

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : « Mesures de performances » de l'Internet

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-2000-ALE-003>

Gestion du document

Date de la première version	26 mai 2000
Date de la dernière version	-
Source(s)	Réseau de confiance du CERTA

TAB. 1 – gestion du document

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

1 Systèmes concernés

Tout site connecté à l'Internet.

2 Risque

- déni de service qui s'apparente au type SYN Flood ;
- divulgation d'information concernant votre site.

3 Description

Une jeune pousse voulant mesurer les performances de l'Internet réalise actuellement des « tests » sur certains sites. L'exécution des « mesures » par cette société perturbe le fonctionnement du site testé en augmentant sa charge et, à ce titre, peut être assimilé à un déni de service.

Un site WEB de l'administration a été victime de ces « mesures ». Lorsque le responsable de ce site a exigé que cesse cette activité, la société lui a demandé ses journaux de garde barrière pour justifier le trouble subi.

Les journaux des gardes barrières contiennent de nombreuses informations sur ce que votre site accepte ou rejette. De ce fait, vous publiez une partie de vos vulnérabilités en divulguant vos journaux.

L'exploitation qui sera faite des informations recueillies concernant votre site n'est pas connue.

L'éthique d'Internet suppose que l'on demande l'autorisation avant de faire une consommation anormale des ressources offertes par un site. Par ailleurs, Le nouveau code pénal reprenant les termes de la loi Godfrain punit le fait d'entraver le fonctionnement d'un système automatisé de données ou même de tenter de le faire.

De telles « mesures » ne peuvent être entreprises sur votre site sans l'accord écrit du responsable de la sécurité du site.

4 Solution

Les « mesures » que le CERTA a pu observer laissent des traces très caractéristiques dans les gardes barrières. Vous trouverez ci-joint un extrait de journal d'un garde barrière dans lequel les adresses IP ont été cachées :

```
000001 25May2000 6:17:03 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 6663 x.x.x.x w.w.w.w 6663 nameserver len 28
000002 25May2000 6:17:03 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 6664 x.x.x.x w.w.w.w 6664 nameserver len 28
000003 25May2000 6:17:03 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 6665 x.x.x.x w.w.w.w 6665 nameserver len 28
000004 25May2000 6:17:03 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 6666 x.x.x.x w.w.w.w 6666 nameserver len 28
000005 25May2000 6:17:03 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 6667 x.x.x.x w.w.w.w 6667 nameserver len 28
000006 25May2000 6:17:03 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 6668 x.x.x.x w.w.w.w 6668 nameserver len 28
000007 25May2000 6:17:03 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 6669 x.x.x.x w.w.w.w 6669 nameserver len 28
000008 25May2000 6:17:05 y.y.y.y drop x.x.x.x z.z.z.z icmp 35 x.x.x.x w.w.w.w icmp-type 8 icmp-code 0
000009 25May2000 6:17:10 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 6649 message SYN -> SYN-ACK -> RST
000010 25May2000 6:17:10 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 6648 message SYN -> SYN-ACK -> RST
000011 25May2000 6:17:10 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 6647 message SYN -> SYN-ACK -> RST
000012 25May2000 6:17:10 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 6646 message SYN -> SYN-ACK -> RST
000013 25May2000 6:17:10 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 6645 message SYN -> SYN-ACK -> RST
000014 25May2000 6:17:10 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 6644 message SYN -> SYN-ACK -> RST
000015 25May2000 20:23:51 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 8193 x.x.x.x w.w.w.w 8193 nameserver len 28
000016 25May2000 20:23:51 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 8194 x.x.x.x w.w.w.w 8194 nameserver len 28
000017 25May2000 20:23:51 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 8195 x.x.x.x w.w.w.w 8195 nameserver len 28
000018 25May2000 20:23:51 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 8196 x.x.x.x w.w.w.w 8196 nameserver len 28
000019 25May2000 20:23:51 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 8197 x.x.x.x w.w.w.w 8197 nameserver len 28
000020 25May2000 20:23:51 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 8198 x.x.x.x w.w.w.w 8198 nameserver len 28
000021 25May2000 20:23:51 y.y.y.y drop nameserver x.x.x.x z.z.z.z udp 35 8199 x.x.x.x w.w.w.w 8199 nameserver len 28
000022 25May2000 20:23:53 y.y.y.y drop x.x.x.x z.z.z.z icmp 35 x.x.x.x w.w.w.w icmp-type 8 icmp-code 0
000023 25May2000 20:23:58 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 8179 message SYN -> SYN-ACK -> RST
000024 25May2000 20:23:58 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 8178 message SYN -> SYN-ACK -> RST
000025 25May2000 20:23:58 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 8177 message SYN -> SYN-ACK -> RST
000026 25May2000 20:23:58 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 8176 message SYN -> SYN-ACK -> RST
000027 25May2000 20:23:58 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 8175 message SYN -> SYN-ACK -> RST
000028 25May2000 20:23:58 y.y.y.y reject http x.x.x.x z.z.z.z tcp 0 8174 message SYN -> SYN-ACK -> RST
```

Les requêtes DNS sont effectuées sur toute machine y compris celle qui ne possède pas de serveur de DNS.

Une telle signature peut être le signe d'une « mesure » de votre site. Dans ce cas, nous vous demandons de bien vouloir en informer le CERTA.

Ne transmettez *jamais* les journaux de vos gardes barrières à des tiers. Les journaux ne doivent être communiqués qu'à des organismes de confiance comme votre CERT de tutelle. En France, il s'agit des CERT-RENATER, du CERT-IST et, pour l'administration, du CERTA.

Historique du document

26 mai 2000 première version.