https://www.dane.ac-versailles.fr/spip.php?article625

ACADÉMIE
DE VERSAILLES
Liberté
Égalité
Fraternité

Sécurité numérique : l'affaire de tous !

Les techniques d'attaques les plus répandues

- Mes enjeux - Sécurité numérique -

Date de mise en ligne : lundi 2 octobre 2023

Copyright © Délégation Académique au Numérique Éducatif - Tous droits réservés

Les médias relatent souvent des attaques d'entreprises ou d'organisations par des pirates informatiques sans expliquer les techniques employées par ces derniers.
Dans cet article, dans une perspective d'acculturation cyber, nous présentons les techniques d'attaques les plus répandues.
L'attaque DDoS ou l'injection SQL n'auront bientôt plus de secret pour vous !

L'attaque DDoS : quand la toile devient tempête

L’attaque "DDoS" [1] a pour objectif de saturer de requêtes un site afin qu’il ne soit plus en mesure d’y répondre.

En février 2018, l’une des plus grandes attaques DDoS jamais enregistrées a visé GitHub, un célèbre service de gestion de code en ligne utilisé par des millions de développeurs. Cette attaque a atteint 1,3 Tb/s et a envoyé des paquets de données au rythme de 126,9 millions par seconde rendant la plateforme GitHub inaccessible pour ses utilisateurs pendant une vingtaine de minutes avant que les contre-mesures se montrent efficaces !

Avec l’augmentation exponentielle des échanges commerciaux sur le web, le nombre de chantage au déni de service connaît une forte croissance. Elle consiste pour un pirate à lancer une attaque DDoS contre une entreprise ou un site commercial et de demander une rançon pour la faire cesser. **Une interruption de service, même de quelques minutes, peut engendrer de lourdes pertes financières pour les entreprises ou les sites ciblés.**

[https://www.dane.ac-versailles.fr/local/cache-vignettes/L400xH201/ddos-de3c0-f2230.png]

Schéma d'une attaque DDOS - CNPP
Voir la transcription

Visuel du schéma d'une attaque DDOS. Visuel extrait de l'article de Damien LEROY (Consultant en sécurité des systèmes d'information chez CNPP)

Pour se défendre, les organisations doivent mettre en place des solutions de protection telles que :

- les pare-feux
- les systèmes de détection d'anomalies
- les services de mitigation DDoS.

Cependant, **les utilisateurs peuvent également jouer un rôle en évitant de participer involontairement à ces attaques**. Les ordinateurs et les dispositifs connectés non sécurisés, tels que les caméras de surveillance, peuvent être compromis pour former des botnets [2] alimentant les attaques DDoS.

Garder ses logiciels à jour et sécuriser les objets connectés contribue à limiter ces risques.

Copyright © Délégation Académique au Numérique Éducatif

L'injection SQL : quand une base de données est compromise

L'injection "SQL" [3] consiste à exploiter des failles de sécurité existantes sur une application échangeant des informations avec une base de données. Un cas typique est celui d'un site web comportant un formulaire en ligne mal protégé permettant l'exécution de requêtes SQL malicieuses permettant d'ajouter, modifier ou supprimer des données stockées dans la base de données relationnelle.

De cette manière, **un attaquant peut contourner les contrôles de sécurité et visualiser ou modifier des éléments existants dans la base de données, tels que des mots de passe ou des coordonnées bancaires.** Par conséquent, l'injection SQL **permet d'accéder à toutes les données personnelles** (telles que les identifiants et coordonnées des utilisateurs ou des employés) **ou non personnelles** (articles qui existent, leurs prix, etc.) contenues dans la base de données SQL.

Les développeurs peuvent contrer ce type de menace en utilisant des paramètres préparés et en appliquant une validation stricte des entrées utilisateur. Quant aux utilisateurs, ils doivent être conscients des risques et éviter de partager des informations sensibles sur des sites potentiellement vulnérables.

XSS - Cross-Site Scripting : quand les sites web deviennent des vecteurs d'attaque

Le "Cross-Site Scripting" (XSS) [4] est l'**une des menaces les plus courantes sur Internet aujourd'hui**.
Il s'agit d'une faille de sécurité qui permet aux attaquants d'injecter du code malveillant dans les sites Web, ce qui expose les utilisateurs à de grands risques.

Les cybercriminels exploitent souvent cette vulnérabilité pour voler des informations sensibles telles que les identifiants, les données financières et personnelles.

Le fonctionnement de XSS est relativement simple. Un attaquant insère un code malveillant, généralement sous la forme d'un script, dans les champs de saisie d'un site Web, tels que des commentaires, un formulaire de recherche ou un forum. Lorsque d'autres utilisateurs visitent ces pages, un code malveillant s'exécute dans leur navigateur, permettant aux attaquants de voler des informations ou de compromettre leur expérience en ligne.

[https://www.dane.ac-versailles.fr/local/cache-vignettes/L400xH255/simple_schema_xss_attack-9f1bd-bd2cf.png]

Schéma d'une attaque XSS - Wikipédia
Voir la transcription

Visuel de l'attaque XXS

Afin de se protéger contre le XSS, il est crucial pour **les développeurs** de sites web de **mettre en œuvre des pratiques de codage sécurisé**, telles que l'échappement des données d'entrée, la validation côté serveur et l'utilisation de bibliothèques de sécurité. **Les utilisateurs** peuvent également contribuer à leur propre sécurité **en évitant de cliquer sur des liens suspects et en maintenant leurs navigateurs et plugins à jour.**

Copyright © Délégation Académique au Numérique Éducatif

Le sidejacking : quand vos sessions en ligne sont compromises

Le **"sidejacking"** [5], également connu sous le nom de détournement de session, est une menace sérieuse pour la sécurité en ligne. Cette technique malveillante permet aux attaquants de prendre le contrôle des sessions des utilisateurs légitimes sur les sites Web, leur donnant accès à des informations confidentielles et à des comptes privés.

Les conséquences peuvent être dévastatrices, allant de la fuite de données personnelles au vol d'informations d'identification.

Le fonctionnement du sidejacking repose sur l'interception des cookies de session. Lorsqu'un utilisateur se connecte à un site Web, un cookie de session est généré pour maintenir son authentification. Les attaquants utilisent des méthodes telles que la détection de réseaux dangereux ou l'exploitation des vulnérabilités des sites Web pour voler ces cookies, ce qui leur permet d'usurper l'identité d'utilisateurs légitimes.

[https://www.dane.ac-versailles.fr/local/cache-vignettes/L400xH220/sidejacking-2af36-8b84e.png]

Schéma du Sidejacking
Voir la transcription

Visuel du Sidejacking

Pour se protéger contre ce type d'attaque, **les utilisateurs doivent privilégier les sites qui utilisent le protocole HTTPS** qui crypte les communications entre les utilisateurs et les sites Web. De plus, **éviter les réseaux Wi-Fi publics non sécurisés** et **se déconnecter correctement des sessions après utilisation** contribue à réduire le risque.
Les développeurs de sites Web doivent mettre en œuvre des mécanismes de sécurité tels que l'utilisation de jetons anti-CSRF (Cross-Site Request Forgery [6]) ainsi que la rotation régulière des cookies de session.

Le buffer overflow : quand les failles de mémoire deviennent une menace

Le débordement de mémoire tampon est une faille de sécurité qui se produit lorsque les données dépassent la capacité du tampon nécessaire à leur stockage temporaire. Les attaquants exploitent cette vulnérabilité en insérant intentionnellement trop de données dans le cache, ce qui peut entraîner l'exécution de code malveillant ou un comportement de programme inattendu.

Ces attaques peuvent avoir de graves conséquences, allant de l'exécution de programmes malveillants à la prise de contrôle du système cible.

Pour se protéger, les développeurs doivent implémenter des méthodes de chiffrement sécurisées, telles que la validation des entrées utilisateur et la gestion correcte de la mise en cache. Des mises à jour régulières du logiciel peuvent également réduire le risque.
Côté utilisateur, il est essentiel de maintenir à jour les systèmes d'exploitation et les applications pour

Copyright © Délégation Académique au Numérique Éducatif

bénéficier des correctifs de sécurité. Éviter de télécharger des fichiers ou de cliquer sur des liens suspects peut également aider à prévenir les attaques par débordement de mémoire tampon.

Le cryptojacking : quand votre ordinateur mine à l'insu de votre plein gré

Le cryptojacking, une menace émergente, impliquant l'utilisation secrète de la puissance de calcul des ordinateurs d'autres personnes pour extraire des crypto-monnaies. **Les attaquants exploitent souvent des sites Web compromis ou des logiciels malveillants pour injecter des scripts de minage** dans les navigateurs des utilisateurs sans leur consentement.

Les conséquences du cryptojacking peuvent être une **réduction des performances de l'ordinateur, une surchauffe et une consommation d'énergie accrue**.

Pour se protéger, les utilisateurs peuvent :

- installer un bloqueur de script
- mettre à jour leur navigateur
- prêter attention aux performances inhabituelles de l'ordinateur peut aider à détecter les activités illégales de minage de crypto-monnaies.

Du côté des entreprises, la sécurisation des sites Web et des applications est primordiale pour empêcher l'injection de scripts malveillants. **Les solutions de pare-feu et de sécurité réseau peuvent également aider à identifier et à bloquer le trafic d'exploitation indésirable.**

Le sniffing : quand la surveillance d'un réseau devient une menace pour la confidentialité

Le "sniffing", ou écoute clandestine du réseau, est une **technique utilisée pour intercepter et collecter des données qui sont échangées entre des appareils sur un réseau non sécurisé.**
Les attaquants exploitent cette vulnérabilité en collectant des informations sensibles telles que les identifiants de connexion, les données financières et les informations personnelles.

Les conséquences du sniffing sont **alarmantes**, car elles peuvent envahir la vie privée des utilisateurs et entraîner des failles de sécurité.

Pour se protéger, les utilisateurs doivent donner la priorité aux connexions sécurisées utilisant le protocole HTTPS, éviter les réseaux Wi-Fi publics non protégés et envisager d'**utiliser un VPN pour chiffrer leur trafic réseau.**

Du côté des entreprises, l'utilisation du cryptage pour les communications et la mise en œuvre de protocoles de sécurité, tels que WPA3 pour les réseaux Wi-Fi, sont essentielles pour empêcher le "sniffing". Les administrateurs réseau peuvent également surveiller activement le trafic à la recherche de signes d'activité

Copyright © Délégation Académique au Numérique Éducatif

suspecte.

L'ARP poisoning : quand la confiance au sein d'un réseau devient un piège

L'ARP poisoning (empoisonnement ARP), également connu sous le nom d'ARP spoofing (usurpation d'identité ARP), est une **technique utilisée par les attaquants pour manipuler les tables ARP à l'intérieur d'un réseau**, ce qui peut conduire à une interception et à des attaques de type "man-in-the-middle". En usurpant la correspondance entre les adresses IP et les adresses MAC, les pirates peuvent rediriger le trafic réseau vers leurs propres systèmes.

https://www.dane.ac-versailles.fr/local/cache-vignettes/L400xH171/capture_d_e_cran_2023-08-28_a_13.45_12-3e9ec-21b48.png

Schéma du ARP Poisening
Voir la transcription

Visuel du Schéma du ARP Poisening

Les conséquences de l'empoisonnement ARP sont graves, car les attaquants peuvent espionner le trafic, obtenir des données sensibles et même injecter du contenu malveillant dans les communications.

Pour se protéger, les utilisateurs et les administrateurs réseau doivent **surveiller de près les activités réseau anormales et mettre en œuvre des mesures de sécurité telles que la détection ARP anormale.**

Du côté de l'entreprise, la segmentation du réseau, à l'aide de mécanismes de protection tels que la commutation de réseau sécurisée et des protocoles d'authentification forts, tels que IEEE 802.1X, **est essentielle pour prévenir l'empoisonnement ARP.**

Les ransomwares : quand les cybercriminels prennent les données en otage

Les ransomwares sont devenus une menace informatique majeure, mettant en péril la sécurité des données personnelles et professionnelles.
Ces malwares **cryptent les fichiers de la victime et demande ensuite le paiement d'une rançon en échange de la clé de décryptage**.

Les conséquences des attaques de ransomwares sont dévastatrices, entraînant la perte de données critiques, des perturbations opérationnelles et des coûts financiers élevés.

Pour se protéger, les utilisateurs et les entreprises doivent adopter une approche de sécurité à plusieurs niveaux qui comprend des mesures telles que :

- des sauvegardes régulières

Copyright © Délégation Académique au Numérique Éducatif

- des solutions de sécurité de qualité
- une sensibilisation continue aux menaces.

La prévention est la **meilleure défense** contre les ransomwares :

- éviter de cliquer sur des liens ou des pièces jointes suspects
- maintenir les logiciels et les systèmes à jour
- éduquer les employés sur les bonnes pratiques de sécurité

... sont tous nécessaires pour réduire les risques !

Pour aller plus loin

Avec Cybermalveillance.gouv.fr (ACYMA), le Ministère lance une série de quatre podcasts accompagnant le parcours M@gistère « SensCyber - Agir pour contribuer à la sécurité numérique et à celle de mon organisation ».

---

[1] Distributed Dental of Service ou « déni de service »

[2] Un botnet est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches.

[3] Structured Query Langage - SQL est un langage informatique normalisé servant à exploiter des bases de données relationnelles. La partie langage de manipulation des données de SQL permet de rechercher, d'ajouter, de modifier ou de supprimer des données dans les bases de données relationnelles.

[4] Le cross-site scripting est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, provoquant ainsi des actions sur les navigateurs web visitant la page.

[5] En informatique, le détournement de session, parfois également appelé détournement de cookies, est l'exploitation d'une session informatique valide, parfois également appelée clé de session, pour obtenir un accès non autorisé à des informations ou à des services dans un système informatique.

[6] En sécurité des systèmes d'information, le cross-site request forgery, abrégé CSRF ou XSRF, est un type de vulnérabilité des services d'authentification web.

Copyright © Délégation Académique au Numérique Éducatif