Gehacktes Forum bzw. Webspace der Schwyz

Beitrag von „Wernher Graf von Perleburg“ vom 5. Februar 2013, 17:28

Hallo,

man sollte es nicht für möglich halten, aber ich habe tatsächlich aus Geistesabwesenheit nochmal auf den Link in meiner Favoritenleiste zur Schwyz geklickt und mir den Trojaner dort jetzt tatächlich eingefangen. Soviel Dummheit gehört bestraft, mag man mit einigem Recht sagen (nachdem ich es ja bereits vor einigen Tagen festgestellt hatte, daß dort etwas im Busch ist). Ich habe gewiß auch kein sonderliches Verlangen, mich nun dem öffentlichen Spott hinzugeben, da ich allerdings überhaupt nur noch durch abschießen des entsprechenden Prozesses (es ist eine Abwandlung dieses GVU-Trojaners) in den PC reinkomme und Antivierenprogramm, Systemwiederherstellung und abgesicherter Modus blockiert sind (erste Recherchen legen nahe, daß ich u.U. die Festplatte werde formatieren müssen, um das alles wieder loszuwerden), scheint mir das ganze so übel zu sein, daß ich es doch als meine Schuldigkeit ansehe, hier ganz ausdrücklich vor einem Besuch der Seite zu warnen, bis das Problem nicht beseitigt ist und Minasol zu ersuchen, den Zugang von außen zu sperren, damit der Schaden von den übrigen MNlern abgewandt werden kann.

es grüßt ein Volltrottel

Beitrag von „Walter Albrecht“ vom 5. Februar 2013, 18:16

Ach du Schande...

Das tut mir wirklich sehr Leid. Ich habe selbst schon alles versucht, um alles veränderte zu löschen bzw. zu säubern, habe es aber - wie schon bekannt - nicht hinbekommen. Ich habe jemanden angesprochen und darum gebeten, sich das mal anzuschauen. Meine Bitte an Herrn Schiefner wäre jetzt, den Zugang zu sperren, sodass nicht noch weitere Personen von den Trojanern belästigt werden. Wird sich anscheinend leider noch ein bisschen hinziehen bis man die SDR wieder besuchen kann, mir und Bonecker sind jedenfalls die Hände gebunden.

Beitrag von „Juarez Curbain“ vom 5. Februar 2013, 18:30

Ich weiss nicht was sich manche Leute davon versprechen, anderen den Spaß zu nehmen.

Ich hoffe für dich, das du es wieder hinbekommst und sowohl der PC als auch die Schwyz keine folgenschäden davon tragen.

Es mag kein Trost sein, aber im Mittelalter hätten wir solche Leute ausgepeitscht...

Beitrag von „Wernher Graf von Perleburg“ vom 5. Februar 2013, 19:06

Ist ja sonst nicht meine Art, aber diese ausgemachten Arschlöcher könnte man meinetwegen für einige Jahre in einem nordkoreanischen Arbeitslager verschwinden lassen.

Beitrag von „Atropos“ vom 5. Februar 2013, 19:07

UPS, jetzt habe ich das hier weg editiert anstatt zu antworten ... #fail

---

Beitrag von „Walter Albrecht“ vom 5. Februar 2013, 20:09

Danke für den Tipp, erledigt.

Beitrag von „Atropos“ vom 5. Februar 2013, 20:26

Interessant die Seiten dahinter sind noch erreichbar

also board.php etc....

scheinbar machen sie das über ein include an irgendeiner stelle...

Du könntest das ganze jetzt noch für die index.php machen, wenn du willst schreibe ich dir das hier auch noch kurz auf

Du hast FTP Zugriff oder?

Beitrag von „Walter Albrecht“ vom 5. Februar 2013, 20:29

Kann ich dir einfach die FTP-Zugangsdaten geben? Ich kenne mich mit solchen Codeangelegenheiten echt null aus. (Außerdem hat im Grunde mittlerweile jeder die Zugangsdaten, da ich praktisch bei jedem für eine Reparatur des Forums bettle. :D)

Beitrag von „Atropos“ vom 5. Februar 2013, 21:12

Ahh, Sicherheit durch... xD

Muss erst mal gucken wie ich FTP mache, habe zu meinem Server aus Gründen nur SSH

Aber wenn du willst, dann gib mir das

Beitrag von „Walter Albrecht“ vom 5. Februar 2013, 21:16

Das Forum ist ja schon im Arsch, mehr hacken kann man da eh nicht, von daher...

Kommt per PN.

Beitrag von „Atropos“ vom 5. Februar 2013, 21:24

War das Passwort vorher weniger Komplex?

Beitrag von „Friedrich Alexander I.“ vom 5. Februar 2013, 21:24

Sehr ärgerlich das Ganze.
Vor dem Umzug hatte ich bereit eine Kopie des Forums auf meinen Server gestellt, als es dann soweit war, hatte sich dort auch ein Trojaner eingenistet. Die Lösung war das Neuaufspielen des Forums samt dem Einlesen eines Backups.

> Zitat von Juarez Curbain
>
> Es mag kein Trost sein, aber im Mittelalter hätten wir solche Leute ausgepeitscht...

Eher wäre die Person wohl an den Pranger gekommen. 

Beitrag von „Walter Albrecht“ vom 5. Februar 2013, 21:37

> Zitat von Atropos
>
> War das Passwort vorher weniger Komplex?

War genau dasselbe.

Beitrag von „Walter Albrecht“ vom 5. Februar 2013, 21:38

> Zitat von Friedrich Alexander I.
>
> Sehr ärgerlich das Ganze.
> Vor dem Umzug hatte ich bereit eine Kopie des Forums auf meinen Server gestellt, als es dann soweit war, hatte sich dort auch ein Trojaner eingenistet. Die Lösung war das Neuaufspielen des Forums samt dem Einlesen eines Backups.

Ich glaube, das werde ich auch machen müssen.

Beitrag von „Joan Batista“ vom 5. Februar 2013, 21:39

Das ist vermutlich der Bundestrojaner, der gegen Linksextremisten eingesetzt wird. 

Den Verantwortlichen könnte man ruhig mal bei 200 Grad die Hände bügeln.

Beitrag von „Atropos“ vom 5. Februar 2013, 22:25

Wie testet man, ob die Seite Trojaner verbreitet?

Beitrag von „Atropos“ vom 5. Februar 2013, 22:33

Ich habe folgende Dateien bereinigt:

Code

```
cache/templates/0_memberslist_fieldheader.php
cache/templates/4_header.php
cache/templates/4_index.php
cache/templates/2_footer.php
cache/templates/0_footer.php
cache/templates/2_header.php
cache/templates/0_archive_index.php
cache/templates/0_index.php
cache/templates/4_footer.php
```

Beitrag von „Atropos“ vom 5. Februar 2013, 22:38

Weiß jemand wie der Angriff erfolge? War es über FTP?

Beitrag von „Walter Albrecht“ vom 5. Februar 2013, 22:44

Die Datenbank scheint noch ganz zu sein, zumindest sind alle Threads und Posts noch da. Die Index.php's sind gesprengt und wollen nicht mehr funktionieren.

Beitrag von „Atropos“ vom 5. Februar 2013, 22:48

ja, die board.php zeigt mir auch noch Beiträge...

Der Ordner mit dem alten Forum ist auch betroffen...

Beitrag von „Walter Albrecht“ vom 5. Februar 2013, 22:51

Hätte man den Angriff irgendwie verhindern können?

Beitrag von „Atropos“ vom 5. Februar 2013, 22:55

ich glaube es war eine FTP Password Attacke...

Ich habe für diese Art von kritischer Infrastruktur Passworte von über 50 Zeichen, zufallsgeneriert... Wenn es aber ein andere Art von Angriff war, hilft es dort nicht unbedingt...

Beitrag von „Walter Albrecht“ vom 6. Februar 2013, 00:24

Also, aktueller Stand:

Trojaner-Meldungen kommen bei mir keine mehr, das ACP funktioniert einwandfrei, die Boards (somit auch die Threads und Posts) sind da und sind einsehbar, man kann Beiträge schreiben und abschicken usw. Das einzige, was nicht funktioniert: Die index.php will immer noch nicht! Das heißt: Die Übersichtsseite des Forums ist nicht da. Ich gucke mir das ganze Desaster morgen nochmal an und sollte ich zu keinen Ergebnissen kommen, wird das gesamte Forum neuinstalliert, wobei ich nicht wirklich weiß, ob das was bringen wird bzw. würde. Egal, jedenfalls ein dickes Danke an Atropos für die Hilfe!

Beitrag von „Atropos“ vom 6. Februar 2013, 00:33

Kein Problem, da wo ich helfen kann, helfe ich gerne... xD

Beitrag von „Wernher Graf von Perleburg“ vom 6. Februar 2013, 12:07

> Zitat
>
> Ich weiss nicht was sich manche Leute davon versprechen, anderen den Spaß zu nehmen.

Das sind ganz erbärmliche Parasiten, die durch diese Trojaner versuchen, die Rechner anderer Leute auszuspionieren, um an deren Paßwörter und Geld zu kommen oder den Internetanschluß für ihre kriminellen Machenschaften zu mißbrauchen. An der Schwyz als solches hatte dieses Lumpenpack überhaupt kein Interesse. Der GVU-Trojaner verlangt überdies zum Beispiel 100 EUR wegen angeblicher Urheberrechtsverletzungen zu bezahlen, damit diese vermeintliche Sperre durch die GVU wieder freigeschaltet wird.

Beitrag von „Juarez Curbain“ vom 6. Februar 2013, 17:21

Lass uns hoffen, das es sich mit dem "bereinigen" erledigt hat und nicht noch irgend etwas nachkommt. Ich muss zugeben, das ich es etwas beängstigend finde, da ich auch ab und an auf Schwyz-Seite unterwegs war. Nicht das ich mir was eingefangen habe, aber McAff sollte da mir ja schon eine hilfe sein. Interessant wäre es aber alle mal zu erfahren wie es dazu kam, das die Schwyz lahm gelegt wurde.

Gebt doch bitte bescheid, wenn ihr dahingehend einen konkreten verdacht habt. Wobei dies sicherlich nicht zu 100%iger Sicherheit zusagen ist...

@Wernher:
Hast du eigentlich deinen Rechner wieder säubern können?

Beitrag von „Wernher Graf von Perleburg“ vom 6. Februar 2013, 17:31

Sagen wir mal so, er geht wieder, von gesäubert ist er wohl noch weit entfernt. Abgesicherter Modus, Systemwiederherstellung und Firewall sind immer noch nicht benutzbar. Die zusätzlich installierten Virenscanner und die alternative Firewall behindern sich beim Systemstart nach Strich und Faden gegenseitig. Da ich den PC allerdings momentan brauche, bzw. keine Zeit für großartige Datensicherungsaktionen und Neuaufspielen des Betriebssystems habe, bleibt wir wohl nichts anderes übrig, als ihn vom Internet getrennt zu halten bzw. wenn ich doch mal damit reingehe, eben nichts Wichtiges einzugeben.

Beitrag von „Atropos“ vom 6. Februar 2013, 17:38

Guck mal ob dir hiervon etwas hilft:

http://www.youtube.com/user/SemperVideo/videos?query=GVU

Beitrag von „Walter Albrecht“ vom 6. Februar 2013, 19:44

> Zitat von Wernher Graf von Perleburg
>
> Sagen wir mal so, er geht wieder, von gesäubert ist er wohl noch weit entfernt. Abgesicherter Modus, Systemwiederherstellung und Firewall sind immer noch nicht benutzbar. Die zusätzlich installierten Virenscanner und die alternative Firewall behindern sich beim Systemstart nach Strich und Faden gegenseitig. Da ich den PC allerdings momentan brauche, bzw. keine Zeit für großartige Datensicherungsaktionen und Neuaufspielen des Betriebssystems habe, bleibt wir wohl nichts anderes übrig, als ihn vom Internet getrennt zu halten bzw. wenn ich doch mal damit reingehe, eben nichts Wichtiges einzugeben.

Das tut mir wirklich sehr Leid. 

~~-> Ich darf verkünden, dass ich es hingekriegt habe, das Forum wieder zum laufen zu bringen, aber auch nur durch die Hilfe von Atropos. Vielen Dank nochmal - denn: Weil ich ja jetzt auf den ACP-Zugriff hatte, habe ich mich mal durch die Styles durchgeklickt. Das einzig beschädigte index-Template war das vom Style "sdr13". Bei den anderen funktionierte dieses Template. So habe ich das Template einfach ersetzt - und schon wird das Forum wieder angezeigt, zwar mit kleinen Fehlern wegen des Styles, aber die sind leicht zu beseitigen. Damit ist die SDR wieder erreichbar und mein Anti-Viren-Programm zeigt mir auch keine Trojaner mehr an. Ach Wernher, hättest du mit dem Besuchen der Seite doch nur einen Tag abgewartet...~~

Beitrag von „Atropos“ vom 6. Februar 2013, 20:37

Glückwunsch

Jetzt noch Wernher und alles ist gut

Beitrag von „Walter Albrecht“ vom 6. Februar 2013, 23:22

Bitte besucht nicht die SDR-Seite plus das SDR-Forum. Das FTP-Passwort ist anscheinend geknackt, die index.php wurden um 23:11 schon wieder bearbeitet, es sind wieder Viren drauf. Ich könnte kotzen.

Beitrag von „Atropos“ vom 6. Februar 2013, 23:34

Soll ich nochmal?

Beitrag von „Walter Albrecht“ vom 6. Februar 2013, 23:42

Lohnt sich nicht.

Ich habe die Codes aus den index.php rausgenommen, sodass Forum und HP wieder sauber sind. Die dummen Spanier aus Bilbao könnten aber halt jederzeit neue Codes hochladen, diesmal war es ein Java-Dingenskirchen. Die FTP-Zugangsdaten müssen so schnell wie möglich geändert werden, Minasol ist angeschrieben.

Beitrag von „Atropos“ vom 6. Februar 2013, 23:43

Ich glaube eher, dass die Spanier selbst gehackt wurden, das passt ins Bild über einen "Proxy" den Code zu verteilen...

Beitrag von „Walter Albrecht“ vom 6. Februar 2013, 23:45

Wahrscheinlich wieder irgendwelche Hobby-Hacker aus Osteuropa.

Beitrag von „Atropos“ vom 6. Februar 2013, 23:50

Oder fern Ost...

Du könntest den Link hier melden, also mit Image/etc dann sollte Firefox bald die URL blocken...

http://www.google.com/safebrowsing/report_phish/?tpl=mozilla&hl=de

---

Beitrag von „Walter Albrecht“ vom 6. Februar 2013, 23:55

Ich bin mir halt nicht sicher. Ich halte mich da besser raus.

Beitrag von „Atropos“ vom 6. Februar 2013, 23:59

Überlege einfach, wie vielen du hilfst, wenn du die Seite meldest 

Beitrag von „Walter Albrecht“ vom 7. Februar 2013, 00:00

Könnte aber auch eine falsche Fährte sein.

Beitrag von „Atropos“ vom 7. Februar 2013, 00:04

Wenn ihnen keiner sagt, das bei ihnen etwas schiefläuft, werden sie nie etwas ändern 

Beitrag von „Walter Albrecht“ vom 7. Februar 2013, 01:11

Ich schaue mal, ob ich die Webseite irgendwo niedergeschrieben hatte.

Beitrag von „Walter Albrecht“ vom 7. Februar 2013, 14:30

Passwort des FTP ist jetzt geändert. Jetzt dürften keine Viren mehr hochgeladen werden, solange es nicht anderweitige Skripte gibt.

Beitrag von „Wernher Graf von Perleburg“ vom 7. Februar 2013, 15:05

> Zitat von Atropos
>
> Guck mal ob dir hiervon etwas hilft:
>
> http://www.youtube.com/user/SemperVideo/videos?query=GVU

Danke für den Tipp, werde ich mir mal ansehen. Ich habe eigentlich schon einiges abgegrast, einschließlich dem Trojanerboard.

Es sind da wohl Dinge in der Registry geändert worden, die jetzt wieder korrigiert werden müssen - mir fehlt, wie gesagt, gerade die Zeit. Aber es sind auch noch ein paar unsichtbare Quälgeister drauf, die scheinbar immer wieder kommen, vermutlich haben die Burschen auf meinen Rechner Zugiff, obschon mittlerweile keine nennenswerte Aktivität der LAN-Verbindung im Leerlauf mehr zu erkennen ist. Das war direkt nach dem Angriff und vor meinen Gegenmaßnahmen anders.

Letzten Endes werde ich wohl formatieren und Neuaufspielen müssen, sonst ist doch immer ein mumiges Gefühl dabei. Wobei sich zur Zeit das Problem stellt, daß meine letzte CD für ein Betriebssystem Windows 98 ist, was ich eher nicht in Erwägung ziehe. Da sollte der Gesetzgeber mal tätig werden und die PC-Anbieter gesetzlich verpflichten, diese CDs bzw. DVDs wieder beizulegen. So werde ich mich wohl an Microsoft wenden müssen, daß ich eine CD bekomme.

> Zitat
>
> Das tut mir wirklich sehr Leid.

Du kannst ja wirklich nichts dazu. Wenigstens werden die MNler jetzt ein wenig für diese Problematik sensibilisiert, um der Sache etwas abzugewinnen. Ja und ich muß wohl auch mir selbst gegenüber einräumen, die Systemsicherheit etwas vernachlässigt zu haben.

Beitrag von „Hendrik Wegland“ vom 7. Februar 2013, 19:22

> Zitat von Walter Albrecht
>
> Passwort des FTP ist jetzt geändert.

Hoffentlich ist das Passwort diesmal hinreichend sicher.

Beitrag von „Jónas Sigurðsson“ vom 7. Februar 2013, 19:58

> Zitat von Wernher Graf von Perleburg
>
> Letzten Endes werde ich wohl formatieren und Neuaufspielen müssen, sonst ist doch immer ein mumiges Gefühl dabei. Wobei sich zur Zeit das Problem stellt, daß meine letzte CD für ein Betriebssystem Windows 98 ist, was ich eher nicht in Erwägung ziehe. Da sollte der Gesetzgeber mal tätig werden und die PC-Anbieter gesetzlich verpflichten, diese CDs bzw. DVDs wieder beizulegen. So werde ich mich wohl an Microsoft wenden müssen, daß ich eine CD bekomme.

Also auf Win 98 laufen die meisten aktuelen Viren sicher nicht mehr, und auf heutigen Rechnern sollte das auch richtig fix laufen. Falls es überhaupt läuft.

Du könntest dir natürlich auch einfach ein freies Betriebssystem ziehen, dann hättest du gleichzeitig was modernes und weniger virenanfälliges. Wobei sich Umlernen mit keine Zeit natürlich ein Stück weit beißt.

Beitrag von „Hendrik Wegland“ vom 7. Februar 2013, 20:26

> Zitat von Wernher Graf von Perleburg
>
> Da sollte der Gesetzgeber mal tätig werden und die PC-Anbieter gesetzlich verpflichten, diese CDs bzw. DVDs wieder beizulegen. So werde ich mich wohl an Microsoft wenden müssen, daß ich eine CD bekomme.

Ähh... Freunde? Wiederherstellungs-CD?

Beitrag von „Mani Küre“ vom 8. Februar 2013, 10:04

Eine CD liegt doch immer dabei?
Bei meinem neuen Laptop war alles installiert, dennoch die Windows 7 CD dabei.

Beitrag von „Walter Albrecht“ vom 8. Februar 2013, 23:55

Beim zweiten Angriff waren es übrigens Russen, sagt mir der Link im Java-Script, den sie überall auf der Homepage verteilt haben... So ein Dreck.

Beitrag von „Wernher Graf von Perleburg“ vom 9. Februar 2013, 13:05

> Zitat
>
> Also auf Win 98 laufen die meisten aktuelen Viren sicher nicht mehr, und auf heutigen Rechnern sollte das auch richtig fix laufen. Falls es überhaupt läuft.
>
> Du könntest dir natürlich auch einfach ein freies Betriebssystem ziehen, dann hättest du gleichzeitig was modernes und weniger virenanfälliges. Wobei sich Umlernen mit

> keine Zeit natürlich ein Stück weit beißt.

Auf den freien Betriebssystemen läuft dann aber auch wahrscheinlich kein Office und keine sonstigen Programme für Windows, oder war das mal?

> Zitat von Hendrik Wegland
>
> Ähh... Freunde? Wiederherstellungs-CD?

Ja, ich werde mal rumhören, aber ich hatte da schon von unterschiedlichen inkompatiblen Versionen usw. gehört

> Zitat von Mani Küre
>
> Eine CD liegt doch immer dabei?
> Bei meinem neuen Laptop war alles installiert, dennoch die Windows 7 CD dabei.

Beim googeln finden sich genug Beispiele für Leute, die auch keine CD mitbekommen haben, sondern bei denen bloß ein Aufkleber auf dem Gehäuse klebt. Als ich meinen letzten PC kaufte, brauchte ich auch auf die Schnelle einen, weil der alte das Zeitliche gesegnet hatte und habe mich damit nur bedingt auseinandergesetzt. Das gehört jetzt aber wirklich nicht in diesen Thread, wie ich finde.

Beitrag von „Kaetyr Veuxin II.“ vom 9. Februar 2013, 18:33

> Zitat von Wernher Graf von Perleburg
>
> Auf den freien Betriebssystemen läuft dann aber auch wahrscheinlich kein Office und keine sonstigen Programme für Windows, oder war das mal?

Gibt immer noch Wine. Ansonsten: Es läuft Office, aber halt nicht Microsoft Office, sondern OpenOffice oder (besser) LibreOffice.

Beitrag von „Friedrich Alexander I.“ vom 11. Februar 2013, 22:15

> Zitat von Wernher Graf von Perleburg
>
> Sagen wir mal so, er geht wieder, von gesäubert ist er wohl noch weit entfernt. Abgesicherter Modus, Systemwiederherstellung und Firewall sind immer noch nicht benutzbar. Die zusätzlich installierten Virenscanner und die alternative Firewall behindern sich beim Systemstart nach Strich und Faden gegenseitig. Da ich den PC allerdings momentan brauche, bzw. keine Zeit für großartige Datensicherungsaktionen und Neuaufspielen des Betriebssystems habe, bleibt wir wohl nichts anderes übrig, als ihn vom Internet getrennt zu halten bzw. wenn ich doch mal damit reingehe, eben nichts Wichtiges einzugeben.

Bei Windows 7 ist die Sache recht einfach. Nutzt du noch XP?

Ich habe mir das Ding auch mal auf einer eigentlich harmlosen, wie auch verseuchten Seite eingefangen. Habe mich dann über den Affengriff abgemeldet und mich über das Adminkonto von Windows 7 wieder eingeloggt und die Systemwiederherstellung laufen lassen, die betroffenen Systemdateien wurden dann durch Backups ersetzt. Dann die ganzen temporären Internetdateien zur Sicherheit löschen, fertig.

Beitrag von „Wernher Graf von Perleburg“ vom 12. Februar 2013, 01:18

Hat leider in den Fall nichts mit Windowxs XP, Vista oder 7 zu tun. Der Vrirus wurde gegen Ende des letzten/Anfang dieses Jahres so umprogrammiert, daß die Systemwiederherstellung gleich mit lahmgelegt wird (so habe ich es jedenfalls im Netz gefunden). Ich weiß inzwischen auch, was im Prinzip zu tun ist, um den rest wieder in Ordnung zu bringen. Da gibt es auch Rettungs-CDs zum Downloaden, bisher schreckt mich bloß, daß es Leute gibt, bei denen nach Gebrauch

dieser CDs rein gar nichts mehr ging. Im Prinzip ist es aber sowieso angezeigt, das Betriebssystem neu aufzuspielen, hinter diesen Trojanern stecken wohl Verbrecherbanden.

Beitrag von „Hendrik Wegland“ vom 12. Februar 2013, 18:01

> Zitat von Friedrich Alexander I.
>
> Ich habe mir das Ding auch mal auf einer eigentlich harmlosen, wie auch verseuchten Seite eingefangen. Habe mich dann über den Affengriff abgemeldet und mich über das Adminkonto von Windows 7 wieder eingeloggt und die Systemwiederherstellung laufen lassen, die betroffenen Systemdateien wurden dann durch Backups ersetzt. Dann die ganzen temporären Internetdateien zur Sicherheit löschen, fertig.

Würde mich mit der Methode nicht verlassen, wieder ein sauberes System zu haben.

Beitrag von „Dr. Maximilian Gönner“ vom 12. Februar 2013, 20:12

Bei mir wurde beim Versuch die HP der SDR aufzurufen ein Trojanderangriff gemeldet. Es scheint also wieder/immer noch Probleme zu geben. Kann man das ding nicht temporär ins leere laufen lassen, damit zumindest nicht mehr jeder infiziert wird, der drauf geht?

Beitrag von „Walter Albrecht“ vom 12. Februar 2013, 20:33

> Zitat von Dr. Maximilian Gönner
>
> Bei mir wurde beim Versuch die HP der SDR aufzurufen ein Trojanderangriff gemeldet. Es scheint also wieder/immer noch Probleme zu geben. Kann man das ding nicht temporär ins leere laufen lassen, damit zumindest nicht mehr jeder infiziert wird, der drauf geht?

Entschuldige, dachte bis eben, dass das schon so wäre, hatte aber das Hochladen vergessen. Danke für den Hinweis.

Das Problem ist aber nur temporär, ich weiß schon wie das Dingens da wegkriege

---

Beitrag von „Wernher Graf von Perleburg“ vom 12. Februar 2013, 20:34

Wäre es denkbar, daß die den Rechner bereits ausspähen, von dem aus das Paßwort in der Schwyz geändert wurde? Das Paßwort wurde ja schließlich geändert.

Ansonsten fällt mir noch ein, daß das wbb2 ja ftp-Zugang über das ACP haben muß. Ich meine mich da an Gerüchte von Sicherheitslücken zu erinnern. Vielleicht wäre es sinnvoll, den ACP-Ordner noch per .htaccess zu sperren?

Beitrag von „Walter Albrecht“ vom 12. Februar 2013, 20:56

Die Homepage wurde infiziert bevor das Passwort geändert wurde, und zwar zusammen mit dem Forum. Das Forum hab ich einigermaßen zum laufen gekriegt und bei der Homepage fehlt mir eine Datei. Wenn ich die habe, kann ich auch dort alles wieder geradebiegen.

Beitrag von „Atropos“ vom 15. Februar 2013, 02:58

Wenn du nochmal hilfe brauchst, weißt ja wie du mich erreichst

---

Beitrag von „Walter Albrecht“ vom 15. Februar 2013, 17:37

Jop danke! 

Beitrag von „Jan Kozek“ vom 15. Februar 2013, 21:22

Wann ist die Seite ufähr wieder erreichbar? 

Beitrag von „Walter Albrecht“ vom 16. Februar 2013, 11:59

Das Forum ist erreichbar und virenfrei, bei der Homepage kann es noch ein bisschen dauern - aber nur aus zeitlichen Gründen.

Beitrag von „Jan Kozek“ vom 16. Februar 2013, 12:16

Link?

Beitrag von „Jan Kozek“ vom 16. Februar 2013, 12:48

already found