Nouvelle version de Conficker, avec une utilisation plus intensive du DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 mars 2009. Dernière mise à jour le 30 mars 2009

https://www.bortzmeyer.org/conficker-version-c-et-le-dns.html

---

L'une des originalités du ver Conficker est qu'il utilise des noms de domaine et pas des adresses IP pour contacter son maître, afin de lui demander des mises à jour, des listes d'actions à effectuer, etc. Mais la nouvelle version, analysée il y a quelques jours, pousse cette logique encore plus loin.

L'ancienne version avait été bien analysée dans des articles comme " *Detecting Conficker in your Network*" <http://www.cert.at/static/conficker/TR_Conficker_Detection.pdf> ou " *An Analysis of Conficker's Logic and Rendezvous Points*" <http://mtc.sri.com/Conficker/>. Une mise en œuvre complète se trouve en <http://mhl-malware-scripts.googlecode.com/files/downatool.zip>. Dans cette ancienne version, Conficker se connecte à son maître via un nom de domaine, dans huit domaines de tête possibles comme .com ou org. Ce n'était pas assez pour le ver : dès que son code a été analysé, plusieurs registres ont bloqué les noms en question, empêchant leur utilisation.

Mais cette version n'est plus complètement d'actualité : Conficker nouvelle mouture, analysé dans "*W32.Downadup.C Digs in Deeper*" <https://forums2.symantec.com/t5/Malicious-Code/W32-Downadup-C-Di
ba-p/393245> et dans "*Conficker Call-home Protocol v2*" <http://www.sophos.com/security/blog/2009/03/3484.html>, fait mieux en générant de très longues listes de noms de domaines, dans presque tous les domaines de tête, rendant ainsi plus difficile le blocage. Un rapport encore plus complet a été publié (avertissement : c'est très technique), " *Conficker C Analysis*" <http://mtc.sri.com/Conficker/addendumC/>, avec presque tous les détails.

Il ne semble pas que ces nouveaux noms aient été activés. L'ICANN a demandé <http://lists.aftld.org/pipermail/aftld-discuss/2009-March/000287.html> à tous les TLD de les bloquer. Certains se sont exécutés comme l'ACEI qui l'a annoncé dans un communiqué <http://www.acei.ca/pr-conficker/>.

Sur Conficker C, on peut aussi consulter :

- Le site du groupe de travail Conficker <http://www.confickerworkinggroup.org/>, organisation privée qui regroupe Microsoft et des éditeurs d'anti-virus,
- L'avis <http://www.us-cert.gov/cas/techalerts/TA09-088A.html> lancé par le CERT états_unien,
- L'article <http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx> de Microsoft (attention, Microsoft appele D la version C),
- "*Detecting and Containing Conficker - Management Overview*" <https://www.honeynet.org/node/389>.