Referendar.de gehackt / Trojanerschleuder?

Beitrag von „alias“ vom 4. November 2012 08:46

Beim Aufruf von Referendar.de erscheint folgende Meldung (Browser: Mozilla 16.0.2 für Ubuntu/Linux)

> Zitat
>
> Safe Browsing
> Diagnoseseite für referendar.de
>
> Wie wird referendar.de momentan eingestuft?
>
> Diese Website ist momentan als verdächtig eingestuft und kann Ihren Computer beschädigen.
>
> Ein Teil dieser Website wurde aufgrund verdächtiger Aktivitäten in den letzten 90 Tagen 6 mal auf die Liste gesetzt.
>
> Was ist passiert, als Google diese Website aufgerufen hat?
>
> In den letzen 90 Tagen haben wir 114 Seiten der Website überprüft. Dabei haben wir auf 15 Seite(n) festgestellt, dass Malware (schädliche Software) ohne Einwilligung des Nutzers heruntergeladen und installiert wurde. Der letzte Besuch von Google war am 2012-11-03. Verdächtiger Content wurde auf dieser Website zuletzt am 2012-11-03 gefunden.
>
> Die Malware umfasst 12 trojan(s). Bei einer Infizierung verursachte die Malware im Durchschnitt 5 neue(n) Prozess(e) auf dem Zielrechner.
>
> Malware wird auf 1 Domain(s) gehostet (z. B. enginepresented.net/).
>
> Diese Website wurde über 2 Netzwerk(e) gehostet (z. B. AS24940 (HETZNER), AS15169 (Google Internet Backbone)).
>
> Hat diese Website als Überträger zur Weiterverbreitung von Malware fungiert?
>
> referendar.de hat in den letzten 90 Tagen scheinbar nicht als Überträger für die Infizierung von Websites fungiert.
>
> Hat diese Website Malware gehostet?

> Nein. Diese Website hat in den letzten 90 Tagen keine Malware gehostet.
>
> Wie ist es zu dieser Einstufung gekommen?
>
> Gelegentlich wird von Dritten bösartiger Code in legitime Websites eingefügt. In diesem Fall wird unsere Warnmeldung angezeigt.
>
> Nächste Schritte:
>
> Zur vorherigen Seite zurück
> Falls Sie der Inhaber dieser Website sind, können Sie eine Überprüfung Ihrer Website hinsichtlich Malware beantragen. Benutzen Sie hierzu die Google Webmaster-Tools. Weitere Informationen über den Prüfprozess erhalten Sie in der Webmaster-Tools-Hilfe.
>
> Alles anzeigen

Beitrag von „beaumchen“ vom 4. November 2012 09:22

Hallo,

ich habe diese Meldung seit gestern abend. Ich habe ehrlich gesagt noch keine Ahnung, hoffen wir auf schnelle Reaktion des Admins.

Grüße

Melle1 im Refforum

Beitrag von „Peach“ vom 4. November 2012 18:39

Hi,

und ich dachte schon es liegt mal wieder an meinem Rechner...bei mir kommt die Meldung seit gestern Nachmittag.
Bin mal gespannt wann sich das klärt - wir hatten gerade vor zwei Wochen einen Hackerangriff in unserem Unisystem. Irgendwie scheints mich gerade zu verfolgen

LG

Beitrag von „Dalyna“ vom 4. November 2012 21:23

Bei mir sah die Meldung anders aus. Aber es lief nach dem Motto: hier weiter und Du hast einen Virus!

Beitrag von „Elternschreck“ vom 4. November 2012 21:41

Hauptsache, dass die Übeltäter bald hinter Schloss und Riegel kommen ! 8_o_) Image not found or type unknown

---

Beitrag von „Bolzbold“ vom 4. November 2012 22:09

Das Einloggen scheint dort mit Trojanern belohnt zu werden. Aktuelle Spyware und Virensoftware scheint das aber problemlos in den Griff zu kriegen.
Solange das nicht behoben ist - Finger weg von der Seite.

Der Admin weiß Bescheid - mal sehen, wann und wie er reagiert.

Gruß
Bolzbold

Beitrag von „Orasa“ vom 5. November 2012 19:11

Super, dass man hier immer ne Antwort findet. War total irritiert, als ich eben die Seite besuchen wollte. Bin mal gespannt, wie schnell was passiert.

Beitrag von „WispyWaterfall14734“ vom 5. November 2012 19:47

jop, mich wundert, dass der admin die seite nich erstmal ganz off genommen hat^^

Beitrag von „jole“ vom 5. November 2012 20:21

Ich habe es auch gemerkt und gedacht, es liegt an mit. Ich habe jetzt bisschen Sorge mir etwas zugezogen zu haben, da meine Rechner dort immer angemeldet sind... Blöd! Reicht Virenprogramm bei Windows? Was ist mit Apple?

Argh....

Beitrag von „Bolzbold“ vom 5. November 2012 21:21

Ein aktuelles Virenprogramm sollte ausreichen. Über Apple kann ich nichts sagen.

Beitrag von „alias“ vom 6. November 2012 20:08

Bin gerade auf eine Beschreibung gestoßen, wie solche "Hacks" arbeiten und wo die von Referendar.de drehen müssten, um das los zu werden - falls diese Form verwendet wurde
http://www.tumblr.com/tagged/hack?before=1329947869

Beitrag von „Dalyna“ vom 6. November 2012 22:04

In der Regel sollte Apple okay sein. Die meisten Viren greifen bei Apple nicht.

Beitrag von „alias“ vom 6. November 2012 22:08

Auch die Pinguin-Familie hat ein dickes Fell - bzw. eine beinahe undurchdringliche Schwarte - den Rest packt ClamAV

[Blockierte Grafik: http://www.vereinpromedien.de/pictures/promedien/pi/size1_70px/pinguin-tafel.gif]

Beitrag von „chrisy“ vom 9. November 2012 06:14

> Zitat von cressi
>
> jop, mich wundert, dass der admin die seite nich erstmal ganz off genommen hat^^

Ist die Site abgesehen vom Forum schon seit Jahren nicht mehr aktualisiert worden. Vermutlich eine Website, deren Existenz nur noch zwecks Werbeeinnahmen und hoher Zugriffszahlen besteht.

Beitrag von „WispyWaterfall14734“ vom 10. November 2012 08:38

es ist/ war das Forum schlechthin für Referendare....bis jetzt tut sich nichts auf der Seite...weiß jemand genaueres über den Neustart?

Beitrag von „beaumchen“ vom 11. November 2012 20:45

Wir wissen, dass sich jemand darum kümmert, mehr leider nicht.

Beitrag von „Bolzbold“ vom 13. November 2012 15:52

Die Seite ist ab sofort wieder clean und online abrufbar.

Aktuelle Virenprogramme sollten jetzt keine indizierte Seite mehr anzeigen.

Gruß
Bolzbold

Beitrag von „chilipaprika“ vom 13. November 2012 16:11

Gab es eventuell einen Datenverlust?

Ich kann mich nicht einloggen und die Maske sagt mir sogar, dass es keinen Benutzer mit der Kombination von Email-Adresse und Name gibt...
an wen kann ich mich dann wenden?

Chili

Beitrag von „flockenschaf“ vom 13. November 2012 16:15

Mein McAfee mag die Seite noch immer nicht und ganz einwandfrei läuft sie auch nicht, zumindest bei mir kommt öfter mal die Meldung "Beitrag/User existiert nicht"....

Beitrag von „alias“ vom 13. November 2012 16:20

Kann sich überhaupt jemand anmelden? Momentan sind nur 3 Mitglieder online:

> Zitat
>
> Insgesamt sind 54 Besucher online: 3 registrierte, 0 unsichtbare und 51 Gäste (basierend auf den aktiven Besuchern der letzten 5 Minuten)
> Der Besucherrekord liegt bei 226 Besuchern, die am 16.08.2012, 17:57:55 gleichzeitig online waren.
>
> Mitglieder: Bing [Bot], Google [Bot], Google Adsense [Bot]

Referendar.de hat interessante Mitglieder 

Mal abwarten, was geschieht. Im Augenblick ist ja auch kein Kommentar der Admins zum "Blackout" zu sehen.

Beitrag von „tiffy“ vom 13. November 2012 18:18

geht mir genauso

Beitrag von „Cambria“ vom 13. November 2012 18:21

Zwei Beiträge von heute sind aber drin, allerdings von Usern, die sich neu registriert haben und ihren ersten Beitrag geschrieben haben.

Beitrag von „cassiopeia“ vom 13. November 2012 18:43

ist vielleicht die ganze datenbank leer?

ich habe heute gesucht, in der suche wurden auch ergebnisse angezeigt. wenn ich aber auf den jeweiligen beitrag geklickt habe, dann war die aufgerufene seite leer.

Beitrag von „beaumchen“ vom 13. November 2012 19:41

Ich-als Mod- kann mich auch nicht anmelden.

Beitrag von „Bolzbold“ vom 13. November 2012 20:12

Der Admin weiß Bescheid.

Das mit der Datenbank könnte in der Tat ein Problem sein.

Warten wir es ab.

Gruß
Bolzbold

Beitrag von „indidi“ vom 13. November 2012 21:38

> Zitat von chilipaprika
>
> Gab es eventuell einen Datenverlust?
>
> Ich kann mich nicht einloggen und die Maske sagt mir sogar, dass es keinen Benutzer mit der Kombination von Email-Adresse und Name gibt...
> an wen kann ich mich dann wenden?
>
> Chili

Genau das Problem habe ich auch.---Und ich bin seit Jahren mit dabei.

Beitrag von „Schmeili“ vom 14. November 2012 16:07

> Zitat
>
> Hackerangriff
>
> [Blockierte Grafik: http://www.referendar.de/forum/styles/prosilver/imageset/icon_post_target.gif]von **admin** » 14.11.2012, 14:50:15
>
> Liebe Foristen, liebe Teilnehmerinnen und Teilnehmer

Wie Ihr alle mitbekommen habt, gab und gibt es seit ca 10 Tagen massive technische Probleme mit unserer Seite und dem Forum.

Die
ganze Seite war einem - leider erfolgreichen - Hackerangriff
ausgesetzt. Wir wissen nicht, über welches Tor der Angreifer sich
Schreibrechte besorgte. Eine Möglichkeit wäre das phpbb-Forum
(Schwachstelle in der Software). Da unsere Systeme eigentlich sehr
sicher und stabil laufen, denken wir eher an ein Softwareproblem des
Forums.
Wer hat uns angegriffen? Auch dies ist nicht ganz klar. Wir beobachteten allerdings eine Zunahme von Zugriffen aus Russland.
Zwischenzeitlich
war die Seite deshalb auf einer Blacklist von Google und McAfee. Hier
sind wir wieder als "unbedenklich" eingestuft.
Unser IT-Spezialist hat nun in einer langen Nachtschicht den gesamten Server, Software, Forum neu aufgesetzt.
Jetzt
besteht gerade noch ein großes Problem, da wir zwar wirklich ein
-unverseuchtes - Backup haben (vom 27.10.), aber die Forensoftware
weigert sich standhaft, dieses Backup mit allen Werten und Inhalten
korrekt einzuspielen. Warum dies so ist, wissen derzeit die Götter; ich
jedenfalls muss auf meinen IT-Gott warten, vielleicht hat der eine
Lösung.

Habt Ihr Euch nun nach dem 3.10. einen Virus wegen unserer Seite eingefangen?
Genau kann ich das nicht sagen. Auf all unserern Rechnern war kein dauerhaftes Problem erkennbar.
Alle
Antivirenprogramme haben schlicht und einfach den Zugriff verweigert.
(Wir verwenden mehrere Programme, vor allem kostenfreie! Alle haben
einwandfrei funktioniert.)
Zur Sicherheit könnt Ihr ja noch eine
vollständige Systemprüfung mit einem Antivirenprogramm Eurer Wahl
durchführen. Das müsste genügen.

Vielen Dank für Euer Verständnis.

Wir hoffen, dass es bald weitergeht - bleibt bei uns und schaut in ein paar Tagen wieder rein.

Viele Grüße
admin

Alles anzeigen