# Behavorial xbits with Suricata

travisgreen.net/2021/07/22/behavioral-xbits.html

Jul 22, 2021

## The Setting:

While attempting to build detection for DeepRats as revealed by @benkow_, I managed to have (what I think) is a pretty good idea about using xbits. I'll admit its a bit basic but I think sometimes the best ideas are deceivingly simple.

## The Idea:

1.) observe potentially malicious behavior, set an xbit
2.) observe another potentially malicious behavior, set another xbit
3.) build detection consisting of a good fast_pattern match and xbits checks

Example (edited for clarity, full working example here):

IP check xbits set here:

```
alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY IP Check Domain (myexternalip .com in TLS SNI)"; flow:established,to_server; tls.sni; content:"myexternalip.com"; endswith; nocase; xbits:set,ET.ipcheck,track ip_src; classtype:policy-violation; sid:7704131; rev:1;)
```

```
alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY IP Check Domain (freegeoip .live in TLS SNI)"; flow:established,to_server; tls.sni; content:"freegeoip.live"; endswith; nocase; xbits:set,ET.ipcheck,track ip_src; xbits:set,ET.ipcheck,track ip_src; classtype:policy-violation; sid:7704132; rev:1;)
```

Known abused storage as dropper site xbit set here:

```
alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY IPFS Domain (storage.snark .art in TLS SNI)"; flow:established,to_server; tls.sni; content:"myexternalip.com"; endswith; nocase; xbits:set,ET.dropsite,track ip_src; classtype:policy-violation; sid:7704133; rev:1;)
```

Tor & final detection:

```
alert tcp any ![21,25,110,143,443,465,587,636,989:995,5061,5222,8443] -> any any (msg:"ET MALWARE Possible DarkRats Tor Traffic"; flow:established,from_server; content:"|06 03 55 04 03|"; pcre:"/^.{2}www\.[0-9a-z]{8,20}\.com[01]/Rs"; content:"|06 03 55 04 03|"; distance:0; pcre:"/^.{2}www\.[0-9a-z]{8,20}\.net/Rs"; xbits:isset,ET.ipcheck,track
```

```
ip_dst; xbits:isset,ET.dropsite,track ip_dst; classtype:trojan-activity;
sid:7704134; rev:1;)
```

Note: `track ip_dst` here because this detects the Tor RESPONSE traffic.

The final sig could probably also be a great HUNTING sig. Other HUNTING sig ideas:

- Tor -> coinmining
- IP Check -> HTTP POST
- IP Check -> HTTP to frequently abused TLD

tweet me your ideas!