BLATSTING C&C transcript

laanwj.github.io/2016/09/09/blatsting-lp-transcript.html

Laanwj's blog

Randomness

Blog About
This showterm session shows a transcript of a session controlling BLATSTING.

(the site is not wide enough to embed the entire thing, so it's better to follow the link).

- **At the left side** it shows the listening post output, this is what the operative controlling it would see.
- **At the right side** scrolls by corresponding debugging output of the emulation framework. This shows the (decrypted) packets in transfer and what the emulated implant is doing.

No actual Fortinet/TOS routers were harmed in this process. The setup is the same as in previous post, however many more modules are succesfully loaded and emulated. Almost the entire framework besides TADAQUEOUS and SECONDDATE, which have their own means of C&C that I may come back to at some other time, and `file` and `install` which deal with affairs that are simply not part of the emulation.

Overview:

- Connect to VM domain. Start listening post.
- `1` : Open a session.
- LP connects to the implant, and loads the LP modules corresponding to the implant modules (to populate the menu). Apparently it fails to load the LP module for the sniffer (`m10000000`). We don't be sniffing any packets today.

```
Attempting to open a session.
CHALLENGE Type packet received.
AUTH_RESP Type packet received.
You are accessing BLATSTING.
Session opened.
dlopen error: ./lpconfig/m10000000/m10000000.lpmod: undefined symbol:
bp_bf_bpf_validateProgram
Corresponding LP module not found for (16 0 0).
...
Operation succeeded.
Connected to node 00000000
      Firewall Type : 00000000      Firewall Version: 00000000
      Remote Code Version: 666.6.6
      Remote IP Addr: 192.168.001.002
      Remote interface : 0000
      Listen IP Addr : 000.000.000.000
      Listen IP timeout (on remote node) : none
      Remote IP Sticky?: True
      LP IP: 192.168.001.001
      Source Port: 4000  Destination Port: 3000
      Session Start Time (on remote node): Thu Sep  8 11:44:36 2016
```

LP shows menu*:

```
----- Base Commands
  1) Open a session with the remote node
  2) List loaded LP modules
  3) Toggle expert mode [currently OFF]
  6) Re-synchronize LP module list (will not unload explicitly loaded modules)
  7) Toggle logging [currently ON]
  8) Toggle menu display [currently ON] (Recommended ON)
  9) Close session
999) BURN
  0) Quit Program

----- core interface
   0,0,0) Retrieve the list of exported interfaces
   0,0,1) Retrieve the current time on the remote node

----- crypto interface

----- network interface
   3,0,0) Read interfaces
   3,0,2) Send ARP

----- command and control interface
   7,0,0) Get comms state
   7,0,1) Set filter addresses

----- hash interface

----- tunnel interface
   9,0,0) Query tunnel module state
   9,0,1) Add a tunnel via command line
   9,0,2) Add a tunnel interactively
   9,0,3) Remove a tunnel
   9,0,4) Toggle printing active connections (expert only)

----- bpf interface

----- network profiler interface
  13,0,0) Query state
  13,0,1) Start scan
  13,0,2) Stop scan
  13,0,3) Restart scan
  13,0,4) Reset
  13,0,5) Get records
  13,0,6) Get records; dump to file
```

- `8` : Toggle “show menu” off otherwise it will print the screen-full menu after every command and it’s impossible to see any output without scrolling back all the time.
- `0,0,1` : Print time on remote node.

```
Time on remote node (GMT): Thu Sep  8 15:44:48 2016
```

`0,0,0` : Show the list of loaded modules and interfaces.

```
Exported interfaces:
  Module ID      Module type          Provider ID    Provider type
    0   0   3    core                   0   0   3    core
    1   1   0    crypto                 1   1   1    crypto
    3   1   1    network                3   1   0    network
   16   0   0    sniffer               16   0   1    sniffer
    7   0   0    cnc                    7   0   1    cnc
    8   1   0    hash                   8   1   1    hash
    9   0   0    tunnel                 9   0   2    tunnel
   12   1   0    bpf                   12   1   1    bpf
   13   0   0    networkProfiler       13   0   1    networkProfiler
```

`13,0,0` : Show networkProfiler configuration.

```
(13 0 0) networkProfiler module configuration:
networkProfiler module not configured.
```

`13,0,1` : Start networkProfiler scan. This shows the command line option help output:

```
Please enter your networkProfiler command line (-h for help, CTRL-n to cancel)?

  -S/--scantype <scan name>   name of predefined scan (enter ? to be provided with a
list)
  -i/--interface <interface index (as from interface listing)>  limit to the specified
interface
  -t/--traffictypes <traffic queue flags>  receive traffic of the specified types only
(enter ? to be provided with a list)
  -P/--prefilter netmask <netmask length>  netmask length for prefilter (0-32, default
0)
  -p/--prefilter <pcap filter string>  pcap pre-filter definition (enclose this in
double quotes)
  -s/--duration_seconds <seconds>  test duration in seconds
  -m/--duration_minutes <minutes>  test duration in minutes
  -r/--duration_hours <hours> test duration in hours
  -y/--duration_days <days>   test duration in days
  -N/--nperiods <# of scan periods>  number of periods to scan (default: 1)
  -n/--maxNRecords <# of records>  maximum number of records to keep per period
  --hashTableSize <# of entries>  size of the hash table
  -h/--help                   print this usage message
```

Show list of predefined scans (these are the files in `Firewall/BLATSTING/BLATSTING_201381/LP/lpconfig/m0d000000/predefinedScans`):

```
TCPUDP_condense_bytes_512  IPv4 TCP/UDP connection information, ports above 512
condensed, with total byte count (IPs, IP protocol, condensed ports, ttl, byte count)
TCPUDP_bytes          IPv4 TCP/UDP full connection information with byte count (IPs, IP
protocol, ports, ttl, byte count)
TCPSYN_condense_256   IPv4 TCP/UDP connection information, ports above 256 condensed,
with SYN count (IPs, IP protocol, condensed ports, ttl, SYN count)
TCPSYN                IPv4 TCP/UDP connection information with SYN count (IPs, IP
protocol, ports, ttl, SYN count)
TCPSYN_condense_bytes_3072  IPv4 TCP/UDP connection information, ports above 3072
condensed, with SYN and total byte count (IPs, IP protocol, condensed ports, ttl, SYN
count, total byte count)
TCPSYN_condense_1536  IPv4 TCP/UDP connection information, ports above 1536 condensed,
with SYN count (IPs, IP protocol, condensed ports, ttl, SYN count)
TCPSYN_condense_2560  IPv4 TCP/UDP connection information, ports above 2560 condensed,
with SYN count (IPs, IP protocol, condensed ports, ttl, SYN count)
TCPUDP_condense_1536  IPv4 TCP/UDP connection information, ports above 1536 condensed
(IPs, IP protocol, condensed ports, ttl)
TCPSYN_condense_bytes_1024  IPv4 TCP/UDP connection information, ports above 1024
condensed, with SYN and total byte count (IPs, IP protocol, condensed ports, ttl, SYN
count, total byte count)
TCPUDP_condense_1024  IPv4 TCP/UDP connection information, ports above 1024 condensed
(IPs, IP protocol, condensed ports, ttl)
TCPUDP_condense_2560  IPv4 TCP/UDP connection information, ports above 2560 condensed
(IPs, IP protocol, condensed ports, ttl)
MAC2MAC               Ethernet (MAC) src/dst address collection
TCPUDP_condense_bytes_256  IPv4 TCP/UDP connection information, ports above 256
condensed, with total byte count (IPs, IP protocol, condensed ports, ttl, byte count)
IP2IP_bytes           source, destination IP collection with total byte count
TCPUDP_condense_256   IPv4 TCP/UDP connection information, ports above 256 condensed
(IPs, IP protocol, condensed ports, ttl)
TCPSYN_condense_bytes_2048  IPv4 TCP/UDP connection information, ports above 2048
condensed, with SYN and total byte count (IPs, IP protocol, condensed ports, ttl, SYN
count, total byte count)
IP2IP                 IPv4 IP-to-IP address collection (who is calling whom?)
TCPSYN_condense_bytes_2560  IPv4 TCP/UDP connection information, ports above 2560
condensed, with SYN and total byte count (IPs, IP protocol, condensed ports, ttl, SYN
count, total byte count)
TCPUDP_condense_2048  IPv4 TCP/UDP connection information, ports above 2048 condensed
(IPs, IP protocol, condensed ports, ttl)
srcMACIP              source Ethernet (MAC) and source IP address collection
TCPSYN_condense_1024  IPv4 TCP/UDP connection information, ports above 1024 condensed,
with SYN count (IPs, IP protocol, condensed ports, ttl, SYN count)
TCPUDP_condense_bytes_1536  IPv4 TCP/UDP connection information, ports above 1536
condensed, with total byte count (IPs, IP protocol, condensed ports, ttl, byte count)
TCPSYN_condense_bytes_256  IPv4 TCP/UDP connection information, ports above 256
condensed, with SYN and total byte count (IPs, IP protocol, condensed ports, ttl, SYN
count, total byte count)
TCPSYN_condense_bytes_1536  IPv4 TCP/UDP connection information, ports above 1536
condensed, with SYN and total byte count (IPs, IP protocol, condensed ports, ttl, SYN
count, total byte count)
TCPUDP_condense_bytes_2560  IPv4 TCP/UDP connection information, ports above 2560
condensed, with total byte count (IPs, IP protocol, condensed ports, ttl, byte count)
TCPUDP_condense_bytes_1024  IPv4 TCP/UDP connection information, ports above 1024
condensed, with total byte count (IPs, IP protocol, condensed ports, ttl, byte count)
srcIP                 source IP address collection
TCPUDP                IPv4 TCP/UDP full connection information (IPs, IP protocol,
```

```
ports, ttl)
TCPSYN_condense_512   IPv4 TCP/UDP connection information, ports above 512 condensed,
with SYN count (IPs, IP protocol, condensed ports, ttl, SYN count)
TCPSYN_condense_bytes_512  IPv4 TCP/UDP connection information, ports above 512
condensed, with SYN and total byte count (IPs, IP protocol, condensed ports, ttl, SYN
count, total byte count)
TCPSYN_condense_3072  IPv4 TCP/UDP connection information, ports above 3072 condensed,
with SYN count (IPs, IP protocol, condensed ports, ttl, SYN count)
TCPUDP_condense_3072  IPv4 TCP/UDP connection information, ports above 3072 condensed
(IPs, IP protocol, condensed ports, ttl)
TCPSYN_condense_2048  IPv4 TCP/UDP connection information, ports above 2048 condensed,
with SYN count (IPs, IP protocol, condensed ports, ttl, SYN count)
TCPUDP_condense_bytes_3072  IPv4 TCP/UDP connection information, ports above 3072
condensed, with total byte count (IPs, IP protocol, condensed ports, ttl, byte count)
TCPUDP_condense_512   IPv4 TCP/UDP connection information, ports above 512 condensed
(IPs, IP protocol, condensed ports, ttl)
TCPUDP_condense_bytes_2048  IPv4 TCP/UDP connection information, ports above 2048
condensed, with total byte count (IPs, IP protocol, condensed ports, ttl, byte count)
```

Create a `-STCPUDP` predefined scan, using default settings, and start it:

```
  traffic types: IP4
  total scanning time:    0 days 03:00:00
  scan period duration:   0 days 03:00:00
  number of scan periods: 1
    record size:       18  table size:       96  hash table size:       64
    memory usage for scan results:         1754 bytes
    approximate run-time memory usage:     2266 bytes
    Prefilter: n   Link layer filter: n    Network layer filter: y
Tracking the following elements:
    IPv4 source address
    IPv4 destination address
    IPv4 protocol
    TCP/UDP source port
    TCP/UDP destination port
    IPv4 TTL (recorded once, not tracked)
This configuration could be established with the following command line:
  -S <scan type> -t IP4 -s 10800 -N 1 -n 96 --hashTableSize 64
Sending start request to implant. Are you sure (y/n) [y]? y
  networkProfiler scan started.
```

- `8` : Re-show menu.
- `13,0,5` : Show records of ongoing networkProfiler scan.

```
(13 0 0) networkProfiler module data:
Scan period 0:
    total packets collected:                2
    packets discarded due to error:         0
    number of records collected:            1
    number of records dropped:              0
    scan start (target box time, displayed as GMT):  Thu Sep  8 15:45:37 2016
    scan end (target box time, displayed as GMT)  :  Thu Sep  8 18:45:37 2016A
        scan in progress

Records:
IPv4 source address                     : 192.168.001.001
IPv4 destination address                : 192.168.001.002
IPv4 protocol                           : 0x11
TCP/UDP source port                     : 3000
TCP/UDP destination port                : 4000
IPv4 TTL (recorded once, not tracked)   : 64
   count: 2
```

- This shows one record which summarizes the two UDP packets exchanged between the implant and LP. Nothing else is happening on the simulated network. To get a better idea of what it is doing it would make sense to inject some fake traffic.

- `7,0,0` : Get comms state. This simply shows the same information again as when connecting.

```
Connected to node 00000000
      Firewall Type : 00000000      Firewall Version: 00000000
      Remote Code Version: 666.6.6
      Remote IP Addr: 192.168.001.002
      Remote interface : 0000
      Listen IP Addr : 000.000.000.000
      Listen IP timeout (on remote node) : none
      Remote IP Sticky?: True
      LP IP: 192.168.001.001
      Source Port: 4000  Destination Port: 3000
      Session Start Time (on remote node): Thu Sep  8 11:44:36 2016
```

`7,0,1` : Set a filter. Apparently I botched this as it loses contact to the implant.

```
Please enter the new filter IP/netmask [255.255.255.255/32]: 192.168.1.0/24
Please enter the filter timeout in minutes (0 for no timeout) [0]: 100
About to install filter IP 192.168.001.000/24, timeout 100 minutes.
Are you sure? (y/n) [n]? y
Operation succeeded.
2016-09-08 11:44:48  Menu Selection>? 0,0,0
11:44:55 2016-09-08  ===> selection 0 0 0

Timed Out
createSendRecv_5iHelper: attempt 1 of 3 timed out.
```

`0` : Exit session.

* 999) BURN sure sounds enticing, but can't demonstrate it as the necessary interface is not simulated. Drats.

Written on September 9, 2016

Tags: eqgrp malware
Filed under Reverse-engineering