10 sneaky things a spammer will do

Just when you thought your inbox was safe...

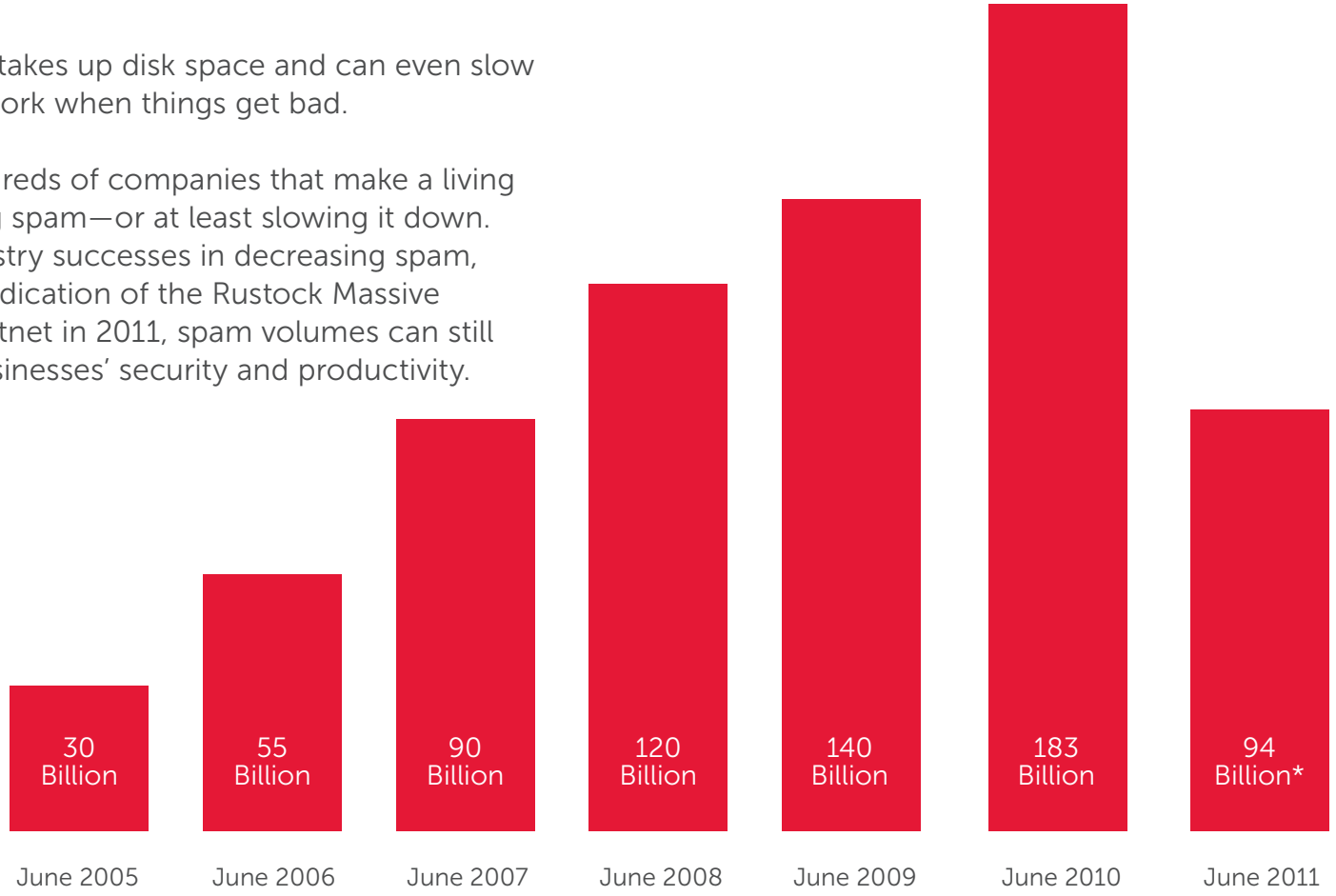
Table of contents

The overwhelming volume of email spam

Email spam—we hate it.

It wastes time, takes up disk space and can even slow down the network when things get bad.

There are hundreds of companies that make a living out of stopping spam—or at least slowing it down. Even with industry successes in decreasing spam, such as the eradication of the Rustock Massive Email Spam Botnet in 2011, spam volumes can still overwhelm businesses' security and productivity.



**Decline in spam can be directly correlated to the Rustock Massive Email Spam Botnet being eradicated in 2011.*

...so why is there still so much spam?

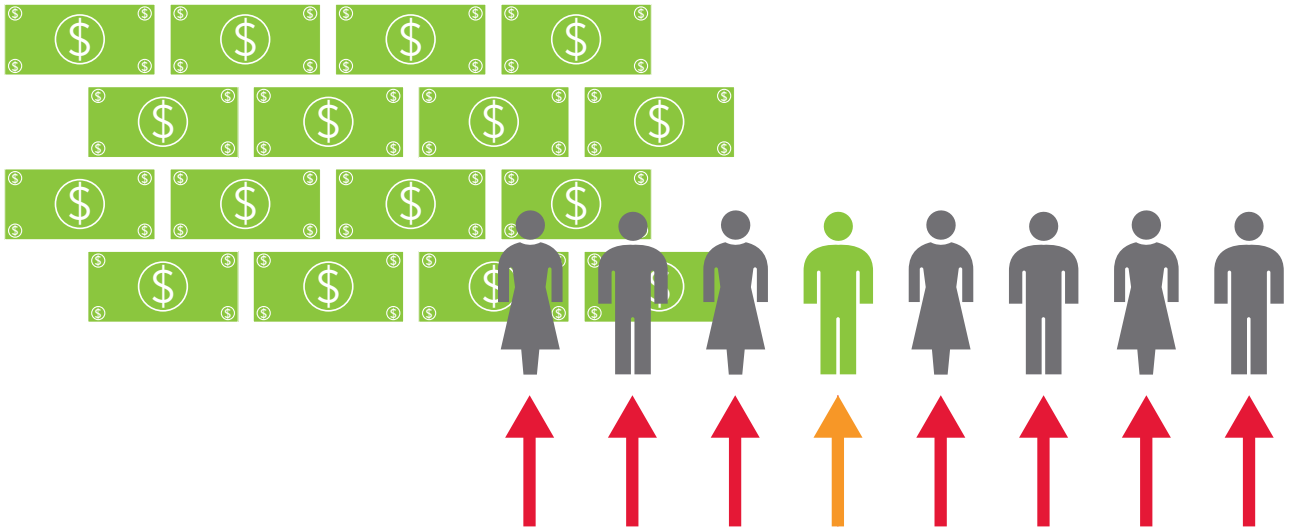
A reason for spam and a reason for more spam

Money

Yes, spammers can make money with email spam. Most spammers are just sales people looking for an avenue to sell their products or services. Sending out email is cheap and believe it or not some people do respond to their spam advertisements. It only takes a few people to respond to a spam ad to make it profitable for the spammer—so the game is to reach as many people as possible with the spam message to increase the odds of finding a few respondents.

Reaching the right people

With spammers using the "shotgun" approach to marketing (shoot at everything and you'll hit something) the increase in spam messages makes sense. Also, to improve their chances, spammers are constantly working to improve their effectiveness at getting past spam filters. Let's take a look at a few of the tricks that spammers use to improve their odds of reaching their target audience.

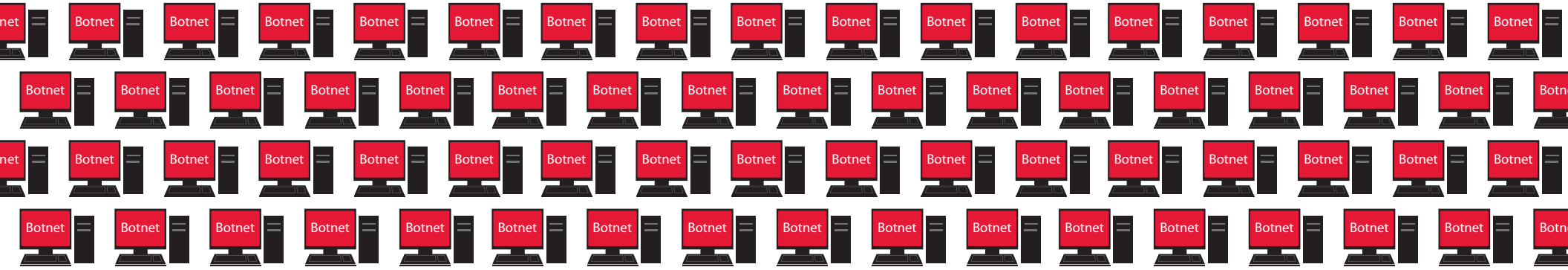


1st sneaky thing: Botnets, zombies and you

Botnet
A "botnet" is a collection of compromised computer systems that are under a common control structure. The compromised systems, called "zombies", can be directed to send out spam, phishing, viruses and other malware.

Botnets attack
A spam attack of millions of spam messages can be sent using a botnet. Each zombie may only send out 1,000 messages for a given attack, but with 10,000 zombies in a botnet, that's 10 million messages.

A zombie's reputation
When a zombie sends out a spam email, it does so from an assigned Internet address—the "Sender" IP address. But by limiting the number of spam messages a zombie sends, the spammer hopes to keep the IP address from getting a "bad" reputation.



2nd sneaky thing: Borrowing a reputation

Spammers adapt
Many spam filters rely on Sender IP reputation analysis to block spam. To lessen the effectiveness of systems which rely on Sender IP reputation, spammers will "borrow" IP addresses with a good, or at least neutral, reputation.

ISPs – Spammers create email accounts on Internet Service Providers (ISPs) big and small, all around the world. Blocking all the email coming from an ISP because one user is sending spam could be a problem.

Hacks – Spammers have been known to buy access to a hacked email server. They quickly generate a high number of spam messages using the reputation of the company whose server has been hacked.

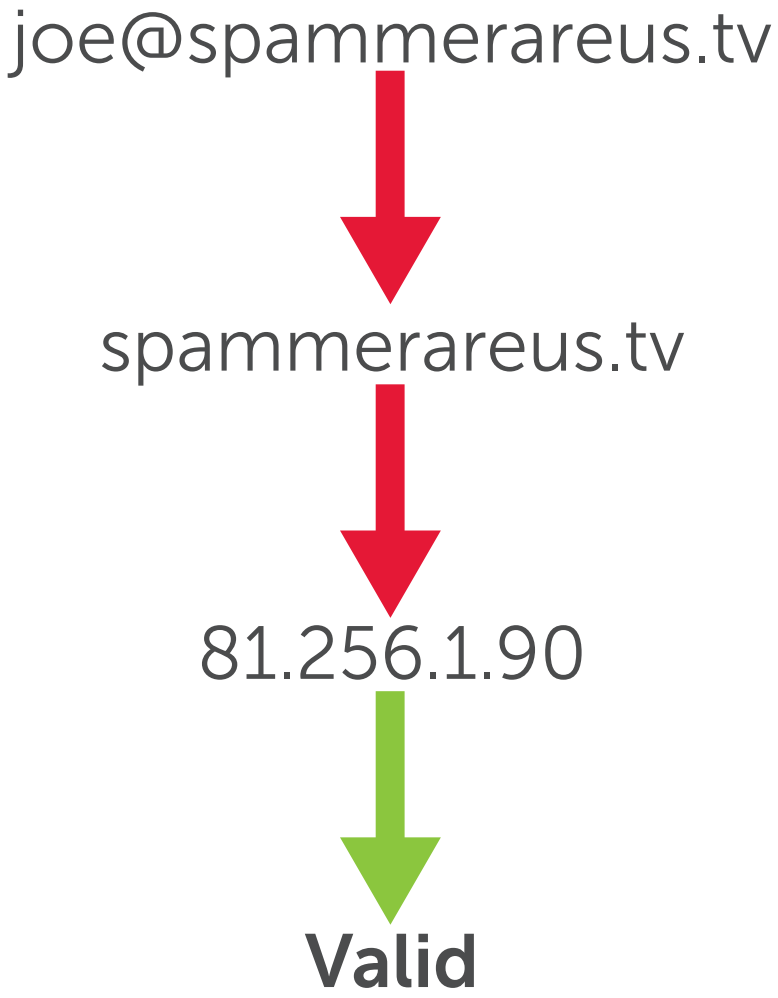
You – Or more precisely your company. A zombie system on your network is potentially compromising your Sender IP reputation, especially if there are multiple zombies living the undead.

3rd sneaky thing: Spammers can authenticate too

Authentication
Email authentication is basically testing to see if the domain an email says it is "from" is really from the IP address of the sending email server. To work, it requires an organization to publish an SPF record, which tells email receivers that a given IP address is allowed to send email for a given domain.

How can a spammer get around authentication?

- Strict set-up of an SPF record means that third party services (such as an email marketing company) typically cannot send email on a company's behalf. As a consequence, many companies set up authentication, but leave open the option for other IP addresses to send email (for example a third party marketing company or a spammer).
- Just like anyone else, spammers can register domain names and set them up to authenticate properly and then send email from them.



4th sneaky thing: Word salad

"Word salad" is the term used when spammers add what appears to be random words to an email message.

What's the scam?

- The spammer adds "extra" words to the email assuming they will be read and evaluated by the recipient's spam filter.
- The "extra" added words are "good" words not typically found in a spam email.
- When the message is evaluated there are now more "good" words than "bad" words (such as "enhance" and "love life"). If there are more good words than bad words, the spam filter may decide the message is good.

5th sneaky thing: Light reading

Some email spam messages contain more than extra words, they have entire sentences and paragraphs added to the message. Just like "Word Salad" the idea is to add in good words and phrases to the evaluation. Also, word salad and splice text frequently change, evading thumb print filtering. The use of complete sentences attempts to make it harder to exclude these "good words" from the evaluation of the message content.

"Love life in the dumps?"

www.enhanceyourlovelife.tv

It was a dark and rainy night.
It was the best of times, it was the worst of times.
Once upon a time in a land far, far away.
I'm nobody, who are you? Are you a nobody too?
How do I love thee? Let me count the ways.

6th sneaky thing: Tiny text

Who reads better—you or your computer?
Your spam filter reads your email looking for words and phrases it considers "bad" and if there is enough "bad" content a message can be considered spam. A spammer tries to disguise the bad words and phrases from the filter but still make them readable to you, the recipient, on the hope you'll want what the spammer is selling.

The big and small of the trick
The spammer changes the size of the fonts, making the extraneous letters "disappear" so that you can easily read the message, while your computer sees a line of gibberish.

What you see: **Gain Inches Patch**

What your computer sees:
asdGaindfisdfiohInchesdfjsdfPatch

7th sneaky thing: If only I could spell

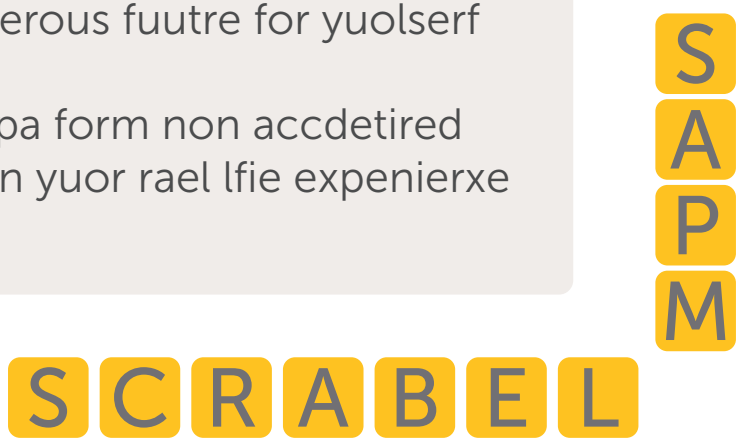
"Scrabble spam"
Most people can read the message above where the spammer uses misspelled words hoping the spam filter will not be able to understand the words.

Things to consider
How many of your emails would make it past a spam filter if the words needed to be spelled correctly? Many people use acronyms, abbreviations and even IM and text messaging slang in email.

Can you read this?

Domlipa program
Crteae a mroe ppsorerous fuutre for yuolserf

Reveiee a full dimolpa form non accdetired unieersiitvs beasd upon yuor rael lfie expenierxe



8th sneaky thing: How to spell \/!ägr/-\

Optical Illusions
Like Scrabble Spam, the trick here is to disguise the "bad" words. In this case the spammer uses symbols, special characters and even alternate character sets to create the different variations. Using this method, it is estimated that there are over 600 quadrillion ways to spell "Viagra"—that's a lot of rules to write if you want to do this yourself!

9th sneaky thing: What you see isn't what you see

Image tricks

Although images may look the same, often they are not. Small changes can make the images different.

Day one

Inbox: Receive this image spam message

You: ***"Junk it"***

Day two

Inbox: Receive the "same" image spam message

You: ***"Junk it again"***

Day three

Inbox: Receive the "same" image spam message

You: ***"Really junk it"***

Day four

Inbox: Receive the "same" image spam message

You: ***"Call IT now"***

Image layout changes by a pixel or two

The backgrounds change from white to clear

Image size changes by one or two percent

10th sneaky thing: Social engineering

Most spammer tricks try to bypass or sneak past your spam filter using subversion. Tricks based on social engineering do the opposite—they try to look and sound legitimate so they can get past your spam filter and into your inbox.

Not so friendly friend
If a friend's system gets compromised your name may be in their address book—oops. And if your friend's name is on your "allow" list—double oops.

Extra, extra
Spammers use the latest headlines as the email subject. It not only ads legitimacy to the email, but also often raises our interest in opening the email.

Phishing
Phishing emails try to use the trust of pretending to be from your bank or other trustworthy sources. The intent is to obtain your account, financial or even identity information.

Attachment spam
Spammers will attach real PDF or similar files to a message that contains the spam message. The actual email says little, except maybe something like "Joe, check this out" or "Q3 revenue forecast".

Beating the sneaky spammer

Spam will continue to plague our inboxes until it is no longer profitable for the spammer or there is a hack-proof prevention method that everyone uses. There is no singular technology that can stop all spam, and history has shown us that when a given technology begins to work well, spammers attack it with a vengeance. That's why multiple anti-spam techniques working together provide the best solution over the long run. These techniques break down into three groups:

1. Reputation analysis
This is examining the reputation of many email attributes, including the Sender IP Address, the content, the links/URLs, images, attachments, the email's structure and more.

2. Content analysis
Powerful techniques like Bayesian filtering, lexigraphical distancing and image inference analysis, along with simpler checks like allow/block lists and SPF checks, are combined to thoroughly analyze an email and dig out its true purpose.

3. Thumbprinting
When an email is disassembled, each component is encrypted using a non-reversible hash process to create a "thumbprint" of that component. These thumbprints—not the original component data itself—are then sent to the data center with a corresponding reputation of good or bad, and tabulated in real time.

Dell SonicWALL Anti-Spam/Email Security Solutions

Dell™ SonicWALL™ delivers a wide variety of industry leading award winning email protection solutions for one to one million users.

Dell SonicWALL Comprehensive Anti-Spam Service
Email spam, phishing and virus protection service for TZ, Network Security Appliance (NSA), and E-Class NSA firewalls

Dell SonicWALL Email Security for Small Business Server
Inbound and outbound email protection for Windows SBS and Windows EBS environments

Dell SonicWALL Email Security Software
Complete inbound and outbound email protection software ready to install on a Windows Server

Dell SonicWALL Email Security Appliance
Complete inbound and outbound email protection, available as hardware appliance, virtual appliance or software

Dell SonicWALL Anti-Spam Desktop
Client-based email spam and phishing protection for Outlook, Outlook Express and Windows Mail

Dell SonicWALL Hosted Email Security
Cloud-based protection from spam, phishing attacks and malware, while minimizing deployment, administration and bandwidth expenses

How can I learn more?

- Download the Whitepaper: "The Dell SonicWALL GRID Network: Collaborative Cross-vector Protection for Email Security"
- Download the Whitepaper: "Building a Better Spam Trap"
- Opt-in to receive Dell SonicWALL Newsletters

For feedback on this e-book or other Dell SonicWALL e-books or whitepapers, please send an email to feedback@sonicwall.com.

Forward to a friend

About Dell SonicWALL

Dell™ SonicWALL™ provides intelligent network security and data protection solutions that enable customers and partners to dynamically secure, control, and scale their global networks. Securing any organization with multi-threat scanning based on global input at wire speed, Dell SonicWALL is recognized as an industry leader by Gartner and NSS Labs. For more information, visit the web site at **www.sonicwall.com**.

DELL Software

05/13 DS 0238L