Grasshopper Module Guide - Wheat v1.0

June 2012

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

1 Overview

Wheat is a persistence module that deploys and installs a Windows Driver payload. When a payload is chosen that uses this module, Wheat will drop the payload to disk, install it, and exit immediately.

This module is meant to be used with existing drivers, and simply installs them. It does not start them or interact with them.

The Wheat Module supports installing 32- and 64-bit drivers.

2 Installation

Wheat uses direct registry modification to register a payload as a Windows driver 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 Wheat's installation behavior.

Field	Default	Description
Driver Name	*None*	Overt name of the Driver registry key.

2.2 Driver Options

The following installation options are used when installing the driver.

Field	Value	Description
Type	0x01	Specifies the type of the service as 'Driver'
Start	0x02	Specifies the start time of the service as 'Auto Load' during system startup
Error Control	0x03	Specifies the service as a Critical process

3 Payload Execution

Whenever the system starts, the Windows OS will run the payload as a Windows driver. Wheat has no more interaction with the payload/system after installation.

The payload is responsible for deleting itself from the target.

4 Footprint

Wheat writes the unobfuscated payload binary to the target filesystem at `%SYSTEMROOT%\System32\drivers\<DriverName>.sys`.

A registry key will be placed in `HKLM\System\CurrentControlSet\services\<DriverName>`.

5 Receipt

Wheat'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>
   <DriverInstall>
      <DriverName>Cover Name</DriverName>
   </DriverInstall>
</PersistModule>
```

5.2 Field Definitions

UUID

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

DriverInstall

The driver configuration information used by the Wheat module.

DriverName

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

Appendix A: 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