Network detector for Winnti malware

github.com/TKCERT/winnti-detector

TKCERT

winnti-detector detects Winnti (as of 2016/2017) communication patterns in network traffic.

It can read PCAPs or listen on a live interface.

Winnti

Winnti is a malware that is used by some APT groups.

It has been used since at least 2013 and has evolved over time. You can find some information here

- https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf
- https://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf
- https://hitcon.org/2016/pacific/0composition/pdf/1201/1201%20R2%201610%20winnti%20polymorphism.pdf

Handshake

The driver component of Winnti (aka "NdisReroute") is able to reroute network traffic from ports that are already occupied by legit applications to the malware's userspace component.

The first packet of a TCP stream signals the driver that the stream shall be rerouted. I call such a packet a "Winnti HELO". It is exactly 16 bytes long and the bytes match the following relation:

```
Winnti handshake Example:

    dw0           dw1           dw2             dw3
5B 44 B4 91   xx xx xx xx   31 18 30 59   [84 C8] {6A 5C}

5B 44 B4 91       ==        31 18 30 59 ^ {6A 5C} [84 C8]
```

- **dw0** calculated from *dw2* and *dw3*
- **dw1** random but not zero. Only seen timestamps in here but any value works.
- **dw2** random but not zero
- **dw3** random but not zero

Installation

winnti-detector uses libnids which you can install with

```
# git clone https://github.com/MITRECND/libnids.git
# cd libnids
# ./configure --enable-shared && make && sudo make install
# sudo ldconfig -i
```

You can then compile and run winnti-detector

```
# make
# ./wntidect
wntidect version 1.6 using libnids 1.25 -- Stefan Ruester
Usage: ./wntidect <-i device|-f pcapfile> [-l]
  -l  Log to syslog (local7.alert 'nsm')
```

Output

stdout

```
$ wntidect -f finding.pcap
wntidect version 1.6 using libnids 1.25 -- Stefan Ruester
[i] Reading PCAP file eth0_capture.pcap
[!] 2018-01-23 09:12:50.709193Z Found WINNTI session setup: (TCP) 10.123.12.123:59308
-> 10.34.34.34:443
[!] 2018-03-06 00:28:46.525901Z Found WINNTI session setup: (UDP) 10.123.12.123:58762
-> 10.34.34.35:443
```

syslog

As the usage text suggests, you can use the parameter `-l` to write syslog entries whenever a match is found. The program always also outputs findings on stdout.