SPAM
Everyone's favorite food

Aviram Jenik

מהו ספאם

- SPAM (אותיות גדולות) הוא סוג של בשר
- spam (אותיות קטנות) הוא שליחת דוא"ל ללא רשות המקבל (unsolicited)

ההסבר המלא נמצא ב:
http://www.spam.com/ci/ci_in.htm

- לפי ההערכות כ- 40% מהדוא"ל באינטרנט הוא ספאם
- AOL חוסמת 780 מיליון הודעות ספאם ביום
- כמות הספאם גדלה פי 5(!) בשנה וחצי האחרונות

מאיפה הוא מגיע?

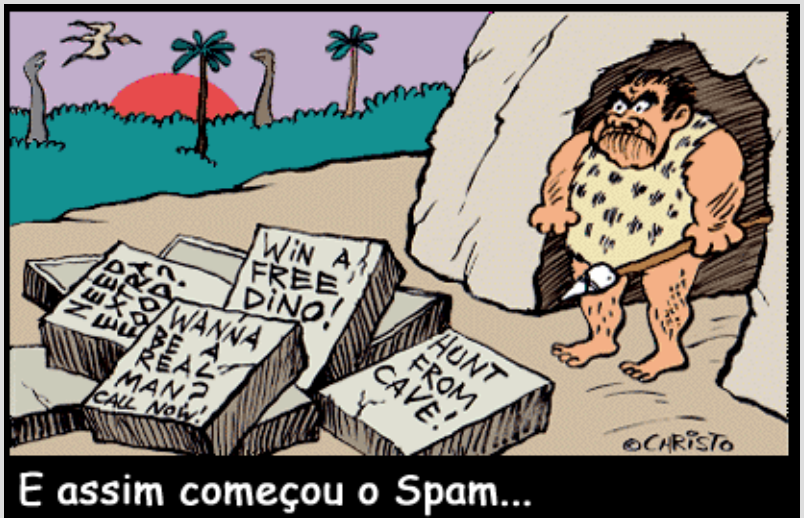
- אתרי web
- newsgroups
- chat rooms
- ICQ
- מיחזור כתובות: ניתן לקנות רשימה עם מיליון כתובות ב- 19.95$
- ניחוש שמות: aviram@netvision, aviram@bezeqint, aviram@aol..
- התקפות מילון: asmith@acme, bsmith@acme, csmith@acme..

במקרה אחד תועדה התקפה של 4 נסיונות בשניה במשך 5 חודשים רצופים על hotmail

למה הוא ממשיך להגיע?

בדר"כ הספאם "מתחזק" אם כתובתכם אומתה:

- web-bugs
- "unsubscribe"
- out-of-office reply
- spyware



כלכלת ספאם

מי מרוויח?

- אחוז העונים לספאם הוא כ- 0.005%, כלומר 50 תשובות ("לידים") ב- 20$
- חלק מהספאם (העוקץ הניגרי) ריווחי מאוד

מי מפסיד?

- בהנחה שכל עובד מבזבז 4.4 שניות על כל הודעה, ארה"ב מפסידה 8.9 מיליארד דולר בשנה על ספאם (עלות ישירה!)

איך נלחמים

התנהגות חכמה:

- לא לאפשר web bugs (כל תוכנות הלינוקס, outlook 2003)
- לא לענות לספאם (אף פעם!)
- תוכנות לפילטור ספאם: בצד השרת + בצד הלקוח

החדשות הטובות: אני אלמד אתכם איך מפלטרים 96.2% מהספאם בצורה אוטומטית

חושבים שמצבכם גרוע?...

- מתוך 16,000 מיילים בחודש, 11,800 הם דוא"ז (74%)
- כתובת פיקטיבית ששתלנו באתר (בתוך קוד ה-HTML) קיבל ספאם אחרי 4 ימים ושעתיים

למה קשה לנו לפלטר:

- אסור false positives (לקוחות...)
- תמיכה בכל השפות (לקוחות...)
- הרבה מהדואר שאנו מקבלים הוא "חצי-עוין"
- אסור שתהיה הפרעה לצורה בה מותקן השרת
- zero maintenance מצד השרת

spam assassin

- SA נותן ניקוד חיובי (=ספאם) לפי סט ארוך של מבחנים לדוא"ל:
  - yelling
  - click-to-remove
  - unknown mailer
  - penis enlarge
  - וכו'. רשימה מלאה ב:
    http://www.spamassassin.org/tests.html
- כמו כן, יש ניקוד שלילי (=לא ספאם) לדברים "אנושיים"
- אם הסה"כ עובר את ה- threshhold, הדוא"ל נזרק
- כמו כן, האינפורמציה שאסף SA נמצאת ב- header, ומאפשרת לפלטר עוד בצד הלקוח (למשל, השרת יזרוק ניקוד מעל 5, והלקוח יזרוק מעל 3)

התקנת SA

- apt-get install spamassassin
- או למאותגרים:
  - הורידו את ה-tar מ- http://spamassassin.org/

```
[unzip/untar the archive]
cd Mail-SpamAssassin-*
perl Makefile.PL
make
make install                    [as root]
```

- לעבודה עם procmail, qmail וכן הלאה, חפשו בגוגל
- השקף הבא יסביר איך להתקין ללא לשנות את תוכנת הדואר בצד השרת
- אבל קודם, סיפורים מהחזית...

SA + fetchmail

- שרת הדואר לא בשליטתכם?
- רוצים להתקין SA בלי לשנות את הגדרות הדואר?
- מחפשים להתנסות בלי התחייבות?

בבקשה:

1. התקינו על המחשב שלכם procmail ו- fetchmail
2. הגדירו בשרת הדואר וגם אצלכם, את התיבות aviram ו- aviramspam
3. הגדירו את fetchmail שימשוך דואר מהשרת ויעביר אותו דרך procmail: (הטקסט הבא לקוח מ- ~/.fetchmailrc)

```
set daemon 1
set syslog
defaults proto pop3, timeout 30, fetchall, forcecr, mda "/usr/bin/procmail"
poll example.com interval 1 user "aviramspam" pass "secret"
```

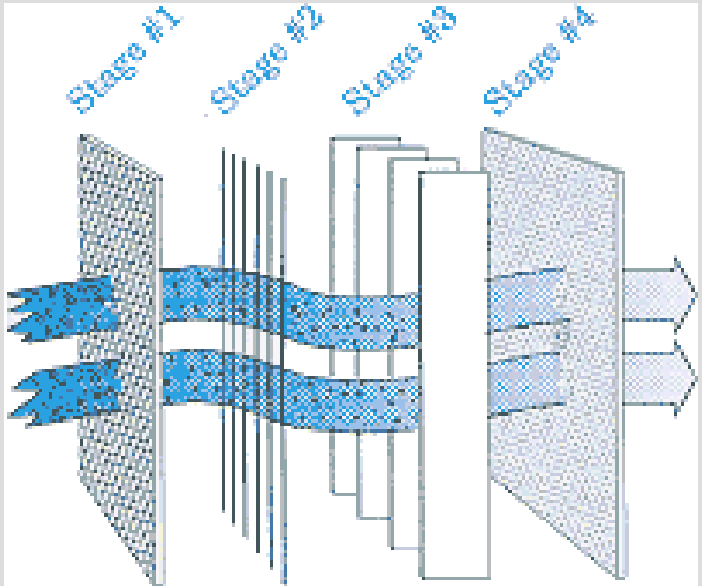
המשך...

בשלב זה ברגע שתעשו login, תוכנת fetchmail תביא את כל הדואר מ- aviramspam ל- aviramspam המקומי, כל דקה, ותעביר אותו דרך procmail. עכשיו נשאר רק להגדיר את procmail: (הטקסט הבא לקוח מ- procmailrc./~)

```
PATH=/bin:/usr/bin:/usr/local/bin
MAILDIR=$HOME/mail
DEFAULT=inbox/
LOGFILE=$MAILDIR/logfile


:0fw
| /usr/bin/spamassassin -L


:0
* ^X-Spam-Status: Yes
spam/


:0
! your-spamfree-mailbox@example.com
```

הערות

- כמובן ש- yourspamfreemailbox מנותב לתיבה האמיתית
- השלב האחרון לא הכרחי: אני פשוט אוהב למשוך דואר משרת הדואר :-)
- אצלנו SA חוסם 51% מהדואר, כזבל ברמה 5. עד עתה לא היו false positives כלל.
- 51% לא מספיק? פלטרו בצד הלקוח



spamoracle

- spamoracle מבוסס על תיאוריה בשם bayesian:
  http://www.paulgraham.com/spam.html
- הרעיון הכללי: למדו אותו מה זה "דואר טוב" ומה זה "ספאם"
- בונוסים: תופס גם וירוסים...
- איך מתקינים? apt-get install spamoracle (חפשו את המקבילה שלכם)
- איך מגדירים? בשקף הבא...

הגדרת spamoracle

- צרו 2 תיקיות: מלאו אחת ב(לפחות) 1500 הודעות "טובות" ואת השניה ב- 500 הודעות ספאם (אצלי היחס היה 5000 / 1500)
- הוסיפו את התיקיות ל-SO:

```
find archives -type f -print | xargs spamoracle add -good
find spam -type f -print | xargs spamoracle add -spam
```

- הדוגמה מתייחסת ל- maildir, חפשו ב- man פתרונות למקרה שלכם
- עכשיו תגדירו את 2 החוקים הבאים בלקוח הדואר:

```
remove header X-Spam
remove header X-Attachments
pipe through spamoracle mark
```

-ו

```
Filter criteria: match all of the following rules
X-Spam contain yes;
Filter action:
remove header X-Spam
remove header X-Attachments
move to folder spam
mark as unread
```

הערות

- שימו לב שהחוק הראשון צריך לרוץ תמיד, לא לעצור אחריו!
- החוק השני הוא זה שמבצע את פעולת הסינון עצמה
- כדי לחסוך זמן, שימו את 2 החוקים בסוף רשימת החוקים (אחרי המיון האוטומטי)
- אפשר גם להוסיף חוק ל- spamassassin שמחפש, למשל:
  X-Spam-Level: ***

אימון זה הכל בחיים. שימו ב- cron:

```
spamoracle add -v -good Mail/.Spam.directory/NonSpam -spam
    Mail/.Spam.directory/MissedSpam
```

- אחרי שבוע אימון הגעתי ל- 3.8% ספאם סה"כ ב- inbox
- בתקופה של 5 חודשים היו לי לא יותר מ- 3 מכתבים שסומנו כ-"ספאם" בטעות (כולם בעברית)

don't get mad, get even

- :form fucker

http://groups.google.com/groups?selm=33da4940.0305231034.5565d17%40posting.google.com

- עוקץ ניגרי: הנקמה המתוקה
- /http://www.419eater.com
- /http://www.ebolamonkeyman.com

תודה!

שאלות?

aviram@beyondsecurity.com