file path)
    f. Memory buffer exfil (given start memory location and block size)

Functional Diagram of test scenario

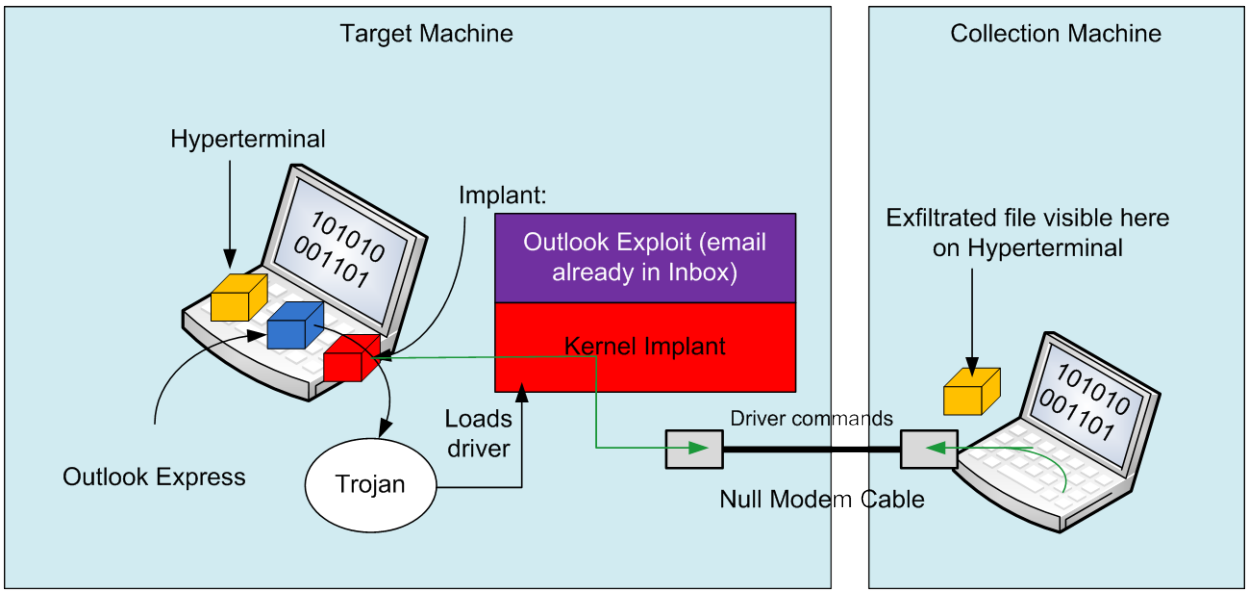

Figure 1 - diagram of the demonstration

Demonstration Steps:

- Exploit is launched from Inbox of Outlook on target computer
- Exploit introduces a simple user-mode Trojan
- The Trojan is a simple user-mode app that installs the Implant
- The Implant is a kernel driver which receives commands via the serial port
- The kernel driver exfiltrates a file (arbitrary) and demonstrates control.

  Additional functions that can be remotely enabled include
  g. Open CD tray
  h. Blink keyboard LEDs
  i. Delete a file (given file path)
  j. Open a file (given file path)
  k. Memory buffer exfil (given start memory location and block size)
- The collection laptop, connected via a null modem cable, clearly illustrates the data being collected over the serial connection (using HyperTerminal)

2.2 Analysis Documentation

- As part of the development of the project, HBGary will provide an architecture diagram explaining the process paths, including any architectural dependencies for the finalized solution including all technical specifications.

- In the event that HBGary identifies through its development, an issue which presents a failure point, HBGary would initiate a conference call with the client to readdress architecture issue, and initiate any needed alternative planning.

- HBGary will provide the client a project schedule with dependencies and milestones listed.

2.3 Hardware Requirements

- N/A

2.4 Project Management

HBGary will provide project coordination services during the course of the project, including the following:

- Development & management of a project plan and schedule for completion of the implementation
  - Development of the Project Implementation Plan
  - Development of the Project Implementation Timeline
  - Development of the Project Milestone Checklist
  - Development of the Professional Services Summary
  - Revisions (if needed) to the Bill of Materials
  - Facilitation of the Application Design Schematic
  - Development & communication of the Testing Plan
  - Development & communication of the Training/hand-off Plan
- Identification and management client communication requirements
  - Internal status on tasks, risks, schedule impacts
  - Weekly client updates, including preparation of material & agenda, and closure minutes
  - Follow-up on action items, and resolve client & project issues
- Management of Performance to schedule
  - Ongoing management of project delivery milestones with both client and HBGary resources to ensure all facets of the project scope is complete
  - Scope changes communicated and processed with appropriate change orders

3 Client Responsibilities

General Dynamics is responsible for the following:

- Client will designate a primary contact for all project status updates, issues, and change order requests. All change order requests must be made through this contact to be considered official and valid.
- Client will coordinate with HBGary to verify the development schedule.
- Client will provide workspace and network (both internal private and public switched telephone network) connectivity for HBGary as needed to complete any onsite work for the client.
- Client will make available an employee when needed to assist HBGary and provide physical and/or remote access to Client facilities.
- Client will coordinate installation schedules with HBGary.
- If HBGary' staff is delayed in the performance of their work by client's failure to provide any of these items, the delay time will be billable at the same rate as the work scheduled to be performed.

4 Bill of Services

HARDWARE: N/A

PROFESSIONAL SERVICES ESTIMATE

Note: Rates are based on previously negotiated figures

Billing Rates, Travel Expenses

Contract Bill Rates and Travel Expenses:

The following are the Hourly Bill Rates for HBGary personnel and/or subcontractors:

HBGary Job Classification	Standard Hourly Bill Rate	Emergency OR Overtime Hourly Bill Rate	Emergency AND Overtime, or HBGary Holiday Hourly Bill Rate
HBG Security Engineer	$294.44	N/A	N/A
Subcontract Specialist	$304.00	N/A	N/A
Project Manager	$244.47	N/A	N/A

- Travel Expenses will be billed at actual cost to General Dynamics. Time in Transit will be billed at $150.00 per round trip within a 50 mile radius of HBGary facility or $150/hr for each engineer outside the 50 mile radius.