STAMUS NETWORKS

Attaque de type Supply Chain sur Suricata

7 juin 2023 | Eric Leblond

STAMVS NETWORKS

Création: 2014 par Éric Leblond et Peter Manev

Headquarters: Indianapolis, USA et Paris, France

Website: www.Stamus-Networks.com

Stamus et l' Open-Source:

- SELKS - un Suricata IDS/NSM clé en main téléchargé >1000/mois
- Auteur du livre open-source - *Le guide Suricata pour l'analyste sécurité*
- Premier contributeur sur Suricata en dehors de l'OISF…

Offre commerciale:

- *Stamus Security Platform: Network detection and Response*

Suricata is far more than an IDS/IPS

Network Traffic
Cloud & On-premise

SURICATA

- IDS Alerts
- Protocol Transactions
- Network Flows
- PCAP Recordings
- Extracted Files

Source: Stamus Networks

STAMUS NETWORKS

Pass the Salt, Lille, 2022

- Conférence open source et sécurité
- Présentation par Mickaël Salaün
  - Sandboxing your application with Landlock
  - https://archives.pass-the-salt.org/Pass%20the%20SALT/2022/slides/PTS2022-Talk-04-Sandboxing-your-application-with-Landlock.pdf
- Tutorial sur l'implémentation de Landlock

Concept de Landlock

- L’application se sandboxe elle-même
  - Pas de fichier de configuration géré par un démon externe
  - Le code définit ses permissions
  - Si landlock est activé, la protection est appliquée
  - Apporte une flexibilité importante par la prise en compte
    - Des options de ligne de commande
    - Du fichier de configuration
- Pro & cons
  - Application doit être modifiée
  - Flexibilité pour une utilisation dynamique
  - Encore peu de variétés dans les permissions (systèmes de fichier)

Implémentation de Landlock dans Suricata

- Suricata peut être lancé:
  - en démon (sniff interface)
  - par la ligne de la commande (rejeu d'un pcap)
- Les répertoires d'écritures et lecture sont donc différents selon le run
  - Dans Suricata, la ligne de commande écrase les valeurs de configuration
  - Utilisation des valeur de configuration pour définir les droits
- Implémentation:
  - Prépare une politique
  - Pour chaque répertoire utilisé
    - positionne lecture ou écriture
  - Applique la politique
- Plus d'info: https://docs.suricata.io/en/latest/configuration/landlock.html

Suricon, Athènes, 2022

- Présentation dataset par Eric Leblond
  - Comment utiliser les datasets pour la détection d'IOC et d'anomalies
  - https://youtu.be/2eyX0sNtJ3I
- Plan de la présentation
  - Rappel des fonctionnalités
  - Contributions sur dataset par Stamus Networks dans Suricata 7
  - Exemples d'utilisation

Dataset et IOC

- Concept initial des datasets
  - Trouver rapidement une valeur dans une liste
  - Application dans la vérification d'IOC
    - Liste de nom d'hotes
    - Liste de user agents
  - Fonctionnement par champ fichier utilisable sur les sticky buffers

http.host; content:".com"; endwith; dataset:isset,mylist,type string;

Dataset et découverte

- Enrichissement des datasets sur le chemin des paquets
- Exemple en stockant les urls pour une liste de domaine

```
http.host; dataset:isset,company-hosts.lst \\
http.uri; dataset:set,company-urls.lst
```

Rump sur landlock

- Landlock dans Suricata par Eric Leblond
  - 5 min pour présenter le support de landlock dans Suricata 7
  - Préparer suite à une demande lors de la conf
- Une de mes plus mauvaises présentations
  - Pas réussi à montrer que, en vrai, c'est utile
  - Avant de descendre de l'estrade

SSTIC, Rennes, 2023

- Attaque de type supply chain sur Suricata
  - Signatures utilisant les datasets avec les options
    - save ou state

```
dataset:<set|isset|isnotset>,<name> \
     [, type <string|md5|sha256>, save <file name>, load <file name>, state <file name>,
 memcap <size>, hashsize <size>];
```

  - 2 problèmes:
    - configuration dans la signature
    - <file name> peut être un chemin absolu
  - Écriture possible avec les droits de l'utilisateur
    - Effacement du contenu de fichiers critiques
    - Souvent l'utilisateur est root

Protection offerte par landlock

- L’écriture est limitée aux:
  - Répertoire de log
  - Répertoire d’état
- Aucune réécriture possible sur le système
  - En dehors de répertoires dédiés à Suricata

Demo

```
suricata on  master [$?] via C v12.2.0-gcc via 🌙 via 🐍 v3.11.2 took 3s
❯ cat tests/dataset-reload.rules
alert http any any → any any (msg:"test dataset"; sid:2; rev:1; http.host; dataset:set,test,type string,state /home/regit/

suricata on  master [$?] via C v12.2.0-gcc via 🌙 via 🐍 v3.11.2 took 1m31s
❯ ~/builds/suricata/bin/suricata -r ~/Downloads/2019-07-05-Ursnif-with-Trickbot-and-IcedID.pcap -l ~/tmp/out -c ~/builds/su
yaml  -S tests/dataset-reload.rules
Notice: suricata: This is Suricata version 7.0.0-rc2-dev (6154bab49 2023-06-02) running in USER mode [LogVersion:suricata.c
Error: datasets: fopen '/home/regit/toto' failed: Permission denied [DatasetLoadString:datasets.c:506]
Error: detect-dataset: failed to set up dataset 'test'. [DetectDatasetSetup:detect-dataset.c:387]
Error: detect: error parsing signature "alert http any any → any any (msg:"test dataset"; sid:2; rev:1; http.host; dataset
home/regit/toto;)" from file tests/dataset-reload.rules at line 1 [DetectLoadSigFile:detect-engine-loader.c:192]
Warning: detect: 1 rule files specified, but no rules were loaded! [SigLoadSignatures:detect-engine-loader.c:355]
Notice: threads: Threads created → RX: 1 W: 12 FM: 1 FR: 1   Engine started. [TmThreadWaitOnThreadRunning:tm-threads.c:188
Notice: suricata: Signal Received.  Stopping engine. [SuricataMainLoop:suricata.c:2827]
Notice: pcap: read 1 file, 49027 packets, 40213927 bytes [ReceivePcapFileThreadExitStats:source-pcap-file.c:388]

suricata on  master [$?] via C v12.2.0-gcc via 🌙 via 🐍 v3.11.2
❯
```

Considérer les sources comme vecteur d'attaques ?

- Source:
  - Ensemble de signatures / fichiers de données
  - URL de téléchargement des données
- Plusieurs types de sources :
  - Interne : développé par le SOC
  - Public : disponible sur internet
  - Communautaire : partage de type MISP
- Évolution :
  - Modèle initial : Fournisseur + Interne
  - Modèle actuel : Complètement ouvert
- Le niveau de confiance doit être pris en compte

Contrôle de la chaîne d'approvisionnement

- Deux fonctions potentiellement dangereuses disponibles dans les signatures
  - dataset avec l'option save ou state
  - lua script dans les signatures

http.header; content:"cmd"; lua:myscript.lua

- Limitation au niveau des sources de signatures
  - Source interne peut avoir accès aux fonctions
  - Source externe non contrôlée doit être filtrée
    - Source publique
    - Partage communautaire (MISP)

Contre mesure dans Suricata

- Abandon des chemins absolus dans la configuration des datasets
  - Écriture limitée au répertoire de données
  - Pas d’écrasement de fichier possible
- Option de désactivation de Lua
  - Souvent compilé dans les distributions
  - Fonction rarement utilisée

Conclusion

- Les sources de signatures doivent être contrôlées
  - Implémentation d'un niveau de confiance
- Problème touchant beaucoup de système de détections
  - Basé sur des signatures/règles de détection
- Landlock s'avère offrir une protection intéressante
  - pour un faible coût de développement
  - avec peu de configuration pour l'utilisateur
- Merci à l'ANSSI pour la CSPN sur Suricata 6
  - https://www.ssi.gouv.fr/entreprise/certification_cspn/suricata-version-6-0-8/
  - Mais attention à bien sécuriser toute la chaîne

Merci !

Eric Leblond
Directeur Technique
el@Stamus-Networks.com

STAMUS NETWORKS