

# TOP 10 des méthodes de hacking les plus utilisées | Le Net Expert Informatique

 <p><b>Le Net Expert</b> <b>INFORMATIQUE</b> Protection des données personnelles Sécurité Informatique - Cybercriminalité</p>  <p><b>vous informe...</b></p>	<h2>TOP 10 des méthodes de hacking les plus utilisées</h2>
--	--

**BalaBit présente en exclusivité lors de la 15<sup>e</sup> édition des Assises de la Sécurité, les résultats d'une étude menée auprès des participants de la Black Hat en août dernier, conférence de référence mondiale en matière de sécurité de l'information.**

BalaBit a interrogé 349 professionnels de la sécurité afin de définir le top 10 des méthodes de hacking actuellement les plus populaires. Cette étude offre aux entreprises l'opportunité de mieux connaître leurs ennemis en identifiant les méthodes et les vulnérabilités les plus utilisées par les hackers lorsqu'il s'agit de s'attaquer à leurs données sensibles. Cette base de connaissance est la première étape fondamentale pour toute entreprise souhaitant mettre en place une stratégie de sécurité IT efficace, et cela quelque soit son secteur d'activité.

#### **Attaquant interne ou externe ? Pas si évident...**

Les menaces sont différentes et plus sophistiquées aujourd'hui et la frontière entre les menaces internes et externes est devenue très étroite. La majorité des attaquants externes tentent de pénétrer le réseau, d'acquérir des niveaux d'accès basiques et d'utiliser leurs droits pour petit à petit remonter jusqu'à des niveaux d'accès privilégiés. Dans la plupart des cas, ils restent invisibles dans le réseau pendant plusieurs mois, puisqu'ils parviennent à s'identifier comme des utilisateurs internes.

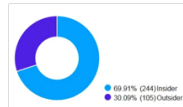
Qu'en est-il des utilisateurs internes malveillants ? : Sont-ils conscients des conséquences de leurs actes lorsqu'ils partagent leurs identifiants ou lorsqu'ils cliquent sur des liens de phishing – dans ce cas, la fuite de données est-elle le résultat d'actions intentionnelles ou accidentelles ? Doivent-ils être considérés comme malveillants seulement si leur action était intentionnelle ? Cela a-t-il vraiment beaucoup d'importance si la fuite de données est très grave ?

70% des personnes interrogées considèrent les menaces internes comme les plus risquées

54% des personnes interrogées déclarent avoir très peur des hackers qui pénètrent au sein du réseau de l'entreprise via leur pare-feu, alors même que 40% d'entre elles déclarent qu'un pare-feu n'est pas assez efficace pour empêcher les hackers d'entrer.

Les participants ont également été interrogés sur les attaquants – internes ou externes – qu'ils considèrent les plus à risques :

> Les résultats soulignent un point important en vue de la définition d'une stratégie de défense efficace : 70% des personnes interrogées considèrent que les utilisateurs internes présentent le plus de risques (et seulement 30% estiment que les attaquants externes posent plus de risques).



**Une chose est sûre : les attaquants externes cherchent à devenir des utilisateurs internes, et les utilisateurs internes les aident pour y parvenir – accidentellement ou intentionnellement.**

Quelque soit la source de l'attaque, la liste des 10 méthodes de hacking les plus populaires -présentées ci-dessous – démontre qu'il est crucial pour les entreprises de savoir ce qu'il se passe sur leur réseau en temps réel. Qui accède à quoi ; est-ce le bon utilisateur derrière l'identifiant et le mot de passe ou est-ce un attaquant externe utilisant un compte compromis ?

#### **Le top 10 des méthodes de hacking les plus utilisées :**

1. Ingénierie sociale (ex : phishing).
2. Compromission de comptes (sur la base de mots de passe faibles par exemple).
3. Attaques web (ex : injection SQL/de commandes).
4. Attaques de clients de l'entreprise ciblée (ex: contre des destinataires de documents, navigateurs web).
5. Exploits avec des mises à jour de serveurs connus (ex: OpenSSL, Heartbleed).
6. Terminaux personnels non sécurisés (manque de politique de sécurité BYOD).
7. Intrusion physique.
8. Shadow IT (utilisation personnelle de services Cloud à des fins professionnelles).
9. Attaque d'une infrastructure outsourcée en ciblant un fournisseur de services externe.
10. Attaque de données hébergées sur le Cloud (via l'IaaS, le PaaS).

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !  
Un avis ? Laissez-nous un commentaire !

Source : <http://www.programmez.com/actualites/balabit-presente-un-top-10-des-methodes-de-hacking-les-plus-utilisees-23280>