

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Chronique d'un incident ordinaire

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-003>

Gestion du document

Référence	CERTA-2002-INF-003
Titre	Chronique d'un incident ordinaire
Date de la première version	29 novembre 2002
Date de la dernière version	–
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Comme au cinéma.

L'industrie du cinéma nous a souvent présenté le pirate informatique comme un être flamboyant. On a pu ainsi voir une équipe de terroristes sur-entraînés s'emparant des plans du dernier missile balistique en fracturant, via le Réseau, un super-calculateur ou un psycho-techno-gourou mettant au point un virus à l'intelligence rare, et artificielle, afin de prendre le contrôle des ordinateurs de l'Univers ...

Dans le cadre de sa mission, le CERTA a pu constater combien la réalité est différente de la fiction hollywoodienne. Croyez-en notre expérience : vous avez plus de chance d'être confronté à un des vandales qui sévissent sur Internet que de croiser la route d'un agent secret ...

2 Un trafic non sollicité ...

Au début du mois de novembre 2002, un scan sur la plage d'adresses du CERTA ayant pour objectif d'identifier des serveurs possédant un service d'impression (port tcp/515) est enregistré dans les journaux d'événements de notre pare-feu.

La machine à l'origine du scan appartenant à la communauté d'utilisateurs du CERTA, l'administrateur est aussitôt contacté :

- CERTA : Pouvez-vous me fournir une explication sur le "trafic non sollicité" en provenance d'un de vos serveurs, la machine w.x.y.z .

- Administrateur : Cette machine a été utilisée pour tester une application client-serveur en début d'année. On ne s'en sert plus depuis quelques mois ...
 - C : Je pense que cette machine a été compromise et sert de rebond pour compromettre d'autres systèmes.
 - A : Mais cette machine ne contient aucune donnée sensible !
 - C : Vous n'êtes probablement pas victime d'une attaque ciblée visant votre entité. Ce qui intéresse le pirate ce sont les ressources de votre machine. En l'occurrence, il s'en sert comme plate-forme d'attaque pour dissimuler son identité et compromettre d'autres systèmes ...
 - A : C'est très gênant. Que préconisez-vous ? Reformater le système ?
 - C : Non. Pas dans l'immédiat. Je vous préconise dans un premier temps de :
 - débrancher la machine du réseau (afin que les attaques contre des tiers ne puissent plus avoir lieu);
 - mettre en évidence la compromission en prenant le maximum de précautions pour ne pas modifier l'état de la machine (éviter tout accès au système de fichiers).
- Ensuite, si la machine est réellement compromise, je vous invite à réaliser une analyse de cette compromission. En effet, si vous ne mettez pas en évidence la vulnérabilité utilisée par le pirate pour prendre le contrôle de ce serveur, il est probable qu'il sera de nouveau compromis. L'analyse va également révéler l'étendue de la compromission : le pirate a peut-être réussi à pénétrer sur d'autres serveurs du réseau
- A : Je ne sais pas par où commencer. Pouvez-vous m'aider ?
 - C : Envoyez-moi, dans un premier temps, le résultat de la commande `netstat -an -inet et ps -efl`. Envoyez-moi également les exécutables `/bin/ps` et `/bin/netstat`. Et ne touchez-plus à cette machine afin de ne pas modifier les traces présentes sur le disque ...

3 Mise en évidence de la compromission.

La commande `ltrace -e fopen netstat` permet de visualiser les appels à la fonction `fopen()` réalisés lors de l'exécution de la commande `netstat`.

Ici, le résultat obtenu à partir de l'exécutable envoyé par l'administrateur est surprenant :

```
fopen("/usr/include/hosts.h", "r")      = 0
fopen("/proc/net/tcp", "r")            = 0x08056288
fopen("/proc/net/udp", "r")           = 0x0805c450
fopen("/proc/net/raw", "r")           = 0x08056288
fopen("/proc/net/unix", "r")          = 0x0805c450
fopen("/proc/net/ipv6", "r")          = 0x0805c450
```

La commande `netstat` essaie d'ouvrir un fichier `/usr/include/hosts.h` ... comportement pour le moins inhabituel ! Cet exécutable contient un cheval de Troie : le fichier `/usr/include/hosts.h` est un fichier de paramétrage contenant les connexions réseaux à dissimuler.

L'exécutable `ps` contient aussi un cheval de Troie : il ne fait aucun doute que la machine est compromise, `ps` et `netstat` proviennent d'un rootkit installé par le pirate après la compromission de la machine.

Un rootkit est un ensemble d'outils permettant de dissimuler l'activité du pirate (masquer des connexions réseaux, des processus actifs, la présence de certains fichiers). Outre les classiques chevaux de Troie qui viennent altérer le comportement de certaines commandes (`ps`, `netstat`, `ls`, etc), le rootkit contient des utilitaires permettant d'effacer les journaux systèmes, des portes dérobées permettant au pirate de se connecter sur le système sans s'authentifier ...

La compromission étant mise en évidence, l'étape suivante consiste à réaliser une copie physique des disques de la machine compromise puis procéder à l'analyse ...

4 Analyse de la compromission.

L'analyse de la compromission a pour objectif de répondre aux questions suivantes : comment le pirate a-t-il pu pénétrer sur le système ? qu'a-t-il fait par la suite ?

Etablir le scénario de la compromission n'est pas envisageable sur la machine compromise : le pirate a installé un rootkit qui altère le fonctionnement du système d'exploitation. Les données récoltées sur un système compromis ne sont pas fiables.

L'analyse se fera donc sur un système sain, à partir de la copie physique des disques du système compromis. Et si la copie s'est faite dans de bonnes conditions, l'"autopsie" des disques va apporter de nombreuses réponses ...

4.1 Identification de la vulnérabilité.

L'examen des journaux d'événements ne révèle aucune anomalie. Rien de bien étonnant, nous verrons plus tard que le pirate a pris soin de purger les journaux d'événements.

Cependant, le visiteur a laissé des traces à son insu ! Sur beaucoup de systèmes d'exploitation, supprimer un fichier ne détruit pas les blocs de données associés. Linux n'échappe pas à cette règle ...

Une recherche sur le disque dur permet de retrouver des blocs de données ayant appartenus à un journal d'événements qui a été supprimé. Un extrait de ce journal d'événements est reproduit ci-dessous :

```
[...]
Oct 15 04:28:14 localhost SERVER[15701]: Dispatch_input: bad request line 'BB
Oct 15 04:28:19 localhost SERVER[15702]: Dispatch_input: bad request line 'BB
Oct 15 04:28:21 localhost SERVER[15703]: Dispatch_input: bad request line 'BB
Oct 15 04:28:22 localhost SERVER[15704]: Dispatch_input: bad request line 'BB
[...]
Oct 15 04:29:31 localhost sshd[15754]: log: Server listening on port 1200.
Oct 15 04:29:31 localhost sshd[15754]: log: Generating 768 bit RSA key.
Oct 15 04:29:31 localhost sshd[15754]: log: RSA key generation complete.
```

Ces lignes sont riches d'enseignements :

- on sait avec certitude que la machine a été compromise le 15 octobre à 4h28 du matin : on peut voir en effet le démarrage d'un processus (sshd) en écoute sur le port 1200/tcp. Le pirate s'est emparé des privilèges de l'administrateur système (root) et a immédiatement installé une porte dérobée !
- le pirate a utilisé une vulnérabilité présente dans le service d'impression (LPRng) pour compromettre la machine. Les lignes "SERVER[15704]: Dispatch_input: bad request line 'BB" sont caractéristiques de l'exploitation de la vulnérabilité du service LPRng sous RedHat 7.0.

L'affichage en hexadécimal d'un de ces enregistrements permet de visualiser le code malicieux utilisé :

```
290: 4f 63 74 20 31 35 20 30 34 3a 32 38 3a 31 39 20 Oct |15 0|4:28|:19
2a0: 6c 6f 63 61 6c 68 6f 73 74 20 53 45 52 56 45 52 loca|lhos|t SE|ERVER
2b0: 5b 31 35 37 30 32 5d 3a 20 44 69 73 70 61 74 63 [157|02]:| Dis|patc
2c0: 68 5f 69 6e 70 75 74 3a 20 62 61 64 20 72 65 71 h_in|put:| bad|req
2d0: 75 65 73 74 20 6c 69 6e 65 20 27 42 42 e0 f3 ff uest| lin|e 'B|B
2e0: bf e1 f3 ff bf e2 f3 ff bf e3 f3 ff bf 58 58 58
2f0: 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 30 XXXX|XXXX|XXXX|XXX0
300: 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000|0000|0000|0000
310: 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000|0000|0000|0000
[...]
380: 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000|0000|0000|0000
390: 30 30 30 30 30 30 30 30 30 30 30 30 30 34 38 30 0000|0000|0000|0480
3a0: 30 30 30 30 30 30 31 30 37 33 38 33 35 30 38 38 0000|0010|7383|5088
3b0: 73 65 63 75 72 69 74 79 30 30 30 30 30 30 30 30 secu|rity|0000|0000
3c0: 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000|0000|0000|0000
[...]
500: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....|....|....|....
510: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....|....|....|....
520: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....|....|....|....
530: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....|....|....|....
540: 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66
550: 89 d0 31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89
560: 4d fc 8d 4d f4 cd 80 31 c9 89 45 f4 43 66 89 5d
570: ec 66 c7 45 ee 5e 4f 27 89 4d f0 8d 45 ec 89 45
580: f8 c6 45 fc 5e 50 89 d0 8d 4d f4 cd 80 89 d0 43
590: 43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0
5a0: cd 80 89 d0 41 cd 80 eb 5e 58 5e 89 75 5e 48 31
5b0: c0 88 46 5e 47 89 45 5e 4c b0 5e 4b 89 f3 8d 4d
5c0: 5e 48 8d 55 5e 4c cd 80 e8 e3 ff ff ff 2f 62 69 /bi
5d0: 6e 2f 73 68 27 0a n/sh|'.
```

Le code malicieux (cf. ligne 540) et la signature "security" (cf. ligne 3b0) sont identiques à ceux trouvés dans l'outil "SEClpd", dont le code source est largement diffusé sur Internet.

4.2 Exécution de code arbitraire à distance.

Le service d'impression LPRng enregistre dans le journal des événements les requêtes d'impression (reçues sur le port 515/tcp) qui ne sont pas conformes au protocole LPR décrit dans le RFC 1179. La version vulnérable du service LPRng utilise l'appel système `syslog` sans préciser le format des données. Il est alors possible, via une requête habilement constituée adressée au service d'impression, de forcer l'exécution d'un code arbitraire contenu dans la requête elle-même.

Ce type de vulnérabilité est connu sous le nom de vulnérabilité de type chaîne de format.

Un avis de sécurité décrivant la vulnérabilité du service d'impression LPRng (cf. avis CERTA-2000-AVI-087) a été publié à la fin de l'année 2000.

Des outils exploitant cette vulnérabilité ont été diffusés peu de temps après sur Internet. Un de ces outils (SEClpd) a été réutilisé dans le ver Ramen (cf. alerte CERTA-2001-ALE-01 du CERTA).

4.3 Exploitation de la vulnérabilité de LPRng sous RedHat 7.0.

L'attaque se déroule en quatre phases :

1. le pirate connecté sur la machine a.b.c.d repère un serveur (w.x.y.z) dont le port 515/tcp est accessible (phase de repérage) ;
2. il lance ensuite l'exécutable SEClpd. SEClpd se connecte sur le port tcp/515 correspondant au service LPRng et envoie une requête habilement constituée contenant un code malicieux ;
3. le code malicieux va ouvrir un service (un simple interpréteur de commandes /bin/sh) en écoute sur le port tcp/3879 ;
4. le pirate peut alors établir des connexions vers ce port (via telnet par exemple) et taper des commandes qui seront exécutées par la machine distante avec les droits du super-utilisateur (root).

Et voici ce que l'on peut visualiser au moyen de la commande `netstat` sur la machine vulnérable pendant la phase 4 de l'attaque :

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 w.x.y.z:3879           a.b.c.d:4958           CLOSE_WAIT
tcp      0      0 0.0.0.0:3879           0.0.0.0:*              LISTEN
tcp      1      0 w.x.y.z:515            a.b.c.d:4955           CLOSE
```

Revenons à notre compromission du 15 octobre ...

Grâce à l'outil SEClpd, "un utilisateur mal intentionné a pu réaliser, à distance, l'exécution de code arbitraire". Le pirate est maintenant maître de la machine vulnérable. La première action qu'il va réaliser sur la machine compromise est d'installer un rootkit.

4.4 Où il est de nouveau question du rootkit ...

L'analyse des "mouvements" de fichiers le 15 octobre à partir de 4h, va permettre de visualiser les actions réalisées par le pirate sur la machine compromise.

La première activité suspecte est visible à 04:28:33. Le pirate télécharge (via la commande `lynx`) une première archive (.a. signifie que la date d'accès a été modifiée):

```
Oct 15 2002 04:28:23 1102236 .a. -rwxr-xr-x 0 0 663612 /usr/bin/lynx
```

Le pirate parvient peu de temps après à télécharger une archive, rk.tgz.

```
Oct 15 2002 04:29:12 382403 m.. -rw----- 0 7 1462 /rk.tgz (deleted)
```

L'intégralité de l'archive ne peut être récupérée (certains blocs de données ont été réalloués). Par contre, le script d'installation du rootkit (effacé après exécution) a pu être extrait de la copie physique du disque.

Le script d'installation réalise plusieurs actions :

- il arrête certains services vulnérables (portmap par exemple) et installe des correctifs pour certains autres (notamment LPRng) : le pirate évite ainsi que la machine vulnérable ne soit compromise par un autre pirate ;
- il installe des chevaux de Troie pour plusieurs commandes systèmes : `ifconfig`, `netstat`, `ps`, `login`, `pstree`, `top`, etc ;
- il crée les fichiers `/usr/include/proc.h` (processus à masquer), `/usr/include/hosts.h` (connexions réseaux à masquer) et `/usr/include/file.h` (fichiers à masquer) utilisés par les chevaux de Troie ;

- il modifie le fichier `/etc/rc.d/rc.sysinit` pour qu'une porte dérobée (`sshd`) et un renifleur réseau (`linsniffer`) soient lancés automatiquement au démarrage de la machine ;
- il envoie un mél contenant la configuration du système et les mots de passe vers une boîte aux lettres hébergée sur un compte de messagerie gratuit ;
- il détruit le fichier archive (`rk.tgz`) et le répertoire d'installation (`rk`).

On peut dater très précisément la fin de l'exécution du script : 04:29:36.

```
Oct 15 2002 04:29:36          0 mac drwxr-xr-x 0    0    33865 /rk (deleted)
                        382403 .c -rw----- 0    7    1462 /rk.tgz (deleted)
```

Aucune autre activité suspecte n'est visible le 15 octobre. La compromission et l'installation d'un rootkit aura pris ... moins de 1 mn et 30s. Le pirate a maintenant de multiples possibilités pour se connecter sur le système (SECLpd ne lui est plus d'aucune utilité puisqu'il a pris le soin de "sécuriser" le système distant) :

- une porte dérobée de type `ssh` ;
- une porte dérobée dans l'exécutable `login`.

De plus, il peut utiliser un compte légitime pour se connecter (il lui suffit pour cela de déchiffrer les mots de passe contenus dans le mél).

5 Les motivations du pirate.

L'activité du 16 octobre nous éclaire sur les motivations de notre pirate.

5.1 Bataille rangée sur les réseaux IRC ...

Le pirate installe le 16 octobre au petit matin, un "bouncer" IRC (serveur mandataire pour IRC). Cet outil permet à un utilisateur de se connecter sur IRC tout en dissimulant son adresse IP réelle.

Il installe ensuite une archive contenant différents exécutables (`smurf`, `synflood`, etc.) dans le répertoire `/usr/man/man1/. . .` (noter le "blanc" dans le nom du répertoire). Peu de temps après, la date d'accès de l'exécutable `smurf` est modifiée, signe que des attaques en déni de service sont lancées.

Pour réaliser une attaque de type `smurf`, on adresse à une liste de machines (appelées amplificateurs) ou plus exactement à l'adresse de diffusion de réseau, un paquet ICMP de type `echo-request` dont la source semble être l'adresse IP de la victime. Le paquet ICMP est alors reçu par toutes les machines du réseau qui répondent par un paquet `echo-reply`, inondant ainsi la victime.

Les réseaux IRC sont des véritables champs de bataille pour certains individus : le déni de service est très souvent utilisé pour prendre le contrôle d'un channel IRC. C'est ce que réalise ici le pirate ... en masquant au préalable son adresse afin que, s'il est lui même victime d'un déni de service, seul son "bouncer" soit mis hors service.

5.2 La machine compromise est utilisée en rebond pour compromettre d'autres systèmes.

Le pirate a un comportement agressif.

D'autres attaques sont lancées et visent à exploiter différentes vulnérabilités présentes dans des services comme `LPRng`, `portmap`, `bind` (`dns`) ...

C'est une de ces attaques, balayant la plage d'adresse du CERTA à la recherche de serveurs vulnérables, qui aura permis de mettre à jour cette compromission ...

6 La vraie Vie.

Le CERTA est souvent amené à se déplacer pour aider l'administrateur d'un système informatique (d'une administration ou d'un service public) victime d'une attaque à réaliser l'analyse de la compromission : quelle vulnérabilité a été utilisée par le pirate pour prendre le contrôle du serveur ?, quelle est l'étendue de la compromission ? ...

Identifier les vulnérabilités, étudier les outils et techniques utilisés par les pirates permet ensuite d'affiner la politique de prévention des risques.

Hélas, la perception du risque de compromission d'un serveur connecté à Internet est trop souvent éloigné de la réalité et rejoint la vision Hollywoodienne : "Mon serveur est compromis ? Impossible ! Il ne contient aucune donnée sensible ...".

Ne vous méprenez pas ! Même si votre ordinateur ne détient pas d'informations sensibles, il présente un intérêt pour les vandales de l'Internet.

Si vous avez un système sur Internet, il a déjà été attaqué. Et est peut-être compromis. L'attaque ne vous vise pas personnellement. Des plages d'adresses sont scannées tous les jours à la recherche de serveurs vulnérables. L'objectif du vandale est d'exploiter les ressources de votre ordinateur. Ces motivations sont nombreuses :

- vous faire supporter l'hébergement d'un site contenant des copies de logiciels ou des images illicites;
- installer un réseau de déni de service ;
- participer à la "gué-guerre" sur IRC via l'hébergement d'un serveur mandataire IRC (bouncer) ou Bot Irc ;
- utiliser la machine en rebond pour attaquer d'autres sites ;

... ou simplement parce que votre serveur va permettre au groupe de pirates X de s'affirmer par rapport au groupe de pirates Y qui n'aura compromis que 32 machines ce week-end, 3 de moins que le groupe X.

Donc, si vous avez entre les mains un bulletin de sécurité affirmant qu'une faille est présente dans un applicatif alors ... appliquez les correctifs. Toute vulnérabilité non corrigée sera exploitée (ce n'est qu'une question de temps). Le pirate le sait bien : aussitôt la machine compromise, il applique les correctifs afin d'empêcher les concurrents de lui ravir son butin !

L'histoire se termine plutôt bien pour notre administrateur : la machine n'étant pas en production, l'impact de cette compromission (perte de temps, atteinte à l'image de marque, etc.) reste limité. A condition toutefois que personne ne vienne demander des comptes pour une intrusion frauduleuse perpétrée à partir de sa machine ...

7 Documentation

- Avis CERTA-2000-AVI-087 "Problèmes de validation pour LPRng" :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-AVI-087/index.html>
- Alerte CERTA-2001-ALE-001 "Propagation du ver Ramen sous Linux" :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-ALE-001/index.html>
- Note d'information CERTA-2002-INF-002 "Les bons réflexes en cas d'intrusion sur un système d'information" :
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html>

Gestion détaillée du document

29 novembre 2002 version initiale.