[This chapter talks about what are Spam messages, what Spammers aim to achieve, how they achieve it and what is the role of a user in a spam related attack. It will mainly focus on Phishing threats.]

SPAM can generally be defined as unsolicited messages sent to users usually in a digital format, also referred to as ‘junk mail’. These messages often contain advertisements for ‘special’ offers on a variety of products or services and other times they contain information about certain events on a particular topic. They are often associated with malware and gathering of information and are commonly spread via: e-mail, instant messaging applications [SPIM], voice over IP services (calls that take place over the internet) [SPIT] and SMS (Short Message Service) messages.

A website called SecureList, run in part by members of Kaspersky Lab, reported information from their (security) products where on average SPAM took up approximately 70% of the e-mail traffic in the 3rd quarter of 2014. The amount of SPAM in previous years has reached similar if not greater percentage of the e-mail traffic.

Spammers aim to collect as many active e-mail addresses as possible in every way and any way they can. Some of the ways that they collect addresses are:

* By purchasing information from databases or accessing information from leaked databases (Illegal)
* Search the internet for any and every e-mail address
* Generating e-mail address by using words from a dictionary and checking whether a service considers them as valid. This is called a brute force attack (trial and error attack) and is usually used to decrypt cipher text (encrypted messages).
* People that open Spam e-mails or click on links in those e-mails.

Phishing threats

Phishing is a form of SPAM where the purpose of this message is to gather sensitive information from potential victims such as username, password or credit card details and exploit it in order to gain profit. Phishing attacks try to deceive users into handing over information. These messages usually imitate an official letter from a service or redirect users to a website which imitate that service’s website. It can start by urging users to take immediate action on reviewing some unusual activity on their account or by asking users confirm account details or other personal information. The result of a phishing attack is essentially identity theft.

**Clone Phishing:**  This form of phishing attack creates a cloned version of a delivered e-mail that contained attachments. The attachments are replaced with malicious code and the message is resent to the original e-mail addresses, making it look like the original sender was the one sending it.

**Spear Phishing:** This is a form of phishing is more focused; it uses some knowledge about you and your internet usage. This can include:

* Contacts (Friends or Family)
* Websites that you have visited
* Services that you have used
* Information that you have shared in different social media

This information is used in order to attempt to access your accounts and other personal information.

**Whaling:** This form of phishing attack is a variation of spear phishing attacks that mainly focuses on people of a higher profile/status such as celebrities.

**DNS-Based**: This form of phishing attack uses a router as a public access point to attract a user and then through the attackers DNS and phishing server the victim (user) is tricked into entering personal/account details on fake web pages that imitate an official website’s pages.

**Smishing**: This form of phishing attacks takes place on a mobile device through SMS messages that usually request information or include malware infested website links.

Phishing attacks can also make a user subscribe to premium rate text messaging services or take the form of bogus security software/applications such as an antivirus. Malware that can be spread through these attacks can also be used to gain access to certain information on devices or even spy on users.

Android permission system involves what actions an application can perform, a list of permissions are shown before the installation of an application where it requests the user to grant them. If the user does not want to grant these permissions then he/she is unable to install the application. Permissions are usually split into groups such as SMS where an application is granted permission to read, receive and send SMS messages. Other permissions include Location where an application can keep track of approximate or precise location, Contacts where an application can read or modify contacts on a device et al. .

Users can agree to an application’s permissions without considering the possibility that the application can abuse them. Recently there were reports of top-rated flashlight applications in the android market that were requesting a lot more of permissions than they required. Applications like these required permissions such Location, Identity, Microphone etc. The problem with this is that applications like this record information that has nothing to do with the application functionality and can quite possibly be used to spy on users (Spyware). Some people however could argue that installing an application like this is optional and the user has the power to grant the permissions. In some cases application can request for new permissions before updating to the latest version, if they are not granted the user cannot acquire the update. This might be a problem with security as older versions might be more vulnerable.

In the paper “**Android SMS Malware: Vulnerability and Mitigation**” ­ by Khodor Hamandi, Ali Chehab, Imad H. Elhajj and Ayman Kayssi there is a study that talks about malware that use a device’s SMS services and how privileges that were granted by a user can be abused and still remain undetected by security software. It stresses the fact that privileges that have been granted before installation can be dangerous as they remain unmodified. Android’s broadcast service which distributes data to services/applications that request them, does not guarantee that all applications will receive the original/unmodified data. Malicious software can be registered with top priority which means that they would receive the data first and therefore can modify the data.

This software, with the malicious code can suppress notifications of misuse and can continue to drain a user’s credit without them noticing. In order to prove these events an application has been developed to act as a malicious application, suppressing misuse notifications, sending messages and removing them from the local messages database so that a user cannot have a history of these events. The application was implemented in such a way that it would rerun services that have been terminated, continuing its malpractice.

It has been tested between two devices one of which being an Android smartphone. When antimalware applications were run this application was not detected and it also was successfully published to the official android market. Finally the study suggested solutions such as: not allow applications to set their own priority (and possibly assigning a trusted application as the highest that will be in control), always inform a user when with the receipt of a SMS message and request permission each time a SMS message will be sent.

Avoiding Detection

Spam filter is a program that filters incoming messages. Messages are classified by the filter based on certain rules and algorithms. If a message is marked as spam it is usually added to a junk/spam folder. If a message does not show any signs of being spam it is added to the user’s inbox folder.

According multiple online sources on spam, there are a lot of tricks used in order to fool spam filters into thinking that the message is a legit message and therefore avoid detection. Here are some of the techniques used by spammers:

* Line breaks at unexpected parts of a message
* Adding spaces between characters in words
* Replace spaces with a specific character
* Use of null characters
* Use of characters from foreign languages that look like English characters
* Switching around some letters in words
* Exploiting the Unicode right to left override
* Hiding the malicious URL in a < map > tag within an HREF tag
* Using HTML encoded characters
* Using HTML to add tiny letters in words which can’t be noticed by a user
* Using HTML tables
* Use of JavaScript to hide messages
* Use of ASCII characters in a way that visually they look like characters.
* Spam engines imitating real mailers such as Hotmail, Outlook
* Using multiple ‘zombie’ computers to send spam since IP addresses can be added to block lists
* In order to fool spam filter algorithms they add more sentences to pass the spam filter’s threshold
* These additional sentences can be the same colour with the background of a message so that a user does not notice them
* Use IP address with neutral or positive reputation
* Using tiny URLs instead of full length URLs
* Using encoded URLs
* Use HTML to fool recipient by adding a malicious link on a legitimate service’s URL
* Splitting URLs in different parts and showing how the user can attach the parts to get the original URL

Spammers study how spam filters work and then try to exploit their algorithms in order to bypass detection. Therefore spam filters need to continuously be updated with detecting techniques and improved algorithms. Problems that can appear are false positive classifications which are legitimate messages that were marked as spam. Email services such as GMAIL by Google try to improve their algorithms in order to reduce the number of false positive detections either by using familiarity such as adding an e-mail address to an approved senders list (contacts) or creating your own filters.

There numerous of patterns that filters tend to look at and there are many websites that help legitimate users avoid spam classification by following some rules.

Some of the rules that are mentioned online are:

* Use of words such as ‘free’, ’urgent’, ‘click here’, ’once in a lifetime’ or characters such as $$, XXX
* Talks about money, claims money back guaranteed
* Excessive use of caps lock
* Excessive amount of images or links with not enough text
* Use of bright colors and irregular font size (too small)
* Use of attachment of files of these formats: exe, bat, com etc.
* Claiming that is a legitimate e-mail
* Use well known mailers
* Timing : frequent e-mails from an address can be marked as spam

Bibliography

<http://searchmidmarketsecurity.techtarget.com/definition/spam-filter>

<http://www.windowsecurity.com/uplarticle/anti-spam/Spammer_tricks.pdf>

<http://www.google.com/support/enterprise/static/postini/docs/admin/en/troubleshooting_spe/faq_spam_falsepositives.html>

<https://support.google.com/mail/answer/9008?hl=en>

<https://support.google.com/mail/answer/25760?hl=en>

<http://www.process.com/psc/fileadmin/user_upload/whitepapers/pmas/common_spammer_tricks.pdf>

<http://www.itnewsafrica.com/2009/11/10-tricks-used-by-spammers-to-get-into-your-inbox/>

<http://www.seas.upenn.edu/cets/answers/spamblock-false.html>

<http://www.seas.upenn.edu/cets/answers/send-prohibited-attachments.html>

<http://mailchimp.com/resources/guides/how-to-avoid-spam-filters/html/>

<http://blog.crazyegg.com/2012/06/26/avoid-email-spam-filter/>

<http://www.theemailadmin.com/2012/03/5-tricks-spammers-use-to-get-past-your-filter/>

<http://www.pandasecurity.com/homeusers/security-info/types-malware/spam/>

<https://www.campaignmonitor.com/blog/post/1971/what-are-some-good-methods-for>

How to stay safe

“Better safe than sorry” is a popular saying that is used in situations where it is important to stay safe and avoid any risks even if the situation might not seem all that risky. This is often true when it comes to reading digital messages, even if it might not seem as something that might harm you, it can and you might not realise the extent of the damage that it has or will cost you until it’s too late. Companies can rely on their reputation and productivity in order to be successful. Spam can have a negative effect on a worker’s time and productivity; it can also cost a company or an individual a significant amount of money to repair the damages that it might inflict due to the possibility of malware infections or loss of information. These are some of the reasons of why it is important to take appropriate measures in order to defend against spam.

Spam often present ideal situations to their potential victims whether it is a job opportunity or a great offer on certain products/services and the saying that comes to mind is “if something is too good to be true, it probably is”. One of the first things to look out for is these messages that present ideal situations which are can be unrealistic and avoid them. The general rule is to not open spam messages, some of these messages summarize their purpose in the subject field but a lot of them either prefer to leave it blank or ambiguous in order to tempt a user into opening it. If the message that you have received is from an unknown or unfamiliar sender then do not open it.

A message may not look as spam as spammers can make messages look like they are legit by using a company’s logo and layout. However services in general do not request account details to be confirmed or shared via e-mail, contact the service via telephone to confirm or report the message.

Spam can often keep the message as general as possible, not using a user’s name or any specific detail about the user. If the message looks suspicious avoid replying to it and avoid clicking on any link in the e-mail content. If you are unsure type the link into your browser (do not click to open the website) or hover over the link and try to look for any unusual patterns or do some research to find the official link to the service’s website and see if they match. Spam often includes an ‘Unsubscribe’ link in their message that does nothing but confirm that the e-mail address that they used to contact you is active. As an extra security measure disable the preview pane and loading of images in your mailing software.

Finally, it is highly recommended that antivirus software and filtering software are regularly used and are kept them up-to-date. Some email services such as GMAIL use antivirus software to scan attachments of incoming and outgoing messages for malware. If malware are detected then attachments are made unavailable for download to the receiver or notify the user/sender that the message cannot be sent until the infected attachment is removed.

Bibliography

https://support.google.com/mail/answer/25760?hl=en

<http://www.encyclopedia.com/doc/1O214-smthngsndstgdtbtrtprbblys.html>

<http://dictionary.cambridge.org/dictionary/british/better-safe-than-sorry>

<http://www.telstra.com.au/consumer-advice/download/document/cyber-safety-consumer-phishing.pdf>

<http://www.fbi.gov/scams-safety/fraud/internet_fraud>

<http://www.quepublishing.com/articles/article.aspx?p=1234199&seqNum=6>

<http://www.kaspersky.com/downloads/pdf/staying_safe_online_home_guide.pdf>

<https://www.staysafeonline.org/stay-safe-online/keep-a-clean-machine/spam-and-phishing>

<http://www.gcflearnfree.org/internetsafety/4.2>

<http://www.air-it.co.uk/2014/09/staying-safe-spam-phishing-emails/>

<http://www.ikeepsafe.org/be-a-pro/online-security/how-can-i-avoid-spam-and-phishing-scams/>

<http://www.pandasecurity.com/homeusers/security-info/types-malware/spam/>

Bibliography

<http://www.pandasecurity.com/homeusers/security-info/types-malware/spam/>

<http://www.howtogeek.com/180477/htg-explains-how-do-spammers-get-your-email-address/>

<http://securelist.com/analysis/quarterly-spam-reports/67851/spam-and-phishing-in-the-q3-of-2014/>

<http://media.kaspersky.com/pdf/Kaspersky_Lab_KSN_report_The_Evolution_of_Phishing_Attacks_2011-2013.pdf>

<http://www.phishing.org/resources/phishing-identity-theft/>

<https://www.ecrimewales.com/en/archive/clone-phishing>

<http://uk.norton.com/spear-phishing-scam-not-sport/article>

<http://searchsecurity.techtarget.com/definition/whaling>

<http://www.exploit-db.com/wp-content/themes/exploit/docs/20875.pdf>

<http://www.theguardian.com/technology/2014/oct/03/android-flashlight-apps-permissions-privacy>

* <http://www.howtogeek.com/177904/androids-permissions-system-is-broken-and-google-just-made-it-worse/>
* <https://support.google.com/googleplay/answer/6014972?hl=en-GB>
* <http://www.makeuseof.com/tag/app-permissions-work-care-android/>

Hamandi, K.; Chehab, A.; Elhajj, I.H.; Kayssi, A., "Android SMS Malware: Vulnerability and Mitigation," *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on* , vol., no., pp.1004,1009, 25-28 March 2013  
doi: 10.1109/WAINA.2013.134  
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6550526&isnumber=6550285>

<https://computerobz.wordpress.com/tag/clone-phishing/>

<http://www.networkworld.com/article/2164211/infrastructure-management/how-to-avoid-becoming-a-victim-of-smishing-sms-phishing.html>

<http://www.t-mobile.com/company/privacyresources.aspx?tp=abt_tab_phishingsmishing>

**Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions** by Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Cranor, Julie Downs

This paper presents results from a survey with 1001 respondents that focused on user demographics and risk of falling victim of phishing threats. It consisted of role play scenarios where phishing attacks were simulated along with actions that could have been taken by the user. In addition to a demographic survey to look at their background and knowledge of phishing attacks. The survey tested the user’s background by presenting possible definition of certain terms where only one was correct and it also included questions about user’s previous experiences and risk perception. Users were given education materials such as tasks to participate in online training websites and material. The results showed that users from age **18 to 25 were more likely to fall victim of phishing attacks** due to lack of experience or education. It also showed how educating users reduced the amount of phishing attack victims but it also resulted in false positive actions where real messages/websites were treated as the phishing type. In addition to that it’s said that demographics such as age did not affect the amount of learning, meaning training material can be beneficial to all groups.