Der Starke 1.4 Companion User Guide

DESCRIPTION

Der Starke is a diskless, EFI-persistent version of Triton. Once active on a target system, the implant executed within diskarbitrationd and typically performs network communications through a browser process so that PSPs like Little Snitch cannot easily detect it’s presence. This Companion User Guide is meant to supplement the Triton User Guide.

SYSTEM REQUIREMENTS

- Supported Build/Postprocessing Systems
    - ♦ Mac OS X 10.7+
    - ♦ Linux with openssl and fdisk
- Supported Target Systems: Mac OS X 10.8 or 10.9; MacBook Air or MacBook Pro from 2012-Present
- Tested Hardware:
    - ♦ MacBook Air 6,1 (Mid 2013 - 11")
    - ♦ MacBook Air 5,2 (Mid 2012 - 13")
    - ♦ MacBook Air 4,1 (Mid 2011 - 11")
    - ♦ MacBook Air 4,2 (Mid 2011 - 13")
    - ♦ MacBook Pro 11,2 (Late 2013 - 15" Retina)
    - ♦ MacBook Pro 10,1 (Mid 2012 - 15" Retina)
    - ♦ MacBook Pro 10,2 (Mid 2012 - 13" Retina)
    - ♦ MacBook Pro 9,1 (Mid 2012 - 15")
    - ♦ MacBook Pro 8,1 (Late 2011 - 13")
    - ♦ MacBook Pro 8,2 (Late 2011 - 15")
    - ♦ MacBook Pro 6,2 (Mid 2010 - 15")

BUILD INSTRUCTIONS

- Run tar -zxf DerStarkeBuilder.tar.gz
- Edit config.plist
- Run derstarke_builder.pyz -c config.plist
- After building, a directory called DerStarkeDeployment_XXXX will be created; The following notable files will be present:
    - ♦ dmconfig..........................configuration information
    - ♦ TRITON-XXXX/......................Triton-related build files
    - ♦ triton.pz.........................The build/tasking binary for the implant
    - ♦ originalConfig.plist..............The build config
    - ♦ mkusb.sh..........................Script to create a USB drive with the disk image from this build
    - ♦ InstallImageFortargetID.iso........Disk image containing implant installer
- Refer to the Triton 1.3 User Guide on how to task the implant. Note derstarke_builder.pyz automatically executed "triton.pz created". User can skip straight to tasking.

INSTALLATION INSTRUCTIONS

1. Create the installation media
    1. Insert a USB device to be formatted
    2. Run "diskutil list" to determine the device’s name
    3. Run "mkusb.sh /dev/device_name InstallimageFortargetID.iso"
    4. Confirm that the USB device contains the following files:
        1. /EFI/BOOT/BOOTX64.EFI
        2. /S.efi
        3. /VI.efi
    5. Unmount/remove the USB device
2. Turn Off the target system
3. Insert USB install device
4. Hold the power button for 10 seconds

5. Immediately hold down the option key after the system turns on
6. Select the item named "EFI Boot" from the boot selection screen
7. For MacBook Air 6,x and MacBook Pros 11,x, a special unlock driver will need to be loaded
    1. Installer will automatically detect and load the driver, and the following text should appear:
        - ◊ "Tap power after shutdown, and wait 5 secs for reboot"
    2. Afer the machine reboot, the flash will be unlocked
    3. Once again hold the option key and select the same "EFI Boot" option
8. Installation will begin immediately: You should see "INSTALLING" XX% (Steps 1 of X) and "SUCCESS"
9. If the screen says FAILURE start over, and be sure that the power button is held for 10 seconds
10. Once the installation is complete, the system will turn off, and a receipt may have been recorded to the USB device
11. If installing from a CD instead of a USB device, one more boot, while holding option may be necessary to remove the CD

CONFIG.PLIST PARAMETERS

TRITON OPTIONS

- **Target ID**: A number used to identify and manage the implant’s files and keys
- **Listening Post**: The URL of the CGI script to which the implant will beacon
- **Minimum Beacon Interval**: The minimum number of seconds between beacon attempts. Random jitter may increase any given beacon interval by up to 33% of the specified value.
- **Check URLs**: A list of HTTP URLS that will be used to verify Internet connectivity before communication with an LP is attempted. A random URL is selected from this list during each beacon. It must return HTTP 200 in order for a beacon to occur.
- **Network Injection Target**: Processes into which the implant may inject it’s networking bundle. The process list is scanned in the order specified. The first process found is used until it exits.
- **Trigger Paths**: Paths that create trigger events when their contents are changed. User directory-relative paths must be begin with a tilde and must be quoted. This parameter is only relevant for Der Starke deployments.
- **Full Authentication**: Indicates whether or not the implant should use a fully authenticated SSL connection to the LP
- **Uninstall Alert** (optional): A domain name that will be queried when the implant uninstalls.
- **Uninstall Period** (optional): The number of seconds the tool waits for a successful beacon before deciding to uninstall. The start of the wait time is either the first time Triton is injected into OSX, or the last successful beacon.

EFI OPTIONS

- **Hibernation Period**: The number of seconds after installation time EFI delays injecting into the operating system. This check is only done at boot time. If Hibernation Period is set for 30 days (2592000 sec), Triton will be injected into OSX after 30 days from installation on the next reboot. If this option is set and NVRAM happens to get cleared, installation time will be assumed at the moment NVRAM was cleared, and a full hibernation cycle will take place before the next injection. Note that Hibernation Period and Hibernation Date cannot both be set.
- **Hibernation Date**: The UTC date after which Triton will be injected into diskarbitrationd during boot. Note that Hibernation Period and Hibernation Date cannot both be set.
- **Uninstall Date**: The UTC date after which a system reboot will cause the implant to uninstall or deactivate
- **Warning Threshold**: The number of times the Triton portion of the implant can fail load before the EFI portion uninstalls. Booting into an unsupported operating system and kernel panics increment the warning count
- **Patch Firmware**: A flag indicating whether or not the firmware should be unlocked to allow the implant to be securely deleted during an uninstalled. If set false, the implant will only deactive during an uninstall. If set true, this can add 10-45 secs to installation time depending on laptop.
- **Make Receipt File**: A flag indicating whether or not an installation receipt should be generated.
- **Uninstall if NVRAM Cleared**: A flag indicating whether or not the implant should uninstall if the system’s NVRAM is cleared. NVRAM is not cleared under normal circumstances, so it’s safe to leave this as, "NO"
- **Patch PEI for update persistence**: A flag indicating whether or not to reinject the implant during an OSX firmware update. This option will write two extra implants to firmware and can add 15-30 secs of installation time.

INSTALLER STATUS CODES AND MESSAGES

The installer may output the following status codes:

- 0x80000001 - Firmware Parse Error
- 0x80000002 - Firmware Append Error
- 0x80000003 - Firmware Write Error
- 0x80000004 - Firmware Compression Error
- 0x80000005 - Firmware Out of Space Error
- 0x40010000 - Firmware Unlock Patch Warning
- 0x40020000 - Receipt Warning: The receipt could not be written to the installation media
- 0x40040000 - PEI Find Warning: Unable to find PEI Core. Update persistence will not be enabled.
- 0x40080000 - PEI Append Receipt Warning: Unable to append implant to PEI Core. Update persistence will not be enabled
- 0x40100000 - PEI Write Warning: Unable to write implant to PEI Core. Update persistence will not be enabled

During Install the following message indicates the installer detected a machine that can be unlocked by holding the power butter for 10 secs:

- ERROR: TRIGGER NOT NEEDED

UNINSTALL COMMENTS

- After an uninstall, the flash memory will be unlocked until an Apple firmware update is applied
- If patch firmware option was not enabled, the implant is deactivated by setting a variable in NVRAM. If NVRAM is cleared and the "Uninstall if NVRAM Cleared option is not set, then the implant may become active again.
- Secure deletion of implant is performed on the first system reboot after an uninstall is triggered. It increases boot time by 30-60 seconds. Since BIOS/EFI will need to flush NVRAM every 40-60 boots, it is reasonable to ocassionally see boots that take a longer amount of time.
- If the power button is held down or power is lost during a secure delete of the implant, MacBooks mid 2012 and newer have run length fields that prevent the laptop from bricking. Parts of the implant may still forensically exist in firmware, but only as partial encrypted blobs. On laptops older than mid 2012, there is a possiblity of a corrupt firmware, but it has also been observed that secure deletes take less time on older hardware.

BOOTCAMP COMMENTS

- Booting Windows may affect the time and date settings in OS X. This can cause Der Starke to beacon several hours later than expected.