Suricata rules to detect Winnti communication

github.com/TKCERT/winnti-suricata-lua

TKCERT

This ruleset enables Suricata to detect the handshake of certain Winnti variants as seen in the wild in 2016/2017.

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

Copy the rules and lua files to your suricata rules directory

```
cp winnti.lua   /etc/suricata/rules/
cp winnti.rules /etc/suricata/rules/
```

activate the rules by adding them to `suricata.yaml`

```
[...]
rule-files:
 - winnti.rules
[...]
```