International Journal of Cyber-Security and Digital Forensics (IJCSDF) 3(1): 72-83
The Society of Digital Information and Wireless Communications, 2014 (ISSN: 2305-0012)

Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors

Thomas Nagunwa
Department of Computer Science
Institute of Finance Management
Tanzania
nagunwa@ifm.ac.tz

ABSTRACT

Increased consumer anti-phishing awareness and improved anti-spam technologies has gradually reduced the impact of traditional phishing spams in recent years. To keep up their game in a multi-billion dollar cybercrime industry, hackers have been continuously innovative in developing polymorphic phishing vectors. Spear phishing, malware, search engines poisoning, use of rogue Secure Socket Layer (SSL) certificates, mobile and social media attacks are among the modern and prominent vectors for phishing attacks today. This paper examines today's most adopted phishing vectors by cybercriminals as observed by security vendors, security analysts and anti-phishing campaigners. Learning the current landscape of these vectors is a key step in developing effective technological, social and legal devices to mitigate the impacts of these threats across the globe. The paper concludes that almost of all today's phishing attacks begin with spear phishing. Phishers focus more their attacks towards small and medium enterprises. Malware toolkits are the key player in all major attacks. Mobile and social media attacks have rapidly grown recently and promise to be the future of phishing.

KEYWORDS

Phishing, vector, website, URL, email, spam, online fraud, identity theft, malware, online credentials.

1 INTRODUCTION

The history of phishing goes as far as 1996, by then the word referred to fishing of online users' identities from the sea of internet users and uses them for various malicious intents including fraud [1], [2]. Phishing involves different enticing skills including technology and social engineering to trick online users into giving up their online credentials and purporting them to steal money or make unauthorized online purchases [3]. These credentials may include usernames, passwords, bank account numbers, credit card details, social security numbers, ATM PINs, birthdates, addresses and others [2], [4].

Over the years, phishing activities leading to fraud have caused many economic and social damages to online communities. In 2012, for instance, global online consumers experienced a total loss of US $110 billion when 556 million consumers were victimized in more than 30 million hacking activities including phishing [5], [6]. About 187.2 million online identities were stolen in 2011 for online fraud [12]. Some business brands have lost reputations and confidence towards sections of their online markets leading to fall of businesses [4].

Despite global efforts in imposing technological solutions, anti-phishing educational campaigns and anti-cybercrime legal frameworks, phishing has been relatively growing over the years. Phishers have been frequently evolving their techniques to elude advanced security technologies and lure even phishing-aware online users successfully [7]. From a tradition phishing approach of generic email scams, phishers are shifting towards targeted email scams, rogue websites, and deployment of sophisticated malware to infect legitimate websites and hosts to steal identities. Recent popularity of mobile devices and social media to online communities has opened new effective phishing vectors as security solutions deployed are still at immaturity

level while their users think they are in trust zones [6]. Cloud computing has shown signs as the future target of phishing as more businesses are converging their services and data to cloud.

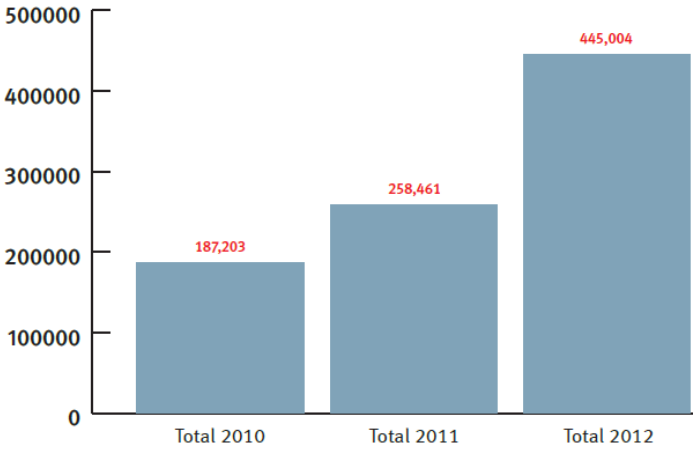

Figure 1 Global growth of phishing attacks between 2010 and 2012 as detected by RSA [8].

This paper aims at exposing phishing vectors being deployed in recent years. Learning the trends of these vectors is a key step in educating online consumers about the existing online threats, risks and the need to adopt safe internet access practices. Online businesses, anti-phishing campaigners, security communities and legal societies should find this information as a basis to develop adaptive and effective strategies to educate and protect both online consumers and businesses.

2 PHISHING SPAMS

Phishing email is a category of spam, an unsolicited email message, sent to multiples users to lure them to provide their online identities for impersonation. Phishing spam is the earliest phishing vector and is still being deployed by phishers though at a reduced rate due to the diversification of attacking methods in recent years [6]. In 2012, 1 in every 414 legitimate emails was observed to be a phishing one while the ratio was 1:299 in 2011 [6]. Up to 5% of all phishing emails sent globally succeed to lure recipients [9].

Phishing spams are sent with 'calls for action' oriented message, convincing a user to respond in order to get a certain advantage [10]. These messages are crafted in such a way that they are seemed to be coming from legitimate businesses like banks, online retailers or payment processing providers customers have an association with. Some often used 'calls for action' crafted by phishers are;

- The business has opened a new service and is freely offered to only first few confirming members, the rest will be required to pay for the service. Member is argued to respond for confirmation with personal details.
- Unusual number of attempts of log in, high number of transactions or changes in settings has been observed at member's account. To prevent fraud, the business has closed the account temporarily. To activate the account, member is required to log in
- The business's system has experienced breakdown and all accounts were shut down during servicing. The system is up now, to activate the account, member is required to submit log in details.
- A failure to process a bill due to unverified payment details. A customer is required to verify the payment details through a given link [1], [10].

Figure 2 A typical phishing email purporting to be from AOL [11].

To respond to 'call for action', user is given a URL link which directs user to a malicious fake website or deformed legitimate website to which is either prompted to submit credentials or malware are installed to spy and steal the credentials.

2.1 URL Obfuscations

To facilitate phishing email vector, phishers craft email links' URLs to hide the actual URLs directing them to phishing websites. One of the ways is to design a link in html form in which the real URL redirecting the user is hidden underneath the visible html-crafted URL to avoid user's suspicion. For instance, in the link below;
* https://oib.westpac.com.au/ib/default.asp *
user sees the first innocent URL but actually is directed to the second malicious URL [10].

The use of bad domain is largely applicable where a URL's domain is slightly changed to look close to the real one. For example,
https://www.paypal.com/cgi-bin/webscr?cmd=_login-run
its domain can be modified from **.com** to **.com.cn** as shown below. User can hardly notice the difference.
*https://www.paypal.**com.cn**/cgi-bin/webscr?cmd=_login-run*

The real domain can also be placed as a path of a fake domain.
http://2iphoto.cn/https://www.paypal.com/cgi-bin/webscr?cmd=_login-run
User may think is accessing a PayPal website but is redirected to 2iphoto.cn site [13].

IP addresses of the phishing sites are used to hide their suspicious domain names [1], [13].
http://217.80.34.66/https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

The use of third party's shortened URLs is one of the popular methods used by phishers [14]. Most of the phishing URLs are very long which become easy to raise suspicions. To evade the scenario, phishers convert their URLs to short forms using free services offered by companies such as tinyurl and smallurl as legitimate websites do. For instance the URL
http://0322.0206.0241.0043/http://signin.ebay.com/ebayisapidllsignin.html
can take a new short form of *http://tinyurl.com/4* [1].

Latest trend in this approach is the use of phishers' fake URL shortening services [15]. In this case, email link is crafted using legitimate short URL which when clicked, links to a fake short URL then to the phisher's website [15].

2.2 Malicious Domain Name Uses

To spoof brands, phishers often ensure phishing websites' URLs contain domain information of the brands. 94.6% of all phishing URLs use brands' compromised domains [16]. This is achieved by hacking web hosts and then create rogue subdomains and their URLs. Also phishers, in other cases, register their own fake domains to domain registrars using fake company identities. Top level domains (TLD) popular to phishers are .COM which records 55.9% of all malicious domains, .NET (6.2%), .ORG (5.0%), .BR (2.5%) and .INFO (2.3%) [16]. One domain is often used to launch up to 20,000 unique phishing attacks through unique subdomains and URLs [16]. Of 89,748 domains used for phishing in the second half of 2012, 6.5% were the phishers' domains [16].

3 SPEAR PHISHING

This is a fast emerging and most practiced form of phishing emails in which phishes are a specific targeted group. The target can be specific customers of a particular service, bank or retail, employees or members of an organization, government agency or a social group [2]. About 91% of all cyber attacks today begin with spear phishing [17].

In this vector, phisher crafts an email with a specific and relevant content to the targeted group to gain readers' trust and then direct them to either click a provided malicious link or download a malicious attachment [18]. By responding to the email, user installs vulnerability exploit malware injected in the download or redirected to a phishing website to launch the attack. Once the attack is successfully, the hacker intrudes the user's host or network and steals intellectual properties and financial assets for fraud [18], [19]. 94% of spear phishing attacks deploy malicious file attachments while 6% use links to malicious websites [18]. Common file formats used for malicious attachments are RTF, XLS, ZIP, RAR, DOC, DOCX, PPT and PDF [7], [19].

To craft relevant email content, phisher spies a target before the attack through a previous intrusion or from online information about the organization or its specific key members. Ease availability of detailed information such as email addresses and corporate reports from corporates' websites and social media has been the key driving factor for the growth of this form of attack [17].

10% of all spear phishing attacks are directed to financial sector for online fraud [7]. Other major victims are governments (65%), activists (35%) and manufacturing industries (22%) [7]. Since 2006, one hacking group was found to have attacked more than 100 companies and organizations using spear phishing vector [20].

4 VISHING

It is a use of telephone to lure users to reveal their personal details to phishers. There are two forms of vishing, by phishing email or telephone [2], [21]. By email, phisher craft an email pretending to be from a legitimate business, bank or law enforcement explaining about customer's account being compromised, for instance. To help investigation or activating the account, customer is required to call a toll-free telephone number provided as a link and asked to provide account details [21]. Voice over Internet Protocol (VoIP) has been used for calls in this form of vishing [2].

In vishing by telephone, phisher deploys VoIP software to call a customer pretending to be an employee of a legitimate company the customer has a business with [21]. The software is well crafted that the number or call ID appears to be a legitimate one while using also professional sounding automated service line such as those used in large firms [2]. When calling, customer is prompted for account details to either activate/reset his account or for maintenance purpose.

Vishing has been growing over the years as users are becoming more educated on phishing spams and their failure to determine legitimate and fake calls. In UK, for instance, 23% have experienced telephone vishing while in 2012 alone, customers lost about £7m from vishing activities across the country [22]. 39% of UK population admits a challenge in differentiating genuine calls from fake ones [22].

5 MALWARE

Use of malicious programs for identity theft is one of the most preferred and effective vectors by phishers today. Malware can be deployed by phishers to install other malware, spy and steal host's user data, change host configurations and block host's access to operating system (OS) or to some applications [6], [23].

Malware are distributed and installed in the hosts through drive-by downloads, compromised websites or malvertising [3], [6], [23]. In drive-by download channel, a malware is injected in an email attachment file and distributed through a phishing spam or spear phishing vectors. When a file is downloaded, the malware exploits a particular vulnerability, usually of an OS, Microsoft office, acrobat reader, Java platform, web browsers, web plug-ins or other common applications, to infect the host. Peer to peer file sharing also plays a major role in this channel.

A compromised legitimate website through injection of malicious codes is another common channel. Hacker attacks a web host and then

injects a JavaScript or a piece of a code in a website that dynamically download vulnerability exploiting malware payload when a particular web page is visited [6]. 1 in every 532 websites was found to be compromised by malware in 2012 [6].

Malvertising is an online advertising with a malware embedded advertisement (ad). In this approach, phisher designs an ad with an injected malware and then pay for it to be hosted and advertised by legitimate ad websites [6]. When the ad is clicked, a dynamic malware is installed by exploiting a specific vulnerability of the host.

Trojans, malware kits and bots are the major forms of malware that have been deployed by phishers in recent years.

Trojans

Trojans are the most deployed malware by phishers, contributing to 77% of all malware attacks [3]. These are malware installed for malicious operations including stealing credentials or linking the host to a botnet [14]. Trojans are used for phishing mainly in four channels; as key and screen loggers, as rogue websites, as web proxy, as scareware or as spam relays [14], [23], [24], [25], [26].

Once installed, a trojan can be designed to spy a user's access to particular websites mostly of banks. When a specified website's login page is accessed, it takes screen shots of the page or log in typed data and then sends to phisher's server [14], [26]. Zeus family of trojans, one of the dominant trojans in 2012, used this approach [14].

In the other form, a trojan, launches a fake log in web page looking similar to a legitimate one [25]. User's data is then submitted and sent to the phisher's server. PWSteal.Bancos was one of the trojans to deploy the method. In other cases, a legitimate log in page is launched but with a hacker injected log in window [14].

Trojan can act as a web proxy such that it redirects web traffic to phisher's DNS and then connects to a phishing server [25]. Log in credentials can all be trapped and then sent to the phisher. Alternatively, the proxy can be used to intercept a transaction such as bank transfer and falsify some of the information to the phisher's advantage before committing data to a legitimate server [26]. A bank trojan, SilentBanker.D, was used to falsify online bank statements [14].

Some variants of trojans have been designed as scareware/ransonware. They usually block host OS or some of the applications/files and while posing as law enforcement or anti-malware software, enforce users to pay some money or submit credit card details as a way to regain access [23]. PGPCoder trojan used a typical approach by encrypting users' data files and forces user to pay a ransom to re-access them [23]. About 250,000 of new and unique ransonware were observed globally in the first quarter of 2013 [27]. 3% of the victims agree to pay the money [14].

Figure 3 A typical ransonware in action [14].

Trojans have been observed to be deployed as spam relays. They are connected to a botnet, receive spams from botnet spam generators and then distribute to recipients' mail servers [25]. Through this, they play a key role in hiding true identities of spam generators.

Malware Toolkits

These are commercially developed advanced malware to allow cybercriminals with less or without programming skills to undertake hacking

operations [12]. Toolkits are designed to perform multiple phishing operations using different techniques. Operations may include creating backdoors, key and screen logging, generation of phishing websites, ransonware and others [12], [28]. Use of malware kits have been growing each year due to the growth of online black markets selling these products [8]. 61% of all attacks through malicious websites use toolkits [12]. The toolkits take advantage of vulnerabilities in OS, web browsers, web databases, web plug-ins and applications to infect hosts [28]. Lizamoon toolkit took advantage of web database vulnerability to attack 4 million websites through SQL injection [29].

Malware toolkits are effective over a long time because they are usually designed to dynamically generate unique signatures in each attack [28]. Also they are often updated into new versions and to each version, there may be so many variants used in different phishing attacks [6], [12].

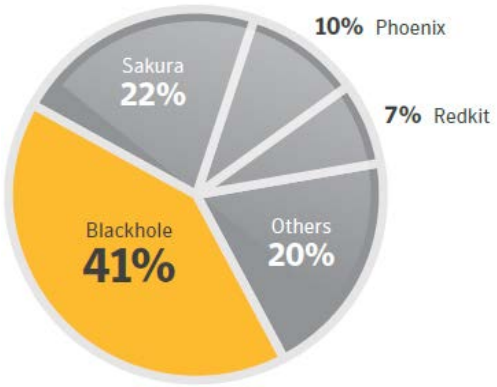

Figure 4 Top web-attacks malware toolkits in 2012 [6].

Bots

Bots are programs installed in multiple hosts controlled and commanded by remote hacker's servers to coordinate malicious activities [30], [31]. Bots are often distributed by spams, worms or malicious websites and installed through backdoors or exploitation of vulnerabilities [31]. Bots coordinated by the same servers and serve the same purposes form a botnet.

Due to their abilities to infect up to millions of hosts in short time, leading to massive impacts, botnets of malware toolkits have been the most attracting phishing approach. Bots are the main generators of spams, contributing to more than 81.2% of all global spams [12]. They can also be used as backdoors, stealers of users' online credentials for particular websites or as ransonware [31].

Zbot, a botnet of Zeus trojan, is one of the notorious botnets observed in recent years, with 3.6 million infected hosts in US only [14]. The bots use various phishing methods to steal users' online banking credentials and then send to remote phishing servers.

6 PHARMING

Pharming is the hijacking of domain name services to deviate DNS requests to spoofed websites for malicious operations [32]. This is done by altering DNS server/cache IP entries or adding new bogus entries. Potential DNS attacking points are host file (local host DNS cache), LAN's DNS server, ISP's DNS server and home wireless router [32]. Pharming can be achieved through infection of malware, injected web based malicious codes, sniffing traffic between hosts and DNS servers or hijacking DNS server administrators' accounts [32].

Home or small office users with wireless routers are the most vulnerable to this attack as more than 50% of them observed to use routers with default settings or without passwords, while 95% of them allow JavaScript in their browsers [32]. Through phishing spams, users can be lured to click attached links which lead to downloading of malware or injection of poisonous web browser scripts. The infections then launch access to router to edit some of specific DNS entries to point to phishing sites.

By hijacking administrative privileges of DNS servers through numerous ways, hackers can malconfigure the entries unnoticed. Sniffing of hosts – DNS traffic can allow hacker to learn sequence of requests' IDs generated, and then be

able to spoof DNS server responses by directing users to fake IPs [32].

New form of pharming was observed by Symantec in the wild in 2012, using free DNS services offered by afraidDNS [33]. Attackers used a weakness of the company's services by creating spoofed webpages as subdomains of legitimate domains using afraidDNS's free DNS services [33]. Users thought they were directed towards subdomains of original websites but fell into phishing traps.

7 SQL INJECTION

SQL injection attack is the incorporation of SQL statements with genuine user's SQL queries into SQL based applications to perform malicious activities [34], [35]. The attack takes advantage of inability of the applications to validate user inputs [36]. Once the attack is successfully, SQL injected codes can expose user credentials in the database, display database administrator's log in credentials, add a new administrator or allow hacker to gain access to a host OS [34], [35], [36].

Web based SQL applications have been the most victims of the attacks due to their global audiences and therefore difficult to trace the attackers [11]. Also most of dynamic websites use SQL databases management systems such as MySQL, MS SQL and Oracle SQL to host millions of customers' information potential to lucrative frauds [11]. Many of these sites lack strong input validation implementations making them vulnerable to this attack, without web masters' knowledge. In 2011, about four million websites were attacked by the biggest ever SQL injection attack known as Lizamoon [37]. Users of the infected websites were infected with scareware which report that their machines are infected with viruses. To clean up, they had to purchase hacker's rogue antivirus thus their monies were stolen [36].

Typical SQL injection can be executed in two ways, by adding a code within the original SQL query or by adding a new malicious query to form multiple queries [11], [36]. For instance, in *SELECT * FROM Users WHERE UserID=' $ID' AND Password='$pwd';*
hacker can enter userID as ***' OR 1=1 - -*** instead of a genuine username, forming a new query
*SELECT * FROM Users WHERE UserID='* ***' OR 1=1 - -*** *AND Password='$pwd';*
1=1 is always true, - - terminates the query meaning that a table of users will be displayed without knowing the password, exposing all accounts [34], [35], [36].

8 CROSS SITE SCRIPTING

Cross site scripting (XSS) attack occurs when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user [38]. The attack takes advantage of invalidation of user's inputs and the retrieved contents from the application's server [34]. On successful attack, hacker can be able to capture users' session cookies thus compromising their accounts, installing malware into the web browser or host, monitoring web browsing habits or redirecting users to a phishing website [38], [39].

XSS malicious code is injected in the form of scripting languages most notably JavaScript. Html tag <body> with attributes such as onload, onmouseover or onerror is also used to inject the codes [38]. There are two forms of XSS, reflected XSS and stored XSS. In reflected XSS, user is enticed to click on the URL link provided in the phishing spam. The linked XSS code injected rogue website prompts user to provide inputs and then forward them to the vulnerable website's server along with XSS code [38], [39]. The server returns the content with XSS code which in turn is executed at the browser and then hijacks user session.

For stored XSS, user's inputs are stored into the application's database along with the XSS code. When the same data set is retrieved by any other user to the browser, the code is also invoked and executed to hijack users' sessions [34], [38], [39]. Samy worm, in 2005, deployed this technique to infect more than one million user accounts of MySpace in just 24 hours [40].

9 BLACKHAT SEARCH ENGINE OPTIMIZATION (SEO)

This is a technique used by hackers to poison a search engine such as Google, Yahoo or Bing by injecting and ranking highly their malicious links when popular trends or events are searched [41]; [42]. Hackers design their malicious websites and then inject keywords of popular events such as Halloween and Olympics or link their sites to blogs/websites with articles about those events [42]. When search results are presented, malicious links are usually ranked highly compared to legitimate links due to their richness in the keywords. When links are followed by users, they inject malware into the web browsers or hosts leading to phishing activities.

92% of the poisoned search results contain images of the related events while 8% being text based results [41]. Bing is found to be the most victimized engine with 65% of all poisoned results, Google being the second with 30% [41].

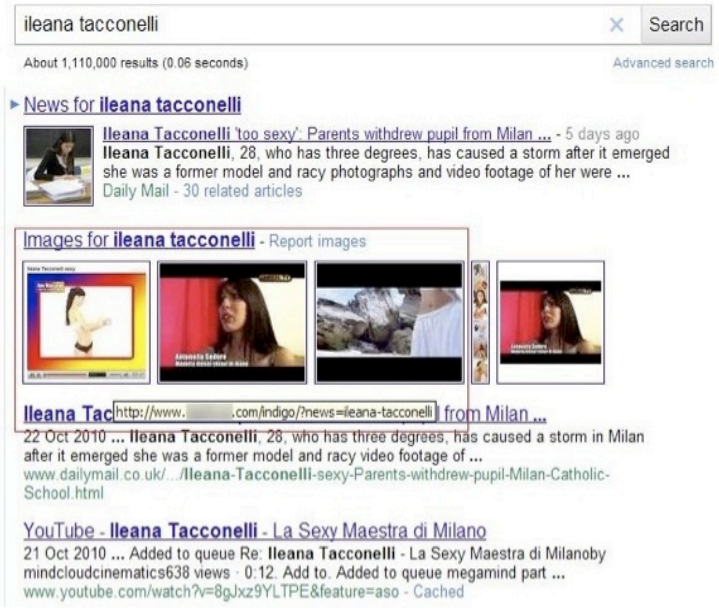

Figure 5 A typical BlackHat SEO with image based malicious link ranked second in a search result [43].

10 ROGUE SSL CERTIFICATES

There has been a tremendous increase in the use of SSL encrypted channels by websites to protect their communications from man-in-the-middle attacks [6], [12]. Some websites like Facebook, Google, Twitter and others have extended the use of secured channels from log in pages only to other non-transactional pages [12]. Hackers have also started to adopt the authentication approach to legitimize their malware or phishing websites by signing them with genuine looking SSL certificate keys.

One way of hackers to acquire the certificates is by purchasing them from Certificate Authorities (CA) using fake company identities. CAs with improper validation procedures of certificate requests have fallen in this trap in many cases. For instance in May 2012, authors of banking trojans in Brazil were able to purchase certificates from Comodo, the CA, using false identities, to sign their trojans and then launch massive phishing attacks [6], [44].

In other cases, hackers break into CAs' networks and generate fraudulent certificates and use them in multiple attacks [12]. In 2011, DigiNotar, a Dutch CA, was attacked by one hacker leading to generation of 500 certificates which were then used for Google related hacking activities [44].

11 MOBILE PHONE PHISHING

The popularity of smartphones among global phone users has encouraged businesses to innovate mobile services such as mobile payments or bank transfers, making mobile phones as one of the most attractive arenas to phishers. Phishers have developed variants of malware to hijack smartphones, using mobile OS exploits, to steal users' data or sending premium rated contents [6], [7]. With a market share of 72%, android OS is the main target of mobile threats followed by Apple's iOS at 14% [6].

More than 1,300,000 android malware belonging to few malware families and variants were observed in the wild in 2012 only, raised by 58%

compared to 2011 [6], [7]. 40.6% were premium service abusers, 24.9% data stealers, 22.8% malicious downloaders while the rest were adware, click fraudsters and rooters [7]. Publicly reported mobile OS vulnerabilities have also been increasing over the years, reaching 415 in 2012 only, suggesting that as more exploits are found, phishers keep developing new malware variants to use these exploits [6].

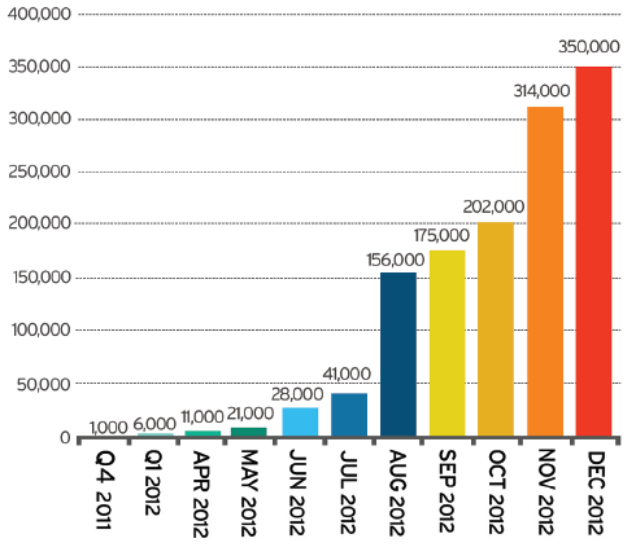

Figure 6 Growth of android malware between 2011 and 2012 as observed by Trend Micro [7].

Malware are distributed through official app store such as Google play or third party stores by trojanized legitimate apps [6], [12]. Once infected app is downloaded, it gets installed by exploiting a particular OS vulnerability. Malware can scan and steal personal data from the phone, data to be entered in a particular mobile website or monitoring web browsing habits of the user and then send to the phisher's server [7]. In some cases, malware can access and purchase apps from mobile app stores on behalf of the phone owner [23]. A malware can silently generate and frequently send premium contents such as sms to premium rate numbers while the bill is charged to the phone's owner [6], [7], [12]. A phishing sms can be generated and sent by a malware, containing a link to a phishing website which when accessed by a user, personal data can be stolen [45].

Large botnets of mobile malware have been observed in the wild, controlling hundreds of thousands of mobile phones [6].

12 SOCIAL MEDIA AND WEB 2.0 PHISHING

Scams through social networking sites such as Facebook, Twitter, Instagram, Tumblr and others appear to be a popular attacking trend today, Facebook being the leading victim [6], [23]. Phishing via social media grew from 8.3% of all phishing attacks in 2010 to 84.5% in 2011 [8]. These attacks are preferred by phishers because users often trust messages from their friends while users' messages can quickly propagate to large communities of friends [6]. Also the media are easy source of personal data as users expose a lot of their credentials such as birthdates, mobile numbers, friends' contacts, addresses, driving license details and even credit card particulars [6], [23], [46]. Phishers use these data to break user accounts' passwords, collecting email address lists to send phishing spams, spreading phishing messages in the social media or making illegal online purchases [6], [23]. Obtained mobile numbers observed to be used for smishing by sending premium rated contents [23].

Phishing messages are spread with messages and/or images often about product offers accompanied with phishing links [6], [23]. To complete processing the offers, users are supposed to follow the links which direct them to submit their personal data. In other cases, the links lead to installation of phishing malware. Fake "likes" can be embedded in an image based Facebook post which when clicked, leads a user to a phishing website or installation of a phishing malware [23].

Figure 7 A typical twitter scam message with a phishing link [6].

Web 2.0 sharing media sites such as YouTube and Digg have also experienced phishing attacks of their own forms [42]. Phishers, using their bogus site accounts, spread enticing comments to articles/videos of popular events [42]. These comments contain malicious links which lead to phishing websites or downloading of phishing malware.

Hackers have also been able to inject rogue web browsers adds-on to allow display of their phishing advertisements in web 2.0 sites. When these ads are clicked, they lead to phishing websites or downloading of phishing malware. Wikipedia has experienced this form of attack through a fake Google Chrome add-on [23].

13 CLOUD COMPUTING ATTACKS

37% of global businesses had already adopted cloud services by 2011 and increased by 20% in 2012 [6], [12]. From emails, financial data to advertisements, companies today go cloud to reduce their ICT operational costs as well as data security risks. Though cloud providers have heavily invested in security measures, consolidation of massive data at one point is a lucrative attraction to hackers [6]. Intrusion can start from a cloud client or through cloud provider, possibly through spear phishing, to hijack provider's infrastructure.

Few incidents of cloud attacks have been reported so far but it is promising to be one of the biggest vectors in the near future. For instance, in 2012, Dropbox file sharing cloud service was hacked leading to a breach of thousands of usernames and passwords of users [23].

14 CONCLUSION

Spear phishing and use of malware are the leading vectors in all phishing attacks today. Though traditional phishing spam rate is decreasing every year, it still contributes significantly in numbers of global phishing attacks. New phishing trends have emerged in recent times such as malvertising, search engine optimization, mobile phishing and social media attacks and promise to be the leading vectors in the near future. New corporates' trend towards cloud is already attracting phishers as massive harvests of data are centralized at fewer points. SQL injections, XSS and pharming vectors are still persistent over the years and appear not to vanish in the near future.

Phishing has been successful mainly due to ignorance and lack of awareness of users and businesses on the best practices of internet and computer safety. Failure to frequently patch operating systems and applications expose many software vulnerabilities that are exploited by malware. Users still find it hard to distinguish phishing emails and calls from legitimate ones. Majority of home users use default settings of their wireless routers. Some web developers do not validate inputs of their web applications. Many businesses today have mobile websites and social media accounts which increase availability of their information for spear phishing while exposing their customers to mobile and social media attacks.

Businesses need to invest more in securing their applications, limiting their online information and have specific programs to train their employees and customers on anti-phishing practices. Specific security training software such as phishme can be used by firms to practically engage their staff in learning spear phishing. Also firms must have specific email gateway solutions with spear phishing protection capabilities such as proofpoint. Websites of online businesses should be equipped with interesting programs to educate their customers on ways to evade phishing traps.

Cloud service providers must invest heavily in security measures, from multi-layer secured infrastructure approach to strong authentication procedures to access clients' applications and data. Zero-day vulnerabilities should immediately be addressed by software vendors and initiate imminent public awareness of the patches. Online business community must abandon the use of SSL certificates for extended SSL certificates (EV) to prevent phishers from buying rogue certificates from certificate authorities (CA).

15 REFERENCES

1. Ollman, G., (2004), "The Phishing Guide: Understanding and Preventing Phishing Attacks", *The Next Generation Security Software*.
2. Banday, M.T., Qadri, J.A., (2007). "Phishing - A Growing Threat to E-Commerce," *The Business Review*, 12(2): 76-83.
3. Anti-Phishing Working Group (APWG), (2012), *Phishing Activity Trends Report 4th Quarter 2012*, APWG.
4. Lynch J., (2005), "Identity theft in cyberspace. Crime control methods and their effectiveness in combating phishing attacks", *Berkeley Technology Law Journal*, 20: 259-300.
5. Symantec Corporation, (2012), "2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually", *Symantec Press Release*. Available at: http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02 [Accessed September 2013].
6. Symantec Corporation, (2013), *Symantec Internet Security Threat Report 2013*, Symantec Corporation.
7. TrendLabs, (2012a), *Evolve threats in a 'post-pc' worl*d, TrendLabs Annual Security Roundup, Trend Micro.
8. RSA, (2013), *The year in phishing 2012*, EMC.
9. Dhamija, R., Tygar, J., Hearst, M., (2006), "Why Phishing Works?", *Proceedings of the conference on Human factors in Computing Systems (CHI-2006)*, pp 581-590. Available at: ACM Digital Library [Accessed September 2013].
10. Emigh, A., (2005), "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures", *Radix Labs*.
11. Nagunwa, T. (2008), *Investigation of data privacy threats in online retail industry and assessment of strategies used in mitigating their impacts*, Msc Thesis, Dublin Institute of Technology.
12. Symantec Corporation, (2011b), *May 2011 Intelligence Report*, Symantec Corporation.
13. Garera, S., Provos, N., Chew, M., Rubin, A. (2007), "A Framework for Detection and Measurement of Phishing Attacks", *Proceedings of the 2007 ACM Workshop on Recurring Malcode*, pp 1-8. Available at: ACM Digital Library [Accessed September 2013].
14. Symantec Corporation, (2011a), *Defend your institution against Trojan-aided fraud: Banking Trojan*, Symantec Corporation.
15. Symantec Corporation, (2011c), *Internet security threat report: 2011 trends*, Symantec Corporation.
16. Aaron, G., Rasmussen, R., (2013), *Global Phishing Survey: Trends and Domain Name Use in 2H 2012*, Anti-Phishing Working Group (APWG).
17. Savvas, A., (2012), "91% of cyberattacks begin with spear phishing email", *Tech World*. Available at: http://news.techworld.com/security/3413574/91-of-cyberattacks-begin-with-spear-phishing-email/ [Accessed September 2013].
18. Ashford, W., (2013), "FBI warns of increased spear phishing attacks", *Computer Weekly*. Available at: http://www.computerweekly.com/news/2240187487/FBI-warns-of-increased-spear-phishing-attacks [Accessed September 2013].
19. TrendLabs, (2012b), *Spear-phishing email. The most favored APT attack bait*, Trend Micro.
20. Cinstantin, L., (2013), "Mandiant report on Chinese cyberespionage used as bait in spear-phishing attacks", *Computer World*. Available at: http://www.computerworld.com/s/article/9237036/Mandiant_report_on_Chinese_cyberespionage_used_as_bait_in_spear_phishing_attacks [Accessed September 2013].
21. Hicks, D., (n.d), "Vishing: Another Internet Fraud Scam", *Federal Reserve Bank of Boston*, Available at: http://www.bos.frb.org/consumer/spotlight/vishing.htm [Accessed September 2013].
22. The Guardian, (2013), "'Vishing' scams net fraudsters £7m in one year", *The Guardian*. Available at: http://www.theguardian.com/money/2013/aug/28/vishing-scams-fraudsters-seven-million-pounds [Accessed September 2013].
23. PandaLabs, (2013), *PandaLabs Annual Report 2012*, Panda Security.
24. Stewart, J. (2003), "Reverse Proxy Spam Trojan, Migmaf", http://www.secureworks.com/research/threats/migmaf/ [Accessed July 2008].
25. Levy, E., Arce, A., (2004), "Criminals Become Tech Savvy, Security and Privacy", *IEEE Communications Society*, 2 (2): 65-68.

26. Westervelt, R., (2010), "Security report finds rise in banking Trojans, adware, fewer viruses", *Search Security*, Available at: http://searchsecurity.techtarget.com/news/1378277/Security-report-finds-rise-in-banking-Trojans-adware-fewer-viruses [Accessed September 2013].
27. McAfee Labs, (2013), "McAfee Threats Report - First Quarter 2013", *McAfee*.
28. Sophos, (2013), *Security threat report 2013*, Sophos.
29. PC Tools, (2011), "Lizamoon: A Serious SQL Injection Attack", *PC Tools*, Available at: http://www.pctools.com/security-news/lizamoon-a-serious-sql-injection-attack/ [Accessed September 2013].
30. Berinato, S., (2006), "Attacks of the Bots", *Wired Magazine*, 14:11.
31. Schiller, C., Binkley, J., Harley, D., Vron, G., Bradley, T., Willems, C., Cross, M., (2007), "Botnets the Killer Web App", *Syngress Publications*.
32. Stamm, S., Ramzan, Z., Jakobsson, M., (2006), "Drive-by Pharming", Indiana University School of Informatics and Cumputing, Technical Report TR641. Retrieved from: http://www.cs.indiana.edu/cgi-bin/techreports/TRNNN.cgi?trnum=TR641 [Accessed September 2013].
33. Sharf, E., (2012), "Christmas-Themed Facebook Scams: How Cybercrooks Kick it up a Notch and Piggyback on Big Brands", Websense Security Labs Blog, Available at: http://community.websense.com/blogs/securitylabs/archive/2012/12/06/merry-xmas-on- facebook.aspx [Accessed September 2013].
34. Kals, S., Kirda, E., Kruegel, C., Jovanovic, N., (2006), "Secubat: A Web Vulnerability Scanner", *Proceedings of the 15th international conference on World Wide Web*, pp 247-256. Available at: ACM Digital Library [Accessed September 2013].
35. Rietta, F., (2006), "Application Layer Intrusion Detection for SQL Injection", *Proceedings of the 44th Annual Southeast Regional Conference*, pp 531-536. Available at: ACM Digital Library [Accessed September 2013].
36. The PHP Group, (2013), "PHP SQL Injection", *The PHP Group*, Available at: http://php.net/manual/en/security.database.sql-injection.php [Accessed September 2013].
37. Jacob, J., (2011), "What is Lizamoon, the viral scareware that infected four million websites", *International Business Times*, Available at: http://www.ibtimes.com/what-lizamoon-viral-scareware-infected-four-million-websites-278289 [Accessed September 2013].
38. OWASP, (2013), "Cross-site Scripting (XSS)", *OWASP*, Available at: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS) [Accessed September 2013].
39. Glynn, F., (n.d), "XSS Cheat Sheet Prevent Cross Site Scripting Attacks, Injections", *Veracode*, Available at: http://www.veracode.com/security/xss [Accessed September 2013].
40. Auger, R., (2011), "Cross Site Scripting", *Web Application Security Consortium*, Available at: http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting [Accessed September 2013].
41. Leyden, J., (2012), "Bing is the most heavily poisoned search engine, study says" The register, Available at: http://www.theregister.co.uk/2012/10/08/bing_worst_search_poisoning/ [Accessed September 2013].
42. PandaLabs, (2009), *Annual Report PandaLabs 2009*, Panda Security.
43. Arfunnis, (2010), "Searching for 'Ileana Tacconelli' leads to Fake Adobe Flash Update and TDSS", *PC Tools*, Available at: http://www.pctools.com/security-news/ileana-tacconelli-fake-adobe-flash-update-tdss/ [Accessed September 2013].
44. Ragan, S., (2012), "Comodo Certificates Used to Sign Banking Trojans in Brazil", *Security Wee*k, Available at: http://www.securityweek.com/comodo-certificates-used-sign-banking-trojans-brazil [Accessed September 2013].
45. Tufts, A. (2012), "How to protect your Android against 'smishing'", One Click Root, Available at: http://www.oneclickroot.com/how-to/how-to-protect-your-android-against-smishing/ [Accessed September 2013].
46. Kharouni, L., (2012), "The Dangers of Posting Credit Cards, IDs on Instagram and Twitter", TrendLabs Security Intelligence Blog, Available at: http://blog.trendmicro.com/trendlabs-security-intelligence/the-dangers-of-posting-credit-cards-ids-on-instagram-and-twitter/ [Accessed September 2013].