Popcorn Time, un rançongiciel bien vicieux

Popcorn Time, un rançongiciel bien vicieux

Depuis peu, les rançongiciels (ou ransomware) constituent de véritables fléaux dans l'univers de l'informatique et du web. Ils touchent les données personnelles de millions de gens de par le monde. Les experts en sécurité se sont même mis à taxer 2016 comme étant « l'année des rançongiciels ».

Payez ou infectez vos amis

Sur cette année, il se peut que Popcorn Time soit le rançongiciel qui vienne clore la propagation de ces logiciels de chantage. Ce nouveau ransomware pose un gros dilemme à sa victime en lui imposant de payer une rançon ou d'infecter ses amis.

Pour commencer, il emprunte le nom d'une application de streaming vidéo ayant défrayé la chronique en 2015, ce qui incite au téléchargement de celle-ci. Ensuite, il infecte l'ordinateur de la victime par le biais d'un courriel piégé ou d'un lien malveillant, puis crypte ses données personnelles en usant d'un algorithme de chiffrement AES 256 bits.

Après que les données ont été cryptées, il impose à la victime de donner la valeur de 1 bitcoin (soit environ 700 €) ou de le transmettre sur l'ordinateur d'un ami. C'est une méthode toute nouvelle avec en plus une limite du nombre d'introductions de clé de déchiffrement. Entrer quatre fois la mauvaise clé ferait perdre définitivement ses données.

Les dossiers Windows sont les premières cibles

D'après la conclusion des enquêtes réalisées par le site Bleeping Computer sur ce rançongiciel, il ciblerait en premier les fichiers présents dans les dossiers Windows : Mes Documents, Images, Musiques et toutes les données sur le Bureau.

Afin de faire face à ce logiciel de rançon, la meilleure façon pour un utilisateur lambda est de prendre des précautions préventives basées sur les mesures de sécurité les plus basiques :

• faire des copies de ses données personnelles vers un support externe qui se débranche de l'ordinateur après chaque usage de ce dernier et sur les Clouds comme Dropbox, OneDrive, Google Drive, Mediafire, Mega, pCloud, Flipdrive… ;

• éviter d'ouvrir les mails aux destinateurs inconnus et contenant des liens ou des pièces jointes. Il est aussi possible que Popcorn Time provienne d'une personne de votre liste de contact. Prenez les mêmes réserves tant que le contenu n'a pas été formellement reconnu ;

• mettre à jour son système d'exploitation et son antimalware.

…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Certifié ISO 27005 Risk Manager, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Popcorn Time : le plus vicieux rançongiciel de cette année – @Sekurigi

---

Alerte ! Un virus informatique peut vider votre compte bancaire

Alerte ! Un virus informatique peut vider votre compte bancaire

---

77% des ménages possèdent un ordinateur et 75% une connexion internet. A l'heure ou le numérique gagne toujours plus de terrain, de nouvelles menaces s'invitent dans nos foyers, les virus.
Quand les nouvelles technologies veulent nous simplifier la vie en numérisant toutes nos informations, les hackers eux, redoublent d'ingéniosité pour créer des virus de plus en plus performants. Tous les jours des dizaines ne milliers de nouveaux virus sont créés, et si l'efficacité des antivirus est parfois relative, il reste que nous manquons aussi de vigilance.

Avertissement de la gendarmerie
« En consultant internet, une mise en garde indique que votre ordinateur est infecté par le virus « Zeus ». La page d'alerte vous oriente alors vers le numéro de téléphone d'un spécialiste de la sécurité informatique. […] L'escroc, homme ou femme, recommande alors le nettoyage de votre ordinateur et l'intégration à distance d'un antivirus, moyennant une somme d'argent variant entre 99 et 249 euros. »

C'est le message que la gendarmerie du Cher a fait paraître sur son Facebook afin de prévenir la population. Ce nouveau virus est d'autant plus dangereux que le hacker, télécharge et utilise vos données bancaires pendant que vous payez l'antivirus recommandé. Prudence donc si ce message apparaît sur votre écran, n'appelez surtout pas et confiez votre ordinateur à un spécialiste…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Certifié ISO 27005 Risk Manager, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

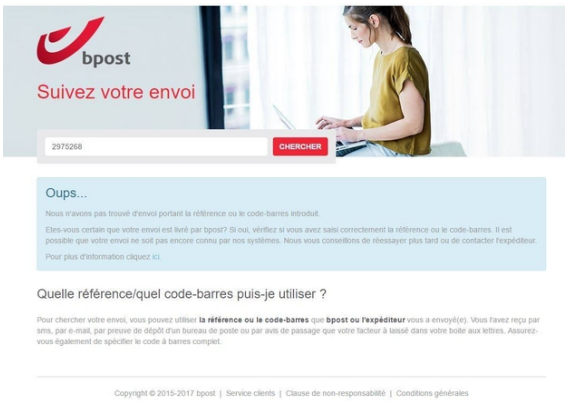
Original de l’article mis en page : « Zeus » : un virus informatique qui peut vider votre compte bancaire !

Attention à ce mail suspect. Ne cliquez pas !

	Attention à ce mail suspect. Ne cliquez pas !

Il s'agit en réalité d'un ransomware, un logiciel malveillant qui vise à prendre vos données et fichiers personnels en otage et les bloquer !

Après la fausse facture de Free, c'est cette fois la marque et le logo bpost qui ont été détournés par des hackers avec l'ambition d'essayer de *pomper* vos données personnelles et de les prendre en otage afin de réclamer, par après, une « rançon » contre la libération de celles-ci ! Pour ce faire, les pirates utilisent ce qu'on appelle un *ransomware*.
Pour tenter d'arriver à leurs fins, les hackers ont donc emprunté les traits de bpost afin de vous demander de cliquer sur un lien permettant, soi-disant, de retrouver trace d'un colis qui n'a pas encore été livré. Le piège est en marche. Le principe est donc simple et diabolique puisque les utilisateurs qui reçoivent ce fameux mail ont, en théorie, toute confiance en l'institution.



En effet, s'il est trop tard et que vous avez déjà appuyé sur le bouton de votre souris, le mal est fait. Le logiciel ainsi installé aura tout le loisir de prendre connaissance de vos données et fichiers personnels, voire même prendre le contrôle de votre poste de travail, bloquant au passage l'accès à vos précieuses infos via une clé de cryptage… permettant aux malotrus de réclamer une rançon contre la libération de vos données ou de votre ordinateur ! Inutile de préciser que dans bien des cas, la spirale infernale est enclenchée !
L'excellente série de *Netflix Black Mirror* avait d'ailleurs centré un de ses épisodes sur cette problématique, les protagonistes perdant au fil de celui-ci, le contrôle total sur les événements.
Que faire en cas d'infection ?
Si vous avez installé ledit logiciel, il faudra de toute façon passer, au minimum, par la case du scan antivirus. Sans plus attendre également, il est fortement conseillé de débrancher immédiatement tous les disques durs externes et autres qui pourraient être plus facilement sauver, d'autant plus s'ils contiennent des sauvegardes de vos fichiers. Idem, pensez à déconnecter vos espaces de stockage virtuel (Dropbox, iCloud,…)
Dans certains cas, certains logiciels sont capables de combattre l'infection. Une petite recherche sur Google et différents forums s'impose donc.
Il est aussi très important de rappeler qu'il ne faut surtout pas rentrer dans « le jeu » et donc absolument éviter de payer la rançon demandée. Rien ne dit en effet que les pirates la joueront *fair play*… De plus, il est aussi très utile de prévenir les autorités compétentes…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Vous avez reçu un mail suspect de bpost ? Ne cliquez pas ! (PHOTOS) – DH.be

Rakos, un nouveau botnet qui vise aussi les Objets connectés

	Rakos, un nouveau botnet qui vise aussi les Objets connectés

Après Mirai, voici venir Rakos, un malware infectant des serveurs et des réseaux d'objets connectés, tournant sous Linux, afin de créer des botnets. ET, demain, lancer des attaques DDoS.

Comme le tristement célèbre malware Mirai, Rakos prend pour cible l'Internet des objets (IoT). Ces deux logiciels malveillants compromettent en effet des serveurs sous Linux et des réseaux d'appareils connectés. La capacité de nuisance de ces botnets contrôlés à distance est bien réelle. Si Mirai se propage essentiellement via les ports logiciels Telnet, Rakos vise lui les ports SSH. Les périphériques embarqués et les serveurs ayant un port SSH ouvert ou un mot de passe très faible sont les plus exposés. Rakos a été découvert cet été par les chercheurs de ESET.

À ce jour, Rakos est utilisé pour mener des attaques par force brute, indique l'entreprise dans un billet de blog. Et ce, afin d'ajouter d'autres appareils compromis à son réseau de machines zombies. Mais le programme pourrait également servir à mener des campagnes de spam ou des attaques par déni de service distribué (DDoS) d'ampleur, comme l'a fait Mirai…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Rakos, un nouveau botnet IoT en constitution

Alerte : Des routeurs domestiques attaqués par malvertising via DNSChanger

Alerte : Des routeurs domestiques attaqués par malvertising via DNSChanger

Des routeurs domestiques font l'objet d'une attaque par le biais d'une campagne de publicités malveillantes et via le navigateur Web sur Windows et Android.

Depuis la fin du mois d'octobre, les chercheurs en sécurité de Proofpoint indiquent avoir constaté l'utilisation d'une version améliorée du kit d'exploits DNSChanger dans le cadre de campagnes de publicités malveillantes (du malvertising).
Pour ce retour, DNSChanger – qui avait infecté des millions d'ordinateurs en 2012 – cible des routeurs domestiques et fonctionne la plupart du temps via le navigateur Google Chrome sur Windows et les appareils Android. Toutefois, il s'agit bel et bien d'exploiter des vulnérabilités affectant des routeurs.
Du code JavaScript malveillant permet de révéler une adresse IP locale par le biais d'une requête WebRTC (Web Real-Time Communication) vers un serveur STUN (Session Traversal Utilities for NAT) de Mozilla. WebRTC est un protocole pour la communication en temps réel sur le Web, et STUN est un protocole permettant de découvrir l'adresse IP et le port d'un client ainsi que déterminer des restrictions au niveau du routeur.

Si l'adresse IP est jugée digne d'intérêt, une fausse publicité est affichée. Elle prend la forme d'une image au format PNG. Un code exploit est caché dans les métadonnées et pour rediriger la victime vers une page hôte de DNSChanger.

Proofpoint explique que DNSChanger va une nouvelle fois vérifier l'adresse IP locale de la victime grâce à des requêtes STUN. Puis, le navigateur Google Chrome chargera plusieurs fonctions et une clé de chiffrement AES cachée par stéganographie dans une petite image. La clé sert à dissimuler du trafic et décrypter une liste d'empreintes numériques afin de déterminer si un modèle de routeur est vulnérable.
L'attaque menée dépend du modèle de routeur. Elle est utilisée pour modifier les entrées DNS (Domain Name System ; correspondance entre un nom de domaine et une adresse IP) dans le routeur et tenter de rendre accessibles les ports d'administration depuis des adresses externes. Le chercheur Kafeine de Proofpoint évoque alors une exposition du routeur à d'autres attaques et cite l'exemple des botnets Mirai.
À noter que s'il n'y a pas d'exploits connus, une attaque tentera tout de même sa chance en essayant de tirer parti d'identifiants qui sont ceux par défaut (pas modifiés par l'utilisateur), et toujours pour modifier les paramètres DNS.
Soulignons bien que le navigateur n'est ici pas mis en cause…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : DNSChanger attaque des routeurs domestiques via malvertising

---

Alerte ! Des publicités Internet contaminées par des malwares

Alerte ! Des publicités Internet contaminées par des malwares

De très nombreux sites Internet à forte notoriété ayant des millions de visiteurs quotidiens sont touchés. Les systèmes de détection ESET montrent qu'au cours des deux derniers mois, Stegano a été affiché auprès de plus d'un million d'utilisateurs. Stegano se cache dans les images publicitaires affichées sur les pages d'accueil des sites Internet.

Bonjour,
Depuis le début du mois d'octobre 2016, des cybercriminels ciblent les utilisateurs d'Internet Explorer et analysent leur ordinateur pour détecter les vulnérabilités dans Flash Player. En exploitant leurs failles, ils tentent de télécharger et d'exécuter à distance différents types de malwares.
Ces attaques se rangent dans la catégorie des publicités malveillantes, c'est-à-dire que des codes malicieux sont distribués via des bannières publicitaires. **La victime n'a même pas besoin de cliquer sur la publicité** : il suffit qu'elle visite un site Internet l'affichant pour être infecté. Elle est alors renvoyée automatiquement vers un kit d'exploitation invisible **permettant aux cybercriminels d'installer à distance des malwares sur son ordinateur.** Vous trouverez ci-joint notre infographie expliquant la technique utilisée par Stegano pour infecter les ordinateurs.
« **Certaines des charges utiles que nous avons analysées comprennent des chevaux de Troie, des portes dérobées et des logiciels espions, mais nous pouvons tout aussi bien imaginer que la victime se retrouve confrontée à une attaque par ransomware,** » explique Robert Lipovsky, senior malware researcher chez ESET. « Cette menace montre combien il est important d'avoir un logiciel entièrement patché et d'être protégé par une solution de sécurité efficace et reconnue. Si l'utilisateur applique ces recommandations, il sera protégé contre ce genre d'attaque, » poursuit Robert Lipovsky.
« Stegano » fait référence à la sténographie, une technique utilisée par les cybercriminels pour cacher une partie de leur code malveillant dans les pixels d'images présents dans les bannières publicitaires. Ceux-ci sont masqués dans les paramètres contrôlant la transparence de chaque pixel. Cela entraîne un changement mineur des tons de l'image, rendant ces derniers invisibles à l'œil nu pour la victime potentielle.
Afin d'éviter de se retrouver infecté par le malware Stegano, ESET recommande aux utilisateurs de protéger leurs machines avec une solution de sécurité fiable et de mettre à jour les applications et le système d'exploitation.
Pour plus d'informations sur Stegano, nous vous invitons à consulter les deux articles suivants venant de WeliveSecurity. Le premier est l'analyse technique détaillée de Stegano, le second est une interview de Robert Lipovksy, Senior malware researcher chez ESET, expliquant la menace pour le grand public. Nous nous tenons à votre disposition pour plus de détails.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Le malware Stegano infecte les machines à l'insu de ses victimes

---

Et si la publicité sur Internet était aussi infectée par des malwares ?

Et si la publicité sur Internet était aussi infectée par des malwares ?

Les chercheurs ESET viennent de découvrir Stegano, un nouveau kit d'exploitation se propageant via des campagnes publicitaires. De très nombreux sites Internet à forte notoriété ayant des millions de visiteurs quotidiens sont touchés.

Les systèmes de détection ESET montrent qu'au cours des deux derniers mois, Stegano a été affiché auprès de plus d'un million d'utilisateurs. Stegano se cache dans les images publicitaires affichées sur les pages d'accueil des sites Internet.
Depuis le début du mois d'octobre 2016, des cybercriminels ciblent les utilisateurs d'Internet Explorer et analysent leur ordinateur pour détecter les vulnérabilités dans Flash Player. En exploitant leurs failles, ils tentent de télécharger et d'exécuter à distance différents types de malwares.
Ces attaques se rangent dans la catégorie des publicités malveillantes, c'est-à-dire que des codes malicieux sont distribués via des bannières publicitaires. **La victime n'a même pas besoin de cliquer sur la publicité** : il suffit qu'elle visite un site Internet l'affichant pour être infecté. Elle est alors renvoyée automatiquement vers un kit d'exploitation invisible **permettant aux cybercriminels d'installer à distance des malwares sur son ordinateur**.
« **Certaines des charges utiles que nous avons analysées comprennent des chevaux de Troie, des portes dérobées et des logiciels espions, mais nous pouvons tout aussi bien imaginer que la victime se retrouve confrontée à une attaque par ransomware**, » explique Robert Lipovsky, senior malware researcher chez ESET. « Cette menace montre combien il est important d'avoir un logiciel entièrement patché et d'être protégé par une solution de sécurité efficace et reconnue. Si l'utilisateur applique ces recommandations, il sera protégé contre ce genre d'attaque, » poursuit Robert Lipovsky.
« Stegano » fait référence à la sténographie, une technique utilisée par les cybercriminels pour cacher une partie de leur code malveillant dans les pixels d'images présents dans les bannières publicitaires. Ceux-ci sont masqués dans les paramètres contrôlant la transparence de chaque pixel. Cela entraîne un changement mineur des tons de l'image, rendant ces derniers invisibles à l'œil nu pour la victime potentielle.
Afin d'éviter de se retrouver infecté par le malware Stegano, ESET recommande aux utilisateurs de protéger leurs machines avec une solution de sécurité fiable et de mettre à jour les applications et le système d'exploitation.
Pour plus d'informations sur Stegano, nous vous invitons à consulter les deux articles suivants venant de WeliveSecurity. Le premier est l'analyse technique détaillée de Stegano, le second est une interview de Robert Lipovksy, Senior malware researcher chez ESET, expliquant la menace pour le grand public. Nous nous tenons à votre disposition pour plus de détails.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Boîte de réception (31) – denis.jacopini@gmail.com – Gmail

---

Un malware multi compétences est né. Proteus

Un malware multi compétences est né. Proteus

Les experts de sécurité de Fortinet ont découvert un malware multifonction nommé Proteus. Il vérifie notamment les comptes e-commerce piratés.

Imaginer un malware capable de transformer les ordinateurs en serveur proxy, de miner différentes monnaies virtuelles, d'enregistrer les frappes au clavier et de vérifier la validité des comptes victimes d'un vol de données. Et bien cela existe. Les experts de Fortinet ont déniché ce couteau suisse du logiciel malveillant.
Baptisé Proteus, le malware est écrit en .Net et se diffuse à travers le botnet Andromeda. Les spécialistes de Fortinet constatent que ce malware peut éliminer d'autres logiciels malveillants sur les PC compromis. Tout comme Andromeda, il communique via un chiffrement symétrique avec des serveurs C&C pour contrôler les actions du malware sur les PC. De plus, il est capable d'ajouter des modules additionnels, les télécharger et les exécuter à la demande. Proteus s'épanouit dans le minage de crypto-monnaies. Il supporte les outils, HA256 miner, CPUMiner et ZCashMiner utilisés pour les monnaies virtuelles comme Bitcoin, Litecoin, Zcash.

Un vérificateur de comptes e-commerce piratés

Pour les spécialistes de la sécurité, la grande spécificité de Proteus réside dans sa capacité à vérifier la validité des comptes volés sur certains sites. Dans les cas présent, le code source du malware a montré que la vérification est réclamée par le serveur de C&C qui fournit des identifiants et des mots de passe. Le PC infecté va donc envoyer une requête sur certains sites de e-commerce comme Amazon, eBay, Spotify, Netflix et plusieurs sites allemands…[lire la suite]

Original de l'article mis en page : Proteus, le couteau suisse

du logiciel malveillant

---

900 000 routeurs de Deutsche Telekom infectés par un malware

900 000 routeurs de Deutsche Telekom infectés par un malware

Deutsche Telekom a confirmé la thèse d'un malware ayant infecté plus de 900.000 de ses routeurs. Selon Flashpoint, environ 5 millions de routeurs à travers le monde seraient vulnérables à la faille exploitée par cette variante de Mirai.

Le Cert-FR alerte les utilisateurs français sur cette attaque. L'équipe rappelle ainsi que « plusieurs version du binaire malveillant sont en circulation ». Le Cert-FR recommande de changer les mots de passe par défaut, de restreindre l'accès aux outils d'administration et de désactiver « les services inutilement lancés sur les équipements exposés sur le réseau. »
Mirai se tourne vers de nouvelles cibles et la nouvelle version du ver informatique s'attaque maintenant aux routeurs. On avait déjà constaté par le passé des variantes de ce malware modifiées afin de s'attaquer à de nouveaux appareils. Mais l'attaque ayant visé Deutsche Telekom montre que les opérateurs de cette nouvelle variante entendent maintenant changer de cible et délaisser les objets connectés pour s'attaquer aux routeurs.

Comme l'explique Flashpoint dans une note de blog, la mise à disposition du code source de Mirai par son créateur a entraîné une guerre entre les cybercriminels, alors que plusieurs groupes tentaient d'utiliser Mirai pour prendre le contrôle du maximum d'objets connectés vulnérables. « L'évolution logique pour ce malware était de découpler le mécanisme d'infection de la charge utile du malware, en exploitant un nouveau vecteur d'attaque » précise ainsi Flashpoint sur son blog.
La dernière déclinaison de Mirai n'exploite donc plus simplement Telnet pour tenter de se connecter à des objets connectés en utilisant les identifiants par défaut. Selon Flashpoint, celle-ci exploite des vulnérabilités connues au sein des protocoles TR-064 et TR-069, des protocoles de maintenance utilisés par les opérateurs. C'est grâce à cette faille que les opérateurs du réseau botnet sont parvenus à infecter plus de 900.000 routeurs livrés par Deutsche Telekom à ses clients. Mais selon Flashpoint, l'opérateur allemand n'est pas le seul à devoir s'inquiéter de ce type d'attaques. Flashpoint évoque ainsi le fait que des appareils infectés ont également été détectés au Brésil et en Grande-Bretagne. Selon Flashpoint, environ 5 millions de routeurs à travers le monde sont vulnérables à cette nouvelle variante.
Reste à déterminer l'origine de l'attaque contre l'opérateur. Flashpoint précise que les administrateurs de cette variante semblent être des habitués de Mirai, puisque le nouveau malware présente plusieurs points communs (notamment des serveurs de command and control) avec des Botnets déjà identifiés lors d'attaques précédentes effectuées grâce à Mirai.
Selon le journal allemand Tagesspiegel, les soupçons se tournent vers la Russie. Dans une prise de parole, la chancelière Angela Merkel s'est refusée à confirmer cette thèse, mais précise néanmoins que de nombreuses cyberattaques ont été constatées en Europe et appelle ses citoyens à s'habituer à ce type d'attaques. Cité par la presse locale, le directeur de l'équivalent allemand de l'Anssi, le BSI, évoque de son côté « le crime organisé » à l'origine de l'attaque, mais rappelle que l'attaque n'a pas fonctionné. Le malware a bien déconnecté les routeurs des abonnés, mais celui-ci n'est pas parvenu à s'installer correctement. Plus de peur que de mal donc…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs. Vous apprendre à vous protéger des pirates informatiques, vous accompagner dans votre mise en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles (RGPD). (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Deutsche Telekom : 5 millions de routeurs vulnérables au malware – ZDNet

---

Alerte : 1 million de comptes Google dérobés. Outil gratuit pour vérivier votre compte

Alerte : 1 million de comptes Google dérobés. Outil gratuit pour vérivier votre compte

---

Un logiciel malveillant, ou malware, nommé Gooligan, a infecté plus d'un million de téléphones fonctionnant sur Android et permis à des pirates de dérober les données d'autant de comptes Gmail, a révélé aujourd'hui la compagnie israélienne spécialisée en solutions de sécurité, Check Point.
«Grâce à ces informations, les agresseurs peuvent accéder aux données confidentielles des utilisateurs dans Gmail, Google Photos, Google Docs, Google Play, Google Drive et G Suite», précise la compagnie dans un communiqué.

13 000 appareils infectés chaque jour

Gooligan infecterait 13 000 appareils par jour, en ciblant les appareils sur Android 4 (Jelly Bean, KitKat) et 5 (Lollipop), soit 74% des appareils Android aujourd'hui en usage. C'est la première fois qu'une cyberattaque de ce genre parvient à toucher plus d'un million d'appareils.
Selon Check Point, environ 57% de ces appareils infectés sont situés en Asie et environ 9% en Europe.

Comment fonctionne ce malware ?
L'infection se produit lorsqu'un utilisateur télécharge puis installe une application infectée par *Gooligan* sur un appareil Android vulnérable, ou s'il clique sur des liens malveillants dans des messages de *phishing*. «Une fois que les agresseurs parviennent à prendre le contrôle d'un appareil, ils gênèrent des revenus frauduleux en installant des applications à partir de Google Play et en les évaluant au nom de la victime», explique Check Point.

Vérifier l'état de son compte en ligne

Prévenu par la société israélienne, Google aurait contacté les utilisateurs concernés pour «désinfecter» les appareils touchés et ajouter de nouvelles protections à sa technologie Verify Apps.

Check Point propose un outil en ligne gratuit permettant aux utilisateurs d'Android de vérifier si leur compte n'a pas été infecté par *Gooligan*.
[Lien vers l'outil gratuit en ligne]

Réagissez à cet article

Original de l’article mis en page : Cyberattaque : les données d’un million de comptes Google dérobées par Gooligan – Le Parisien