

MARC BLANCHARD VIRUS DOCTEUR

Pourquoi autorunner.5555 alias Confiker - Kido est un fléau?

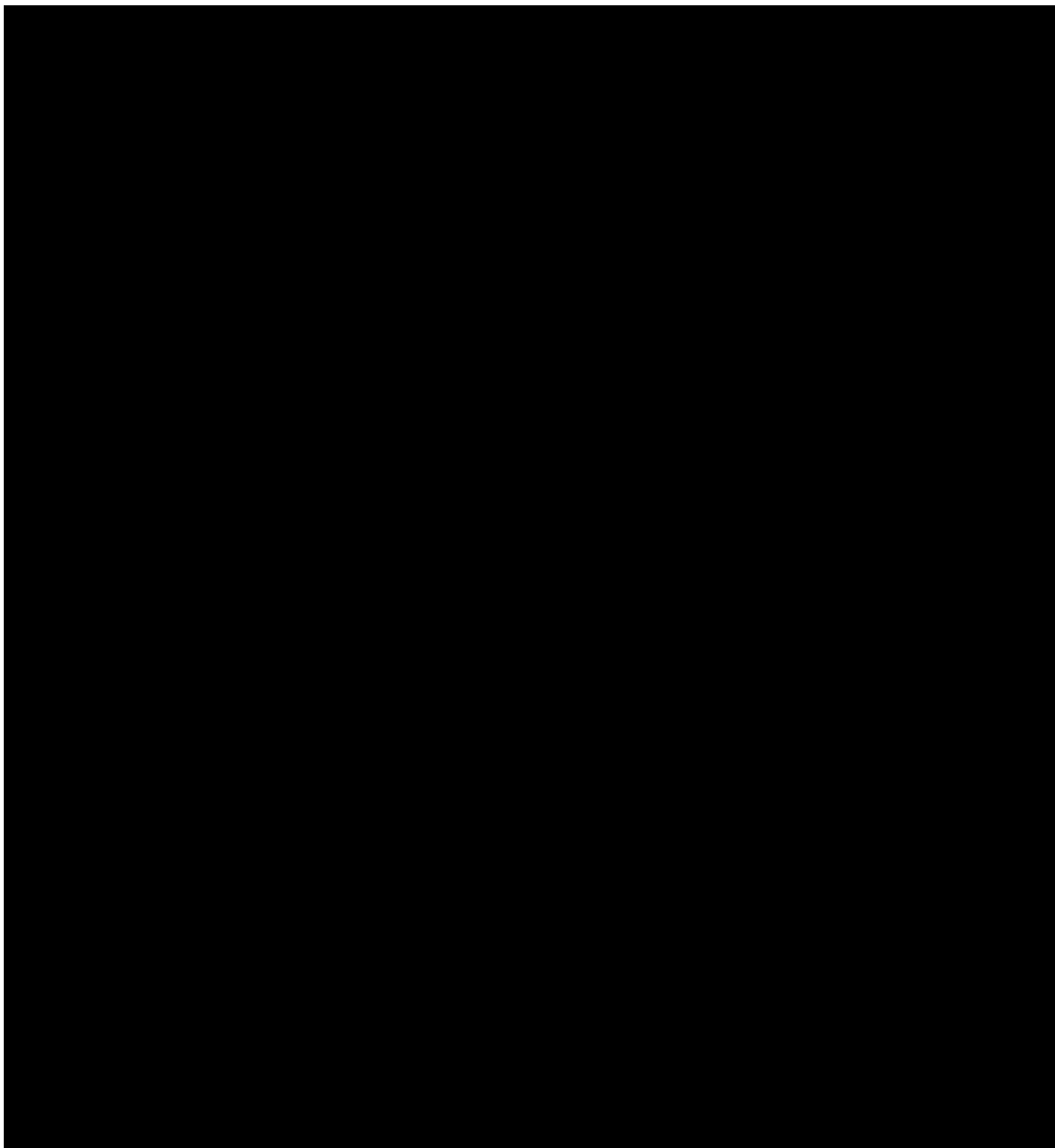
2009 commence avec une infection dite fulgurante avec Autorunner.5555 alias confiker / kido / Worm_DOWNAD.

Ce storm worm utilise toutes les technologies les plus récentes, en utilisant, entre autres, les compétences transversales, complexifiant ainsi ses méthodes de propagations, mais également ses méthodes d'infections.

Son action est en train de servir pour l'ouverture d'un réseau parallelezombie de grande ampleur.

Pour des informations sur les réseaux parallèles zombies un peu moins scientifiques, j'avais été interviewé par TiVi Pro à ce sujet: Voir la Vidéo cliquer ici !

Voici le phontype de Autorunner.5555 alias confiker



Rapport :

OPERATING SYSTEM : OS XP OS WIN 2000 WKS OS WIN 2003 SRV OS WIN VISTA

COMMENTAIRES ANALYSTE INFECTION PAR AUTORUNNER.5555 LES CLIENTS
SUBISSENT UNE INFECTION HAUTEMENT EMERGENTE

PRODUIT DE NETTOYAGE :DRWEB CUREIT

COMMENTAIRES ANALYSTE LE CLIENT NE POSSEDANT PAS D'ANTIVIRUS RESIDENT NE STOPPANT PAS LE STORM, L'INFECTION BOUCLE CAR NOTION DE MACHINES INFECTANTES ET MACHINES INFECTEES PAR REBOND

IDENTITE EGENE : AUTORUNNER.5555

CLASSIFICATION EGENE : WORM A EMERGENCE RAPIDE DUE A DES TECHNIQUES DE STORM

HOTFIX NECESSAIRE : MS-08-067 MS-08-068

TECHNOLOGIE EGENE : PROXY-DOWNLOADER VULNERABILITE OS BACKDOOR BOTNET MULTI THREADING WORM PROCESS MUTEX DOWNLOAD EXPLOIT POLYMORPHE CODE MODULAIRE SCANNER DE PORTS ZOMBIE INTEGRATION NETWORK AUTORUNNER

PROPAGATION HAUTEMENT EMERGENTE

Commentaires :

Le probleme est que si sur la machine infectée on bloque le port 445, le storm essaie via les compétences transversales d'autres ports.

On a constater des refus de connexion sur les sites de mises a jour des antivirus, mais également un refus de mise a jour automatique de Windows Update (normal le storm est grandement freiné par l'application des patchs MS-08-067 et 068), pour se relancer, il peut utiliser également les commandes AT, qui correspondent au planificateur de tâches.

Concernant le nettoyage : Le nettoyage est fastidieux car il doit etre tres rigoureux.

Dans un premier temps, s'assurer que le résident temps reel de l'antivirus bloque bien la tentative d'infection venant d'une autre machine.

Deuxieme temps, s'assurer que le nettoyage est bien fait, et qu'il ne reste aucune trace.

Troisieme temps, patcher avec MS-08-067 et 068

Quatrieme temps, redemarrer la machine

Cinquieme temps, verifier les regles de parefeux qui ont du etre modifiée par le storm worm quelque soit votre parefeu logiciel.

Sixiemement, rescanner avec un scannerex:CureIt pour etre sur de la non presence entre toutes ces manipulations du storm

Septiemement, bien redemarrer la machine apres le scan du point 6.

NOTA : Ce storm est hautement polymorphe due a ses modifications de codes en temps reel

(infections actives)

Par conséquent, il est possible qu'après nettoyage complet, l'antivirus réagisse de nouveau. C'EST NORMAL !!! Il s'agit en fait qu'une autre machine infectée sur le réseau tente une infection, faisant ainsi réagir le temps réel de l'antivirus....mais si votre antivirus est efficace, aucune infection devrait apparaître dans la machine nettoyée.

Commentaires

2009-01-22 20:43:28 - la mouche

Merci pour votre explication, votre procedure fonctionne à merveille.
Par contre ma clef usb est infectée et cureit me l'a bien nettoyée

Norbert

2009-02-03 16:48:57 - Fill

Bonjour, il y a aussi cet article intéressant qui permet de cibler les entrées touchées par l'infection :
support.microsoft.com/kb/...

2009-02-09 13:37:59 - Azura - topic@gmail.com

Le problème, c'est une décision grave et il doit être globale. J'aime votre façon de résoudre le problème.

Copyright : Blanchard [Virus Docteur] Marc - 2009-01-22 18:44:58
Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- * de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>