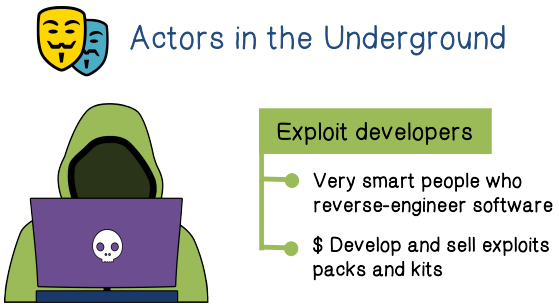
The recommended readings for this lesson are:

Spamalytics: An Empirical Analysis of Spam Marketing Conversion

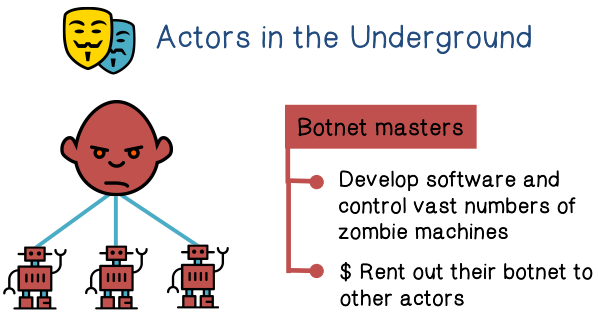
PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs

You can find the short summaries of the papers at the end of the document.

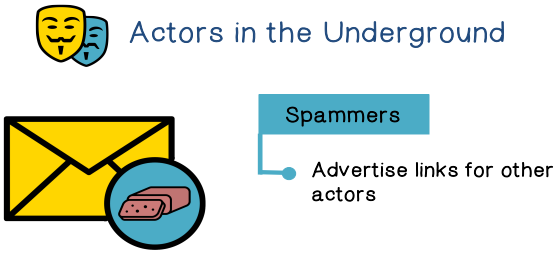
In this lesson, we will examine cybercrime, its economy, and some of the motivations of the players. When you finish this lesson, you should have a much better understanding of where legitimate Internet commerce ends and Internet crime begins.



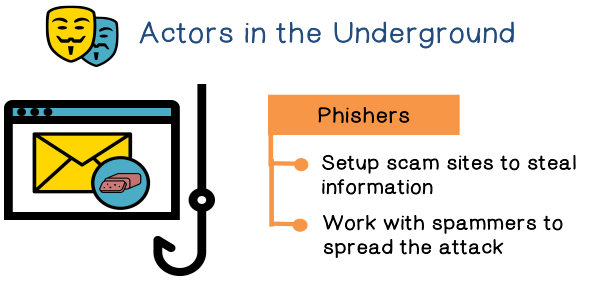
Now let's talk about underground economy. To understand the underground economy of cybercrimes we have to first understand who the actors are in the underground. The first are the ones who write exploits. They discover bugs that can be exploited to cause security compromise and they sell them for a profit.



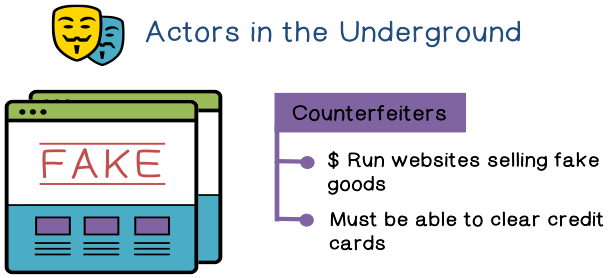
Then there are the botnet masters, or bad guys that create and operate a malicious network composed of compromised computers. Essentially, they buy exploits and turn them into malware and they put in the botnet command and control components. So, when they release the malware, they have a botnet under their control. Then they rent out the botnet to other bad actors for malicious and fraudulent activities.



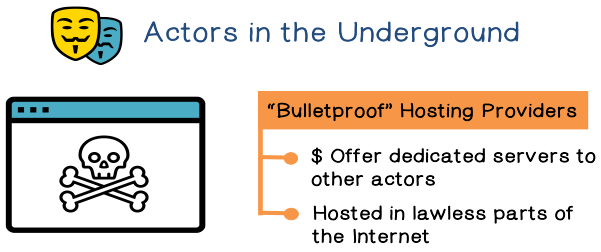
One of the utilities of a botnet is to send spam. And so the bot master of a botnet can simply rent out his botnet to a spammer, and the spammer in turn sends out a spam contents on behalf of other bad actors.



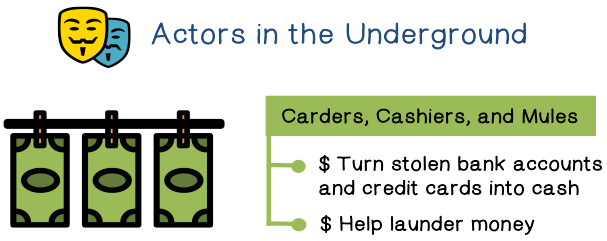
One type of bad actors that can use the help of spammers are the phishers. They set up scam sites to steal information and they ask the spammers to send the URL's to victim users to the scam sites.



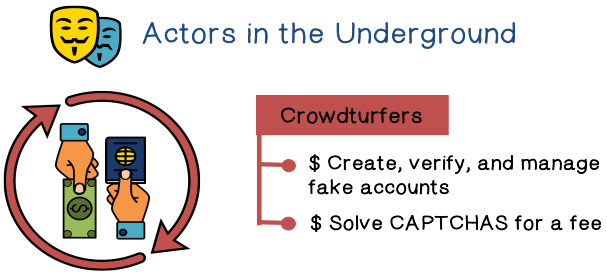
Similarly, counterfeiters use spams to sell their counterfeit goods and obviously, they need to be able to collect money from the victim users. For example, from their credit cards.



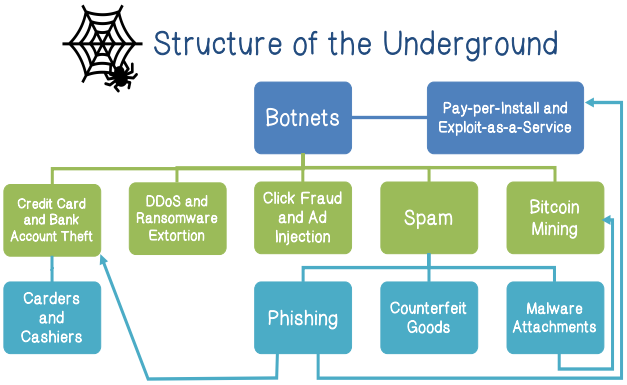
A bad actor in a cyberspace needs to consider the possibility that his operation, in particular, his websites, may be detected and shut down by the law enforcement. And so, he needs to find a so-called bulletproof hosting providers. These providers typically operate in lawless places and they are expensive.



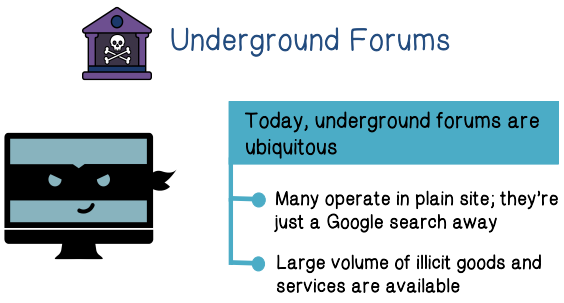
A majority of the bad actors are in it for the money. And on the Internet, what they can steal are the bank accounts and credit cards. And so, they need to turn them into cash. They allow carders, cashiers, and mules to do just that.



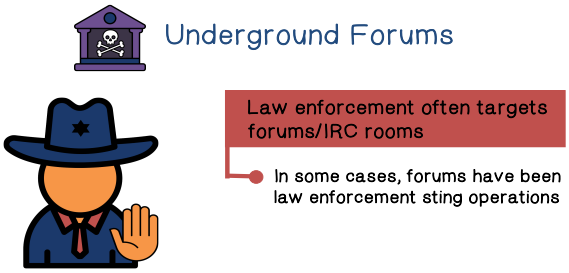
The crowdturfers leverage human powered crowd sourcing platforms to create and manage fake accounts that are not tied to real users. And they can use crowd sourcing to solve CAPTCHAs.



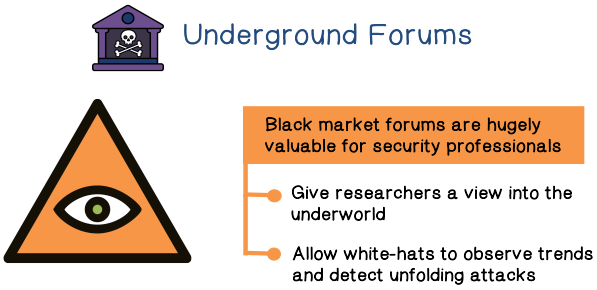
As we have discussed, there are quite a few types of bad actors in the cyber space and they form an interconnected ecosystem. For example, a botnet is created when computers are compromised and a malware is installed. A botnet is used to launch a number of malicious and fraudulent activities. For example, these are activities that can be launched by botnet, in particular, spam. Spam can be used to facilitate a number of other activities such as phishing, selling counterfeit goods or malware installation. Again, the point here is that the bad actors form an interconnected ecosystem because their activities or infrastructures support each other.



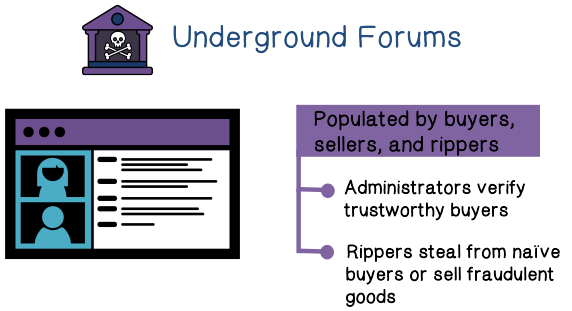
Underground forums are one of the entry points of the bad guy's communication systems, especially for those new to the underground. There are many underground forums on the Internet. And they are just one search and one click away. And there are a large number of illicit activities being advertised on these forums.



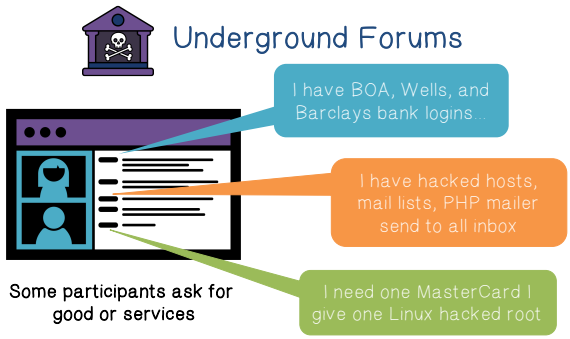
Obviously law enforcements are watching and can shut down these sites. However, new forums can always pop up and fill the void.



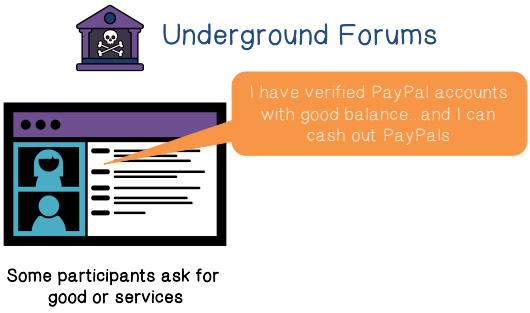
These forums also provide valuable data sources to researchers. For example, researchers can study the data to learn about new trends and detect unfolding attacks.



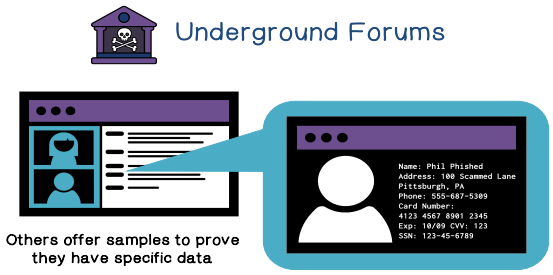
The forums are full of buyers, sellers, and the rippers. There are honest deal makings but there are also rip-offs of the buyers. Basically, these forums are as regulated as what administrators can handle.



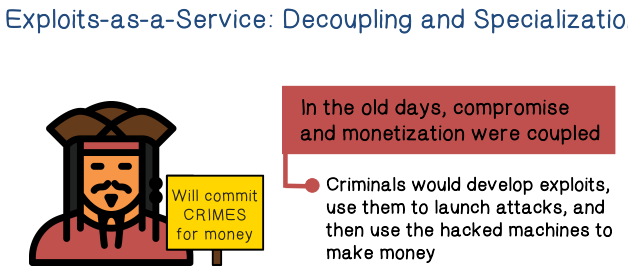
Most messages on the forums are just advertisements. For example, one can advertise that he has stolen bank accounts or access to computers or email lists. Or one can ask for stolen credit card numbers in exchange for access to a hacked Linux machine.



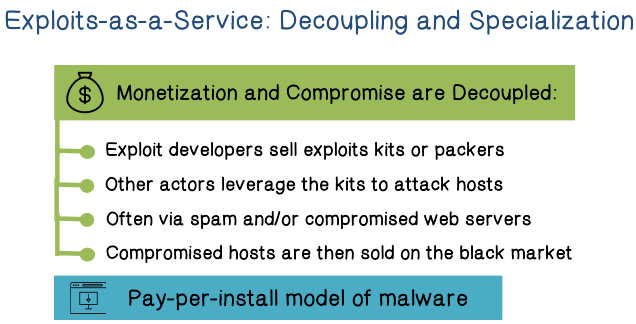
Many of these advertisements include evidence of the advertisers capabilities, for example, to demonstrate that the stolen accounts are valid



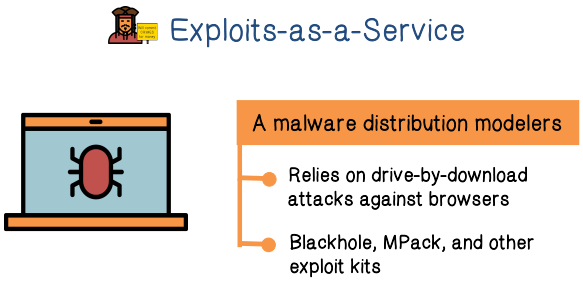
Or they show samples of the stolen information. Again, the forum is typically used for advertisement. The actual due-making is typically done via private messaging.



Now let us discuss a few underground activities. The first is Exploits-as-a-Service. In the past, compromising computer systems and using them for profit are typically done by the same criminal or criminals gangs. For example, the same criminal gangs will develop their own exploits, launch them, and then use the hacked machines to make money.

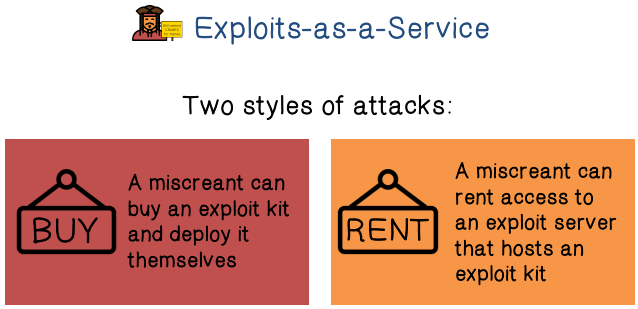


Nowadays, the bad guys are specialized and do different functions. For example, there are developers who develop exploit kits and packets, and sell them to other bad guys. And the other bad guys are responsible for using these exploit kits to compromise computers. For example, they can send out spam with malware attachment. Or they can put the malware in a compromised web servers, so that when a victim's computer visit those servers, they will be compromised. These compromised computers are then sold on the black market so that other bad guys can use them to launch malicious and fraudulent activities. And the bad actors here are being paid using the pay-per-install model.

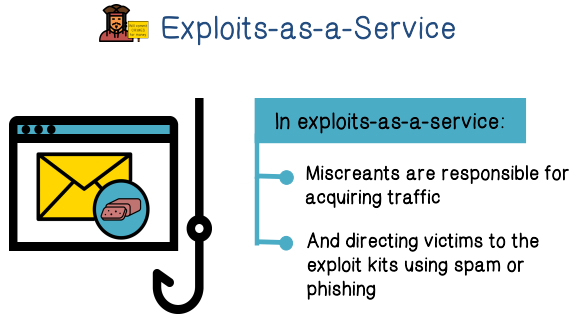


Let us discuss exploits-as-a-service, and in particular, the pay-per-install model in more details. One way to distribute malware, or causing computers to be compromised by the malware, is through

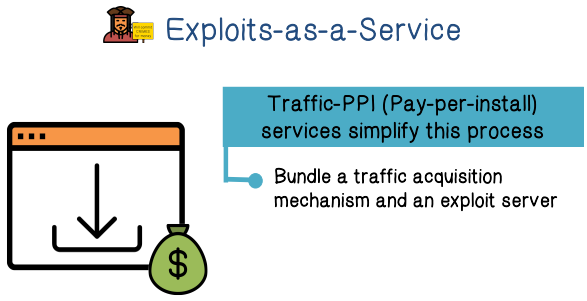
so called drive-by-download. Basically a website is compromised to have malware embedded in their scripts. And then when a client computer visits the website, the malware will be installed on the computer. The exploit kits are responsible for packaging the malware, and installing the malware on the client computers.



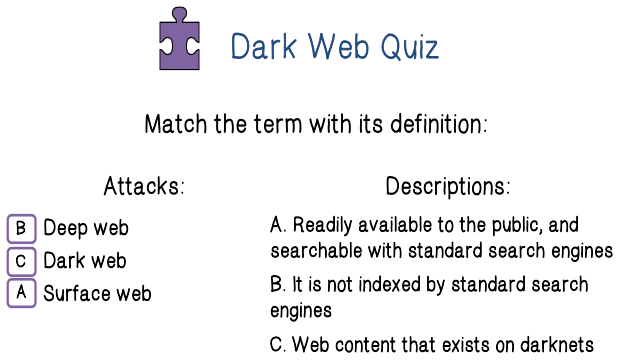
There are two components in this malware distribution model. The first is that the bad guy needs the exploit kit because the exploit kit will be responsible for installing the malware on the victim computers. The bad guys can buy an exploit kit and deploy it themselves. Or, they can simply rent access to an exploit server that hosts the exploit kit. In the first option, the bad guy needs to figure out how to distribute the malware themselves, and typically that means at least he has to set up a server with exploit kits. A more convenient option is for the bad guy to rent access to a server that already hosts an exploit kit.



The second component of this malware distribution model is that the bad guy needs to have the victims' computers visit the exploit server so that malware will be installed on these computers. The most common way to accomplish this is to use spam or phishing to attract traffic to this exploit server.

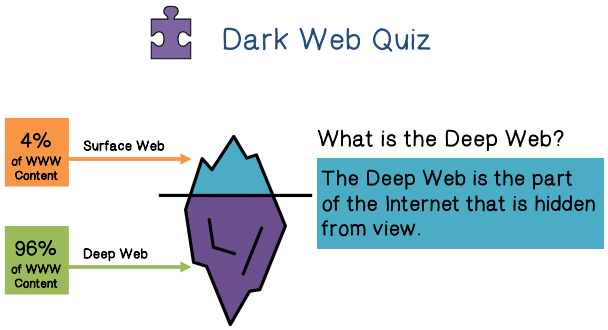


Traffic pay-per-install simplifies this malware dispersion process. It essentially combines the two elements into a single service. And pay-per-install is now the most popular way of distributing malware.

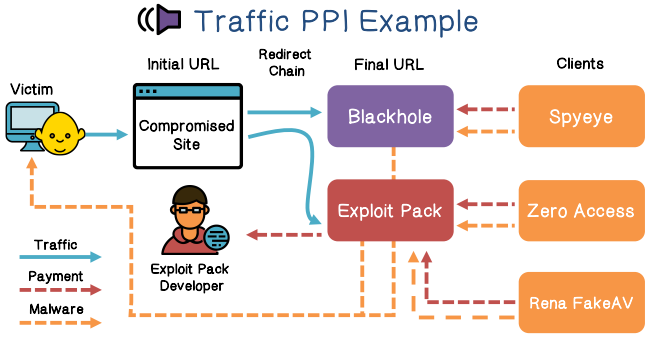


The fact that there are so many underground forums and malware sites on the internet, it is just one example that the web actually has multiple facets. So, let's do a quiz, match the term with its definition.

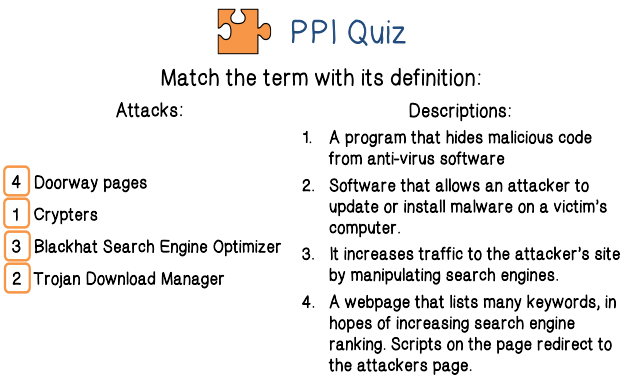
A deep web is one that is not indexed by the standard search engines such as Google. A dark web refers to also invisible web or hidden web where the web content typically only exists on so-called darknets. And so what is a darknet? It is an overlay network that can only be accessed with specific software, configurations or authorization, often using non-standard communication protocols and ports. Two example darknets are the friend-to-friend peer-to-peer networks and the privacy-protection network such as Tor. And a surface web is one that we are probably most familiar with. It contains web contents that are public, searchable and indexed by standard search engines.



When we think of the Internet we are usually referring to the surface web. As you can see in this visual, the surface web is actually a very small part of the Internet.

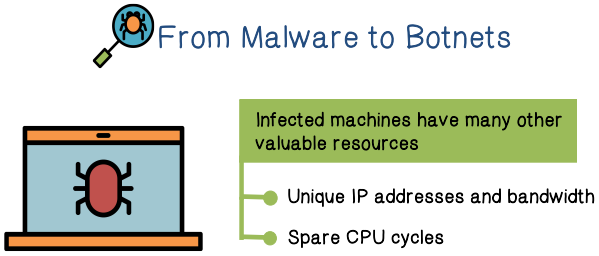


Let us look at a traffic-per-install example. There are three classes of actors in traffic-per-install. There are the victims, the exploit developers, and the clients, or bad guys that use the exploits to dispute malware. If we look at the traffic flow, we notice that the payment flows from the clients or the bad guys who buy or rent the exploits to exploit developers. The malware flows from these attackers to the victims. The payment amount depends on the volume of malware installation.

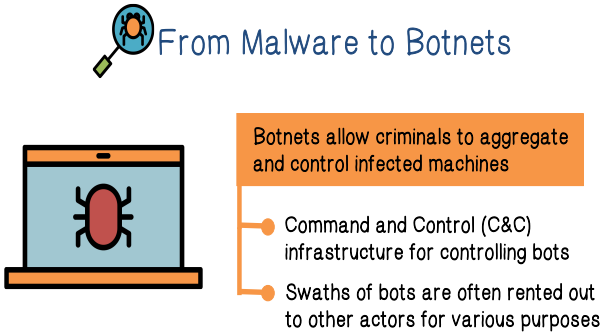


Now let's do a quiz on pay-per-install. Match the term with its definition.

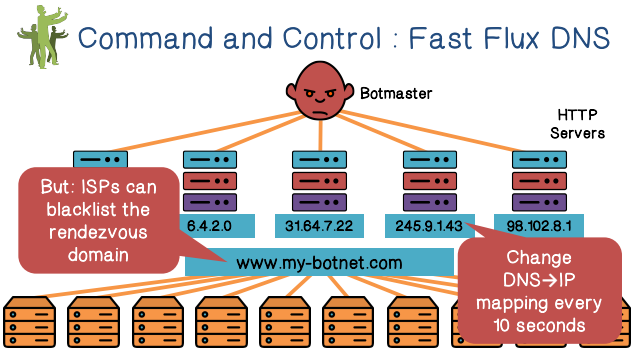
A doorway page is a web page that lists many keywords in hopes of increasing search engine ranking. And then, scripts on that page will redirect the visit to attacker's website. A crypter is a program that hides malicious code from anti-virus software. A Blackhat Search Engine Optimizer, or Blackhat SEO, is one that tries to increase traffic to the attacker's website by manipulating search engines. A Trojan Download Manager is a piece of software that allows an attacker to update or install malware on a victim's computer.



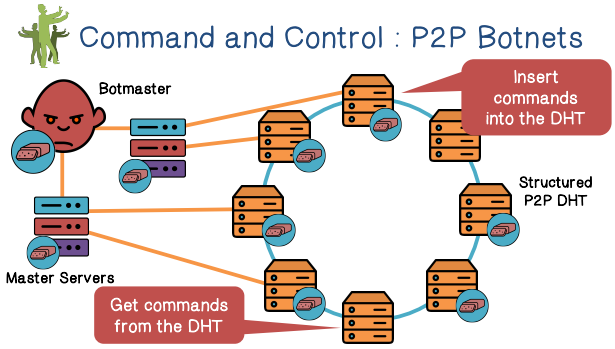
So, we have just discussed how malware can be distributed and installed on victim's computers. These infected computers are valuable resources. For example, they have a unique IP addresses and bandwidth, and they are typically distributed across the internet. And they have spare CPU cycles that can perform a wide range of activities. From an attacker's point of view he wants to control and utilize these infected machines and the way to do this is to turn the compromised computers into a botnet.



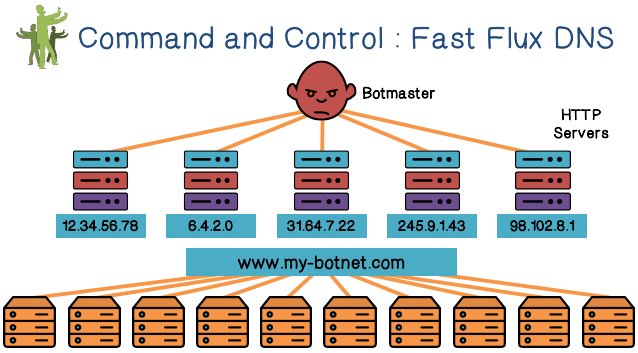
The bad guy or the botmonster will need a command-and-control infrastructure to control the bots. For example, he can then ask every bot to update its malware or can send commands to the bots to launch synchronized activities. And the botnet can be rented out to other bad guys to launch their activities, such as sending spams. Once in place, the botnet now becomes a platform to launch any number of malicious and fraudulent activities.



The key to a botnet's success is efficient and robust command-and-control. And this is not always easy. The simplest, most efficient way to perform command control is through centralized control. For example, through IRC commands, the botmaster can instruct the bots to send spam. However, this kind of command-and-control is not robust, even though it is very efficient, because it has a single point of failure. There is only one command channel from the attacker. For example, the IRC channel can be taken down. Or the twitter account used for command-and-control can be shut down.



A more robust command-and-control structure is to use peer-to-peer network. Here, the botmaster can connect to a number of bots in this peer-to-peer network, and upload his commands, and update to the malware, and make advertisements, so that other bots can get the commands and updates from the peers. The drawback is that the botmaster does not have a direct, synchronized communication with other bots. In fact, the botmaster does not know how many bots will get his commands and when.

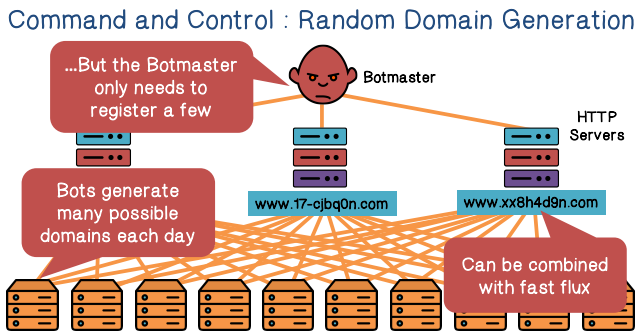


Nowadays, the most popular approach for command control is for all the bots to connect to a command-and-control website. Obviously, this is very efficient. And the botmaster can make this setup more robust. For example, the botmaster can map this website to different IP addresses. The website is not always fixed on one physical server. It can be moved to different servers.

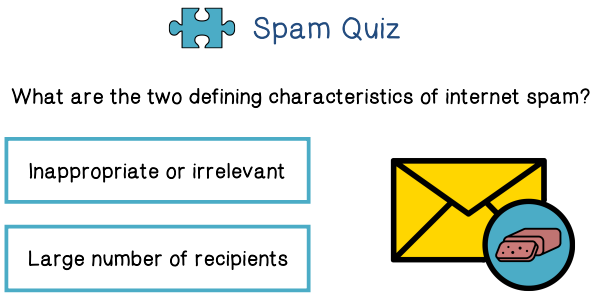
In fact, in Fast Flux, the botmaster can change the DNS IP mapping for the website every few

seconds. This can defeat detection or blocking based on IP addresses. But since the domain name is not changed, this domain can still be detected as being used for botnet command control. And the ISPs can block access to this domain.

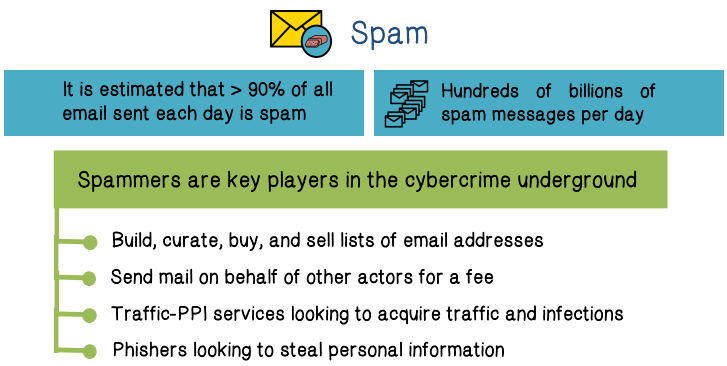
Instead of using fixed domains that can be detected and blocked. Botmasters now used random domain generation. On each day, a bot will generate a large number of random-looking domain names and lock them up. The botmaster will know exactly the same set of random domains each day because each domain are generated using the same algorithm and the same random seed is shared between the botmaster and the bot malware. The botmaster only registers a few of these random domains. Although each bot generates many randomly looking domain names, and looks up each of them, only a few of them will actually connect to the websites. These are the sites that are registered by the botmaster. And of course, these sites can use fast flux to move around on the Internet by mapping to different IP addresses every few seconds. This command and control approach is very robust, because it is hard for detection. This is because each of these command-and-control domains are random-looking. And they're new, and they are only used for a very short period of time, say, one day.



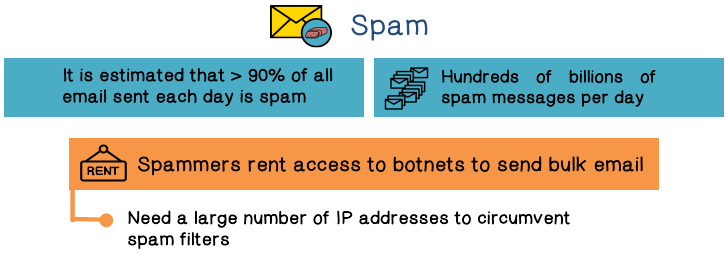
Let's do a quiz on spam. What are the two defining characteristics of internet spam?



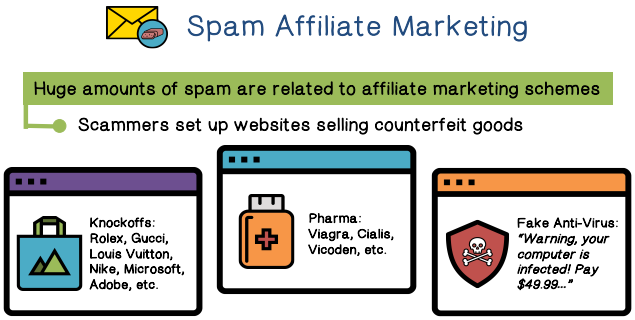
They are typically inappropriate or irrelevant to the user and typically it's being sent to a large number of recipients.



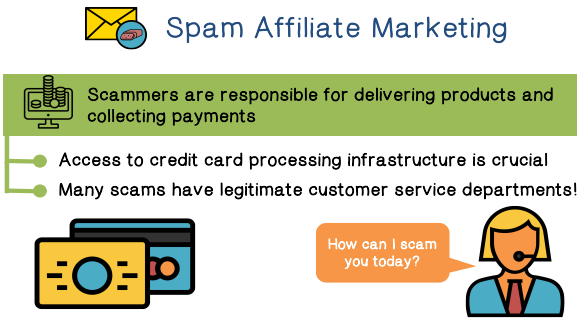
It is estimated that more than 90% of our email are actually spam. That will translate into hundreds of billions of spam messages every day. Spammers play a very key role in the underground economy and cybercrime. They have contacts of many, many people and many organizations. They send messages on behalf of other bad actors. They can be used to push malware or phish to steal information.



Spammers typically use botnets to send spam. They need a large number of IP addresses because otherwise, sending a large number of emails from a few IP addresses will easily trigger detection and blocking by spam filters.

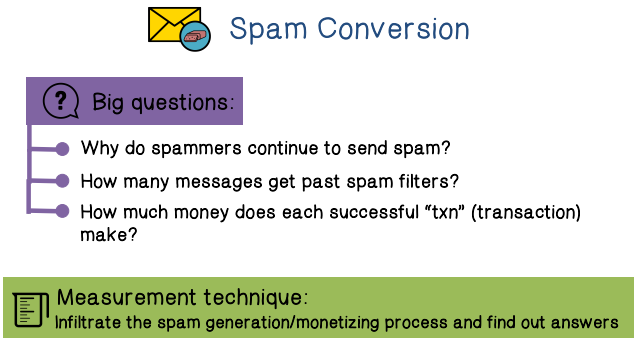


Let's start with a few examples of how spam works in the underground economy. Many spammers are affiliates of various kinds of scam campaigns. Scammers typically set up websites to sell counterfeit goods.

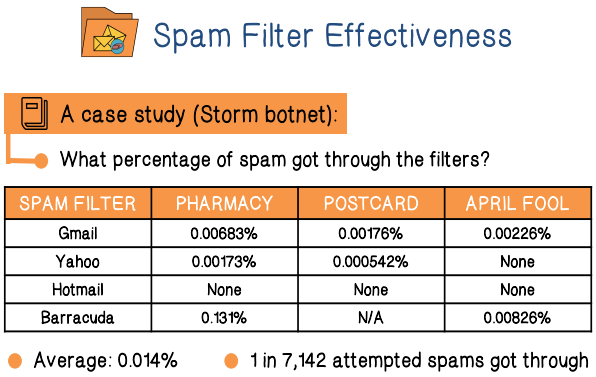


The scammers try to act legitimately by delivering goods and collecting payments. They can even have customer services.

But how do the scam websites attract traffic? They need the spammers to advertise for them. And in return, the spammers collect commissions. For example, the commission can be as high as 30% to 50% of the final sales price.

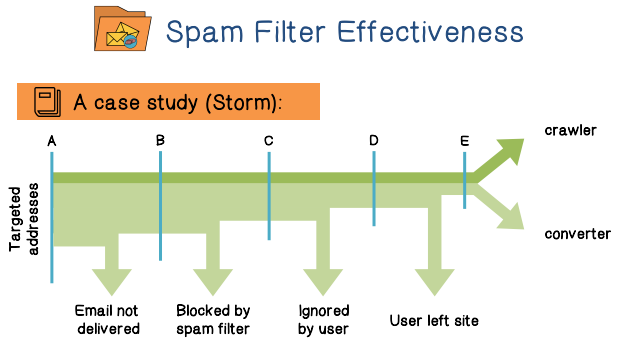


Now the key to the success of both the scammers and the spammers is the spam conversion rate. The spam conversion rate is the percentage of spam messages that result in a final sale. We know that there are spam filters around. And we have the feeling that a lot of them are very effective. So why do spammers continue to send spam? And how many messages get past spam filters? We heard numbers such as more than 99% of the spams are filtered. How many spams lead to successful transactions? How much money can be made? The only way to precisely answer these questions is to infiltrate and instrument the spam generation and monetization process because by doing so we can find out exactly what is going on.

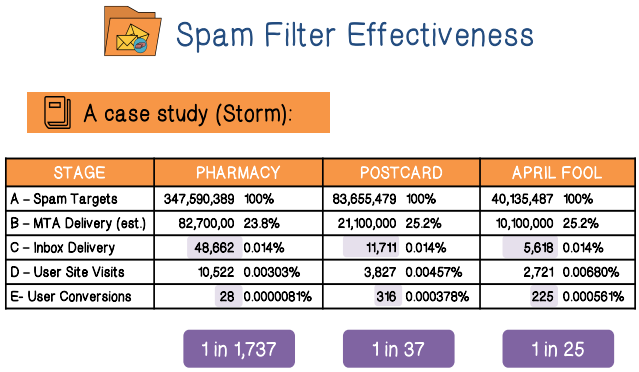


SPAM FILTER	PHARMACY	POSTCARD	APRIL FOOL
Gmail	0.00683%	0.00176%	0.00226%
Yahoo	0.00173%	0.000542%	None
Hotmail	None	None	None
Barracuda	0.131%	N/A	0.00826%

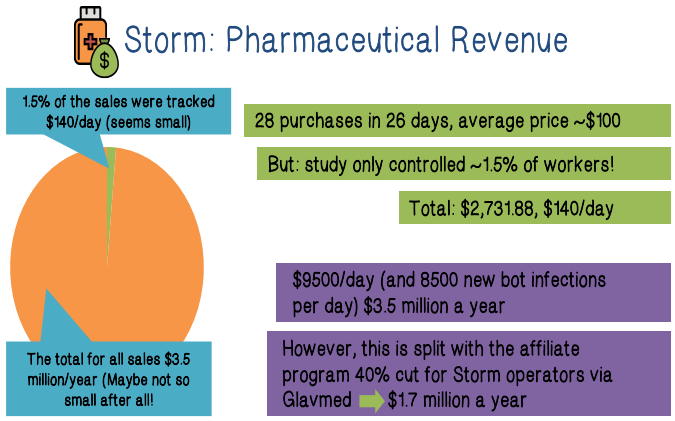
Let us discuss a case study on the Storm botnet. This botnet was used to send spams. And this research was performed by the University of California in San Diego, where the researchers penetrated into the Storm botnet. The researchers were able to measure the percentage of spam that got through the spam filters. Here are different campaigns carried out by the spams. Pharmacy is a spam advertising an online pharmacy. The postcard and April Fool campaigns are for installing malware. As we can see here from data that is available, there are spam filters that can actually filter out more than 99% of the spam messages. On average, only 0.014% of the spam messages can get through the filters, which translates into 1 in more than 7,000.



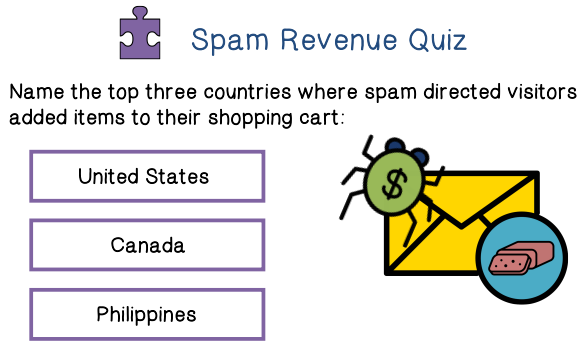
Looking at the whole lifecycle of a spam message, some are not delivered, some get blocked by spam filters, some are ignored by the users, and users may just leave the sites. Of course, some of them will actually commit a transaction. But some of these traffics are due to crawlers, meaning that they are not actual users.



This table shows that for each campaign, the percentage of spams that can be delivered, filtered, result in user visiting the website, and user conversion. Obviously, user conversion is the most interesting number that we should look at. For pharmacy, it is 1 in 1,737. For postcard, it is 1 in 37. For April Fool, it is 1 in 25. This conversion rate is computed for the spams that got into the user's inbox, i.e., how many of them result in user transactions.

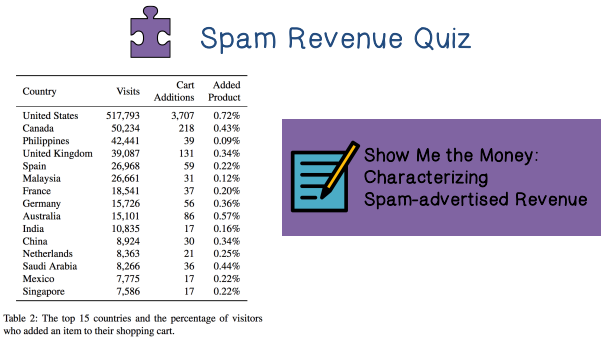


The pharmacy campaign advertises a fake online pharmacy. The researchers observed that there were 28 purchases in 26 days. The average price per purchase is $100. But the researchers only controlled 1.5% of the bots sending the spams. If we extrapolate this amount to the whole botnet population, then we get close to $9500 a day, or $3.5 million a year. Of course, the scammer and spammer will divide up this money. So, the Storm operators or the spammers will get $1.7 million a year.

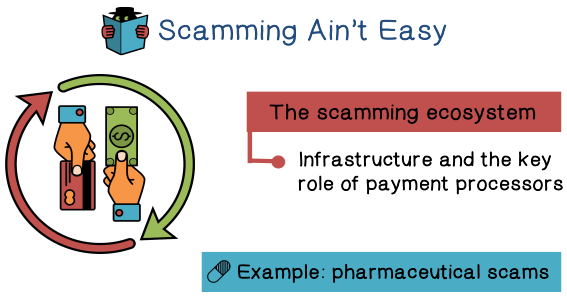


Now, let's do a quiz on spam revenue. Name the top three countries where spam directed visitors added items to their shopping cart. These are the visitors that can make transactions.

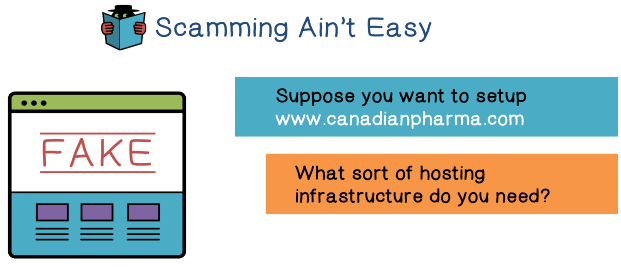
This may be a surprise to you, but a top country is the United States, followed by Canada, followed by Philippines.



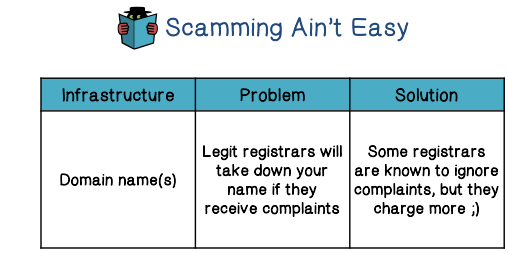
There is an interesting paper called Show Me the Money: Characterizing Spam-advertised Revenue, and I encourage you to study this paper.



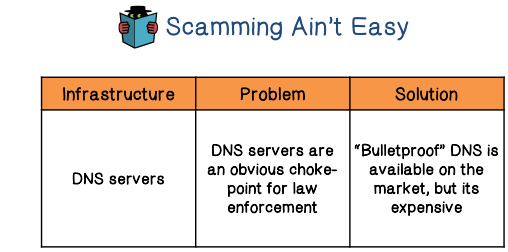
With the example Storm botnets, you may think that making money is easy in the underground. Actually, it is not easy. In fact, scamming is supported by a whole ecosystem that includes network infrastructure and payment system. For example, we are going to start the pharmaceutical scams.



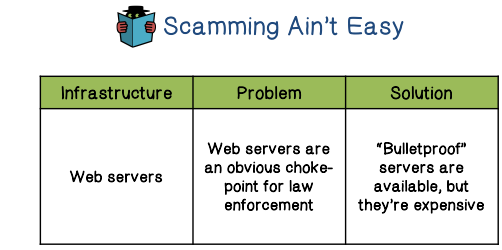
Suppose you want to set up a website called canadianpharma.com. The question is that how do you do this? What sort of infrastructure do you need? Because obviously you should worry about law enforcement agencies shutting down your website.



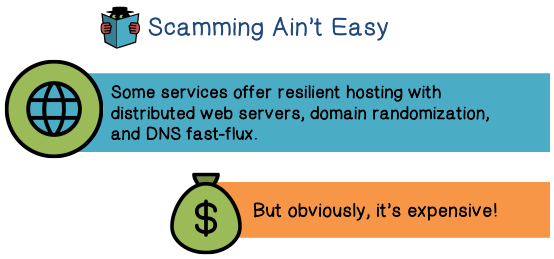
Even before that, you should worry about that legitimate registers may not even let you register your domain name. So, you go to the shady registrars, but they would charge you more.



After you obtain your domain, you want a DNS server that maps the domain name into an IP address. Some DNS providers will shut down your domain if they hear complaints. So, you go to the so-called bulletproof DNS providers, that operates in lawless land, but they are expensive.



Now to set up your website, you need to stand up a web server. For example, a machine in ISP. But the ISP or law enforcement can shut down your website. So, you want to go to the bulletproof network providers. Again, they are expensive.



There are indeed service providers that offer very resilient hosting services, but obviously they are very expensive.

After you set up the network infrastructure, now you need to consider how you receive payments. Basically, you need to handle credit card payments and get money out of these accounts.

Pharmaleaks

In 2012, the databases for GlavMed, SpamIt, and RX-Promotion were breached, dumped, and publicly released

The databases contained complete logs of sales, customers, and affiliate relationships

Program	Period	Affiliates	Customers	Billed orders	Revenue
GlavMed	Jan 2007 – Apr 2010	1,759	584,199	699,516	$81M
SpamIt	Jun 2007 – Apr 2010	484	535,365	704,169	$92M
RX-Promotion	Oct 2009 – Dec 2010	415	59,769 – 69,446	71,294	$12M

Source: *PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs*

The trouble is that most banks and credit card processors won't do business with scammers. Again, your solution is to go to a few banks in some lawless countries to handle your payment.

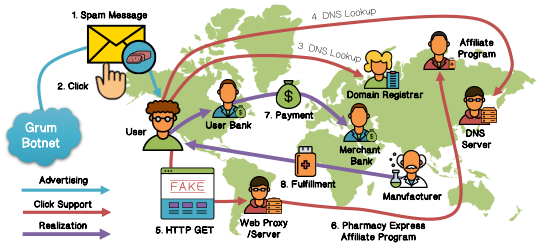
Scamming Ain't Easy

Scam sites almost always ship products to customers — Why?

Unhappy customers → Processor shuts down account → Bank account seized

To be successful in scamming, you almost have to learn it like a legitimate business. For example, you should ship products to customers, why? Because if the customers are not happy, they will complain, and the processors and banks will shut down your accounts.

Example: Pharmacy Express



Now let's study an example of scam. First, the Botnet sends scam messages to the victim users. The user clicks on the link and the link will eventually lead him to website to purchase fake drugs. And payment will then be withdrawn from his bank account and he will receive shipment of the fake drug.

Example: Pharmacy Express

Affiliate Program		Distinct Domains	Received URLs	Feed Volume
RxPro	RX-Promotion	10,585	160,521,810	24.92%
PhEx	Pharmacy Express	14,381	69,959,629	23.48%
EDEx	ED Express	63	1,578	0.01%
ZCashPh	ZedCash (Pharma)	6,976	42,282,943	14.54%
DrMax	Dr. Maxman	5,641	32,184,860	10.95%
Grow	Viagrow	382	5,210,668	1.68%
USHC	US HealthCare	167	3,196,538	1.31%
MaxGtn	MaxGentleman	672	1,144,703	0.41%
VgREX	VigREX	39	426,873	0.14%
Smul	Smul Extreme	42	66,907	0.03%
GlvMd	GlavMed	2,933	28,313,136	10.32%
Eva	EvaPharmacy	11,281	12,795,646	8.7%
WldPh	World Pharmacy	691	10,412,850	3.55%
PHOL	PH Online	101	2,971,368	0.96%
Aptke	Swiss Apotheke	117	1,586,456	0.55%
HrbGr	HerbalGrowth	17	265,131	0.09%
RxPtr	RX Partners	449	229,257	0.21%
Stmul	Stimul-cash	50	157,537	0.07%
Maxx	MAXX Extend	23	104,201	0.04%
DrgRev	DrugRevenue	122	51,637	0.04%
UltPh	Ultimate Pharmacy	12	44,126	0.02%
Green	Greenline	1,766	25,021	0.36%
Vrlty	Virility	9	23,528	0.01%
RxRev	RX Rev Share	299	9,696	0.04%
Medi	MediTrust	24	6,156	0.01%
ClFr	Club-first	1,270	3,310	0.07%
CanPh	Canadian Pharmacy	133	1,392	0.03%
RxCsh	RXCash	22	287	<0.01%
Staln	Stallion	2	80	<0.01%
	Total	54,220	346,993,046	93.18%
ExqsI	Exquisite Replicas	128	620,642	0.22%
DmdRp	Diamond Replicas	1,307	506,486	0.27%
PrgeR	Prestige Replicas	101	382,964	0.1%
OneRp	One Replica	77	20,313	0.02%
Luxry	Luxury Replica	25	8,279	0.01%
AffAc	Aff. Accessories	187	3,669	0.02%
SwsRp	Swiss Rep. & Co.	15	76	<0.01%
WchSh	WatchShop	546	2,086,891	0.17%
	Total	7,530	15,330,404	4.73%
	Grand Total	69,002	365,395,278	100%

RX-Promotion and GlavMed account for around 35% of all affiliate scams…remember them, we'll see them again :)

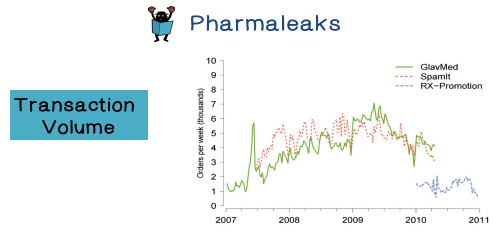
Data collected from spam feeds, botnet infiltration, and various types of honeypots in Fall 2010

Using data collected from spam feeds, botnet infiltration and various types of honeypot data. The researchers were able to find some interesting data regarding this Pharmacy Express scam.

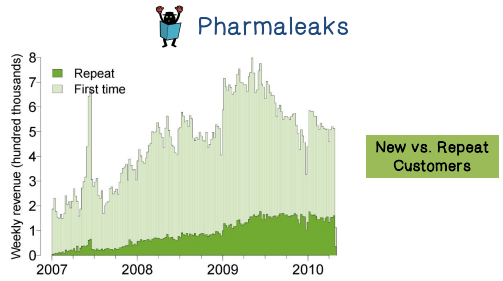
In particular, they found that these two account for around 35% of all affiliate scams. And we will look more into these scammers in more details shortly.

In 2012, some of these scammers got breached and their data were dumped and made publicly available. The data contained complete logs of sales, customers, and affiliate relationships. So,

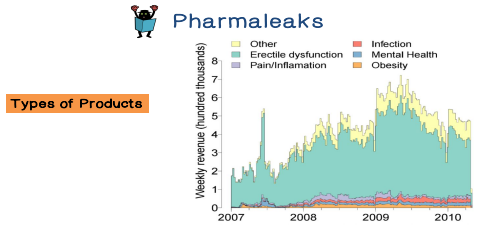
researchers studied this data and published their findings in this paper.



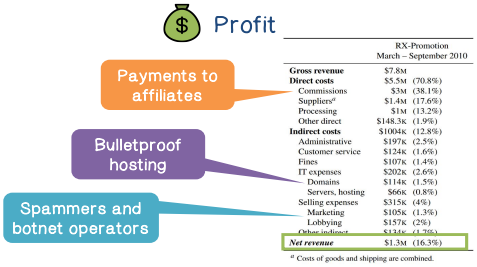
Here is a look at the transaction volumes per week for these scammers. We can see that these scammers were around for a long time.



We can see here that the repeat customers or the repeat orders are an important part of the business. This data presents a counter-point to the conventional wisdom that online pharmacies are pure scams. They do not simply take credit card and either never providing goods or providing goods of no quality. Because if that is true, then we would not see repeat customers.



Here's a breakdown of the different types of drugs being purchased by customers.



Here we see that pharma scams bring in a lot of revenue, but there are also a lot of costs. The actual net revenue, or profit, is not huge. These costs include payment to the affiliates, cost of the network infrastructure, and payment to spammers and botnet operators.

Spamalytics: An Empirical Analysis of Spam Marketing Conversion

Abstract

The "conversion rate" of spam — the probability that an unsolicited e-mail will ultimately elicit a "sale" — underlies the entire spam value proposition. However, our understanding of this critical behavior is quite limited, and the literature lacks any quantitative study concerning its true value. In this paper we present a methodology for measuring the conversion rate of spam. Using a parasitic infiltration of an existing botnet's infrastructure, we analyze two spam campaigns: one designed to propagate a malware Trojan, the other marketing on-line pharmaceuticals. For nearly a half billion spam e-mails we identify the number that are successfully delivered, the number that pass through popular anti-spam filters, the number that elicit user visits to the advertised sites, and the number of "sales" and "infections" produced.

The outline, introduction, background parts of the paper describe the economic basis for spam and reviews prior research. The conversion analysis part analyzes the possible influences on spam responses.

Conclusions

This paper describes what we believe is the first large-scale quantitative study of spam conversion. We developed a methodology that uses botnet infiltration to indirectly instrument spam e-mails such that user clicks on these messages are taken to replica Web sites under our control. Using this methodology, we instrumented almost 500 million spam messages, comprising three major campaigns, and quantitatively characterized both the delivery process and the conversion rate. We would be the first to admit that these results represent a single data point and are not necessarily representative of spam as a whole. Different campaigns, using different tactics and marketing different products will undoubtedly produce different outcomes. Indeed, we caution strongly against researchers using the conversion rates we have measured for these Storm-based campaigns to justify assumptions in any other context. At the same time, it is tempting to speculate on what the numbers we have measured might mean. We succumb to this temptation below, with the understanding that few of our speculations can be empirically validated at this time.

PharmaLeaks

This paper primarily concerns itself with an in-depth study of the business model – as opposed to the technological infrastructure – behind the ubiquitous spam-based pharmaceutical advertising business that pepper the Internet. Prior to the work of the authors, not much studies had been conducted into this topic owing to the underground nature of the entities in question. The authors, however, managed to gain access to four years of transactional data on GlavMed and SpamIt and one year of data on RX-Promotion. Using the data, they provide an in-depth empirical analysis on the four cornerstones of this business – the customers, affiliates, costs, and payment processing. The data obtained by the researchers went through some pre-processing before analysis – involving things like de-duplicating data as well as filtering for only customers who succeeded in completing transactions with these companies or their affiliates.

When analyzing the customer data of over a million customers, the researchers reached the conclusion that the affiliates seemed to be acquiring first time customers at a steady pace and the market showed no signs of saturation. As relates to repeat customers, the paper points out that purchases from repeat customers seem to constitute on average about a third of sales for the companies, thus suggesting a counterpoint to the conventional wisdom that online pharmacies are pure scams which simply take credit cards and either never provide goods or provide goods of no quality; if that were true, these numbers would be much lower. A deep dive into the distribution of demand shows that drugs aimed at addressing ED are in highest demand for customers of GlavMed and SpamIt, while RX-Promotion customers seem to favor other drugs such as pain meds and sleeping aids – all of which have the potential for serious abuse and addiction.

GlavMed and RX-Promotion have open affiliate programs, while SpamIt has a closed one, but all share the common commission model in which 30-40% of sales revenue goes to these advertisers as commission. The analysis on the affiliate program revealed a skew in revenue contribution from affiliates with about 10% of the partners accounting for 75% to 90% of revenue coming in. In the end, the most important affiliates for a program are just a small fraction of all affiliates; a double-edged sword – with these top affiliates seeming to be the oldest and most well-established of all affiliates. Given the commissions-based nature of the game, the top partners pull in about $1 million per year for themselves, while the rest coast at around $2,000, with SpamIt's closed program bringing in on average three times more for the affiliates that are part of it. It is not all roses for these advertisers however as their work comes with a significant cost – in things like supplier costs, shipping costs, bank and credit card processing fees, and customer

refunds to name a few.

To summarize the findings of the researchers: the customer market is large and far from fully tapped, with repeat orders playing a key role in mature programs. A small number of big affiliates can dominate the revenue equation and that disrupting these particular affiliates would have disproportionate damage on the whole program. Finally, even very large programs such as GlavMed/SpamIt depend on a handful of payment service providers to reliably monetize their activities, reinforcing the observation that financial services are a “weak point” in the value chain. Surprisingly, while affiliate programs can drive substantial sales, their costs are significant and ultimately net revenues are modest, typically under just 20% of sales. This finding again suggests that such organizations are fragile to economic disruptions of even a modest scale.