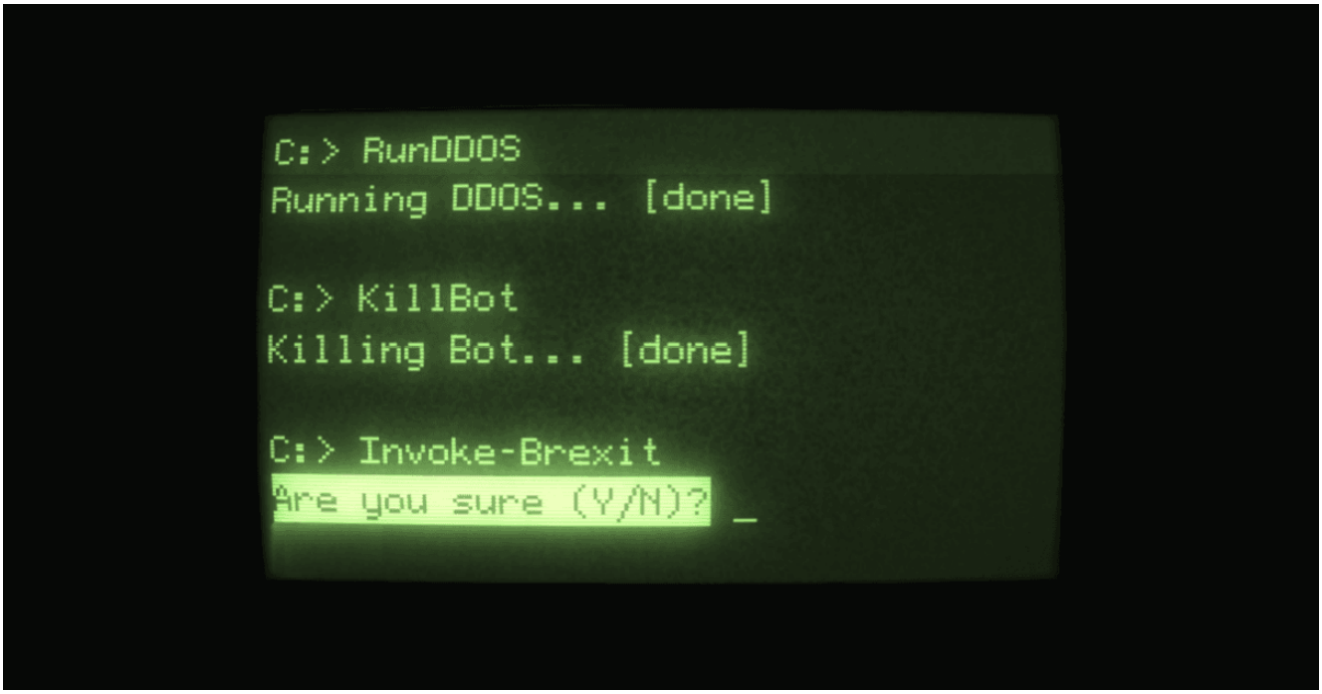
WannaMine : Même les cybercriminels veulent avoir leur mot à dire sur le Brexit !

news.sophos.com/fr-fr/2020/01/22/wannamine-meme-cybercriminels-veulent-avoir-mot-a-dire-sur-brexit/

Sophos France January 22, 2020



Et il semble que bien plus de personnes que l'on ne pourrait s'imaginer soient fascinées ou aient des idées bien arrêtées sur le Brexit !

En effet, les créateurs de malwares semblent vouloir se faire entendre à ce sujet …

A une époque bien révolue où les cybercriminels ne savaient pas encore comment faire véritablement de l'argent avec les malwares, ils avaient tendance à laisser les virus se déchaîner pour diverses raisons, à des fins politiques, pour encourager leurs équipes préférées, pour causer de sérieux dégâts au sein de la société, pour se vanter auprès d'amis imaginaires, pour célébrer des évènements et des anniversaires et, dans un cas tristement célèbre, pour nous dire à tous : "Beer and tequila forever!".

Parfois, les messages étaient évidents, tels que des boîtes contextuelles qui apparaissaient, la lecture de fichiers audio, des fichiers mis à la poubelle à des jours bien précis.

Et parfois, ils étaient cachés, enfouis comme un trésor dans le code du malware lui-même, de sorte que si vous ne saviez pas où ni comment les chercher, vous n'aviez aucune chance de percer leur secret.

Eh bien, l'art du commentaire politique caché dans les malwares n'est pas mort !

Dans un certain nombre d'attaques récentes, les SophosLabs ont rencontré une **variante de la famille de malware WannaMine** qui était suffisamment similaire aux autres échantillons de cette même famille pour deviner ces intentions, mais avec un changement sournois et inattendu juste à la fin du script principal de ce dernier.

La famille de malware WannaMine

Vous vous souvenez peut-être de **WannaMine** quand il est apparu pour la première fois : il doit son nom au fait qu'il était capable de se propager de manière virale comme le faisait le *ransomware WannaCry*, ce qui lui a donné la partie **Wanna** au début, mais au lieu de diffuser un ransomware, il vous proposait un logiciel de minage de cryptomonnaie à la place, d'où le suffixe **-Mine** dans le nom.

En fait, la **famille de malware WannaMine** fait bien plus que du simple cryptojacking, bien que ce soit effectivement le code de minage qui accélère votre CPU, ralentit votre ordinateur, utilise massivement votre électricité, fait chauffer le système et garde les cryptocoins pour lui, ce qui ne devrait pas manquer d'attirer votre attention.

Contrairement aux ransomwares, qui veulent que vous sachiez qu'ils sont bien là pour que vous puissiez vous concentrer sur le paiement de la rançon afin de récupérer vos fichiers, les mineurs préfèrent rester inaperçus, car les sommes d'argent gagnées par les escrocs sont directement proportionnelles à leur durée de vie dans votre système.

Mais le coinmining est, en général, une tâche très gourmande en CPU qui a un réel impact sur votre système, par exemple au niveau de la batterie de votre ordinateur portable, de la température de votre CPU, de votre consommation d'électricité et de la vitesse avec laquelle tous vos autres logiciels fonctionnent.

Néanmoins, pendant qu'il est occupé, *certaines variantes du malware WannaMine* essaient tout de même de faire un tas d'autres choses en arrière-plan, telles que :

- Se faufiler dans la mémoire à la recherche d'identifiants pour accéder à des comptes déjà connectés.
- Cracker les mots de passe d'autres ordinateurs du réseau pour permettre de se propager davantage.
- Rechercher des ordinateurs sur le réseau qui peuvent être compromis en utilisant l'exploit ETERNALBLUE.
- Désactiver les paramètres de sécurité de Windows.
- Lancer des attaques DoS (déni de service).
- Rechercher des mises à jour pour pouvoir récupérer la dernière version du malware.

Prêt pour attaquer

Les dernières lignes du script principal configurent la partie centrale de l'attaque, comme suit :

```
$mimi = ([WmiClass] 'root\default:Window_Core_Flush_Cach').Properties['mimi'].Value
$a, $NTLM= Get-creds $mimi $mimi
$ipsu = ([WmiClass] 'root\default:Window_Core_Flush_Cach').Properties['ipsu'].Value
$i17 = ([WmiClass] 'root\default:Window_Core_Flush_Cach').Properties['i17'].Value
$scba= ([WmiClass] 'root\default:Window_Core_Flush_Cach').Properties['sc'].Value
[byte[]]$sc=[System.Convert]::FromBase64String($scba)
```

Le code PowerShell ci-dessus crée de nombreuses variables de données qui incluent un mélange de données et de code.

Par exemple, la variable `$mimi` possède une copie en mémoire du *célèbre programme Mimikatz*, un outil de récupération et de craquage de mot de passe couramment utilisé par les cybercriminels une fois qu'ils sont à l'intérieur de votre réseau.

La variable `$scba` est un outil de téléchargement qui peut être utilisé pour récupérer de nouveaux fichiers; **ba** fait référence à "*codé en base64*", car le contenu de `$scba` est immédiatement décodé en *base64* pour produire `$sc`, une autre copie en mémoire d'un programme qui, dans un monde conventionnel, serait enregistré sur le disque en tant que fichier .EXE standard.

Vous remarquerez également que les données sont extraites à l'aide de WMI, abréviation de *Windows Management Instrumentation*, signifiant ainsi que le code et les données utilisés par ce malware sont enfouis dans la base de données Windows WBEM (abréviation de *Web-Based Enterprise Management*).

En d'autres termes, même si les composants malveillants sont, à proprement parler, enregistrés sur le disque, ils ne sont pas visibles en tant que fichiers standards qu'un programme normal pourrait lire et analyser : la base de données WBEM est très similaire au registre Windows, bien que complètement différente.

NB : Au cas où, sachez que vos fichiers de base de données WMI locaux se situent généralement dans un répertoire appelé `C:\Windows\System32\Wbem\Repository`, mais soyez très prudent si vous prévoyez de les manipuler manuellement !

Montrez-moi le Brexit !

Alors, où est le Brexit ?

Dans la dernière ligne du script du malware, le créateur du virus appelle sa fonction principale "*do-the-bad-stuff*".

Plus tôt dans le code, ils étaient plutôt ennuyeux, avec des noms de fonction tels que :

```
RunDDOS
KillBot
```

Mais la dernière salve dans celui-ci est une fonction appelée comme suit :

```
Invoke-Brexit -sccccccc $sc -ipsu $ipsu -i17 $i17 -nic $nic -a $a -NTLM $NTLM
```

Ce que nous ne pouvons pas vous dire précisément, c'est si le créateur du virus a incorporé un message secret pour laisser entendre que le Brexit était une bonne chose, et si nous devrions continuer…

… ou bien s'il voulait que ce code soit une métaphore pour nous inviter à en déduire que *l'invocation du Brexit est quelque chose qu'il valait mieux éviter*.

Nous n'allons pas nous lancer dans l'expression d'une opinion publique sur le Brexit, mais nous pouvons vous dire par contre que le Brexit du créateur du virus n'est certainement pas celui que vous souhaitez !

Billet inspiré de Brexit – even cybercriminals want to have their say…, sur Sophos nakedsecurity.