Grasshopper Module Guide - Crab v1.0

June 2012

CL BY: 2355679
CL REASON: Section 1.5(c),(e)
DECL ON: 20370522
DRV FRM: COL 6-03

1 Overview

Crab is a persistence module that uses a Windows Service Executable to persist a payload. When a payload is chosen to use this module, Crab will install a stub Windows service and deploy the payload to the target.

Crab supports 32- and 64-bit EXE, DLL, and GH1 payloads. The bitness of the stub and DLL, GH1 payloads must match the target OS. A 32-bit EXE payload may be installed on a 64-bit target, but not vice versa.

2 Installation

Crab uses direct registry modification to register a Crab stub executable as a Windows Service using the user-provided configuration. If the module fails to install the payload, it will delete any deployed components and remove the registry modifications.

2.1 Configuration

The following fields are configured at build time to specify Crab's installation behavior.

Field	Default	Description
Service Name	*None*	Overt key value for service stored in registry
Service EXE Path	*None*	Path to stub EXE on target installed as a service If the path does not exist, it is created.
Payload Path	*None*	Path to payload EXE or DLL on target If the path does not exist, it is created.
Display Name	*None*	Overt name of service displayed by Windows Services MMC
Description	*None*	Overt description of service displayed by Windows Services MMC

3 Payload Execution

Whenever the system starts, the Windows OS will run the Crab service executable stub with SYSTEM privileges. The behavior of the Crab stub depends on the payload type. Crab supports three kinds of payload: EXE, DLL, GH1.

3.1 EXE and DLL

If the payload is an EXE or DLL, the stub is configured with the path to the payload and the name of the service that identifies it. Upon execution by Windows services, the stub will run the payload.

If the payload is an EXE, the Crab stub will execute it with SYSTEM privileges and terminate. If the payload is a DLL, the stub will call `LoadLibrary()` and begin monitoring the payload.

If the stub is unable to locate or start the payload or if the payload disappears, it will uninstall. During uninstallation, Crab will delete the payload, remove the service, and self delete the stub.

The EXE or DLL payload is responsible for deleting itself from the target to trigger uninstallation.

3.2 GH1

If the payload implements the GH1 interface, Crab embeds the payload as a resource in the stub and configures the stub with the name of the service that identifies it. Upon execution, the stub will load the payload DLL in memory.

The stub will uninstall itself on demand or failure to start the payload. During uninstallation, Crab will remove the service and self delete the stub and payload.

4 Footprint

Crab writes unobfuscated binaries to the target filesystem. The service executable stub is written to the filesystem at a user-specified path. If the payload is an EXE or DLL, it is written to the filesystem at a user-specified path. If the payload implements GH1, the payload is embedded as a resource in the Crab stub.

The processes of the service executable stub and payload EXE are visible in the Task Manager during execution.

Crab will create a service visible in the Services view of the Microsoft Management Console with the user-specified display name and description.

A registry key will be placed in `HKLM\SYSTEM\CurrentControlSet\services\<ServiceName>` holding the description and the path to the service stub.

5 Receipt XML Format

Crab's configuration is recorded in the Grasshopper receipt at build time under `build.xml`. An example and description of the xml format is provided below.

5.1 XML Example

```
<PersistModule>
   <UUID>9d03da02ab3a47d7bd28c9a776ba9806</UUID>
   <ServiceExe>
      <ServiceName>Cover Name</ServiceName>
      <ServiceExePath>C:\Target\stub.exe</ServiceExePath>
      <PayloadPath>C:\Target\payload.dll</PayloadPath>
      <DisplayName>Cover Name</DisplayName>
      <Description>This is a description.</Description>
   </ServiceExe>
</PersistModule>
```

5.2 Field Definitions

UUID

The universally unique identifier for the module variant used in the build.

ServiceExe

The service executable configuration information used by the Crab module.

ServiceName

The overt name of the service created by the module. The service name is used as the key in the registry.

ServiceExePath

The path to the Crab service executable stub started by Windows as a service.

PayloadPath

The path to the payload on the target run by the Crab stub.

DisplayName

The overt name of the Windows service created by the module.

Description

The overt description of the Windows service created by the module.

Appendix A:

Appendix B: Change Log

Date	Change Description	Authority
05/2012	Document Initialization	2355679
09/2012	Update for Grasshopper v1.0 Phase 2 Delivery	2355679
11/2012	Update for Grasshopper v1.0.1 Delivery	2355679