

## **PC Tools remet en question l'approche des classements des menaces informatiques**

**PC Tools, l'éditeur de logiciels anti-spywares et de technologies sécuritaires PC Tools a déclaré aujourd'hui qu'il remettait en question l'approche quant aux classements des menaces informatiques établis et publiés par les acteurs de la sécurité informatique. Il avance que la plupart de ces classements répertorient uniquement les menaces en fonction de leur quantité, sans aucune référence au véritable danger qu'elles représentent pour les consommateurs.**

PC Tools indique que de tels classements ne reflètent pas la réelle situation des menaces, et ne sont pas d'une grande utilité pour l'industrie de la sécurité informatique ou pour les consommateurs.

*« L'analyse des menaces informatiques est quelque chose de très complexe. Il fût un temps où le nombre de virus et autres malwares en activité suffisait à évaluer le niveau de menace »,* indique Simon Clausen, PDG de PC Tools. *« Mais ces menaces ont considérablement évolué et, hormis leur nombre, de nombreux autres paramètres entrent désormais en considération. Ces derniers sont même plus importants dans l'identification et le classement des menaces. »*

Outre la quantité, PC Tools a identifié trois autres paramètres qui pourraient permettre d'identifier et de classer les menaces informatiques:

- La complexité d'un virus ou d'un malware et le défi que cela représente pour les détecter et les supprimer.
- L'adoption de nouvelles techniques et leur réactivité quant à la détection.
- Le danger qu'un virus ou un malware représente pour le système et le type de contenu nuisible qu'il transporte.

Par exemple, les spécialistes de la sécurité informatique chez PC Tools indiquent que **Netsky**, qui a été mis à jour il y a quatre ans, apparaît encore dans les classements des malwares les plus nuisibles, en raison de son taux de propagation élevé. Pourtant, les recherches conduites par PC Tools ont montré que la menace réelle que représente Netsky serait surestimée. Kurt Baumgartner, Directeur du département des menaces informatiques chez PC Tools, déclare que *« le comportement de Netsky et ses caractéristiques sont bien connus des experts de l'industrie des anti-malwares. Des logiciels gratuits détectent et suppriment Netsky facilement. Par conséquent, nous pensons qu'il ne s'agit pas tout à fait d'un malware comme l'ont annoncé d'autres fabricants de sécurité informatique. »*

Autre exemple d'approche inappropriée : la détection de « cheval de Troie ». Des éditeurs de logiciels de sécurité informatique ont assimilé la détection générique de **NSAnti** à une « menace à haut risque ». La détection de « NSAnti » reconnaît simplement le contenu d'un programme et que celui-ci peut dissimuler un virus lors d'une analyse. Mais le « cheval de Troie » lui-même n'est pas un virus et PC Tools considère que ce dernier ne devrait pas figurer dans les classements de menaces informatiques.

Les recherches menées par le leader australien ont également permis de révéler que les utilisateurs sont souvent infectés à cause de défaillances sur leur système informatique qui ne sont pas réparées, comptant ainsi pour beaucoup dans le taux de propagation élevé des menaces plus anciennes et bien connues qui résistent aux anti-virus. Bien que la majorité des fabricants aient commercialisé il y a quelques années des solutions pour y remédier, certains systèmes informatiques continuent d'être infectés à cause de ces défaillances.

*« Cette conjoncture assez banale montre que soit les utilisateurs ne mettent pas à jour leurs ordinateurs afin de les protéger contre ces défaillances, ce qui entraîne une infection des systèmes, soit les consommateurs utilisent des versions piratées de logiciels de sécurité. Celles-ci nécessitent souvent des mises à jour automatiques pour être désactivées afin de ne pas être détectées en tant que copies piratées, laissant ainsi les utilisateurs vulnérables aux virus, »* poursuit Baumgartner.

Ce dernier prévient également que *« les utilisateurs continuent de se faire piéger par des méthodes qui sont, certes, persuasives, mais qui sont désormais répandues. »*

PC Tools souligne qu'avec l'arrivée de la nouvelle génération de malwares 2.0, l'analyse des futurs virus sera plus complexe que celle pour des virus actuels, comme les classements le laissent penser.

*« Pour un certain nombre de raisons, ces classements apportent peu, voire rien à l'utilisateur moyen. Tout d'abord, ils ne reflètent pas la réalité de la situation actuelle des différentes menaces informatiques. Ensuite, ils ne donnent pas de renseignement sur une protection adéquate. Enfin, dans le meilleur des cas, la plupart des fabricants ne publie ces classements qu'une fois par mois, »* déplore Simon Clausen.

L'éditeur australien encourage donc les fabricants à considérer les classements des menaces informatiques de façon plus régulière, avec une approche davantage multi-dimensionnelle, en identifiant avant tout les menaces par rapport au véritable danger que ces dernières représentent. PC Tools prend en compte d'autres paramètres tels que la complexité des menaces et leur contenu nuisible. Cette approche donnera aux utilisateurs des informations à jour, utiles et réelles concernant les virus.

### **En bref, l'actualité des menaces informatiques :**

- Un certain nombre de bots montrent des caractéristiques suffisamment élaborées pour contourner les logiciels de sécurité informatique et sont capables de diffuser quotidiennement des milliards de spams. Les menaces les plus sérieuses sont **Kraken/Bobax, Srizbi, Citwail/Pandex** et **Storm**.
- De nouvelles recherches révèlent la "reconversion" réussie d'anciennes ruses telles que l'infection de fichier par **Trats/Vundo/Virtumonde** ou bien encore l'infection Master Boot Record par Mebroot. Le fait d'associer les anciennes techniques de l'ère du système DOS avec les techniques avancées d'aujourd'hui crée des combinaisons extrêmement nuisibles, telles que **Torpig/Mebroot**. Celle-ci est capable de prendre le contrôle de systèmes informatiques tout en échappant à la détection des logiciels anti-malwares.
- Le phénomène grandissant des spywares du type **Zlob/FakeAlert**, destinés à des fins financières frauduleuses, adopte de plus en plus de nouvelles méthodes de propagation, parmi lesquelles les programmes "pay-per-click", les malwares infiltrés dans les réseaux communautaires et autres techniques associées avec des auteurs du "camp malware. »

Ce communiqué de presse s'inscrit dans le cadre d'une démarche destinée à présenter aux consommateurs comment assurer facilement la sécurité de leur système informatique.

### **A propos de ThreatFire :**

ThreatFire utilise une technologie brevetée élaborée afin de détecter tout signe de comportement nuisible couramment utilisé par les virus malware. ThreatFire est différent des logiciels anti-virus traditionnels qui se basent sur la technologie de la signature et qui nécessitent une mise à jour à chaque apparition d'un nouveau virus. La technologie ActiveDefence de ThreatFire est capable d'identifier et de neutraliser les virus qui sont trop récents ou trop sophistiqués pour être reconnus par un logiciel de sécurité traditionnel.

#### **A propos de PC Tools**

Basée à Sydney, PC Tools est une société australienne éditrice de solutions de sécurité informatique, notamment connue pour ses produits phares récompensés à plusieurs reprises par les professionnels informatiques : ISpyware Doctor, Registry Mechanic, Privacy Guardian, PC Tools Antivirus.

Malware Research Center, le centre de recherche et de lutte contre les malwares de PC Tools surveille les tendances du marché et identifie les problématiques émergentes en matière de spywares afin d'élaborer des solutions de sécurité destinés aux particuliers et aux entreprises. Etablie à Sydney, la société a de nombreuses filiales à San Francisco, Londres, Dublin, Melbourne et Kiev, qui couvrent le marché informatique au niveau international. PC Tools travaille avec un réseau international de distributeurs et de revendeurs.

**Spyware Doctor** a été désigné « meilleur anti-spyware 2005 » par PC Magazine, « meilleur anti-spyware 2006 » par PC Advisor et Computer Shopper Best et « produit phare 2006 » recommandé par les magazines PC Pro, Windows XP Magazine, PC Answers.

**Plus d'informations sur [www.pctools-fr.fr](http://www.pctools-fr.fr)**

#### *Contact Presse*

AGENCE AUVRAY & ASSOCIES  
Judith ROZENBLUM / Sandrine AUVRAY  
97, boulevard Malesherbes – 75008 PARIS  
Tél. : 01 58 22 25 95 – Fax : 01 42 93 08 01  
[pctools@auvray-associes.com](mailto:pctools@auvray-associes.com)