What is spam?

A History of Spam

In a nutshell, spam has evolved from an annoyance to a criminal enterprise, it has, as a headline recently noted, taken a journey from hobby to profit-driven attack.

Spam started out, just as email did, as a thought experiment (Question: Can I do this? Answer: yes). Email systems were set up initially between two computers in the same room, then colleagues on the same floor, then the same campus, and ultimately on the same network. In essence, societal norms and peer pressure were the crowd-sourcing required to keep the network clean. Everyone knew everyone else, and transgressions for violating community norms were rapid and severe.

When Gary Thuerek sent the first spam message touting a new DEC computer system to ARPANET users in 1978, the backlash was instantaneous, and it took years before another spam incident occurred. But, occur it did, after the initial network deployment ARPANET was expanded to other concerns beyond its nascent educational-U.S. military cooperative iteration.

Along came immigration lawyers Canter and Siegel, who, in 1994, pretending to be unaware of the cultural norms, made mass postings advertising their services to hundreds of USENET topic-specific discussion groups (none of them on the topic of immigration to the United States).

Simultaneously, others new to the net quickly realized that email too had been developed without any security considerations, and used the loopholes to spam easily and readily on that medium.

In the early 1990s it was a challenge to obtain an email address, and so when one sent spam, the source was quickly identified and blocked quickly at receiving sites. Spammers soon discovered they could forge addresses and domains, and so IPs were blocked. Spammers in turn discovered that they could relay their messages through third-party mail servers facilitating the exchange of email in a collegial fashion, and the era of ‘open relay’ spam was born.

Domains became more readily available in the 1990s, and some were used for no other purpose than spamming. So the industry began to block entire domains.

By 1996 we had seen the first spammer sued by major business concerns, as AOL, Microsoft and Earthlink took former junk-faxer Sanford Wallace to court.[1]

[1] Sanford Wallace’s lifelong abuse of services that don’t belong to him is an analog for the development from annoyance to criminality. Wallace came into the illicit advertising by way of junk faxing, taking advantage of the relatively low cost of faxing (locally, at least) until he was told to stop by law enforcement agencies.

[1] He moved into the field of email spamming, and by 1996 had been sued by the major ISPs of the day.

[1]He announced his retirement, and became a D.J. and club owner in New Hampshire for a time, but soon reverted to his criminal activities; He shifted gears and began to distribute spyware, and again was sued in 2006 to put a stop to that activity.

[1]He turned his gaze upon social media networks, and began to spam MySpace in 2007-2008 and was again sued to

As open relays were systematically closed at the start of the 2000s, hackers developed malware to insert onto individual computers that allowed them to form vast botnets, which we are dealing with today.

Just as originally the payload of spam was relatively benign, with exhortations to purchase immigration services or actual legitimate goods, things quickly turned to illicit drugs, pornography, advance fee fraud scams, counterfeit goods, fake dating websites and so on.

Phishing was originally fairly straightforward, looking to steal users' email login credentials so the spammer could use them to send more spam. Soon after, individuals' financial accounts became a popular target for phishing. As things progressed through the 2000s, phishers turned their attention to higher-value targets, the bank accounts of small and medium-sized enterprises (SMEs). Abuse researcher Brian Krebs mapped out attacks on SMEs for a couple of years, one can only imagine how financially devastating the loss of operating funds has been to townships, and churches and other small businesses. An interactive map can be found here :
http://www.batchgeo.com/map/483cd995e217a9dc46d4386db15413c5

The step we've seen recently is attacks on extremely high-value targets, such as the large American retailer, Target Inc. Phishers determined a back-door way into Target by way of their heating and ventilation control vendor, who had certain systems access. From there, they planted malware that was able to exfiltrate access to financial systems, and in a short while, 140,000,000 credit and debit cards were stolen from the retailer.

Definitions of spam

The classic definition of spam is unsolicited bulk messages, that is, messages sent to multiple recipients who did not ask for them. The problems caused by spam are due to the combination of the unsolicited and bulk aspects; the quantity of unwanted messages swamps messaging systems and drowns out the messages that recipients do want.[2]

For practical and legal reason, different organizations have different definitions of spam. When a recipient gets a single message, it can be difficult to tell whether that message was part of a group sent in bulk, so a common alternative definition is unsolicited commercial e-mail, on the theory that most unwanted mail is commercial. Many mailbox providers consider it to be mail their users don't want, or mail their users complain about, since their goal is to minimize the support costs associated with complaints. In practice these varying definitions describe approximately the same set of messages.

In countries that have laws related to spam, the most common legal definition is unsolicited commercial e-mail, along with mail that is misleading or fraudulent. The United States is an outlier; its CAN SPAM act only forbids commercial e-mail that is fraudulent, or was sent after the recipient told the sender to stop. Non-commercial mail generally gets more lenient legal treatment than commercial mail.

stop that activity.

[1] In 2009 he began to send phishing messages to Facebook users, and the social network filed suit against him. The activity continued, and as he stole additional user credentials, a criminal suit was brought against him. Wallace was arrested for his phishing activities in 2011 and awaits trial for several serious charges.

[2] The name comes from an old Monty Python skit in which actors in a movie lot canteen dressed in Viking costumes chant spam, Spam, SPAM so loudly and repeatedly as to drown out everything else.

Where spam appears

Spam has been a problem in many different media, and invariably arises whenever a medium allows people to send many messages without per-message charges. A short-lived flat-rate telegraph service in the 1800s closed down due to spam in Morse code.

On the Internet, spam has affected usenet (the shared bulletin board system), e-mail, instant messaging, blogs and blog comments, and social media including Facebook and Twitter. It has also appeared as junk faxes, VoIP telephony, Instant Message (AOL Instant Message aka AIM, Apple iMessage, etcetera) and SMS (phone text messages.)

Spamming techniques have evolved as conditions have changed. For example, junk faxes were initially a local problem, as advertisers with new cheap fax machines used them to make free local calls, but high toll rates kept them from making long distance calls. Now, with toll rates in much of the world approaching zero, junk faxes are as likely to come from the other side of the world as from around the corner. On the Internet, as users have moved from one service to another, e.g., from Geocities to MySpace to Facebook to Pinterest, spammers have followed them.

What spam does

The original impetus for spam was advertising. A famous early usenet spam was from a lawyer advertising immigration service ("green card lottery") and early e-mail spams advertised computer equipment, purported blueprints for atomic bombs, and magazine subscriptions. Since spam is so cheap, and is often anonymous, it is also popular for marginally or completely illegal schemes including fake drugs, pump and dump stock touts, money mule recruiting, and advance fee fraud (often called 4-1-9 after the section of the Nigerian criminal code that outlaws it.)

Some spam also does non-commercial advertising. There has always been a modest amount of religious spam, and surges of political spam before elections. Although these kinds often have a different legal status from commercial spam, the practical problems they present are the same, and providers generally treat them the same.

An increasing motivation for spam is to distribute malware, either by including an infected program or document directly in the spam, or by linking to a web site with infected content. These spams generally contain misleading headlines and content to encourage victims to open them, e.g., pretending to include a receipt for an expensive order the victim never made.

The other major use of spam is *phishing*, impersonating a trusted party to steal the victim's credentials. Phish spam often pretends to be from banks, ISPs, or mail providers, telling victims to confirm or update their accounts. Links in the phish lead to a web site that resembles the real organization's login page, so the victim will enter his or her credentials, which are then sent to the phisher.

Spear-Phishing takes phishing one step further, where the miscreants specifically target organizations or individuals who are likely to have access to high-value assets. For example, determining who the financial staff are in a given company may allow access to bank accounts; similarly, specific technical staff may have login credentials to organizational infrastructure that can be compromised with a specially crafted, socially engineered spear phishing attack.