GENERAL
Actualité du jour
Lettres d'information
Recommander ce site
Signaler un incident
Nous écrire

VIRUS
Alertes virus
Dossiers virus
Alertes par email
Antivirus gratuits
Antivirus en ligne
Désinfection
FAQ virus

PROTECTION
Alertes sécurité
Dossier firewall
Alertes par email
Firewalls gratuits
Scanner de ports
Antirootkits gratuits
Traceur IP/domaine
Windows Update
FAQ sécurité

PHISHING
Alertes phishing
Logiciels antiphishing
FAQ phishing

SPAM
Dossier spammning
Logiciels antispam
FAQ spam

VIE PRIVEE
Paiements en ligne
Dossier spywares
Antispywares gratuits
Vos traces sur le Net
FAQ vie privée

HOAX
Alertes hoax
Dossier hoax
Dossier viroax
Antihoax en ligne
FAQ hoax

NEWSLETTER
Recevez chaque semaine la lettre de Secuser.com :
email
Ok

DOSSIER

Dossier précédent | Archives dossiers | Dossier suivant

PUBLICITE

Entretien avec alcopaul, auteur du virus Perrun

Propos recueillis et traduits par Emmanuel JUD (21/06/02)

Perrun est un pseudo virus JPEG qui a défrayé la chronique en juin 2002 grâce au coup de projeteur d'un éditeur d'antivirus, largement amplifié et déformé par les médias. Son auteur, un certain alcopaul, revient avec passion et excès sur son virus, ainsi que sur ses motivations, ses habitudes, ses relations avec les éditeurs d'antivirus et sur les nouvelles tendances en matière d'infection. Portait d'un créateur de virus avide de reconnaissance et d'un système qui favorise encore trop souvent le sensationnalisme.

Emmanuel JUD : Qui est alcopaul?
alcopaul : J'ai 21 ans, je vis aux Philippines dans une province du nord de Manille, j'aime le reggae, la musique ska et punk, ma famille et mes amis. Je suis étudiant dans une université d'Etat de ma province et prépare une licence en ingénierie électrique. J'ai récemment rompu avec ma petite amie et suis actuellement à la recherche d'une nouvelle...

Une raison particulière d'avoir choisi alcopaul comme pseudo?
Autrefois j'étais alcoolique.... alco et Paul, qui est mon prénom... alcopaul.

Depuis combien de temps vous intéressez-vous aux virus et à la conception de virus?
Je m'intéresse aux virus depuis 1997. J'ai conçu mon premier ver en décembre 2001.

Avez-vous créé d'autres virus avant Perrun?
W32.Alcarys et ses variantes, quelques VBS dont Bimorph et des Batch (Redirect, Jerm, etc.). La plupart sont des vers et quelques uns sont destructifs (file overwriters). Perrun est mon premier infecteur de fichiers et par chance je l'ai conçu pour infecter non pas des exécutables mais un type de fichiers de données *[NDEJ : alcopaul considère que modifier un fichier pour y insérer une portion de code viral est une infection même si le fichier modifié ne peut pas contaminer un ordinateur sain]*. J'ai simplement commencé par JPEG et le battage médiatique qui allait avec... J'ai envoyé aux éditeurs d'antivirus une version de Perrun qui infecte les fichiers *.TXT présents dans son répertoire.

Pourquoi créez-vous des virus?
Exercice intellectuel... Pour que les autres soient conscients que les ordinateurs sont en danger et mettent à profit cette prise de conscience pour lutter contre les virus et autres malwares.

Et pourquoi avoir créé Perrun en particulier?
J'ai écrit une chanson pour mon ex-copine intitulée "ton baiser, ton amour et quelques images" qui est la raison pour laquelle l'article "Infection des images : une approche désespérée" a ensuite été écrit. J'ai conçu Perrun pour fabriquer une preuve fonctionnelle des idées présentées dans l'article. Après avoir terminé Perrun, des idées me sont venues à propos des dangers d'un concept de virus comme Perrun donc j'ai écrit un autre article : "Les dangers des techniques utilisées par W32/Perrun". C'est une sorte de prédiction des implications de mon virus pour décrire les méthodes qui pourront être utilisées par des personnes malveillantes pour de futures attaques.

Quelles ont été les étapes de la création de Perrun?
C'est un secret pour l'instant... Mais le virus a été écrit en Visual Basic 6... Après avoir terminé l'article, ça m'a pris un jour pour conceptualiser (le 12 juin 2002) et 4 heures pour coder le virus (le 13 juin). Je l'ai alors envoyé aux éditeurs d'antivirus, puis McAfee a fait un battage médiatique du tonnerre :-)

Comme vous le savez, un virus est un programme capable de se reproduire identique à lui-même pour se propager. Ni votre fichier PROOF.EXE, ni le fichier extracteur, ni l'image JPEG modifiée ne peuvent s'autoreproduire, donc Perrun est-il un virus?
Perrun n'est pas votre virus traditionnel... C'est un virus dans le sens où une fois que l'extracteur est installé sur votre ordinateur, l'infection par une image JPEG peut se produire. Mais beaucoup de puristes considèrent que Perrun est un pseudo virus... C'est un nouveau concept de virus/extracteur, pas la vieille école *[NDEJ : cette vision est propre à l'auteur. L'extracteur étant capable d'extraire tout code exécutable caché dans un fichier de données, il s'agit en réalité d'un concept "code exécutable caché/extracteur", donc d'un troyen]*. La probabilité que la technique soit implémentée à grande échelle est faible, mais si Microsoft fait quelques modifications tsk tsk tsk...

Perrun ne peut pas permettre à une image de contaminer un ordinateur sain mais modifie un ordinateur pour qu'il puisse être contaminé par une image inoffensive mais contenant une portion de code viral caché, donc Perrun est-il vraiment un virus JPEG?
Le virus cible les fichiers JPEG... Quand un virus cible un type de fichiers, on appelle ça un virus... Le virus qui ciblait les fichiers SWF a été appelé virus SWF. Mais peut-être est-ce une lubie des médias...

RECHERCHE
Recherchez un mot-clé dans le site Secuser.com :
Ok

LIENS AMIS
Hoaxkiller.fr
Ne vous laissez plus piéger par les fausses informations qui envahissent le Net.
Inoculer.com
Annuaire de logiciels gratuits pour protéger votre ordinateur.

LFM.926 (le virus SWF en question) est un virus parce que la simple visualisation de l'animation SWF contaminée avec un Player Flash infecte réellement les autres fichiers SWF et donc propage le virus.
Les fichiers .SWF contiennent des instructions vulnérables à l'infection par un virus... Certains fichiers de données comme JPEG sont sûrs... J'ai simplement montré comment une infection de fichier JPEG était possible. C'est une sorte de force brute, en fait...

Votre virus a fait les gros titres des médias en France et probablement dans le monde entier. Qu'est-ce que cela vous fait?
Honnêtement, j'ai eu un moment de vrai bonheur, mais quand j'ai pensé que d'autres internautes ne comprendraient pas le but de mon travail et pourraient croire à la fin des échanges de photos sur le Net je me suis senti coupable. Je remercie ceux qui informent les utilisateurs du caractère non destructif de mon virus. Il a simplement été conçu pour valider un concept et laisser entrevoir des possibilités.

Quelles sont vos relations avec McAfee et les autres éditeurs d'antivirus?
McAfee et les éditeurs d'antivirus sont comme les Oscars ou n'importe quelle récompense qui nourrit la scène des concepteurs de virus (virus scene). Une fois que votre virus ou autre création figure dans leurs descriptions, vous vous sentez reconnu pour le talent que vous avez. Mais personnellement, je n'ai aucune relation avec eux. McAfee et les autres ne m'ont rien offert comme récompense... Sauf la renommée... :-)

Votre virus a offert une énorme campagne de presse à une multinationale. Etait-ce le prix à payer pour un moment de célébrité?
Je n'étais déjà plus une personne anonyme. Mon vrai nom a été posté sur le Net et tout le monde sait qui est alcopaul. Mais c'est agréable. On ne vit qu'une fois en ce bas monde, et j'ai laissé une trace...

Sincèrement, continuerez-vous à concevoir des virus si personne ne parlerait de vous ou de vos créations?
Oui... J'ai juste eu beaucoup de chance que mon virus fasse la une des magazines.

Que dites-vous à ceux qui pense que Perrun n'est pas un virus important?
Il est important car il remet complètement en question la gamme de types de fichiers qu'un virus peut infecter. Et c'est un nouveau concept de virus/extracteur.

Les images modifiées et éventuellement propagées par un virus de type Perrun ne peuvent pas contaminer un ordinateur sain, si un des deux composants du virus n'est pas ouvert (du fait de l'utilisateur, parce que le cache du navigateur est régulièrement vidé, etc.) il ne peut pas y avoir de contamination, si le fichier extracteur est neutralisé par un antivirus toutes les images modifiées compatibles restent sans effet, etc. Vous décrivez des scénarios catastrophiques à propos de Perrun, mais en fait ce type de virus n'est-il pas plutôt une chance pour les internautes, parce qu'il est condamné à être moins efficace que les virus traditionnels?
Le danger est lié à la dormance du code infectieux. Imaginez des gens qui téléchargent, visualisent ou enregistrent des images contenant du code viral et qu'un fichier extracteur arrive par le biais d'un logiciel piégé, d'un shareware, d'un email, d'une disquette... Ca serait comme une bombe à retardement.

Même si un utilisateur est infecté après avoir téléchargé une image modifiée contenant du code viral et le fichier extracteur correspondant, le résultat aurait été identique si au lieu du fichier extracteur le même utilisateur avait téléchargé et exécuté un virus traditionnel, donc où est le progrès?
(pas de réponse)

Vous évoquez une infection directe par le biais d'un navigateur consultant une page web contenant des images, mais votre concept-virus ne démontre rien sur ce point. Les navigateurs intègrent leur propre visualisateur d'images, donc dans votre hypothèse il faudrait modifier le code du navigateur, ce qui est largement plus compliqué que de changer le visualisateur JPEG de Windows, non?
Peut-être que des concepteurs de virus ou des hackers dans le futur trouveront des moyens de piéger un logiciel et d'inclure une routine qui agisse comme un extracteur. C'est une possibilité. Ou peut-être que Microsoft fera cela pour doper les ventes des éditeurs d'antivirus...

Si un virus de type Perrun se répand, même les utilisateurs qui n'ouvrent pas les pièces jointes exécutables et qui appliquent régulièrement les correctifs de leurs logiciels auront besoin d'un antivirus simplement pour nettoyer les images et être sûre de ne pas perdre bêtement de l'espace disque avec des fichiers inoffensifs mais contenant peut-être une portion de code virale. Etes-vous sûr de ne pas travailler pour les éditeurs d'antivirus?
Perrun était juste une preuve bénigne de mon concept, je ne travaille pour personne... Mais ils ont très justement attribué à ma création un faible niveau de risque. J'aurais été furieux s'ils l'avaient qualifié de haut-risque-super-dangereux-c'est-la-fin-des-échanges-de-photos-sur-le-web. Tout cela est du battage médiatique, Perrun en lui-même n'est pas une menace.

La mise à jour d'un malware lors de la visualisation d'une image est également moins efficace qu'un moyen traditionnel via par exemple un canal IRC étant donné qu'il n'y a pas de connexion active de la part du malware donc que ce dernier doit compter sur le hasard pour rencontrer une image contenant du code viral; cependant c'est original. N'est-ce pas là la seule innovation de Perrun?
C'est la seule innovation à laquelle j'ai pensé à ce moment. Peut-être que je penserai à d'autres plus tard...

Sur votre site web vous expliquez comment créer un virus, comment désactiver un antivirus et proposez de télécharger Perrun. Est-ce vraiment responsable?
L'ignorance est un danger... La prise de conscience est une protection...

Que pensez-vous de ceux qui répandent des virus sur le web?
ils doivent être punis pour les dommages causés par leurs virus.

Les virus informatiques sont surtout dangereux pour les internautes débutants et ceux qui n'ont pas les moyens d'acheter un antivirus. Les virus et autres actes de cybercriminalité permettent également aux gouvernements de justifier la mise en place de lois toujours plus intrusives pour la vie privée. En êtes-vous bien conscient?
Oui... Je ne lâche jamais mes créations sur le web... Je suis sûr de moi et je n'ai peur de rien...

Vous êtes peut-être sûr de vous mais les lois invasives pour la vie privée concernent l'ensemble des internautes, donc ne pensez-vous pas que votre activité contribue à la restriction des libertés sur le web?
Parfois les dangers sont nécessaires pour rendre les choses plus sûres. Et plus les lois apportent de la sécurité, plus vous avez conscience de l'attention que vous portent les législateurs...

Lorsque des internautes sont infectés par un virus, pensez-vous que c'est bien fait pour eux, êtes-vous désolé pour eux ou pensez-vous que ça n'est pas votre problème?
Faire des choses responsables est plutôt mon truc... Si je lâchais mes virus sur le web, je me sentirais assurément coupable... Si certains sont infectés par des virus, je suis désolé pour eux.

Qu'est-ce qui pourrait vous décider d'arrêter de créer des virus?
Lorsque je ne me sentirai plus créatif et si j'ai de plus agréables opportunités vers lesquelles orienter ma créativité.

Comment avez-vous appris à créer des virus?
Avec des livres et avec des didacticiels présents sur le Net.

Quel(s) langage(s) et quel(s) logiciel(s) utilisez-vous pour cela?
Microsoft Visual Basic 6, programmation Batch, VBScript.

Quel est votre antivirus favori?
Aucun... Les antivirus consomment des ressources système.

Combien de temps consacrez-vous aux virus?
En moyenne, 3 heures par jour...

Etes-vous en contact avec d'autres concepteurs de virus?
Oui, pour chatter et pour parler de conception de virus...

Que pensent les autres concepteurs de virus à propos de Perrun? Considèrent-ils vraiment Perrun comme un virus JPEG?
La plupart, je pense, ne reconnaissent pas Perrun comme étant un virus JPEG, mais comme un virus multicomposant qui cible les fichiers JPEG.

Selon vous, quelles seront les nouvelles tendances en matière de virus?
Virus multicomposant, infection simultanée de tous les types de fichiers, virus capable de modifier le fonctionnement des logiciels, infection multiplate-forme,...

Quels sont vos projets maintenant?
De nouvelles techniques d'infection en Visual Basic 6.

Une dernière chose à ajouter?
Imaginez que Microsoft intègre la technique de mon virus comme fonctionnalité de son navigateur pour rendre facile l'exécution de certaines tâches... Ce serait alors très alarmant. De nouvelles générations de virus émergeraient. En tout cas, Perrun n'a jamais été créé pour répandre la peur... Son but était de nous faire prendre conscience.

Depuis cet entretien, le virus Perrun n'est plus disponible en téléchargement sur le site de son auteur, de même que les articles techniques cités.

LIEN UTILE :

- Fiche du virus Perrun avec l'analyse du virus et ses risques réels
- Dossier Secuser : virus