AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Le Botnet GoldBrute

Contenu

I. Contexte

GoldBrute. C'est le nom donné par des chercheurs en sécurité à un botnet potentiellement dévastateur. Selon les analystes, plus d'1,5 millions de serveurs RDP (Remote Desktop Protocol) exposés sur Internet seraient actuellement la cible d'une vaste opération de cyberattaque. GoldBrute utiliserait l'attaque par force brute, en testant un à un les multiples mots de passe possibles. Il est conçu de manière à s'améliorer graduellement à mesure qu'il ajoute chaque système piraté à son réseau, les contraignant ainsi à trouver d'autres serveurs RDP disponibles, qu'il force à leur tour.

La découverte du botnet GoldBrute a également montré qu'actuellement, les attaques par force brute restent la principale menace pour les systèmes RDP exposés en ligne. Malgré toute la panique qui entoure la menace imminente de la vulnérabilité BlueKeep RDP, les chercheurs en matière de sécurité affirment que la plupart des attaques RDP sont aujourd'hui des attaques classiques de force brute. Selon les statistiques publiées aujourd'hui par les chercheurs en sécurité, les analyses RDP concernant la vulnérabilité BlueKeep ne représentent que 3,4% de tout le trafic malveillant RDP observé la semaine dernière.

D'autre part, les attaques par force brute de RDP et les tentatives d'exploitation de vulnérabilités plus anciennes représentent 96,6% des attaques. Cela montre que la décision de nombreuses entreprises de sécurité et des chercheurs en sécurité de s'abstenir de publier l'exploit BlueKeep a été une bonne décision.

La taille du réseau botnet GoldBrute n'est pas encore clairement définie. Ce que l'on sait, c'est que la liste de cibles figurant dans le botnet a grossi au cours des derniers jours, car elle a progressivement trouvé de nouveaux points de terminaison RDP contre lesquels lancer des attaques. Cette croissance de la liste principale des cibles RDP de GoldBrute suggère également une augmentation de sa base de périphériques infectés. La mauvaise nouvelle pour les entreprises et les utilisateurs exécutant des points de terminaison RDP exposés sur Internet est que le botnet est également difficile à détecter et à arrêter. En effet, chaque système infecté par GoldBrute ne lance qu'une seule tentative de recherche de mot de passe par victime, contournant ainsi les systèmes de sécurité offrant une protection en force brute.

II. Fonctionnement

Un système infecté sera d'abord invité à télécharger le code du bot », explique des chercheurs en sécurité, le téléchargement est très volumineux (80 MBytes), il comprend le code Java GoldBrute et l'intégralité du Java Runtime. Initialement, le bot commencera à scanner des adresses IP aléatoires pour trouver d'autres hôtes avec des serveurs RDP exposés. Ces adresses IP sont transmises au serveur C&C. Après que le bot ait signalé 80 nouvelles victimes, le serveur C&C lui assigne un ensemble de cibles pour des attaques par force brute. Au final, l'attaquant ou le groupe derrière GoldBrute aura accès à toutes les combinaisons valides.

Pour passer sous le radar des outils de sécurité et des analystes de logiciels malveillants, les attaquants derrière cette campagne commandent à chaque machine infectée de cibler des

millions de serveurs avec une seule combinaison unique de nom d'utilisateur et de mot de passe afin qu'un serveur cible reçoive des tentatives de force brute provenant de différentes adresses IP. Une méthode qui rend malheureusement difficilement détectable le botnet.

En résumé GoldBrute fonctionne ainsi :

- Le botnet tente une attaque de force brute afin d'accéder à un système Windows via RDP.
- Télécharge un fichier ZIP avec le code du programme malveillant GoldBrute.
- Analyse des nouveaux points de terminaison RDP visibles sur Internet et qui ne font pas partie de la liste principale de points de terminaison RDP de GoldBrute.
- Après avoir trouvé 80 nouveaux points de terminaison RDP, il envoie la liste des adresses IP à son serveur de commande et de contrôle.
- L'hôte infecté reçoit une liste d'adresses IP à attaquer par force brute. Pour chaque adresse IP, le bot tente de s'authentifier avec un seul nom d'utilisateur et mot de passe. Chaque bot GoldBrute reçoit un nom d'utilisateur et un mot de passe différents.
- Le bot effectue une attaque par force brute et transmet les résultats au serveur de commande

À l'heure actuelle, on ne sait pas exactement combien de serveurs RDP ont déjà été compromis et participent aux attaques en force brute contre d'autres serveurs RDP sur Internet. Une rapide recherche sur l'outil Shodan indique néanmoins qu'environ 2,4 millions de serveurs Windows RDP sont accessibles sur Internet, et donc potentiellement en danger. Ironiquement, cet incident intervient très peu de temps après que Windows ait corrigé la faille BlueKeep, qui concernait également les serveurs RDP.

III. Comment se protéger ?

Limiter la possibilité de tentative par brute force:

- En désactivant l'accès au service RDP exposés sur internet sur les machines où l'accès bureau à distance n'est pas nécessaire
- En définissant les comptes utilisateur autorisé à être utilisé via le service RDP
- En définissant les clients RDP (adresses IP) autorisés à effectuer des connexions sur ces services.

Définir et appliquer une politique de gestion de mot de passe :

- qui exige un mot de passe d'une complexité élevé pour les services exposés sur internet
- qui exige une durée de validité de mot de passe réduit pour les services exposés sur internet

Garder à jour les systèmes et appliquer les patches de sécurité publiés par les éditeurs des solutions et services exposés sur Internet.