Actualités, Renseignements sur les menaces

Les voyageurs visés lors de la connexion aux réseaux Wi-Fi d'hôtels

par Pieter Arntz | 4 août 2026

Microsoft a averti que les réseaux Wi-Fi des hôtels, des centres de conférence et d'autres établissements d'accueil sont activement exploités par un groupe russe pour cibler des voyageurs dans le monde entier. Cette campagne, baptisée « CaptiveCrunch », transforme l'étape habituelle de connexion au Wi-Fi en une opportunité de compromettre des comptes et des appareils d'entreprise.

> Du point de vue de l'utilisateur, rien ne semble inhabituel : il se connecte au Wi-Fi de l'hôtel, voit s'afficher le portail captif habituel et peut-être un message d'apparence familière indiquant qu'une mise à jour est nécessaire avant de pouvoir naviguer. Cependant, en coulisses, le groupe — présumé lié à un État — s'intercale dans le flux réseau et manipule le trafic DNS (Domain Name System) et HTTP provenant du portail captif Wi-Fi.

À partir de là, plusieurs scénarios peuvent se produire :

Vol d'identifiants : la session de navigation de l'utilisateur est redirigée vers des pages d'hameçonnage contrôlées par les attaquants (comme de fausses pages de connexion Microsoft), où sont récoltés des identifiants, des codes d'appareil ou des jetons OAuth.
Téléchargement de logiciels malveillants : l'utilisateur se voit proposer de fausses boîtes de dialogue de mise à jour ou de type « ClickFix » qui téléchargent des logiciels malveillants. Il s'agit généralement d'un cheval de Troie d'accès à distance (RAT) accompagné d'un logiciel de vol d'informations (*infostealer*).
Attaque de type « machine-in-the-middle » (MitM) : le trafic transite discrètement par l'infrastructure des attaquants, exposant l'utilisateur à un risque accru de vol d'identifiants.
Selon les rapports, l'une des principales souches de logiciels malveillants utilisées dans ces attaques se nomme CornFlake ; il s'agit d'un cheval de Troie d'accès à distance (RAT) capable de capturer des images de la webcam, le son du microphone et les frappes au clavier.

Le logiciel de vol d'informations a été identifié sous le nom de ChocoShell ; il s'agit d'un programme sans fichier (*fileless*) basé sur PowerShell, ciblant principalement les cookies de session de navigation, les mots de passe enregistrés, les jetons d'authentification unique (SSO) Microsoft 365 et les identifiants Wi-Fi des systèmes compromis.

Microsoft dresse la liste de plusieurs fausses boîtes de dialogue susceptibles d'apparaître lors de la connexion à un réseau Wi-Fi compromis :

winupdate : une fausse fenêtre Windows Update affichant « Préparation des mises à jour… N'éteignez pas votre ordinateur ».
defender : une fausse analyse antivirus Windows Security.
directx : « DirectX End User Runtime Web Installer ». vcredist : un programme d'installation de composants redistribuables Microsoft Visual C++.
sysopt : un utilitaire d'optimisation de disque.
netfix : un outil de réparation pour les diagnostics réseau de Windows.
browser : une invite de mise à jour du navigateur.
pdfview : un programme d'installation de visionneuse de documents/PDF.
Comment rester en sécurité
Malwarebytes met en garde depuis longtemps contre les risques liés aux réseaux Wi-Fi publics. Voici comment rester en sécurité lors de vos déplacements :

Utilisez le point d'accès de votre propre téléphone plutôt que le Wi-Fi public. Une connexion mobile, en particulier avec une eSIM et un opérateur fiable, réduit considérablement les risques d'attaque par rapport à un réseau d'hôtel inconnu.

> Si vous êtes obligé d'utiliser un Wi-Fi public, utilisez un VPN doté d'une fonction « Kill Switch » (arrêt d'urgence) active : effectuez d'abord l'authentification sur le portail de l'hôtel, puis lancez votre VPN avant d'ouvrir un site web ou une application. La fonction Kill Switch bloquera instantanément tout trafic Internet si le VPN se déconnecte, ne serait-ce qu'une seconde, empêchant ainsi les cybercriminels d'injecter du code malveillant. Bien que CaptiveCrunch cible les vulnérabilités liées aux

portails captifs et aux flux précédant l'activation du VPN, ce dernier réduit tout de même d'autres risques et limite la collecte passive de données une fois que vous êtes en ligne.

Examinez toujours le certificat de tout portail de connexion ou de « sécurité » Wi-Fi public qui demande plus qu'un simple numéro de chambre ou des identifiants de base. Ces éléments ne sont pas toujours révélateurs d'une menace, mais ils peuvent parfois constituer un indice évident : des noms d'hôte qui ne correspondent pas, des émetteurs non approuvés ou l'utilisation du protocole HTTP (non sécurisé) sont autant de signaux d'alerte qui doivent vous dissuader de poursuivre.

De nombreux portails captifs demandent une adresse e-mail pour l'inscription ou à des fins marketing. Même dans les cas anodins, il n'est guère utile de communiquer votre véritable adresse e-mail principale. Si vous devez fournir une adresse, pensez à en utiliser une fausse ou un alias temporaire sans lien avec vos comptes principaux.

Si l'on vous demande de télécharger un logiciel, un certificat, une mise à jour de navigateur ou un outil de réparation pour vous connecter, arrêtez-vous. Vous ne devriez jamais avoir à télécharger quoi que ce soit simplement pour vous connecter à un réseau Wi-Fi.

Ne vous précipitez pas pour suivre les instructions affichées sur une page web ou dans une fenêtre contextuelle, surtout si l'on vous demande d'exécuter des commandes sur votre appareil ou de copier-coller du code. Méfiez-vous des pages incitant à une action immédiate : les pages sophistiquées de type « ClickFix » utilisent des comptes à rebours, des compteurs d'utilisateurs ou d'autres tactiques de pression pour vous pousser à agir rapidement.

Sécurisez vos appareils. Utilisez une solution anti-malware à jour et fonctionnant en temps réel, dotée d'un module de protection Web.

Évitez de saisir vos identifiants Microsoft 365, Google Workspace ou tout autre compte sensible sur une page accessible via la redirection d'un portail captif. Si vous devez consulter votre messagerie professionnelle, accédez directement aux adresses URL connues plutôt que de cliquer sur les invites qui s'affichent.

Enfin, veillez à mettre à jour votre navigateur, vos systèmes d'exploitation et autres logiciels importants avant de partir en voyage. Vous réduirez ainsi le risque de recevoir des demandes de mise à jour légitimes pendant votre absence.

Du signalement des menaces à leur suppression.

Ne laissez pas les risques de cybersécurité faire la une de l'actualité. Protégez vos appareils contre les menaces en téléchargeant Malwarbyte

News, Threat Intel
Travelers targeted when logging into hotel Wi-Fi networks
by Pieter Arntz | August 4, 2026

Microsoft has warned that hotel, conference, and other hospitality Wi-Fi networks are being actively abused by a Russian group to target travelers worldwide. The campaign, dubbed “CaptiveCrunch” turns a routine Wi-Fi login moment into an opportunity to compromise corporate accounts and devices.

From the user’s perspective, nothing looks out of the ordinary: they connect to hotel Wi-Fi, get the usual captive portal prompt, and perhaps see a familiar-looking message about needing to update something before they can browse. However, behind the scenes, the allegedly state-linked group position themselves in the network path and manipulate DNS (Domain Name System) and HTTP traffic from captive-portal Wi-Fi.

From there, several things can happen:

Logins are stolen: The user’s browser session is redirected to attacker-controlled phishing pages, like fake Microsoft login prompts, where credentials, device codes, or OAuth tokens are harvested.
Malware is downloaded: The user is presented with fake update or ClickFix dialogs that download malware. In these cases, usually a remote access trojan (RAT) plus an infostealer.
A machine-in-the-middle attack (MitM) where traffic is quietly proxied through attacker infrastructure, putting the user in a position for further credential theft.
Reportedly, one of the main malware strains used in these attacks is called CornFlake, a remote access trojan (RAT) that can capture webcam images, microphone audio, and keystrokes.

The infostealer was identified as ChocoShell, a fileless Powershell-based information stealer which primarily goes after browser session cookies, saved passwords, Microsoft 365 Single Sign-On (SSO) tokens, and Wi-Fi credentials from compromised systems.

Microsoft lists a set of fake dialogs that may appear once you connect to compromised Wi-Fi:

winupdate: A bogus Windows Update window with "Working on updates… Don't turn off your computer."
defender: A fake Windows Security virus scan.
directx: "DirectX End-User Runtime Web Installer."
vcredist: A Microsoft Visual C++ redistributable installer.
sysopt: A disk optimization utility.
netfix: A Windows Network Diagnostics 'fix' tool.
browser: A browser update prompt.
pdfview: A document/PDF viewer installer.
How to stay safe
Malwarebytes has long warned about the safety of public Wi-Fi. Here's how you can stay safe while traveling:

Use your own phone's hotspot instead of using the public Wi-Fi. A mobile connection, especially with an eSIM and a reputable carrier, significantly reduces the likelihood of an attack compared to an unknown hotel network.
If you're forced to use public Wi-Fi, use a VPN with an active Kill Switch: Complete the authentication on the hotel portal first, then launch your VPN before opening any website or app. The Kill Switch feature will instantly block all internet traffic if the VPN disconnects even for a second, preventing cybercriminals from injecting malicious code out in the open. While CaptiveCrunch operates around captive portals and pre-VPN flows, a VPN still reduces other risks and limits passive data collection once you're online.
Always inspect the certificate of any public Wi-Fi login or 'security' portal that asks for more than a room number or basic credentials. These aren't always a straight-up giveaway, but sometimes they can be an obvious clue: mismatched hostnames, untrusted issuers, or plain HTTP are red flags that should stop you from proceeding.
Many captive portals ask for an email address for registration or marketing. Even in benign cases, there is little value in handing over your real inbox. If you must provide an address, consider giving a fake one or a throwaway alias that is unrelated to your primary accounts.
If you are asked to download software, a certificate, a browser update, or a fix tool in order to connect, stop. You should never have to download anything just to log into Wi-Fi.
Don't rush to follow instructions on a webpage or prompt, especially if it asks you to run commands on your device or copy-paste code. Be cautious of pages urging immediate action: sophisticated ClickFix pages add countdowns, user counters, or other pressure tactics to make you act quickly.
Secure your devices. Use an up-to-date, real-time anti-malware solution with a web protection component.
Avoid entering Microsoft 365, Google Workspace, or other high-value credentials directly into any page reached via captive portal redirection. If you need to check corporate mail, follow known URLs rather than clicking through prompts.
And last but not least, update your browser, operating systems, and other important software before you travel. That reduces the chance of getting legitimate update requests while you're away.

From reporting threats to removing them.

Cybersecurity risks should never spread beyond a headline. Keep threats off your devices by downloading Malwarebytes today.