Le HTTP, vecteur privilÃ©giÃ© d'attaques et de compromission de donnÃ©es
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 4/7/2012 11:30:00

Si l'on parle souvent de "nouvelles technologies de l'information et de la communication" pour Ã©voquer Internet, on oublie souvent que le Web, principal protocole de communication du rÃ©seau, repose sur des technologies vieilles de plus de vingt ans qui n'ont que trÃ¨s peu Ã©voluÃ©esâ¦

ConÃ§u en 1989 et mis en pratique un an plus tard par Tim Berners-Lee du CERN, le protocole HTTP vÃ©hicule aujourd'hui le contenu du "Web" sur des spÃ©cifications dont la derniÃ¨re version date de 1999 soit il y a plus de 23 ans.

DÃ©sormais omniprÃ©sent et utilisÃ© Ã diverses fins (applications communautaires et mÃ©tier, sites vitrines et transactionnels, Intranet/Extranet, etc.), ce protocole est devenu de plus en plus dynamique, s'adaptant ainsi aux besoins des utilisateurs du Web.

Or cette course Ã la sophistication n'a pas Ã©tÃ© suivie d'une Ã©volution Ã©quivalente en termes de sÃ©curitÃ© et de fiabilitÃ© des donnÃ©es vÃ©hiculÃ©es. Ce dÃ©calage entre utilisation massive et sÃ©curitÃ© provoque aujourd'hui une brÃ¨che importante dans les systÃ¨mes d'information, faisant du protocole HTTP un vecteur privilÃ©giÃ© d'attaques et de compromission de donnÃ©es.

Les cybercriminels l'ont bien compris et en font une cible principaleâ¦ Il ne se passe pas une semaine sans qu'une sociÃ©tÃ© ou organisation se fasse compromettre via le protocole HTTP (Sony, RSA, Oracle, etc.) affirme **Matthieu Estrade**, Directeur Technique de Bee Ware, qui dÃ©crit l'importance du protocole HTTP et du Web dans les " Advanced Persistent Threats "

IdentifiÃ©es par le terme APT pour Advanced Persistent Threat, ces attaques sont orchestrÃ©es dans la durÃ©e avec un but prÃ©cis : rÃ©cupÃ©rer des donnÃ©es sensibles.

Anatomie d'une APT

De plus en plus mÃ©diatisÃ©es et nocives pour l'image des sociÃ©tÃ©s, les APT se dÃ©composent en 4 Ã©tapes principales :

â¢ l'intrusion

â¢ le maintien dans le systÃ¨me d'information

â¢ le rebond et la progressions en profondeur

â¢ l'extraction de donnÃ©es.

L'intrusion est opÃ©rÃ©e en attaquant une zone exposÃ©e au public sur Internet (Site Web, Blog, etc.). Cette porte d'entrÃ©e permet le plus souvent de poser un premier pied dans l'infrastructure et offre ainsi un point de dÃ©part permettant de rÃ©colter des informations importantes pour la suite (mots de passe utilisateurs, destinations rÃ©seau et machine, connecteurs vers d'autres systÃ¨mes, etc.).

De plus, selon la localisation de l'application dans l'infrastructure et le manque de cloisonnement, il est possible qu'une application simple et peu utilisÃ©e se retrouve Ã cotÃ© ou sur le mÃªme serveur qu'une application mÃ©tier, qui deviendra alors accessible via ce rebond, et avec des droits plus Ã©levÃ©s.

J'y suis... j'y reste...

Une fois le premier pied posÃ© dans l'infrastructure, il est nÃ©cessaire d'assurer le fait de pouvoir revenir sur la machine et de l'utiliser sans Ã©veiller les soupÃ§ons des administrateurs systÃ¨mes.

Pour rester le plus furtif possible, l'idÃ©al est d'insÃ©rer une backdoor dans l'application Web ou sur le service applicatif, en vue d'utiliser les connexions HTTP comme une connexion directe et/ou un tunnel vers les autres applications (sans Ãªtre filtrÃ© et sans attirer l'attention sur un processus ouvrant un port inconnu sur le systÃ¨me).

Les Ã©tapes d'intrusion et de maintien sont ensuite rÃ©pÃ©tÃ©es autant de fois que nÃ©cessaire jusqu'Ã atteindre les donnÃ©es sensibles.

Le protocole HTTP prend une place importante dans cette Ã©volution au sein du systÃ¨me d'information car ce dernier est souvent laissÃ© ouvert pour permettre aux administrateurs de naviguer ou de mettre Ã jours les machines (dialogue entre serveurs applicatifs, Web Services, interface d'administration, etc.).

Une fois la cible atteinte, le protocole HTTP, dont les restrictions en sortie sont gÃ©nÃ©ralement faibles, reste Ã nouveau le moyen le plus discret pour faire sortir les donnÃ©es sensibles.

Comment se protÃ©ger ?

Dans l'idÃ©al, la sÃ©curitÃ© doit Ãªtre abordÃ©e dÃ¨s la conception de l'application ou de l'infrastructure applicative. La norme PCI DSS recommande par exemple d'associer Ã chaque zone de l'infrastructure applicative des politiques de sÃ©curitÃ©s adaptÃ©es Ã leur contenu, que ce

soit sur le flux entrant ou sortant (compliquant ainsi les diffÃ©rents rebonds nÃ©cessaires pour atteindre les donnÃ©es sensibles).

La sÃ©curitÃ© rÃ©seau reste assez conventionnelle et s'appuie sur du filtrage de destinations, sources, IP et Ports pour la majoritÃ© des cas. Cependant, les firewalls rÃ©seaux classiques ne filtrent pas les protocoles applicatifs et restent clairement insuffisants dans le cadre des APT.

La sÃ©curitÃ© applicative est plus complexe car elle touche des applications souvent uniques, conÃ§ues sur mesure ou dÃ©ployÃ©es avec plusieurs spÃ©cificitÃ©s liÃ©es Ã l'infrastructure. Chaque zone contenant des applications Web doit donc Ãªtre filtrÃ©e autant en entrÃ©e qu'en sortie, sur le contenu et l'utilisation du protocole HTTP lui-mÃªme. Ce type de dÃ©ploiement est souvent appelÃ© "dÃ©fense en profondeur" et permet de contrÃ´ler les diffÃ©rentes attaques tant au niveau rÃ©seau qu'au niveau applicatif.

Pour rÃ©pondre Ã ce besoin, la mise en place d'un Web Application Firewall (ou WAF), considÃ©rÃ© comme une extension applicative d'un firewall rÃ©seau, est fortement conseillÃ© par le point 6.6 de la norme PCI DSS.

Un WAF analysera le protocole HTTP ainsi que le contenu qu'il vÃ©hicule, et permettra d'alerter en cas de menace pour une rÃ©action rapide (blocage de l'IP de l'attaquant via un protocole de dialogue avec les firewalls rÃ©seaux, etc.). FrÃ©quemment utilisÃ© en mode reverse-proxy, un WAF permet notamment d'effectuer une rupture protocolaire et de structurer plus facilement les zones entre applications.

Le document WAFEC (Web Application Firewall Evaluation Criteria) du WASC permet de comprendre et d'Ã©valuer les diffÃ©rents vendeurs en fonction des besoins sÃ©curitaires.

Un Web Services Firewall (extension du WAF) sera enfin un moyen efficace de sÃ©curiser les protocoles vÃ©hiculant du contenu XML sur HTTP (comme par exemple les protocoles SOAP ou REST).

Les Web Services, vulnÃ©rables aux mÃªmes attaques que les applications Web, nÃ©cessitent le mÃªme type de protection mais leur situation dans l'infrastructure applicative est en revanche beaucoup plus critique (car souvent au cÅ□ur de l'information sensible et ils sont souvent reliÃ©s aux infrastructures des partenaires).

Un Web Service Firewall assurera ainsi une sÃ©curitÃ© sur le format des messages et leur contenu, mais Ã©galement sur l'utilisation mÃªme du service.

Comprendre pour prÃ©venirâ□¦

Comprendre un comportement anormal sur une application permet de localiser une attaque, cependant, une infrastructure applicative peut comporter des centaines d'applications. Pour comprendre l'attaque dans sa globalitÃ© et en suivre l'Ã©volution (DÃ©couverte, agression, compromission), il est nÃ©cessaire d'avoir une vue d'ensemble.

Pour cela, il est impÃ©ratif de mettre en place une corrÃ©lation de logs pour avoir en temps rÃ©el cette analyse globale et comprendre le type de menace.

Le dialogue entre les Ã©quipes applicatives, sÃ©curitÃ© et rÃ©seaux est souvent complexe au sein d'une organisation. La formalisation, sous forme de rapports, des attaques et de l'utilisation de l'application permet d'avoir une base de travail et une comprÃ©hension de la menace applicative pour ces diffÃ©rentes Ã©quipes.

Les processus d'alerting permettront quant Ã eux de rÃ©agir et de dÃ©clencher des

procÃ©dures, que ce soit au niveau rÃ©seau avec le blocage de l'IP de l'attaquant, ou au niveau applicatif avec l'interdiction d'accÃ¨s Ã certaines ressources/zones ou plus directement le renvoi vers un honeypot pour analyser le comportement de l'attaquant.

Pour chaque zone compromise, il est important de comprendre quels sont les Ã©lÃ©ments compromis, et de retracer l'attaque sur la base de l'intrusion, la compromission avec installation de backdoor, le rebond vers d'autres zones et/ou l'extraction de donnÃ©es. L'aspect "forensics" est donc essentiel.

Les moyens mis en Å□uvre pour rÃ©aliser une APT sont souvent consÃ©quents et gÃ©nÃ©ralement proportionnels Ã la criticitÃ© des donnÃ©es ciblÃ©es. Les APT ne sont donc pas de simples attaques temporaires, mais de vraies menaces permanentes et latentes qu'il faut combattre sur le long terme.

MÃªme si la rÃ©alitÃ© du terrain met en Ã©vidence des difficultÃ©s Ã appliquer toutes les bonnes pratiques, une Ã©tude approfondie des menaces, une rÃ©ponse appropriÃ©e ainsi que l'anticipation des incidents possibles et l'Ã©tude de forensics sont aujourd'hui la meilleure rÃ©ponse face Ã ces attaques applicatives.