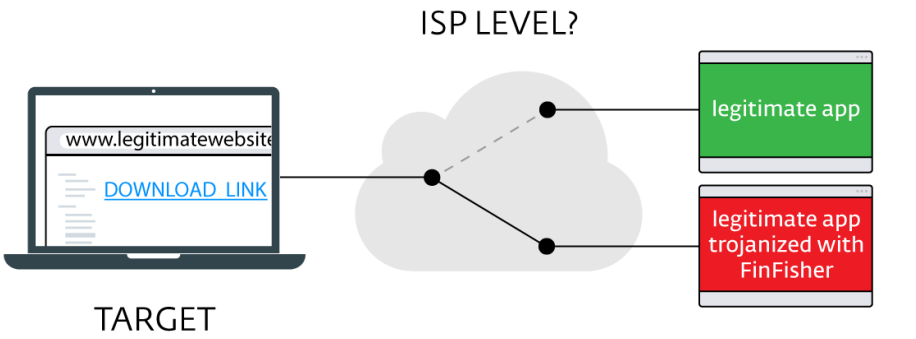
Campagne d’espionnage de grande envergure sur Internet



Campagne d’espionnage de grande envergure sur Internet

Les chercheurs ESET® ont détecté des campagnes d'espionnage liées à FinFisher, le célèbre spyware également connu sous le nom de FinSpy. Sept pays sont infectés.

FinFisher est un spyware (logiciel espion) **commercialisé en tant qu'outil de surveillance et d'intrusion informatique.**Il est **vendu à une vingtaine d'organismes gouvernementaux** à travers le monde. ESET pense qu'il a également été utilisé par des régimes autoritaires.

Les capacités d'espionnage de FinFisher s'étendent à :

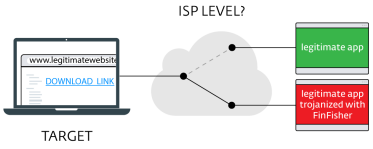
• la surveillance via les webcams et les microphones (images retransmises en direct)

• l'enregistrement de frappe (keylogger)

• l'exfiltration des fichiers

Ce logiciel espion a reçu un certain nombre de modifications via des correctifs dans sa dernière version. Elles améliorent ses fonctions pour se montrer plus intrusif. FinFisher peut ainsi rester sous le radar de détection des solutions de sécurité et empêcher une analyse approfondie de son comportement. L'innovation la plus importante reste la méthode pour pénétrer les machines ciblées.

Lorsqu'un utilisateur ciblé est sur le point de **télécharger une application populaire telle que WhatsApp®, Skype® ou VLC Player®,** il est **automatiquement redirigé vers le serveur de l'attaquant. La victime installe alors une version qui inclut un malware de type Trojan et se trouve ainsi directement infectée par FinFisher.**



Mécanisme d'infection de la dernière variante de FinFisher

« Sur deux des sept campagnes menées, les logiciels espions se sont propagés au moyen d'une attaque man-in-the-middle. Autrement dit, les communications sont interceptées à l'insu des parties concernées. Nous pensons que **les principaux fournisseurs d'accès à Internet de ces deux pays ont joué un rôle crucial dans cette infection** », explique Filip Kafka, Malware Analyst chez ESET et à l'origine de cette recherche. Ces campagnes sont les premières à révéler publiquement la probable implication (volontaire ou pas) d'un fournisseur d'accès à Internet dans la diffusion de malwares. « Les campagnes FinFisher sont des projets de surveillance perfectionnés et tenus secrets. Les méthodes utilisées associées à la portée de ces attaques en font une menace sans précédent », poursuit Filip Kafka.

Par le passé, ESET a publié un certain nombre d'articles sur les campagnes FinFisher. Vous pouvez les consulter ici. Les experts ESET ont également rédigé un article détaillé sur cette nouvelle campagne. Pour plus de détails, notre cybersecurity leader Benoit Grunemwald peut répondre à vos questions.

Note pour les éditeurs:

FinFisher, le soi-disant malware du gouvernement et l'approche de l'industrie de la sécurité sont sous les feux de la rampe. Pour ESET, il n'existe pas de malware dans la mesure où ce programme a été acheté d'une part puis modifié et détourné d'autre part par des individus mal intentionnés.

Lire la réponse d'ESET à une lettre ouverte adressée à Bits of Freedom, un groupe de défense des droits numériques…[lire la suite]

Réagissez à cet article

Source : ESET