Une victime du virus Windigo témoigne

	Une victime du virus Windigo témoigne ! Le 19 mars dernier, je vous informais au travers d'un article (http://www.lenetexpert.fr/alerte-virus-windigo) de la découverte du virus Windigo par une équipe de spécialistes en sécurité. Quelques semaines après les premières attaques, En exclusivité pendant 24h sur notre site, le gérant d'une entreprise internationale touché par ce virus témoigne sur les dégâts qu'il a subit.

Une victime du virus Windigo témoigne !

Le 19 mars dernier, je vous informais au travers d'un article de la découverte du virus Windigo par une équipe de spécialistes en sécurité.

Quelques semaines après les premières attaques, le gérant d'une entreprise internationale témoigne sur les dégâts qu'il a subit.

Pour rappel, cette importante opération a généré des attaques sur plus de 25 000 serveurs UNIX dans le monde entier.

Windigo, a été découverte il y a quelques semaines par l'équipe de chercheurs en sécurité d'ESET , en collaboration avec le CERT-Bund (Allemagne), l'agence nationale suédoise de recherche sur les infrastructures réseau (SNIC) et d'autres agences en sécurité.

Pour rappel, cette importante opération, contrôlée par un gang de cybercriminels, a généré des attaques sur plus de 25 000 serveurs UNIX dans le monde entier.

A l'apogée de Windigo, ont été envoyés 35 millions de pourriels par jour et 500.000 internautes ont été redirigés vers des sites malveillants.

Pierre-Marc Bureau, Directeur du programme Security Intelligence d'ESET déclare :

« ESET a investi des mois d'efforts pour analyser, comprendre et expliquer l'Opération Windigo. A l'acmé des analyses, 6 chercheurs ont enquêté. Nous sommes très fiers des résultats actuels et continuons de surveiller la situation. Tous les serveurs n'ont pas été nettoyés et le gang malveillant à l'origine de l'opération contrôle toujours des ressources importantes. Il y a encore beaucoup de travail à effectuer ! »

Témoignage d'une victime du virus Windigo

Résumé de l'entretien avec François Gagnon*, dirigeant d'une entreprise dont les serveurs en France et au Canada ont été les victimes de ces attaques pendant plusieurs semaines.

Il explique comment une entreprise internationale peut devenir la proie de cybercriminels sans s'en apercevoir. Ce témoignage a été recueilli par Pierre-Marc Bureau.

« Comme toutes les entreprises de notre taille, nous savons que nous sommes la cible de cybercriminels, mais nous n'avions jamais fait l'objet d'une attaque sérieuse. Au début nous n'avions pas mesuré l'ampleur de cette attaque. C'était subtil. Personne n'avait jamais volé nos bases de données. Mais nous ne ressentions pas cela comme une attaque offensive, le malware a été exécuté silencieusement. Je pense que c'est pourquoi il avait infecté tant de serveurs avant que les gens commencent à réagir (…) La première chose que l'on sait dans n'importe quelle entreprise IT est que rien n'est impossible (…) Je suppose que nos serveurs ont été infectés quelques semaines avant.

Lorsque nous nous en sommes aperçus, nous avons poussé l'enquête. C'est là que nous nous sommes rendu compte que les serveurs ont été infectés après l'ouverture de tickets avec cPanel. Leurs serveurs étaient infectés et ils ont donc infectés les nôtres via une connexion SSH. (…) Nous avons d'abord pensé à une attaque ciblée, puis nous nous sommes aperçus que beaucoup d'autres entreprises se posaient les mêmes questions avec des récits de comportements étranges sur de nombreux forums. (…) Nous avons rapidement été contactés par ESET qui nous a informé de l'ampleur de l'infection, nous avons très vite été en étroite collaboration. ESET nous a conseillé de nettoyer et réinstaller nos serveurs. Certains serveurs ont été utilisés pour aider les chercheurs à comprendre l'infection. (…) Nous avons été une cible, tout simplement parce que nous avons beaucoup de serveurs, et de nombreux clients en France et au Canada (…). Nous remercions ESET qui a été réactif pour nous venir en aide (…), nous n'avons pas souffert de graves pertes financières.
La réputation de notre entreprise n'a pas été impactée. (…) Nous sommes pleinement opérationnels aujourd'hui. »

*A sa demande et pour des raisons de sécurité, le blog a utilisé un faux nom pour notre interlocuteur. Le gang derrière Windigo est toujours en fuite et les représailles sont une possibilité.

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Sources :

Welivesecurity, ESET: Interview