spam and businesses over a coffee

Business Services

orange™

editorial

Just over 20 years ago, I sent my first message using a Unix sendmail command. Little did I know then how important these little messages would become in my personal and professional life, but still less could I fathom how these electronic messages would revolutionize the way we work and do business.

But this new way of communicating also brought with it the plague of modern times: spam. You're familiar with it, all those messages that try to entice you to buy luxury watches at cut-rate prices, miracle pills that cure everything, and any number of gimmicks you never knew you needed. Like everyone at the time, I fell victim to spam. But that was back in the days when our protection tools were far from sophisticated.

In this blog book's first article, Jean-François Audenard explains how spam can thrive on gaps in SMTP protocol.
Our next article demonstrates how spam can even attack corporate e-mail systems. We'll then learn how the global fight against "traditional" spam has finally made some headway by significantly reducing the total volume of spam sent around the world. And to conclude, we'll take a look at how spammers use news stories and seasonal events to hone their attacks and disguise the ir traps. Spam attacks now use basic marketing tools and look more and more like full-fledged ad campaigns!

I hope you enjoy reading this, and I look forward to more discussions on our blogs!

Philippe Macia

content

how does spam work ?

by Jean-François Audenard

Everyone has come across unsolicited messages in their inbox. Certain periods of the year are particularly bad. During the holidays, for example, a full-scale assault is launched on our e-mail accounts:

- deals on luxury items at unbeatable prices
- medicine to enhance our sexual performance
- even the occasional 100 million dollar inheritance from a long lost relative

And among these can't-miss offers there are sure to be a few viruses and other IT attacks. OK, so everyone knows about spam, but what is it exactly?

no standard tools for securing your inbox

The system currently used to protect your e-mail was developed way back at the dawn of the Internet. In those days, there were a very small number of servers, and almost all admins knew each other (or at least they shared a set of common values).
In this environment of relative "trust," usage remained "normal" and abuse was rare.

However, the explosion in the number of machines and the massive growth of the Internet changed absolutely everything. Sadly, the systems used to send and receive electronic messages have not evolved with the times.

So we’re still using a system originally designed for a world where self-control was the only rule. This has given birth to the Internet as we know it today, where the “law of the jungle” reigns supreme.

e-mail is a digital postcard

Sending a postcard is as simple as can be: just drop it in the mailbox and off it goes. In some ways, mail is the same as email:

- you can send a postcard to anyone you want
- no sender address is required (or you can make it up)

What’s different about e-mail:

- you don’t have to buy a postcard
- you don’t need to buy a stamp

Here’s another important point (that has nothing to do with spam), which many have failed to grasp (you can take my word for it): anyone at all can read what’s written on the card (it’s all in plain view)…

anyone can get his or her own mailbox

Unlike mailboxes on the street, the mailboxes used for e-mail are servers. These servers are called SMTP servers: they're created by Internet service providers, businesses and anyone with a passion for computing.

In fact, anyone can set up their very own SMTP server.

Once an e-mail is sent to an SMTP server, this server then sends it on to another SMTP server which is in charge of managing the addressee's inbox (using the DNS system).

SMTP servers set up as open relays

Ordinarily, an SMTP server only handles e-mail addressed to one of its users (or "clients"). Up until a few years ago, the goal was to find open relays that accepted e-mail to or from anyone, which left the door wide open for spammers. Now that most of these open relays have been closed, spammers have had to come up with some new tricks.

the rise of the botnets

If an SMTP server automatically accepts any e-mail belonging to its "legitimate clients," then spammers just have to pose as legitimate clients to make sure their spam gets through.

The best way to pose as a legitimate client is to infect a machine and control it remotely. And now we meet our enemy: the network of zombie machines known as botnets.

“never reply to spam and never purchase any service or item mentioned in spam”

warning

security techniques: senders and receivers

Fighting spam is no walk in the park. It demands a huge amount of resources that have to be renewed continually. Sometimes it can be a pretty one-sided battle…

We'll see that different techniques do indeed exist to prevent spam on the sender side and to keep it out of your inbox on the receiver side. But that's for another time!

One last thing: never reply to spam and never purchase any service or item mentioned in spam.

read the original article
http://oran.ge/14BRXyY

businesses sending spam: fact or fiction?

by Jean-François Audenard

With computer viruses posing a constant threat, spam is something every Internet user knows about. Of the several e-mail addresses I use at any given time, I receive at least twenty messages a day inviting me to buy this or that, or check out this or that website…

Since e-mail addresses are essentially untraceable, spammers are free to flood whatever message platform they choose, from major services used by millions of Web users for their personal e-mail, to company inboxes used for business communications.

This kind of "incoming" spam is familiar to everyone. That's why there's a big push to block these unsolicited messages: multiple filtering systems are available that offer a variety of services and solutions ("in the Cloud" filtering, spam boxes, software for e-mail servers and programs installed directly on work machines). Almost every company uses at least one of these solutions.

what about spam sent by companies?

While everyone knows about “incoming” spam, **spam sent by company networks** suffers from a serious lack of communication. Sometimes it’s even a taboo subject, since it points directly to security problems within a company’s local network.

First of all, let’s set aside companies that send spam deliberately. These can be “online marketing” companies sending out e-mails for their customers, or other companies that send messages to expand their potential customer base. In both cases, these businesses may run up against a variety of sanctions if they don’t follow several rules. This can be a problem in particular for small companies that don’t always operate in gray areas.

Our topic today, however, is **companies that send out spam without realizing it.**

what companies are we talking about?

We’re talking about companies of all sizes: small businesses with just one website, nationwide companies and multinationals. But of course, this tends to be a particular problem for smaller companies.

All sectors are concerned: this means companies that manufacture precision tools for the automotive industry, for example, or those who provide IT services, supply heavy equipment for construction, or work in finance. Essentially, everyone!

All Internet connection types are concerned: experience has shown that the Internet connection type does not notably alter the problem. This means companies that connect with separate interconnection routers are just as vulnerable as businesses using more complex protection services such as gateways or services offered by their ISP.

how is this possible?

After analyzing feedback on this problem, we can recognize two main categories of businesses affected by these problems:

- businesses whose internal message server is **hacked by a third party**
- businesses where employee machines are **infected by a “bot”** or “zombie” program

improperly secured message servers

In this case, a company fails to take sufficient measure to secure its internal e-mail server. This will be quickly noticed, as spammers **use the company server as a relay to send out spam!** Spam will then be sent from the company server to the greater Web community. This means the company and its access provider will be responsible for the spam. In this situation, spam is sent over servers configured as open relays.

Failure to take action in this situation can have a significant impact on the company's activities: the message server will eventually be registered on **"blacklists"** and consequently "forbidden" (impossible to send e-mail to customers or partners).

Correcting this problem is fairly easy: simply change your server settings to deactivate the open relay mode.

employee machines infected by a "zombie" or "spambot" program

good to know

It's important to treat each complaint received for spam sent from your network, as the consequences can be greater than they appear at first.

In this next case, spammers do not hack a server; instead, they take control of employee machines connected to the company's LAN. First, spammers will try to infect machines with a program that will enable them **to remotely control the machine.** Once this is done, the machine (also called a "bot," "robot," "zombie," or "spambot") is now ready to send out spam.

Once again, failure to take serious action in this situation can have adverse consequences. Aside from the obvious risk of "banishment" through "blacklists," there is the added problem that **machines are no longer under company control.** This means an attacker has the means to access documents stored on the network, listen to internal communications on the network, etc.

This can be a tough problem to fix. A little planning and method are required. First, block messages moving in and out of the network, and then "follow the trail" to locate suspicious machines. Last, disinfect the machine or, for more security, reformat it entirely.

how do you know if you are sending spam?

First off, it's important to know that your ISP's "Abuse" cell will be the first to receive any complaints issued by third parties. After this cell conducts an initial investigation, it will contact the person in charge of the service contract. In general, this is a company's executive or general manager. Any communication of this sort should be taken very seriously, since it almost always means there is a real problem. Mistakes are rare.

If you want to go the extra mile, you may also want to **test your "reputation"** using several different websites to determine if spam is being sent from your network.

recommendations: e-mail servers

1. **Check your settings on a regular basis:** when you set up the network and during any maintenance actions.
   Any "anti-open-relay" features are as important as any other security measure.

2. **Determine if your servers are seen as open relays.**
   A variety of free testing services are available on the Web. For the more tech-heavy tests, a simple "Telnet" and knowledge of some basic SMTP commands will suffice.

3. **Monitor your message server:** keep an eye on the number of messages sent per day, the length of queues, the number of send failures, etc. Any sharp fluctuations in these numbers should tell you something is up.

recommendations: employee machines

1. **Block** (or set up a service to block) **SMTP fluxes** (TCP/25) at your Internet access point. Only authorize communication through your ISP's relay servers.

2. **Even better: reconfigure your message client** (Outlook, Thunderbird, etc.) so your e-mails are submitted through a protocol requiring authentication (Submission Protocol RFC2476, TCP/587) and block all outbound SMTP flux (TCP/25).

3. **Monitor bandwidth usage** on your network to detect any suspicious behavior.

4. **Regularly update security measures** used on your machines, and update your antivirus software on a daily basis.

“spam sent by company networks is underestimated”

warning

conclusion

Spam sent from company networks is a real problem: this problem touches all businesses of every size and in every sector. It's important to treat each complaint received for spam sent from your network. The consequences of not taking action can be heavier than they appear at first. If you have any questions or problems, I suggest you follow the recommendations outlined by your ISP and browse through the wealth of information available on the Web.

"Road warriors" and other advocates of mobility will immediately recognize the value of using the "Submission Protocol" (TCP/587) to send e-mail. It works de facto no matter where you connect to the network. Changing outbound SMTP servers is a thing of the past! :-) When security helps improve ease of use, you have to mention it, right?

read the original article
http://oran.ge/19g7OVJ

is the end near for spam?

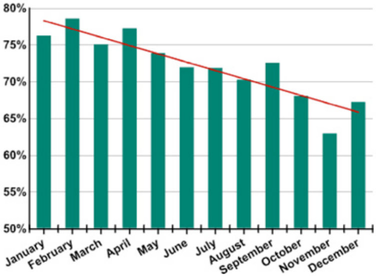
by Philippe Macia

Security developers all seem to agree: **spam is on the decline!** But even if the volume of spam has diminished since its glory days, **does this really mean spam is dead?** Not quite. The beast is still kicking, and is now using more insidious methods.

a notable drop in "traditional" spam

How do we observe this decline? Security developers often publish an annual threat report. Some, like Symantec, even provide weekly spam reports. Rankings are compiled based on observed spam. Developers then analyze trends based on these rankings.

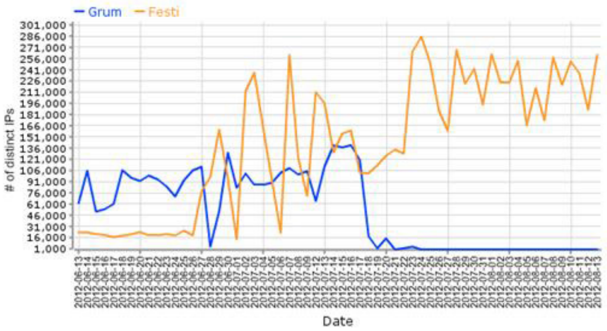
According to Kaspersky, **spam reached a five-year low in 2012.** By the average annual rate, only 72.1% of e-mail is spam! That's a far cry from just a few years ago, when the spam level reached 95%.



why is spam on the decline?

1 – battling the botnets

Developers agree that campaigns to eliminate certain botnets have helped cut down on spam considerably. According to some estimates, shutting down two command servers on the Grum network in summer 2012 led to an 18% **drop in spam.** But these figures are hard to confirm, especially since Spamhaus and Symantec have unfortunately found that as soon as one botnet is shut down, another takes its place. In this case, Grum's downfall led to the rise of Festi. And now that Festi is lying dormant, we can only wonder what's next.



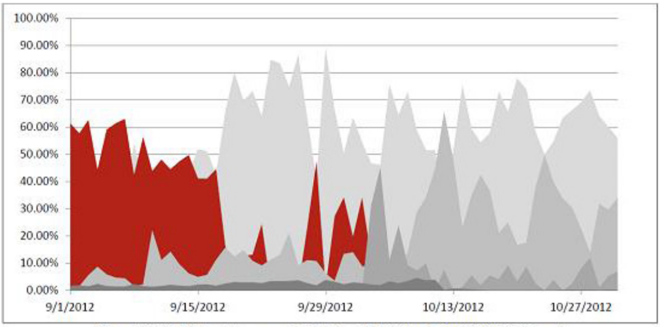


Figure 7 – Festi botnet disappears in October. (NB. Dates in MM/DD/YYYY format)

2 – e-mail is no longer top dog

E-mail is no longer the preferred method for transmitting viruses. The percentage of attachments containing viruses has plummeted. According to Cisco and Kaspersky, only 3-4% of spam still contains attachments with viruses.

3 – protective measures are increasingly effective

Anti-spam measures used by businesses often combine antivirus software, blacklists, DNS request analysis, lexical analysis and heuristic analysis: it's becoming increasingly difficult to get spam through all these layers of defense.

spam 2.0 on the horizon?

The fight against spam has upped the cost per click (the amount spent for each click on a link in a spam message) for spammers. This has forced spammers to find new ways to keep costs down.

Showing good economic sense, spammers have learned a few tricks from viral marketing and have made the following realization: you have to **take advantage of message systems** powered by social networks and use viral techniques that remain largely unmonitored. For example, you post an offer for a smartphone at a low price and then let the social network go to work. The more likes and reposts your post gets, the more it will be seen by users who will then open the ad and pass it along.

Spammers quickly realized it was much cheaper to create fake commercial websites, post real ads on legitimate web 2.0 sites and **take advantage of the power of social networks** to launch their gimmicks.
This is the biggest trend in the new form of spam 2.0!

good to know

Spammers quickly realized it was much cheaper to take advantage of the power of social networks to launch their gimmicks.

One last figure: according to Kaspersky, the price per click for traditional spam is as high as $4.45, compared with just $0.15 for a real ad for a fake site on Facebook.

We might ask, when will we see effective anti-spam measures on our browsers and social network message systems? The answer is certainly soon.

It’s not all peaches and cream just yet, but we can still relish the positive side of all this, that traditional spam is on its way out and no one is going to miss it!

read the original article

http://oran.ge/1exdTKx

is spam a seasonal activity?

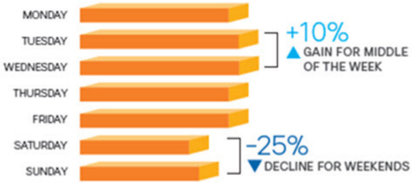
by Philippe Macia

Let's admit it: spammers are not stupid. And even if it looks like their traditional activity (sending spam to classic message systems) is on the decline, let's take a look at what they're now doing to get us to fall into their traps. In particular, let's look at how **spammers target the times when we are most vulnerable.**

anyone out there need spam?

As I explained in a previous article, spammers are doing everything they can to cut their cost per click. That's why it's in their interest to send spam when we'll be most certain to receive it. And when's that? During the workweek!

Unlike robberies, which take place when no one is home, spam is more effective when someone is around. That's why **a good spammer will always target peak days**, as demonstrated by Cisco. Spam volume drops 25% over the weekend and peaks midway through the week.

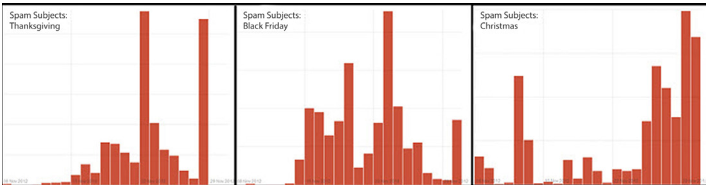


These statistics are based on data collected by anti-spam software developed for businesses. To my knowledge, no similar studies have been conducted for spam intended for individuals. But something tells me the trends may be the exact opposite…

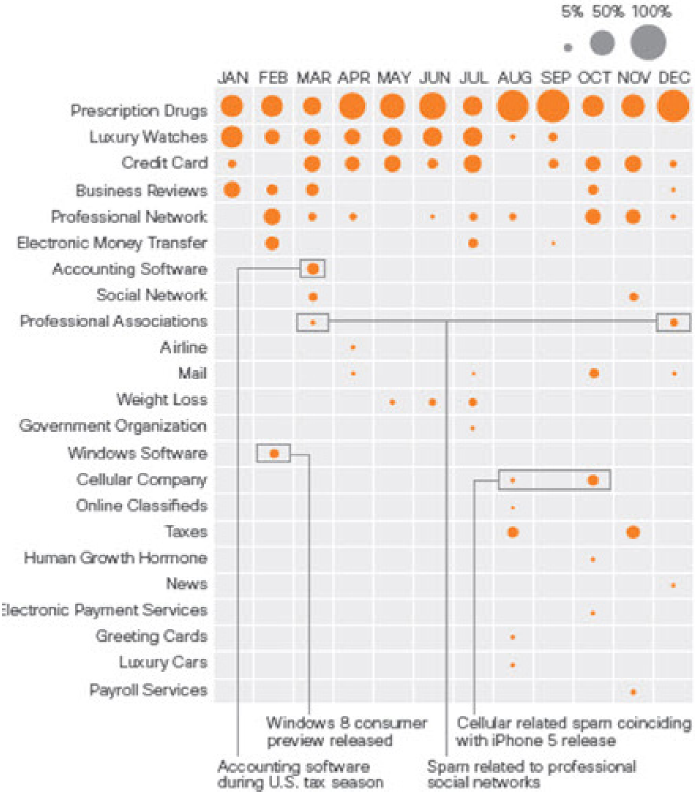
Let's also keep in mind that although spam slows down over the weekend, a company's inbox over that time is almost entirely composed of spam, since spam can pose as legitimate e-mail.

how do you like your spam?

Spammers also aim to slip right in with our (presumed) interests and take advantage of everything that may **help spam blend in with legitimate e-mail.** So they always use seasonal keywords like Christmas, Thanksgiving or Black Friday to catch our eye, as Symantec showed us in November 2012.



Lastly, spammers also try to bait us with news events in addition to holiday keywords. See Cisco.



Tax season, the launch of a new smartphone, a new OS, summer diet season, anything is fair game when it comes to launching a new spam campaign!

Spammers are a wily bunch: real ad men!

read the original article
http://oran.ge/11R7HKK

about the authors

Jean-François Audenard

At Orange Business Services, I am in charge of integrating security in the core of our cloud computing services and packages. I'm passionate about my work and I try to only consider things from a thoughtful, rounded perspective: I don't do things half-heartedly. I'm a committed and (hopefully) engaging blogger who likes to get off the beaten path and explore new ways of doing things. Honesty is my motto, while optimism and determination are my two driving forces.

Philippe Macia

After previously working as a training manager, on-site IT officer, pre-sale technical officer, and customer service manager, I joined the Orange Business Services security team as a product manager.

I'm very committed to the user experience and easy administration of the solutions we create. My watchwords: knowledge sharing, logic, pragmatism and simplicity.

Our blog :
http://www.orange-business.com/en/blogs/connecting-technology/

Document available for download at:
http://www.orange-business.com/en/library/

Edited by Orange Business Services
14.08.2013

Orange, French “anonymous society” (S.A.) with an operating capital of 10,595,541,532, 78 rue Olivier de Serres – 75015 Paris – 380 129 866 RCS Paris

Business
Services

orange™