
L'Expertise Sécurité

# Passé l'injection, Ajax entre en action

Par Philippe Humeau

# Contexte

- Les utilisateurs sont désormais "éduqués" et le Web est à la fois devenu un outil de travail, une source d'information, et il présente un intérêt à titre privé. Ces utilisateurs, souvent peut avertis, ont vu leurs vies transformées par l'utilisation croissante du Web.

- L'émergence de techniques de pointes pour attaquer ces nouveaux consommateurs, ou les entreprises dans lesquelles ils travaillent, par l'intermédiaire du Web devient un axe majeur pour les pirates.

- Si le Web "2.0" Javascript et Ajax sont des mystères pour eux, les entreprises et leurs dirigeants informatiques doivent eux maitriser ces nouveaux vecteurs de compromission tout à fait réels et efficaces.

- Les attaques connaissent de nouvelles contraintes tout en ouvrant de nouvelles possibilités.

# Limites et avantages

- La première limite et non des moindres, l'attaque ne durera que tant que le navigateur de l'utilisateur est ouvert. A sa fermeture, la possibilité d'exploiter celui-ci devient caduque.

- L'avantage connexe est qu'une fois le navigateur clos, il n'existe plus de réelles traces de compromissions sur la machine de l'utilisateur.

- Les navigateurs embarquent tous une limite d'exécution du code Javascript nommée « Same Origin Check » qui limite l'interaction du code Javascript à des objets provenant d'un même domaine.

- Le vecteur d'ingénierie sociale peut permettre de ne pas compromettre un site tiers pour arriver à ses fins. En hébergeant son propre code malicieux et en invitant l'utilisateur à se connecter à ces pages piégées par l'entremise d'une ingénierie sociale, il devient possible de se passer de la recherche d'une faille XS/CSRF/SQL Injection sur un site qu'il fréquente.

# Buts d'un « pirate 2.0 »

Comme à l'accoutumé, il existe deux buts distincts, servis par des méthodes différentes. Les acteurs de ces attaques sont souvent des personnes ou des groupes différents qui n'opèrent que dans l'un des deux milieux.

- L'attaque de masse, dont le succès est directement lié à la quantité de navigateurs compromis, qui permet d'obtenir des navigateurs zombies pour obtenir un mouvement massif, une attaque à grande échelle.

- L'attaque ciblée, qui vise une entité en particulier, afin d'obtenir une information importante ou faire un premier pas dans la compromission plus complète du SI visé.

# L'attaque de masse

- Un grand nombre de navigateurs compromis pour :
  - détourner des payements en lignes ou l'obtenir de coordonnées bancaires qualifiées puis les revendre (voir slide suivant)
  - attaquer massivement par D.D.O.S un service en ligne
  - agir en lieu et place des utilisateurs dans le but d'être anonyme (vendre des actions en son nom par exemple)
  - obtenir des informations personnelles sensibles (lire les mails, obtenir des coordonnées bancaires)
  - Fishing d'utilisateurs (en ouvrant une popup sans le contexte du browser et en remaquillant celui-ci)
- La condition sinéquanone est de compromettre un site à très large audience par l'entremise d'une faille XSS ou d'une injection SQL.

# Pour quel gains ?

| Elément | Prix (en dollars américains) |
|---|---|
| Carte de crédit américain avec vérification | $1-$6 |
| Carte de crédit britannique avec vérification | $2-$12 |
| **Identité : RIB, carte de crédit, date de naissance, numéro de sécurité sociale** | **$14-$18** |
| Liste de 29 000 adresses mail | $5 |
| Compte bancaire en ligne avec un solde de $9 900 | $300 |
| Yahoo Mail Cookie | $3 |
| Ordinateur accessible | $6-$20 |
| Phishing par site web | $3-$5 |
| Compte Pay Pal vérifié | $50-$500 |
| Compte Pay Pal non vérifié | $10-$50 |
| Compte Skype | $12 |
| Compte World of Warcraft – un mois | $10 |

**Le prix de l'identité volée**
www.bulletins-electroniques.com/actualites/41965.htm
Crédits : MS&T Source : Données Symantec Corporation

Les attaques par D.D.O.S quand à elles sont très simples à mener une fois un grand nombre de navigateurs compromis puisqu'il suffit de tous leur faire effectuer une requête Ajax vers le service à bloquer, généralement pour appuyer un chantage électronique.

# L'attaque de masse

Ajax est donc un bras de levier d'une efficacité remarquable dans le cadre des attaques de masse :

- Anonyme
- Distribué
- Plus simple à programmer qu'un vers ou qu'un cheval de Troie
- Il dispose des identifications du possesseur du navigateur
- Travail sur la couche applicative et peut être obfusqué par l'utilisation de HTTPS

A ce titre, par exemple, si l'utilisateur est authentifié sur son portail de banque en ligne ou de trading et que celui-ci a été compromis par un pirate, une requête Ajax peut lui faire vendre ses actions.

Mener la même action simultanément sur tous les comptes utilisateurs pour obtenir une baisse sensible de la dite action lui permet de positionner de l'argent sur un mouvement contraire.

# L'attaque ciblée

Elle est souvent le fait d'une personne mal intentionnée, douée techniquement, qui connaît bien sa cible. Elle peut aussi être le fait d'un groupe de Blackhats de haut niveau, payé par la concurrence.

- Obtenir une première compromission du SI ciblé pour :
  - Scanner le réseau local ou la DMZ à la recherche de services
  - Ré écrire à la volée d'autres pages du site compromis (Same Origin Check)
  - Consulter l'historique d'un utilisateur (en utilisant des feuilles de style)
  - Sniffer les frappes clavier de l'utilisateur compromis (et potentiellement découvrir un mot de passe qui sera utilisé aussi ailleurs dans le SI)
  - Bruteforcer des accréditations vers d'autres service Web
  - Piloter à distance des périphériques disposants d'une interface Web
  - Nuire à l'image de la société en compromettant les navigateurs des clients surfant sur son site institutionnel
- Méthode : compromettre un utilisateur par une ingénierie sociale et l'amener sur un site piégé ou compromettre un site de l'entreprise.

# L'attaque ciblée

Il serait long de détailler tous ces exemples mais voici certaines applications simples d'une partie d'entres-eux :

- Scanner le réseau local ou la DMZ

  permet de construire la suite de l'attaque en ayant une meilleure connaissance du SI ciblé. Cela s'effectue avec de simples requêtes Ajax.

- Bruteforcer des accréditations vers d'autres service Web

  En utilisant tout simplement *xmlhttpRequest.open("GET", "url", true, "username", "password")*

- Piloter à distance des périphériques disposants d'une interface Web

  En forgeant des requêtes particulières dont le but peut être de reconfigurer un routeur ou une borne wifi ou encore de couper des caméras de surveillance pour faciliter un cambriolage ultérieur. (voir slide suivant)

# L'attaque ciblée

- Exposer la machine en ip 192.168.1.42 directement en DMZ sur une borne Wifi Linksys :

  *xmlhttprequest.open("GET", "http://admin:password@192.168.1.1/security.cgi?dod=dod&dmz_enable=dmz_enable&dmzip1=192&dmzip2=168&dmzip3=1&dmzip4=42&wan_mtu=1500&apply=Apply&wan_way=1500", true, "", "")*

- Désactiver une caméra de surveillance Axis, à distance :

  *xmlhttprequest.open("POST", "http://192.168.1.1/admin/netw_tcp.shtml",true);*
  *xmlhttprequest.send("conf_Network_IPAddress=240.123.123.123&conf_Network_SubnetMask=255.255.255.0&conf_Network_Media=auto&.....");*

- ou encore faire imprimer des pages de tests en boucle à toutes les imprimantes
- compromettre des serveurs Web en lançant des overflow sur les parsers
- poster des mails de spams
- etc, le jardin de ce qui peut être fait par requêtes Web ne demande qu'à être exploré avec créativité.

# Pour quel gains ?

Les gains et buts sont fonctions du profile de l'assaillant :

Quelques exemples pour une personne mal intentionnée :

- Prendre une revanche sur son ex société en :
  - dégradant son image
  - diffusant des informations confidentielles
  - se rendre indispensable ou exercer un chantage en mettant le SI en panne

Et pour un groupe de pirates missionné par la concurrence :

- Être payé une forte somme pour :
  - dégrader une image de marque
  - effectuer de l'espionnage industriel ou commercial
  - mettre en panne un SI
  - détourner des accréditations sensibles (VIP / Direction)

# Vos interlocuteurs

L'Expertise Sécurité

**140, boulevard Haussmann**
**75 008 Paris**

Philippe Humeau
Directeur Commercial
Tel : 01.58.56.60.86, Fax : 01.58.56.60.81
Mail : philippe.humeau@nbs-system.com

Retrouvez nous sur le Web à l'adresse suivante : http://www.nbs-system.com