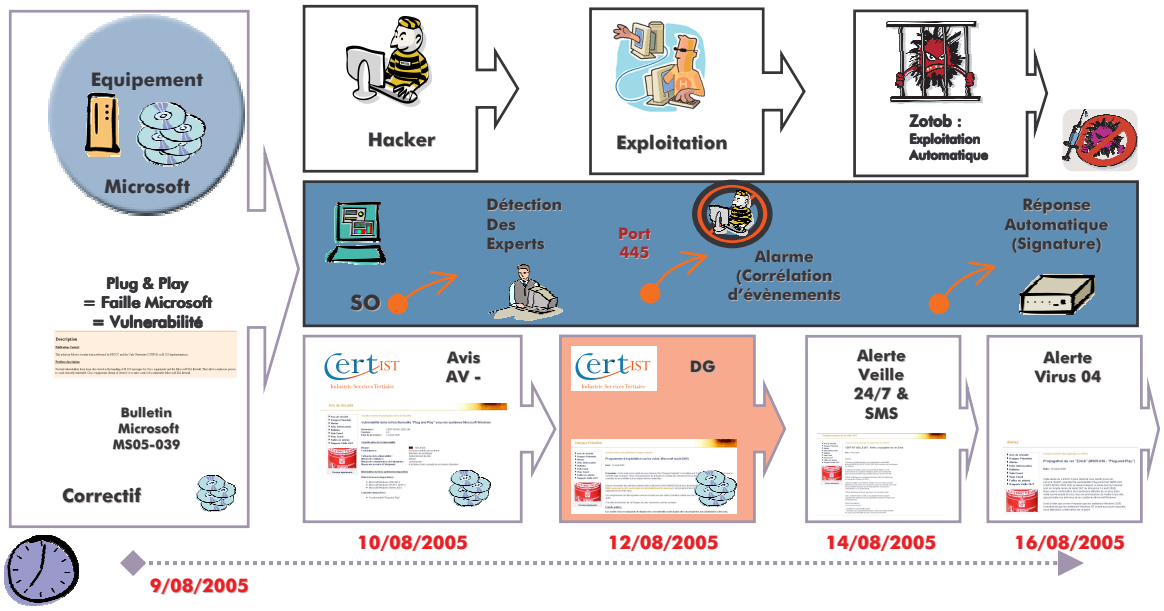
Le suivi des Menaces par le « Hub de gestion de crise » : analyse du cas « Zotob »

Chaque grande crise virale liée à l'exploitation d'une vulnérabilité Microsoft a été l'occasion pour le Cert-IST d'ouvrir un chantier pour analyser a posteriori son fonctionnement et le rôle qu'il a joué pour ses adhérents, et de remettre en cause en permanence l'équilibre prévention - réaction (émission de bulletins de veille – activités d ' « Emergency Response »).
La crise « Blaster » fut l'un des thèmes phares du Forum 2003. La crise « Sasser » fut analysée lors du Forum 2005, et les enseignements qui en furent tirés sont à l'origine de nombreuses évolutions aujourd'hui opérationnelles.

La dernière crise virale en date, « Zotob », a été l'occasion de vérifier en conditions réelles l'adéquation des nouveaux outils qui avaient été conçus face à ce type de situations. En effet "l'évènement" Faille « PNP » / ver « Zotob » a suivi tout le cycle en terme d'information prévention/alerte et fournit donc un cas d'école intéressant.
- cycle complet vulnérabilité logicielle puis attaque virale
- utilisation chronologique de la totalité des outils Avis/Hub de gestion de crise/astreinte (Veille 24/7)



Nous allons maintenant suivre la chronologie détaillée et exhaustive des informations diffusées (typiques d'un blog/accompagnement gestion de crise, ici en 11 étapes), et des mesures de réaction ou d'accompagnement recommandées, en les analysant. Seront mentionnées des informations qui ne sont accessibles habituellement qu'aux titulaires de certains services tels que la « Veille 24/7 ».

1/ Parmi les 6 failles révélées par Microsoft dans son bulletin mensuel d'Aout 2005 le Mardi 9 vers 19h (heure Française), apparait la faille dans le composant "Plug and Play".

MS05-039 - Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)
http://www.Microsoft.COM/TechNet/securit/bulletin/MS05-039.mspx
Criticité : **Elevé**
CVE : CAN-2005-1983

2/ Dans son premier message diffusé dans la liste « Vuln-coord » le Mercredi 10, à 7h56, le Cert-IST attribue une criticité élevée à cette vulnérabilité et écrit :

Selon notre première analyse, nous avons classé ces avis de sécurité par ordre d'importance et de criticité (**Elevé**, **moyen**).

MS05-038 - Cumulative Security Update for Internet Explorer (896727)
MS05-039 - Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)

...
Elle permet à :

un attaquant distant sur Windows 2000 de **prendre le contrôle** de la machine vulnérable,
un utilisateur ayant un compte sur un système Windows XP (SP1 et SP2) et Windows Server 2003 **d'augmenter ses privilèges**.

Cette vulnérabilité n'impacte pas Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), et Microsoft Windows Millennium Edition (ME). Comme Microsoft ne mentionne rien sur Windows NT 4, il est fortement recommandé de contacter son support Microsoft pour savoir si cette vulnérabilité impacte cette plate-forme et si il existe des correctifs.

A ce stade, il s'agit d'initialiser la diffusion de l'information concernant les correctifs proposés par Microsoft, accompagnés d'un premier niveau d'analyse concernant l'urgence de leur déploiement. Cette diffusion passe par un mail sur la liste vuln-coord, canal souple permettant des diffusions rapides sans gestion de la base de données des Avis.
Les informations diffusées permettent d'être comparées avec le parc de l'entreprise pour localiser ses vulnérabilités, et éventuellement, en attente de l'application de ces correctifs, mettre sous surveillance certaines machines ou certains services.

3/ Dans sa première version de l'avis circonstancié (CERT-IST/AV-2005.294), diffusée le Mercredi 10, à 14H35, le Cert-IST attribue une criticité élevée à cette vulnérabilité, et écrit entre autres:

Nature du problème

Une vulnérabilité a été découverte dans la fonctionnalité "Plug and Play" sous les systèmes Microsoft Windows. Elle permet :

à une personne malveillante, d'exécuter à distance du code arbitraire, avec les privilèges administrateur, sur un système vulnérable,
à un utilisateur local d'un système vulnérable, d'obtenir illégalement les privilèges administrateur sur ce système.

Analyse détaillée

Cette vulnérabilité est due à un débordement mémoire dans le service "Plug and Play". Elle permet d'exécuter du code arbitraire avec les privilèges administrateur.
Sur les systèmes Windows 2000 le composant vulnérable est accessible à distance avec une connexion anonyme. Cette vulnérabilité permet alors à un attaquant distant, via un message spécifiquement formaté, de prendre le contrôle d'un système vulnérable.
Sur les systèmes Windows XP SP1 le composant vulnérable est accessible à distance avec une connexion authentifiée. Cette faille permet alors à un attaquant distant et authentifié, via un message spécifiquement formaté, de prendre le contrôle d'un système vulnérable.
Sur les systèmes Windows XP SP2 et Windows Server 2003 le composant vulnérable est accessible à distance uniquement aux utilisateurs authentifiés ayant déjà les privilèges administrateur. Cette vulnérabilité permet donc uniquement à un utilisateur local, via une application malveillante, d'obtenir illégalement les privilèges administrateur sur un système vulnérable.

Les solutions proposées sont à ce stade l'application du correctif proposé, et ce dans un délai nominal par rapport à un avis de risque « Elevé », qui dans la nomenclature Cert-IST (http://www.cert-ist.com/fra/ressources/Avis/NomenclatureFR/), correspond à :
Agir immédiatement sur les systèmes frontaux et les serveurs.

4/ Dans sa deuxième version de l'avis circonstancié du Vendredi 12, à 10H38, suite à la parution d'un programme d'exploitation la criticité de la vulnérabilité devient « Très Elevée », le Cert-IST écrit :

Risque Très Elevé
L'avis initial a été mis à jour et ré-émis en version 2.0 suite à la publication d'un programme d'exploitation concernant Windows 2000.
Sur les systèmes Windows 2000 le composant vulnérable est accessible à distance avec une connexion anonyme.
Cette vulnérabilité permet alors à un attaquant distant, via un message spécifiquement formaté, de prendre le contrôle d'un système vulnérable.
Nota : Un programme d'exploitation de cette vulnérabilité a été diffusé sur Internet. Il permet à une personne malveillante, non authentifiée de prendre à distance le contrôle d'un système Windows 2000 vulnérable.

Les solutions proposées restent, en ce qui concerne la faille elle-même, l'application du correctif proposé, et ce dans un délai qui a évolué. Le passage à un avis de risque « Très élevé », dans la nomenclature Cert-IST, correspond à :

Agir immédiatement sur tous les systèmes

Par ailleurs, l'identification d'un code d'exploit permet d'envisager la mise en place de mesures de détection via les Intrusion Detection Systems (IDS) ou les outils de corrélation liés à l'utilisation d'un Security Operation Center (SOC).

5/ Cette montée du risque donne lieu à l'émission d'un Danger Potentiel (DG) le Vendredi 12, à 11h57. Le Cert-IST écrit :

Depuis la parution des derniers bulletins Microsoft d'août 2005 (09/08/2005) et de la disponibilité des correctifs (http://www.microsoft.com/technet/security/bulletin/ms05-aug.mspx), des programmes d'exploitation exploitant ces failles apparaissent au fil de l'eau. Ces programmes ont été signalés comme circulant sur des listes et certains d'entre eux ont été mis en ligne sur des sites à grande diffusion.
A la date de rédaction de ce Danger, les avis concernés sont les suivants :
Exploits publiés :
Le Cert-IST vous recommande de déployer les correctifs Microsoft au plus vite concernant les avis mentionnés ci dessous.
CERT-IST/AV-2005.294 (Risque Trés Elevé) *Vulnérabilité dans la fonctionnalité "Plug and Play" sous les systèmes Microsoft Windows* (MS05-039 - Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)
Le programme d'exploitation permettant d'exploiter cette vulnérabilité, permet de **prendre le contrôle d'une machine Windows 2000 server** vulnérable. Il a été intégré à l'outil "Metasploit Framework". Ce facteur est souvent précurseur d'attaques.
Nous vous recommandons d'appliquer le correctifs sur les plates-formes Windows 2000 au plus tôt.

A ce stade, la recommandation d'application du correctif est de plus en plus péremptoire. Le Cert-IST n'émet pas -encore- d'ALerte puisque les attaques (massives) n'ont pas commencé (et que vu du Vendredi, il est possible qu'elles n'aient jamais lieu, en tout cas de façon massive). Toutefois le risque étant accru par le facteur intégration dans l'outil « Metasploit Framework », le Cert-IST active le hub de gestion de crise en initialisant le blog de suivi.

Accueil | Hub de gestion de crises | Vulnérabilité Windows "Plug-and-Play" (MS05-039) - Ver "Zotob" — Version imprimante

Ce blog détaille les informations sur la vulnérabilité "Plug-and-Play" sous Microsoft Windows (MS05-039 - Avis CERT-IST/AV-2005.294) et les informations relatives aux programmes d'exploitation et aux vers l'exploitant tel que "Zotob".

Date	Liste des posts
05 septembre 2005	Programmes de détection de la vulnérabilité PNP et de nettoyage du ver Zotob
26 août 2005	Un programme d'exploitation pour la vulnérabilité PnP pour les versions FR fonctionne
26 août 2005	Arrestations de pirates impliqués dans la diffusion de zotob.
24 août 2005	Cas des plates-formes Windows XP (SP1 et SP2) avec "Simple File Sharing & ForceGuest" actif
19 août 2005	Point sur "Zotob" et ses variantes ou alias (exploitant MS05-039)
19 août 2005	Quelles plates-formes Windows sont impactées par la vuln MS05-039 ?
18 août 2005	Notice de "Cisco" donnant des recommandations sur "Zotob" et "Rbot"
17 août 2005	Variantes de "Zotob"
16 août 2005	Diffusion de l'Alerte AL-2005.001
16 août 2005	Avis de sécurité AV-2005.301 sur le ver "Zotob"
14 août 2005	La Veille 24/7 informe d'une Alerte sur le ver "Zotob" exploitant la vulnérabilité PnP MS05-039
12 août 2005	Diffusion du Danger potentiel DG-2005.005
12 août 2005	Ouverture Blog vulnerabilité Windows "PnP" MS05-039

6/ Le début de la propagation du ver **« Zotob »** donne lieu à l'émission d'une **Alerte le Dimanche 14 Août** à 16h46. Il est à noter que cette détection/signalisation intervient lors de l'astreinte du pont du 15 Août, et qu'un indice révélateur de l'état de vigilance dans lequel s'était mis l'équipe est que cette détection intervient hors de toute sollicitation d'un adhérent, et en fin d'après-midi, alors que le Compte rendu de veille 24/7 du dimanche avait déjà été rédigé et envoyé. Le Cert-IST écrit :

```
Comme cela était prévisible, un ver exploitant la vulnérabilité Microsoft MS05-039 (CERT-
IST/AV-2005.294) commence à se propager sur Internet.
Il s'agit du ver "Zotob", basé sur le principe de "Mytob". Ce ver tente d'infecter les
systèmes Windows 2000 via la vulnérabilité dans la fonctionnalité "Plug and Play" (PnP) sur le
port TCP 445.
"Zotob" n'affecte que les systèmes Windows 2000 (il n'affecte pas les systèmes Windows XP
SP2).
Une fois installé sur le système, "Zotob" ouvre un shell sur le port 8888 et un serveur FTP
sur le port 33333, puis se connecte à un canal IRC permettant à l'auteur du ver d'exécuter des
commandes malveillantes sur le poste infecté.
"Zotob" télécharge le fichier "haha.exe" sur la machine cible.
Nota : L'Internet Storm Center a reçu également des rapports signalant des infections par des
programmes binaires ("pnpsrv.exe" et "winpnp.exe").

Recommandations :
=================
 o Installer les correctifs Microsoft.
 o Au niveau des équipements réseau, il est recommandé de filtrer
les accès aux ports 8888 et 33333, ainsi que 139 et 445.
```

Cette ALerte a été doublée d'une alerte envoyée sous forme de SMS.

A ce stade, le Cert-IST a émis une de ses rares alertes annuelles, ce qui est caractéristique du plus haut niveau d'urgence répertorié. La recommandation d'installer les correctifs est répétée, mais cette fois-ci, pour ceux qui pour des raisons qui leur appartiennent n'ont pas voulu ou pu appliquer les correctifs à temps (*), elle est complétée par des recommandations complémentaires.

(*) Concernant l'application « immédiate » des correctifs, il s'agit bien évidemment d'une recommandation théorique, et on rappelle que les principes de la gestion de crise (« l'accompagnement pendant la traversée de la zone de danger maximum ») ont justement été définis après avoir constaté que l'éditeur, et plus encore les équipes d'exploitation, avaient forcément des difficultés pour déployer les correctifs à temps.

Le cas dont nous traitons aujourd'hui l'illustre parfaitement : on rappelle que les correctifs sont publiés pour les Européens dans la nuit du mardi au mercredi, que l'exploit est apparu le vendredi, ce qui veut dire que les exploitants n'ont pas eu plus de 72h pour évaluer les effets secondaires des correctifs, et moins de 24h pour évaluer la montée du risque liée à l'exploit et accélérer le processus.
Ainsi, en conformité avec l'esprit d'accompagnement qui caractérise le « Hub de crise », on complète la recommandation de « patcher », par des indications sur les ports et flux caractéristiques d'une propagation du ver qui permettent soit d'être utilisés directement pour l'application de solutions palliatives de filtrage, soit indirectement pour la définition d'un seuil (à surveiller) révélateur de propagation interne et qui déclenchera des mesures d'urgence applicables coûte que coûte.

7/ Le rapport de Veille 24/7 du lundi 15 août (jour férié) à 10h58 poursuit son analyse et réitère ces recommandations.

```
Bonjour,

Ci-joint un point sur la veille technologique du lundi 15 août 2005 à 11h00.
Évènements marquants :
======================
 o Suite à l'apparition du ver "Zotob" signalé hier après-midi, la majorité des éditeurs
d'anti-virus ont publié des descriptions de ce ver et mis à jour leur base de signature :
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FZOTOB%2EA
http://www.sophos.com/virusinfo/analyses/w32zotoba.html
http://vil.nai.com/vil/content/v 135433.htm
http://www.symantec.com/avcenter/venc/data/w32.zotob.a.html

Voici les informations complémentaires que l'on peut apporter par rapport à la description
faite hier :

1/ "Zotob" tente d'infecter les systèmes vulnérables sur le port TCP 445. Il tente ensuite
d'utiliser la vulnérabilité "PnP" pour télécharger et exécuter la charge utile (fichier
haha.exe) du ver via FTP, sur un port TCP élevé (port 33333 selon certaines sources).Le
système infecté devient à son tour un serveur FTP pouvant compromettre de nouveaux systèmes.

2/ "Zotob" tente de se connecter sur des serveurs IRC ("diabl0.turkcoders.net" sur le port TCP
8080, "l33t.freeshellz.org" sur le port TCP 5232, par exemple), via des ports TCP aléatoires,
afin de permettre l'accès à distance au système infecté.

3/ Il existe déjà une variante "B" de ce ver : "Zotob.B" :
http://www.symantec.com/avcenter/venc/data/w32.zotob.b.html
http://vil.nai.com/vil/content/v 135435.htm

4/ Au moins deux robots exploitent cette vulnérabilité
("pnpsrv.exe" et "winpnp.exe") :
http://vil.nai.com/vil/content/v 135434.htm
http://www.symantec.com/avcenter/venc/data/w32.spybot.ubh.html

Recommandations :
=================

 o Appliquer les correctifs Microsoft MS05-039.
 o Au niveau des équipements réseau, il est recommandé de filtrer les accès aux ports 8888
(porte dérobée) et 33333 (serveur FTP), ainsi que 139, 445 et 8080 (utilisé pour se connecter
aux serveurs IRC).
 o Mettre à jour vos solutions anti-virales.
```

Le seul élément réellement nouveau est le statut concernant les signatures et mises à jour des solutions anti-virales. On pourrait presque considérer à ce stade, qu'on est sortis de la zone de danger, et qu'il « suffit » d'avoir automatisé (ou décidé de « pousser » sur réception de l'alerte du Cert-IST) les mises à jour anti-virales pour être hors de danger.
En effet, de nombreuses entreprises vont considérer que la principale menace à court terme est la propagation de « Virus » utilisant la faille « PnP », et dont l'écriture a été facilitée par le programme d'exploitation réutilisable. Du moment qu'on détecte et éradique le (ou les, on verra plus loin que ce point pose problème) ver(s) qui tire(nt) parti de cette faille, on doit pouvoir tenir jusqu'à l'application effective des correctifs proposés par Microsoft, seule solution à même d'éliminer la totalité des menaces liées à cette vulnérabilité, entre autres les attaques « manuelles » et/ou venant de l'intérieur.

8/ Le Mardi 16 Août à 9h45, les informations du week-end sont répercutées dans la base de connaissances accessible à tous les adhérents sous la forme de l'ALerte concernant le ver « Zotob »:

```
Cette alerte du Cert-IST a pour objet de vous avertir qu'un ver, nommé "Zotob", exploitant la
vulnérabilité "Plug-And-Play" MS05-039 (CERT-IST/AV-2005.294) se répand depuis ce week-end sur
Internet (voir le compte-rendu de veille 24/7 du dimanche 14 août 2005).
Nous avons confirmation de la présence effective de ce virus dans notre communauté et nous
vous recommandons de mettre à jour dès que possible vos anti-virus et vos systèmes Microsoft
Windows.
Il est à noter que ce ver n'impacte que les systèmes Windows 2000.
Il semblerait que les systèmes Windows NT soient eux aussi impactés, nous attendons
confirmation de ce point.

Un avis de sécurité Cert-IST décrivant le ver "Zotob" sera rédigé prochainement.

Description du ver :
====================
"Zotob" tente d'infecter les systèmes vulnérables sur le port TCP 445, en utilisant la
vulnérabilité "PnP" ("Plug-and-Play").
Une fois installé sur le système, "Zotob" ouvre une porte dérobée sur le port 8888 afin de
télécharger et exécuter la charge utile du ver (exécution du script FTP "2pac.txt" qui
télécharge et exécute un copie du ver, sous le nom de fichier "haha.exe) via FTP, sur un port
TCP élevé (port 33333 selon certaines sources).
Le système infecté devient à son tour un serveur FTP servant à la compromission de nouveaux
systèmes.

"Zotob" dépose une copie de son code dans le répertoire "%System%", sous le nom "botzor.exe"
et crée un mutex nommé "B-O-T-Z-O-R".
"Zotob" ajoute la valeur "botzor.exe" aux clés de registre suivantes:
HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WINDOWS SYSTEM
HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\WINDOWS SYSTEM
"Zotob" positionne la valeur de la clé de registre suivante à "4" :
HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Start
"Zotob" écrase le fichier "%System%\drivers\etc\hosts" afin de bloquer l'accès à certains
sites.

"Zotob" tente de se connecter sur des serveurs IRC ("diabl0.turkcoders.net" ou
"wait.atillaekici.net" sur le port TCP 8080, "133t.freeshellz.org" sur le port TCP 5232, par
exemple), via des ports TCP aléatoires, afin de permettre l'accès à distance
au système infecté.

Nota :
 o Il existe déjà une variante "B" de ce ver : "Zotob.B" :
http://www.symantec.com/avcenter/venc/data/w32.zotob.b.html
http://vil.nai.com/vil/content/v_135435.htm
 o Au moins deux chevaux de Troie exploitent cette vulnérabilité
("pnpsrv.exe" et "winpnp.exe") :
http://vil.nai.com/vil/content/v_135434.htm
http://www.symantec.com/avcenter/venc/data/w32.spybot.ubh.html

Recommandations :
=================
 o Appliquer les correctifs Microsoft MS05-039.
 o Au niveau des équipements réseau, il est recommandé de filtrer les accès aux ports 8888
(porte dérobée) et 33333 (serveur FTP), ainsi que 139, 445, 5232 et 8080 (ces deux derniers
sont utilisés pour se connecter aux serveurs IRC).
 o Mettre à jour vos solutions anti-virales.
```

9/ Le Mardi à 11h52 émission de l'Avis de Sécurité CERT-IST/AV-2005.301
(Ver "Zotob" sur les systèmes Microsoft Windows, Version 1.0)
(voir détails dans l'avis lui-même.)

A noter cependant la présence des informations suivantes :

```
Analyse détaillée

En plus du comportement général donné précédemment, on notera les points suivants :
"Zotob" tente d'exploiter les vulnérabilités de la fonctionnalité "Plug-and-Play" de machines
distantes via le port TCP 445. Le ver utilise des adresses IP aléatoires afin de rechercher
des systèmes vulnérables.
"Zotob" ouvre une porte dérobée sur le port TCP 8888 permettant ainsi à une personne
malveillante de supprimer, de télécharger, d'exécuter des fichiers, ....
Via cette porte dérobée, "Zotob" installe un serveur FTP sur le port TCP 33333. Le système
infecté devient à son tour un serveur FTP servant à la compromission de nouveaux systèmes.
"Zotob" exécute le script FTP "2pac.txt" afin de télécharger et exécuter une copie du ver,
sous le nom de fichier "haha.exe".
"Zotob" dépose une copie de son code dans le répertoire "%System%", sous le nom "botzor.exe"
et crée un mutex nommé "B-O-T-Z-O-R", afin qu'une seule instance de son code ne soit exécutée
simultanément sur un système.
"Zotob" écrase le fichier "%System%\drivers\etc\hosts" afin de bloquer l'accès à certains
sites (voir les documents des éditeurs anti-virus indiqués dans la section "Documentation
additionnelle" pour obtenir la liste des sites bloqués).
"Zotob" tente de se connecter sur des serveurs IRC ("diabl0.turkcoders.net" ou
"wait.atillaekici.net" sur le port TCP 8080, "133t.freeshellz.org" sur le port TCP 5232, par
exemple), via des ports TCP aléatoires, afin de permettre l'accès à distance au système
infecté.
Nota : Il existe au moins deux chevaux de Troie exploitant cette vulnérabilité ( "pnpsrv.exe"
et "winpnp.exe" ).

Diagnostic

Voici les caractéristiques visibles du ver "Zotob" permettant de le détecter sur un système
infecté :

1°) Activité réseau :
Port(s) réseau ouvert(s) : Ports TCP 8888 (porte dérobée), 33333 (serveur FTP), 139 , 445 ,
5232 et 8080 (ces deux derniers sont utilisés pour se connecter aux serveurs IRC)

Site(s)/Serveur(s) contacté(s) : "diabl0.turkcoders.net", "wait.atillaekici.net",
"133t.freeshellz.org"

Adresse(s) e-mail contactée(s) : NA

2°) Modifications du système :
Fichier(s) ajoutés :
%System%\botzor.exe
où %System% indique le répertoire système (ex.:"C:\Windows\System32")
Clé(s) de Registre modifiée(s) ou ajoutée(s) :
Ajout de la valeur :
"WINDOWS SYSTEM" = "botzor.exe"
aux clés de registre :
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
```

```
Modification de la valeur :
"Start" = "4"
dans la clé de registre :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess

Modification de la valeur :
%System%\botzor.exe = "%System%:*:Enabled:botzor"
dans la clé de registre :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications\
```

Toutes les informations pouvant être utiles à l'identification et la détection, ainsi qu'à la correction de l'attaque, ont donc été diffusées, et intégrées dans la base de connaissances au cas où cette attaque se reproduirait sous forme de crise dans l'avenir chez un membre particulier qui n'aurait pas fait les mises à jour requises sur l'ensemble de son parc.

Comme déjà constaté lors des propagations de « Mydoom », « Bagle », « Netsky », les solutions anti-virales à base de signatures ne vont clore la crise que momentanément, et être rapidement contournées par l'apparition de nombreuses variantes réactivant la menace pour les parcs de machines Windows non encore mises à jour.

10/ Le Vendredi 17août, à 11h09, le Cert-IST diffuse un second message dans la liste Vuln-coord.

```
Bonjour

Cet e-mail est un complément d'information de l'alerteCERT-IST/AL-2005.001 et de l'avis CERT-IST/AV-2005.301.

La propagation de nombreuses variantes du ver "Zotob" est signalée par de nombreuses sources d'information dont le "SANS Institute" et "ISS".
Il semble que ces variantes, parfois désignées sous des noms différents (W32/IRCbot.worm!MS05-039, WORM RBOT.CBQ, ... ), aient attaqué les systèmes informatiques de plusieurs grands médias et sociétés aux Etats-Unis.

Plusieurs éditeurs d'anti-virus ont émis des alertes relatives à une variante plus particulièrement mise en cause (variante E du ver "Zotob" pour Symantec) :
  o Symantec :
http://www.symantec.com/avcenter/venc/data/w32.zotob.e.html (W32.Zotob.E)
  o McAfee : http://vil.mcafeesecurity.com/vil/content/v_135491.htm (W32/IRCbot.worm!MS05-039)
  o Trend Micro :
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FRBOT%2ECBQ
(WORM RBOT.CBQ)
  o Sophos : http://www.sophos.com/virusinfo/analyses/w32tpbota.html (W32/Tpbot-A)

Les descriptions des différents éditeurs varient à propos des ports TCP utilisés pour les connexions aux portes dérobées, aux serveurs FTP ou IRC, mais toutes ont en commun de signaler:
  o l'exploitation de la vulnérabilité MS05 039 ("Plug and Play") via le port 445,
  o l'utilisation du nom de fichier  "%System%\wintbp.exe" pour se copier sur les systèmes infectés.

Le Cert-IST réitère les recommandations suivantes :
  o Appliquer de toute urgence les correctifs Microsoft MS05-039.
  o Filtrer l'accès au port 445 au niveau des équipements réseau.
  o Mettre à jour vos solutions anti-virales.
```

11/ Le Cert-IST continuera d'accompagner ses adhérents en diffusant dans le « blog » des informations utiles « à la traversée de la zone de danger ».
Ainsi le 18 Août est mentionnée une « Notice de Cisco donnant des recommandations sur Zotob et Rbot ». Le Cert-IST dit :

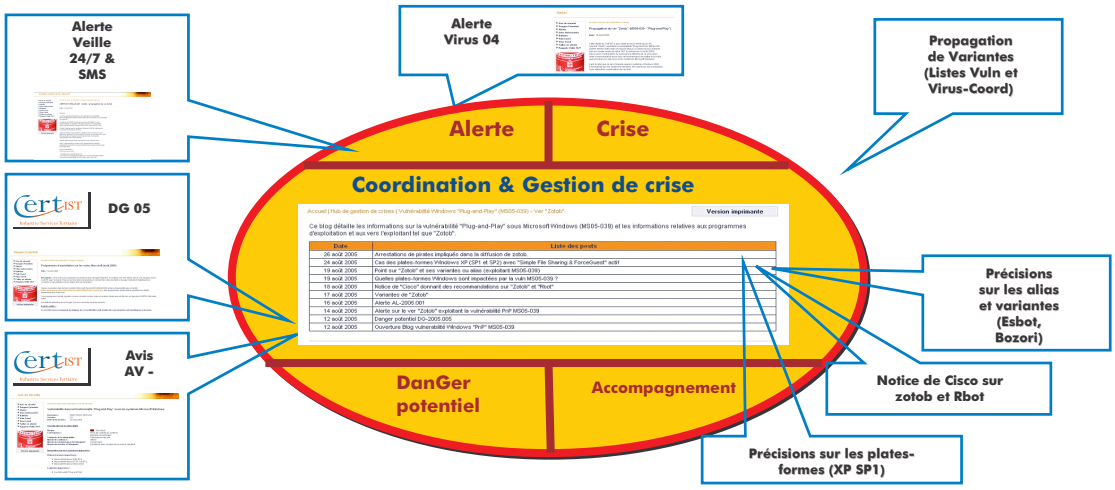
Cisco vient de publier une notice (Cisco - ZOTOB and WORM_RBOT.CBQ Mitigation Recommendations) donnant des moyens de détecter au travers de "NetFlow" des host infectés mais aussi pour mentionner certains plates-formes vulnérables.

Le 19 Août, suite à une question d'un adhérent concernant certaines versions de Windows, le Cert-IST demande (et obtient) des précisions de la part de Microsoft, clarifiant en particulier la vulnérabilité des versions de Windows 2000 antérieures au SP4, ainsi qu'une confirmation pour Windows NT. Ces précisions sont remises à la disposition de la communauté dans le « blog ».

Ce même 19 Août, le Cert-IST diffuse un nouveau message dans le liste « Virus-coord » :

Suite à la multiplication des variantes des codes malicieux exploitant la vulnérabilité "Plug-and-Play" (MS05-039 -CERT-IST/AV-2005.294), le récapitulatif ci-dessous tente de clarifier leurs différentes appellations :
A ce jour, voici l'ensemble des vers/robots actuellement répertoriés qui exploitent cette vulnérabilité : - 8 variantes de "Zotob" (variantes "A" à "H") - 1 de "Rbot" (variante "YK") - 2 de "SDbot"/"Esbot" (variante "ADB") - 1 de "CodBot" - 3 de "IRCbot" (variantes "ES", "ET" et "EX") - 2 de "Bozori" (variantes "A" et "B")
Suivi d'un certain nombre de recommandations et de liens pour continuer à se prémunir contre ces menaces.

Le 24 août , le Cert-IST apporte une précision concernant le cas des plates-formes Windows XP SP1 et SP2 avec une configuration particulière (« Simple File Sharing & Forceguest » actif).



Le 26 août, le Cert-IST mentionne qu'un programme d'exploitation exploitant les plates-formes Windows XP version Française circule et fonctionne.

Enfin le 5 septembre, le Cert-IST dresse un bilan des outils de type scanner de la vulnérabilité "PNP" et de nettoyage du ver "Zotob".

Le détail des informations transmises, aura pu rendre la lecture de cette note parfois fastidieuse. Toutefois, nous avons choisi d'intégrer de nombreux extraits avec un degré de précision permettant effectivement au lecteur de vérifier qu'ils permettaient de mettre en place (pendant la propagation de « Zotob ») :
- des mesures sur le trafic sur certains flux et ports (y compris cette fois les trafics FTP, canal IRC, serveurs etc ... connus),
- des mesures sur le code/la signature du ver lui-même,
- une corrélation avec des informations remontées par exemple par des contrôles d'intégrité (puisque le ver laisse de nombreuses traces ...).

A notre sens, ces informations ont dû permettre à tous d'optimiser leur stratégie de « patch management » et le paramétrage de leurs solutions anti-virales ou des dispositifs de filtrage. Nous espérons que la qualité, le timing et la classification des informations diffusées ont permis à tous de prendre les mesures adéquates en terme de :
- mesures de monitoring,
- mesures de levée de flag/alerte,
- mesures de filtrage.

et également d'appliquer au bon moment des mesures :

- préparées à l'avance pour application si on le décide,
- préparées à l'avance pour application automatique si conditions réunies et dispositif adéquat .. (ex : dispositifs de mise en quarantaine de type NAC),
- pour application immédiate.

Ainsi, en suivant en temps réel la montée et les formes prise par la menace « Plug-and-Play » (MS05-039) - Ver « Zotob », le Cert-IST a tenté d'assumer au mieux sa mission de prévention, d'alerte, et d'accompagnement en situation de crise. Les nouveaux outils ont permis d'utiliser une graduation fine dans l'évaluation et la communication du risque, et de valider, mettre en commun et diffuser une sélection pertinente des informations les plus utiles.