

Chinesischer Wetterballon über dem Hackintosh-Forum?

Beitrag von „EmilDeumel“ vom 5. Februar 2023, 08:20

Oder steht der HF server in China?

Beitrag von „Basti Wolf“ vom 5. Februar 2023, 08:28

Mods sind bereits informiert und ich bin schon am verschieben. Sollte bald vorbei sein.

Edit: sind noch Threads auf dem Dashboard zu sehen ?

Beitrag von „N0b0dy“ vom 5. Februar 2023, 08:39

[Basti Wolf](#) ja noch eins

Beitrag von „al6042“ vom 5. Februar 2023, 09:38

Habe die Threads eben entfernt.

Beitrag von „EmilDeumel“ vom 5. Februar 2023, 13:44

War das jetzt eine technische Fehlfunktion oder ein blinder chinesischer "Racheakt" für ihren

dämlichen ballon?

frage nur aus Neugier.

Beitrag von „al6042“ vom 5. Februar 2023, 13:49

Wen interessiert das letztendlich wirklich?

Wenn es eine Politisch motivierte Aktion war, hat sie hier nichts zu suchen.

Wenn es ein "technische Fehlfunktion" war, kümmert sich das Team um die Behebung.

Beitrag von „griven“ vom 5. Februar 2023, 15:06

EmilDeumel generell wie [al6042](#) schon schrieb darüber hinaus war es weder das eine (Racheakt) noch das andere (Fehlfunktion) sondern ein Phänomen das so alt ist wie Internetforen selbst 😊

Man nennt das Forenspam und es ist eine ebenso aufdringliche wie nervige Art und Weise "Werbung", oftmals für zweifelhafte Dinge, in Foren zu platzieren. Normalerweise kümmert sich unsere Firewall darum das solche Bots gar nicht erst den Weg ins Forum finden es kommt aber immer wieder vor das Botnetze noch nicht von den einschlägigen Blocklisten erfasst sind und dann eben doch durch die Firewall schlüpfen. Nachdem jetzt eine ganze Weile relative Ruhe geherrscht hat ist in den letzten Wochen wieder vermehrte Aktivität zu verzeichnen es sind also wieder mehr Bots unterwegs und somit schlagen auch wieder öfter mal welche trotz Firewall und allen möglichen Schutzmaßnahmen doch im Forum auf. Das ganze ist leider ein ziemlich lästiges Katz und Maus Spiel und es gibt keine zuverlässige und zu 100 Prozent wirksame Methode das komplett zu unterbinden. Ist ein bisschen wie nen Schnupfen halt da und lästig aber mit den richtigen Medikamenten und genügend Taschentüchern nicht lebensbedrohlich und ziemlich gut in den Griff zu bekommen 😊

Beitrag von „thahammer“ vom 5. Februar 2023, 15:34

Konnte das überhaupt jemand lesen bzw. verstehen bei uns im Forum?

Beitrag von „EmilDeumel“ vom 6. Februar 2023, 05:32

also mich hat das durchaus interessiert, auch weil da ja meistens was von College und university of Soundso Dstand hatte ich gedacht, dass vielleicht ein Irrläufer oder sowas war.

Dankefür die sachlich und zivilisiert vorgetragene Info [griven](#) .

Beitrag von „Raoul Duke“ vom 6. Februar 2023, 06:54

Text kopieren und von einem Online Übersetzer übersetzen lassen, ist ganz einfach und dauert nicht länger als ein Thema zu erstellen

Aber das ist ja langweilig 😊

Beitrag von „EmilDeumel“ vom 6. Februar 2023, 07:08

Habe ich vorhin bei der zweiten Attacke gemacht als hier noch alle geschlafen haben.

Scheinen Stellenanzeigen zu sein wenn Google Translate nicht gelogen hat.

Beitrag von „Coaster“ vom 6. Februar 2023, 07:16

Schade, ich wollte mir schon nen Doktor Titel kaufen 😞 Ich hab doch sonst nur die Brille zum schlau aussehen

Beitrag von „apfel-baum“ vom 6. Februar 2023, 08:27

ja, immer diese groschenhefte, arzt und försterromane... dafür reicht es dann, das die hier immer so spammen müssen

Beitrag von „Raoul Duke“ vom 6. Februar 2023, 08:57

Stellenangebote für IT-Sicherheit wäre mal originell

Oft ist es sinnlos und nicht mal für Muttersprachler zu verstehen

Beitrag von „EmilDeumel“ vom 6. Februar 2023, 12:46

[Zitat von Coaster](#)

Schade, ich wollte mir schon nen Doktor Titel kaufe. 😞 Ich hab doch sonst nur die Brille zum schlau aussehen

Dann hat Google also gelogen und esging um käufliche Dr Titel.

Beitrag von „guckux“ vom 8. Februar 2023, 06:12

Mein Mitgefühl an die "Ordner des Forums" (landläufig auch Moderatoren genannt) - schon

wieder eine Welle reimgeschwappt 😞

Seufz - auf daß die Wogen sich bald glätten!

Beitrag von „EmilDeumel“ vom 8. Februar 2023, 06:15

Anscheinend haben die einen Narren an diesem Forum gefressen und imer morgens um 5

Immerhin, jetzt weiß Googele Translate worums geht:

"Ein Diplom machen, ein Diplom ausstellen, ein Diplom kaufen, ein Abschlusszeugnis erhalten und vom Auslandsstudium zurückkehren"

Beitrag von „griven“ vom 8. Februar 2023, 07:14

Naja das sind Bots also automatisierte Skripte und da hat auch niemand einen Narren gefressen sondern da geht es schlicht und ergreifend ums Geld. Die Betreiber dieser Netzwerke werden dafür bezahlt eine gewisse Menge von dem Schund mit einer gewissen Streuung und Reichweite zu verbreiten und genau das tun sie hier und anderswo. Der Aufwand lohnt anscheinend denn solange auch nur wenige dumm genug sind die Links anzuklicken ist das Ziel schon erreicht (und nein es geht sehr wahrscheinlich nicht primär darum irgendwelche Abschlüsse an den Mann oder die Frau zu bringen)...

Anyway auf unserer Seite bleibt eigentlich nur die Augen aufzuhalten und zu löschen/sperrern bzw. die Netzwerke eben auch in die Firewall zu prügeln solange sie nicht in den einschlägigen RBL's enthalten sind aktuell gerade maximal nervig 😞

Beitrag von „ozw00d“ vom 8. Februar 2023, 07:25

[griven](#) reicht eine netzsperre nicht aus?

Hatte ich in meinem Forum damals auch via cloudflare eingerichtet. Einfach alles sperren was aus ru,cn etc. eben alles woher dieses gespamme kommt (lässt sich abfangen) wegsperren. Immer größere Hürden einbauen. Je schwieriger es für die Vögel ist ihren netz-dung abzusondern, um so eher habt ihr Ruhe.

Beitrag von „griven“ vom 8. Februar 2023, 07:33

[ozw00d](#) genau das tun wir schon 😊

Die Firewall prüft jedes Paket gegen diverse RBL's (Spamhaus, StopForumSpam etc.) und ist normalerweise auch recht effektiv dabei nur handelt es sich bei der Welle offenbar um noch relativ neue und unbekannte Netzwerke. Die IP's sind bunt gestreut es lässt sich also nicht mit Sicherheit sagen wo die her kommen. Aktuell haben wird unter anderem Singapur,Deutschland,Taiwan als Herkunftsländer ausgemacht denke aber das werden noch mehr werden. Den Block aus Singapur habe ich eben manuell in die Firewall gepackt. Generell mag ich es gerne vermeiden ganze Länder (Geo Location) zu banen denn damit sperrt man auch legitime User aus und das kann ja nicht das Ziel sein. Mich würde es nicht wundern wenn das alles kompromittierte Maschinen aus dem ESXi Hack sind die da gerade aktiv sind (erklärt auch ein wenig die bunte Streuung der IP's)...

Beitrag von „apfel-baum“ vom 8. Februar 2023, 08:09

jupp, das vermute ich auch, daher sind ja einige dabei auf etwas anderes ala proxmox zu migrieren, mute maße ich mal so 😊

Ig 😊

Beitrag von „cologneskater“ vom 8. Februar 2023, 11:16

Ein Lob an die Admins und Forenverwalter für Eure aufopfernde Pflege, das Forum von diesem Bot-Mist freizuhalten.

Ich selbst hatte vor Jahren in einem Skaterforum selbst damit zu kämpfen. Das Forum lief damals als zusätzliches Modul unter TYPO3 und war einige Zeit besonders anfällig für Spam. Die Entfernung von Spam führte letztlich dazu, dass User-Neuanmeldungen erst nach manueller Freischaltung durch den Admin etwas posten konnten. Weil zeitweise nachts so 30 bis hin zu 50 Neuanmeldungen auftraten und die Usernamen glücklicherweise sehr skriptgeneriert aussahen und eine Kontakt-Email-URL enthielten, die zu einem deutschsprachigen Forum keinen Bezug aufwiesen, war es dennoch aufwändig, das System sauber zu halten.

Hohe Pflegeaufwände werdet Ihr derzeit auch haben, deshalb: Vielen Dank für Euer Engagement!!!

Beitrag von „EmilDeumel“ vom 9. Februar 2023, 06:10

Anscheinend geht das jetzt jeden Morgen so wenn ich mir das so ansehe. Grad ja auch wieder
Müsst ihr da immer manuell ran weil die immer manuell ein Account anlegen oder wie?

Beitrag von „griven“ vom 9. Februar 2023, 07:13

So schaut das aus EmilDeumel zumindest so lange bis die IP Ranges bekannt sind von denen die Angriffe aus erfolgen und in die entsprechenden Blocklisten aufgenommen sind. Was es schwer macht ist die Tatsache das die Accounts ziemlich bunt durch den Garten von Netzwerken überall auf der Welt verteilt erzeugt werden. Der Kollege heute kam mit einer IP rein die in die USA auflöst (Kalifornien) was meine Theorie eines Zusammenhangs mit dem ESXi Hack eher bekräftigt als entkräftet. Obendrein sind die auch "schlau" genug sich nicht wie üblicherweise zu verhalten es werden also nicht wie sonst gleich 4 oder 5 Accounts erzeugt

und dann losgelegt sondern es ist pro IP immer nur ein Account manchmal zwei was zeigt das sie ebenfalls gelernt haben auf Automatismen wie die Erkennung von Doppelaccounts zu reagieren...

Beitrag von „guckux“ vom 9. Februar 2023, 08:05

Tja, da hat sich in den letzten 30 Jahren nichts geändert, man rennt dem Schotter immer hinterher... 😞

Beitrag von „EmilDeumel“ vom 9. Februar 2023, 10:24

Nur so ne Idee [griven](#) - die Registrierungs Funktion zwischen 4 und 6 Uhr morgens abschalten?

Die scheinen ja ihre festen Zeiten zu haben.

Beitrag von „griven“ vom 9. Februar 2023, 10:36

Nö dat bringt nix dann kommen sie später oder früher...

Das kannste drehen und wenden wie Du willst auf so "relativ" einfache Art wird man das nicht los. Abgesehen davon das es eben nichts bringt muss man, meiner Meinung nach, zudem bei allem was man tut auch im Auge behalten das man den "normalen" Betrieb damit nicht über Gebühr einschränkt bzw. legitime Nutzer so wenig wie möglich belastet bzw. eingeschränkt werden. Wir sind dran und arbeiten an, hoffentlich wirksamen, Maßnahmen die es zwar nicht verhindern werden das sich auch in Zukunft Bots anmelden aber vielleicht dazu beitragen das unsere Plattform als Ziel uninteressant wird. Spam und Linkplatzierungen bringen nur dann was wenn sich auch gesehen werden gelingt es uns zu unterbinden das der Kram gesehen wird dann sind wir ganz schnell einfach kein lohnendes Ziel mehr. Morgen um die Zeit werden wir schlauer sein und sehen ob unsere ergriffenen Maßnahmen fruchten oder nicht.

Beitrag von „simon0302010“ vom 9. Februar 2023, 10:40

Wie kommen die eigentlich um den Captcha Test bei der Account-Erstellung? Vielleicht gibt ja auch Anti-Bot Tests, die besser funktionieren...

Beitrag von „bluebyte“ vom 9. Februar 2023, 12:22

[simon0302010](#) automatische Capture-Erkennung kenne ich seit 2008. Bekommt man mit ein wenig Programmieraufwand in den Griff. Ist also kein großes Ding.

Beitrag von „Nightflyer“ vom 9. Februar 2023, 12:34

Captcha-Erkennung und Capture-Erkennung sind zwei verschiedenen Paar Schuhe.

Oder hast du dich vertippt [bluebyte](#) ?

Beitrag von „griven“ vom 9. Februar 2023, 13:59

Bluebyte wird schon Captchas meinen und recht hat er ein Captcha ist für jeden einigermaßen ernsthaft gestrickten Bot keine wirklich Hürde (mehr) und der gebotene Schutz durch ein Captcha ist bestenfalls noch als rudimentär einzustufen. Ein Captcha ist halt eine Hürde die einem wenigstens die vom Leibe hält die so gar keinen Bock haben ein wenig Hirnschmalz in ihre Skripte zu investieren der ganze Rest lacht halt drüber und löst ein Captcha genau so effektiv und selbstverständlich wie wir es tun. Eine Möglichkeit wäre eine Art Quiz bei dem während der Registrierung aus einem zufälligen Fragenpool eine Frage ausgewählt wird und bei dem man die Antwort auf die Frage manuell eintippen muss (Stichwort keine vorhersehbaren Muster) allerdings sind solche Quizze auch wieder eine Hürde die potentielle

Nutzer einschränkt/abhält denn zum einen muss man die Antwort kennen und zum anderen muss man sie auch noch orthografisch richtig schreiben können...

Wie auch immer im Bereich der Registrierung/des Onboardings anzugreifen ist eher nicht praktikabel und sinnvoll umsetzbar da es entweder mit unverhältnismäßig hohem Aufwand (manuelle Freischaltung) oder unakzeptablen Einschränkungen (captcha Alternative, Fragen etc.) einher geht. Filterung muss demnach entweder schon passieren bevor der User sich überhaupt registrieren kann (Firewall/RBL Abgleiche) oder eben auf Content Ebene nachdem er aktiv geworden ist. Bisher realisieren wir das Filtern "nur" auf Netzwerkebene also bevor ein User sich überhaupt registriert hat und bisher sind wir damit gut gefahren. In der aktuellen Welle scheint ein filtern auf Netzwerkebene aber nicht ausreichend zu sein einfach weil die Bots offenbar noch nicht in den Blocklisten enthalten sind. Wir haben daher jetzt notgedrungen Maßnahmen ergriffen die auf Content Ebene eingreifen also quasi dann wenn der User bereits registriert und aktiviert ist. Notgedrungen deshalb weil ein filtern auf Content Ebene eben immer auch damit einhergeht das man einschränkt was User im Forum dürfen und was nicht.

Es ist schwierig hier das richtige Maß zu finden denn auf der einen Seite steht, zumindest für mich, an oberster Stelle das legitime Nutzer keine Einschränkungen in der Nutzbarkeit des Forums erfahren dürfen auf der anderen Seite geht es aber eben auch nicht ohne Einschränkungen. Die Kunst liegt nun darin so zu agieren das die ergriffenen Maßnahmen zielgenau die User die den Spam verbreiten soweit einschränken das sie das nicht mehr tun können ohne alle anderen zu behindern bzw. einzuschränken. Ich denke wir haben einen Weg gefunden der das auf Content Ebene gut und zuverlässig erledigen kann trotzdem kann es zu Fällen kommen wo der Filter zuschlägt ohne das die betroffene Person ein Spammer ist. Sollte das der Fall sein bitte ich die betreffenden User sich bei uns zu melden denn in diesen Fällen ist dann eine Einzelbetrachtung angesagt.

Beitrag von „bluebyte“ vom 9. Februar 2023, 21:02

Natürlich meinte ich CAPTCHA. Schuld war meine automatische Rechtschreibkontrolle vom iPhone.

Früher gab es CAPTCHA hauptsächlich beim Login auf irgendwelchen Game-Servern. Ich erinnere mich noch gut an das CAPTCHA-Tool von SRO. Dieses wurde später auch in den Sbot integriert. Jetzt wird man überall mit diesen wirklich nervigen reCAPTCHA konfrontiert. Diese

lassen sich mittlerweile auch schon automatisch lösen.

Beitrag von „Coaster“ vom 9. Februar 2023, 21:54

Brauch ich auch mal, so nen Bot, der die für mich löst, ich scheitere da gerne im ersten Versuch dran

Beitrag von „user232“ vom 9. Februar 2023, 22:38

Die beste Verifizierung hat die HUK. Hab das zuvor noch nirgends gesehen, ist auch für registrierter Nutzer einfach zu bedienen und braucht keinerlei Aufmerksamkeit und Hirnschmalz.

Passwort
●●●●●●●● 

E-Mail-Adresse merken

 Anti-Roboter-Verifizierung 

[Zugangsdaten vergessen?](#)

Beitrag von „griven“ vom 10. Februar 2023, 07:43

Ich bin einigermaßen zufrieden denn unsere ergriffenen Maßnahmen zeigen ganz offensichtlich Wirkung 😊

Beitrag von „EmilDeumel“ vom 15. Februar 2023, 06:28

Der Chinese war wieder zwischen 3 und 4 Uhr da.

Beitrag von „bluebyte“ vom 15. Februar 2023, 06:43

<https://westerndiploma.com>

Server stehen in Arizona/USA

Ich tippe hier mal auf Desinformation-Kampagne.

Beitrag von „griven“ vom 15. Februar 2023, 07:22

Diesmal kam der Bot "mal wieder" aus den USA (die IP löst in den Pool von DigitalOcean auf). Ich bin nach wie vor davon überzeugt das ein Zusammenhang zwischen dem ESXI Hack und der Spam Welle besteht und hier keine gezielte Desinformations Kampagne dahinter steckt sondern es schlicht und ergreifend dämlicher Spam ist den niemand wirklich will und braucht. Die Machart sowie das Thema (Diplom, Abschluss Handel) ist eigentlich ein für Spambots typisches Thema. Was diese Welle von anderen unterscheidet ist die Tatsache das die Bots sehr viel breiter gestreut sind und somit sehr viel schwerer effektiv zu erfassen und zu sperren sind als sonst.

Ziemlich genau vor einem Jahr gab es eine ähnliche Welle nur war es in dem Fall einfach die Bots abzufangen bevor sie wirklich was absondern konnten. Im letzten Jahr wurden zunächst mehrere Accounts in kurzen Abständen von jeweils der gleichen Maschinen aus registriert was dann auf unserer Seite Automatismen ausgelöst hat die dafür gesorgt haben das die Accounts gesperrt wurden bevor irgendwas von denen kam diesmal machen sie das nicht so sondern es kommt pro Maschine immer nur ein Account an. Die Streuung rund um den Globus macht zudem ein effektives Sperren über RBL Listen schwierig denn nach allem was ich bisher beobachtet habe folgt auch das keinem wirklichen Muster und alterniert ständig.

Beitrag von „simon0302010“ vom 15. Februar 2023, 08:13

Könnte man velleicht die Nachrichten abfangen, indem man die, die zu mehr als der Hälfte aus chinesischen Schriftzeichen bestehen... Mehr als die Hälfte Schriftzeichen sollte in einem Deutschen Forum ja nicht oft vorkommen...

Beitrag von „griven“ vom 15. Februar 2023, 08:34

Das mit dem Abfangen von Nachrichten die aus non-ascii Zeichen bestehen ist erst kürzlich mehr als gründlich schief gegangen. Leider ist das so einfach dann doch nicht zumindest nicht im Umfeld unser eingesetzten Software aber natürlich sind wir weiter dran und versuchen hier eine Lösung zu finden die effektiv ist aber diesmal bitte ohne Posts einfach verschwinden zu lassen oO

Beitrag von „Hackintosh-Info.de“ vom 15. Februar 2023, 11:23

[griven](#), haben wir hier Sicherheitsfragen eingebaut bei der Regierung? So wie im WBB oft angewandt wird: <https://www.wolflab.com/commun...bot-anmeldungen/?pageNo=2>

hab zum Glück seit einiger Zeit Ruhe mit Bots, allerdings handelt es sich um Reptilien-Foren und sind in den letzten Jahren eher mau was den Connect betrifft.

Aber vielleicht hilft es..

Beitrag von „apfel-baum“ vom 15. Februar 2023, 16:45

oh, ein reptoidenforum obacht 😊 hihi,

alles gute

lg 😊

Beitrag von „griven“ vom 16. Februar 2023, 07:21

[Hackintosh-Info.de](https://www.hackintosh-info.de) witzig ist ja Tatsache das der Poster drüben bei Wolflab von den selben Bots heimgesucht wird aber das nur am Rande 😊

Sicherheitsfrage habe ich zwischenzeitlich auch probiert der Effekt ist aber gleich null. Es macht keinen Unterschied ob ReCaptcha oder Frage die kommen trotzdem durch. Das Problem bei den Sicherheitsfragen ist das wir diese so wählen müssen das jeder potentiell legitime Nutzer sie auch beantworten kann will meinen die Fragen dürfen nicht zu kompliziert sein und müssen sowohl im deutschen als auch im englischen einen Sinn ergeben. Behält man diese Anforderungen im Hinterkopf schränkt das den Pool möglicher Fragen auf einigermaßen einfach lösbare mathematische Rätsel oder simple Quiz Fragen ein was sie wiederum eben auch für Bots einfach lösbar macht.

Anyway ich habe mich nochmals mit dem filtern von Zeichen beschäftigt und tatsächlich heute morgen die Aktivität des Bots in der Moderation gefunden anstelle vom Forum mit anderen Worten es scheint als hätte ich eine Lösung die so funktioniert wie gedacht. Man wird das jetzt einige Tage beobachten müssen aber wenn niemand Probleme hat beim absenden seiner Posts

und keiner der "altgedienten" User behelligt wird dann kann man damit leben denke ich. Wer weiß wenn ein paar Tage in Folge nichts von dem was die absondern im Forum sichtbar wird vielleicht sind wir dann ja recht bald auch schon nicht mehr interessant für die...

Beitrag von „bluebyte“ vom 17. Februar 2023, 06:07

[griven](#) Desinformations-Kampagne war wohl nicht das richtige Wort.

[griven](#) warum muss die Frage auch auf englisch lösbar sein? Habe es bisher in keinem englischen, französischem oder italienischem Forum erlebt, dass Sicherheitsfragen auch in anderen Sprachen gestellt wurden.

Seit gestern wissen wir ja, wer hinter den Angriffen auf die deutschen Flughäfen steckt.

Auf keinen Fall waren es die Chinesen.

Beitrag von „griven“ vom 17. Februar 2023, 08:22

[bluebyte](#) weil deutsch zwar unsere primäre aber eben nicht die einzige Sprache ist die wir unseren Nutzern anbieten und weil englisch gerade in IT orientieren Foren einfach auch den kleinsten gemeinsamen Nenner darstellt. Das alles spielt aber eigentlich auch gar keine Rolle denn am langen Ende taugen die Sicherheitsfragen als Botabwehr genau so viel oder wenig wie ein ReCaptcha zumindest wenn man sie so wählt das sie nicht zu einer unüberwindbaren Hürde für den durchschnittlichen legitimen User werden.

Ich habe es weiter vorne schon mal gesagt und ich bleibe dabei für mich steht an aller erster Stelle das Maßnahmen die wir ergreifen den regulären Betrieb des Forums so wenig wie möglich belasten und im zuge dessen die Nutzer des Forums so wenig wie möglich, idealerweise gar nicht, einschränken alles andere ordne ich dem unter auch wenn das bedeutet das wir eben ein paar Tage damit leben müssen diesen Kram händisch zu entfernen. Wie es scheint ebbt die Welle aber eh gerade ab und/oder wir sind inzwischen als nicht lohnenswertes Ziel eingestuft worden. Gestern gab es nur einige wenige Posts in der

Moderation und heute gar keine. Wegen meiner kann/darf es gerne so bleiben. Was die Herkunft und die intention der Spamwelle angeht bitte ich davon abzusehen irgendwelche Spekulationen anzustellen denn nur weil der Inhalt aus chinesischen Schriftzeichen besteht heißt das ja noch lange das der Kram auch daher rührt. Am langen Ende ist spam spam egal aus welchen Zeichen er besteht oder welche Intention der Kram hat...

Beitrag von „bluebyte“ vom 18. Februar 2023, 08:47

[griven](#) dein letzter Satz sagt genau das aus, was ich mit meinem Kommentar sagen wollte. Mit Desinformation bzw. Falschinformation meinte ich eher die Verschleierung der Herkunft. Vielleicht habe ich mich da etwas unglücklich ausgedrückt.

Um es so weit wie möglich neutral auszudrücken.

Möglich ist alles. Oftmals sind es Ursachen die man gar nicht in Betracht zieht.