ΚΕΦΑΛΑΙΟ 7
ΠΟΛΕΜΩΝΤΑΣ ΤΟ SPAM

Λίγα λόγια για το spam

Αμέτρητος είναι ο όγκος του spam email που καθημερινά γεμίζει τα mailboxes των χρηστών του internet. Το spam email είναι ίσως η μεγαλύτερη ενόχληση που δέχεται ένας χρήστης, μαζί με τα διαφημιστικά ad-ons που μπαίνουν στις ιστοσελίδες και φυσικά τις επιθέσεις από worms. Σε πολλές περιπτώσεις τα spam email γεμίζουν το mailbox και ο λογαριασμός του χρήστη αχρειστεύεται, μέχρι να σβήσει το spam.

Η προώθηση του όγκου του spam καθυστερεί τους mail servers να δεχτούν και να στείλουν τα νόμιμα email και πολλές φορές προκαλεί προβλήματα. Επιπλέον, ο χρόνος που σπαταλάει ένας χρήστης για να σβήνει καθημερινά τα spam email δεν είναι καθόλου αμελητέος.

Οι spammers πληρώνονται για να προωθούν το spam email, για το λόγο αυτό το στέλνουν σε τεράστιες ποσότητες. Συνήθως είναι διαφημιστικού περιεχομένου, ή φάρσες, είτε πρόκειται για phishing. Το τελευταίο είναι η πιο επικίνδυνη μορφή spam.

Τι είναι το phishing

Το phishing είναι η πρακτική όπου στέλνονται ψεύτικα emails και spam τα οποία είναι γραμμένα σαν να προέρχονται από τράπεζες ή άλλους ευυπόληπτους οργανισμούς, με την πρόθεση να αποσπάσουν από τους παραλήπτες usernames, κωδικους, λογαριασμούς τραπεζών, ATM pins, πληροφορίες για πιστωτικές κάρτες και άλλο ευαίσθητο υλικό [1].
Το anti-phishing working group [2] περιέχει αρχείο με τα περισσότερα phishing emails που έχουν σταλεί [3] πολλά από τα οποία δείχνουν ιδιαίτερα πειστικά και πάρα πολλοί χρήστες έχουν πέσει θύματα.

Πώς δουλεύουν οι spammers

Η δουλειά των spammers χωρίζεται σε διαφορετικές κατηγορίες:

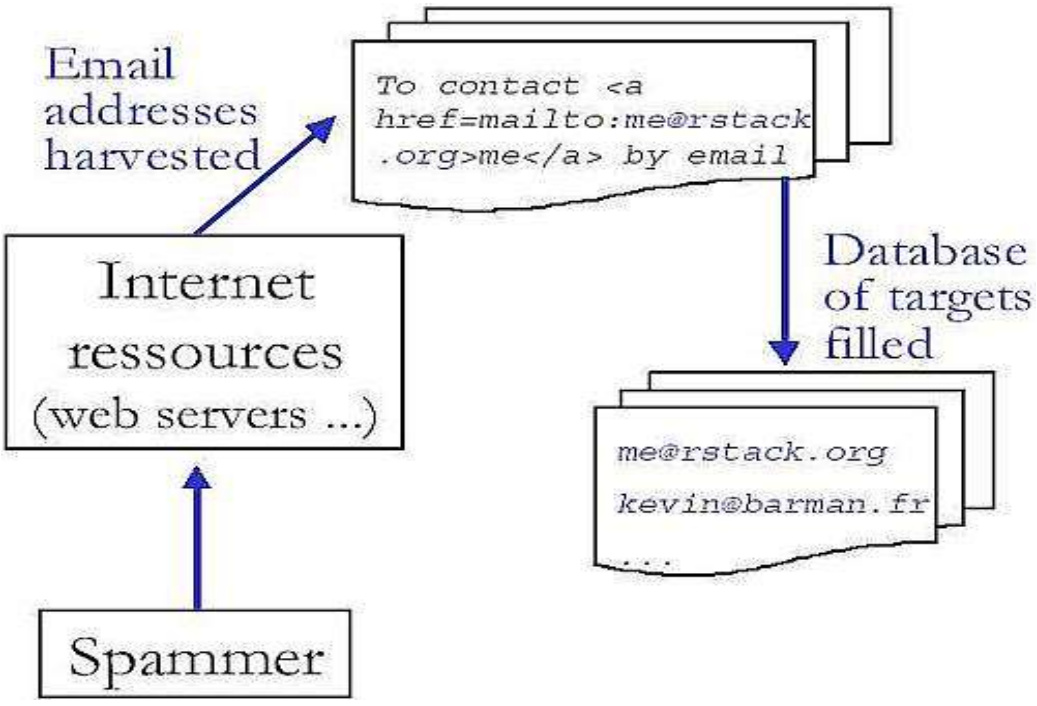
Harvest: βρίσκουν έγκυρες email διευθύνσεις και φτιάχνουν βάσεις δεδομένων με τους στόχους.
Εύρεση open proxies: μέσω αυτών στέλνουν τα email και παραμένουν ανώνυμοι.
Εύρεση open mail relay servers: ώστε να μπορούν να στέλνουν τα email, μέσω των open relay servers που τα προωθούν παντού.

Για να αποσπάσουν έγκυρες email διευθύνσεις οι spammers συνεργάζονται με διάφορα άτομα που κάνουν αυτή τη δουλειά. Μάλιστα, στο internet χρησιμοποιείται ο όρος spaker, για να περιγράψει τους hacker οι οποίοι κάνουν hacking ώστε να προμηθεύσουν τους spammers με έγκυρες διευθύνσεις, επι πληρωμής φυσικά. Ο όρος spaker είναι πολύ απαξιωτικός και τα άτομα που κάνουν αυτή τη δουλειά δεν το περηφανεύονται.

Οι spakers εισβάλουν σε e-commerce web sites και γενικά σε ιστοσελίδες οι οποίες περιέχουν βάσεις δεδομένων με πολλές χιλιάδες ή και εκατομμύρια άτομα ανα τον κόσμο που έχουν κάνει αγορές. Όσο πιο συγκεκριμένο είναι το target group που θα αποσπάσει ο spaker τόσο καλύτερη θα είναι και η αμοιβή του.

Εκτός όμως απο εμπορικά sites, οι spammers βρίσκουν έγκυρες email διευθύνσεις σε πολλά σημεία στο internet-public lists, forums, κοινότητες όπως τα hotmail.com, aol.com κα.

Μια ακόμα τεχνική για να αποσπάσουν email διευθύνσεις βασίζεται σε προγράμματα που ψάχνουν ιστοσελίδες στο internet και ελέγχουν για τη σύνταξη mailto:username@site.com. Όταν βρίσκουν τη σύνταξη αυτή, αποθηκεύουν τη διεύθυνση email και η αναζήτηση συνεχίζεται. Σαν προστασία σε αυτή την τεχνική προτείνεται να μην υπάρχει πουθενά email με την παραπάνω σύνταξη, αλλά να γράφεται mailto: username at site dot com. Βέβαια τα πιο προχωρημένα εργαλεία για αναζήτηση μπορούν να το καταλάβουν αυτό. Το google.com, η μεγαλύτερη μηχανή αναζήτησης στο internet είναι σύμμαχος για τους spammers και συνήθως τα προγράμματα που χρησιμοποιούν για αναζήτηση email βρίσκουν τις ιστοσελίδες μέσα απο το google.

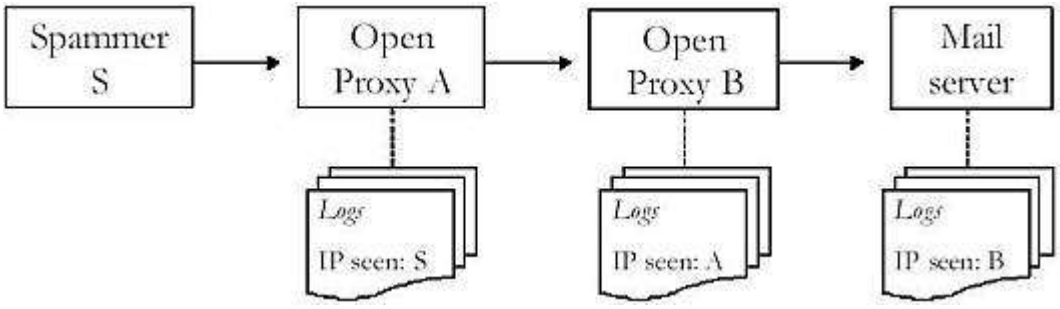


Χρήση open proxies

Οι spammers μπορούν είτε να συνδεθούν απευθείας στον απομακρυσμένο mail relay server που θα στείλει το spam τους, είτε να συνδεθούν μέσω open proxies και έτσι να μην μπορούν να εντοπιστούν εύκολα, πετυχαίνοντας να μένουν συνέχεια ανώνυμοι. Ένας open proxy είναι μια υπηρεσία ανοικτή στον κόσμο που προωθεί οποιαδήποτε σχεδόν αίτηση, επιτρέποντας έτσι σε κάποιον να παραμένει ανώνυμος. Οι proxy servers χρησιμοποιούνται ιδιαίτερα από τους spammers και γενικότερα από το internet undergroung. Συνήθως οι spammers θα χρησιμοποιήσουν περισσότερους από ένα proxy servers για να καλύψουν τα ίχνη τους. Όσο περισσότερα ενδιάμεσα σημεία υπάρχουν, τόσο πιο δύσκολη θα είναι η ανίχνευσή τους. Οι spammers φοβούνται την πιθανότητα να εντοπιστούν, καθώς ξέρουν οτι οι δραστηριότητες τους είναι παράνομες και μπορούν να καταδικαστούν σε μεγάλα πρόστιμα και ποινές [4]. Όσο πιο μεγάλη είναι η αλυσίδα των proxies στους οποίους συνδέονται τόσο καλύτερη ανωνυμία θα έχουν, αν και η ταχύτητα μειώνεται, αφού τα δεδομένα ταξιδεύουν περισσότερο.

Εικόνα 7.2 -relaying ανάμεσα σε proxy servers για να μην είναι εύκολος ο εντοπισμός του spammer

Χρήση open relays



Οι open relays είναι mail transfer agents (MTA's) που δέχονται να προωθήσουν email μηνύματα ακόμα και αν δεν προορίζονται για το δικό τους domain. Οι spammers χρησιμοποιούν open relays για να προωθήσουν τα email τους σε οποιαδήποτε διεύθυνση θέλουν. Οι MTA's είναι συνήθως mail servers που έχουν ρυθμιστεί λάθος, γι'αυτό και επιτρέπουν την προώθηση μηνυμάτων από οποιονδήποτε host επικοινωνεί.

Τρόποι αντιμετώπισης spam

1 Οι τεχνολογίες φίλτρων που έχουν αναπτυχθεί, οι οποίες χρησιμοποιούν διάφορες τεχνικές ώστε να αναγνωρίσουν σωστά το spam email και να μην φτάσει στο mailbox μας. Μια από τις πιο αξιόπιστες εφαρμογές που είναι υπεύθυνες για το μπλοκάρισμα των spam email είναι το spamassasin [5].
Ένας άλλος τρόπος για να σταματήσουμε το spam email απο το να σταλεί είναι η δημιουργία

ψεύτικων mail servers που στον spammer φαίνονται σαν open mail relay servers, αλλά φυσικά δεν προωθούν τα μηνύματα. Ο spammer συνδέεται με τον ψεύτικο mail server, στέλνει τα email, τα οποία δεν προωθούνται από τον relay server.

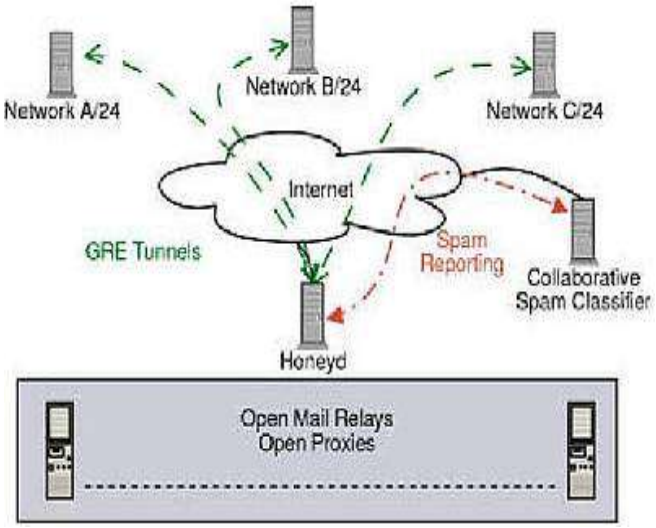
Το σενάριο μπορεί να πραγματοποιηθεί εύκολα με κάποιον mail server, ο οποίος ρυθμίζεται να μοιάζει οτι δέχεται την προώθηση μηνυμάτων, αλλά στην ουσία αποθηκεύει τα email χωρίς να τα στέλνει.

Μια παρόμοια λύση που προτείνεται είναι η δημιουργία ενός ψεύτικου mail server που προσομοιώνει το sendmail, το οποίο ξεγελά τον spammer χωρίς να προωθεί το spam. Η εφαρμογή που πραγματοποιεί το σενάριο είναι το spamd [6], φτιαγμένο για το λειτουργικό σύστημα OpenBSD, και σε συνδυασμό με το pf, το packet filter/firewall του OpenBSD καταναλώνει πόρους και χρόνο από τον spammer, χωρίς να προωθεί το spam [7].

Το honeyd μπορεί να χρησιμοποιηθεί σαν εργαλείο για την καταπολέμηση του spam. Δημιουργούμε ψεύτικους open mail relay servers και καταγράφουμε τις ip's των spammers που επικοινωνούν μαζί μας, ώστε να ενημερώσουμε κάποια black list. Επίσης δεχόμαστε τα spam email χωρίς φυσικά να προωθούνται.

Honeyd vs spammers

Το honeyd μπορεί να χρησιμοποιηθεί για να καταλάβουμε πώς λειτουργούν οι spammers, να τους κάνουμε να σπαταλήσουν χρόνο και πόρους και τελικά να ενημερώσουμε κάποιες black lists. Η αρχιτεκτονική που προτείνει ο δημιουργός του honeyd είναι η εξής [8]: Δημιουργούμε διάφορα δίκτυα με virtual hosts που περιέχουν open proxies και open mail relays. Με τη χρήση GRE tunneling που παρέχει το honeyd κατευθύνουμε την κίνηση που δέχονται σε κάποιο κεντρικό host και ο οποίος λειτουργεί σαν παγίδα για spam, στον οποίο προωθείται όλη η δραστηριότητα των spammers και το spam email. Αυτός ο host αναλαμβάνει να στείλει το συγκεντρωμένο spam σε κάποιο διεθνές φίλτρο spam. Ο συγγραφέας του honeyd υποστηρίζει οτι η παραπάνω αρχιτεκτονική μέχρι στιγμής έχει δεχτεί πάνω από 6 εκατομμύρια email απο περισσότερες από 1500 διευθύνσεις.



Εικόνα 7.3-κατανεμημένη αρχιτεκτονική για συλλογή spam από έναν κεντρικό server

Δημιουργία open proxies

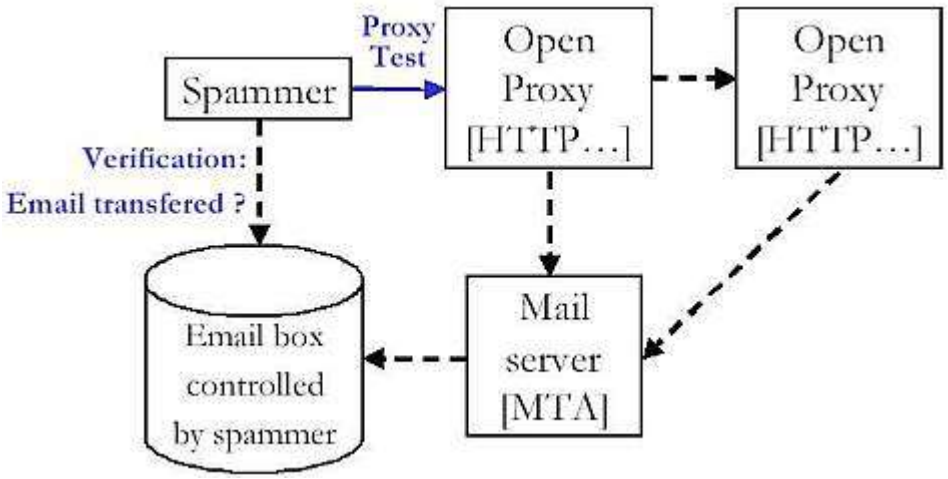
Με το honeyd είναι πολύ εύκολο να δημιουργήσουμε open proxies. Η ρύθμιση

```
create relay

set relay personality "OpenBSD 2.9-stable"

add relay tcp port 3128 "sh /usr/local/share/honeyd/scripts/squid.sh $ipsrc $sport $ipdst $dport"
add relay tcp port 8080 "sh /usr/local/share/honeyd/scripts/proxy.sh $ipsrc $sport $ipdst $dport" set
relay default tcp action block
set relay default udp action block

bind xxx.xxx.xxx.xxx relay
```

δημιουργεί έναν OpenBSD 2.9 virtual host με υπηρεσίες που προσομειώνουν τον squid proxy server που τρέχει στην 3128 και τον web proxy που τρέχει στην 8080.

Για να ξεγελαστεί ο spammer και να νομίζει ότι πρόκειται για πραγματικό open proxy server πρέπει να προσομειωθεί μέρος της συνόδου που θα είχε με έναν πραγματικό open proxy server. Αυτό το πραγματοποιούμε σε συνδυασμό με το Bubblegum Proxypot [9]. Το proxypot προσπαθεί να ξεγελάσει τον spammer και να τον πείσει ότι ο relay server είναι ανοικτός και προωθεί τα email. Για να το πετύχει αυτό, συνδέεται με τον mail server στον οποίο απευθύνεται το spam και διαβάζει το banner του, για να πάρει πληροφορίες.

Συνήθως όταν ένας spammer συνδέεται με κάποιον open proxy server προσπαθεί να δει αν ο proxy server δέχεται πραγματικά συνδέσεις και τις προωθεί και γι'αυτό στέλνει ένα δοκιμαστικό email σε κάποια δικιά του διεύθυνση ώστε να σιγουρευτεί οτι θα φτάσει. Γι'αυτό το proxypot προωθεί το πρώτο email ώστε ο spammer να ξεγελαστεί και να στείλει όλο το spam.



Εικόνα 7.4-ο spammer ελέγχει αν ο proxy server προωθεί τα email

Πείραμα

Στο πείραμα που διεξάγομε δημιουργήσαμε έναν open relay virtual server ο οποίος έτρεχε μια προσομοίωση του sendmail, που απλά δέχεται τα email, χωρίς να τα προωθεί. Δεχτήκαμε συνδέσεις από 35 διαφορετικές ip's και κυρίως από τα δίκτυα 222.101.92, 61.84.140, 222.120.41, τα οποία βρίσκονται στην Σεουλ, στη Νότια Κορέα. Η δουλειά πάντως που κάνει το honeyd σε συνδυασμό με το Proxypot Bubblegum είναι σίγουρα πολύ πιο ενδιαφέρουσα.

markos@amorgos # cat 61/80/47/242/d0/1
Return-Path: <smtphunter21@yahoo.co.kr>
Received: from 143.xxx.xxx.96 ([61.80.47.242])
by edunet-cas7 (Postfix) with ESMTP id
0041244B7B for <smtphunter00@daum.net>; Sat,
26 Feb 2005 05:22:10 +0200 (EET)
Received: from [8.210.195.198] by 143.xxx.xxx.96
with ESMTP id 3CB96C1A75B; Sat, 26 Feb 2005
09:12:31 +0400 Message-ID:
<b$z1$20fd5em8$01d3cr@8q6iw48e> From: ""
<smtphunter21@yahoo.co.kr> To:

<smtphunter00@daum.net> Subject:
BC_143.xxx.xxx.96 Date: Sat, 26 Feb 05 09:12:31
GMT MIME-Version: 1.0 Content-Type:
multipart/alternative;
boundary="----
=_NextPart_000_000D_01C2CC60.49F4EC70"

Το παραπάνω είναι ένα από τα email που δεχτήκαμε. Ο spammer δοκιμάζει να δει αν θα σταλεί το email του στη διεύθυνση smtphunter21@daum.net, μέσω του 8.210.195.198 ο οποίος είτε είναι open mail relay server είτε κάποιο μηχάνημα υπό την κατοχή του spammer.

Συμπεράσματα

Η έρευνα πάνω στην αντιμετώπιση του spam είναι σίγουρο οτι πρέπει να εντατικοποιηθεί, καθώς ολοένα και περισσότερα άχρηστα email καταφθάνουν στα mailboxes των χρηστών, ενώ οι spammers συνεχώς βελτιώνουν τα εργαλεία και τις τεχνικές τους. Το πρόβλημα εντείνεται και από worms που κυκλοφορούν κατά καιρούς και εκμεταλλεύονται τρύπες στα λειτουργικά συστήματα της microsoft για να εγκαταστήσουν smtp proxies για αποστολή spam [10].

Ένα όπλο για την αντιμετώπιση του spam είναι και το honeyd. Με τη δημιουργία ψεύτικων virtual open proxies και open mail relays μπορούμε να μπερδέψουμε τους spammers και να εντοπίσουμε από που συνδέονται, να τους καθυστερήσουμε και τελικά να κρατήσουμε το spam email τους, το οποίο φυσικά δεν θα σταλεί.

ΣΗΜΕΙΩΣΕΙΣ - ΠΑΡΑΠΟΜΠΕΣ

[1] Άρθρο από το honeynet project πάνω στο phishing
www.honeynet.org/papers/phishing

[2] Η σελίδα του anti-phishing working group www.antiphishing.org

[3] Αρχείο με phishing email που έχουν σταλεί
www.antiphishing.org/phishing_archive.html

[4] http://msnbc.msn.com/id/6337242/

[5] http://spamassassin.apache.org

[6] Spam daemon from OpenBSD, http://www.openbsd.org/cgi-bin/man.cgi?query=spamd

[7] Daniel Hartmeier, Annoying spammers with pf and spamd
http://www.benzedrine.cx/relaydb.html

[8] Honeyd research about spam, provos
http://www.honeyd.org/spam.php

[9] Proxypot, a fake proxy daemon to fool spammers
http://world.std.com/~pacman/proxypot.html

[10] Norton Antivirus, Hogle Backdoor
http://securityresponse.symantec.com/avcenter/venc/data/backdoor.hogle.html