Wordpress, un backdoor amb funcionalitats de blog

Pau Muñoz

`Coordinador, defcon group 170`

Topic: threat intel and detection

Tema

Realitzarem una introducció a la seguretat informàtica amb especial atenció a les aplicacions web, concretament WORDPRESS.

PRE REQS

- PHP
- WORDPRESS
- basic sistemes i xarxes

Ciberatacs en l'actualitat

A tan solo unos días de finalizar el año, llega la hora de echar la vista la atrás y analizar lo que ha ocurrido en estos doce meses pero también de ver qué nos espera para el año próximo. Eso es lo que han querido hacer los expertos de Check Point quienes han decidido repasar las **principales ciberamenazas del año y ver qué nos deparará un 2018 que se prevee más peligroso.**

Figure: atacs

Fases d'un ciberatac

- Obtenció d'informació
- Estudi de vulnerabilitats
- Explotació
- Assoliment d'objectius
- Neteja de proves

Recopilació d'informació

L'obtenció d'informació sobre l'objectiu és fonamental per garantir l'èxit de l'atac. + informació = + éxit.
Info sobre el domini, sobre el servidor, software, personal de l'empresa, gustos dels empleats.

Google hacking

Google i altres cercadors permeten filtrar la informació molt bé.

site:girona.cat

filetype:pdf

Analitzar metadades

Shodan

Cercador de dispositius connectats a internet. Cerca software en comptes de "contingut".
shodan.io

dnsEnum

Enumerar subdominis, poden contenir informació interessant.

theHarvester

Serveix per llistar direccions de correo i/o persones a partir d'una empresa o domini.
Podem atacar a les persones, per acabar accedint a la informació.

WPSCAN

Eina específica per detectar vulnerabilitats en wordpress

Estudi de vulnerabilitats

Les vulnerabilitats de software i de configuració són un vector d'entrada "infalible". Cal tenir en compte les vulnerabilitats que tenim.

WPSCAN i altres

Permet, atacar el login de wordpress, detectar males configuracions i vulnerabilitats de software.

Enumeració d'usuaris de wordpress

Molts wordpress permeten enumerar usuaris.

Navegant a urls estil victima.co/?author=X

Atacs de força bruta

Un atac de força bruta consisteix en provar usuaris i passwords fins a obtenir el desitjat

Força bruta sobre usuaris de wordpress

wpscan permet fer atacs de força bruta contra usuaris.

Podem usar diccionaris personalitzats.

Captura de credencials no xifrades

Mitjançant atacs estil "man in the middle" un atacant pot interceptar el tràfic entre el client (navegador) i el servidor (servidor web amb wordpress) i obtenir les credencials.
Fer servir TLS (HTTPS) ens dona protecció.

Atac sobre el CMS i els seus plugins

Utilitzar una versió antiga de wordpress o plugins vulnerables, garanteix l'accés al wordpress a un atacant.

Mitigació i protecció

Protegir un wordpress és senzill. El principal és mantenir totes les versions actualitzades i instal·lar el mínim de plugins possibles. També cal fer servir passwords segures i connexions segures.

Contrassenyes segures

https://howsecureismypassword.net/

Has sigut hackejat?

https://gotcha.pw/

Actualització de versions

Mantenir les versions actualitzades. Wordpress ens permet mantenir un control de versions i actualitacions fàcil des del panell principal.

Plugins de seguretat

Existeixen certs plugins que ens poden ajudar a mantenir una certa seguretat, comprovant vulnerabilitats automàticament o arxius infectats.
Sucuri és interessant.

Detecció de malware en el servidor

Els plugins de seguretat ens permeten detectar malware.
També podem usar CLAMAV i YARA

Gràcies per venir

Fins aviat!