Vault 7 : WikiLeaks dans le rôle de l'arroseur arrosé

WikiLeaks poursuit la diffusion de fuites d'information de sa série **Vault 7** sur les outils de piratage exploités par la CIA.

Hier (31 août), la plateforme de leaks de Julian Assange a dévoilé le projet **Angelfire**, un ensemble de cinq outils visant à maintenir une backdoor persistante sur une machine infectée et installer des logiciels dédiés à l'usage de l'agence américaine du renseignement.

Angelfire se compose de Solartime, Wolfcreek, Keystone (MagicWand auparavant), BadMFS, et Windows Transitory File system (TFS).

« Comme les projets CIA précédemment publiés (Grasshopper et AfterMidnight) dans la série Vault7, il s'agit d'un framework persistant qui peut charger et exécuter des implants personnalisés sur des ordinateurs cibles exécutant le système d'exploitation Microsoft Windows (XP ou Win7) », indique WikiLeaks.

Qui détaille le rôle de chacun des outils : Solartime modifie le secteur de démarrage de la partition afin d'exécuter l'implant Wolfcreek chargé d'installer et exécuter d'autres pellets. Dont Keystone qui lance des applications malveillantes.

La plateforme alternative, qui prône la transparence dans la gestion des affaires du monde et dans la vie politique, souligne que *« les implants chargés ne touchent jamais le système de fichiers, donc il y a très peu de traces de l'exécution du processus »*.

BadMFS est utilisé pour collecter tous les pilotes et implants démarrés par Wolfcreek. *« Tous les fichiers sont chiffrés ou cachés pour éviter les détections »*, affirme le site.

Enfin, Windows TFS est utilisé pour installer Angelfire. Notons que le document propre à Wolfcreek est daté de novembre 2011.

Si l'existence de l'outil remonte à quelques années, la poursuite de son exploitation aujourd'hui n'est pas à exclure même si des correctifs sont censés avoir été développés depuis.

WikiLeaks piraté par OurMine

Fait du hasard ou manœuvre calculée, au moment ou WikiLeaks diffusait ces nouvelles révélations, un piratage s'est produit. Une opération revendiquée par le groupe OurMine.

Cette organisation aux intentions mystérieuses s'est contentée de remplacer la page d'accueil de la plateforme adulée des lanceurs d'alertes par un message revendicatif.

« Bonjour, c'est OurMine (Security Group), ne vous inquiétez pas, nous testons votre … Blablablab, oh attendez, ce n'est pas un test de sécurité ! Wikileaks, rappelez-vous quand vous nous avez défié de vous pirater? », a affiché le ou les pirate(s), selon cette capture retweetée.

Le message se poursuit en interpellant les Anonymous à qui OurMine reproche visiblement d'avoir tenté de le manipuler.

Pour certains, dont Raven, WikiLeaks n'a pas été piraté mais victime d'une «simple» redirection d'adresse IP par attaque DNS. On pourra discuter de la nuance tant le résultat est à peu près le même. Dans tous les cas, la page de WikiLeaks a rapidement retrouvé ses couleurs habituelles.

OurMine n'est pas inconnu dans le domaine de la sécurité. Ce groupe est à l'origine des piratages de comptes de personnalités de l'industrie informatique comme Mark Zuckerberg (CEO fondateur de Facebook), Sundar Pichai (CEO de Google), ou encore Brendan Iribe (co-fondateur d'Oculus). Sans jamais chercher à extorquer ses victimes ou détruire leurs données.

L'intention est peut-être purement promotionnelle. Sur son site, le groupe propose ses services pour sécuriser les systèmes des entreprises.

« En tant que pirates professionnels et évaluateurs de vulnérabilité, nous vous aiderons à sécuriser votre réseau, à vous montrer toutes les vulnérabilités disponibles et à les réparer », peut-on y lire.

Les opérations de piratage pourraient donc être considérées comme des campagnes publicitaires… à la légalité douteuse.

Lire également
Quand la CIA installait des spywares pour surveiller le FBI et la NSA
https://www.silicon.fr/vault-7-wikileaks-devoile-les-rapports-caches-entre-la-societe-de-securite-raytheon-et-la-cia-180881.html
Apple agacé par les révélations de Wikileaks

Crédit photo : Louis Lumière – http://www.moma.org/collection/browse_results.php?object_id=107633, PD-US, Link