Popular strategies and strategies of Spammer

Throughout 2007, spammers around the world basically demonstrated their adaptability to the spam and software vendors' efforts to prevent spam. So what strategies do spammers use to accomplish this behavior?

Dancho Danchev

Throughout 2007, spammers around the world basically demonstrated their adaptability to the spam and software vendors' efforts to prevent spam. So what strategies do spammers use to accomplish this behavior? What strategies do they use to collect email addresses, validate them, and many other issues with the shortest possible time while ensuring their spam campaigns are maintained?

In this article we will discuss some recent spam campaigns to demonstrate key concepts that spammers use, and provide helpful help on how to reduce current attacks. of them.

Break the direct marketing model

Around the time we finished the last lines of this article, hundreds of thousands of spam emails were sent to many mailboxes. So why is spam successful at such a critical point? The truth is that their direct marketing model has been broken. So how can this be done? Quite simply, while some marketing participants are busy with harvesting email addresses to sell them later, other components that are implemented later will be an effective system used for spamming. , where there is an investment in sending millions of messages to each user, or rather each other email address.

* ***Pump-and-dump*** : An attempt to raise the price of a stock through misrepresentation or excessive exaggerated statements.The perpetrators of this ploy are those who have a position in a certain company, selling their position after this hype makes the price of the stock higher.This action is completely invalid with securities laws and can lead to many problems.Victims of this plot often lose a large amount of investment because the stock will be reduced after the process is completed.

Some of the most recent cases involving spam can shed some light on what tactical battles take advantage of. When anti-spam vendors solve a photo-based anti-spam problem, the spammers use the attached PDF files and even the pump-and-dump * MP3 spam messages. According to a famous anti-spam firm, in October alone, approximately 15 million mp3 audio files were circulated globally. So what is the next logical plan used by spammer. It is spam based on video. In addition, the spam campaign cycle exploiting vulnerabilities should also be mentioned here, but it is not yet an indication of the consolidation of spammers, impostors and malware authors who are gradually becoming more organized. Along with the most recent examples of consolidation is a PDF vulnerability that is currently spam in large numbers.

Tricks of spammer

Spammer tricks are often very different. Here we will learn some of their tricks.

Redirectors and doorway pages

The redirector and doorway page take advantage of the visual social engineering problem so that the spammers can establish a trust relationship with customers later and can help them to overcome the anti-spam filters. In some cases, accounts at free web space providers such as Geocities are an example, are registered and have two lines of javascript code to refresh the account, so direct users to a real spam domain. Let's prove this. For example, all of the following Geocities pages are currently responding and acting as a redirectors for recent spam domains such as *onlinemedcross.com* ; *rxlovecaptain.com* and *pharmacysitetown.com* .

1. geocities.com/RickieWood35
2. geocities.com/AdolphBarr30
3. geocities.com/BlakeBender94
4. geocities.com/JohnieWaller66
5. geocities.com/ChangWashington95
6. geocities.com/AvaMendoza19
7. geocities.com/KimberleyHebert77
8. geocities.com/TaylorSanchez69
9. geocities.com/FrankieCase81
10. geocities.com/ElliotPugh01
11. geocities.com/VernonCantrell39LI>

** ***Social engineering*** is a term derived from the information technology world, referring to trick computer users and the Internet to reveal passwords so that hackers can gain access to the system.The most common way of doing this is to contact the victim through chat or e-mail, pretending to be the security officer in the system who is conducting the inspection and asking the user to declare the secret. password to authenticate identity or account will be closed.

How is the spammer managing the registered accounts at home providing free web space effectively through CAPTCHA, is CAPTCHA an appropriate way to ensure automatic registrations become useless? By adapting to the fairly broken CAPTCHA process or completely outsourcing it as you will see later in this article.

The strategy is quick

From ASCII, to TXT, XLS, FDF, RTF, PDF, image and now MP3 spam, there are many fascinating examples of persistent strategy around the distribution issues of reactions by firms. anti-spam.

Verify or confirm distribution

With hundreds of thousands of spam emails being sent, only a small percentage will be successfully distributed and this is not because they are filtered because many emails will be fake or non-existent. Therefore, the spammer has started to care about applying different methods in appraising and validating distribution, even verifying whether spam emails are real or fake with a software tool like High Speed ??Verifier, either by pretending to be the recipient in a manual verification of the email by asking him or her about not registering.

'Your *unregistered request for the email address' example@example.com' has been successfully received. Please allow 24-48 hours for your email to be deleted from the system* . '

Another commonly used trick is to confirm both the recipient's validation and validation, by embedding a remotely loaded image with a unique check ID on each email, thereby misusing the Default remote image loading function within popular email reader applications and web services.

Popular strategies of spammer

Strategies are the long-term goals that spammers set up to perform during a specific time period, while the previously discussed tricks often get interest from the mass media. . Now we will go into this picture.

Consolidation

As we know about ongoing consolidation between spammers, phishers and malware authors, it is also worth discussing why it happened and how each participant started to rely on each other. to improve their effect. The charm of viability does not seem to be an appropriate component when it comes to spammer's results-oriented perspective. Spammers can reap a lot of money and buy email addresses, send and distribute mail successfully, fake guys are social engineering issues, while malware authors have a different path. , providing the infrastructure for both spam and spoofers as hacked hosts. We will have evidence for this consolidation through some recent events, which are excellent examples of this development of an ecosystem below. Take for example cases of spam with embedded keyloggers, fake emails with malware and another sarcastic situation that malware has infiltrated hosts inside Pfizer and spamed viagra emails.

Outsourcing

Outsourcing is still a new word, cost effective with many other advantages that come with it, obviously it has a big impact on the spammers. A recently discovered spam management device service can be used as a good example of all the spammer's outsourcing needs for third party service providers. Basically, this service is interested in providing hacked bots, spam email templates and spam sites, and also fast-flux infrastructure for spam campaigns to increase Its submitted and maintained undetected in a possible way. Get an example redirector URL that we provided at the beginning of the article, onlinemedcross. It is currently a fairly current fast-flux, quite normal in the sense of slow updates compared to the Storm Worm's fast-flux domains.

Index	IP Address	Host Name	Original Name
6	82.131.17.224	ip224.cab17.mus.starman.ee	onlinemedcross.com
8	87.122.106.68	i577A6A44.versanet.de	onlinemedcross.com
2	61.18.58.223	cm61-18-58-223.hkcable.com.hk	onlinemedcross.com
1	61.15.245.139	cm61-15-245-139.hkcable.com.hk	onlinemedcross.com
15	222.167.18.38	cm222-167-18-38.hkcable.com.hk	onlinemedcross.com
11	125.59.84.66	cm125-59-84-66.hkcable.com.hk	onlinemedcross.com
4	75.64.49.224	c-75-64-49-224.hsd1.tn.comcast.net	onlinemedcross.com
10	89.179.40.113	89-179-40-113.broadband.corbina.ru	onlinemedcross.com
9	89.178.130.179	89-178-130-179.broadband.corbina.ru	onlinemedcross.com
5	78.106.134.242	78-106-134-242.broadband.corbina.ru	onlinemedcross.com
7	85.29.194.212	212-194-n.ipv4.vnet.ee	onlinemedcross.com
12	210.6.7.20	210006007020.ctinets.com	onlinemedcross.com
3	61.238.130.148	061238130148.ctinets.com	onlinemedcross.com
13	218.191.172.19		onlinemedcross.com
14	221.127.153.98		onlinemedcross.com

Merged models

The merging model is quite new in the spam world. Whether spammer based on provided truth is encouraging enough, third parties will be interested in finding their own ways of sending mail to a large number of users, even outside the field. email area and start targeting instant messaging.

Conclude

Suppose in a perfect world, there is no malware-infected computer so the spammers won't have to search for configuration-corrupted SMTP servers and attack them. With time going on, the spammer will conduct strategic warfare and in parallel with it, the best plans that anti-spam firms can take for a long time are to become more innovative with Spam filtering is taking place from the organization's network.

The big picture doesn't seem to be very realistic and from the perspective of the international spam battle is conducted the wrong way. It needs to implement both a practical legal perspective and self-regulation as an ISP. The current legal regime must promote responsibility to individuals who are sending spam and a certain process. However, even if the spam is tracked, the spammer will quickly replace the failed mode in some other appropriate way.

In each country, there are often one or more ISPs causing spam, but those ISPs themselves also provide anti-spam services in some way, possibly by filtering incoming spam from a compromised host their own network. Battle incoming spam or outgoing spam? That's all about how your solution really matters to this problem and what its real power will be.