Mobile Devices
A Phisher's Paradise

Nikos Virvilis[1], Nikolaos Tsalis[1], Alexios Mylonas[1, 2] and Dimitris Gritzalis[1]
[1] *Information Security & Critical Infrastructure Protection Laboratory, Dept. of Informatics, Athens University of Economics & Business, 76 Patission Ave., Athens, GR-10434, Greece*
[2] *Faculty of Computing, Engineering and Sciences, Staffordshire University, Beaconside, Stafford, ST18 0AD, U.K.*

Keywords: Phishing, Mobile, Smartphone, Android, Ios, Windows, Web Browser, Security.

Abstract: Mobile devices - especially smartphones - have gained widespread adoption in recent years, due to the plethora of features they offer. The use of such devices for web browsing and accessing email services is also getting continuously more popular. The same holds true with other more sensitive online activities, such as online shopping, contactless payments, and web banking. However, the security mechanisms that are available on smartphones and protect their users from threats on the web are not yet mature, as well as their effectiveness is still questionable. As a result, smartphone users face increased risks when performing sensitive online activities with their devices, compared to desktop/laptop users. In this paper, we present an evaluation of the phishing protection mechanisms that are available with the popular web browsers of Android and iOS. Then, we compare the protection they offer against their desktop counterparts, revealing and analyzing the significant gap between the two.

1 INTRODUCTION

The proliferation of smarpthones is increasing. According to (Gartner, 2014 a), in the Q3 of 2013 more than 445M mobile phones were sold, out of which 250M were smartphones. Despite the unarguable important benefits and capabilities which they offer, the use of such devices - especially for sensitive online tasks - has turned them into a new profitable target for attackers. More specifically, nowadays: (a) smartphones are frequently used as part of a two-factor authentication scheme for online services (e.g. e-banking), (b) wireless payments using NFC-enabled smartphones are getting continuously more popular, exceeding 235B$ in 2013 (Gartner, 2014 b), (c) the use of smartphones in business is also increasing (e.g. under the Bring Your Own Device (BYOD) trend), even in sensitive environments, with iOS and Android devices getting accredited for use in the US Dept. of Defence (Capaccio, 2014), and (d) smartphones have become appealing targets as recent reports have revealled (CBC, 2014).

One of the threats that target (smartphone) users suffer by is phishing. Phishing can be deemed as one of the most popular and profitable attacks, having almost 450,000 attacks in 2013 and estimated losses of over 5.9B$. NIST defines phishing (Mell, 2005) as: *"Phishing refers to use of deceptive computer-based means to trick individuals into disclosing sensitive personal information. Phishing attacks aid criminals in a wide range of illegal activities, including identity theft and fraud. They can also be used to install malware and attacker tools on a user's system."*

Although the majority of phishing attacks are widespread and focus on financial gain, targeted phishing attacks also exist. These attacks are widely known as *spear-phishing* and have been used in a large number of sophisticated attacks against government, military and financial institutions. The analysis of past major security incidents, involving Advanced Persistent Threats (APT) (Virvilis and Gritzalis, 2013) (Virvilis, 2013), has revealed that attackers used targeted phishing attacks in order to gain access to the internal network of their target.

In this paper, we evaluate the protection offered against phishing attacks on smartphone platforms. The scope of our analysis includes the popular browsers in Android and iOS. We measured the protection offered by these browsers, by accessing more than 5,000 manually verified phishing URL, within a period of two months. We

Virvilis N., Tsalis N., Mylonas A. and Gritzalis D..
Mobile Devices: A Phisher's Paradise.
DOI: 10.5220/0005045000790087
In *Proceedings of the 11th International Conference on Security and Cryptography* (SECRYPT-2014), pages 79-87
ISBN: 978-989-758-045-1

performed the same evaluation against popular desktop browsers and compared their detection rate. Our results indicate a significant gap in the effectiveness of phishing protection between smartphone and dekstop browsers. Finally, we collected and analyzed all the URL of phishing campaigns that have not been filtered out by the browsers in any of the two platforms to identify common characteristics that enable us to strengthen our defences against the above threat.

This paper makes the following contributions:

- It provides a comparison of the phishing protection offered by popular browsers in Android, iOS and Windows platforms.
- It provides insights of the characteristics of successful phishing campaigns, i.e. phishing URL that were not filtered out by web browsers. We discuss how these characteristics can be used to further stregthen the defences against phishing.

The remainder of the paper is structured as follows. Section 2 presents related work. Section 3 describes the methodology and Section 4 presents our results. The paper ends with conclusions and suggestions for further work in Section 5.

2 BACKGROUND

The main defence against phishing attacks is based on lists (i.e. 'blacklists'), which are used by browsers to identify if a requested URL must be blocked or not. Such a prominent blacklist is Google's Safe Browsing (Google, 2014), which protects users both from phishing and malware web sites. Safe Browsing is currently used by Google Chrome, Mozilla Firefox and Apple Safari browsers. Internet Explorer is using Microsoft's proprietary blacklist, the SmartScreen (Microsoft, 2014). Other browsers also use their own proprietary lists, as well as aggregate information from third parties. For instance, Opera uses a combination of blacklists from Netcraft (Netcraft, 2014) and PhishTank (PhishTank, 2014), as well as a malware blacklist from TRUSTe (Abrams et al., 2013).

Although each blacklist implementation is different, all of them follow a basic concept, i.e., before a URL is loaded by the browser, a URL check occurs via data from a local or remote database. If the current URL matches a known malicious site, a warning is raised to the user advising her to avoid browsing to the current URL. Limited information is available on how these blacklists get updated and maintained, as this could enable attackers to bypass them more easily. However, a considerable part of the submissions to blacklist are performed manually by users (PhishTank, 2014).

Based on the number of the submissions to anti-phishing sites, such as PhishTank, it turns out that phishers are still very active, generating several hundred phishing pages/domains on a daily basis. The main reason for the popularity of such attacks, regardless of the attackers objective (e.g. identity theft, malware infection, information gathering, etc.), is their effectiveness. The use of blacklists always allows a window of several hours - on average 26 hours - when attackers can exploit their victims (Abrams et al., 2013). To make the matters worse, our work shows that this window is significantly larger on mobile devices (i.e. Safari Mobile) due to the way blacklists are getting updated.

The academic literature has also focused on combating this threat. As a result, a number of approaches have been proposed in an effort to protect the users from phishing attacks. This research varies from surveys regarding user awareness, to experiments of the effectiveness of current security mechanisms and proposals of novel ones. More specifically, the work in (Banu et al., 2013), (Rosiello et al., 2007), (Rani and Dubey, 2014) focuses on phishing with regards to its properties, characteristics, attack types, and available counter-measures. Also, (Rani and Dubey, 2014) and (Jansson and Von Solms, 2013) present a survey on user training methods, as well as their effectiveness against phishing attacks, as user participation plays an major role in phishing protection.

Literature has also focused on the use of visual indicators to protect users from phishing. In (Bian, 2014) an overview of the warning indicators and its advances over the last decade is presented. Also, (Darwish and Bataineh, 2012) has surveyed users' interaction with security indicators in web browsers. A study on the effectiveness of browser security warnings was published in (Akhawe and Felt, 2013), focusing on the Google Chrome and Mozilla Firefox browsers. The authors collected over 25M user reactions with phishing and malware security warnings, measuring the user reactions to these warnings. A similar study (Egelman and Schechter, 2013) analyzed the impact on the users' decision based on the choice of background color in the warning and the text descriptions that were presented to them. In (Egelman et al., 2008), the authors conducted a survey regarding the effectiveness of security indicators, comparing the warning messages of Firefox and Internet Explorer.

In (Seng et al., 2009), the authors focused on the effectiveness of phishing blacklists, in particular on their update speed and coverage. The authors used 191 phishing sites that had been active for 30 min or less, and compared 8 anti-phishing toolbars. Less than 20% of the phishing sites were detected at the beginning of the test. In addition, they identified that blacklists were updated in different speeds, which varied from 47-83%, 12 hours after the initial test. Similarly in (Kirda and Kruegel, 2005), the authors proposed the use of 'Anti-Phish', a browser extension for the Mozilla Firefox browser, so as to detect web site-based phishing attacks.

A Novel-Bayesian classification, based on textual and visual content, was proposed in (Zhang et al., 2011). Authors used a text classifier, an image classifier, and a fusion algorithm to defend against known properties of phishing attacks. Furthermore, (Rosiello et al., 2007) provides a methodology that aims to distinguish malicious and benign web pages, which is based on layout similarity between malicious and benign web pages.

In (http://www.av-comparatives.org/images/docs/avc_phi_browser_201212_en.pdf, 2014), the authors analyzed 300 phishing URL and measured the effectiveness of desktop browsers in detecting them. Opera browser offered the highest level of protection, by blocking 94.2% of the phishing sites. In (Mazher et al., 2013), the authors tested the effectiveness of anti-phishing add-ons for Internet Explorer, Google Chrome and Mozilla Firefox. In their evaluation Google Chrome outscored the other browsers. Finally, in (Abrams et al., 2013) authors tested popular desktop web browsers (i.e. Firefox, Chrome, Opera, IE, Safari), focusing on the time required for browsers to block a malicious site. The initial results (zero-day) ranged from 73.3% (IE) to 93.4% (Safari), while the final results (7-day) varied from 89.3% (IE) to 96.6% (Firefox).

A number of anti-phishing mechanisms have been proposed for use in smartphones. In (Vidas et al., 2013), the authors investigate the viability of QR-code-initiated phishing attacks (i.e. QRishing) by conducting two separate experiments. A similar approach was presented in (Xu and Zhu, 2012), where the authors worked on how notification customization may allow an installed Trojan application to launch phishing attacks or anonymously post spam messages.

Related work on browser security revealed that security controls that are typically found on desktop browsers are not provided in their smartphone counterparts (Mylonas et al., 2013), (Mylonas et al., 2011). In our work we also find that smartphone browsers still do not offer anti-phishing protection. Moreover, the analysis in (Mylonas et al., 2013) revealed that the implementation of the security controls (among them the security control against phishing attacks) was not hindered by restrictions from the security architecture (i.e. the application sandbox). The related literature does not adequately focus on the effectiveness of anti-phishing mechanisms on Android and iOS browsers.

3 METHODOLOGY

The scope of our work includes popular desktop browsers, i.e. Chrome, Internet Explorer, Firefox, and Opera, together with their smartphone counterparts. In smartphones, the scope of our analysis focuses in iOS and Android, as they are the prominent smartphone platforms, having ~90% of the global market share (Mylonas et al., 2011) (Bradley, 2014).

For the evaluation of smartphone browsers, an iPhone 5S was used for iOS, and a Sony Xperia Tipo for Android. The smartphone counterparts of desktop browsers may appear either as a pre-installed browser (e.g. Safari Mobile in iOS), or as a third party application that the user has to download from an app marketplace (e.g. Firefox Mobile for Android). Their availability in the two smartphone platforms is heterogeneous (see Table 1).

To evaluate the protection that is offered by the above mentioned web browsers, we visited phishing URL that were indexed in PhishTank. We selected phishing URL that were confirmed - i.e. PhishTank confirmed the reported URL as a fraudulent one - and online. However, the state of a phishing URL is dynamic, namely a confirmed URL might be cleaned or be taken down short after its submission to an anti-phishing blacklist list. Therefore, all the URL were manually examined to separate web pages that have been cleaned (i.e. false positives) from the ones that were fraudulent and not filtered out by the browsers' blacklists (i.e. false negatives).

We collected URL from PhishTank for 2 months (Jan-Mar 2014). During this period we noticed that their number fluctuated significantly, with an average of several hundred URL per day. Although some of the evaluation could be automated (e.g. URL that returned HTTP Error Codes or URL for which the browsers raised warnings), it was necessary to verify whether URL, that were not filtered- out by the browsers as fraudulent, were actually legitimate sites (i.e. not false negatives).

Table 1: Browser availability in iOS and Android

	iOS 7.0.4	**Android 4.0.4** (Sony Xperia Tipo)	**Windows 7** (64bit)
Safari Mobile	X		
Chrome Mobile	X	X	
Opera Mini	X	X	
Browser†		X	
Firefox Mobile		X	
Opera Mobile		X	
Chrome			X
Firefox			X
Internet Explorer			X
Opera			X

† 'Browser' is the pre-installed browser in Android

Table 2: Support of anti-phishing mechanisms.

Platform	**Browser name**	**Phishing protection**†
iOS	Safari Mobile	Y
	Chrome Mobile	N
	Opera Mini	N
Android	Browser†	N
	Firefox Mobile	Y
	Chrome Mobile	N
	Opera Mobile	Y
	Opera Mini	N
Windows 7	Firefox	Y
	Chrome	Y
	Opera	Y
	Internet Explorer	Y

† **Y**: Security control available, N: Security control not available
†† 'Browser is the pre-installed browser in Android

This required manual verification. To keep the analysis manageable, each day we manually verified at most 100 URL, which were indexed in PhishTank as confirmed and online. In cases, more than 100 URL were indexed in PhishTank on a given day, we randomly selected 100 URL from them.

In total, we collected and evaluated the web browsers that were in our scope, against 5651 phishing sites. Each URL was categorized into one of the following three categories:

a. *Blacklisted*: The URL was filtered-out by the web browser, i.e. the user receives a warning indicating the threat of a potential phishing site.

b. *False Negative*: Denoting a phishing site that was manually verified by us as fraudulent, but was not on the browser's blacklist (e.g. the browser generated no warning).

c. *Non-Phishing/Timeout/Error*: A site that during our manual verification had either been cleaned, or suspended/taken down when we accessed it.

For each URL found to be a false negative, we kept the URL and the contents of the malicious phishing page. This enabled us to identify the most popular phishing targets, as well as identify patterns that helped us improve the detection mechanisms.

Finally, for each URL that was collected, we used the Safe Browsing Lookup API (Google, 2014) to query directly the Safe Browsing database. This enabled us, to compare the results from the Safe Browsing Lookup API with the web browsers' results.

4 RESULTS

4.1 Overview

A finding that arose early in our analysis is that only a subset of the mobile browsers supported anti-phishing protection (see Table 2). Thus, their respective users were unprotected from phishing attacks. On the contrary, all desktop browsers provided anti-phishing protection, even though their effectiveness differed significantly. Table 2 summarizes the availability of anti-phishing protection per operating system and browser (as of March 2014).

The results of our analysis are presented in Figs. 1-3. More specifically, (a) Fig. 1 presents the percentage of blocked URL per browser,

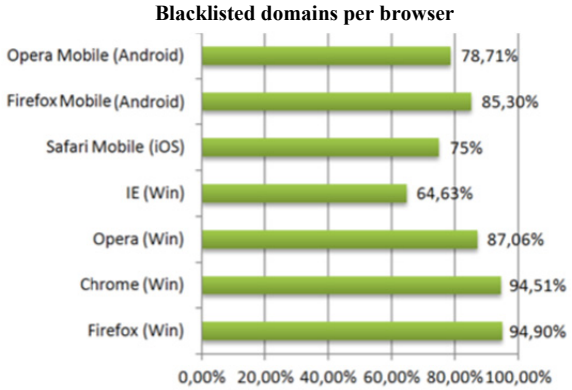

Figure 1: Percentage of blocked URL (n=5651).

(b) Fig. 2 depicts the percentage of active phishing URL that were not filtered out, namely the ones that were not in the browser's blacklist and were manually verified as active malicious sites (false negatives), and (c) Fig. 3 presents the percentage of

URL that were not in the browser's blacklist and were manually verified during our analysis as non-malicious sites (i.e. URL that had been cleaned, or domains that had been taken down or were not accessible when we accessed them). The browsers that did not support any anti-phishing mechanism are not included in the charts, as their detection rate is zero.

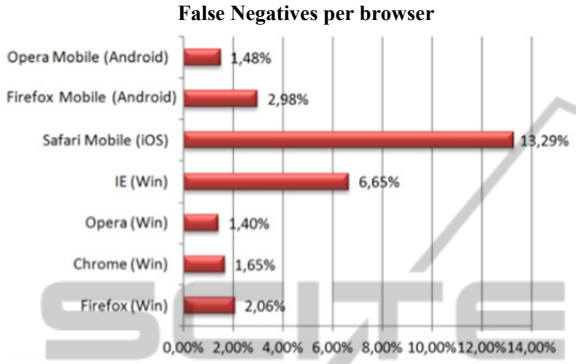

Figure 2: Percentage of phishing URL that were not filtered out (n=5651).

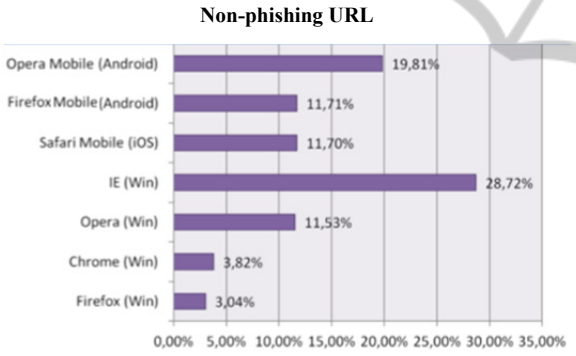

Figure 3: URL not in blacklist and not phishing (manual verification, n=5651).

For further information, the detailed results (per browser) are depicted in the following table:

Table 3: Detailed results per browser.

Browser	Black-listed	False negatives	Non-phishing
Safari Mobile (iOS)	4239	751	661
Firefox Mobile (Android)	4821	168	662
Opera Mobile (Android)	4448	84	1119
Firefox (Windows)	5362	117	172
Chrome (Windows)	5341	94	216
Opera (Windows)	4920	79	652
IE (Windows)	3653	376	1622

In the next sections we discuss the findings in every platform, the protection offered by Safe Browsing API. Also, we perform a brief analysis of phishing URL that were not filtered out (i.e. false negatives). Detailed results per browser are available in the Appendix.

4.2 iOS Browsers

In iOS devices, Mobile Safari - which is the default (i.e. pre-installed) web browser of the platform – supports the detection of fraudulent websites by utilizing Google's Safe Browsing blacklist. Our evaluation revealed that the anti-phishing control suffers from a significant design weakness. This holds true, since the Safe Browsing blacklist is only updated when a user synchronizes her iOS device with iTunes (on a desktop/laptop). Considering that a subset of iOS users may not synchronize their devices frequently (e.g. when they are on a trip) or at all, they end up with an outdated blacklist. Thus, these users eventually receive only a limited protection against phishing attacks.

Our analysis also revealed that (see Fig. 1-3): (a) Mobile Safari had significantly more false negatives (i.e. phishing URL that were not filtered out) comparing to the other mobile web browsers, and (b) iOS users can be protected from phishing attacks only when they use Mobile Safari, since Chrome Mobile and Opera Mini do not offer such protection.

4.3 Android Browsers

In Android, the default web browser (commonly known to Android users as "Browser") offers no phishing protection. The same applies to the Mobile Chrome and Opera Mini browsers. Our evaluation revealed that Android users can only be protected from phishing attacks if they use Firefox Mobile and Opera Mobile. Also, our results revealed that the two above mentioned browsers offer comparable but not equal protection from phishing with their desktop counterparts.

If one considers that: (a) not all users are willing and/or capable to install a third party browser on their devices and (b) the pre-installed browser offers no protection, then a very large number of Android users is not adequately protected from phishing attacks.

4.4 Desktop Browsers

All desktop web browsers offered phishing protection using either Google's Safe Browsing (i.e.

Chrome and Firefox) or their own proprietary blacklists (i.e. in Opera and Internet Explorer). The protection against phishing in Chrome and Firefox was similar; both blocked almost all the fraudulent URL that we tested. At the same time, they achieved low false negatives. However, this similarity in their performance was expected, as both use the same blacklist.

During our experiments we found another issue with the synchronization of blacklists, which, similarly to (Abrams et al., 20013), offered a window of exploitation to phishers. We noticed that if the desktop browsers were not executing for a few minutes before we started our evaluation, then the blacklist was not properly updated. This is especially true for Firefox, as in this web browser we frequently encountered a large number of false negatives (i.e. phishing pages that were not blocked) during the first few minutes of our tests. This is very likely due to the way that the Safe Browsing protocol updates the list of malicious sites (Sobrier, 2014). Interestingly enough we did not face this problem in Chrome. In (Abrams et al. 2013), authors highlighted the same issue during their tests for an older version of Chrome, which adds to our suspicion that the inconsistent results are due to the Safe Browsing protocol's update procedure.

As summarized in Figs. 1-3, Opera outscored in our evaluation the rest browsers. Even though the percentage of blocked URL was less, this does not translate to a less accurate blacklist. This holds true, as the percentage of false negatives (i.e. the phishing sites that were not filtered out) is lower than both Chrome and Firefox. As a matter of fact, it seems that Opera's blacklist is updated more frequently, as it did not block URL that had been cleaned or taken down, while these URL were still blocked by the browsers that used the Safe Browsing blacklist.

Finally, the proprietary blacklist that Internet Explorer uses, i.e. Microsoft's SmartScreen, offered the least protection in the desktop browsers. As our results indicate, Internet Explorer had the highest rate of false negatives among them, i.e. filtered out fewer manually confirmed phishing URL than the other desktop web browsers.

4.5 Safe Browsing API

For each test URL of our analysis we used Google's Lookup API (Sobrier, 2014) to query directly the Safe Browsing blacklist, to compare its results with the browsers' results. The results from Safe Browsing Lookup API differed significantly from those of Chrome and Firefox browsers. More specifically, on average only 73.21% of the URL that were blocked by Chrome and Firefox, were reported as malicious by Google's Safe Browsing Lookup API. After manually verifying the URL that were not blocked, we noticed that their majority were active phishing sites (i.e. false negatives of the API).

Two ways are available for querying the Safe Browsing database: (a) using the Google Safe Browsing API v2, or (b) using the Lookup API (Google, 2014). The first, which is used by web browsers, offers better privacy as the browser does not need to send the queried URL to Google for analysis; also, it is optimized for a large number of requests. The latter offers simpler implementation (i.e. a single HTTP GET request) and can be used for testing up to 10.000 URL per day. Nevertheless, both API query the same database according to Google (Google, 2014) and should provide the same results.

Our experiments reveal that the results between these two ways differ significantly. This difference is not documented by Google. This may be due to the fact that: (a) web browsers use additional anti-phishing mechanisms which complement the Safe Browsing, and/or (b) the Safe Browsing API v2 and Lookup API do not query the same data set, contrary to Google documentation (Google, 2014).

4.6 Phishing Campaigns

During our experiments we noted every phishing campaign (both URL and page contents) that was manually verified as phishing, but was not filtered out by at least one of the web browsers in our scope that supported anti-phishing protection. The analysis of the phishing URL that were not filtered out aimed at identifying the most popular phishing targets. It also aimed at highlighting similarities between phishing campaigns that could be used to strengthen our defenses against such attacks. Table 4 summarizes these results.

Table 4: Main Phishing Campaigns.

Target	Percentage	String in URL
paypal.com	61.68%	48.19%
appleid.apple.com	15.17%	47.61%
Banks (Multiple)	4.41%	N/A
Web Email (Multiple)	5.10%	N/A
Random Campaigns	13.64%	N/A

PayPal was the primary target of the phishing campaigns, as 61.68% of the phishing URL that were tested targeted PayPal users.

The second most popular target was Apple, with 15.17% of the phishing URL targeting Apple users. A compromised Apple account gives access to all information stored on the victim's iCloud account (iCloud, 2014), including contacts, calendar, email, files and photos. Therefore, this is another fruitful target for attackers.

The rest of the phishing results have been divided in three generic categories:

a. *Banks* - Phishing campaigns that target online banking from various banks.

b. *email* - Phishing campaigns that target web based email providers (Gmail, Yahoo Mail, Outlook).

c. *Misc* - Random phishing campaigns against other websites.

Our analysis revealed that in the two popular phishing campaigns, the 48.19% and 47.61% of them contained in their URL the word "paypal" or "apple", respectively. By including those strings in the beginning of the URL, the phishing attack is more likely to succeed against naive users who do not inspect the whole URL (examples appear in see Table 5).

Our results suggest that web browsers can implement URL filtering based on regular expressions, so as to increase their detection rate against sites that are not yet blacklisted. For instance, web browsers can change the color of the location bar or issue a warning to the user, when visiting a URL that includes the string of a popular site (e.g. "paypal", Table 5), while the URL does not originate from a benign web site (e.g. www.paypal.com or www.paypalobjects.com). Such a solution might not scale adequately for a large number of sites, but it could be implemented to protect a few hundred of popular ones, in the same way that Google Chrome implements Certificate Pinning for specific sensitive

Table 5: Phishing URL[1].

Target	URL[†]
Paypal	http://**paypal.com**.cgi-bin-websc5.b4d80a13c0a2116480.ee0r-cmd-login-submit-dispatch-5885d80a13c0d.b1f8e26366.3d3fae.e89703d295b4.a2116480e.e013d.2d8494db97095.b4d80a13c0a2116480.ee01a0.5c536656g7e8z9.real.domain.name.removed?cmd=_home&dispatch=5885d80a13c0db1f8e&ee=8ae65ec5a442891deac1bc0534a61adb
	http://**paypal.com**.*real.domain.name.removed*/update/?cmd=_home&dispatch=5885d80a13c0db1f8e&ee=46accb06788060b6e5ae1a1a964d625c

[†] The domain names have been anonymized

domains (OWASP, 2014). Nevertheless, such countermeasures can only partially address the problem. Only a multi-layered defense of both technical and procedural means, will enable us to defend effectively against the phishing threat (Theoharidou et al., 2010), (Theoharidou et al., 2009).

5 CONCLUSIONS AND FUTURE WORK

Nowadays phishing is one of the most popular and profitable attacks. Our work reveals that Android and iOS users are not adequately - or sometimes not at all - protected from this threat.

More specifically, our work evaluates the anti-phishing protection that is offered by web browsers within a period of two months. The scope of our analysis includes popular browsers in iOS, Android and Windows platforms. We evaluated and manually verified their protection against several thousand phishing URL.

Our results revealed that only a subset of browsers in iOS and Android offer potentially adequate phishing protection, leaving their users exposed to such attacks. For instance, in Chrome Mobile and Opera Mini do not offer anti-phishing mechanisms. In Android, which is currently the most popular smartphone platform, the pre-installed browser (i.e., Browser) does not offer anti-phishing protection.

Therefore, Android users who are incompetent and/or reluctant to install a third-party browser that offers this protection are exposed to phishing scams. In addition, these users might be unaware of the threat and/or of the browsers that offer the relevant protection.

Our results also point out that the anti-phishing protection that is offered by the mobile browsers is not similar to their desktop counterparts. This is true in cases where the same blacklist is used (e.g. in Safari Mobile that uses the Safe Browsing blacklist), and/or the same browser in different platform (e.g. Opera Mobile and Opera for desktop, Firefox Mobile and Firefox for desktop).

To make the matters even worse, our analysis has revealed implementation/design flaws that limit the effectiveness of blacklists usage. For instance, we discovered that Mobile Safari (i.e. the pre-installed browser in iOS) requires a synchronization with iTunes so as to download the latest version of Safe Browsing list. Thus, if users fail to synchronize their devices they will not be alerted when accessing

known phishing sites. Moreover, it is more likely that iOS users are unaware that failing to synchronize their device with iTunes lowers their security while they browse the web.

In desktop browsers, despite the fact that the popular web browsers included anti-phishing mechanisms, their effectiveness varied significantly. Internet Explorer offers the least protection from phishing attacks, while Opera offers the highest level of protection. Firefox and Chrome offered similar level of protection.

The above mentioned findings can be more worrisome if one considers the proliferation of mobile devices. We consider the lack of anti-phishing mechanism on mobile browsers important due to the impact of phishing attack to their users. We thus suggest that all vendors of mobile browsers need to implement protection mechanisms at least as efficient as the ones offered by the desktop browsers. This task is aided by the 'technological convergence' of desktops and mobile devices, as the latter devices gradually offer adequate resources for anti-phishing protection (e.g. blacklist). In the meantime, users of mobile devices can be protected against phishing attacks by installing the third-party web browsers that offer phishing protection and/or rely on filtering proxies.

For the future, we plan to further test the effectiveness of phishing blacklists that are provided by mobile platforms. We also plan to investigate and implement additional countermeasures that can be used to combat phishing.

REFERENCES

Gartner, "Gartner Says Smartphone Sales Accounted for 55 Percent of Overall Mobile Phone Sales in 3rd Quarter of 2013". (Online). 2014 Available at: https://www.gartner.com/newsroom/id/2623415 (Accessed: 10 Mar 2014).

Gartner, "Gartner Says Worldwide Mobile Payment Transaction Value to Surpass $235 Billion in 2013". (Online). Available at: https://www.gartner.com/newsroom/id/2504915 (Accessed: 10 Mar 2014).

Capaccio, N., "Apple Mobile Devices Cleared for Use on U.S. Military Networks". (Online). Available at: http://www.bloomberg.com/news/2013-05-17/apple-mobile-devices-cleared-for-use-on-u-s-military-networks.html (Accessed: 10 Mar 2014).

CBC, "Smartphones becoming prime target for criminal hackers". (Online). Available at: http://www.cbc.ca/news/technology/smartphones-becoming-prime-target-for-criminal-hackers-1.2561126 (Accessed: 09 Apr 2014).

Mell, P., Kent, K., Nusbaum, J., "Guide to malware incident prevention and handling", National Institute of Standards and Technology (NIST), 2005.

Virvilis N., Gritzalis D., "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?", *in Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing*, pp. 396-403, IEEE Press, Italy, 2013.

Virvilis N., Gritzalis D., "The Big Four - What we did wrong in Advanced Persistent Threat detection?", *in Proc. of the 8th International Conference on Availability, Reliability and Security*, pp. 248-254, IEEE, Germany, 2013.

Google, "Safe Browsing API". (Online). Available at: https://developers.google.com/safe-browsing/ (Accessed: 8 Mar 2014).

Microsoft, "SmartScreen Filter". (Online). Available at: http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/smartscreen-filter (Accessed: 8 Mar 2014).

Netcraft, "Phishing Site Feed". (Online). Available at: http://www.netcraft.com/anti-phishing/phishing-site-feed/ (Accessed: 8 Mar 2014).

PhishTank, "Join the fight against phishing". (Online). Available at: https://www.phishtank.com/ (Accessed: 8 Mar 2014).

Abrams R., Barrera O., and Pathak J., "Browser Security Comparative Analysis", NSS Labs, 2013. (Online). Available: https://www.nsslabs.com/reports/browser-security-comparative-analysis-phishing-protection (Accessed: 2 Feb 2014).

Banu, M. Nazreen, S., Munawara Banu, "A Comprehensive Study of Phishing Attacks", *in Proc. of the International Journal of Computer Science and Information Technologies*, vol. 4, issue 6, pp. 783-786, 2013.

Rosiello, A. P., Kirda, E., Kruegel, C., Ferrandi, F., "A layout-similarity-based approach for detecting phishing pages", *in Proc. of Security and Privacy in Communications Networks Workshops*, pp. 454-463, 2007.

Rani, S., Dubey, J., "A Survey on Phishing Attacks", *International Journal of Computer Applications,* vol. 88, issue 10, 2014.

Jansson, K., Von Solms, R., "Phishing for phishing awareness", *in Proc. of Behavior & Information Technology Conference*, vol. 32, issue 6, pp. 584-593, 2013.

Bian R. M., "Alice in Battlefield: An Evaluation of the Effectiveness of Various UI Phishing Warnings". (Online). Available: https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/725mbian13.pdf (Accessed 2 Feb 2014)

Darwish A., Bataineh E., "Eye tracking analysis of browser security indicators", *in Proc. of Computer Systems and Industrial Informatics Conference,* pp. 1–6, 2012.

Akhawe D., Felt A. P., "Alice in Warningland: A large-scale field study of browser security warning effectiveness", *in Proc. of the 22nd USENIX Security Symposium*, 2013.

Egelman S., Schechter S., "The Importance of Being Earnest (In Security Warnings)", *in Proc. of Financial Cryptography and Data Security*, Springer, pp. 52–59, 2013.

Egelman S., Cranor L., Hong J., "You've been warned: an empirical study of the effectiveness of web browser phishing warnings", *in Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1065–1074, 2008.

Sheng S., Wardman B., Warner G., Cranor L. Hong J., Zhang C., "An empirical analysis of phishing blacklists", *in Proc. of the 6th Conference on Email and Anti-Spam*, 2009.

Kirda E., Kruegel C., "Protecting users against phishing attacks with antiphish", *in Proc. of Computer Software and Applications Conference,* vol. 1, pp. 517–524, 2005.

Zhang, H., Liu, G., Chow, T. W., Liu, W., "Textual and visual content-based anti-phishing: A Bayesian approach", *in Proc. IEEE Transactions on Neural Networks*, vol. 22, issue 10, pp. 1532-1546, 2011.

Vidas T., Owusu E., Wang S., Zeng C., Cranor L., Christin N., "QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks", *in Proc. of Financial Cryptography and Data Security*, pp. 52–69, 2013.

Xu Z., Zhu S., "Abusing Notification Services on Smartphones for Phishing and Spamming", *in Proc. the 6th USENIX conference on Offensive Technologies*, pp. 1–11, 2012.

"Anti-Phishing protection of popular web browsers," AV Comparatives, Dec 2012. (Online). Available: http://www.av-comparatives.org/images/docs/avc_phi_browser_201212_en.pdf (Accessed: 05 Jan 2014).

Mazher N., Ashraf I., Altaf A., "Which web browser work best for detecting phishing", *in Proc. of Information & Communication Technologies Conference*, pp. 1-5, 2013.

Mylonas A., Tsalis N., Gritzalis D., "Evaluating the manageability of web browsers controls", *in Proc. of the 9th International Workshop on Security and Trust Management*, pp. 82-98, Springer (LNCS 8203), UK, 2013.

Mylonas A., Dritsas S, Tsoumas V., Gritzalis D., "Smartphone Security Evaluation - The Malware Attack Case", *in Proc. of the 8th International Conference on Security and Cryptography*, pp. 25-36, SciTePress, Spain, July 2011.

Bradley, T., "Android Dominates Market Share, But Apple Makes All The Money". (Online). Available at: http://www.forbes.com/sites/tonybradley/2013/11/15/android-dominates-market-share-but-apple-makes-all-the-money/ (Accessed: 12 Apr 2014).

Sobrier J., "Google Safe Browsing v2 API: Implementation notes". (Online). Available: http://www.zscaler.com/research/Google%20Safe%20Browsing%20v2%20API.pdf (Accessed: 10/01/2014).

iCloud (Online) Available at: https://www.icloud.com/ (Accessed: 8 Mar 2014).

OWASP. "Certificate and Public Key Pinning". (Online). Available at: https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning (Accessed: 18 Mar 2014).

Theoharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer Criticality Assessment methodology based on interdependencies", *Computers & Security*, Vol. 29, No. 6, pp. 643-658, 2010.

Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based Criticality Analysis", *in Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection*, Springer, USA, March 2009.