Open NRD: Newly Registered Domain Threat Intel Feeds

Al giorno d'oggi i domini sono utilizzati in quasi tutte le transazioni di comunicazione come query DNS e le transazioni HTTP e TLS (HTTP hostnames o TLS Server Name Indication)
Ogni giorno vengono registrati migliaia di nuovi domini, di cui una buona maggioranza viene usata per scopi illeciti come le frodi o gli attacchi informatici. Parte di questi domini sono monouso e vengono creati utilizzando *domain generation algorithms* (**DGA**). Essi vengono sfruttati per ospitare i file malevoli o come stazioni di **Command and Control** (C&C) dei sistemi compromessi. Per questi motivi vi è un bisogno di controllare costantemente la validità dei nuovi domini, soprattutto per identificare tempestivamente il loro utilizzo all'interno delle organizzazioni ed evitare che causino dei danni.

A tal fine Stamus Labs ha creato **Open NRD Feeds**: una raccolta di diversi tipi di feed contenenti domini appena registrati. Ogni giorno ad intervalli di un'ora vengono avviate delle routine per raccogliere, da diversi fornitori, domini appena registrati, e usando molteplici tecniche di elaborazione (i.e. machine learning, analisi di entropia, etc.) vengono estrapolati per creare i batch di **newly-registered domains**, relativi sia all'ultimo mese che alle ultime due settimane.

Ogni lista è organizzata in:

- **NRDs**: una lista completa dei nuovi domini registrati
- **NRDs ad altra entropia**: i domini che registrano una alta entropia (Sono inclusi i domini creati attraverso **DGA**)
- **Phishing NRDs**: domini che cercano di imitare i domini popolari (i.e. *login-office365[.] info*, *microsoftoffice-office365[.] com*)

Attualmente vi sono registrati circa 1,7 milioni di voci (dentro al dataset **NRD** Entropy da 30 giorni)

I batch **Open NRD Feeds** sono ottimizzati per essere usati al meglio con Suricata: un tool open source per l'analisi della rete e il rilevamento delle

minacce. Oltre ad offrire varie funzioni di TLS/HTTP/DNS Logging e analysis, Suricata è anche un Intrusion Detection/Prevention System che implementa un linguaggio di regole (signature/firme) completo per adattarsi alle minacce conosciute. Una sola istanza di Suricata permette di ispezionare traffico multi-gigabit utilizzando il supporto nativo dell'accelerazione hardware dei vari sistemi e sfruttando i framework e interfacce come **PF_RING** and **AF_PACKET**.

Suricata esegue il match contro **NRD feeds** durante l'elaborazione delle transazioni DNS, HTTP o TLS grazie alle regole definite da NRD Feeds.
Per esempio le regole definite sotto generano gli alert (e successivamente un record nei log file) per il traffico generato da una qualsiasi porta degli host della rete locale (*".. $HOME_NET any .."*) verso qualsiasi IP (esterno e non) e qualsiasi porta (*".. → any any .."*) per ogni match avvenuto contro il dataset (in questo caso *nrd-entropy-30day*) per le transazioni DNS, HTTP o TLS (sono definiti aggiuntive specifiche tra le parentesi per ogni regola) :

Signature for DNS Queries:

alert dns $HOME_NET any -> any any (msg:"SN NRD Entropy 30 day range domain"; flow:established,to_server; dns.query; dataset:isset,nrd-entropy-30day,type string,load nrd-entropy-30day,memcap 800mb,hashsize 3000000; classtype:unknown; flowbits:set, stamus.nrd.entropy; sid:3115010; rev:2; metadata:nrd_period 30_days, nrd_key dns.query.rrname, nrd_asset src_ip, stamus_classification nrd_entropy, provider Stamus, created_at 2022_04_29, updated_at 2023_08_16;)

Signature for HTTP Transactions:

alert http $HOME_NET any -> any any (msg:"SN NRD Entropy 30 day range HTTP server hosts"; flow:established,to_server; http.host; dataset:isset,nrd-entropy-30day,type string,load nrd-entropy-30day,memcap 800mb,hashsize 3000000; classtype:unknown; flowbits:set, stamus.nrd.entropy; sid:3115011; rev:2; metadata:nrd_period 30_days, nrd_key http.hostname, nrd_asset src_ip, stamus_classification nrd_entropy, provider Stamus, created_at 2022_04_29, updated_at 2023_08_16;)

Signature for TLS SNI Transactions:

alert tls $HOME_NET any -> any any (msg:"SN NRD Entropy 30 day range TLS SNI servers"; flow:established,to_server; tls.sni; dataset:isset,nrd-entropy-30day,type string,load nrd-entropy-30day,memcap 800mb,hashsize 3000000; classtype:unknown; flowbits:set, stamus.nrd.entropy; sid:3115012; rev:2; metadata:nrd_period 30_days, nrd_key tls.sni, nrd_asset src_ip, stamus_classification nrd_entropy, provider Stamus, created_at 2022_04_29, updated_at 2023_08_16;)

L'autore aggiunge inoltre che questi tipo di feed non devono essere utilizzati come **Indicators of Compromise** (Ovvero artefatti osservati su una rete o un sistema che verificano con un'alta probabilità un'intrusione) per attivare una risposta all'incidente. Essi hanno invece lo scopo di produrre dati aggiuntivi che possono essere utilizzati come indicatore di rischio in un processo di caccia alle minacce

Per poter avere accesso gratuito ai feed bisogna registrarsi e richiedere API Key andando su Newly-Registered Domain Lists from Stamus Labs. Dopo aver installato Suricata sul sistema e ottenuto la chiave d'accesso possiamo scaricare tutti i tipi di feed eseguendo un commando `wget` (o `curl`) specificando il **SECRETCODE** nella URL cosi:

```
wget https://ti.stamus-networks.io/SECRETCODEHERE/sti-domains-entropy-30.tar.gz
```

si estrae l'archivio nella cartella default delle regole di Suricata:

```
tar -zxf sti-domains-entropy-30.tar.gz -C /var/lib/suricata/rules/
```

Se vogliamo caricare la configurazione predefinita (viene scaricato anche **ET Open** ruleset) possiamo eseguire il commando:

```
sudo suricata-update
```

Con le regole installate riavviamo il servizio con:

```
sudo systemctl restart suricata
```

Finalmente possiamo avviare un istanza di test di Suricata specificando il set di regole con il flag `-S` in questo modo:

```
suricata -T -S /var/lib/suricata/rules/entropy30day.rules -i wlan0
```

oppure specificando il file nella configurazione specificata in `/etc/suricata/suricata.yaml`:

```
1872 default-rule-path: /etc/suricata/rules
1873
1874 rule-files:
1875   - suricata.rules
1876   - entropy30day.rules
```

Per vedere se Suricata sia in esecuzione e sta funzionando correttamente possiamo vedere i file di log con:

```
sudo tail /var/log/suricata/suricata.log
```

Infine, l'autore suggerisce di usare soltanto una taglia per ruleset (da 30 o 14 giorni) dato che quello da 14 giorni è un sottoinsieme dello stesso ruleset da 30 giorni.