

Update on the Enemy

A Deconstruction of Who Profits from Botnets

Abstract

The success of spamming botnets is evident by the huge amounts of unwanted email clogging everyone's inbox. However, this success has also led to the commoditization of spam, in which margins have rapidly eroded and volume is the primary means to generate cash. One increasingly popular botmaster response has been to leverage infrastructure developed for spam to branch out into new forms of malicious business.

The botnet business model has become so fragmented and distributed that even legitimate businesses use it to drive online sales.

This tactic carries a number of advantages for a botnet's controller:

- It is a trivial process to reprogram a bot on a compromised host
- Existing botnet investments can be easily leveraged for higher-margin purposes
- Network security, when bot-aware at all, tends to concentrate on spam, not other botnet activities

The result is predictable. Bots now "look around" when first activated. If they find themselves on a corporate network, they seek login credentials and critical data. The street value assigned to this information depends on the level of access and the sensitivity of what can be stolen. If the bot isn't privy to anything that might command a premium price, then it defaults to lower-margin activities, such as malware propagation, Denial of Service attacks or spam.

Introduction

Botnets proliferate rapidly and widely for a single, simple reason. They make money. If they weren't profitable, then they would not be worth the time and effort that is necessary to make them so hard to find and remediate.

However, all those dollars, yuan and euros raise a couple of very important questions:

- Who, exactly, makes money off botnets?
- How do they make that money?

The answer to the first question is – anyone. Botnets have become a very democratic business model. In fact, the botnet business model has become so fragmented and distributed that even legitimate businesses use it to drive online sales. All you need is a PC and a moderate tolerance for online larceny somewhere across your online supply chain. This dispersal of ownership greatly complicates every aspect of combating botnets, from identifying botnet malware on compromised systems to prosecuting businesses and individuals who use botnets for illegal purposes.

The second question can be answered equally directly. Botnets enable sophisticated, multi-tier business operations, in which both revenue and risk is divided amongst software developers, infrastructure hosts, content providers, clients leasing space on networks and aggregators who connect smaller botnets into larger entities.

Each step along this path assumes that large numbers of systems across the Internet can be compromised because businesses and individuals use yesterday's antivirus and intrusion prevention tools to try and catch today's or tomorrow's botnet threats. It's a competition in which speed kills, and successful botnet merchants move far faster than traditional security infrastructure can keep pace. It's a game that anyone can play – and one that will only grow as it continues to be successful.

Follow the Money

Spam is the most mature application of botnets, in both business and technical terms. As such, it provides the best example of just how sophisticated botnet-driven “businesses” have become. The cash flow is huge, even with the commoditization of the market. For example, online pharmacies rely heavily on spam, and were estimated to have earned \$12 billion in 2008 – triple the 2007 estimated amount. And yet, 64% of online pharmacies in the second quarter of 2008 had no privacy protections for consumers. Only two out of 2986 online pharmacies were VIPPS certified¹. Clearly, pharmaceutical spam generates tremendous amounts of illicit cash – and represents only one “business opportunity” among many.

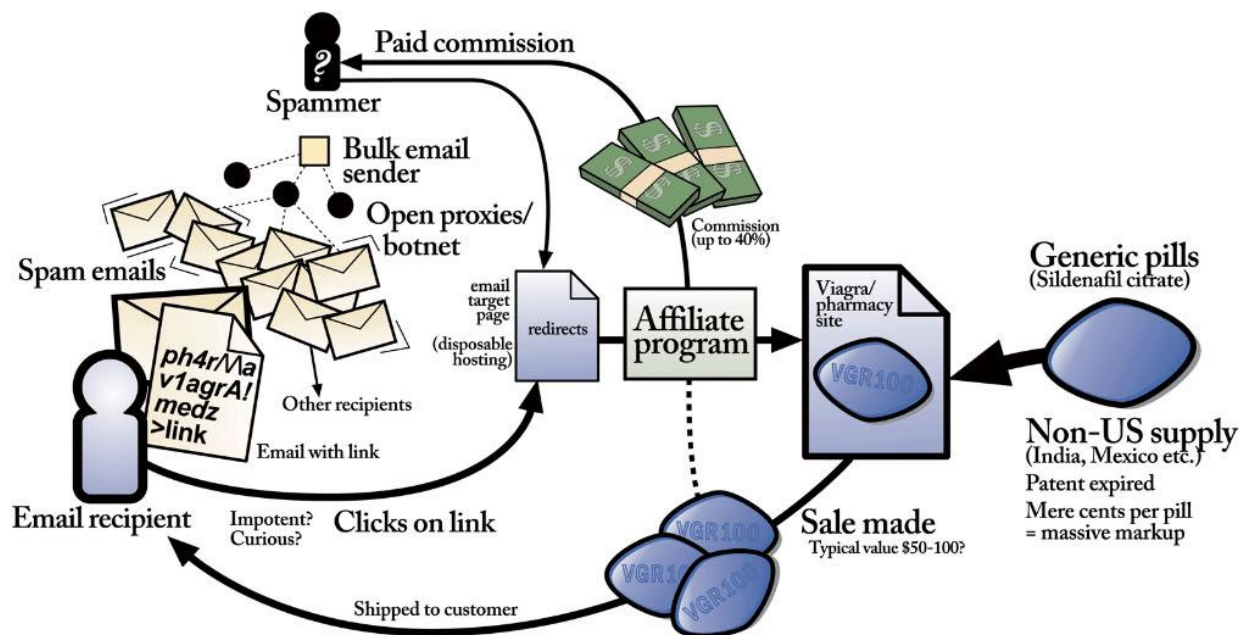


Figure 1: Pharmaceutical spam as a complex, closed-loop business cycle².

However, as the margins for spam have decreased, botmasters have developed other ways to derive income from other aspects of the business cycle. For example, spammers now market “broadcast email” tools and services to legitimate businesses. Whether these applications constitute spam or not is often open to local interpretation. Illegal activity in one country may not be considered criminal in another. As botnet technology becomes increasingly widespread, lower in risk and easily hidden, it becomes much more difficult to determine where the actual “crime” takes place – or even if actually takes place at all from a legal perspective.

In other words, botnets now operate in a mode similar to legitimate multinational businesses. They contain varied distribution channels, local agents, multilingual services, sophisticated marketing, affiliate programs, technical support – even performance guarantees. This democratization of online crime means that malicious activity such as spam is no longer just the domain of the professional criminal organizations that write their own malware and run their own botnets.

Ease of use and wide accessibility mean that almost anyone can get into the game. Even worse, botnet tools produce legitimate business results, which helps blur the line between proper and criminal activity. These efforts may originate on criminal networks, but the nature of botnets means that spam, malicious attacks or malware propagation efforts are as likely to come from internal hosts, compromised systems at customers or trusted partners as anywhere else. These resources may be controlled by botnet controllers, but businesses cannot block or control them without damaging their own commercial interests.

¹ MarkMonitor’s Summer 2008 Brandjacking Index

² <http://www.modernlifeisrubbish.co.uk>

Political and social action organizations add another twist to the challenge. The line between unsolicited email and spam is a fine one. These entities can use spam tools – intentionally or not – and then use freedom of speech and similar objections to resist being shut down. Likewise, some countries freely allow spam and other botnet operations to be hosted within their borders as a spur for economic activity.

Finally, this business model shifts the risks of liability onto the victims whose hosts have been compromised. Enterprise organizations that tolerate spamming botnets risk having their entire domains becoming blacklisted and legitimate email being rejected by customers and partners. Even worse, criminal liability for spamming in the U.S. lies with the server providing the spam. Any enterprise that allows spam botnets to take root on its hosts risks heavy fines and embarrassing publicity. The situation only gets worse for data theft, Denial of Service attacks and other malicious activities.

The end result is that botnets have rapidly evolved into a very complex, very successful engine for generating cash. What has already taken place within the spam market is now a proven, robust formula for success. Criminal organizations no longer need to control the entire “supply chain” in order to make money. As a result, it is more than reasonable to expect that structures similar to the spam ecosystem will soon appear for any other action that a botnet can be programmed to take.

A Closer Look at How Spam Botnets Operate

Spam is not what most people think it is. Well, actually, it is. But how it arrives in the inbox has undergone subtle but significant changes as network and host filters have become more effective. For example, fewer spam messages now arrive using images to encourage viewers to click on a link. Instead, the goal is to get viewers to click on a text-based URL. The text link is more likely to evade antispam filters, and the Web page that gets called is much less likely to trip antiphishing or other defenses. It is at this stage that drive-by malware installation is likely to take place, even for sites that represent “legitimate” business operations.

The domains behind these URLs change very rapidly – as often as 97% within a week³. In addition, many well-known and trusted domains have been compromised as part of a coordinated spamming effort (e.g., blogspot, doubleclick, cnn, msn/msnbs, bbc). Trusted domain names help evade spam filters and fool suspicious users. The growth in the use of fraudulent “legitimate” domains indicates that the tactic is successful.

Simple market economics drive this evolution. Spam makes money. So the volume of spam increases constantly. Businesses and individuals who do not want to receive spam respond with improved defenses. A constant stream of botnet innovation ensures that the cash flows unabated. For example, image-based spam increased to 75% of the level of URL-based spam in early 2007. However, that percentage decreased to near-zero by the end of the year⁴.

The range of spam subjects continues to widen in order to enhance success. For example, one recent survey allocated spam according to the following breakdown⁵:

- 62% Russian spam
- 18% Advertisements
- 6% Adult services
- 5% Products & services
- 4% Stock
- 1% Financial
- 1% IT
- >1% Chinese spam
- >1% Surveys

³ IBM Internet Security Systems X-Force® 2008 Trend & Risk Report

⁴ IBM Internet Security Systems X-Force® 2008 Trend & Risk Report

⁵ McAfee

The subject lines within each spam message have also become more sophisticated. Topical information, such as holidays and breaking news, now accompany more traditional porn, sexual performance and pharmaceutical come-ons. These subject lines are automatically randomized, which increases their chances of evading spam filtering systems.

Commercial spam kits feature polished graphical interfaces and point-and-click simplicity. The inevitable result is that the number of people launching spam botnets has skyrocketed. Many of these kits are built and resold by the same organizations that create and promote “professional” botnets. Not only do these efforts generate additional revenue, they also create widespread proliferation that complicates efforts to identify any single criminal element within a much larger whole.

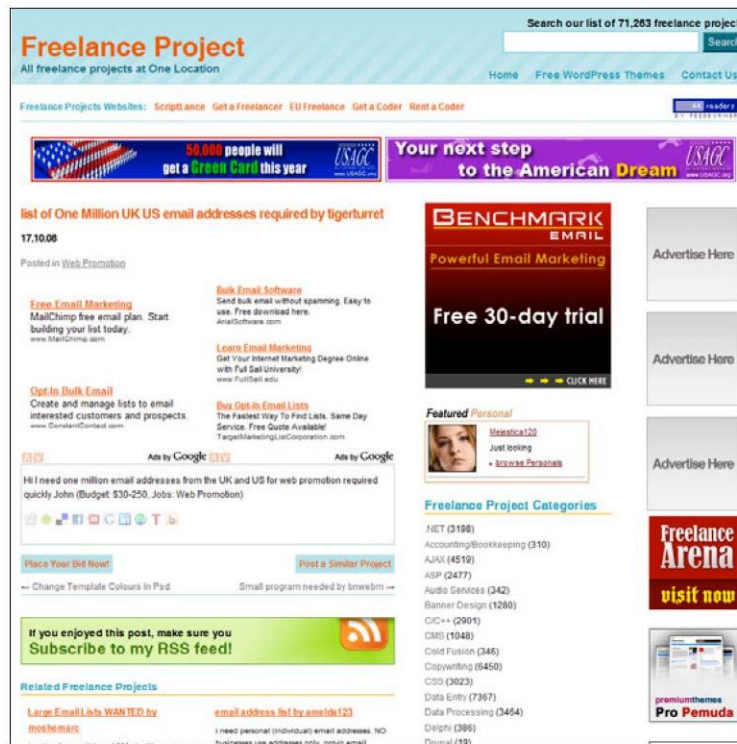


Figure 2: A Web site promoting spam as a freelance employment opportunity, complete with resources for low-cost email lists.

Of course, spam works best when the email distribution lists reach real people. Some spam engines still create random email addresses and hope that a sufficient number reach actual viewers. Proven email addresses are more valuable. For that reason, hosts compromised with spam malware frequently also host screen scrapers and keystroke loggers – or coordinate efforts with systems compromised with this malware – in order to generate lists of “live” addresses that can be sold at a premium price.

The typical rate for these lists range from \$5 to \$45 per million email addresses⁶. The rate depends on the quality of the address, where in the world it is located, if it was verified as “alive” within the previous 10 days, and that it has been tested and proven not to belong to any sort of seeded antispam program. 30% of the world’s spam originates in the United States, Russia or Turkey, but that leaves 70% that can come from anywhere with an Internet connection⁷.

⁶ Damballa, Inc.

⁷ IBM Internet Security Systems X-Force® 2008 Trend & Risk Report

Messages can be targeted by language and local custom. Spam purveyors even provide translation services and outsourcing of multilingual messaging, complete with special rates for rush jobs. It is yet one more means to generate revenue.

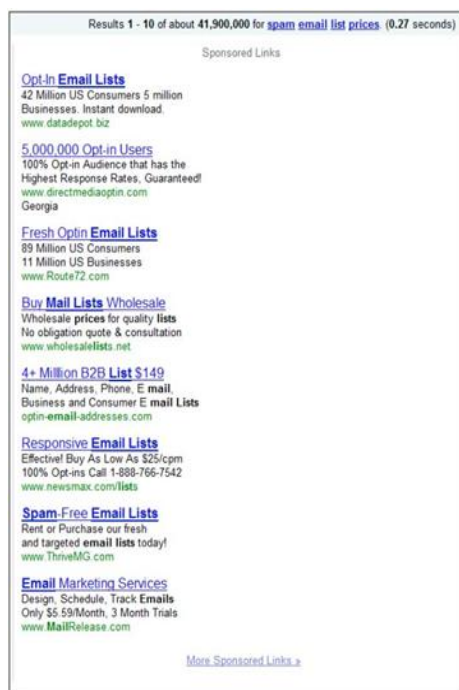


Figure 3: Email address lists at commodity prices are easily found via popular search engines.

Spam also is a hosted service, just like Web sites or blogs. In fact, these services are widely advertised on locations such as porn or social networking sites. This submarket is often structured like direct sales affiliate programs. The goal is to recruit large numbers of contractors who send a portion of their own sales to the person at the top of the chain. In many ways, it is Avon or Amway for spam, complete with online tools to monitor and manage the affiliate network.

The botnets themselves can be bought, sold or leased, with an active market for each possibility. Aggregators purchase smaller botnets so that the larger collection has greater impact. Professional botnet controllers sell or lease out access, as well as anonymity services. As with everything else in the spam business, each variation introduces yet another means to make money.

One of the latest developments in spam hosting is the availability of "bulletproof" hosts. These service providers, mostly based in China, allow spammers to send as much spam as they like for as little as \$700 dollars, and actively and effectively defend their customers against attempts to shut down the source of the spam. Bulletproof domains are available for as little as \$100⁸.

⁸ In China, \$700 Puts a Spammer in Business, CIO.com, May 8, 2009

Worldwide Email Addresses.com

HOME CONTACT FAQ PRODUCTS TESTIMONIALS OPT-IN CATEGORIES MEMBERS

Sign up for your FREE 7 part website traffic course, valued at £97

FREE

* Your first name:

* Your primary email address:

[Yes! Send me my FREE 7 part website traffic course.](#)

Your details will never be shared and you can remove them at any time.

1 billion

Worldwide Email Addresses.
Fresh. Real. Valid. Unduplicated.
Double Opt-in. Updated 24/7. 100% Legal to use.
Fully categorized by interests and geographical location.

BUY NOW
CLICK HERE

MEN GAMES MUSIC SPORT NEWS WOMEN

EXAMPLE INTERESTS

EXAMPLE COUNTRIES

Click here for a full list of our countries and interests.

Stop wasting your money using traditional advertising or expensive single email blasts.

Email 1 billion targeted consumers again and again, and watch your profits grow, with us.

WHAT YOU GET

- * Lifetime membership for a one-off payment
- * Fully licensed email senders and list managers
- * User friendly member's area interface
- * The highest quality double opt-in email list on the market
- * No risk with your internet service provider (ISP). Our bulk email senders have powerful direct send abilities and bypass your ISP's mail server.
- * Zero undeliverable email return messages
- * Plain text or HTML, (allowing for images and video) email message choice
- * Outlook-like user interfaces for ease of use. Anyone can set it up in just a few minutes
- * No spam complaints and no hassle
- * Our email lists are 100% Double Opt-in, updated 24/7 and 100% Legal to use.

One of the most powerful and cost effective advertising methods in the world, which can increase your profits 1200%+ overnight!

We will give you the means to contact millions of people who want to hear about your products.

*Data taken from our clients

Send tomorrow

Download. Choose a category. Send.
The simplest marketing tool available.

3 steps. That is all you need to get your message to millions of potential customers who want to hear about your product. **DOWNLOAD** one of our packages, which includes upto a billion categorized email addresses as well as a powerful email blaster that will do all the sending for you. **CHOOSE A CATEGORY** - interest or geographical location - and then **SEND**. And remember, you can do this as many times as you like because, unlike other services, we only charge you at step 1 not step 3.

OUR PACKAGES

With all our packages you get:
LIFETIME MEMBERSHIP from a ONE-OFF PAYMENT which means NO FUTURE FEES

<p>SILVER</p> <p>250 million email addresses new Fully licensed email senders</p> <p>£45 £100</p> <p>BUY NOW</p> <p><small>Click here for more details.</small></p>	<p>GOLD</p> <p>500 million email addresses new Fully licensed email senders</p> <p>£70 £152</p> <p>BUY NOW</p> <p><small>Click here for more details.</small></p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

PLATINUM

1 billion email addresses
new Fully licensed email senders

£115 ~~\$255~~

Lifetime membership **BUY NOW** One-off payment

Click here for more details.

"Many business people are finding out that they can now advertise in ways that they never could have afforded in the past. The cost of sending mass e-mail is extremely low, and the response rate is high and quick." - USA TODAY

I got \$87 million in Google ads!
Made me \$200 million fast. You can too.

£1 Billion in Page Ads
Generated in 24 Hours
See How You Can Do It Too
http://www.damballa.com

Terms and Conditions

Figure 4: Professional one-stop-shop Web site that promotes spam as a legitimate business opportunity.

Each of these tactics easily apply to any potential use of a botnet, such as the sale of credit card numbers, login credentials, social security numbers, customers lists, trade secrets – even the sale and lease of botnet malware and botnet segments themselves. What already exists inside the spam industry will undoubtedly arrive soon for all of these other “markets,” if for no other reason than the infrastructure already exists and has proven its ongoing value.

In short, botnet-generated spam is nothing more than the foundation for a wide range of other malicious activities. The advantages of this approach (for botmasters) are compelling:

- High margin, low risk opportunities
- A proven business model that capitalizes on existing infrastructure investment
- Highly sophisticated business cycle with multiple sources of income
- Widely distributed risk, with multiple layers of buffer between buyer and seller across the entire supply chain
- High levels of tolerance for spam activity on enterprise and personal systems

In short, botmasters will continue to take advantage how rapidly botnets can be repurposed for other uses, and how ineffective most traditional security techniques are at stopping them. For example, botnets increasingly will seek valuable and confidential corporate data, with an open, illicit market for trading access and information. It will be just as difficult to stop these intrusions as it is to stop spam, unless businesses take a different approach to combating the problem.

Conclusion

The success of botnet-driven spam has created a stable, sophisticated and robust infrastructure that can be applied to a wide variety of malicious uses. This complex, highly evolved business ecosystem generates revenue across multiple touch points, minimizes risk by distributing it across the entire ecosystem, co-opts legitimate businesses into the criminal framework and generates huge amounts of cash.

What this development means for businesses is that botnets cannot be contained in the same way that organizations fight viruses and hackers. The key to success is to shift gears from a narrow definition of malicious activity, such as malware identification or spam transmission. Instead, security staff needs the ability to understand how botnets communicate, ranging from each compromised system to the botnet controllers themselves. These communications are the only constant within the world of a botnet, and so present each botnet's greatest vulnerability, regardless of malware employed or what the bot has been instructed to do.

The quality of this information is as important as the quantity. In other words, defining "good" and "bad" is relatively straight forward. However, much of the activity generated by a botnet is merely suspicious. Any effective anti-botnet solution must be able to quickly, automatically and accurately collect as much evidence as possible, then communicate a "verdict" that gives administrators the insight they need to identify a potential botnet compromise within the enterprise.

It is on these three components – speed, accuracy and automation – where traditional defenses such as antivirus and intrusion prevention fall short. These tools, as proven and invaluable as they might be, fail miserably at identifying internal compromises, isolating external attempts to communicate with internal resources, and recognizing when internal systems attempt to communicate with external botnet elements.

The reasons behind these failures are not complicated. Tools such as antivirus and intrusion prevention depend primarily on techniques such as signature databases that take time to implement. Compromised systems automatically change their malware payload as often as every 30 minutes. Each botnet may comprise tens of thousands of discrete types of malware, many of which will never be identified or analyzed by any security vendor. Malware traffic itself insinuates easily and transparently into normal network operations. Deep protocol analysis may help uncover some aspects of botnet activity, but only at the expense of overall network performance.

Damballa's anti-botnet solutions directly address these limitations, with a detection and remediation regimen that builds on the weaknesses inherent in botnet Command-and-Control (C&C) to quickly, accurately and automatically identify and remediate botnet activity. These solutions work even in the absence of a positive malware identification, to provide real-time protection against botnets, regardless of whether the botnet produces spam or something else that's significantly more malicious.

About Damballa

Damballa is a pioneer in the fight against cybercrime. Damballa provides the only network security solution that detects the remote control communication that criminals use to breach networks to steal corporate data and intellectual property, and conduct espionage or other fraudulent transactions. Patent-pending solutions from Damballa protect networks with any type of server or endpoint device including PCs, Macs, Unix, smartphones, mobile and embedded systems. Damballa customers include mid-size and large enterprises that represent every major market, telecommunications and Internet service providers, universities, and government agencies. Privately held, Damballa is headquartered in Atlanta. <http://www.damballa.com>

*Prepared by:
Damballa Inc.
<http://www.damballa.com>
Copyright 2012. All rights reserved worldwide.*