

Pirater les objets connectés devient simple comme un jeu d'enfant

<pre>hor : Vector/NullArray tter: @Real_Vector e : Mass Exploiter sion: 1.0.0 ##### ----- AutoSploit General Usage and Information ----- The name suggest AutoSploit attempts to automate the exploitation of remote hosts. Targets are collected by employing the Shodan.io API. The 'Gather Hosts' option will open a dialog from which you can define platform specific search queries such as 'Apache' or 'IIS'. By doing so a list of candidates will be retrieved and saved to a file named hosts.txt in the current working directory. Once this operation has been completed the 'Exploit' option will take you out the business of attempting to exploit these targets by running a range of Metasploit modules against them. The 'Local' option will facilitate the execution of a command on the local machine, local host and local port for MSF facilitated</pre>	<p>Pirater les objets connectés devient simple comme un jeu d'enfant</p>
---	--

Avec le logiciel AutoSploit, quelques mots-clés suffisent pour pirater en masse des systèmes accessibles par Internet. Le logiciel provoque une vive polémique parmi les chercheurs en sécurité.

Mauvaise nouvelle pour les utilisateurs d'objets connectés. Un hacker dénommé « VectorSEC » vient de créer un outil diabolique qui permet de pirater en masse ces appareils, et de façon totalement automatique. Baptisé « AutoSploit », ce logiciel combine en effet deux outils bien connus des chercheurs en sécurité : Shodan.io, un moteur de recherche qui permet de détecter des objets connectés vulnérables ; et Metasploit, une plateforme de piratage modulaire utilisée notamment pour faire des audits de sécurité.

L'utilisation d'AutoSploit est ultrasimple. Il suffit d'indiquer un mot-clé qui fasse référence à un système particulier (« IIS », « Apache », « Western Digital », etc.). Le logiciel va alors récupérer auprès de Shodan.io une liste d'appareils accessibles, puis sélectionner dans les modules de Metasploit une série d'attaques permettant d'obtenir un accès direct au système. Emballé c'est pesé...[lire la suite]

LE NET EXPERT

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - FORMATIONS / SENSIBILISATION :
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

Réagissez à cet article

Source : *Pirater les objets connectés devient simple comme un jeu d'enfant*