Furtim, le malware qui détruit les solutions de sécurité.

	Furtim, le malware qui détruit les solutions de sécurité

Alors que de nouveaux malwares sont découverts quasiment chaque jour, voilà que l'un d'entre eux fait beaucoup parler. Il s'agit de Furtim, un #logiciel malveillant qui se caractérise par sa faculté à détruire les solutions de sécurité présentes sur le PC infecté.

Si l'on en croit nos confrères de Silicon, un nouveau malware a été découvert par les équipes d'EnSilo. Comme son nom l'indique, Furtim est capable de passer inaperçu sur les machines qu'il a réussi à infecter.

Probablement crée par des hackers d'Europe de l'Est, ce malware se compose d'un driver qui scanne le PC infecté, d'un module downloader, d'un gestionnaire d'alimentation, d'un voleur de mots de passe et d'un module de communication serveur.

Toutefois, avec une telle composition, impossible de comprendre comment fonctionne réellement ce malware. Pour l'heure, Furtim apparait seulement comme un logiciel malveillant très sophistiqué et capable d'analyser son environnement avant de s'exécuter. Pour cela, il va scanner la machine infectée pour détecter les solutions de sécurité et les outils de filtrage DNS.

Preuve que les pirates ont pensé à tout, Furtim bloque l'accès à de nombreuses sites spécialisés dans la sécurité informatique et à des forums d'aide à la désinfection et désactive les notifications Windows, le gestionnaire des tâches et diverses autres fonctionnalités.

Furtim, un éclaireur en vue de futures attaques

Selon les premières recherches menées par les équipes d'EnSilo, Furtim n'aurait probablement pas vocation à agir seul puisqu'il pourrait bien uniquement jouer un rôle d'éclaireur.

En effet, puisqu'il est capable de déjouer les outils de sécurité, il pourrait être utilisé pour introduire des menaces sur des PC sans que cela ne soit décelable… [Lire la suite]

Réagissez à cet article

Source : *Furtim, le malware qui détruit les solutions de*

sécurité

Auteur : Fabrice Dupuis