The Mask ou Careto : la menace persistante la plus avancée à ce jour

A l'heure où plus de 6 000 sites web ont fermé leurs pages, ce mardi 11 février, pour protester contre la surveillance des Etats qui outrepassent le respect de la vie privée dans le cadre de l'opération The Day We Fight Back, un nouveau scandale d'espionnage pourrait se faire jour. **Kasperky annonce avoir découvert The Mask (ou Careto),** un malware encore plus évolué que Duqu, le cheval de Troie sophistiqué découvert en 2011 et réputé pour ses capacités à intercepter les données des PC Windows.

The Mask s'inscrit en effet comme un agent malveillant aussi raffiné que discret. La bestiole opère visiblement depuis 2007 et a réussi à passer entre les mailles des filets des antivirus jusqu'à janvier 2014, selon Kaspersky Lab. Soit environ **7 ans d'activité en échappant à toutes les protections** ! Ensuite The Mask se distingue la sophistication des méthodes et outils utilisés qui en font *« une des menaces persistantes les plus avancées (APT) jusqu'à présent »*, selon l'éditeur de sécurité qui détaille les exploits de The Mask et son mode opératoire dans un rapport de 65 pages (disponible en PDF).

Exploit de failles zero-day

The Mask ne se contente pas d'ouvrir une banale porte dérobée (backdoor) permettant aux attaquants d'opérer à distance, mais s'appuie sur **un ensemble de logiciels modulaires** taillés pour exploiter la moindre faille système. Y compris les failles zero-day (sans correctif).

Il en va ainsi de **l'*exploit* CVE-2012-0773 du player Flash d'Adobe** pour les versions 10.3 et 11.2, le premier qui avait permis de casser le bac-à-sable de Chrome. Un exploit démontré dans le cadre du concours CanSecWest Pwn2Own en 2012 **par la société française Vupen**. Laquelle avait refusé de révéler ses techniques de contournement du bac-à-sable du navigateur de Google revendiquant le droit de vendre ces informations à ses clients (le modèle économique de Vupen). De là à penser que les concepteurs de The Mask sont clients de Vupen… C'est en tout cas en 2012 que The Mask a connu le plus de variantes (6 en l'occurrence) au cours de sa longue carrière.

53 organisations françaises infectées

Outre les attaques zero-day, The Mask embarque rootkit et bootkit pour Windows 32 et 64 bits, mais aussi Mac OS X et probablement Linux. Ainsi que des versions Android et iPhone/iPad, soupçonne Kaspersky qui déclare également avoir détecté des attaques personnalisées sur des versions antérieures de ses propres produits. Une telle variété de plates-formes supportées laisse à penser que **The Mask se destine plus aux administrations et entreprises qu'au seul grand public**. *« Un tel niveau de sécurité opérationnelle n'est pas courant chez les groupes de cybercriminels »*, avance **Costin Raiu**, directeur de l'équipe internationale de chercheurs et d'analystes (GReAT) de Kaspersky Lab. Une façon de dire que un ou des états ou services para-étatiques sont impliqués dans la conception du malware.

De fait, l'éditeur dénombre **un millier de victimes (dont 383 au Maroc)** dont des administrations, des représentations diplomatiques et des ambassades, des compagnies pétrolières, gazières et énergétiques, des laboratoires de recherche ainsi que des activistes. **La France apparaît comme le troisième pays cible**, derrière le royaume chérifien et le Brésil. 53 organisations ont été infectées dans l'Hexagone. A ce jour, Kaspersky dénombre **plus de 1 000 organisations victimes** du malware. The Mask brasse large mais ne s'intéresse visiblement pas aux données personnelles ou financières des particuliers, ni même à la capacité de calcul de leurs machines.

Voler un maximum d'informations

Les objectifs du malware ? **Voler un maximum d'informations** y compris à travers les communications chiffrées puisque diverses clés de cryptage, configurations VPN, clés SSH (permettant d'identifier un utilisateur sur un serveur SSH) et fichiers RDP (utilisés par le logiciel Remote Desktop Client pour ouvrir automatiquement une connexion avec un ordinateur réservé) figurent également dans le viseur de The Mask / Careto.

S'il s'installe comme une classique backdoor (bien qu'accompagné d'un certificat numérique jugé valide par le système ce qui minimise la menace), **le mode d'infection est des plus banals**. Les attaquants agissent par **campagne de phishing** à travers des e-mails ciblés contenant des liens vers des pages infectieuses. Du classique à la différence que les adresses des liens infectieux sont noyées dans des sous-domaines trompeurs pour un œil distrait (internacional.elpais.linkconf.net, www.washingtonsblog.linkconf.net, world.time.linkconf.net, etc.) et que l'utilisateur n'a pas le temps d'afficher la page infectieuse qu'il est aussitôt redirigé vers le lien original, tel que présenté dans le

courriel (une vidéo YouTube par exemple). Autrement dit, une fois encore, si le mode opératoire est bien pensé, la faille est avant tout humaine. Il reste néanmoins étonnant qu'administrations et grandes entreprises tombent encore dans le panneau.

Furtif et discret

Cerise sur le gâteau, The Mask sait se montrer furtif et discret en effaçant les traces de son passage dans les fichiers journaux au lieu de les supprimer. Du grand art. Une telle sophistication incite à soupçonner **une nouvelle manœuvre de la NSA** (National Security Agency), mais la langue espagnole employée tendrait à dédouaner, pour une fois, l'agence américaine. Néanmoins, il reste aujourd'hui impossible de savoir avec certitude qui est derrière The Mask.

Dans tous les cas, les auteurs du malware ont réalisé avoir été découverts. Selon Kaspersky, **tous les liens avec les serveurs de contrôle et commande ont été coupés** en janvier. Si The Mask est toujours en place sur les machines, que l'éditeur se propose de désinfecter avec ses solutions antivirales, l'agent espion ne serait donc plus en mesure d'envoyer les données collectées à ses auteurs ou commanditaires.

***** *Pas moins de 31 pays ont cependant été visés : Algérie, Argentine, Belgique, Bolivie, Brésil, Chine, Colombie, Costa Rica, Cuba, Egypte, France, Allemagne, Gibraltar, Guatemala, Iran, Iraq, Libye, Malaisie, Mexique, Maroc, Norvège, Pakistan, Pologne, Afrique du Sud, Espagne, Suisse, Tunisie, Turquie, Royaume-Uni, Etats-Unis et Venezuela.*