Enseignant
Choplin

UNIVERSITÉ de Picardie Jules Verne

Étudiants
Kamel Kendak
Marc Lecomte
Fabien Lebourgeois

Etude de l'attaque

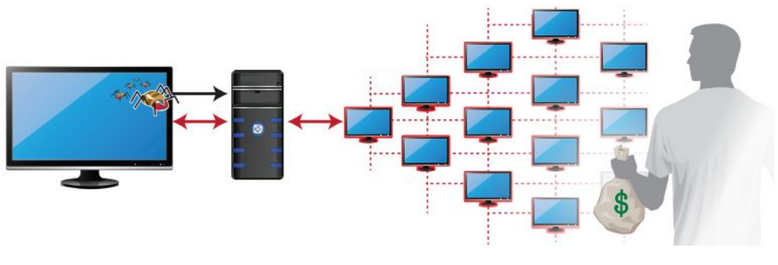
Nom du virus

Gameover Zeus

Quel est ce virus?

GameOver Zeus (« GOZ », que l'on appelle souvent simplement par « GameOver ») est un botnet (réseau de robots) en Peer to Peer (le client est le serveur) basé sur la composition d'un autre virus « ZeuS ». GOZ a été créé et utilisé notamment dans des spams piégés déployés par Cutwail, qui est lui aussi un botnet mais cette fois spécialisé dans le spam.

Comment fonctionne t-il?



GameOverZeus est un "botnet" (« réseau de robots ») principalement utilisé pour voler de grosses sommes d'argent par la fraude en reprenant des milliers de sessions bancaires de clients bancaires. Ces méthodes frauduleuses sont effectuées en temps réel. De plus, les cybercriminels concernés ont distribué les logiciels malveillants par e-mail afin de réaliser des hameçonnages bancaires (sites en phishing usurpant l'identité de la banque de la victime).GameOverZeus utiliserait des attaques sophistiquées pour collecter des informations confidentielles une fois les ordinateurs infectés. Un site bancaire ne demande normalement qu'un numéro d'identifiant et un mot de passe, mais le logiciel malveillant ici rajoutait des champs supplémentaires pour le numéro de sécurité sociale et les informations de carte de crédit, insérés de manière transparente dans la mise en page de la page. Une fois que les attaquants disposaient de suffisamment de données, ils frappaient avec un virement bancaire non autorisé.Ils ont également ciblés les départements RH via Monster et CareerBuilder dans le but de configurer de faux employés et d'accéder aux données de cuisson de cette façon. Une fois l'acte accompli, le virus a infecté l'ordinateur et attend que l'utilisateur accède à son site Web bancaire. Gameover identifie et intercepte ensuite leur session en ligne à l'aide d'une technique communément appelée man-in-the-browser (MITB). Le malware a également la capacité de contourner l'authentification à deux facteurs et peut afficher des messages de sécurité bancaire malveillants pour révéler des informations sécurisées afin d'autoriser les transactions et réclamer frauduleusement l'argent de leur victime.

Zeus ou GameOver Zeus ?

Comparé à ZeuS, GameOver Zeus (GOZ) disposait d'une capacité supplémentaire permettant d'initiniers plusieurs attaques par déni de service à partir de réseaux de zombies comme forme de subterfuge. Il est plus difficile de trouver le responsable d'une attaque quand, une fois la « cible » capturée, s'avère être un utilisateur qui a simplement parfois manqué d'un peu de prudence en ouvrant un mail suspect. Une seconde différence est que le malware GOV est passé par une architecture en « Peer to Peer » pour fonctionner, ce qui a rendu le travail des autorités bien plus compliqué (car le virus transitait d'un ordinateur à un autre, sans passer par un réseau. Les autorités ont alors eu de grandes difficultés à identifier les responsables du virus.

Quels ont été ses impacts financiers?

La plainte fédérale cite quatre attaques de ce type, allant de 190 000 $ volés dans un centre de vie assistée, jusqu'à 7 millions de dollars volés dans une banque régionale du nord de la Floride. Selon le ministère de la Justice, le total des dommages infligés par GameOver totalise plus de 100 millions de dollars.

En 2014, une collaboration multicentrique a été effectuée entre plusieurs services répressifs : on y trouvait notamment plusieurs chercheurs spécialisés en sécurité, ainsi que le Centre Européen contre la Cybercriminalité (appelé le « EC3 »). Ces collaborations ont été financés par les gouvernement (le coût de ces efforts est difficile à quantifier).

Le botnet a également collecté des fonds via Cryptolocker, une attaque qui crypterait le disque dur d'un ordinateur, exigeant une rançon pour déverrouiller les données. Pour ceux qui n'ont pas payé, les coûts de récupération des données ont atteint 80 000 $. Les chercheurs affirment que le botnet est opérationnel depuis octobre 2011, mais a utilisé un mécanisme P2P complexe pour couvrir ses traces, ce qui rend la traçabilité difficile jusqu'à présent. Un cryptage fort a également déguisé l'emplacement des serveurs maîtres. "Ces stratagèmes étaient très sophistiqués et extrêmement lucratifs", a déclaré le sous-procureur général américain Leslie Caldwell dans un communiqué à la presse. "Les cybercriminels ne les ont pas rendus faciles à atteindre ou à perturber."

Sources

Wikipédia - **Gameover ZeuS**	Lien
Clubic.com- **L'activité cybercriminelle liée au malware Gameover Zeus perturbée, mais pas stoppée**	Lien
Assiste.com - **Botnet Gameover ZeuS**	Lien

Quelles mesures ont été prises?

La police britannique a réussi à prendre le contrôle des ordinateurs infectés, pour éviter qu'ils n'en contaminent d'autres. Mais les autorités sont conscientes qu'elles ne pourront pas garder «en quarantaine» bien longtemps ces ordinateurs s'ils ne sont pas rapidement «soignés». Les internautes concernés ont été contactés par leur fournisseur d'accès et doivent lancer un logiciel permettant d'éliminer les virus de leur machine. Ils devront également à mettre à jour leur système d'exploitation, leur antivirus, ainsi que tous les logiciels de leur ordinateur.

Aurait-on pu anticiper et mieux réagir face à ce virus?

Puisque GameOver se cache dans des mails qui offrent des liens vers des sites de phishing. Les antivirus sont inopérants car ils ne peuvent pas scanner un site internet contenu dans un mail (contrairement à une pièce-joint) et déterminer s'il s'agit d'une arnaque ou pas. Même si les utilisateurs ont des droits qui restrictifs qui ont été définis par leur administrateur sur leurs propres ordinateurs, ces solutions deviennent incomplètes pour la raison citée précédemment.

Pour prévenir ce genre d'attaque, une prévention auprès des utilisateurs, notamment en les recommandant de vérifier l'adresse mail à l'origine d'un mail lié à la banque, peut-être un bon moyen de limiter un certain nombre d'escroquerie.

D'autre part, comme ce genre de virus est capable de se répandre très rapidement sur un réseau et que le risque 0 n'existe pas, un système de supervision capable d'agir en isolant le poste à risque de propagation lorsqu'un comportement suspect provenant de l'un des postes survient peut-être un bon moyen d'isoler le danger et de limiter les dégâts.

Le hacker responsable

Evgeniy Mikhailovich Bogachev

Qui est à l'origine de l'attaque?

Evgeniy Mikhailovich Bogachev, utilisant les surnoms en ligne «lucky12345» et «slavik», est recherché pour sa participation présumée à une entreprise et à un programme de racket de grande envergure qui ont installé, sans autorisation, des logiciels malveillants appelés «GameOver Zeus» sur les ordinateurs des victimes. Bogachev était connu pour la dernière fois comme résidant à Anapa, en Russie. Il est connu pour apprécier le canotage et peut voyager à des endroits le long de la mer Noire dans son bateau. Il possède également une propriété à Krasnodar, en Russie.Il a provoqué à multiples reprises les gouvernements à sa recherche, par des photos de lui sur internet le montrant vivant très confortablement.

Quelles sont/ont été ses principales motivations?

L'objectif final du groupe Gameover Zeus est de tirer profit des informations frauduleuses qu'ils reçoivent du botnet. L'équipage P2P Zeus tire principalement un profit du botnet grâce à d'importantes transactions ACH (Automated Clearing House) et à des virements électroniques. Pour que cet anneau malveillant fonctionne, le gang doit siphonner les fonds des comptes bancaires compromis et travailler avec d'autres cybercriminels pour effectuer les transferts. Tout comme les cartels de la drogue, ces complices sont connus sous le nom de mulets d'argent et sont souvent situés dans les mêmes zones que les victimes. Cela réduit le risque de détection et leur permet de terminer la transaction beaucoup plus facilement.

Bogachev et les autorités

Le gouvernement américain (FBI) propose une prime évaluée jusqu'à 3 millions de dollars pour quiconque pourrait fournir des informations concernant le pirate informatique Evgeniy Mikhailovich Bogachev, transmet un journal très réputé aux Etats-Unis. L'homme russe, à l'origine du virus et traqué par un certain nombre de pays autour du globe, vivait à Krasnodar, une ville située dans le sud de la Russie. Il n'hésite pas à s'afficher sur internet en provoquant les gouvernements : visiblement, il ne semble pas craindre d'être arrêté et ne cache en rien sa vie très luxueuse, confortablement installé en Russie. Des photos le montrent ainsi au volant d'une voiture de luxe ou encore en pyjama léopard, un de ses chats dans les bras...

En fait, selon les Fédéraux US, les autorités russes tolèreraient toutes les excentricités du hacker parce qu'il travaillerait désormais pour les services d'espionnage du pays. Il est probable que le Kremlin a fermé les yeux sur les précédents crimes de Bogachev afin de s'assurer ses services et d'utiliser ses «dons». «Le réseau mis en place par Bogachev avec son logiciel GameOverZeus est l'un des plus sophistiqués et nocifs que nous ayions connu», avoue au New York Times un responsable du FBI. Ces hackers russes sont au coeur des dernières tensions entre Washington et Moscou, dont les relations sont déjà au plus bas à cause de leur opposition sur le conflit syrien et la crise ukrainienne. Les Etats-Unis ont ainsi accusé le Kremlin de manipulation à grande échelle lors des élections américaines en se cachant derrière les attaques informatiques de deux groupes de hackers : Cozy Bear et Fancy Bear. Le premier s'est infiltré à partir de l'été 2015 dans les serveurs du comité démocrate national pour intercepter toutes les communications du parti tandis que le second a ciblé et volé des dossiers relatifs à Donald Trump.

Sources

fbi.gov - **EVGENIY MIKHAILOVICH BOGACHEV**	Lien
wired.com - **Inside the Hunter for Russia's Mot Notorious hacker**	Lien
lefigaro.fr - **Un très puissant réseau de cybercriminels démantelé**	Lien