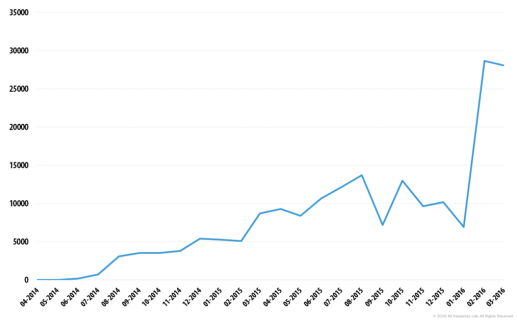
Evolution des Ransomwares pour appareils mobiles en 2014-2016

Evolution des Ransomwares pour appareils mobiles en 2014-2016

L'activité des ransomwares pour appareils mobiles, qui ne bénéficie pas de la même couverture médiatique que les ransomwares pour PC, a également explosé au cours de la période couverte par le rapport. Et plus particulièrement au cours de la deuxième moitié de celle-ci.



Nombre d'utilisateurs confrontés à des ransomwares pour appareils mobiles au moins une fois au cours de la période comprise entre avril 2014 et mars 2016

D'avril 2014 à mars 2015, les solutions de Kaspersky Lab pour Android ont protégé 35 413 utilisateurs contre des ransomwares pour appareils mobiles. Un an plus tard, ce nombre avait presque quadruplé et atteignait 136 532 utilisateurs. La part des utilisateurs attaqués par des ransomware par rapport aux utilisateurs attaqués par n'importe quel autre type de malware a également augmenté : de 2,04 % pour la période 2014-2015, elle est passée à 4,63 % pour la période 2015-2016. La courbe de croissance est peut-être plus modeste que celle observée pour les ransomwares pour PC, mais son ampleur suffit à confirmer une tendance inquiétante.

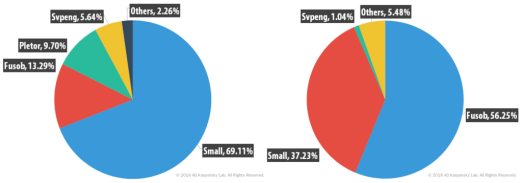
Principaux acteurs dans le milieu des ransomwares pour appareils mobiles

Sur l'ensemble de la période couverte par le rapport, les chercheurs de Kaspersky Lab ont été en mesure d'identifier les quelques familles de ransomwares pour appareils mobiles auxquelles les utilisateurs de nos produits étaient les plus souvent confrontés. En 2014-2015, il s'agissait de : Pletor, Fusob, Svpeng et Small. En 2015-2016, l'activité de Svpeng a enregistré une dégringolade et n'a concerné qu'une part modeste des utilisateurs attaqués.

A un moment donné en 2014-2015, Svpeng, connu à l'origine comme un malware bancaire, a été modifié par ses créateurs afin de pouvoir verrouiller un appareil infecté. Depuis lors, nous avons suivi les deux versions de Svpeng : le malware bancaire et le ransomware. La version ransomware est devenue populaire en 2014-2015 lorsqu'elle a touché 5,64 % des utilisateurs attaqués par un malware quelconque.

La situation a toutefois changé au cours de la deuxième période lorsque le ransomware a chuté vers le bas du Top 30 des menaces. Toutefois, la version malware bancaire de Svpeng a repris du service, ce qui signifie probablement que les créateurs du malware ont simplement perdu leur intérêt dans le développement d'un ransomware et ont décidé de se concentrer sur le malware bancaire.

Pletor, le malware considéré comme le premier exemple de ransomware et prétendument créé par les auteurs du tristement célèbre trojan bancaire Acecard, a connu une situation similaire. Au cours de la période 2014-2015, il a touché une part considérable des utilisateurs mobiles attaqués par des ransomwares mais en 2015-2016, il ne figurait plus dans le haut du classement et laissait le « marché » à seulement trois grandes familles de ransomwares.



Répartition de la part d'utilisateurs attaqués entre les familles de ransomwares pour appareils mobiles les plus actives en 2014-2015 (gauche) comparée à celle de 2015-2016 (droite).

Parmi les autres phénomènes importants observés au cours des 24 mois couverts par le rapport, on ne peut ignorer la concurrence entre deux grandes familles de ransomwares : Small et Fusob. En 2014-2015, c'est la famille Small qui dominait, du moins en termes de parts d'utilisateurs attaqués. Elle était signalée par 69,11 % de l'ensemble des utilisateurs qui avaient été confrontés au moins une fois à des ransomwares pour appareils mobiles. Mais un an plus tard, c'est la famille Fusob qui prenait la tête avec 56,25 % des utilisateurs. Toutefois, la famille Small se maintenait en 2e position avec 37,23 % des utilisateurs attaqués. Il est probable que les malwares Svpeng, Pletor, Small et Fusob seront vendus par leurs auteurs à d'autres cybercriminels ou qu'ils seront propagés via des réseaux d'affiliés. Les quatre familles ont subi de nombreuses modifications. Cependant, Small et Fusob semblent avoir été les plus modifiés, comme on peut le voir clairement dans les statistiques.

A la différence du phénomène des ransomwares pour PC qui est déjà largement couvert par les chercheurs de différentes sociétés, dont Kaspersky Lab, les ransomwares pour appareils mobiles n'ont pas encore fait l'objet d'une analyse en profondeur. Afin de remédier à cette situation, nous proposons une brève description des ransomwares les plus répandus et les plus dangereux à compter d'avril 2016

Pour en savoir plus sur l'évolution de la menace des ransomwares, lisez le rapport complet accessible via.

Article original de Kaspersky Lab

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Rapport KSN : ransomwares pour appareils mobiles en 2014-2016 – Securelist