À la recherche du méchant perdu

É. Leblond

Stamus Networks

9 juin 2017

STAMUS NETWORKS

STAMUS NETWORKS

Suricata

Détection d'intrusion

- Moteur d'analyse réseau
- Détection d'intrusion
- Basé sur des signatures

Network Security Monitoring

- Extraction de métadonnées
- HTTP, SMTP, DNS, TLS, ...

Communautaire

- License GPLv2
- Fondation OISF

STAMUS NETWORKS

Hillar, il demande la liste des méchants

Exercice OTAN

- Simulation d'attaques sur des SI complexes
- Red team/Blue Team/Yellow Team
- Invité par Hillar Aarelaid dans la Yellow team

Yellow team

- Suricata
- Molloch
- Elasticsearch

Trouver les attaquants

- À partir des alertes
- En utilisant Suricata
- Voir leur propagation dans le réseau

STAMUS NETWORKS

Propagation

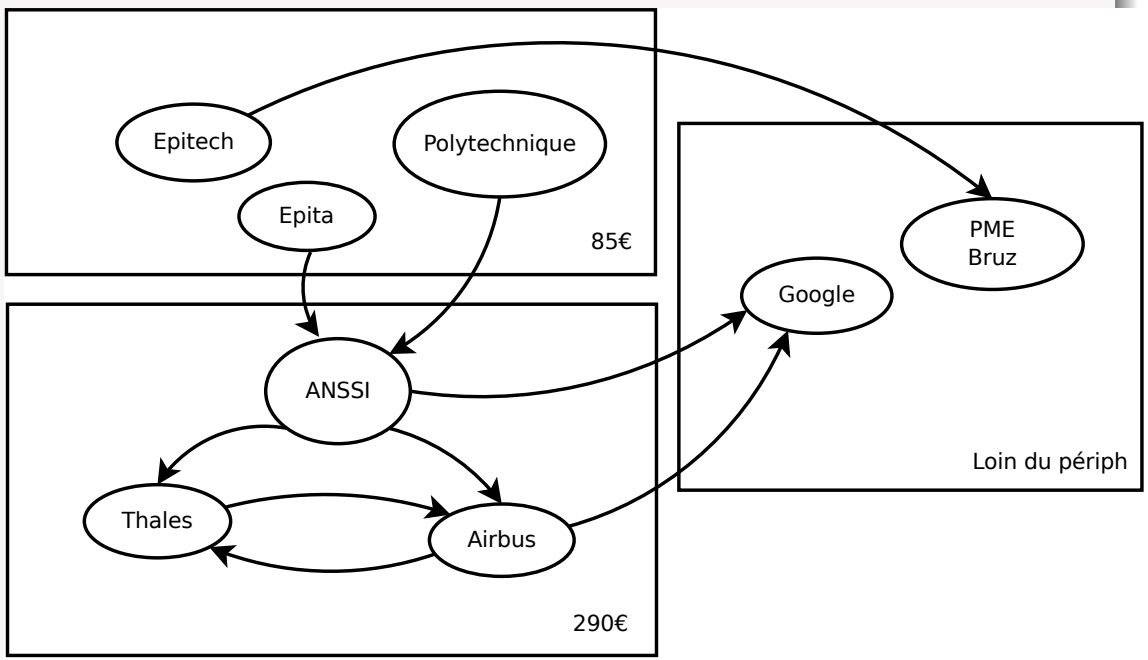
Voir les chemins

- Potentiel
- D'un point externe
- Vers un point interne

Graphe orienté

- Vecteurs sont les adresses IP
- Arête depuis Source vers Target

Exemple anonymisé



STAMUS NETWORKS

Alerte Suricata au format JSON


```
{
  "timestamp": "2017-01-17T09:53:42.511060-0800",
  "event_type": "alert",
  "src_ip": "82.165.177.154",
  "src_port": 80,
  "dest_ip": "10.170.127.169",
  "dest_port": 58146,
  "proto": "TCP",
  "alert": {
    "signature_id": "1234",
    "signature": "Detect secondary executable payload - xbits 2",
  },
  "http": {
    "hostname": "testmyids.com",
    "url": "/exe/testmyids.exe",
    "http_user_agent": "Wget/1.18 (linux-gnu)",
    "http_content_type": "application/x-msdos-program",
    "http_method": "GET",
    "status": 200,
  }
}
```

Identification de la Source de l'attaque

Use the Source

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (
        msg:"ET SCAN NMAP -f -sX"; fragbits:!M;
        dsize:0; flags:FPU,12; ack:0; window:2048;
        classtype:attempted-recon; sid:2000546; rev:7;)
```

Ou pas

```
alert http $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (
        msg:"Fast 403 Error Messages, Possible Web Application Scan";
        flow:from_server,established;
        content:"HTTP/1.1 403"; depth:13;
        threshold: type threshold, track by_dst, count 35, seconds 60;
        reference:url,www.checkupdown.com/status/E403.html;
        reference:url,doc.emergingthreats.net/2009749;
        classtype:attempted-recon; sid:2009749; rev:4;)
```

IDS : Illuminations De Sapin

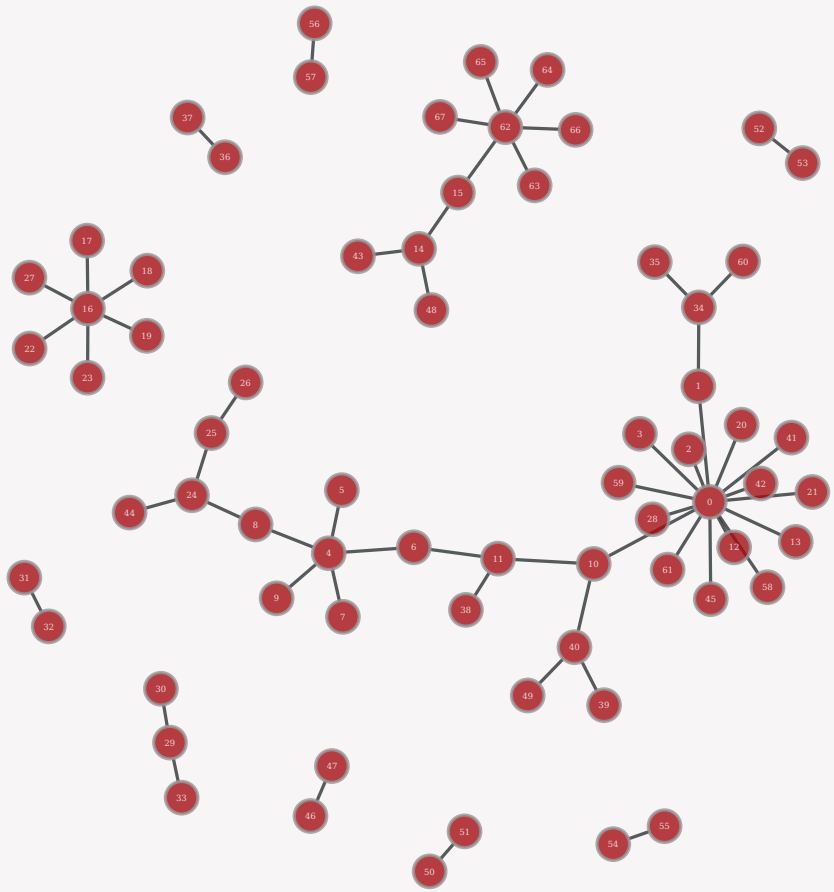
Voir les liens

- Potentiel
- D'un point externe
- Vers un point interne

Graphe non orienté

- Vecteurs sont les adresses IP
- Arête entre source et destination

Résultat anonymisé



NETWORKS

Non, Jef, t'es pas tout seul

Snort

- "Même" langage de signature
- Même logique
- Pas de lien sans analyse externe

Jeux de règles Sourcefire

- A posteriori envisageable
- Utilisation de metadata
- Mais pas pour ça

Prelude

- rfc4765.txt définit Source et Target
- Source : `The source(s) of the event(s) leading up to the alert.`
- Target : `The target(s) of the event(s) leading up to the alert.`
- L'implementation utilise IP source et destination
- Violation de la RFC

STAMVS NETWORKS

Objectifs

- Ajout dans la sortie JSON de la notion de Source et Target
- Fixer la sortie Prelude

Introduction du mot clef `target`

```
target [src_ip|dest_ip]
```

Mise à jour du code

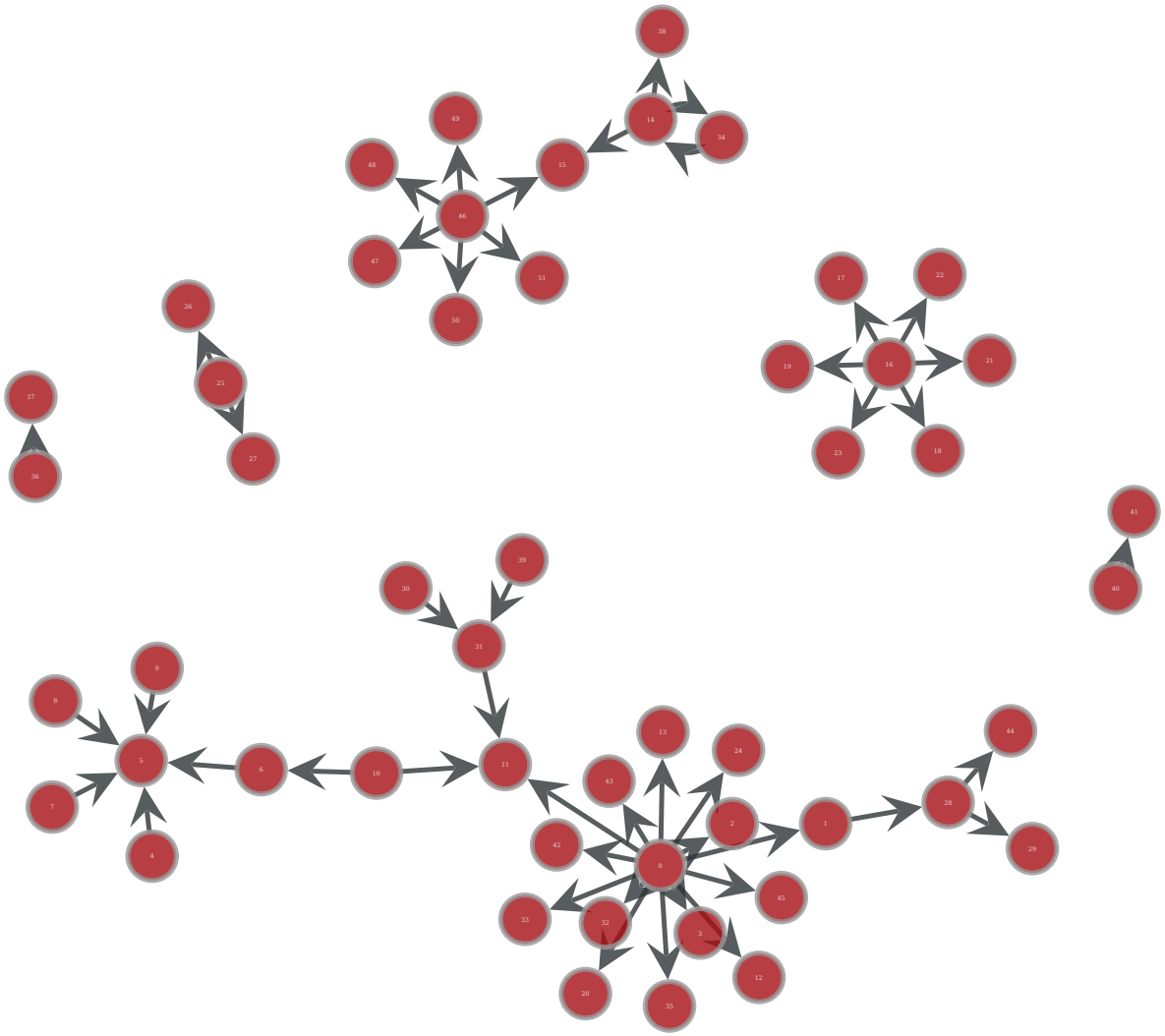
- Modification de la sortie Prelude
- Ajout de nouveaux champs dans la sortie EVE JSON

STAMUS NETWORKS

Alert avec Source et Target


```
{
  "timestamp": "2016-12-07T14:17:45.754203+0100",
  "event_type": "alert",
  "src_ip": "191.18.3.4", "src_port": 59540,
  "dest_ip": "10.242.4.2", "dest_port": 3389,
  "proto": "TCP",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2013479,
    "rev": 4,
    "signature": "fast Terminal Server Traffic, Potential Outbound Scan",
    "category": "Misc activity",
    "severity": 3,
    "source": {
      "ip": "198.18.3.4", "port": 59540
    },
    "target": {
      "ip": "10.242.4.2", "port": 3389
    }
  }
}
```

Graphe orienté obtenu



STAMVS NETWORKS

STAMVS NETWORKS

Conclusion

Vers une automatisation de l'analyse

- Construction de graphes orientés
- Utilisation d'algorithmes de découvertes de chemin

Travail restant

- Acceptation du code dans Suricata
- Mise à jour des règles

Évolution

- Vers des Source/Target évoluées : `target: dest_ip,smtp.rcpt_to`
- Prendre le temps en considération dans le graphe

STAMUS NETWORKS