Bulletin dôalerte : Le malware peer-to-peer GameOver Zeus

Systèmes affectés

- Microsoft Windows 95, 98, Me, 2000, XP, Vista, 7, et 8
- Microsoft Server 2003, Server 2008, Server 2008 R2, et Server 2012

Aperçu

GameOver Zeus (GOZ), une variante peer-to-peer (P2P) du malware voleur dôinformations dôidentification bancaires de la famille de Zeus, identifié en septembre 2011, [1] utilise une infrastructure réseau décentralisée dôordinateurs personnels et de servers web compromis pour exécuter le commandement et le contrôle.

Description

GOZ, qui est souvent propagé à travers les spams et des messages dôhameçonnage, est principalement utilisé par les cybercriminels pour récolter des informations bancaires, telles que les informations de connexion, de lôordinateur dôune victime. [2] Les systèmes infectés peuvent aussi être utilisés pour participer dans dôautres activités malicieuses, telles quôenvoyer des spams ou participer à des attaques par déni de service distribué (DDoS).

Des variantes antérieures du malware Zeus utilisaient une infrastructure botnet centralisée pour le commandement et le contrôle(C2). Les servers centralisés C2 sont régulièrement suivis et bloqués par la communauté de la sécurité. [1] GOZ, cependant, utilise un réseau P2P dôhôtes infectés pour communiquer et distribuer des données, et utilise le cryptage pour se cacher des détections. Ces pairs agissent comme un réseau de proxy massif qui est utilisé pour propager des mises à jour binaires, distribuer des fichiers de configuration et envoyer des données volées. [3] Nôayant pas un seul point de défaillance, la résilience dôune infrastructure P2P de GOZ rend les efforts de nettoyage plus difficiles. [1]

Impact

Un système infecté avec GOZ peut être employé pour envoyer des spams, participer à des attaques DDoS et collecter les données dôidentifications des utilisateurs pour les services en lignes, y compris les services bancaires.

Solution

Il est recommandé aux utilisateurs de prendre les mesures suivantes pour assainir les infections de GOZ :

- *Utiliser et maintenir un antivirus* ï un antivirus reconnait et protèges votre ordinateur contre la plupart des virus connus. Il est important de garder votre antivirus à jour.

- *Changer vos mots de passe* ï Vos mots de passe au départ peuvent avoir été compromis durant lôinfection, donc vous devriez les changer.
- *Garder votre système dôexploitation et vos applications à jour* ï Installer les correctifs pour éviter que des attaquants prennent avantage de problèmes ou de vulnérabilités connus. Plusieurs systèmes dôexploitation offrent des possibilités de mises à jour automatiques. Si cette option est disponible, vous devriez lôactiver.
- *Utiliser des outils anti-malware* ï Utiliser un programme légitime qui identifie et supprime les malwares peut aider à éliminer une infection. Les utilisateurs peuvent considérer lôemploi dôun outil de suppression (voir les exemples ci-dessous) qui vont aider à supprimer GOZ de votre système.

  F-Secure

  http://www.f-secure.com/en/web/home_global/online-scanner (Windows Vista, 7 et 8)

  http://www.f-secure.com/en/web/labs_global/removal-tools/-/carousel/view/142 (Windows XP)

  Heimdal

  http://goz.heimdalsecurity.com/ (Microsoft Windows XP, Vista, 7, 8 et 8.1)

  Microsoft

  http://www.microsoft.com/security/scanner/en-us/default.aspx (Windows 8.1, Windows 8, Windows 7, Windows Vista, et Windows XP)

  Sophos

  http://www.sophos.com/VirusRemoval (Windows XP (SP2) et versions supérieures)

  Symantec

  http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network (Windows XP, Windows Vista et Windows 7)

  Trend Micro

  http://www.trendmicro.com/threatdetector (Windows XP, Windows Vista, Windows 7, Windows 8/8.1, Windows Server 2003, Windows Server 2008, et Windows Server 2008 R2)

  Les produits cités plus haut sont des exemples et ne constituent pas une liste exhaustive.

- GOZ a été associé avec le malware CryptoLocker.

Références

- [1] Highly Resilient Peer-to-Peer Botnets Are Here: An Analysis of Gameover Zeus
- [2] Malware Targets Bank Accounts
- [3] The Lifecycle of Peer-to-Peer (Gameover) ZeuS

Révisions

- Publication Initiale - Juin 2, 2014