

Insolite : Le côté obscur des Smartphones

Insolite

Posté par : JerryG

Publié le : 13/5/2011 14:00:00

Cinq milliards : c'est le nombre d'abonnés en téléphonie mobile dans le monde, selon l'Union Internationale des Télécommunications (UIT). Un chiffre impressionnant, surtout quand on sait qu'il y a 6.8 milliards d'habitants sur Terre! Les smartphones ont définitivement envahi nos vies privées mais également nos vies professionnelles, est-ce pour notre bien ou notre malheur, **Axelle Apvrille**, expert anti-virus chez Fortinet, nous propose de partager son point de vue sur les nombreuses menaces qu'ils représentent pour les réseaux des entreprises..

Il y a encore quelques années, les smartphones étaient réservés aux cadres dirigeants des entreprises pour leur permettre de gérer leurs responsabilités quotidiennes et d'être facilement joignables. Aujourd'hui, ils sont devenus un outil de communication répandu car utilisés par de nombreux employés comme une extension mobile de leurs ordinateurs. Grâce aux smartphones, ces individus peuvent accéder au réseau de l'entreprise, lire leurs emails, répondre aux messages urgents, trouver les indications pour assister à une réunion, sauvegarder une carte d'embarquement, une présentation ou un rapport d'activité, etc.



Petit, pratique, utile, polyvalent; les smartphones présentent de nombreux avantages. Cependant, du fait que la sécurité des téléphones mobiles et de leur infrastructure n'est pas encore arrivée à maturité, ils exposent malheureusement les réseaux des entreprises à de nombreuses menaces.

Bataille perdue entre sécurité et facilité d'utilisation

Aujourd'hui, les sociétés exigent souvent de leurs employés d'utiliser un VPN pour accéder au réseau d'entreprise via leurs ordinateurs portables ou PC à distance (qui sont de plus en plus équipés de logiciels antivirus). Un VPN permet un accès sécurisé au réseau d'entreprise grâce à l'encapsulation des transferts de données par l'utilisation d'une méthode cryptographique. Malheureusement, les solutions VPN pour les appareils mobiles ne sont pas encore très répandues. Le principal frein à leur adoption réside dans le fait que les VPN exigent une puissance de calcul que les smartphones ont rarement aujourd'hui. Les tâches telles que l'encryption ou le décryptage à la volée sont lourdes à gérer et rendent ainsi l'accès à distance difficile pour l'utilisateur final.

Face à ces contraintes techniques, les administrateurs des systèmes doivent choisir entre

compromettre la sécurité de leurs réseaux pour permettre l'accès aux utilisateurs de téléphones mobiles, et limiter leur accès ou les diriger vers un autre réseau moins sensible. En pratique, chaque fois qu'il y a un compromis à faire entre facilité d'utilisation et sécurité, la sécurité perd la bataille... Aujourd'hui, nous observons que la plupart des employés peuvent accéder aux réseaux d'entreprises via leur smartphone de n'importe où¹, et avec une protection dégradée. Imaginez les dégâts potentiels quand ces utilisateurs utilisent des points d'accès publics pour obtenir une connexion mobile !

La propagation des logiciels malveillants : Du mobile au réseau d'entreprise

Le choix inévitable de la facilité d'utilisation sur la sécurité fait des smartphones un moyen idéal pour les cybercriminels d'attaquer les réseaux d'entreprises. Les cybercriminels sont similaires à des cambrioleurs : ils cherchent le point faible d'entrée (à partir d'un PC à distance ou d'un téléphone mobile infecté), trouvent un moyen de le faire ceder, et ensuite, propagent des logiciels malveillants, collectent des adresses emails à spammer, volent les données confidentielles, infectent les serveurs des entreprises, etc.

Un moyen de se glisser dans le réseau des entreprises consiste à profiter de l'opération de synchronisation du téléphone mobile. Lorsque l'employé synchronise son téléphone mobile au travail, son appareil infecte l'ordinateur pendant la synchronisation. Le téléphone mobile agit comme un cheval de Troie, infecte le PC et fournit involontairement l'accès au réseau de l'entreprise. Il y a plusieurs années, c'est ainsi que MSIL/Overcross a été propagé d'un appareil Windows Mobile à un PC Windows, via ActiveSync.

Les attaques sur les téléphones mobiles à partir des PC

Réciproquement, les téléphones mobiles où plus exactement les données qu'ils transportent peuvent être ciblés par des PC (par exemple, par les ordinateurs infectés sur l'intranet ou à la maison, ou encore par des serveurs externes malicieux contrôlés par les cybercriminels). C'est ainsi que le malware SymbOS/Zitmo a récemment opéré : un ordinateur infecté par Zeus, l'un des Trojans les plus nuisibles et répandus, a réussi à contaminer les téléphones mobiles des victimes. Cette attaque a été particulièrement intéressante pour les cybercriminels car elle leur a permis d'avoir un moyen efficace de vaincre la technique d'authentification à deux facteurs, utilisée par des organisations telles que les banques, via l'interception du mot de passe unique envoyé par SMS à l'utilisateur du téléphone mobile.

Les attaques directes sur les téléphones mobiles

Les smartphones sont légers et faciles à transporter. Par conséquent, les employés les utilisent souvent pour transporter des documents essentiels. Au-delà de sa fonction première, le téléphone mobile est utilisé comme un carnet d'adresses, une clé USB, un bloc-notes, ou même un dictaphone. Qu'il s'agisse d'une présentation PowerPoint, de caractéristiques d'un nouveau produit, du numéro de téléphone du PDG de l'entreprise, d'une liste des adresses emails de la société ou de la dernière situation financière du trimestre, ces documents sont non sécurisés sur le téléphone mobile.

La plupart des employés sont rassurés quand ils verrouillent leur téléphone mobile (avec un mot de passe ou un geste secret sur l'écran tactile) car ils pensent que son contenu est sécurisé. La réalité est différente: les chercheurs allemands de l'institut Fraunhofer

ont récemment débloqué un iPhone en moins de 6 minutes en utilisant un équipement standard. Certains employés tentent de renforcer la sécurité de leur iPhone en utilisant un logiciel spécial anti-vol ou en cryptant la carte mémoire de leur iPhone.

Ces solutions ont pour but d'augmenter la protection des données contre les attaques physiques, celles faites par des pickpockets, qui ne sont pas intéressés par le contenu du iPhone mobile mais par la possibilité de ré-utiliser ou de revendre l'appareil. Les cybercriminels, eux, se soucient des informations confidentielles stockées sur les smartphones mais ils n'ont pas besoin d'un accès physique au iPhone pour les récupérer. Ils exploiteront plutôt une vulnérabilité, par exemple une vulnérabilité dans le navigateur web du iPhone comme les vulnérabilités WebKit sur les iPhones Android, ou utiliseront une astuce pour installer un malware sur le iPhone. Une fois que le iPhone est infecté, il est alors facile pour les cybercriminels d'accéder à toutes les données. Dans ce cas, le verrouillage savant est inutile et la carte mémoire est le plus souvent déchiffrée de façon dynamique lors de son utilisation.

Quelques conseils pour minimiser les menaces mobiles dans l'environnement des entreprises

Comme indiqué précédemment, même si la puissance de calcul des smartphones reste la plus grande limitation de leur protection, il existe tout de même certaines mesures de sécurité informatique qui devraient être implémentées pour minimiser les menaces mobiles entrant dans les réseaux des entreprises :

- Déployez des filtres antivirus aux points d'entrée du réseau de l'entreprise utilisés par les iPhones mobiles (points d'accès WiFi, stations de synchronisation),
- Préférez les opérateurs mobiles qui filtrent le trafic mobile pour supprimer les malwares et essaient de fournir un canal de communication propre à leurs clients,
- Implémentez des solutions de sécurité auprès de constructeurs dont la recherche en menaces inclut la détection et la protection contre les menaces mobiles,
- Surveillez les factures de communications et soyez vigilant lorsque les frais semblent anormaux sur un appareil mobile particulier. C'est un symptôme fréquent d'infection mobile,
- Eduquez les employés sur des pratiques de précautions simples :
- Appliquer les mises à jour logicielles des plateformes mobiles dès qu'elles sont disponibles,
- Ne pas ouvrir les SMS/MMS d'un inconnu et ne pas cliquer sur les liens Internet d'amis. Supprimer ces SMS ou les signaler à l'opérateur mobile,
- Ne pas communiquer son numéro de iPhone aux sites Internet sans rapport avec son activité professionnelle. Par exemple, il n'y a pas de raison de fournir son numéro de mobile sur son compte personnel Facebook,
- Demander à l'administrateur système une recommandation sur les applications qui peuvent être utiles. En règle générale, installer uniquement les applications qui sont nécessaires et les télécharger à partir de sites légitimes uniquement,
- Désactiver les canaux de communications tels que le Bluetooth par défaut pour les activer uniquement en cas de besoin. Cette mesure évite de nombreuses attaques potentielles et permet d'économiser la batterie du iPhone!

- S'assurer que les données personnelles peuvent être effacées à distance, au cas où le smartphone soit volé. Cette recommandation est importante dans la prévention de l'espionnage industriel,

- Choisir le protocole TLS pour plus de confidentialité.