A Study in Spam

Matthew Edwards

Focus: Security Economics

November 12, 2020

Spam: advertising gone wild

Business model: cheap product + low-value, low-return advertisement.

Single successful spam campaigns can generate up to $1 million in revenue, and sustained programmes can be multi-million-dollar industries.

1. Harvest email addresses
2. Write spam email
3. Send spam in bulk
4. Process orders from responses

Harvesters

Deploy crawling infrastructure, sometimes distributed across a number of machines.

Often run ‘off the shelf’ harvesting software (“ECrawl”, “Email Harvester”).

Seen spoofing the Google bot, even coming from a Google AS.

Turnaround times range from 5 days to more than a year

Templating

Identical spam messages can quickly be filtered.

The sophisticated spammer uses spam *templates*, and tests them against existing spam filters.

Plenty of support for template creators, including friendly web interfaces (available in Russian or English), instruction manuals, interactive technical support lines...

Delivery

Modern email system effectively prevents bulk email from a single sender.

Spammers turn to distributed system of compromised machines.
Typical example: Curtwail

- Machine is compromised, executes a loader (Pushdo)
- Loader identifies victim system, contacts botnet CC server, downloads malware modules, incl. rootkit, spam engine, server list.
- Spam engine spins up, contacts Curtwail CC, waits for instructions
- Once paid by spammers, Curtwail CC server provides spam template, target list, configuration file for behaviour.
- Compromised machine then uses spam engine to send email.

Competition

Botnets can be competitive, often identify and delete other malware from victim systems, even applying security patches in order to retain ownership.

More worrying: “those other cybercriminals might hack our command-and-control servers”.

The e-commerce platform

URLs in emails often chain redirects, to hamper takedowns.

Platform *needs*:

1. Goods
2. Website
3. Payment processor
4. Shipping

Also important: *customer services*. Spam-advertised businesses take good care of their customers.

The payment lynchpin

Researchers identified that there was a payment bottleneck in the spam economy

Just 3 banks were providing payment processing for 95% of spammers studied.

New banks and payment processors were difficult and expensive for spammers to recruit. This intervention would *cripple* the entire spam economy.

Who buys?

Three different broad categories of drugs sold:

1. "Lifestyle" drugs like painkillers, which can be abused.
2. Erectile dysfunction drugs like Viagra, which are embarrassing to ask your doctor for.
3. Chronic disease medication.