Chère relation de presse,

SophosLabs Uncut a publié un nouveau rapport sur Baldr, une famille de malware disponible sur les marchés obscurs depuis janvier 2019.

Le rapport entier **Baldr vs. The World** offre une compréhension complète et donne de plus amples informations à propos de l’arrivée et de la disparition du ‘deep web’.

Jusqu’à présent les informations à propos de Baldr étaient plutôt rares. C’était donc un défi pour Sophos de s’y atteler. SophosLabs est passé en infiltration pour suivre les activités du deep web de près. Dans son rapport circonstancié SophosLabs décortique le malware et révèle leur fonctionnement interne, leur comportement visiblement cybercriminel et les ‘erreurs’ du côté de la vente et de l’achat. Quelques constats :

* Les développeurs de Baldr l’ont élaboré pour les cybercriminels débutant sur le web invisible et ils ont visé en premier lieu les gamers de PC
* Baldr est allé plus loin et exerce maintenant une nette influence sur différentes solutions logicielles
* Bladr utilise (comme de nombreux types de malware) des fragments de code empruntés à d’autres familles de malware. Baldr peut être considéré comme le monstre Frankenstein qui est composé de bribes de codes venant d’un grand nombre d’autres familles de malware
* Baldr peut obtenir une large gamme d’informations de ses victimes. Non seulement les mots de passe, des données mises en cache, des fichiers de configuration et d’autres fichiers, des cookies et une panoplie d’applications, notamment :
* 22 différents navigateurs
* 14 différents portefeuilles de crypto-monnaie
* des applications client VPN
* des outils pour le transfert de fichiers
* des clients pour la messagerie et le chat instantanés
* des clients de jeux vidéo et des services de gaming, comme Steam, Epic et Sony
* des services adjacents au gaming tels que Twitch of Discord
* Les attaques s’étendent au-delà du gaming et les infections sont perçues mondialement. Selon SophosLabs les pays les plus impactés sont : l’Indonésie (21% des victimes), les Etats-Unis (10,52%), le Brésil (14,14%), la Russie (13,68%), l’Inde (8,77%) et l’Allemagne (5,43%)
* Le code serveur de Baldr comprenait des bugs grâce auxquels les pirates pouvaient installer des portes dérobées pour ensuite voler des données et des mots de passe des clients
* Certains clients avaient mal configuré leur code serveur, et ainsi les outils et données étaient exposés aux autres. SophosLabs a découvert plus de 150 fichiers journal contenant des données volées d’ordinateurs de victimes, qui avaient été envoyés ‘par accident’ au site web Total Virus.
* Les chercheurs estiment que le malware est probablement d’origine russe et que les données des victimes de Russie et des pays avoisinants sont sauvegardées dans un fichier spécial sur le serveur de commande des assaillants
* Baldr a disparu du commerce en juin après une dispute entre le concepteur et le distributeur. SophosLabs s’attend à ce que la famille réapparaisse à terme, probablement sous un autre nom

“Il est possible que Baldr ait fait feu de paille, connaissant un pic rapide, et soit devenue elle-même victime d’une querelle entre cyber-voleurs. Or il reste à savoir si Baldr reviendra après une menace de longue durée”, prétend Brian Schippers de Sophos aux Pays-Bas. “Sa seule existence est toutefois la preuve que même de petits morceaux de maliciel volés peuvent être assemblés pour créer un monstre de malware comme Frankenstein qui est capable de cambrioler de façon efficace, de s’emparer de tout et de prendre la clef des champs tout de suite après.”

Le rapport, ainsi qu’une explication des constats principaux, est accessible sur SophosLabs Uncut et Naked Security. Dorénavant un lien direct vers **Baldr vs. The World** est également accessible. Si, suite à la lecture de ce mail, vous êtes intéressé(e)(s) par une interview téléphonique avec les auteurs de ce rapport, faites-le-moi savoir. Nous le réglerons pour vous avec le plus grand plaisir.

Mes sincères salutations,

Sandra van Hauwaert

Jacob-Jan Esmeijer