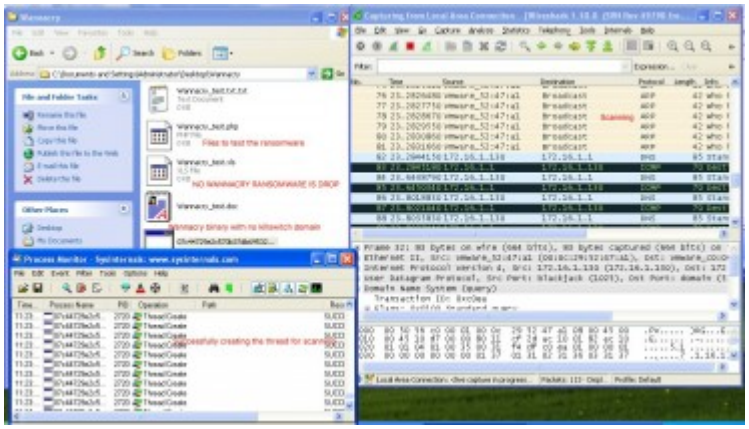
WannaCry et maintenant les variantes !

Le monde a connu un véritable blietzkrieg mené par le ransomware WannaCry. Sa facile duplication au sein des réseaux, en a fait une arme redoutable. Un jeune hacker, @malwaretechblog, a réussi cependant à freiner la propagation du virus en découvrant un « kill switch » caché dans le code. Il s'agissait d'un nom de domaine libre : *iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.* Ce système est une sécurité imaginée par les développeurs du malware, afin d'éviter les analyses par les systèmes de sécurité basée sur des sandbox.

Une variante sans kill switch

Une pause salutaire, mais éphémère, comme l'explique le jeune hacker son blog. « *Notre système de screening n'a arrêté que cet échantillon, et rien n'empêche les hackers de supprimer la vérification du domaine et d'essayer à nouveau.* »

Effectivement, les cyber-escrocs derrière WannaCry ont rapidement mis à jour la souche du ransomware. Le hacker Matt Suiche et Kaspersky Lab ont découvert des variantes intégrant de nouveaux kill switch, bloquées temporairement par l'achat de ces nouveaux noms de domaines. Plus inquiétant, Kaspersky a livré un échantillon d'un dérivé de WannaCry ne comprenant pas de kill switch. Ce sample est difficile à analyser, souligne l'éditeur, car il est partiellement corrompu.

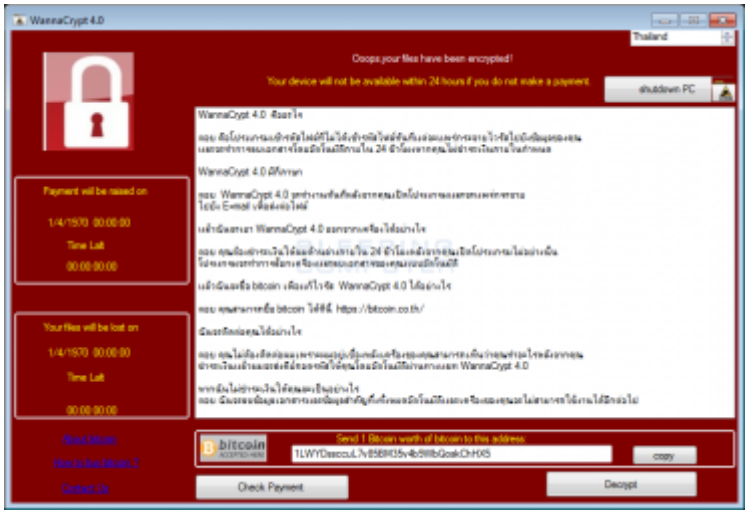


Les copycats personnalisables fleurissent

Dans la même veine, nos confrères de *Bleepincomputer* ont dégoté des variantes de WannaCry avec comme élément commun, une personnalisation du rançongiciel en fonction des cibles. Premier de ces imitations, **DarkoderCrypt0r** semble le plus avancé en reprenant la fenêtre de WannaCry et en le personnalisant à ses couleurs (titre, adresses bitcoin). La différence avec son sinistre homologue est que DarkoderCrypt0r ne fait que chiffrer les données en ajoutant l'extension .Darkcry.

Seconde imitation: **Aron WanaCrypt0r 2.0 Generator v1.0**. Cette déclinaison donne au développeur une grande possibilité de personnalisation de l'écran de verrouillage. Le texte, la couleur et les images de cette fenêtre sont adaptables. Par contre la variante ne permet pas de personnaliser l'exécutable du ransomware, qui reste la souche WanaCrypt0r.

La copie **WannaCrypt 4.0** est pour l'instant en plein développement. Elle est orientée vers la Thaïlande, car la langue par défaut pour l'écran de verrouillage est le thaïlandais. Une adaptation probablement réalisée par un développeur adepte de cette langue, car la version originale de WannaCry ne supportait pas le thaïlandais.



Enfin, **Wanna Crypt v2.5** en est à des balbutiements. Pour l'instant, seul l'écran de verrouillage s'affiche. On peut remarquer un menu déroulant pour permettre de choisir sa langue.

D'autres imitations devraient suivre pour amplifier une diffusion déjà bien répandue.

A lire aussi :

WannaCry : autopsie du ransomware 2.0, boosté par les exploits de la NSA

La parade n'existe pas pour contrer les futures affaires WannaCry