World Terminator Flow with Suricata

Éric Leblond

OISF

6 Juin 2013

WTF: Word Terminator Flow

Objective

- Fight against Word file transfer
- Because it is Office is heavy like hell
- And you even have to pay for it

Method

- Mark packet when a Word file is transferred
- Limit bandwith with Linux QoS

Suricata configuration

The rule

```
alert http any any -> any any ( \
  msg: "Microsoft Word upload"; \
  nfq_set_mark:0x1/0x1; \
  filemagic:"Composite Document File V2 Document"; \
  sid:666 ; rev:1;)
```

Running suricata

```
suricata -q 0 -S word.rules
```

Netfilter configuration

Queueing packets

```
iptables -I FORWARD -p tcp --dport 80 -j NFQUEUE
iptables -I FORWARD -p tcp --sport 80 -j NFQUEUE
# iptables -I OUTPUT -p tcp --dport 80 -j NFQUEUE
# iptables -I INPUT -p tcp --sport 80 -j NFQUEUE
```

Propagating the mark

```
iptables -A PREROUTING -t mangle -j CONNMARK --restore-mark
iptables -A POSTROUTING -t mangle -j CONNMARK --save-mark
# iptables -A OUTPUT -t mangle -j CONNMARK --restore-mark
```

Linux QoS configuration

Setting up QoS tree

```
tc qdisc add dev eth0 root \
        handle 1: htb default 0
tc class add dev eth0 parent 1: \
        classid 1:1 htb \
        rate 1kbps ceil 1kbps
```

Sending marked packets to their fate

```
tc filter add dev eth0 parent 1: \
        protocol ip prio 1 \
        handle 1 fw flowid 1:1
```

Evasion technique

Detecting the evasion

```
alert http any any -> any any ( \
  msg:"Tricky Microsoft Word upload"; \
  nfq_set_mark:0x2/0x2; \
  fileext:!"doc"; \
  filemagic:"Composite Document File V2 Document"; \
  filestore; \
  sid:667; rev:1;)
```

Watching the clever ones

Using ipset to mark packets

```
ipset create cheaters hash:ip timeout 3600
iptables -A POSTROUTING -t mangle -m mark \
    --mark 0x2/0x2 \
    -j SET --add-set cheaters src --exists
```

Logging marked packets

```
iptables -A PREROUTING -t raw \
    -m set --match-set cheaters src,dst \
    -j NFLOG --nflog-group 1
```

Ulogd to keep the trace

Configuring ulogd

- Ulogd will log packets to a pcap file
- We need to activate a stack in ulogd.conf:

```
plugin="/home/eric/builds/ulogd/lib/ulogd/ulogd_output_PCAP.so"
stack=log2:NFLOG,base1:BASE,pcap1:PCAP
```

Starting ulogd

```
ulogd -c ulogd.conf
```

Questions

Avez vous des questions ?

Plus d'information

- L'article de blog : `https://home.regit.org/2012/10/defend-your-network-from-word/`
- Version longue aux RMLLs : `http://schedule2013.rmll.info/programme/technique/securite/article/defendez-votre-reseau-contre-les`