Comment se débarrasser d’un cryptovirus qui revient sans arrêt ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Comment se débarrasser d’un cryptovirus qui revient sans arrêt ?				

Vous vous êtes fait piéger par un Cryptovirus ? Après un bon nettoyage de l'ordinateur, vous avez réinstallé les fichiers perdus grâce à de précieuses sauvegardes. Cependant, quelques jours ou quelques semaines plus tard, vos fichiers sont à nouveau cryptés. Que faire ?

Que ça soit à la suite des nombreux défaçages de sites Internet (piratage du site Internet et changement de la page d'accueil) dont ont été victimes des dizaines de milliers de sites Internet en 2015 ou à la suite de vagues de virus cryptant la quasi totalité des données de votre ordinateur et vous demandant de payer une rançon pour continuer à les utiliser, nous avons été surpris par les mesures prises par le ou les informaticiens.
En effet, à la suite d'échanges avec ces pompiers informatiques afin de vérifier les mesures prises à la suite de l'attaque informatique, nous avons eu, et leurs clients également, la désagréable surprise que leurs actions se restreignaient à nettoyer le ou les postes infectés et restaurer la dernière sauvegarde. En d'autres termes, excepté pour ceux profitant de cette situation pour constater que leurs systèmes de sauvegardes parfois lourdement facturés ne fonctionnait pas ou ne sauvegardait pas tout, la quasi totalité des techniciens contactés nous ont confirmé que le grand changement dans leurs procédure à la suite d'une telle attaque de pirate, consistait à renforcer la vérification des procédures de sauvegarde !!!
Vous l'aurez compris, la conséquence évidente que si l'on ne soigne pas la cause du mal et qu'on ne fait qu'atténuer les effets, le mal reviendra.
Sauf à que ça vous plaise de passer votre temps de restaurer des données à chaque nouvelle attaque, il est peut-être temps de changer quelque chose.

En cas d'attaque par ransomware (cryptovirus), nous vous recommandons de vous former ou d'utiliser un spécialiste pour suivre les étapes suivantes (l'ordre peut être adapté en fonction de vos priorités) :

1. Payer ? nous ne recommandons pas ça car non seulement vous favorisez le développement de ces actes en récompensant les cybercriminels, mais également rien ne vous assure que vous pourrez récupérer l'utilisation de vos fichiers et enfin, même si vous payez et que vous en avez pour votre argent, il est fort probable que le même pirate ou un autre vous piège à nouveau.
2. Constatez et recueillez les preuves ;
3. Conservez les preuves soit pour une analyse ultérieure en vue de la recherche d'un antidote, soit pour une analyse approfondie de la technique utilisée par le pirate informatique, soit pour pouvoir porter plainte (si vous avez une assurance ou pour vous protéger si votre système informatique victime contamine d'autres systèmes informatique , ce qui vous rendraient responsable) ;
4. Éventuellement, portez plainte ;
5. Nettoyez votre système informatique de toutes traces du virus ;
6. Pour éviter qu'elle se reproduise, analysez avec précision l'attaque informatique afin de trouver la faille utilisée pour pénétrer votre système informatique en vue de sa réparation;
7. Restaurez les données pour pouvoir remettre en route son système informatique le plus rapidement possible ;
8. Recherchez la faille ;
9. Corrigez la faille ;
10. Recherchez d'autres failles ;
11. Par prévention, corrigez d'autres failles et augmentez vos mesures de sécurité ;
12. Contactez éventuellement les autorités compétentes (Police, Gendarmerie, OCLCTIC, BETFI, votre CERT, le CERTA, PHAROS…) ;

Denis JACOPINI, Expert Informatique assermenté, est spécialisé en cybercriminalité et en protection des données personnelles pourra vous accompagner pour chacune de ces étapes.
Contactez-nous
Vous êtes une société d'informatique démunie devant une situation spécifique, il n'y a aucun inconvénient à vous faire aider par un spécialiste en cybercriminalité. Nous pouvons également vous accompagner.

Remarque :
Certaines de ces étapes peuvent être longues et nécessiteront un accès à distance de votre installation.

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Un outil gratuit pour analyser et nettoyer votre ordinateur

Un outil gratuit pour analyser et nettoyer votre ordinateur

Avec plus de 40.000 visiteurs uniques par an, ESET Online Scanner apparaît comme l'un des outils gratuits les plus plébiscités par les internautes soucieux de leur sécurité. Fort de ce constat, ESET améliore son scanner basé sur le moteur d'analyse ThreatSense® permettant d'analyser et nettoyer son ordinateur sans contrainte d'installation logicielle.

Conçue pour être conviviale, cette dernière version devient complètement indépendante des navigateurs Internet. De plus, l'installation est désormais possible sans les droits d'administrateur, ce qui rend l'analyse et le nettoyage des ordinateurs contenant des logiciels malveillants encore plus simples.
ESET Online Scanner améliore l'élimination des logiciels malveillants, par l'ajout de ces nouvelles fonctions :
• **Analyse des emplacements de démarrage automatique** et du secteur d'amorçage pour les menaces cachées – choix de cette option dans setup / cibles d'analyse avancées
• **Nettoyage du registre système** – Supprime les traces des logiciels malveillants du registre système
• **Nettoyage après analyse lors du redémarrage** – Si nécessaire, ESET Online Scanner est capable de repérer les malwares les plus persistants afin de les nettoyer après redémarrage
Pour plus d'informations sur l'outil gratuit ESET Online Scanner, contactez-nous ou rendez-vous sur http://www.eset.com/fr/home/products/online-scanner/

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : Boîte de réception (10) – denis.jacopini@gmail.com – Gmail

52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois				

En France, 52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois. Elles étaient 48 % en 2019. Le coût moyen d'une attaque par rançongiciel est de 420 000 euros en dehors de la rançon exigée. Ce montant prend en compte les temps d'arrêt, la perte de chiffre d'affaires et les coûts opérationnels. En cas de paiement de la rançon, cette somme double.

LA CLÉ DE CHIFFREMENT N'EST PAS UNE SOLUTION MIRACLE

« *Les entreprises se sentent parfois sous pression pour payer la rançon afin d'éviter les temps d'arrêt préjudiciables. À première vue, effectuer le paiement de la rançon semble être une manière efficace de restaurer les données, mais ce n'est qu'illusoire (…) En effet, une simple clé de chiffrement n'est pas un remède miracle et il faut souvent bien plus pour restaurer les données*« , a expliqué Chester Wisniewski, Principal Research Scientist chez Sophos.

En France, plus de la moitié (61%) des responsables IT interrogés déclarent avoir pu restaurer leurs données à partir de sauvegardes sans payer la rançon. Dans 2 % de cas, le paiement de la rançon n'a pas permis de restaurer les données. À l'échelle mondiale, ce chiffre s'élève à 5 % pour les organisations du secteur public.

…[lire la suite]

Commentaire de notre Expert : Denis JACOPINI

La demande de rançon est la résultante dans la quasi totalité des cas de l'ouverture d'une pièce jointe à e-mail piégé ou le clic sur un lien aboutissant sur un site Internet piégé.

Les conséquences

Il n'est plus a rappeler qu'être victime d'un ransomware entraînent un arrêt de l'outil informatique, une perte de productivité et une dégradation de la réputation auprès des clients et partenaires.

Les solutions

Nous le répéterons jamais assez, les seuls moyens d'empêcher ce type de situation sont l'utilisations d'outils de filtrage et la sensibilisation. N'hésitez pas à nous contacter pour l'organisation de sessions de sensibilisation auprès de vos équipes pour leur apprendre à détecter e-mails et sites Internet malvéillants, en quasi totalité à l'origine des rançongiciels dans les systèmes informatiques.

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Source : *Etude : Payer la rançon multiplie par deux le coût total d'un ransomware*

Alerte ! Ces 42 applications du Play Store cachent un logiciel malveillant

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Alerte ! Ces 42 applications du Play Store cachent un logiciel malveillant				

Un malware Android a une nouvelle fois été repéré sur le Google Play Store. Les chercheurs d'ESET ont en effet trouvé la trace d'un agaçant logiciel publicitaire dans le code de 42 applications en apparence inoffensive. Pour éviter d'être repéré par Google ou par leurs victimes, le malware multiplie les astuces.

Depuis un peu plus d'un an, **un malware publicitaire baptisé Android/AdDisplay.Ashas** rôde sur le Google Play Store, rapporte Lukas Stefanko, expert en sécurité informatique chez Eset. Après enquête, les chercheurs ont repéré la présence du maliciel dans 42 applications Android. Au total, ces applications ont été téléchargées par 8 millions d'internautes….[lire la suite]

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :
Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?
Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par*

des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Source : *Malware Android : ces 42 applications du Play Store cachent un logiciel malveillant – PhonAndroid.com*

Envoyé spécial sur les Cyberattaques : les braqueurs de l’ombre – 14 décembre 2017 (France 2)

Envoyé spécial sur les Cyberattaques : les braqueurs de l’ombre – 14 décembre 2017 (France 2)

Les hold-up 2.0 par des « rançongiciels », logiciels de rançon, se multiplient : en France, une entreprise sur deux aurait déjà été piratée de cette façon. Enquête du magazine « Envoyé spécial » sur un fléau invisible en pleine explosion.

Merci à Clément Le Goff et Guillaume Beaufils pour ce beau travail d'enquête. Tout est vrai, et encore, tout n'est pas dit. Quelles conséquences avec les objets connectés, bientôt principaux cadeaux de noël, les voitures connectées, et tous les outils informatiques ou algorithmiques dont leurs usages peuvent être détournés à des fins malveillantes.

Depuis plusieurs années, Denis JACOPINI essaie par le biais de conférences ou en participant à des émissions de radio ou de TV (D8, LCI, NRJ12, Sud Radio, Sputnik…) de sensibiliser la population à ces risques afin de les aider à anticiper et éviter le plus possible ces attaques en leur apprenant à se protéger des pirates informatiques.
Avec un tel reportage, j'espère que le plus grand nombre de personnes sera sensibilisé de manière à enrayer ce phénomène incoercible.

Seul petit bémol dans ce reportage. Beaucoup auront entendu et retenu les recommandations de la police qui sont qu'il ne faut pas payer la rançon lorsqu'un pirate prend vos données en otage. Je compléterais par le fait qu'il ne faut pas payer si vous avez la possibilité d'utiliser des sauvegardes ou si les conséquences sont minimes. Par contre, si la vie d'une entreprise est en jeu et la seule chance restante (même infime) pour sauver l'entreprise est de payer la rançon, ne pas la payer risquerait bien de vous être reproché… à moins que ça soit, comme dans le reportage un coup de grâce accepté par désespoir.
Corriger le message afin de ne pas induire les entreprises en erreur me paraît indispensable.

Réagissez à cet article

Les hold-up 2.0 par des « rançongiciels », logiciels de rançon, se multiplient : en France, une entreprise sur deux aurait déjà été piratée de cette façon. Enquête du magazine « Envoyé spécial » sur un fléau invisible en pleine explosion.

Depuis plusieurs années, Denis JACOPINI essaie par le biais de conférences ou en participant à des émissions de radio ou de TV (D8, LCI, NRJ12, Sud Radio, Sputnik) de sensibiliser la population à ces risques afin de les aider à anticiper et éviter ces attaques.
Merci à *Clément Le Goff et Guillaume Beaufils*
Avec un tel reportage, j'espère que

Réagissez à cet article

De Britney Spears aux ambassades, ESET livre ses recherches sur le groupe Turla

	De Britney Spears aux ambassades, ESET livre ses recherches sur le groupe Turla

Il y a quelques mois, le groupe de cybercriminels Turla utilisait le compte Instagram® de Britney Spears pour mener des campagnes de cyberespionnage. ESET® est le premier éditeur à identifier et documenter leur nouvelle backdoor, nommée Gazer, visant principalement des institutions européennes. ESET publie un document complet d'analyse.

Qui est le groupe Turla

Groupe de cybercriminels menant des campagnes d'espionnage depuis plusieurs années, il **cible principalement les gouvernements européens et les ambassades.** Turla est connu pour mener des attaques dites de « point d'eau » (surveiller les habitudes de navigation de la victime) et des campagnes de spearphishing (e-mails infectés ciblés).

Les chercheurs d'ESET ont découvert **la backdoor Gazer sur nombre d'ordinateurs à travers le monde, mais principalement en Europe.** « Les techniques employées sont similaires aux précédentes campagnes menées par le groupe : une première porte dérobée s'installe par spearphishing, puis une seconde backdoor est envoyée sur le poste compromis. Il s'agit ici de Gazer », explique Jean-Ian Boutin, senior Malware Researcher chez ESET.

Détecter l'indétectable

Comme d'autres backdoors « second stage » avant elle (telles que Carbon et Kazuar), Gazer reçoit ses tâches au format chiffré à partir d'un serveur C&C. Ce dernier peut être une machine déjà infectée ou n'importe quelle autre machine en réseau. Le Groupe Turla utilise ses propres moyens de chiffrement reposant sur 3DES et RSA. L'analyse des clés RSA montre qu'elles contiennent la clé publique du serveur contrôlée par l'attaquant et une clé privée. Pour chaque échantillon analysé, ESET a découvert que les clés utilisées sont uniques et que tous les échanges avec le C&C sont chiffrés.

Architecture de la backdoor Gazer

Pour échapper à la détection et assurer sa persistance, les chercheurs ESET ont découvert que la menace utilisait un système de fichier virtuel dans le registre Windows. « Turla va très loin pour éviter d'être repéré. Le groupe supprime tout d'abord ses fichiers des systèmes compromis, puis change les chaînes et les indicateurs de compromission pour chaque version de leur backdoor. On note un certain sens de l'humour des cybercriminels qui **utilisent des références à des jeux vidéo dans leur code.** », poursuit Jean-Ian Boutin.

Pour plus de détails concernant la nouvelle backdoor employée par Turla, consultez WeLiveSecurity ou notre livre blanc. Nous restons à votre disposition pour plus de renseignements.

Réagissez à cet article

Source : *Boîte de réception (570) – denis.jacopini@gmail.com – Gmail*

Locky : un ransomware envoyé 23 millions de fois en 24 heures

Locky : un ransomware envoyé 23 millions de fois en 24 heures

En seulement 24 heures, 23 millions de mails contenant le ransomware Locky ont été envoyés à des internautes. Heureusement, les chercheurs en sécurité sont parvenus à freiner sa course avant qu'il ne soit trop tard.

Découvert en mars 2016, Locky est à l'origine un malware capable d'envoyer de fausses factures. Alors qu'on pensait que ce malware avait quasiment disparu, ce logiciel malveillant vient de refaire surface. Selon les chercheurs en sécurité d'Appriver, il s'agit de l'une des plus vastes campagnes de malware de 2017.

Rappelons que le début de l'année a été marqué par le terrifiant malware WannaCry. Autant dire que la barre était déjà haute, mais Locky a bien failli prendre une ampleur encore plus vaste. Le 28 août dernier, en seulement 24 heures, plus de 23 millions de mails contenant le malware ont été envoyés…[lire la suite]

Réagissez à cet article

Source : *Locky : un ransomware envoyé 23 millions de fois en 24 heures*

ESET attribue la cyberattaque Petya au groupe TeleBots

	ESET attribue la cyberattaque Petya au groupe TeleBots

Selon les experts ESET®, la cyberattaque dite « Petya » pourrait être attribuée au groupe TeleBots. Il existe des similitudes entre les nombreuses campagnes menées contre l'Ukraine, l'amélioration des outils utilisés par le cyber-groupe entre décembre 2016 et mars 2017 et la menace Diskoder.C (Petya).

« La cyberattaque de 2016 menée contre les institutions financières ainsi que le développement d'une version Linux du malware KillDisk par TeleBots, ont attiré l'attention des chercheurs ESET. En parallèle, le nombre croissant d'attaques contre les systèmes informatiques que connaît l'Ukraine **nous ont fait pointer du doigt le groupe TeleBots,** » déclare Anton Cherepanov, Senior malware researcher chez ESET.

Le mode opératoire du groupe TeleBots est l'utilisation systématique du malware KillDisk qui réécrit les extensions de fichiers des victimes. L'obtention d'une rançon n'est donc pas leur objectif principal, car les fichiers cibles ne sont pas chiffrés, mais réécrit. Si l'évolution du malware contient de nouvelles fonctions, comme le chiffrement ou l'ajout de leurs coordonnées, l'objectif de KillDisk n'est toujours pas de récolter de l'argent.

Entre janvier et mars 2017, TeleBots a compromis une société d'édition de logiciels en Ukraine, utilisant alors des tunnels VPN pour accéder aux réseaux internes de plusieurs institutions financières. Au cours de cette campagne, l**es cybercriminels ont utilisé tout un arsenal d'outils en Python, SysInternals PsExec et des logins de session Windows volés pour déployer un nouveau ransomware.** Il fut détecté par ESET comme Win32/Filecoder.NKH et fut suivi par une version pour Linux, détecté comme Python/Filecoder.R.

TeleBots a ensuite lancé un nouveau malware le 18 mai 2017 : Win32/Filecoder.AESNI.C (également appelée XData). C**e ransomware s'est principalement diffusé en Ukraine via une mise à jour du logiciel financier M.E.Doc, largement utilisé en Ukraine.** Selon le LiveGrid® d'ESET, le malware se déploie juste après l'exécution du logiciel, **ce qui lui permet de se répandre automatiquement à l'intérieur d'un réseau compromis.** Bien qu'ESET ait mis à la disposition un outil de déchiffrement pour la plateforme Windows®, cette attaque ne fut pas très médiatisée.

Le 27 juin 2017, l'épidémie de ransomwares de type Petya (Diskoder.C) ayant compromis de nombreux systèmes notamment en Ukraine, a permis de montrer **la capacité du malware à remplacer le MBR par son propre code malveillant, code qui a été emprunté au ransomware Win32/Diskoder.Petya :** c'est pourquoi certains chercheurs ont nommé cette menace ExPetr, PetrWrap, Petya ou NotPetya.

Cependant, contrairement au ransomware original Petya, **les auteurs de Diskcoder.C ont modifié le code MBR de telle sorte que la récupération de fichiers ne soit pas possible, malgré l'affichage des instructions de paiement.** Une fois le malware exécuté, **il tente de se propager à l'aide de l'exploit Eternablue, en s'aidant de la backdoor DoublePulsar.** Il s'agit de la même méthode utilisée par le ransomware WannaCry.

Le malware est également capable de se diffuser de la même manière que le ransomware Win32/Filecoder.AESNI.C (XData), en utilisant Mimikatz, pour obtenir des mots de passe, puis en exécutant SysInternals PsExec. En outre, les attaquants ont mis en place une troisième méthode de diffusion à l'aide d'un mécanisme WMI.

Ces trois méthodes ont été utilisées pour diffuser les ransomwares, cependant et contrairement à WannaCry, l'exploit EternalBlue utilisé par le malware Diskoder.C cible uniquement des ordinateurs ayant un adressage interne.

Lier TeleBots à cette activité permet de comprendre pourquoi les infections se sont étendues à d'autres pays que l'Ukraine. ESET a analysé les connexions VPN entre les employés, les clients et les partenaires mondiaux de l'éditeur ainsi que le système interne de messagerie et d'échange de documents. Tout cela a permis aux cybercriminels d'envoyer des messages aux victimes (spearphishing). Les pirates ayant eu accès au serveur légitime de mise à jour ont diffusé des mises à jour malveillantes automatiquement (aucune interaction avec l'utilisateur ne fut nécessaire).

« Avec une infiltration si poussée dans l'infrastructure de l'éditeur du logiciel M.E.Doc et de sa clientèle, les pirates disposaient des ressources nécessaires pour diffuser Diskoder.C. Bien qu'il y eut des dommages collatéraux, cette attaque a permis de démontrer la connaissance approfondie de leur cible par les pirates. D'autre part, **l'amélioration du kit d'exploit EternalBlue le rend encore plus sophistiqué, ce à quoi devront faire face les acteurs de la cybersécurité dans les prochaines années,** » conclut Anton Cherepanov.

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 d'expertises, d'audits, de formations et de sensibilisation 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

---

Réagissez à cet article

Source : *ESET*

Toutes les 4 secondes, un nouveau malware téléchargé

	Toutes les 4 secondes, un nouveau malware est téléchargé

Selon Check Point, les téléchargements de logiciels malveillants inconnus ont été multipliés par 9 dans les entreprises. La faute aux employés ?

Dans leur rapport de sécurité 2016, les chercheurs de Check Point ont analysé plus de 31 000 incidents cyber touchant plusieurs milliers d'entreprises dans le monde. Résultat des courses : les téléchargements de logiciels malveillants explosent dans les entreprises.
L'an dernier, les téléchargements de malwares encore « inconnus » des systèmes de sécurité d'organisations ont été multipliés par 9, passant de 106 à plus de 970 téléchargements par heure, selon Check Point. En moyenne, un nouveau programme malveillant inconnu est téléchargé toutes les quatre secondes. Et les employés sont présentés comme le maillon faible dans ce domaine.

Maillon faible

Les malwares « connus » font également des dégâts (un téléchargement toutes les 81 secondes en moyenne) lorsque les systèmes sont irrégulièrement mis à jour et que les correctifs de sécurité font défaut. Une variante d'un programme malveillant peut aussi confondre un antivirus, au risque d'exposer les systèmes et réseaux d'une entreprise à l'espionnage et au vol de données…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Un nouveau malware téléchargé toutes les 4 secondes

---

Comment se prémunir de la

cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?

	Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?

En pleine recrudescence, de nombreuses attaques ciblent les particuliers mais aussi les entreprises et les administrations. Elles visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants de connexion à des sites marchands, etc.). Hameçonnage (phishing) et «Rançongiciel» (ransomware) sont des exemples connus d'actes malveillants portant préjudices aux internautes. Pour s'en prémunir, des réflexes simples existent.

QUELS SONT LES DIFFÉRENTS TYPES D'ATTAQUES ?

Attaque par hameçonnage (phishing)

L'hameçonnage, phishing ou filoutage est une technique malveillante très courante sur Internet. L'objectif : opérer une usurpation d'identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel.

1. Le cybercriminel se « déguise » en un tiers de confiance (banques, administrations, fournisseurs d'accès à Internet…) et diffuse un mail frauduleux, ou contenant une pièce jointe piégée, à une large liste de contacts. Le mail invite les destinataires à mettre à jour leurs informations personnelles (et souvent bancaires) sur un site internet falsifié vers lequel ils sont redirigés.
2. La liste comprend un nombre si important de contacts et augmente les chances que l'un des destinataires se sente concerné par le message diffusé.
3. En un clic, il est redirigé vers le site falsifié qui va recueillir l'ensemble des informations qu'il renseigne.
4. Ces informations sont alors mises à disposition du cybercriminel qui n'a plus qu'à faire usage des identifiants, mots de passe ou données bancaires récupérées.

Voir la vidéo de la Hackacademy sur le phishing (CIGREF – partenariat ANSSI)

Pour s'en prémunir :

• N'ayez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
• Méfiez-vous des pièces jointes, elles pourraient être contaminées. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
• Ne répondez jamais à une demande d'informations confidentielles par mail.
• Passez votre souris au-dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français ou de la langue pratiquée par votre interlocuteur (ex : orthographe).

Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.

Attaque par «Rançongiciel» (ransomware)

Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus (ex : Locky, TeslaCrypt, Cryptolocker, etc.). L'objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

1. Le cybercriminel diffuse un mail qui contient des pièces jointes et / ou des liens piégés. Le corps du message contient un message correctement rédigé, parfois en français, qui demande de payer rapidement une facture par exemple.
2. En un clic, le logiciel est téléchargé sur l'ordinateur et commence à chiffrer les données personnelles : les documents bureautiques (.doc, .xls, .odf…etc), les photos, la musique, les vidéos…etc.
3. Les fichiers devenus inaccessibles, un message s'affiche pour réclamer le versement d'une rançon, payable en bitcoin ou via une carte prépayée, en échange de la clé de déchiffrement. Attention, rien n'indique que le déchiffreur en question soit efficace !

Pour s'en prémunir :

• N'ayez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
• Méfiez-vous des pièces jointes et des liens dans les messages dont la provenance est douteuse. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
• Effectuez des sauvegardes régulièrement sur des périphériques externes.
• Mettez à jour régulièrement tous vos principaux logiciels en privilégiant leur mise à jour automatique.

Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.

VOUS ÊTES VICTIME D'UN RANSOMWARE OU DE FISHING ?

Suite à une escroquerie ou une cyberattaque, déposez plainte auprès d'un service de **Police nationale** ou de **Gendarmerie nationale** ou bien adressez un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

Munissez-vous de tous les renseignements suivants :

• Références du (ou des) transfert(s) d'argent effectué(s)
• Références de la (ou des) personne(s) contactée(s): adresse de messagerie ou adresse postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels ou courriers échangés…
• Numéro complet de votre carte bancaire ayant servi au paiement, référence de votre banque et de votre compte, et copie du relevé de compte bancaire où apparaît le débit frauduleux
• Tout autre renseignement pouvant aider à l'identification de l'escroc

Vous pouvez également signaler les faits dont vous avez été victime via la plateforme de signalement « Pharos » ou le numéro dédié : 0811 02 02 17

Des services spécialisés se chargent ensuite de l'enquête :

• **Police nationale** : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui dépend de la Sous-direction de lutte contre la cybercriminalité (SDLC) : 01 47 44 97 55
• **Gendarmerie nationale** : le centre de lutte contre les criminalités numériques (C3N) du Service Central du Renseignement Criminel (SCRC) :cyber@gendarmerie.interieur.gouv.fr
• **Préfecture de police** : la Préfecture de police de Paris, de la Direction centrale du renseignement intérieur (DCRI) et ses équipes de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) compétente uniquement pour Paris et petite couronne (75, 92, 93 et 94) : 01 40 79 67 50

Article original de gouvernement.fr

Réagissez à cet article

Original de l'article mis en page : Cybercriminalité | Gouvernement.fr