Des serveurs Linux enrôlés sur les botnets IptabLes et IptabLex

Prolexic, filiale d'Akamai Technologies, lance aujourd'hui une alerte au sujet des infections de systèmes Linux. Les attaquants se sont appuyés sur les failles de certains produits OpeS source, comme **Elasticsearch, Struts ou Tomcat**, pour installer un malware sur des serveurs Linux.

Les machines passent alors sous le contrôle des pirates, qui les utilisent afin de créer un botnet lançant **des attaques par déni de service** (DDoS) sur divers sites de la Toile. Essentiellement des sites orientés divertissements, pour le moment. Un débit de 119 Gb/s a pu être constaté lors de l'une des attaques.

Il est à noter que les malwares communiquent avec des serveurs situés en Chine (ce qui ne veut pas dire que les pirates se trouvent eux-mêmes en Chine, bien entendu).

Des dégâts encore limités

Les deux botnets basés sur ces systèmes infectés, **IptabLes et IptabLex**, montrent encore des signes d'instabilité, précise Prolexic. Toutefois, des versions plus stables pourraient apparaître dans le futur, et renforcer ainsi les nuisances provoquées par ces botnets.

À ce jour, seuls 23 antivirus sur 54 testés par VirusTotal détectent la présence de cette menace sur une machine. Toutefois, une méthode simple permet de repérer un système infecté : des fichiers '.IptabLes' et '.IptabLex' se trouvent en effet dans le dossier de démarrage du système (en général /boot).

Sur le même thème

Desktop : Linus Torvalds espère toujours que Linux supplantera Windows
Plus de 1500 applications certifiées pour Linux on Power d'IBM
ARM s'affiche en star du noyau Linux 3.16