The Game Goes On:
An Analysis of Modern Spam Techniques

Ross Thomas, Dmitry Samosseiko, SophosLabs
Virus Bulletin, Montréal, October 2006
About...

Spam tricks (2006)

vs

Filters fighting back
Most games have playing fields...
...and strategies

- Connection-level
- Content analysis
Filter “textbook” strategies

- Connection-level
  - Tracking spam sending networks/hosts (IP/domain blocking)
- Content
  - Checksums
  - Keywords heuristic
  - Call-to-action blocking (URLs, phone number, etc.)
  - Statistical analysis (Bayes, etc.)
  - etc.
Classic spam tricks

• Connection-level
  • “Botnets”
  • Open relays
  • Exploited servers, PHP scripts, etc.
  • Exploited web mail systems

• Content
  • Content randomizations
  • URL rotation
  • Obfuscations
Connection
Nigerian scammers
Exploiting web sites
Not limited to “hacking”

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
Result

I have a new email address!

You can now email me at: greenwatt1010@yahoo.com

Send reply to: greenwatt@terra.com.mx

DEAR FRIEND

I WAS NOT BORN WITH THE PROVERBIAL SILVER SPOON, AND YEARS OF POVERTY AND HUNGER PROVIDED ME A PLATFORM TO STRIVE TO SUCCEED IN

LIFE AND THIS I MUST CONFESS I DID, ALL THE WAY TO THE TOP. IN DOING
URL blocking

• SophosLabs’ own URL list blocks up to 90% of spam
• Public services like SURBL work very well
URL tricks

• Using free web hosting sites as redirectors
• URL shortening services
• Blogs
Dear Sir,

Still paying too much for your current mortgage?

Great News, You are Pre-qualified for the lowest rates. Our loan department is trying to reach you One Last Time since previous attempts to contact you all failed.

You qualify for up to $640,000 for a monthly pmt as low as $550
Save up to 40% off current payment, guaranteed!

Please complete this final step upon receiving this notice immediately, and submit your application now:

http://it.geocities.com/Lawrence64_c562

Warm regards,
Emil Villanueva
<SCRIPT language="JavaScript">
function reportSpam()
{
    alert('Thank you for your report
    We will look further into it');
}
function continueToSite()
{
    window.location.href="http://www4.coreagoussss.com";
}

</SCRIPT>
<body bgcolor="FFFFF0" onLoad=continueToSite()>
Lowest Mortgage Quotes

One short Form will get you the Lowest Rates In America.

First Name: [Input]
Last Name: [Input]
Address: [Input]
City: [Input]
State: [Select]
Zip: [Input]
Email: [Input]
Home Phone: [Input]
Work Phone: [Input] Ext.
Best Time To Contact: [Input] Please Choose
How Would You Rate Your Credit: [Select]
Type of Loan Desired: [Select]
Loan Amount Desired: [Select]
Estimated Property Value: [Select]
Type of Property: [Select]
Approximate 1st Mortgage Balance: [Select]
Approximate 1st Mortgage Interest Rate: [Select]
Interest Rate Type: [Select]

SUBMIT MY REQUEST

*After you have completed this expression of interest form please email your information will be e-mailed to our database.*
Blocking over 2,000 new URLs per day hosted on various geocities.com domains alone
• Not limited to Geocities services, but they are the major target (from 5-15% of all spam)
• Most likely the CAPTCHA tests for Yahoo! IDs have been compromised
Blog abuse

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
URL shortening services

- Up to 20 new URL services discovered every day

Are you still paying too much for your mortgage?
You have been approved for a loan of up to $258,000 for $637 per month.
Visit website to complete your application:
http://myurl.com.tw/ba26
Lowest Mortgage Quotes

One short Form will get you
the Lowest Rates In America.

First Name: [Input]
Last Name: [Input]
Address: [Input]
City: [Input]
State: Select
Zip: [Input]
Email: [Input]

How Would You Rate Your Credit:
- Select
Type of Loan Desired:
- Select
Loan Amount Desired:
- Select
Estimated Property Value:
- Select
Type of Property:
- Select
Approximate 1st Mortgage Balance:
- Select
Approximate 1st Mortgage Interest Rate:
- Select
Interest Rate Type:
- Select

Best Time To Contact: Please Choose

Submit My Request
Proactive URL blocking
Proactive URL blocking

Blocked:

<table>
<thead>
<tr>
<th>date</th>
<th>user</th>
<th>entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006/04/15</td>
<td>unicon</td>
<td>salips.com</td>
</tr>
</tbody>
</table>

Spammed:

<table>
<thead>
<tr>
<th>date</th>
<th>subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006/04/17</td>
<td>Do you know why Katherine the do</td>
</tr>
<tr>
<td>2006/04/17</td>
<td>Advanced Gain Pro consists of</td>
</tr>
<tr>
<td>2006/04/17</td>
<td>Advanced Gain Pro Penis Enlarger</td>
</tr>
<tr>
<td>2006/04/17</td>
<td>Do you know why Katherine the do</td>
</tr>
<tr>
<td>2006/04/17</td>
<td>Be 9 inches with Advanced Gain Pro Penis</td>
</tr>
<tr>
<td>2006/04/17</td>
<td>Advanced Gain Pro Penis Enlarger</td>
</tr>
<tr>
<td>2006/04/17</td>
<td>Advanced Gain Pro not only r</td>
</tr>
<tr>
<td>2006/04/17</td>
<td>Advanced Gain Pro Penis Enlarger</td>
</tr>
<tr>
<td>2006/04/17</td>
<td>Advanced Gain Pro Penis Enlarger</td>
</tr>
<tr>
<td>2006/04/17</td>
<td>Tired of useless exercises for</td>
</tr>
<tr>
<td>2006/04/17</td>
<td>Tired of useless exercises for</td>
</tr>
<tr>
<td>2006/04/17</td>
<td>Tired of useless exercises for</td>
</tr>
</tbody>
</table>
And spammers respond…

With “0-minute” domains

fyefga.org

- Registered at 1:28 AM on February 16 2006
- First seen on spam traps at 1:30 AM
The best way to defeat URL blocking is...

...not using URLs at all
instead…

• Phone numbers
• Fax
• VoIP
• IM (ICQ/AIM/…)
• E-mail addresses
• Stock symbols for “pump-n-dump” scams
Spam Resume

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
Fax + phishing = **Phaxing**

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
AFFIDAVIT OF UNAUTHORIZED USE OF MY PAYPAL ACCOUNT

Please complete this form and Fax it to: 1(800) 410-3595

This affidavit concerns my PayPal Account under the name of: _______________________________ and
my address: (Indicate your Email address originally on your PayPal Account) _______________________________
word: __________________________. I reside at ______________________________, in the City of ____________
________________________, with zip ______________. and the state of ___________________________ Daytime phone
________________________ Evening phone number __________________________

Here your credit card details used in your PayPal account:

3  5  8  2  9  3  1  1
1  0  1  1  1
1  0  1  0  1
0  1  0  1  1
1  0  1  1  1
0  1  0  1  1
Name from the credit card:__________________________________________
Number of the credit card:_________________________________________
Credit card type:_________________
Expiration date:_____/_______
Cvv2:_______
Pin*:______
SSN*:______-_____-_______
Bank name :_____________________________________________________
Bank Routing Number :_________________________
Bank Account number :______________________
Remember:

- Never give out your personal information via email
- Hover over links in email messages to see where they really go
- Login to important websites by typing the address in your web browser

accounts thoroughly, and may refer this information to appropriate law enforcement agencies. I agree to cooperate in any prosecution of individuals charged with fraudulent or Unauthorized Usage of my PayPal account, and I understand that any false declaration of Unauthorized Usage of My PayPal Account will result in immediate termination from further use of PayPal, and may be punishable under Civil or Criminal Law.

_____________________________________________________
Primary Accountholder Signature

PayPal Investigations
Affidavit of Unauthorized Use of a PayPal Account
P.O. Box 45950
Omaha, NE 68145
Vishing

Account Verification

Dear [Email Address],

You have received this email because we have strong reason to believe that your PayPal account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

If your Credit/Debit Card on file is not updated within the next 48 hours, then will assume this account is fraudulent and will be suspended. We apologise for this inconvenience, but the purpose of this verification is to ensure that your PayPal account has not fraudulently used and to combat fraud attempts.

To speed up the process, you are required to call us (1-805-214-4801) to verify your PayPal account.

We apologise in advance for any inconvenience this may cause you and we would like to thank you for cooperation as we review this matter.

Regards,
PayPal Account Verification.
Copyright © 1999-2006 PayPal. All rights reserved.

Please do not reply to this e-mail. Mail sent to this address cannot be answered.
Extract and block phone numbers
Beware of “Joe-Jobs”

We would like to introduce our new-born site, where you can shop around most wanted and needed items in your life. Our weapon section has wide range of hard-to-find machine guns, silencers, armour-piercing ammos and others.

First of all, let’s check our 3 top-selling items:
1. Russian surface-to-air missile SA-14 "Gromlin" (upgraded analog of SS-16 "Strela") from our supplies in Kazakhstan.
   Due to high demand, it takes about 4 weeks to backorder that item.
   - Weight is 10.2 kg., lenght - 1427 mm. You can make a huge party and you can have tons of fun launching your "Gromlin" with your buddies.
2. Israeli bestselling submachine-gun "Tavor" 5.56" (upgraded analog of 7.65" "Uzi"), comes with 2 full clips
   a lighter Zippo (25 grams of C4 inside)
   You can take one with you to the school or college and have alot of fun with your buddies. Buy more than 10 pieces of booby traps, and we upgrade C4 to C4+ for free.
   C4+ can not be detected in airports or any other security point.
   Also we have our Dutch-based shop where you can buy wide selection of ganzha, crack, both synthetic and natural.
   And our prices are affordable for everyone.

If you want to buy anything from us, just visit our site.
All major credit cards, wire transfers and money orders accepted.
Please ask for details if you want to use Western Union.

P.S. Due to our government laws all items from our site will be verified before shipping.

We thank to our hosting company AT&T www.att.com, and covers all our dirty business for the small period.

You can also make an order by the phone:
1-888-642-9675 fax: 571-434-4623

Do not hesitate to contact us via ICO # 176926755
Spammers respond

dial: one-eight-hundred-three-fiv-4-31-two-0

1_3*1*4*4+1+4+4*0*0*1
AGA Resources Inc.
A G A O
Open: $2.25
Close: $3.00
Up: 33%
QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
Not as common these days

• Good spam signs -- most filters are now able to detect them
• Not very legible
• Makes spam appear less trustworthy/legitimate
• Switching to some more advanced tricks to disguise content
QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
MS Word spam

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
Are you smart enough?

From: "welcome@lf.hebiic.gov.cn"
<welcome@hebiic.gov.cn>
To: undisclosed-recipients: ;
Subject: From far far away

Only Humans with an IQ of at least 120 are allowed to: click here
If you can`t open use this freeware: click here
The best way to defeat text filtering is…

…not using (ASCII) text at all
VIAGRA, Cialis, XANAX
$2.40 $3.50 $4.00
www.asciimedz.biz
BUY NOW!
| From: joel <avi@surfeador.com> |
| To: dbid | .com |
| Date: Wed Sep 8 06:08:04 2004 |

Услуги профессиональных грузчиков по умеренным ценам:
- Квартирные переезды
- офисные
- погрузка и разгрузка фур
- такелажные работы
- и т.д.
тел. (095)510-22-53, 8 916 954-00-60, 8 916 255-19-88 Олег
QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
2006: The era of image spam
Why?

- Attractive
- “Invisible” to most filters
- Bandwidth is no longer a limitation
- Unlimited potential for randomization with little or no impact on legibility
What?

Stock pump-n-dump scams        University “degrees”
Image spam with URLs

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
How: “mosaic”

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
How: animation

BUY!!!

BUY!!

BUY!!!

Buy!

BUY!

Buy!
• Not every animated GIF attached to e-mail is spam, apparently…
Anti-(image)-spam techniques

- Connection-level filtering
- Heuristics based on email structure
- Convert to text (Optical Character Recognition)
- Image analysis and “fingerprinting”
Spam vs. legit

30 pixels per byte

QEGY IS THE HOTTEST OF THE SEASON!
WATCH THIS ROCKET SOAR!
WATCH LIKE A HAWK ON WEDNESDAY OCT 11!

Profile
Company: QUANTUM ENERGY INC (OTC BB:QEGY.OB)

Price: $3.30
Symbol: QEGY
5-Day Target: $25

Analysis
Below $20: Strong Buy
Above $20: Moderate Sell
Current Rating: Very Strong Buy

DON'T BE A BYSTANDER ON THIS ONE!
WATCH IT TRADE ON WED OCT 11!!!

3 pixels per byte
Comparing over 30,000 legit and spam images

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
Filtering approaches

• Image metadata within certain bounds:
  • Compression ratio
  • Dimensions
  • Animated or static
• Combined with other information:
  • Sender reputation
  • HTML content
  • MIME structure, headers
• Fuzzy signatures of image metadata specific to a particular spam campaign
Social engineering tricks
The recipient
Subject: COCA COLA PROMOTION

Coca-Cola Enterprises Limited
Customer Service
Charter Place,
Uxbridge,
Middlesex UB8 1EZ,
United Kingdom.
Ref: CCP/491OXI/04
Batch: 12/25/0304

Coca-Cola Enterprises Limited

We happily announce to you the draw of the cocacola
International promotion programs held on the 9th of June
2006 in The United Kingdom. Your e-mail address attached to
ticket number: 564 75600545-188 with serial number
From: MICROSOFT MEGA JACKPOT LOTTERY <info@mswordlottery.info>
Subject: HELLO, 2006 E-MAIL AWARD WINNERS

MICROSOFT MEGA JACKPOT LOTTERY
UNITED KINGDOM. LONDON.
BANK OF ENGLAND/MICROSOFT HOUSE, LONDON.
Director: MR. DOUGLAS WILSON
Phone #: (00944) 701-113-0363

REF NO: M154S/WL06.
MICRO (LOTTERY) CHIP NO: 9465206

ELECTRONIC MAIL AWARD PROMOTION. MICROSOFT MEGA JACKPOT LOTTERY
UNITED KINGDOM.

...
From: <service@eve-online.com>
Subject: Your EVE Online account [Incident: 051111-000185]

We are contacting you because we have some problem with your subscription details. In accordance with Eve`s Agreement your account access will remain limited until this issue has been resolved.

To secure your account and quickly restore full access, we may require some additional information from you for the following reason:

We will assume your issue has been resolved if we do not hear from you within 48 hours, your account may be subject for suspension.

Thank you for allowing us to be of service to you.

To securely confirm your Eve`online information please click on the link below:

https://secure.eve-online.com/subscriptioninfo.asp

We encourage you to log in and perform the steps necessary to restore your account access as soon as possible. Allowing your account access to remain limited for an extended period of time may result in further limitations on the use of your account and possible account suspension...
### Eve Online Account - Character, 48m SP ELITE END GAME
BILLIONS in assets-Thanatos-220k Research-FULLY LOADED
Feedback: 70  |  100.0%

- **Payment Method:** PayPal
- **Bids:** 31
- **Shipping:** Not specified
- **Time left:** 4d 8h 45m

### 29 Million SP Eve Online Character Carrier Pilot!!
Feedback: 114  |  100.0%

- **Payment Method:** PayPal
- **Bids:** 0
- **Shipping:** + $20.00
- **Time left:** 4d 10h 16m

### EVE ONLINE Account Character - 36.7 Mil SP, PvP & Miner
6+Mil SPs Missiles 9.7 Mil Gunnery 1.2 Bill Assets BONUS
Feedback: 5631  |  100.0%

- **Payment Method:** PayPal
- **Bids:** 19
- **Shipping:** + $20.00
- **Time left:** 3d 8h 45m
More victims
Thank you