
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¶ dostañem 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_xgallerylm/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.joomlapi.com/>

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

Proszê do¶wiadczone osoby o pomoc , co w takich przypadkach najlepiej z robiæ, jak z tym 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 wystarczy³o 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) CzeŹæ.

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 ostrzeżeniu jest takie samo, czyli 83.149.77.178. Firma, która współpracuje z Twoimi Adminami, i nie tylko z nimi, od strony bezpieczeństwa, MarkMonitor, wskazała Ci wyraźnie na plik, który jest wykorzystywany dla celów, w świetle prawa, niegodnych, czyli próby wyłudzenia danych osobowych, danych bankowych lub innych. Po prostu zajrzyj przez FTP co masz tam za niespodziankę w pliku "TUTAJ" w postaci tego pliku index.html, bo w oryginalnym komponencie XeGallery takiego pliku tam nie ma. Usuń to, co nie powinno tam się znajdować. (Swoja droga ciekawa metoda, bo index.html jest standardowo wykorzystywany do wstrzymania ochrony katalogu przed indeksowaniem. Zwróćcie na to uwagę!. Wszyscy!. Polecam zainteresowanie się plikiem htaccess Standard SEF). Zostaw tylko te pliki, które są w oryginalnym pliku instalacyjnym komponentu,. Wrzuć ewentualnie jakiś .htaccess, o treści:

Options -Indexes

B) Można zabezpieczyć dowolny katalog wrzucając plik .htaccess o poniżej cytowanych treściach (te kody poniżej nie dotyczą Ciebie, oiz, bo to są tylko przykłady i ciekawostki dla innych użytkowników. Ty masz za zadanie odblokować serwer!!!):

IndexIgnore *

Gwiazdka * (tzw. dzika karta) oznacza że nie chcemy pokazać żadnych plików w katalogu Index of/. Można też np. zablokować wyświetlanie tylko określonych plików, np. obrazków (.jpg, .gif, .png) czy też plików .zip:

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

TUTAJ masz przykład jak to wygląda. TYLKO!:cheer: nie klikaj tam gdzie nie wolno!!!!:woohoo: :woohoo:

B) Swoja droga, to mógłbyś sam trochę pokumać:whistle: . Pisz o podstawowym zabezpieczeniu serwisu w swoich artykułach na tej stronie. Nic, tylko poczytać;) . I ważne. Sprawdź, czy nie masz dla katalogu "administrator", "components" lub "com_xegallerym" ustawionych chmodów na 777. Zmień na domyślnie, czyli 755. Nawet, o ile będzie Ci działało wszystko poprawnie, na 705. Wszystko zależy od ustawień serwera.

B) Pozdrawiam. Jokris.

=====