



LES TENDANCES DE JUILLET ET AOÛT 2007



Baromètre des failles du système d'information

	Microsoft Windows	Unix											Novell	
		Linux				BSD			SCO	HP-UX	IBM	Sun		SGI
		Debian	Mandrake	Red Hat	Suse	Free BSD	Open BSD	Net BSD	Caldera		AIX	Solaris	Irix	
Bulletins émis par les éditeurs	15	38	31	17	13	3	1	0	0	5	6	21	0	1
Classement														
Haute	10	11	7	8	6	3	0	3	-	3	-	2	-	-
Moyenne	9	18	11	12	14	6	1	9	-	2	4	8	-	-
Basse	6	12	16	9	8	7	1	5	-	4	3	12	-	1
Nombre total d'alertes	25	41	34	29	30	16	2	17	0	9	7	22	0	1

- Pour les Unix, il s'agit du nombre de vulnérabilités affectant l'OS en tant que tel ainsi que celles affectant les différents packages pouvant être installés dessus.
- Le nombre de vulnérabilités retenues concerne les nouvelles vulnérabilités (apparues au cours des mois de juillet et août 2007) ainsi que celles pour lesquelles de nouveaux patches correctifs sont apparus.
- Un bulletin d'alerte émis par un éditeur peut concerner plusieurs vulnérabilités.



Marc Guillaumot

Joël Rivière,

fondateur de Lexsi

Spécialiste des problèmes de sécurité, Joël Rivière a dirigé pendant cinq ans le département informatique de l'Institut de recherche criminelle de la gendarmerie nationale. En 1999, il fonde Lexsi, cabinet de conseil en sécurité.

<http://www.lexsi.com>

Attaques à l'échelle industrielle

Mi-juin 2007, les équipes du Cert-Lexsi ont mis au jour l'intégralité d'une fraude au vol d'informations bancaires, emblématique de la menace que représentent les *malwares* bancaires.

L'activité des milliers de serveurs frauduleux sur lesquels se connectent les programmes malicieux les plus virulents était sous surveillance : il s'agissait de profiter des erreurs d'administration commises par les fraudeurs pour accéder au contenu des serveurs quelques heures durant. Cette veille nous a permis de visualiser la quasi-intégralité d'un serveur mère (*motherhip server*) synchronisant et regroupant l'activité de dizaines de versions de *malwares*, et centralisant le stockage des données volées massivement.

Le Cert-Lexsi a ainsi pu récupérer les données volées, appartenant à trois cent mille victimes à travers le monde, et a pris contact avec les établissements bancaires les plus touchés pour bloquer la majorité des millions d'identifiants transactionnels et numéros de cartes bancaires, représentant un potentiel de fraude de plusieurs centaines de millions d'euros.

Les infections actives ont été réalisées par plusieurs dizaines d'individus, «clients» d'un groupe plus structuré gérant de manière centralisée l'ensemble de l'infrastructure, le développement des *malwares*, l'hébergement et le traitement des données. Ce groupe russophone offre des prestations professionnelles via un service central de gestion de tickets d'incidents ; chaque client dispose d'une variante unique du *malware*, à son nom, et chiffré avec une clé unique. Les mises à jour de code sont intensives afin que les attaques puissent rester furtives vis-à-vis des programmes antivirus : plusieurs nouveaux exécutables uniques sont produits chaque jour pour alimenter et maintenir cette organisation.

Pour autant, plusieurs «clients» continuent de maintenir des activités moins rentables comme les sites de *phishing* traditionnels. RBN, Lug Link et Neva Con sont les trois réseaux liés pour l'hébergement de cette fraude.

Cette fraude démontre donc combien les attaques présentent des objectifs financiers évidents et sont effectuées à échelle industrielle.

MÉTHODOLOGIE

Les équipes de Lexsi ont répertorié les vulnérabilités susceptibles d'affecter les systèmes d'information (voir tableau ci-dessus). Ce recensement provient de deux sources : les bulletins d'alerte des éditeurs/constructeurs et la surveillance

ce sur le terrain des spécialistes en sécurité du laboratoire. La cellule de veille technologique de Lexsi a classé les failles selon le degré d'importance des dégâts. L'ampleur des dommages a été évaluée en fonction de l'architecture des systèmes attaqués.