

Malware Warnung

Beitrag von „achso“ vom 17. Oktober 2010 12:36

Seit heute bekomme ich von Google die Warnung, dass lehrerforen.de Malware über einen anderen Server hostet. Gesehen unter Chromium mit aktivierter Malwarewarnung.

Hier:

Warnung: Durch das Aufrufen dieser Website wird Ihr Computer möglicherweise beschädigt!

Die Website unter <https://www.lehrerforen.de> enthält Elemente der Website 333.goldgroupg.com, die anscheinend Malware hostet, also Software, die den Computer beschädigen oder anderweitig ohne Ihre Zustimmung agieren kann. Schon der Besuch einer Website, die Malware enthält, kann den Computer infizieren.

Detaillierte Informationen zu den Problemen mit diesen Elementen erhalten Sie auf der folgenden Google-Seite: SafeBrowsing Diagnosesseite für 333.goldgroupg.com.

Beitrag von „cubanita1“ vom 17. Oktober 2010 13:18

Mir hat der Pc vorhin beim Öffnen von Lehrerforen auch was von "Achtung" und "Bereinigen" erzählt ...

Beitrag von „Meike.“ vom 17. Oktober 2010 13:28

Bei mir poppt das auch immer auf und nervt tierisch - Kaspersky sagt dann im Bericht widersprüchlicherweise aber "ungefährlich" und zeigt es mir nicht an zum "entlisten". löschen oder in die Quarantäne sperren.

Beitrag von „jotto-mit-schaf“ vom 17. Oktober 2010 14:17

AntiVir hat sich eben auch beschwert. Interessanterweise jetzt aber nicht?

Beitrag von „Stefan“ vom 17. Oktober 2010 14:28

Ich habe Chrome mal installiert.

Bei mir meckert er nicht.

Auf welcher Seite war das? Passiert das immer? Nutzen die anderen auch Chrome?
Welche Werbung seht ihr in dem Moment oben und unten?

Also ich schleuse keine Malware ein. Wenn da was auftaucht muss ich untersuchen wo das herkommt.

Im Moment bin ich etwas ratlos.

ACHTUNG: Wenn lehrerforen.de bei euch irgendwas installieren will, lehnt das auf jeden Fall ab.

Stefan

Beitrag von „cubanital“ vom 17. Oktober 2010 14:40

Also, Stefan, als ich heute zum ersten Mal auf lehrerforen gekommen bin, (10 uhr) hat Microsoft Security die Warnung angezeigt und dann wie gesagt bereinigt.

Ich hab jetzt mal im Verlauf nachgesehen und da sagt es mir, das folgendes entfernt wurde, weil böartig

VirTool:JS/Obfuscator.Y

was auch immer das ist ... hilft dir die Info?!

Beitrag von „Stefan“ vom 17. Oktober 2010 15:59

Ich bin noch auf der Suche.

Ich habe im Internet gefunden, dass wir nicht die einzigen Betroffenen sind.
Das Problem scheint also irgendwo zentraler gelegen zu sein.

Ihr solltet aber auf jeden Fall euren Internatcache/temp. Internetdateien einmal löschen.

Stefan

Beitrag von „v1981“ vom 17. Oktober 2010 16:05

Zitat

ACHTUNG: Wenn lehrerforen.de bei euch irgendwas installieren will, lehnt das auf jeden Fall ab.

als ich heute morgen auf die seite ging, sollte irgendwas mit "java" installiert werden, hab leider bestätigt, da ich "java" als nichts schlimmes empfand...jetzt lass ich grad mein virenprogramm drüber laufen und der erste fund ist:

"JAVA/Agent.HN"



Beitrag von „Flipper79“ vom 17. Oktober 2010 16:25

Hallo stefan,

ich habe das Problem auch und hab ne Bildschirmkopie von der Warnmeldung bekommen. Die schick ich dir per Mail.

lg

Beitrag von „Flipper79“ vom 17. Oktober 2010 16:25

Hallo stefan,

ich habe das Problem auch und hab ne Bildschirmkopie von der Warnmeldung bekommen. Die schick ich dir per Mail.

MEdlungen bekommen ich bei FF und IE.

Bei schulthemen.de das gleiche Prob.

Ig

Edit: Mail ist an die im Impressum geannte Mailaddy raus. Aber Meldung bekam ich schon gestern abend. 😞

@ v1981 Dieses Programm möchte sich bei mir auch downloaden, aber schon seit Tagen. DAS nervt mittlerweile. Wenn ich es denn downloade, sagt er mir, dass es schon auf PC ist. Toll! Aber das ist nen anderes Thema.

Edit 2: Hab mal meinen Virens scanner drüberlaufen lassen. Unter "Bericht" wird mir angezeigt, dass eine Datei / Link whatever (333.goldgroupg.com.), die hier im Thread auch schon geannt wurde, verdächtig sei.

Die Gefärdung sei hoch. Aber ich kann das Dingen nicht in Quarantäne stecken oder entfernen (nur aus der Liste entfernen, was mir ja nix bringt).

Beitrag von „Britta“ vom 17. Oktober 2010 21:16

Ich hab das Problem seit gestern. Beim ersten Öffnen der Lehrerforen blockt mein Antivir auch ab und warnt, dass irgendwas downgeloadet werden soll. Wenn ich dann Firefox nochmal schließe und neu aufmache, hab ich kein Problem mehr.

Beitrag von „Stefan“ vom 17. Oktober 2010 21:45

So - nun sollte alles wieder OK sein.

Leider sind wir Opfer eines Angriffs geworden. Jemand ist bei uns eingedrungen und hat Code an die Banner angehängt.

Ich hoffe die Lücke geschlossen zu haben. Die schadhaften Codes habe ich entfernt. Das scheint gestern im größeren Stil passiert zu sein. Jedenfalls habe ich noch mehrere andere Betroffene gefunden.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Bitte leert unbedingt eure temporären Internetdateien und Browsercaches und lasst einen Virenschanner über eure Platte laufen.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Ich werde das die nächsten Tage im Auge behalten.

Sorry.

Stefan

Beitrag von „achso“ vom 17. Oktober 2010 22:24

na, gut dass ich das mal erwähnt habe 😊

Beitrag von „Stefan“ vom 17. Oktober 2010 23:12

Zitat

Original von achso

na, gut dass ich das mal erwähnt habe 😊

In der Tat. Ansonsten hätte ich es wahrscheinlich noch nicht bemerkt.

Ehrlich gesagt, was das sogar noch ein Stück härter als der Servercrash letztens.

Ich bin nur froh, dass ich das Ganze so schnell sauber bekommen habe.

Ansonsten hätte ich das Forum Offline nehmen müssen.

Ich hoffe nur das ich alles gefunden habe (habe mehrfach alles gechecked) und die Lücke nun wirklich dicht ist und die Eindringlinge nicht eine noch unbekannte Lücke genutzt haben.

Danke nochmal

Stefan

PS:

Nochmal an alle. Das Forum wird NIEMALS dazu auffordern etwas zu installieren. Einzige

Ausnahme könnte der Chat beim ersten Aufruf sein.

Beitrag von „Hannah“ vom 18. Oktober 2010 16:00

Mal ne etwas blöde Frage... war das ein Tierchen, das Linux-Rechnern gefährlich werden kann oder stürzt es sich nur auf Windows-Rechner?

Ich hab überhaupt keinen Virenschanner, nachdem es immer hieß, dass man den bei Linux (im privaten Gebrauch) nicht braucht...