servis zamkneli z powodu - phishing u!

Autor: oiz - 2008/03/10 19:46

Witam.
Sporo czytam, zanim zapytam, ale nadszed³ ten moment gdzie musze poprosiæ o pomoc.
Dzi¶ dosta³em informacje od administratora swojego serwera hostingowe ze moja strona www.artradio.pl zosta³a zamkniêta z przyczyn:
On Mar 7, 2008, "Security Operations" <SecurityOperations@markmonitor.com> wrote:
> To Whom It May Concern:
>
> It has come to our attention that you are hosting a fraudulent "phish"
> website that is attempting to steal account information from customers of
> Nationwide Building Society. The URL of the fraudulent site is as follows:
>
> http://artwiecz.webd.pl/radio/administrator/components/com_xegallerylm/index.html
>
> The IP address hosting this phish is 83.149.77.178.
>
> Please shut down this site immediately.
>
> Should you have any questions, please call us at +1-301-515-0820.
>
> Thank you,
>
> Bryce Delbridge
> MM Ops Center
>
> -----
> MarkMonitor is researching phishing attacks. Please complete a
> two-minute survey about this phishing incident to help us protect
> Internet users. Survey link: http://www.markmonitor.com/phishingresearch

Strona zosta³a zablokowana ze wzglêdu na phishing!

Moja joomla 1.0.12.a http://pe.joomlapl.com/

Obecnie serwis udostepniono tylko dla jednego IP w celu zwalczeniu problemu.

Proszê do¶wiadczone osoby o pomoc , co w takich przypadkach najlepiej z robiæ, jak ztym walczyæ jak siê zabezpieczyæ >?

==========

Odp:servis zamkneli z powodu - phishing u!

Autor: Iceman - 2008/03/10 22:16

Zoom mia³ dziurê, nie wiem któr± mia³e¶ wersjê ale zobacz
TU.
Musisz przejrzeæ pliki czy nie masz jakiego¶ prezentu.

==========

Odp:servis zamkneli z powodu - phishing u!

Autor: oiz - 2008/03/11 10:18

Czyli wystarcz³o bu oodinstalowaæ komponent zoom galery :)
W sumie nie jest mi na nic potrzebny
Bo nie wiem nawet co mam szukaæ jesli chodzi "prezent"
Co by mog³o wskazywaæ na intruza?

==========

Odp:servis zamkneli z powodu - phishing u!

Autor: Jokris - 2008/03/12 02:18

B) Cze¶æ.
B) Adres Twojej Nowej Domeny = Adres twojego konta na serwerze hostingowym WEBD.PL, bo na to wskazuje katalog o nazwie "radio" i to samo IP, dla serwera z puli hostingu o adresach IP 83.149.77.X/255. IP twojej strony, jak i podanej w ostrze¿eniu jest takie samo, czyli 83.149.77.178. Firma, która wspó³pracuje z Twoimi Adminami, i nie tylko z nimi, od strony bezpieczeñstwa, MarkMonitor, wskaza³a Ci wyra¼nie na plik, który jest wykorzystywany dla celów, w ¶wietle prawa, niegodnych, czyli próby wy³udzenia danych osobowych, danych bankowych lub innych. Po prostu zajrzyj przez FTP co masz tam za niespodziank± w ¶cie¿ce "TUTAJ" w postaci tego pliku index.html, bo w oryginalnym komponencie XeGallery takiego pliku tam nie ma. Usuñ to, co nie powinno tam siê znajdowaæ.(Swoja drog± ciekawa metoda, bo index.html jest standardowo wykorzystywany do w³a¶nie ochrony katalogu przed indeksowaniem. Zwróæcie na do uwagê!. Wszyscy!. Polecam zainteresowanie siê plikiem htaccess Standard SEF). Zostaw tylko te pliki, które s± w oryginalnym pliku instalacyjnym komponentu,. Wrzuæ ewentualnie jaki¶ .htaccess, o tre¶ci:

Options -Indexes

B) Mo¿na zabezpieczyæ dowolny katalog wrzucaj±c plik .htaccess o poni¿ej cytowanych tre¶ciach (te kody poni¿ej nie dotycz± Ciebie, oiz, bo to s± tylko przyk³ady i ciekawostki dla innych u¿ytkowników. Ty masz za zadanie odblokowaæ serwer!!!):

IndexIgnore *

Gwiazdka * (tzw. dzika karta) oznacza ¿e nie chcemy pokazaæ ¿adnych plików w katalogu Index of/. Mo¿emy te¿ np. zablokowaæ wy¶wietlanie tylko okre¶lonych plików, np. obrazków (.jpg, .gif, .png) czy te¿ plików .zip:

IndexIgnore *.jpg *.gif *.png *.zip

TUTAJ masz przyk³ad jak to wygl±da. TYLKO!:cheer: nie klikaj tam gdzie nie wolno!!!!:woohoo: :woohoo:
B) Swoja drog±, to mógby¶ sam trochê pokumaæ:whistle: . Piszê o podstawowym zabezpieczeniu serwisu w swoich artyku³ach na tej stronie. Nic, tylko poczytaæ;) . I wa¿ne. Sprawd¼, czy nie masz dla katalogu "administrator", "components" lub "com_xegallerylm" ustawionych chmodów na 777. Zmieñ na domy¶lne, czyli 755. Nawet, o ile bêdzie Ci dzia³a³o wszystko poprawnie, na 705. Wszystko zale¿y od ustawieñ serwera.

B) Pozdrawiam. Jokris.

==========