Unerwünschter japanischer Besuch

Beitrag von „Gruenfink“ vom 14. Dezember 2019 18:49

Ich hätte eine Bitte - könnte jemand vom Moderatorenteam die vielen gesperrten Threads, die offenkundig in der Nacht von einem japanischen Bot eröffnet wurden, entfernen?
Immerhin blockieren sie fast eine gesamte Themenseite, und naja, ein bisschen nervig ist der aggressiv-rote Anblick halt auch noch...

Lieben Dank euch! 

Beitrag von „Anja82“ vom 14. Dezember 2019 18:54

Sind das wirklich neue Posts? Hier am Laptop sehe ich nichs japanisches. Auf dem Handy ist bei mir allerdings auch alles auf der Startseite japanisch.

Beitrag von „Wollsocken80“ vom 14. Dezember 2019 18:59

Es ist Koreanisch und nicht Japanisch 

Beitrag von „Gruenfink“ vom 14. Dezember 2019 19:01

Ach herrje... 

Beitrag von „Gruenfink“ vom 14. Dezember 2019 19:03

> Zitat von Anja82
>
> Sind das wirklich neue Posts? Hier am Laptop sehe ich nichs japanisches. Auf dem Handy ist bei mir allerdings auch alles auf der Startseite japanisch.

Es scheinen alle paar Stunden neue hinzuzukommen.
Und ja - die Moderatoren löschen wohl, aber in der Ansicht sind sie halt noch da... 

Beitrag von „Valerianus“ vom 14. Dezember 2019 19:07

Das sind chinesische Schriftzeichen, die kommen in Korea, Japan und China zum Einsatz. Wie kommst du auf koreanisch, Hangul hab ich da nicht gesehen?

Beitrag von „Wollsocken80“ vom 14. Dezember 2019 19:09

Häh? Dich, ich hatte vorhin eine Flut voll Hangul auf dem Bildschirm. Aber vllt ist es jetzt Chinesisch?

Beitrag von „Gruenfink“ vom 14. Dezember 2019 19:17

Dschieses Kraist!
Ich hätte nie gedacht, dass ihr das auch noch lesen könnt! *ehrfürchtiggugg*

Was steht denn da so? 

Beitrag von „chilipaprika“ vom 14. Dezember 2019 19:21

mmm, ich habe eine Menge gelöscht und gesperrt und kann jetzt nichts mehr sehen. Könnt ihr tatsächlich noch Beiträge lesen?

Beitrag von „Valerianus“ vom 14. Dezember 2019 19:24

Seite 2 ist koreanisch, stimmt. 
Bei dem koreanischen geht's glaube ich um Prostitution (das sind nicht die Vokabeln, die ich super gut draufhabe), beim chinesischen geht es um Studienplätze (in den USA wenn ich den englischen Teil dazunehme), vermutlich um Studentenvisa?

Beitrag von „Gruenfink“ vom 14. Dezember 2019 19:26

Aufmachen und lesen kann ich diese Threads nicht mehr.
Aber die Titel (worum auch immer es dabei gehen mag...) stehen halt noch da, wenn ich die Themenliste aufrufe.
Und die sind eben alle rot - und sehr viele.
Deshalb bin ich ja aufmerksam geworden, bei einem einzelnen Thread hätte ich mir wohl nix dabei gedacht.

Beitrag von „Volker_D“ vom 14. Dezember 2019 19:55

Ihr (Webseitenbetreiber) solltet evtl. mal die Logdatein genauer kontrollieren. Bei uns im Forum ging dieser Angriffsversuch letzte Woche auch mit knapp 200 Bots aus China los. Die haben alle Themen abgeklappert und überall versucht zu schreiben (was sie aber bei uns nicht konnten, da sie keine Schreibberechtigung erlangt hatten. Bei uns muss man sich erst "erfolgreich" registrieren, was ein Bot zum Glück (noch) nicht hinbekommt. (Aber leider auch ein paar Menschen nicht, die uns dann (zumindest ab und zu) per Email kontaktieren).
Das perfide (bzw. von euch zu prüfende) ist, dass gleichzeitig ein Rechner aus der Schweiz SQL-Injection Angriffe gemacht hat. Soweit wir das sehen zum Glück auch erfolglos. Wenn das gelungen wäre, dann wäre der Schaden weit größer als nur ein paar Spam-Beiträge.
Daher: Logdatein prüfen und prüfen, ob ihr die neuste Forensoftware nutzt.

Beitrag von „Buntflieger“ vom 14. Dezember 2019 20:51

> Zitat von Volker_D
>
> Ihr (Webseitenbetreiber) solltet evtl. mal die Logdatein genauer kontrollieren. Bei uns im Forum ging dieser Angriffsversuch letzte Woche auch mit knapp 200 Bots aus China los. Die haben alle Themen abgeklappert und überall versucht zu schreiben (was sie aber bei uns nicht konnten, da sie keine Schreibberechtigung erlangt hatten. Bei uns muss man sich erst "erfolgreich" registrieren, was ein Bot zum Glück (noch) nicht hinbekommt. (Aber leider auch ein paar Menschen nicht, die uns dann (zumindest ab und zu) per Email kontaktieren).
> Das perfide (bzw. von euch zu prüfende) ist, dass gleichzeitig ein Rechner aus der Schweiz SQL-Injection Angriffe gemacht hat. Soweit wir das sehen zum Glück auch erfolglos. Wenn das gelungen wäre, dann wäre der Schaden weit größer als nur ein paar Spam-Beiträge.
> Daher: Logdatein prüfen und prüfen, ob ihr die neuste Forensoftware nutzt.

Was mich - als IT-Laien - interessieren würde: Wer organisiert solche Angriffe, wer profitiert davon und was für ein Sinn steckt dahinter? Ist es nur blinde Zerstörungswut von irgendwelchen Möchtegern-Hackern oder evtl. doch noch mehr dahinter? 😲

Beitrag von „Volker_D“ vom 14. Dezember 2019 21:11

Da gibt es viele Gründe. Von Zerstörungswut, "Übungszwecke", sich einen Namen machen, ...

Am gefährlichsten ist folgender Grund:
Solche Foren werden oft nicht professionell überwacht wie bei Google, Facebook, Sparkasse, ...
Schafft man einen Einbruch in die Datenbank eines Forums, dann kann man Namen und E-Mails der Nutzer auslesen. Mit sehr viel Glück auch die unverschlüsselten Passworte. I.d.R. aber oft nur noch die Hashwerte (laienhaft: "verschlüsselte" Passworte). Das gemeine ist, dass mit etwas Aufwand diese Verschlüsselung zu knacken ist ohne das andere es bemerken; weil man das knacken dann auf einen anderen (oder eigenen) Rechner ganz in Ruhe machen kann. (Sprich: Man kann so lange ein Passwort ausprobieren, bis man die abgespeicherten Hash erhält. Damit kennt man dann das Passwort im Klartext. Bei Facebook, Sparkasse, ... könnte man so einen Angriff nicht direkt fahren, da die nicht so viele Millionen Versuche zulassen und vorher sperren würden.)

Der Hacker kann also an Email und Passwort herankommen.
Und jetzt kommt das eigentliche Problem: Viele Leute haben nur eine E-Mail und benutzen auch noch das gleiche Passwort (oder leicht abgeändert) auf anderen Seiten (Amazon, ...). Hat man also so ein "kleine" "Hobbyforum" geknackt, dann ist es ein leichtes diese Daten für größeren finanziellen Schaden zu nutzen. Angefangen von einfachen Bestellungen bis hin zu Erpressung.

Beitrag von „Volker_D“ vom 14. Dezember 2019 21:13

PS: Wer wissen möchte, ob seine E-Mail schon bekannt ist, weil sie (samt Passwort) geknackt wurde, der kann hier fragen:
https://sec.hpi.de/ilc/search?lang=de

Beitrag von „Conni“ vom 14. Dezember 2019 22:02

@Stefan , liest du hier bitte mit?

Beitrag von „Stefan“ vom 15. Dezember 2019 00:39

Ich lese hier mit.
Angriffe ließen sich nicht feststellen.

Die Registrierungen der Bots haben wir immer wieder.
Auch hier muss man sich erfolgreich registrieren. Das bedeutet registrieren, Bot Prüfung bestehen (die leider auch nicht 100%ig sicher ist) und die Emailadresse bestätigen.
Erst dann ist ein Schreiben möglich.

Die nächste Version der Forensoftware, die Ende diesen Jahres/Anfang nächsten Jahres kommen soll (vom Hersteller) soll dann auch mit StopForumSpam verbunden sein (und das auch datenschutzrechtlich abgesichert).
Dann wird es hoffentlich noch etwas weniger Spam geben.

> Zitat von Volker_D
>
> PS: Wer wissen möchte, ob seine E-Mail schon bekannt ist, weil sie (samt Passwort) geknackt wurde, der kann hier fragen:
> sec.hpi.de/ilc/search?lang=de

Diese Prüfung ist durchaus sinnvoll. Dort wird allerdings nicht getestet, ob die E-Mail hier erbeutet wurde, sondern allgemein irgendwo schon auftaucht (von welchen Seite auch immer)

Beitrag von „kleiner gruener frosch“ vom 15. Dezember 2019 01:05

Danke Stefan.

Wobei - dann wird unser Job ja fast langweilig. 

Kl.gr.Frosch

Beitrag von „Volker_D“ vom 15. Dezember 2019 08:25

> Zitat von Stefan
>
> Diese Prüfung ist durchaus sinnvoll. Dort wird allerdings nicht getestet, ob die E-Mail hier erbeutet wurde, sondern allgemein irgendwo schon auftaucht (von welchen Seite auch immer)

Ich sage mal jain.
1) So wichtig ist diese Seite nun wirklich nicht. Da machen die vom Hasso Plattner Institut nicht extra eine Prüfung nur für euch, sondern prüfen natürlich alle bekannten DIebstähle.
2) Die Quelle wird duchaus mit angegeben. Ich habe die meisten meiner E-Mails überprüft. Die meisten von mir sind sauber. Ich tauche aber auch 3 mal auf:
- E-Mail + Passwort bei kickstarter wurden geklaut
- E-Mail + Passwort bei dropbox wurden geklaut
- E-Mail + Passwort von unbekannter Quelle (könnte nicht die von kickstarter oder dropbox sein, da es eine andere E-Mail ist. Passwort wird aus Sicherheitsgründen nicht angezeigt, daher kenne ich nicht die genaue Quelle.)

3) Es sind noch nicht alle Leaks eingearbeitetet. In einem der letzen Sicherheitskurse hatte Herr Prof. Dr. Meinel gesagt, dass sie immer erst die größten Datenbanken einarbeiten und noch fast 1000 kleinere Dankenbanken noch nicht eingetragen sind (Die müssen ja immer einen Konverter schreiben um es in ihre Datenbank einzubinden.)

Beitrag von „Stefan“ vom 15. Dezember 2019 08:42

@Volker_D :
Das ist mir bewusst.
Ich wollte nur vermeiden, dass der Eindruck entsteht man könne dort testen, ob hier von lehrerforen.de der Account geknackt wurde.

Nicht automatisch wenn dort die Email-Adresse auftaucht ist das auf lehreforen.de zurückzuführen.

Aber jedem sollte bewusst sein, dass es 100%ige Sicherheit nicht gibt.

Die Quellen die dort angegeben wurden sind auf jeden Fall hilfreich und man sollte immer mal wieder dort reinschauen.

Beitrag von „Volker_D“ vom 15. Dezember 2019 08:43

Korrektur: Mein dritter Fall kann nicht von dropbox oder kickstarter sein, da es eine andere E-Mail ist. Da einem das Passwort nicht angezeigt wird, kann ich es aufgrund der E-Mail nur auf etwa 20 Quellen eingrenzen.

Beitrag von „Volker_D“ vom 15. Dezember 2019 08:59

Nein, es muss nicht von hier sein. Das wollte ich auch nicht sagen.

Auch die "Besten" können sich nicht gegen alles Schützen. Sie können max sehen, dass die Daten geklaut wurden und dann ihre Nutzer warnen.

hmm...

Wobei es schon sein könnte, dass es von hier geklaut wurde. Da ich ja verschiede E-Mails habe. Die E-Mail, die ich hier im Forum eingegeben habe, habe ich "nur" in 20 Foren benutzt. Sie ist allerdings auch als Bild im Internet zu sehen und sie taucht bei den gestohlenen Passwörtern auf. Dummerweise in der "Collection" von Januar 2019. Sprich: Der Diebstahl kann wesentlich länger her sein. Und der Onliner Spambot von August 2017 (ohne Passwort).

Nur mal so als Frage an alle, die hier im Forum schon wesentlich länger als 1 Jahr sind. Auch betroffen? Und seit wann seit ihr hier im Forum?

Beitrag von „Stefan“ vom 15. Dezember 2019 09:04

Was mich ein wenig erleichtert, ist dass die E-Mail-Adresse des Accounts meiner Frau nicht in der Liste auftaucht. Und sie ist nun wirklich schon lange dabei.

> Zitat
>
> Glückwunsch: Ihre E-Mail-Adresse ********** taucht nicht in unserer Datenbank auf. Das garantiert jedoch nicht, dass keine Ihrer persönlichen Informationen gestohlen wurden.

Beitrag von „Susannea“ vom 15. Dezember 2019 09:39

> Zitat von chilipaprika
>
> mmm, ich habe eine Menge gelöscht und gesperrt und kann jetzt nichts mehr sehen. Könnt ihr tatsächlich noch Beiträge lesen?

In der Mobilen Version alle Titel und wann du sie gelöscht hast. Auf dem PC sind sie gar nicht mehr zu sehen.

Beitrag von „Stefan“ vom 15. Dezember 2019 09:40

> Zitat von Susannea
>
> In der Mobilen Version alle Titel und wann du sie gelöscht hast. Auf dem PC sind sie gar nicht mehr zu sehen.

Das sollte nun für die "normalen" Mitglieder garnicht mehr sichtbar sein.

Beitrag von „Susannea“ vom 15. Dezember 2019 09:51

> Zitat von Stefan
>
> Das sollte nun für die "normalen" Mitglieder garnicht mehr sichtbar sein.

Danke dir

Beitrag von „Gruenfink“ vom 15. Dezember 2019 12:26

Herzlichen Dank - auch bei mir ist jetzt nix mehr zu sehen! 

Beitrag von „Anja82“ vom 15. Dezember 2019 22:17

Da ist wieder einer.

Beitrag von „kleiner gruener frosch“ vom 15. Dezember 2019 22:26

[Erledigt]

kl. gr. frosch

Beitrag von „Bolzbold“ vom 16. Dezember 2019 12:06

Im Moment kommen sowohl asiatische Spammer als auch welche aus dem slawischen Raum. Wir versuchen, sie alle rechtzeitig zu sperren, bevor sie uns zuspammen. Das ist aber gerade nachts schwierig. Morgens findet man dann teils 40 Spam-Accounts, die man alle einzeln sperren muss.

Beitrag von „pepe“ vom 16. Dezember 2019 15:49

Kann man nicht nachts (zur Haupt-Spammerzeit) die Registrierung sperren? Zumindest vorübergehend?