Mirai

Vous avez peut-être récemment reçu récemment une lettre et/ou un e-mail de Sunrise vous expliquant qu'un appareil en ligne sur votre réseau a été infecté par le logiciel malveillant Mirai. Si vous avez reçu cette communication de notre part, veuillez suivre les conseils donnés sur cette page afin de résoudre le problème.

Remarque: cet article a pour but de vous conseiller. Sunrise n'est toutefois pas responsable des problèmes rencontrés lors de la résolution de problème et n'est pas en mesure de fournir une assistance technique pour de tels cas.

Aperçu

Mirai est une forme de logiciel malveillant qui vise spécifiquement les appareils connectés à Internet sur votre réseau. Ces appareils sont souvent appelés «Internet des objets», «IoT». Ces appareils peuvent être des systèmes de vidéosurveillance, des Smart TV, des prises intelligentes, des boîtiers de stockage en réseau (NAS), des appareils USB ou autres.

Que s'est-il passé?

Nous travaillons avec de nombreuses organisations à but non lucratif dans tous les secteurs de la sécurité qui collectent des informations sur les appareils infectés par des logiciels malveillants sur Internet. Ces organisations nous ont informés qu'un appareil de la connexion Internet de votre domicile (ou d'un appareil connecté à votre réseau domestique) est infecté par un logiciel malveillant.

Nous ne pouvons préciser lequel de vos appareils est infecté, mais il s'agit probablement d'un appareil connecté tel qu'une caméra de vidéosurveillance ou un boîtier de stockage en réseau (NAS) plutôt que d'un ordinateur ou d'un ordinateur portable classique.

Si le logiciel malveillant n'est pas supprimé, l'appareil pourra être utilisé pour participer indépendamment de votre volonté à des activités malveillantes, comme une attaque DDoS (attaque par déni de service).

Il est donc important de suivre les conseils de cet article.

Comment résoudre le problème?

Nous sommes là pour vous aider. Si vous possédez des connaissances de base en informatique et en appareils connectés, vous pouvez prendre plusieurs mesures pour sécuriser votre réseau domestique. Assurez-vous de bien suivre les étapes suivantes dans l'ordre.

1. **Sécurisez l'accès à distance de vos appareils**

   Le logiciel Mirai cible les appareils qui utilisent le protocole d'accès à distance Telnet, et toujours sous le nom d'utilisateur et le mot de passe par défaut définis par le fabricant. Ces identifiants par défaut sont souvent facilement disponibles sur Internet, ce qui peut permettre à des tiers d'accéder à distance à votre appareil et d'y installer des logiciels malveillants.

   Pour sécuriser l'accès Telnet sur vos appareils, veuillez suivre l'une des étapes suivantes:

   Modifiez les mots de passe par défaut

   Les appareils connectés à Internet utilisent souvent un nom d'utilisateur et un mot de passe par défaut pour le service Telnet définis par le fabricant. Ils sont souvent identiques sur des centaines, voire des milliers d'appareils de ce fabricant.

   Changer ce mot de passe pour un mot de passe personnalisé vous protégera contre les futures attaques Mirai, car le logiciel malveillant utilise une liste de mots de passe courants pour se connecter à votre appareil via Telnet.

   Assurez-vous de déconnecter l'appareil d'Internet avant de modifier les mots de passe.

Les étapes pour modifier le mot de passe Telnet utilisé par tous les appareils connectés à Internet sur votre réseau domestique varient selon le fabricant et l'appareil. Pour plus de détails, consultez la documentation fournie avec votre appareil.

Désactiver l'accès Telnet si ce dernier n'est pas obligatoire

Si vous n'avez pas besoin du service Telnet pour des systèmes en dehors de votre réseau domestique, il est fortement recommandé de le bloquer afin que seuls les appareils de votre logement puissent l'utiliser.

Le service Telnet n'utilise pas de cryptage: les mots de passe que vous envoyez entre des appareils via Telnet sont partagés en texte clair, ce qui représente un risque de sécurité.

2. **Supprimez l'infection Mirai**

Une fois que le service Telnet a été sécurisé à l'aide de l'une des solutions ci-dessus, l'étape suivante consiste à supprimer l'infection Mirai de votre ou de vos appareils.

Pour ce faire, suivez les étapes ci-dessous:

- Déconnectez l'appareil du réseau

- Lors de la déconnexion au réseau, redémarrez l'appareil. Le logiciel malveillant Mirai existe dans une mémoire dynamique. Un redémarrage de l'appareil l'effacera de votre appareil.

Vous ne devez vous reconnecter au réseau qu'après le redémarrage et la modification de votre mot de passe. Si vous vous reconnectez avant de modifier le mot de passe, l'appareil pourrait rapidement être à nouveau infecté par le logiciel malveillant Mirai.

Comment savoir si je suis désormais en sécurité?

Si vous avez suivi les conseils ci-dessus, vous pouvez être certain d'avoir résolu le problème.

Questions au sujet d'Internet

Sunrise est co-fondateur et membre de iBarry.ch, une organisation à but non lucratif qui travaille avec des experts en sécurité informatique afin de vous fournir toutes les informations dont vous avez besoin pour que vos enfants et vous surfiez en ligne en toute sécurité.

Pour plus d'informations sur iBarry, rendez-vous sur https://www.ibarry.ch/fr/