Qu'est-ce qu'un malware sans clic et comment fonctionnent les attaques zéro-clic ?

Pr Chérif DIALLO, CISSP
Professeur Titulaire des Universités
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept. Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

" Ce qui est caché derrière un sourire est souvent l'invisible tristesse d'un être." Anonyme.

Résumé : Face à la recrudescence des actes cybercriminels, ce bulletin mensuel de sécurité, qui est une communication de vulgarisation et de sensibilisation, présente aujourd'hui un problème crucial de cybersécurité. Il s'agit des attaques zéro clic et des zéro-clic malwares. Ces dernières années, les attaques sans clic ont parfois fait leur apparition sous le feu des projecteurs. Comme leur nom l'indique, les attaques sans clic ne nécessitent aucune action de la part de la victime, ce qui signifie que même les utilisateurs les plus avancés peuvent devenir la proie de cyberpiratages et d'outils de logiciels espions sérieux. Après une brève définition, ce bulletin, donne quelques exemples d'attaques sans clic, leur mode de fonctionnement et les solutions face à ce fléau.

Mots clés : Malware, attaque zéro-clic, logiciel malveillant, logiciel espion.

---

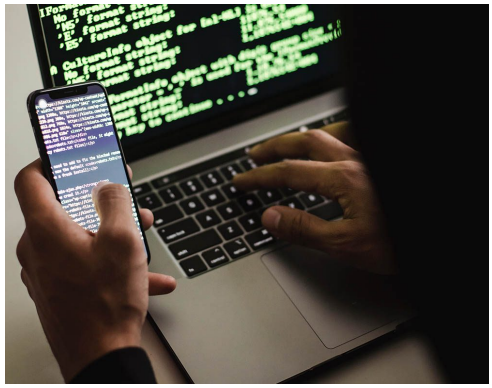
1. Définition

Traditionnellement, les logiciels d'espionnage consistent à convaincre la personne ciblée de cliquer sur un lien ou un fichier compromis pour s'installer sur son téléphone, sa tablette ou son ordinateur. Cependant, avec une attaque sans clic, le logiciel peut être installé sur un appareil sans que la victime ne clique sur un lien. En conséquence, les logiciels malveillants sans clic (zéro-clic malware or no-click malware) sont beaucoup plus dangereux.

Les attaques sans clic sont généralement très ciblées et utilisent des tactiques sophistiquées. Elles peuvent avoir des conséquences dévastatrices sans même que la victime sache que quelque chose ne va pas en arrière-plan. Les termes « attaques sans clic » et « exploits sans clic » sont souvent utilisés de manière interchangeable. Elles sont parfois également appelées attaques sans interaction ou entièrement à distance.

L'interaction réduite impliquée dans les attaques sans clic signifie moins de traces d'activités malveillantes. Ceci, ajouté au fait que les vulnérabilités que les cybercriminels peuvent exploiter pour des attaques sans clic sont assez rares, les rend particulièrement prisées par les attaquants.

Même les attaques de base sans clic laissent peu de traces, ce qui signifie que leur détection est extrêmement difficile. De plus, les mêmes fonctionnalités qui rendent les logiciels plus sécurisés peuvent souvent rendre les attaques sans clic plus difficiles à détecter. Les attaques sans clic existent depuis des années et le problème s'est encore répandu avec l'utilisation croissante des smartphones qui stockent une multitude de données personnelles. Alors que les individus et les organisations dépendent de plus en plus des appareils mobiles, la nécessité de rester informé des vulnérabilités zéro-clic n'a jamais été aussi grande.



2. Quelques exemples d'attaques zéro-clic

Une vulnérabilité sans clic peut affecter divers appareils. Voici des exemples très médiatisés d'exploits sans clic :

- ***BLASTPASS :*** En septembre 2023, une enquête a été publiée indiquant l'infection d'appareils iPhone iOS (16.6) par le logiciel espion Pegasus. Le rapport fait référence à la chaîne d'exploitation sous le nom de BLASTPASS. Il s'agit de loin du dernier exploit connu sans clic. Ce type d'exploit ne nécessite aucune action de la part de l'utilisateur. L'incident de septembre 2023 n'était pas le seul concernant les utilisateurs de produits Apple. En 2021, un autre cas de propagation de malware sans clic a été signalé. Plus tôt, en 2016, certains utilisateurs d'Apple avaient été ciblés par un outil appelé Karma, qui était également de nature zéro clic. En 2019, environ 1 400 utilisateurs de WhatsApp Messenger ont été ciblés par un exploit sans clic qui a infecté leurs appareils avec le logiciel espion Pegasus.
- ***Apple zéro-clic, saisie forcée, 2021 :*** En 2021, un militant bahreïnien des droits humains a vu son iPhone piraté par de puissants logiciels espions vendus à des États-nations. Le piratage, découvert par les chercheurs du Citizen Lab, avait mis en échec les protections de sécurité mises en place par Apple pour résister aux compromissions secrètes. Citizen Lab est un organisme de surveillance d'Internet basé à l'Université de Toronto. Ils ont analysé l'iPhone 12 Pro du militant et ont découvert qu'il avait été piraté via une attaque sans clic. L'attaque sans clic a profité d'une vulnérabilité de sécurité jusqu'alors inconnue dans iMessage d'Apple, qui a été exploitée pour pousser le logiciel espion Pegasus, développé par la société israélienne NGO Group, sur le téléphone de l'activiste. Le piratage a fait l'objet d'une couverture médiatique importante, principalement parce qu'il exploitait le dernier logiciel iPhone de l'époque, à la fois iOS 14.4 et plus tard iOS 14.6, publié par Apple en mai 2021. Le piratage a surmonté une fonctionnalité logicielle de sécurité intégrée à toutes les versions d'iOS 14, appelée BlastDoor, qui visait à empêcher ce type de piratage d'appareils en filtrant les données malveillantes envoyées via iMessage. En raison de sa capacité à vaincre BlastDoor, cet exploit a été surnommé ForcedEntry. En réponse, Apple a amélioré ses défenses de sécurité avec iOS 15.
- ***Violation de WhatsApp, 2019 :*** Cette fameuse violation a été déclenchée par un appel manqué, qui exploitait une faille dans le cadre du code source de WhatsApp. Un exploit Zero Day – c'est-à-dire une cyber-vulnérabilité jusqu'alors inconnue et non corrigée – a permis à l'attaquant de charger un logiciel espion dans les données échangées entre deux appareils en raison de l'appel manqué. Une fois chargé, le logiciel espion s'est activé en tant que ressource d'arrière-plan, profondément ancrée dans la structure logicielle de l'appareil.
- ***Jeff Bezos, 2018 :*** En 2018, le prince héritier Mohammed ben Salmane d'Arabie saoudite aurait envoyé au PDG d'Amazon, Jeff Bezos, un message WhatsApp contenant une vidéo faisant la promotion du marché des télécommunications saoudien. Il a été signalé qu'il y avait un morceau de code dans le fichier vidéo qui permettait à l'expéditeur d'extraire des informations de l'iPhone de Bezos sur plusieurs mois. Cela a abouti à la capture de messages texte, de messages instantanés et d'e-mails, et peut-être même d'écoutes clandestines d'enregistrements pris avec les microphones du téléphone.
- ***Projet Raven, 2016 :*** Le projet Raven fait référence à l'unité des cyber-opérations offensives des Émirats arabes unis, qui comprend des responsables de la sécurité émiratis et d'anciens agents du renseignement américain travaillant en tant que sous-traitants. Ils auraient utilisé un outil connu sous le nom de Karma pour profiter d'une faille dans iMessage. Karma a utilisé des messages texte spécialement conçus pour pirater les iPhones d'activistes, de diplomates et de dirigeants étrangers rivaux afin d'obtenir des photos, des e-mails, des messages texte et des informations de localisation.

3. Comment fonctionne une attaque zéro clic ?

En règle générale, l'infection à distance de l'appareil mobile d'une cible nécessite une certaine forme d'ingénierie sociale, l'utilisateur cliquant sur un lien malveillant ou installant une application malveillante pour fournir à l'attaquant un point d'entrée. Ce n'est pas le cas des attaques sans clic, qui contournent complètement le besoin d'ingénierie sociale.

Une attaque sans clic exploite les failles de votre appareil, en utilisant une faille de vérification des données pour se frayer un chemin dans votre système. La plupart des logiciels utilisent des processus de vérification des données pour empêcher les cyberattaques. Cependant, il existe des vulnérabilités Zero-Day persistantes qui ne sont pas encore corrigées, constituant des cibles potentiellement lucratives pour les cybercriminels. Des pirates informatiques sophistiqués peuvent exploiter ces vulnérabilités Zéro-Day pour exécuter des cyberattaques, qui peuvent être mises en œuvre sans aucune action de votre part.

Souvent, les attaques sans clic ciblent les applications qui fournissent des messages ou des appels vocaux, car ces services sont conçus pour recevoir et interpréter des données provenant de sources non fiables. Les attaquants utilisent généralement des données spécialement formées, telles qu'un message texte caché ou un fichier image, pour injecter du code qui compromet l'appareil.

Une hypothétique attaque sans clic pourrait fonctionner comme ceci :

- Les cybercriminels identifient une vulnérabilité dans un mail ou dans une application de messagerie.
- La vulnérabilité permet à des acteurs malveillants d'infecter l'appareil à distance via des e-mails qui consomment beaucoup de mémoire.
- Ils exploitent la vulnérabilité en envoyant un message soigneusement rédigé à la cible.
- L'e-mail, le message ou l'appel du pirate informatique ne resteront pas nécessairement sur l'appareil.
- À la suite de l'attaque, les cybercriminels peuvent lire, modifier, divulguer ou supprimer des messages.

Le piratage peut prendre la forme d'une série de paquets réseau, de demandes d'authentification, de messages texte, de MMS, de messages vocaux, de sessions de vidéoconférence, d'appels téléphoniques ou de messages envoyés via Skype, Telegram, WhatsApp, etc. Tous ces éléments peuvent exploiter une vulnérabilité dans le code d'une application chargée de traiter les données.

Le fait que les applications de messagerie permettent d'identifier les personnes grâce à leur numéro de téléphone, facilement localisable, signifie qu'elles peuvent constituer une cible évidente tant pour les entités politiques que pour les opérations de piratage commercial.

Les spécificités de chaque attaque sans clic varient en fonction de la vulnérabilité exploitée. Une caractéristique clé des hacks zéro-clic est leur capacité à ne pas laisser de traces, ce qui les rend très difficiles à détecter. Cela signifie qu'il n'est pas facile d'identifier qui les utilise et dans quel but. Cependant, il semblerait que les agences de renseignement du monde entier les utilisent pour intercepter les messages des criminels et des terroristes présumés et surveiller leur localisation.

4. Solutions : comment se protéger contre les attaques zéro-clic ?

Étant donné que les attaques sans clic ne reposent sur aucune interaction de la part de la victime, vous ne pouvez pas faire grand-chose pour vous protéger. Bien que cette idée soit intimidante, il est important de garder à l'esprit qu'en général, ces attaques ont tendance à cibler des victimes spécifiques à des fins d'espionnage ou peut-être de gain monétaire.

Cela dit, pratiquer une cyber-hygiène de base contribuera à maximiser votre sécurité en ligne. Les précautions raisonnables que vous pouvez prendre comprennent :

- Gardez votre système d'exploitation, votre micrologiciel et vos applications sur tous vos appareils à jour lorsque vous y êtes invité.
- Téléchargez uniquement des applications depuis les sites officiels.
- Supprimez toutes les applications que vous n'utilisez plus.
- Évitez de « jailbreaker » votre téléphone, car cela supprimerait la protection fournie par le constructeur. Le jailbreak consiste à exploiter les failles d'un appareil électronique bridé pour installer un logiciel autre que celui fourni par le fabricant de l'appareil. Le jailbreak permet au propriétaire de l'appareil d'avoir un accès total à la racine (« root ») du système d'exploitation et aux fonctionnalités. « Jailbreak » signifie littéralement « libérer » l'appareil de la « prison » formée par les limites imposées sur l'appareil.
- Utilisez la protection par mot de passe de votre appareil.
- Utilisez une authentification forte pour accéder aux comptes, en particulier aux réseaux critiques.
- Utilisez des mots de passe forts, c'est-à-dire des mots de passe longs et uniques.
- Redémarrez régulièrement les appareils pour faire face à certaines menaces persistantes.
- Sauvegardez régulièrement les systèmes. Les systèmes peuvent être restaurés en cas de ransomware, et disposer d'une sauvegarde à jour de toutes les données accélère le processus de récupération.
- Activez les bloqueurs de fenêtres contextuelles ou empêchez l'apparition des fenêtres contextuelles en ajustant les paramètres de votre navigateur. Les fraudeurs utilisent régulièrement des fenêtres contextuelles pour diffuser des logiciels malveillants.
- L'utilisation d'un antivirus complet vous aidera également à assurer votre sécurité en ligne. Les éditeurs d'antivirus offrent des protections contre les pirates informatiques, les virus et les logiciels malveillants, ainsi que des outils de protection des paiements, de confidentialité, etc.

5. En conclusion

" L'invisible est réel. Les âmes ont leur monde." Alfred de Vigny.

Les attaques sans clic ont augmenté ces dernières années en exploitant principalement les vulnérabilités des appareils mobiles et en utilisant des applications de messagerie populaires, telles que iMessage et WhatsApp. Ces attaques transmettent des logiciels malveillants à des utilisateurs peu méfiants et sont difficiles à détecter en raison du manque d'interaction de l'utilisateur. En outre, l'infection peut se propager via un appel manqué. Les attaques sans clic génèrent souvent des logiciels espions pour surveiller et collecter discrètement les données des victimes.