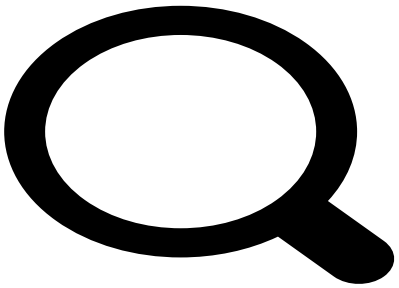
Alerte Ransomware : Attaque massive dans le doc | Le Net Expert Informatique

	Alerte Ransomware : Attaque massive dans le doc

Depuis ce mardi matin, des milliers de courriers malveillants visent entreprises et collectivités locales françaises. Prudence !

Ils se font passer pour des fax en attente ou pour un communiqué de presse. Ils sont cachés dans des courriels publiés ce mardi matin, dans une diffusion massive et malveillante. ZATAZ.COM a pu en référencer 300 différents, en quelques minutes. Des courriers électroniques contenant des pièces jointes qu'il ne faut surtout pas ouvrir. Des fichiers Word, PowerPoint piégés. Ils vont chercher sur la toile un code malveillant qui, dans la majorité des cas, était un ransomware ou encore le code pirate Dridex.

Dridex, est un outil qui exploite la technologie du peer-to-peer (P2P) afin d'attaquer le contenu des ordinateurs infiltrés. Mission, mettre la main sur des données bancaires. Le département américain de la Sécurité intérieure (DHS), en collaboration avec le Federal Bureau of Investigation (FBI) et le ministère de la Justice (DOJ) ont publié une alerte quelques heures après l'annonce de ZATAZ, preuve que cette diffusion massive est à échelle internationale.

Dridex est un ensemble de logiciels malveillants multifonctionnel qui exploite le langage Macro proposés dans les outils de Microsoft. L'objectif principal de Dridex est d'infecter les ordinateurs, voler des informations d'identification, et obtenir l'argent des comptes bancaires des victimes infiltrées. Exploitée principalement comme un cheval de Troie bancaire, Dridex est généralement distribué par courrier électronique, comme le cas de ce lundi matin.

Un système infecté par Dridex peut être utilisé pour envoyer du spam, participer à DDoS… la question est de savoir pourquoi une telle attaque, en pleine semaine. Le bot des pirates a-t-il été mis en action car le besoin en données bancaires se fait sentir chez les malveillants après les dernières importantes arrestations dans le monde du carding international ?

Microsoft propose un outil pour scanner votre ordinateur à la recherche du malveillant code : http://www.microsoft.com/security/scanner/en-us/default.aspx

---

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.zataz.com/attaque-massive-ransomware-dans-le-doc/
Par Damien Bancal