

# Rapport 2017 sur la Cyber Sécurité de F-Secure



Rapport 2017 sur  
la Cyber  
Sécurité de F-  
Secure

**F-Secure vient de publier son Rapport 2017 sur la Cyber Sécurité qui décrit et analyse l'état actuel de la cyber sécurité dans le monde. Ce rapport s'attarde en particulier sur les problèmes que rencontrent les entreprises, dans un contexte où les pirates délaissent les malware conventionnels au profit d'attaques plus sophistiquées, et donc encore plus dangereuses.**

« Les menaces actuelles peuvent déjouer les approches unilatérales classiques de la sécurité, même les plus efficaces. En ayant recours au phishing (avec désormais des listes, vendues en ligne, de comptes ou réseaux pré-exposés) ou via d'autres méthodes, les pirates peuvent beaucoup plus facilement viser un gouvernement ou une entreprise du Fortune 500 », explique Sean Sullivan, Security Advisor chez F-Secure. « Nous vivons dans un monde post-malware, où le piratage s'est industrialisé. Et les cyber criminels ne comptent plus seulement sur les malware les plus communs pour se faire de l'argent. »

Ce rapport offre une analyse détaillée des problèmes majeurs diagnostiqués par les chercheurs et experts sur le plan de la cyber sécurité. Parmi les principaux résultats :

- Une grande partie du trafic de reconnaissance active en 2016 était liée à des adresses IP majoritairement situées dans 10 pays, et notamment la Russie, les Pays-Bas, les États-Unis, la Chine ou encore l'Allemagne.
- Les versions obsolètes d'Android sont de plus en plus nombreuses et rendent les appareils mobiles particulièrement exposés. L'Indonésie possède le nombre le plus important d'appareils Android non mis à jour, la Norvège, le plus faible.
- La plupart des cyber attaques font appel à des techniques basiques et s'en prennent à des infrastructures peu robustes.
- 197 nouvelles familles de ransomware ont été découvertes en 2016, contre seulement 44 en 2015.
- Le recours aux exploit kits a diminué au cours de 2016.

Ce rapport relate également les événements marquants et les tendances de l'année 2016. Au programme : des informations sur les botnets de type Mirai, sur les attaques préparées en amont, sur le cyber crime et sur les dernières tendances globales en matière de cyber menaces. Certaines organisations comme l'Autorité finlandaise de régulation des communication, le Virus Bulletin ou encore AV-Test, ont contribué à ce rapport à travers plusieurs articles...[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 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>



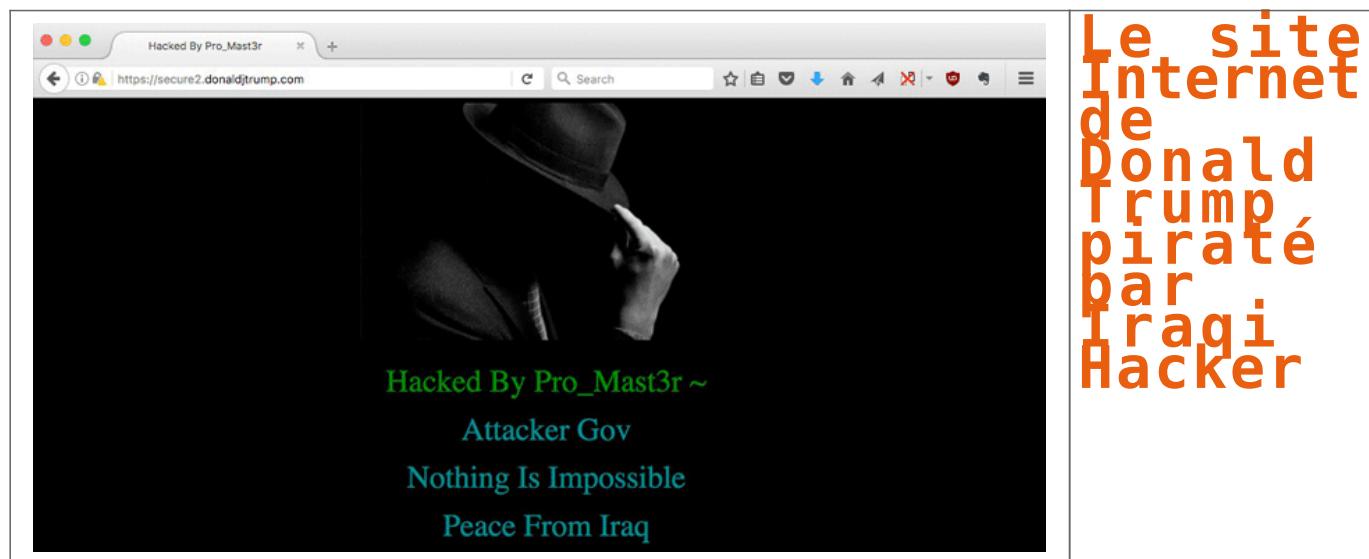
Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- 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.

Source : *Nouveau Rapport F-Secure sur la Cyber Sécurité : un monde « post-malware » – Global Security Mag Online*

---

# Le site Internet de Donald Trump piraté par Iraqi Hacker



**During the 2016 presidential election campaign, we reported about how insecure was the mail servers operated by the Trump organization that anyone with little knowledge of computers can expose almost everything about Trump and his campaign.**

Now, some unknown hackers calling themselves « Pro\_Mast3r » managed to deface an official website associated with President Donald Trump's presidential campaign fundraising on Sunday.

The hacker, claiming to be from Iraq, reportedly defaced the server, secure2.donaldjtrump.com, which is behind CloudFlare's content management system and security platform. The server appears to be an official Trump campaign server, reported Ars, as the certificate of the server is legitimate, « but a reference to an image on another site is insecure, prompting a warning on Chrome and Firefox that the connection is not secure. »

The defaced website displayed an image of a black hat man and included a text message, which reads:

Hacked by Pro\_Mast3r ~

Attacker Gov

Nothing Is Impossible

Peace From Iraq



...[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 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>



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 DRTF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *President Donald Trump's Website Hacked; Defaced By Iraqi Hacker*

---

# Ransomwares : Pourquoi les entreprises préfèrent-elles payer ?



Ransomwares :  
Pourquoi les  
entreprises  
préfèrent-elles  
payer ?

---

## **Le ransomware, 1ère menace informatique en Europe et « machine à cash » pour les cybercriminels : pourquoi les entreprises préfèrent-elles payer ? par Désirée Rodriguez**

Pour Europol (Rapport annuel cybercriminalité 2016), le « *ransomware est devenu la première menace en Europe* » et les faits vont empirer dans les mois et années à venir. Régis Bénard, consultant technique du spécialiste français Vade Secure (leader mondial des solutions de protection des boîtes de messagerie contre ce type de menaces) confirme cette tendance qui n'est pas prête de laisser sa place puisqu'encore aujourd'hui, et malgré une hausse de la sensibilisation, les entreprises préfèrent souvent payer plutôt que de perdre du temps... et de l'argent. C'est tout le dilemme du ransomware.

### **« Pour maximiser leurs profits, les cybercriminels innovent en permanence »**

Les cybercriminels sont organisés comme de vraies entreprises du crime numérique avec un accent très fort mis sur l'innovation pour maximiser leurs résultats.

Actuellement, Cerber est le ransomware le plus actif en France. Connue dans le monde entier, Cerber a notamment initié le concept du *ransomware-as-a-service*. L'idée est simple mais terriblement efficace : pour maximiser leurs profits, les cybercriminels proposent à des volontaires de diffuser le ransomware dans leur propre pays. Depuis 2016, Cerber est également une véritable entreprise du cybercrime avec un marketing quasi professionnel, un service après-vente qui propose d'accueillir les victimes pour les aider à payer leur rançon, etc.

### **« Locky, endormi ? Le ransomware le plus célèbre en France n'a pas fini de faire parler de lui »**

Le ransomware le plus présent en France en 2016, marque une pause. Mais l'accalmie ne va malheureusement pas durer. L'année dernière, Locky avait déjà connu des périodes d'absence quasi totale. Plusieurs raisons peuvent expliquer ce ralentissement de l'activité de Locky mais la plus évidente est que les cybercriminels travaillent à des évolutions sur leur ransomware. Il va donc revenir prochainement sous une autre forme et donc encore plus fort. Deuxième explication possible : les réseaux de PC ou objets connectés piratés (botnets) pour diffuser en masse les attaques de Locky, ne sont pas disponibles car loués à d'autres cybercriminels ».

### **« L'humain : la protection la plus efficace contre les attaques de phishing et ransomware »**

Les ransomwares sont véhiculés par des emails de phishing ou spear phishing (D'après le Gartner 65 % des attaques informatiques étaient initiées par un phishing en 2015 alors qu'une étude récente de PhishMe souligne la montée en puissance du phishing puisque 91% des attaques informatiques commencent aujourd'hui par du phishing). L'email est donc le canal prioritaire utilisé par les cybercriminels pour piéger les entreprises. Le problème est que l'humain est loin d'être infaillible : plusieurs études le rappellent régulièrement.

Les failles humaines peuvent ainsi aller jusqu'à mettre en péril une entreprise. Alors que le nombre de victimes continue d'augmenter, il est temps d'accélérer la résistance pour ne plus tomber dans le piège. Et pour mieux se protéger, l'éducation et la formation des utilisateurs sont des axes primordiaux pour que chacun prenne conscience des enjeux et des risques.

Pour les entreprises tout comme pour les pouvoirs publics, il s'agit d'organiser des réunions d'information régulières sur la sécurité, des formations sur le phishing, des recommandations sur le bon usage des réseaux sociaux, sur des conseils de bon sens, ou sur des bonnes pratiques à mettre en place : n'ouvrir les pièces jointes suspectes que si l'expéditeur est confirmé, supprimer le message d'un expéditeur suspect inconnu sans y répondre, etc...[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 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>



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 DRIEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Le ransomware, 1ère menace informatique en Europe et « machine à cash » pour les cybercriminels : pourquoi les entreprises préfèrent-elles payer ? – Globb Security FR*

---

# Cyberattaques des présidentielles. Qui serait responsable ?

Denis JACOPINI



vous informe

Cyberattaques  
des  
présidentielles,  
Qui serait  
responsables ?

**Les cyber-attaques que la Russie est soupçonnée de mener en France dans le cadre de la campagne présidentielle sont « une forme d'ingérence inacceptable », a estimé dimanche le ministre français des Affaires étrangères Jean-Marc Ayrault.**

» Les cyberattaques russes, grande menace pour les États-Unis et l'Europe

Dans une interview au *Journal du Dimanche*, le chef de la diplomatie française a déclaré : « Il suffit de regarder pour quels candidats, à savoir Marine Le Pen ou François Fillon, la Russie exprime des préférences, dans la campagne électorale française, alors qu'Emmanuel Macron, qui développe un discours très européen, subit des cyberattaques. Cette forme d'ingérence dans la vie démocratique française est inacceptable et je la dénonce ».

« La Russie est la première à rappeler que la non-ingérence dans les affaires intérieures est un principe cardinal de la vie internationale. Et je la comprends. Et bien la France n'acceptera pas, les Français n'accepteront pas qu'on leur dicte leurs choix », a ajouté le ministre.

#### **Quels éléments a-t-on pour de telles affirmations ?**

**Denis JACOPINI** : Aujourd'hui la Russie, hier la Chine et demain qui ? Quels sont les éléments permettant d'affirmer de tels propos ?

L'adresse IP ?

Si c'est l'adresse IP qui est prise en compte, n'est-on nous pas en train de mélanger l'adresse IP ayant accédé aux systèmes informatiques et celle du commanditaire de l'attaque ?

Signatures et codages de caractères

Si ce sont les signatures présentes dans les codes ou les codages de caractères qui sont pris en compte, ne risque t-on pas de reproduire l'attribution hâtive de l'attaque de la chaîne TV5 monde à l'Etat islamique alors même que très vite après l'attaque, de nombreux experts avaient mis en doute la crédibilité de la revendication.

A mon avis

En raison du refus de certains pays pour coopérer en matière de lutte contre la cybercriminalité, il devient très compliqué de remonter jusqu'aux ordinateurs utilisés pour mener de telles attaques, pire encore pour remonter jusqu'aux commanditaires des attaques informatiques. Les infos circulant encore ce matin font référence une fois de plus à des accusations qui sembleraient bien être sans preuve...

Malgré l'absence de preuve, Ayrault dénonce une «ingérence» de la Russie dans la présidentielle

**Je serais bien intéressé**

**En tant qu'Expert judiciaire spécialisé en cybercriminalité, je serais bien intéressé pour expertiser les éléments concernés par cette affaire.**

**A bon entendeur...**

Qu'en pensez-vous ? Merci de me laisser votre avis ou commentaire

---

**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>



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 DRTIEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Paris dénonce à nouveau les cyberattaques de Moscou*

---

# Des élèves de plus en plus confrontés au cyberharcèlement



Des élèves de plus en plus confrontés au cyberharcèlement

**Brimades, insultes, sexting (envoi de messages et photos explicites)... un adolescent sur six, en moyenne, est confronté au harcèlement. Un sujet qui reste pourtant tabou. L'école IESPP a décidé de prendre le problème à bras-le-corps et de lancer des ateliers de sensibilisation auprès de ses plus jeunes élèves.**

On sait à quel point les enfants peuvent être cruels entre eux... mais désormais, avec les réseaux sociaux et les smartphones, les conflits qui éclatent à l'école se poursuivent jusqu'à la maison : « *Ils sont tellement connectés H24 qu'il n'existe plus cette frontière, ce temps de répit le soir...[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 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>



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.



[Contactez-nous](#)



Réagissez à cet article

Source : *Des élèves de plus en plus confrontés au cyberharcèlement – Édition digitale de Charleroi*

# Ce malware aurait la capacité d'empoisonner l'eau potable d'une ville entière



Ce malware aurait la capacité d'empoisonner l'eau potable d'une ville entière

Des chercheurs en sécurité ont créé LogicLocker, un logiciel malveillant capable de bloquer une station d'épuration d'eau dans le but d'extorquer des rançons. Ce type d'attaque serait la prochaine étape dans le domaine des ransomwares.

Les ransomwares cryptographiques, qui chiffrent les données des utilisateurs pour extorquer une rançon, vous font peur ? Alors attendez de voir les « ransomwares industriels », qui s'attaquent aux systèmes de contrôle des usines. Ils vous feront basculer en mode panique, car ils pourraient avoir des conséquences directes et néfastes sur notre environnement physique. Pour l'instant, ce type de malware ne fait pas encore partie de l'arsenal des pirates, mais des chercheurs du Georgia Institute of Technology pensent que ce n'est qu'une question de temps, étant donné la faible sécurité des systèmes industriels. Pour montrer l'étendue de la menace, ils ont développé un prototype d'un tel ransomware et l'ont testé sur une maquette industrielle qui représente une station d'épuration d'eau d'une ville. Ils ont présenté leur travail cette semaine à l'occasion de la conférence RSA 2017, qui s'est tenue à San Francisco.

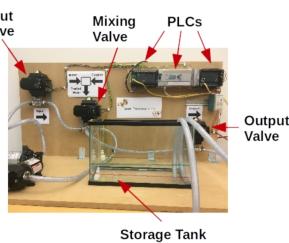


Fig. 2: Water Treatment Testbed

Baptisé LogicLocker, ce malware est capable d'infecter l'automate programmable industriel (programmable logic controller, PLC) qui régule la désinfection et le stockage de l'eau potable. L'attaque consiste à extraire le code exécutable de l'appareil et de le remplacer par un code malveillant, puis de changer le mot de passe d'accès. Ainsi, l'attaquant peut non seulement stopper le processus d'épuration, mais aussi empêcher les ingénieurs de réinstaller le code d'origine sur l'appareil. Le pirate peut alors envoyer aux responsables de la station d'épuration une demande de rançon doublée d'un ultimatum : s'ils ne payent pas au bout d'un certain temps, le code malveillant va surdosser le produit désinfectant et, du coup, rendre toute l'eau potable impropre à la consommation. Une fois la rançon payée, l'attaquant restitue le code volé.

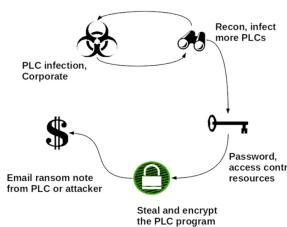


Fig. 3: General Flow of ICS Ransomware Attack

Un tel scénario est faisable dans n'importe quel domaine, à partir du moment où il y a des automates programmables connectées sur un réseau interne ou, carrément, sur Internet. Il suffit de se rendre sur le site Shodan.io pour constater qu'il existe d'ores et déjà des milliers de PLC accessibles par la Toile. Les chercheurs ont en trouvé d'emblée plus de 1400 de marque MicroLogix et 250 de marque Schneider Modicon.

#### Une question de profitabilité

Si les pirates n'ont pas encore exploité ce type d'attaque, ce n'est pas parce que ces automates sont bien sécurisés. Au contraire, leur manque de protection est notoire et connu depuis des années. « La seule explication est que les cybercriminels n'ont pas encore trouvé le business model qui leur permet d'opérer de manière profitable dans ce type d'environnement », estiment les chercheurs dans leur étude. En effet, le ransomware industriel nécessite plus de recherche et de connaissance. Par ailleurs, son mode opératoire est très pointu et ne peut donc faire qu'un faible nombre de victimes. C'est donc exactement l'inverse des cryptoransomwares, qui sont diffusés en masse auprès d'un large parc d'utilisateurs...[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 Cybercriminalité et en Protection des Données à Caractère Personnel.  
• Audits Sécurité (ISO 27001);  
• Expertises techniques et judiciaires (AVIS d'experts, expertises judiciaires téléphoniques, disques durs, e-mails, conteneurs, débrouillages de identité, etc.)  
• Expertises de systèmes de vote électronique ;  
• Formations et conférences en cybercriminalité ;  
(Autorisation de la DDESTI n°70 84 03041 84)  
• Formation du C.I.L. (Correspondants Informatique et Libertés);  
• Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Source : *Ce malware pourrait empoisonner l'eau potable d'une ville entière*

# Popcorn Time, un rançongiciel bien vicieux

# Popcorn Time, un rancônciciel 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 destinataires 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 règlement 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.



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 où 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 de 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, nappelez 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 règlement 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.

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

---

# De nouveaux malwares superfurtifs se cachent dans la mémoire des serveurs



De  
nouveaux  
malwares  
super  
furtifs  
se  
cachent  
dans la  
mémoire  
des  
serveurs

Kaspersky met en évidence une souche malveillante qui se cache dans la mémoire des systèmes et exploite des applications de confiance pour dérober des données. 10 organisations au moins en ont été victimes en France.

Une nouvelle espèce de logiciels malveillants, mise en évidence par Kaspersky Lab, ressemble bien à un cauchemar pour administrateurs système et responsables informatiques. Il s'agit d'une forme de malware utilisant des logiciels légitimes (comme l'outil de tests de pénétration Meterpreter) pour infecter un système, avant de détourner des services Windows couramment utilisés pour assurer son implémentation et son fonctionnement. Une fois le malware en cours d'exécution à l'intérieur de Windows, il efface toute trace de son existence et réside dans la mémoire du serveur. Le temps d'exfiltrer des informations qu'il convoite avant de s'effacer de lui-même.

Parce que ces nouveaux malwares, que Kaspersky a baptisés MEM: Trojan.win32.cometer et MEM: Trojan.win32.metasploit, résident en mémoire, ils ne peuvent pas être détectés par des antivirus standards, qui analysent le disque dur d'un ordinateur. En outre, le malware se cache en réalité à l'intérieur d'autres applications, ce qui le rend pratiquement invisible également des outils utilisant des techniques de listes blanches, comme c'est le cas de nombreux pare-feu.

## **Le redémarrage efface toute trace**

Selon un billet de Kaspersky sur le blog Securelist, le processus fonctionne en plaçant temporairement un utilitaire d'installation sur le disque dur de l'ordinateur. C'est ce petit outil qui loge le logiciel malveillant directement en mémoire en utilisant un fichier MSI standard de Windows avant d'effacer l'utilitaire. Une fois que le malware commence à collecter les données ciblées, il emploie une adresse de port inhabituelle (:4444) comme voie d'exfiltration.

L'ensemble de ces caractéristiques rendent ces malwares très furtifs. Car ils n'existent que dans la mémoire d'un ordinateur, ce qui signifie qu'un logiciel anti-malware n'a une chance d'identifier l'infection que lors d'une analyse de ladite mémoire, et uniquement pendant que le malware est toujours actif. Le redémarrage de l'ordinateur effacera toute trace, rendant inutile toute analyse 'forensic'.

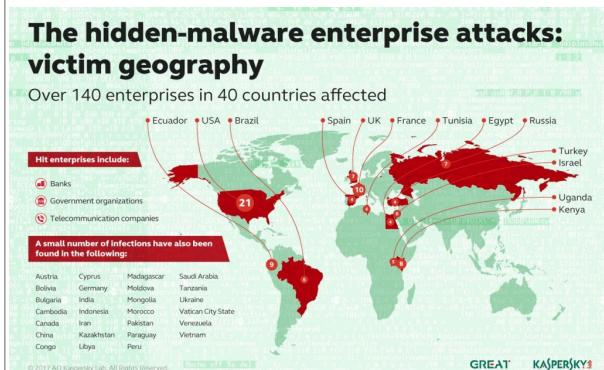
## PowerShell détourné

Kurt Baumgartner, chercheur au sein des Kaspersky Lab, explique que ses équipes de recherche ont d'abord trouvé ce logiciel malveillant dans une banque en Russie. L'équipe a pu accéder au serveur, dans ce cas un contrôleur de domaine, avant que le système ne redémarre, ce qui leur a permis d'isoler la souche infectieuse. L'équipe de Kaspersky a alors constaté que les attaquants utilisaient un script PowerShell pour installer un service malveillant dans la base de registre de l'ordinateur.

Selon le chercheur, si ce malware furtif échappera aux antivirus qui cherchent des signatures sur le disque dur d'un ordinateur, il peut toujours être découvert via des logiciels de protection qui traqueront ses activités suspectes : création de tunnels de communication chiffrée pour exfiltrer les données, démarrage de services ou lancement de l'activité PowerShell. Kurt Baumgartner assure que ses équipes suivent l'évolution du malware – qui devrait muter pour échapper aux défenses qui vont être mises en œuvre suite à la publication de Kaspersky – et qu'il convient notamment de surveiller la diffusion de données à partir de lieux différents sur le réseau utilisant le tunnel de communication caractéristique de la souche.

## **La France, second pays ciblé**

Et de conseiller aux équipes de sécurité de scruter les journaux système et de surveiller le trafic sortant du réseau. Tout en précisant qu'il vaut mieux stocker ces données hors ligne de sorte que le logiciel malveillant ne puisse pas trouver et effacer ces preuves. Autre astuce pour contrarier les assaillants : désactiver PowerShell. Une solution radicale mais parfois difficile à mettre en œuvre, de nombreux administrateurs ayant recours à cet utilitaire...[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 règlement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINET 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 (RGPD).

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, contenueurs, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRIET n°93 84 03041 BH)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de

**Le Net Expert**  
**INFORMATIQUE**  
Cybersécurité & Conformité

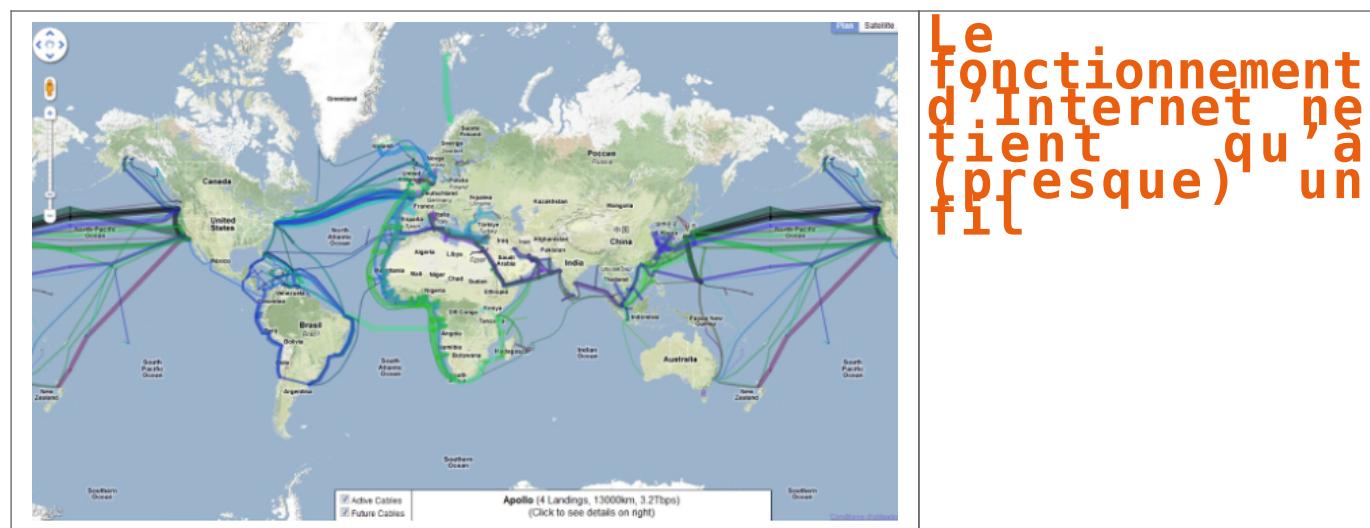
Contactez nous

Réagissez à cet article

Original de l'article mis en page : Anatomie du malware super furtif, caché dans la mémoire des serveurs

---

# Le fonctionnement d'Internet ne tient qu'à (presque) un fil





Original de l'article mis en page : « Qui a le savoir, a le pouvoir »: Les câbles sous-marins, le maillon faible de la cyberguerre