



SELKS



SURICATA
ELASTICSEARCH
LOGTSTASH
KIBANA
SCIRIUS



SELKS

Première étape - Apprendre à lire une règle



ET PHISHING Generic Phishing Panel Accessed on External Server

IP and Time Stats

Advanced Data

Information

History

Definition

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET PHISHING Generic Phishing Panel Accessed on External Server"; flow:established,to_client; file.data; content:"<title>PANEL FREAKZBROHTER"; nocase; fast_pattern; classtype:web-application-activity; sid:2030611; rev:2; metadata:affected_product Web_Browsers, attack_target Client_Endpoint, created_at 2020_07_29, deployment Perimeter, former_category PHISHING, signature_severity Major, tag Phishing, updated_at 2020_07_29;)
```

L'ACTION

HEADER

OPTIONS

drop tcp \$HOME_NET any -> \$EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124;
classtype:trojan-activity; sid:2008124; rev:2;)



сгэсэгАвс:сго]су-сстгггА: атг:2008124: ксА:3:)
ггюмртс:гэсэг'гс-бгого-гко: сонтсуг: "NICK " : бскс: "NICK .*USA.*[0-9]{3,}"\т: ксгсгсугс:сгг'гос-сгсгггггггсгс-сгс\2008124:
гкоб'сгсб \$HOME_NET суА -> \$EXTERNAL_NET суА (мсд:"ET TROJAN Likely Bot Nick in IRC (USA +..)": ггом:сгсгггггггг'сг-сгсгсгс:

L' ACTION

PEUT SE RÉSUMER PAR LA QUESTION
“QUE DOIS FAIRE LORS D'UNE SIGNATURE ?”

Pass

Si une signature correspond et contient un passe, Suricata arrête de scanner le paquet et passe à la fin de toutes les règles (uniquement pour le paquet actuel).

Drop

Cela ne concerne que le mode IPS/en ligne. Si le programme trouve une signature qui correspond, contenant la goutte, il s'arrête immédiatement. Le paquet ne sera plus envoyé. Inconvénient : Le destinataire ne reçoit pas de message sur ce qui se passe, ce qui entraîne un time-out (certainement avec TCP). Suricata génère une alerte pour ce paquet.

Reject



Il s'agit d'un rejet actif du paquet. Le destinataire et l'expéditeur reçoivent tous deux un paquet de rejet. Il existe deux types de paquets de rejet qui seront automatiquement sélectionnés. Si le paquet offensant concerne le TCP, il s'agira d'un paquet de réinitialisation. Pour tous les autres protocoles, il s'agira d'un paquet d'erreur ICMP. Suricata génère également une alerte. En mode Inline/IPS, le paquet incriminé sera également supprimé comme pour l'action "drop".

L'ACTION

PEUT SE RÉSUMER PAR LA QUESTION
“QUE DOIS FAIRE LORS D'UNE SIGNATURE ?”

Alerte

Si une signature correspond et contient une alerte, le paquet sera traité comme tout autre paquet non menaçant, sauf que pour celui-ci, une alerte sera générée par Suricata. Seul l'administrateur du système peut remarquer cette alerte.

Ordre de traitement des actions



>> pass>> drop>> reject >> Alert



Attention seul l'administrateur de l'instance suricata administrateur pourras observer les Alertes

HEADER - ENTÊTE DE RÈGLE

Entête prenant en compte plusieurs champs le protocole , les adresses privées et publique, les ports.

Protocole



```
tcp $HOME_NET any -> $EXTERNAL_NET any
```



Protocole : ce champ s'exprime et attend un protocole connu. Des protocoles de la couche applicative sont aussi possibles: http, ftp, tls (y compris ssl), smb, dns, ssh, smtp, imap, ...etc

tcp

udp

icmp

ip

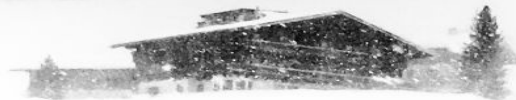
HEADER - ENTÊTE DE RÈGLE

Entête prenant en compte plusieurs champs le protocole , les adresses privées et publique, les ports.

IP PRIVÉE



```
tcp $HOME_NET any -> $EXTERNAL_NET any
```



\$HOME_NET: Définit les adresses dites privées

Variable définie dans le fichier /etc/suricata/suricata.yaml

```
address-groups:  
  HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"  
  #HOME_NET: "[192.168.0.0/16]"  
  #HOME_NET: "[10.0.0.0/8]"  
  #HOME_NET: "[172.16.0.0/12]"  
  #HOME_NET: "any"
```

Le champ \$HOME_NET peut être remplacé par une IP ou un RANGE/IP.

ref. <https://suricata.readthedocs.io/en/suricata-4.1.4/rules/intro.html#source-and-destination>

HEADER - ENTÊTE DE RÈGLE

Entête prenant en compte plusieurs champs le protocole , les adresses privées et publique, les ports.

IP PUBLIQUE



```
tcp $HOME_NET any -> $EXTERNAL_NET any
```



`$EXTERNAL_NET`: Définit les adresses dites publiques.

Variable définie dans le fichier `/etc/suricata/suricata.yaml`



```
EXTERNAL_NET: "!$HOME_NET"  
#EXTERNAL_NET: "any"
```

Le champ `$EXTERNAL_NET` peut être remplacé par une IP ou un RANGE/IP.

ref. <https://suricata.readthedocs.io/en/suricata-4.1.4/rules/intro.html#source-and-destination>

HEADER- ENTÊTE DE RÈGLE

Entête prenant en compte plusieurs champs le protocole , les adresses privées et publique, les ports.

PORT



PORT



```
tcp $HOME_NET any -> $EXTERNAL_NET any
```



“any” Tous ou un numéro de port voire même une selection:



[80,443]

[!9009,8080]

[22,2222,22022]

[3306:3389]

HEADER- ENTÊTE DE RÈGLE

Entête prenant en compte plusieurs champs le protocole , les adresses privées et publique, les ports.

DIRECTION



```
tcp $HOME_NET any -> $EXTERNAL_NET any
```



-> sens de lecture de la règle ou encore <>



Une exception au sens de lecture est signalée à ne surtout pas négliger <- n'existe pas !

OPTIONS

Ce champ prend en compte toute la subtilité est la profondeur de votre règle

MSG



```
(msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124; rev:2;)
```



message exprimé sous la forme msg:"Le message que vous souhaitez voir à l'écran"

OPTIONS

Ce champ prend en compte toute la subtilité est la profondeur de votre règle



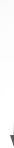
Le champ flow “flux” de paquets prend l’état de connection de flux de paquet. Pour l’exemple ici “established” établit , to_server depuis le serveur

Le champ flowbit donne des précisions sur le type flow et les options choisie. Pour l’exemple ici isset, is_proto_irc assure la remontée d’une alerte si deux paquets remonte le même flux embarquant

OPTIONS

Ce champ prend en compte toute la subtilité est la profondeur de votre règle

content



```
(msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124; rev:2;)
```




Content sous le sens contient, le champ certainement le plus pertinent que vous aurez à définir . suivant ce que vous souhaitez faire remonte vous devrez choisir avec beaucoup de finesse ce champ

Pour l'exemple ici le champ NICK sera observé avec la pcre

OPTIONS

Ce champ prend en compte toute la subtilité est la profondeur de votre règle.

pcr



```
(msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcr:"/NICK .*USA.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124; rev:2;)
```



Perl compatible Regular Expression. permet de matcher précisément sur un champ. Pour des raisons évidentes en consommation de ressources il doit être utilisé avec content et sera systématiquement vérifié avant de rentrer dans la REGEX.

Pour l'exemple ici tout Nickname (irc) avec le champ USA sera matché

OPTIONS

Ce champ prend en compte toute la subtilité est la profondeur de votre règle.

référence



```
(msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124; rev:2;)
```



référence permet de donner une référence vers un lien connu comme une cve un lien VT un hash loC

OPTIONS

Ce champ prend en compte toute la subtilité est la profondeur de votre règle.



classtype



```
(msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:/"NICK .*USA.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124; rev:2;)
```



Classtype nous donne la catégorie d'alerte dans laquelle se situe cette alerte.

OPTIONS

Ce champ prend en compte toute la subtilité est la profondeur de votre règle.



sid



```
(msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124; rev:2;)
```



sid:serial identifier est une norme de nommage qui est à l'instar de l'organisme Mitre pour les CVE. Donc on ne peut pas mettre n'importe quoi . Pour les règles locales ce sera

1000000-1999999 Reserved for Local Use -- Put your custom rules in this range to avoid conflicts

The following are the reservations for SIDs in the 2000000 space allocated to this project:

vous avez toutes les allocations ici : <https://doc.emergingthreats.net/bin/view/Main/SidAllocation>

OPTIONS

Ce champ prend en compte toute la subtilité est la profondeur de votre règle.

rev



```
(msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124; rev:2;)
```



rev: Révision de votre règle - c'est à dire quelle est le numéro de mise à jour de votre règle

FABRIQUES TA RULES L'AMI



Des Questions ?

\0/ *\0/* *\0/*

