

Partie 1

Requête 1

Explication de la pertinence du mot clé, pourquoi il a été choisi et pourquoi c’est sensible

- Recherche : title:"VNC viewer for Java" open

La recherche avec le mot clé "title:"VNC viewer for Java" open" a été choisie pour identifier les instances ouvertes et accessibles publiquement de visionneurs VNC écrits en Java. Cette requête est sensible car elle pourrait révéler des installations non sécurisées de visionneurs VNC, ce qui pourrait potentiellement exposer des systèmes à des risques de sécurité si des mesures appropriées n'ont pas été prises pour restreindre l'accès.

title:"VNC viewer for Java" open									
<div>View ReportDownload ResultsHistorical TrendView on Map</div>									
Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.									
<div>VNC Viewer for Java</div>									
<div>45.79.44.30</div>									
<div>45-79-44-30.ip.linodeusercontent.com</div>									
<div>Linode</div>									
<div>United States, Richardson</div>									
<div>cloudhoneypot</div>									
<div>HTTP/1.1 200 OK</div>									
<div>Composed-By: SPIP 4.1.11 @ www.spip.net</div>									
<div>Connection: keep-alive</div>									
<div>Content-Length: 100453</div>									
<div>Content-Type: text/html</div>									
<div>Last-Modified: Fri, 29 Jul 2022 16:53:01 GMT</div>									
<div>Loginip: 45.79.44.30</div>									
<div>Pragma: private</div>									
<div>Server: E2EE Server 2.0 httpd_four-faith Oracle XML DB/Oracle Database squid/3.5...</div>									
<div>VNC Viewer for Java</div>									
<div>172.232.252.139</div>									
<div>172-232-252-139.ip.linodeusercontent.com</div>									
<div>Akamai Technologies, Inc.</div>									
<div>United States, Cambridge</div>									
<div>cloudcdnhoneypot</div>									
<div>HTTP/1.1 200 OK</div>									
<div>Composed-By: SPIP 4.1.11 @ www.spip.net</div>									
<div>Connection: keep-alive</div>									
<div>Content-Length: 100174</div>									
<div>Content-Type: text/html</div>									
<div>Last-Modified: Fri, 29 Jul 2022 16:53:01 GMT</div>									
<div>Loginip: 172.232.252.139</div>									
<div>Pragma: private</div>									
<div>Server: TwistedWeb/18.4.0 Resin/4.0.58 Boa/0.93.15 kngx/1.10.2 WebSphere App1...</div>									
<div>VNC Viewer for Java</div>									
<div>172.233.79.211</div>									
<div>172-233-79-211.ip.linodeusercontent.com</div>									
<div>Akamai Technologies, Inc.</div>									
<div>United States, Cambridge</div>									
<div>cloudcdnhoneypot</div>									
<div>HTTP/1.1 200 OK</div>									
<div>Composed-By: SPIP 4.1.11 @ www.spip.net</div>									
<div>Connection: keep-alive</div>									
<div>Content-Length: 99569</div>									
<div>Content-Type: text/html</div>									
<div>Last-Modified: Fri, 29 Jul 2022 16:53:01 GMT</div>									
<div>Loginip: 172.233.79.211</div>									
<div>Mime-Version: 1.0</div>									
<div>Pragma: private</div>									
<div>Server: bfe/1.0.8.18 Switch lwIP/1.4.0 (http://savannah.nong...</div>									

Résultat de la recherche "title:"VNC viewer for Java" open".

Lien du truc le plus casser : <https://www.shodan.io/host/45.79.44.30>

Commentaire sur la capture

La capture révèle la présence de plusieurs **VNC Viewer for Java**. Étrangement Shodan détecte beaucoup de technologies différentes qui reviennent souvent:

- Java
- Ruby
- Php
- SonarQube
- AngularJS
- JQuery
- Ruby on Rails
- RoundCube Webmail

Surement autre chose de caché derrière tout ça. Ce qui rend la recherche assez floue mais la chose un peu plus critique.

Explication de pourquoi cette IoT ne devrait pas être là

Il est impératif de restreindre l'accès aux installations de VNC viewer, surtout s'ils sont accessibles publiquement. Des mesures de sécurité appropriées, telles que l'utilisation de mots de passe forts, la limitation des adresses IP autorisées, et l'application de mises à jour régulières, sont nécessaires pour éviter tout accès non autorisé. La présence d'instances ouvertes sans protection adéquate peut potentiellement compromettre la confidentialité et l'intégrité des systèmes.

Conclusion

La recherche a souligné la nécessité d'une gestion sécurisée des installations de VNC viewer en Java. Il est crucial pour les administrateurs de systèmes de mettre en œuvre des pratiques de sécurité robustes, de restreindre l'accès non autorisé, et de surveiller régulièrement ces installations pour garantir un environnement informatique sûr et protégé.

Requête 2

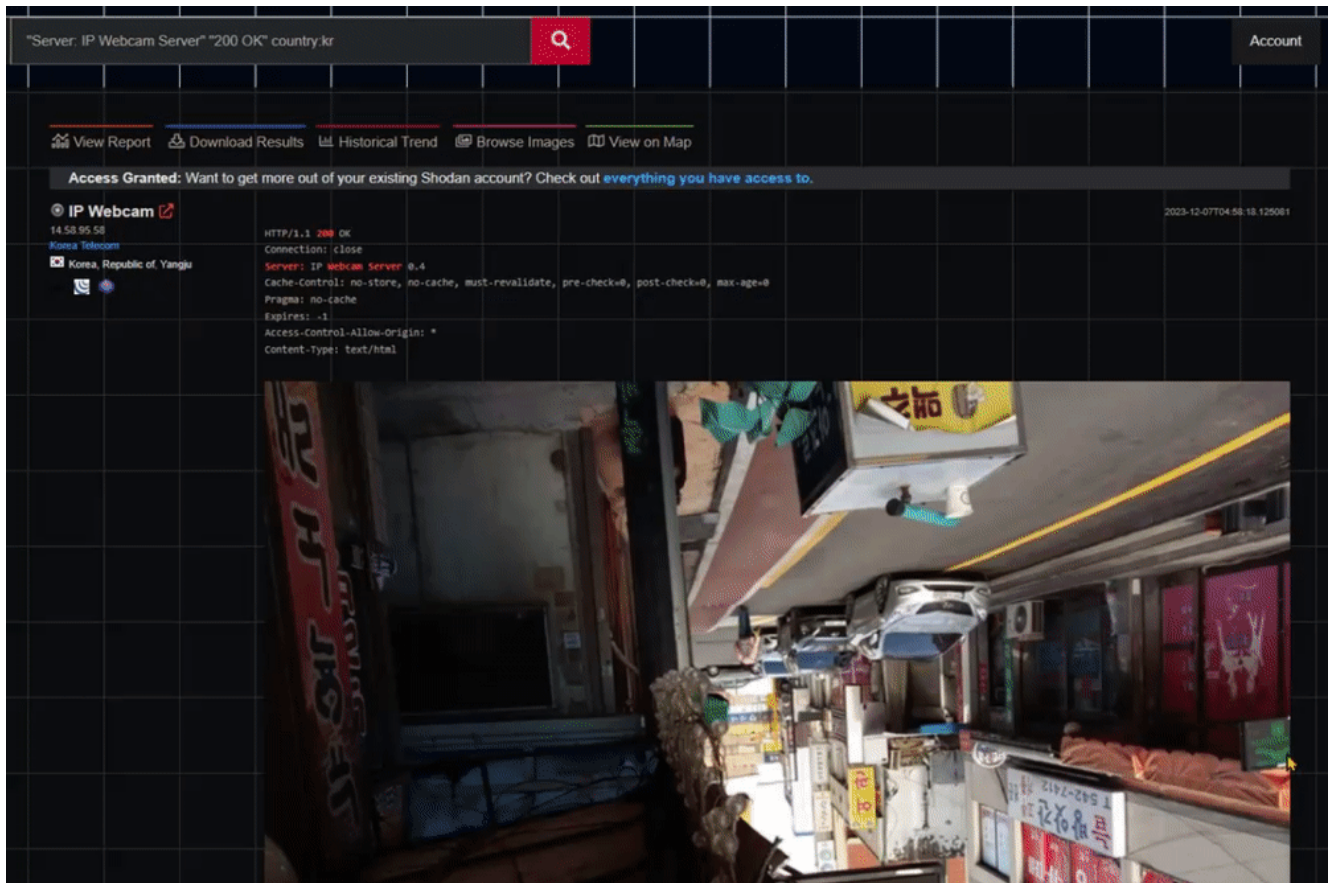
Explication de la pertinence du mot clé, pourquoi il a été choisi et pourquoi c'est sensible

- Recherche : Server: IP Webcam Server 200 OK country:kr

Le mot clé «Server: IP Webcam Server 200 OK country:kr» est pertinent, car il permet de repérer des caméras de surveillance connectées, dont la réponse du serveur est «200 OK». Cela signifie qu'il est possible de se connecter en temps réel à la caméra.

C'est assez sensible car une caméra de surveillance est censée être sécurisée et ne pas être accessible à tout le monde. Le but des caméras de surveillance est d'être utilisé par des personnes de confiance et non par

n'importe qui.



Résultat de la recherche "Server: IP Webcam Server 200 OK country:kr". Plusieurs caméras de surveillance sont visibles en KR

Commentaire sur la capture

La capture révèle la présence de caméras de surveillance en Corée du Sud. Il est possible d'accéder au direct des caméras en suivant le lien. Bien entendu, on ne va pas le faire 😊 On peut voir aussi que ce sont les mêmes marques de caméra qui sont utilisées (On retrouve les mêmes technologies détectées par Shodan).

Explication de pourquoi cette IoT ne devrait pas être là

Comme mentionné précédemment, une caméra de surveillance est censée être sécurisée et ne pas être accessible à tout le monde. Le but des caméras de surveillance est d'être utilisé par des personnes de confiance et non par n'importe qui. De plus, certaines caméras sont directement installées chez des particuliers. Être filmé à son insu est vraiment creepy.

Conclusion

Cette exploration des caméras de surveillance souligne le risque que représente leur accessibilité à tout un chacun. Il est impératif de prendre conscience de la nécessité de sécuriser ces dispositifs. L'achat et l'installation de caméras de surveillance doivent être effectués avec précaution, en veillant à protéger la vie privée des individus.


Requête 3

Explication de la pertinence du mot clé, pourquoi il a été choisi et pourquoi c'est sensible

- Recherche : `http.title:"router" server: nginx 200 OK`

Le mot clé «`http.title:"router" server: nginx`» est pertinent, car il permet de repérer des routeurs dont le serveur est nginx. Ce qui veut dire que le routeur est accessible via un navigateur web (page de connexion ou directement une page de configuration).

C'est assez tragique de voir des routeurs accessible comme ça. On pourrait modifier la configuration du routeur et donc modifier la configuration du réseau.

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.		
<div> <div>13,000</div> <div>TOP COUNTRIES</div>  </div>		
United States	4,281	<div> <div>Cisco RV345 VPN Router</div> <div>95.77.104.40</div> <div>UPC Romania Constanta FO</div> <div>Romania, Constanta</div> <div>self-signed</div> </div>
Brazil	795	<div> <div>SSL Certificate</div> <div>Issued By:</div> <div>- Common Name: 10:F9:20:91:B5:42</div> <div>- Organization: Cisco Systems, Inc.</div> <div>Issued To:</div> <div>- Common Name: 10:F9:20:91:B5:42</div> <div>- Organization: Cisco Systems, Inc.</div> <div>Supported SSL Versions: TLSv1.2</div> </div>
Canada	690	<div> <div>HTTP/1.1 200 OK</div> <div>Server: nginx</div> <div>Date: Thu, 07 Dec 2023 12:22:03 GMT</div> <div>Content-Type: text/html; charset=utf-8</div> <div>Content-Length: 18229</div> <div>Last-Modified: Sat, 02 Dec 2023 00:15:22 GMT</div> <div>Connection: keep-alive</div> <div>Keep-Alive: timeout=5</div> <div>ETag: "656a771a-4735"</div> <div>Cache-Control: no-store, no-cache, must-revalidat...</div> </div>
India	666	
China	426	
More...		
<div> <div>TOP PORTS</div> <div>443</div> <div>80</div> <div>8443</div> <div>10443</div> <div>4443</div> <div>More...</div> </div>		
443	7,778	<div> <div>Cisco RV340 VPN Router</div> <div>143.44.167.101</div> <div>143.44.167.101-rev.convergeict.co</div> <div>Converge ICT Network</div> <div>Philippines, Ormoc</div> <div>self-signed</div> </div>
80	756	<div> <div>SSL Certificate</div> <div>Issued By:</div> <div>- Common Name: BC:4A:56:01:E5:46</div> <div>- Organization: Cisco Systems, Inc.</div> <div>Issued To:</div> <div>- Common Name: BC:4A:56:01:E5:46</div> <div>- Organization: Cisco Systems, Inc.</div> <div>Supported SSL Versions: TLSv1.2</div> </div>
8443	404	<div> <div>HTTP/1.1 200 OK</div> <div>Server: nginx</div> <div>Date: Thu, 07 Dec 2023 12:21:35 GMT</div> <div>Content-Type: text/html; charset=utf-8</div> <div>Content-Length: 18229</div> <div>Last-Modified: Tue, 05 Dec 2023 22:45:43 GMT</div> <div>Connection: keep-alive</div> <div>Keep-Alive: timeout=5</div> <div>ETag: "656fa817-4735"</div> <div>Cache-Control: no-store, no-cache, must-revalidat...</div> </div>
10443	371	
4443	369	
More...		
<div> <div>TOP ORGANIZATIONS</div> <div>Linode</div> <div>Comcast Cable Communications, LLC</div> <div>Verizon Business</div> <div>Charter Communications Inc</div> <div>TELEFÔNICA BRASIL S.A</div> <div>More...</div> </div>		
Linode	646	
Comcast Cable Communications, LLC	514	<div> <div>Cisco RV340W VPN Router</div> <div>165.98.75.250</div> <div>host-250-75-98-165.ligobusiness.c</div> <div>om.ni</div> <div>CENTRO DE ADMINISTRACION NIC.NI</div> <div>Nicaragua, Managua</div> <div>self-signed</div> </div>
Verizon Business	450	<div> <div>SSL Certificate</div> <div>Issued By:</div> <div>- Common Name: 04:EB:40:35:93:42</div> <div>- Organization: Cisco Systems, Inc.</div> <div>Issued To:</div> <div>- Common Name: 04:EB:40:35:93:42</div> <div>- Organization: Cisco Systems, Inc.</div> <div>Supported SSL Versions: TLSv1.2</div> </div>
Charter Communications Inc	350	<div> <div>HTTP/1.1 200 OK</div> <div>Server: nginx</div> <div>Date: Thu, 07 Dec 2023 12:17:18 GMT</div> <div>Content-Type: text/html; charset=utf-8</div> <div>Content-Length: 18230</div> <div>Last-Modified: Thu, 07 Dec 2023 05:55:10 GMT</div> <div>Connection: keep-alive</div> <div>Keep-Alive: timeout=5</div> <div>ETag: "65715e3e-4736"</div> <div>Cache-Control: no-store, no-cache, must-revalidat...</div> </div>
TELEFÔNICA BRASIL S.A	248	
More...		
<div> <div>TOP PRODUCTS</div> <div>nginx</div> <div>lighttpd</div> <div>Allegro RomPager</div> </div>		
nginx	11,532	
lighttpd	26	
Allegro RomPager	1	

Résultat de la recherche "`http.title:"router" server: nginx 200 OK`". Plusieurs routeurs sont visibles dans divers pays.

Commentaire sur la capture

Comme prévu la plus part des routeurs trouver sont des routeurs Cisco. On peut voir que les routeurs sont accessible via un navigateur web. Et sont tous sur nginx.

Explication de pourquoi cette IoT ne devrait pas être là

Un routeur est un élément essentiel dans un réseau. Déjà cela augmente les risques de se faire attaquer. Les fabricants de routeurs font des mises à jour pour corriger les failles de sécurité. Mais si les utilisateurs ne font pas les mises à jour, les routeurs sont vulnérables.

Conclusion

Cette investigation sur les routeurs met en lumière la vulnérabilité potentielle des réseaux domestiques ou pro. Il est crucial que les utilisateurs comprennent l'importance des mises à jour de sécurité pour les routeurs, renforçant ainsi la protection de leurs réseaux contre les attaques. Acheter et installer des routeurs doit s'accompagner d'une vigilance constante en matière de sécurité.

Requête 4





Explication de la pertinence du mot clé, pourquoi il a été choisi et pourquoi c'est sensible

- Recherche : Server: gSOAP/2.8 200 OK

Comme la recherche de base gSOAP/2.8 donnée beaucoup de résultat avec des réponse 401 Unauthorized, j'ai décidé de rajouter 200 OK pour avoir des résultats plus pertinents. Car cela veut dire que la plus sont accessible sans mot de passe. De plus la version gSOAP.2.8 à un directory traversal vulnerability.

Lien : <https://www.exploit-db.com/exploits/47653>

Ce qui est sensible est que l'on peut trouver des versions de gSOAP qui sont encore vulnérable.

View Report		Download	Results	Historical Trend	View on Map
Access Granted: Want to get more out of your existing Shodan account? Check out everything you h					
 217.9.21.131  Telesat d.o.o.  Bosnia and Herzegovina, Lukavac		HTTP/1.1 200 OK Server: gSOAP/2.8 Content-Type: text/html Content-Length: 358 Connection: close			
46.121.188.137  46-121-188-137.static.012.net.il 012 Smile Communications LTD.  Israel, Haifa		HTTP/1.1 200 OK Server: gSOAP/2.8 Access-Control-Allow-Origin: * Content-Type: text/html Transfer-Encoding: chunked Connection: close			
 77.243.213.159  subscr-159.pool-213.microweb.hu GERANT Kereskedelmi es Szolgaltato Kft  Hungary, Vép		HTTP/1.1 200 OK Server: gSOAP/2.8 Content-Type: text/html Content-Length: 358 Connection: close			
shop  47.91.107.139 ALICLOUD-UAE  United Arab Emirates, Dubai  		HTTP/1.1 200 OK Accept-Ranges: bytes Connection: keep-alive Content-Disposition: Content-Disposition Content-Length: 17749 Content-Type: text/html Etag: 5facd2d0-264 Last-Modified: Thu, 12 Nov 2020 06:14:40 GMT Loginip: 47.91.107.139 Pragma: private Server: sw-cp-server CherryPy/3.2.5 n...			
 4G CPE Router  45.79.5.148 45-79-5-148.ip.linodeusercontent.com		 SSL Certificate Issued By:			
		HTTP/1.1 200 OK Composed-By: SPIP 4.1.11 @ www.spip.net			

Résultat de la recherche "Server: gSOAP/2.8 200 OK".

Commentaire sur la capture

On peut voir que le premier et troisième résultat sont des caméras de surveillance. Le deuxième résultat est assez flou. Par contre le 4ème résultat et le 5ème (qu'on voit pas trop) ne font pas du tout partie de ce qui est recherché. A cause de la recherche 200 OK cela inclus aussi des résultat qui utilise pas gSOAP.2.8.

Explication de pourquoi cette IoT ne devrait pas être là

Comme dit au dessus, la version gSOAP.2.8 à un directory traversal vulnerability. Ce qui veut dire que l'on peut accéder à des fichiers qui ne sont pas censé être accessible. On peut donc accéder à des fichiers sensibles.

Conclusion

Cette exploration des caméras et autres dispositifs utilisant gSOAP/2.8 souligne la persistance des vulnérabilités, même avec des versions plus anciennes. Il est crucial de rester informé sur les mises à jour de sécurité et d'éviter l'utilisation de versions obsolètes. La sécurité des dispositifs connectés dépend directement de la vigilance des utilisateurs dans le choix et la maintenance de leurs équipements.

Requête 5

Explication de la pertinence du mot clé, pourquoi il a été choisi et pourquoi c'est sensible

- Recherche : title:"Epson" "port:80" country:fr

Le but de cette recherche est de trouver des imprimantes Epson en France qui sont accessible via un navigateur web. C'est assez sensible car on peut modifier la configuration de l'imprimante. On peut aussi voir les documents qui ont été imprimé.

title:"Epson" "port:80" country:fr							
<div> View Report</div> <div> Download Results</div> <div> Historical Trend</div> <div> View on Map</div>							
Access Granted: Want to get more out of your existing Shodan account? Check out everything you h							
<div><div><div>EPSON AL-M200DN - 90.121.5.155 </div><div>90.121.5.155</div><div>Orange Business Services</div><div> France, Paris</div></div><div><div>HTTP/1.0 200 OK</div><div>Date: Tue Dec 4 11:45:05 2007</div><div>Server: HTTP server</div><div>Pragma: no-cache</div><div>Cache-Control: no-cache</div><div>Content-type: text/html</div></div></div>							
<div><div><div>EPSON TMNet WebConfig Ver.1.00 </div><div>217.128.14.113</div><div>laubervilliers-656-1-215-113.w217-128.abo.wanadoo.fr</div><div>LNPOT657 Puteaux</div><div> France, Paris</div></div><div><div>HTTP/1.1 200 OK</div><div>Content-Type: text/html</div><div>Cache-Control: private</div><div>Expires: Thu, 26 Oct 1995 00:00:00 GMT</div><div>Transfer-Encoding: chunked</div><div>Server: Allegro-Software-RomPager/4.01</div></div></div>							
<div><div><div>Epson Stylus SX510W </div><div>91.162.150.8</div><div>91-162-150-8.subs.proxad.net</div><div>SCALEWAY S.A.S.</div><div> France, Saint-Menoux</div></div><div><div>HTTP/1.1 200 OK</div><div>CONTENT-TYPE: text/html</div><div>CONTENT-LENGTH: 6846</div><div>SERVER: EPSON_Linux-UPnP/1.0-Epson-UPnP-SDK/1.0</div><div>CONNECTION: close</div></div></div>							
<div><div><div>Epson Stylus SX525WD </div><div>82.66.147.228</div><div>rob92-2_migr-82-66-147-228.fbx.proxad.net</div><div>Proxad / Free SAS</div><div> France, Paris</div></div><div><div>HTTP/1.1 200 OK</div><div>CONTENT-TYPE: text/html</div><div>CONTENT-LENGTH: 6856</div><div>SERVER: EPSON_Linux-UPnP/1.0-Epson-UPnP-SDK/1.0</div><div>CONNECTION: close</div></div></div>							

Résultat de la recherche "title:"Epson" "port:80" country:fr". Plusieurs imprimantes sont visibles en France.

Commentaire sur la capture

On peut voir seulement 4 imprimantes de la marque EPSON en France. Les 2 dernières ont CONNECTION : close, ce qui réduit bien le nombre d'imprimante EPSON accessible en France à 2.

Explication de pourquoi cette IoT ne devrait pas être là

Une imprimante est souvent connecter au réseau d'une maison ou d'une boîte et donc accessible par plusieurs personnes. Si une personne malveillante arrive à accéder à l'imprimante, elle peut modifier la configuration de l'imprimante ou même devenir domain admin.

Conclusion

L'accès non sécurisé à une imprimante pourrait permettre des intrusions malveillantes, compromettant ainsi la confidentialité et la sécurité des informations. Les utilisateurs d'imprimantes doivent prendre des mesures pour renforcer la sécurité de ces dispositifs, en modifiant les mots de passe par défaut et en restreignant l'accès aux seules personnes autorisées. La vigilance dans la gestion de la sécurité des périphériques connectés est essentielle pour éviter les compromissions indésirables.

Requête 6

Explication de la pertinence du mot clé, pourquoi il a été choisi et pourquoi c'est sensible

- Recherche : «bulb last-modified»

Le mot clé «bulb» est pertinent car il désigne une ampoule connectée. Sa sensibilité réside dans la possibilité de repérer des ampoules connectées vulnérables aux attaques, surtout lorsque les utilisateurs négligent de modifier les mots de passe par défaut.

Le mot clé «last-modified» est pertinent car il permet d'identifier des objets connectés ayant récemment subi des modifications.

Pricing [↗](#) "bulb" "last-modified" 🔍

[📊 View Report](#) [📄 Download Results](#) [📈 Historical Trend](#) [🗺 View on Map](#)

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to](#)

45.237.176.218 [↗](#)
RED SATELITAL
MOQUEHUA SRL
🇦🇷 Argentina, Chivilcoy

HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Type: text/html
Accept-Ranges: bytes
ETag: "4253441295"
Last-Modified: Wed, 13 Oct 2021 14:59:56 GMT
Expires: Wed, 06 Dec 2023 07:51:03 GMT
Cache-Control: max-age=604800
Cache-Control: public, must-revalidate, proxy-revalidate
X-Frame-Options...

194.53.178.38 [↗](#)
38-178-53-194.mairnet.net
MARLETTA SAT S.R.L.
🇮🇹 Italy, Frumenti

HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Type: text/html
Accept-Ranges: bytes
ETag: "3119670667"
Last-Modified: Tue, 28 Mar 2023 14:15:52 GMT
Expires: Wed, 06 Dec 2023 06:47:01 GMT
Cache-Control: max-age=604800
Cache-Control: public, must-revalidate, proxy-revalidate
X-Frame-Options...

78.31.195.163 [↗](#)
MicroGroup Europe AB
🇸🇪 Sweden, Ömsköldsvik

HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Type: text/html
Accept-Ranges: bytes
ETag: "3326567627"

Résultat de la recherche "bulb last-modified". Plusieurs ampoules connectées sont visibles dans divers pays.

Commentaire sur la capture

La capture révèle la présence d'ampoules connectées dans plusieurs pays. Il est possible d'accéder à la page de connexion en suivant le lien. Bien entendu, cela nécessite un mot de passe et un identifiant, mais de nombreux utilisateurs ne changent pas le mot de passe par défaut. Ainsi, il serait envisageable de prendre le contrôle de l'ampoule.

Explication de pourquoi cette IoT ne devrait pas être là

La possibilité de contrôler l'éclairage d'une maison à l'insu de ses occupants est une menace sérieuse. Elle pourrait entraîner la surchauffe de l'ampoule, voire sa destruction, et augmenter de manière significative la facture d'électricité. Payer une somme importante pour une simple ampoule serait regrettable.

Conclusion

En résumé, cette recherche met en évidence la vulnérabilité des ampoules connectées, exposant le risque potentiel de manipulation à distance. Il est crucial que les utilisateurs prennent conscience de cette menace, modifient les mots de passe par défaut et n'exposent pas en ligne des objets connectés sans protection, garantissant ainsi la sécurité de leur domicile.

Requête 7

Explication de la pertinence du mot clé, pourquoi il a été choisi et pourquoi c'est sensible

- Recherche : "title:voice assistant"

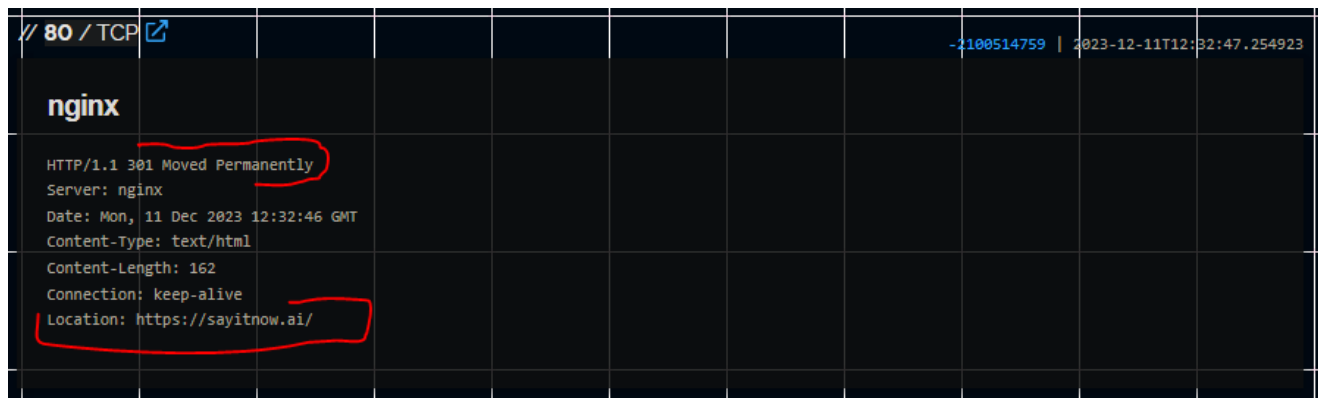
Le mot clé «voice assistant» est pertinent car il permet de repérer des assistants vocaux connectés, tels que Google Home ou Alexa. Et voulant ajouter plus de filtre la recherche devenait pas pertinente. On avait plus de résultat correspondant à ce que l'on voulait. La sensibilité réside dans la possibilité de repérer des assistants vocaux connectés vulnérables aux attaques, surtout lorsque les utilisateurs négligent de modifier les mots de passe par défaut.

"title:voice assistant"									
<div><div> View Report</div><div> Download Results</div><div> Historical Trend</div><div> View on Map</div></div>									
Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.									
Say It Now - Award Winning Voice Assistant Advertising with Alexa									
3.8.60.76		SSL Certificate		HTTP/1.1 200 OK					
sayitnow.ai		Issued By:		Server: nginx					
ec2-3-8-60-76.eu-west-2.compute.amazonaws.com		- Common Name:		Date: Mon, 11 Dec 2023 14:39:21 GMT					
Amazon Data Services UK		R3		Content-Type: text/html; charset=UTF-8					
United Kingdom, London		- Organization:		Transfer-Encoding: chunked					
		Let's Encrypt		Connection: keep-alive					
cloud		Issued To:		Vary: Accept-Encoding					
		- Common Name:		Link: <https://sayitnow.ai/wp-json/>; rel="https://api.w.org/"					
		sayitnow.ai		Link: <https://sayitnow.ai/wp-json/wp/v2/pages/20...					
		Supported SSL Versions:							
		TLSv1.2, TLSv1.3							
Voice assistant									
62.84.124.100		SSL Certificate		HTTP/1.1 200 OK					
vietnamobile.com.vn		Issued By:		Server: nginx/1.20.1					
Yandex.Cloud LLC		- Common Name:		Date: Mon, 11 Dec 2023 06:18:35 GMT					
Russian Federation, Dubna		GlobalSign RSA OV SSL CA 2018		Content-Type: text/html; charset=utf-8					
eo-product		- Organization:		Content-Length: 15464					
		GlobalSign nv-sa		Connection: keep-alive					
		Issued To:		Last-Modified: Fri, 21 Apr 2023 01:19:02 GMT					
		- Common Name:		Vary: Accept-Encoding					
		*.vietnamobile.com.vn		ETag: "6441e486-3c68"					
		- Organization:		Expires: Mon, 11 Dec 2023 06:18:34 GMT					
		VIETNAMOBILE		Ca...					
		TELECOMMUNICATIONS JOINT STOCK COMPANY							
		Supported SSL Versions:							
		TLSv1, TLSv1.1, TLSv1.2							
Rhasspy Voice Assistant - Open and Offline									
159.203.75.182		SSL Certificate		HTTP/1.1 200 OK					
community.rhasspy.org		Issued By:		Server: nginx					
DigitalOcean, LLC		- Common Name:		Date: Sun, 10 Dec 2023 16:47:21 GMT					
United States, Clifton		R3		Content-Type: text/html; charset=utf-8					
		- Organization:		Transfer-Encoding: chunked					

Résultat de la recherche "title:voice assistant". Plusieurs assistants vocaux connectés sont visibles dans divers pays.

Commentaire sur la capture

On peut voir des choses plutôt sympa ici Premier résultat : Say It Now - Award Winning Voice Assistant Advertising with Alexa Et une entreprise qui a compris le principe de Shodan et qui a mis en place une campagne de pub. C'est assez drôle. On est redirigé vers un site web de leur assistant vocal. <https://sayitnow.ai/>



```
// 80 / TCP [icon]
-2100514759 | 2023-12-11T12:32:47.254923

nginx

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Mon, 11 Dec 2023 12:32:46 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: https://sayitnow.ai/
```

Preuve de la redirection

Le 3ème résultat est aussi une redirection vers le site de l'assistant vocal. Mais il y a d'autre port HTTP qui sont ouvert et qui ne font pas de redirection. C'est difficile de savoir si c'est vraiment une campagne de pub ou si c'est un assistant vocal qui est mal configuré.

Par contre le deuxième résultat pas de doute possible. C'est un assistant vocal qui est mal configuré.

Explication de pourquoi cette IoT ne devrait pas être là

La présence d'assistants vocaux accessibles publiquement peut présenter des risques pour la vie privée des utilisateurs. Ces dispositifs sont souvent conçus pour interagir avec des données personnelles, et leur exposition pourrait potentiellement permettre des accès non autorisés à des informations sensibles. En conséquence, il est crucial de restreindre l'accès à ces dispositifs pour garantir la confidentialité des utilisateurs.

Conclusion












Cette recherche souligne la sensibilité de la présence d'assistants vocaux accessibles en ligne. Il est impératif de mettre en œuvre des mesures de sécurité robustes pour ces dispositifs, en restreignant l'accès et en appliquant des pratiques de sécurité adéquates. Les utilisateurs et les administrateurs doivent être conscients des risques potentiels liés à l'exposition des assistants vocaux et prendre les mesures nécessaires pour protéger la vie privée et la sécurité des données.

Requête 8

Explication de la pertinence du mot clé, pourquoi il a été choisi et pourquoi c'est sensible

- Recherche : Fridge

Le mot clé «Fridge» est pertinent car il permet de repérer des frigos connectés. La sensibilité réside dans la possibilité de repérer des frigos connectés vulnérables aux attaques, surtout lorsque les utilisateurs négligent de modifier les mots de passe par défaut.

fridge			
View Report Download Results Historical Trend Browse Images View on Map			
Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to			
 fridge&nbsp;-&nbsp;Synology&nbsp;DiskStation 			
114.23.229.14	HTTP/1.1 200 OK		
Voyager Internet Ltd	Server: nginx		
New Zealand, Auckland	Date: Tue, 12 Dec 2023 14:25:26 GMT		
  	Content-Type: text/html; charset="UTF-8"		
	Transfer-Encoding: chunked		
	Connection: keep-alive		
	Keep-Alive: timeout=20		
	Vary: Accept-Encoding		
	Cache-control: no-store		
	X-Content-Type-Options: nosniff		
	X-XSS-Protection: 1; mode=blo...		
 fridge&nbsp;-&nbsp;Synology&nbsp;DiskStation 			
114.23.229.14	 SSL Certificate		
remote.threelinestudio.co.nz	Issued By:		
Voyager Internet Ltd	- Common Name:		
New Zealand, Auckland	R3		
  	HTTP/1.1 200 OK		
	- Organization:		
	Let's Encrypt		
	Issued To:		
	- Common Name:		
	remote.threelinestudio.co.nz		
	Supported SSL Versions:		
	TLSv1.2		
	Server: nginx		
	Date: Tue, 12 Dec 2023 10:05:48 GMT		
	Content-Type: text/html; charset="UTF-8"		
	Transfer-Encoding: chunked		
	Connection: keep-alive		
	Keep-Alive: timeout=20		
	Cache-control: no-store		
	X-Content-Type-Options: nosniff		
	X-XSS-Protection: 1; mode=block		
	X-Frame-Options: SA...		
107.15.149.177			
107-015-149-177.res.spectrum.co	NetBIOS Response:		
m	Server Name: THE-FRIDGE		
Charter Communications Inc	MAC Address: D8:BB:C1:49:A4:C1		
United States, Raleigh	Names:		
	THE-FRIDGE <0x0>		
	WORKGROUP <0x0>		
	THE-FRIDGE <0x20>		
	WORKGROUP <0x1e>		
	WORKGROUP <0x1d>		

Résultat de la recherche "Fridge". Plusieurs frigos connectés sont visibles dans divers pays.

Commentaire sur la capture

Premier et deuxième résultat : On peut voir des frigo connecter avec un serveur web pour le monitoré. 2 frigos de New Zealand donc il doivent avoir le même frigo. Le 3ème résultat : Et un frigo d'après shodan mais aucun accès web disponible. Mais il reste visible à tout le monde il faudrait sûrement rechercher plus en profondeur pour trouver un accès mais on va pas le faire.

Explication de pourquoi cette IoT ne devrait pas être là

La présence de frigos connectés accessibles publiquement peut présenter des risques. Si jamais j'ai le contrôle du frigo je peux modifier la température du frigo et donc faire pourrir la nourriture/tuer les gens qui mange la

nourriture. Fin bref pas une bonne idée

Conclusion

Cette recherche souligne la sensibilité de la présence de frigos connectés accessibles en ligne. Il est impératif de mettre en œuvre des mesures de sécurité robustes pour ces dispositifs, en restreignant l'accès et en appliquant des pratiques de sécurité adéquates. Les utilisateurs et les administrateurs doivent être conscients des risques potentiels liés à l'exposition des frigos connectés et prendre les mesures nécessaires pour protéger la vie privée et la sécurité des données.

Requête 9

Explication de la pertinence du mot clé, pourquoi il a été choisi et pourquoi c'est sensible

- Recherche : Raspbian

Le mot clé «Raspbian» est pertinent car il permet de repérer des Raspberry Pi connectés. La sensibilité réside dans ce que les personnes mettent sur leur Raspberry Pi. On peut trouver des choses assez sensible.

[illegible]

Résultat de la recherche "Raspbian". Plusieurs Raspberry Pi connectés sont visibles dans divers pays.

Commentaire sur la capture

On peut voir que beaucoup d'appareils disposent d'un SSH. On peut supposer que ces appareils permettent de faire des rebonds sur d'autres équipements non connectés à Internet. On peut aussi voir un Raspberry avec un serveur web.

Explication de pourquoi cette IoT ne devrait pas être là

Il ne doit pas être sur internet, à part si maîtriser, car il dispose d'une grande puissance de calcul et généralement les raspberry sont utilisés pour des montages de machines ou autre.

Conclusion

Ne pas exposer son raspberry sur Internet si pas nécessaire. Préféré une connexion VPN.

Partie 2 : Automatisation de la Recherche avec un Script Python

TODO : Développez un Script Python pour automatiser la Recherche :

- Utilisez la librairie Shodan pour créer un script qui automatise les recherches de mots-clés.
- Le script doit pouvoir saisir des mots-clés, exécuter la recherche et enregistrer les résultats dans un fichier.
- Utilisez une lib python de visualisation statistique, comme matplotlib ou seaborn, pour créer des graphiques représentant les données recueillies. (les marques, les ports ouverts, et toutes les infos importantes) Bonne chance ! Merci !!

Lien du git: <https://github.com/YuToutCourt/Shodan-stats/tree/main/app>