APD.3

AUTO PHISHING DETECTOR

A NEW WAY TO PREVENT PHISHING

APD.3 Auto Phishing Detector

UNIVERSITY OF WOLLONGONG IN DUBAI

Student Lab GITEX EDGE

Contents

Project Description 3

Key Objectives 3

Project Outcome 3

Business Case 4

Problem Statement 4

Phishing Industry Overview 4

Phishing Figures 5

Phishing Scale 5

APD.3 Solution 6

Architecture and Method 7

Features 7

About the Developers 8

Acknowledgements 8

About Auto Phishing Detector – APD.3

Project Description

APD.3 is an anti-phishing innovative tool based on Artificial Intelligence (AI) analysis. APD.3 detects websites that have not yet been reported and recognised as phishing sites. Location specific websites are reported less than generic sites and APD.3 is able to detect them too. Our application prevents you from accessing non-reported phishing sites and minimises the risk of zero-day phishing attacks.

www.APD3.net / info@apd3.net

Key Objectives

To implement a security system with detection and learning phases that would have patterns uploaded on the server. The AI system will analyse the web pages the user is viewing. When any suspicious data is found, the system will notify the user about malicious content.

The application can be used in two modes:

1. As a plugin to a user's browser. Whenever the user attempts to visit a site, the application automatically and seamlessly checks if the site is a phishing site.
2. As a reporting tool. The user can access a web server and submit any URL for a phishing test.

Project Outcome

- Detect most known phishing techniques.
- Alerting the user of phishing attacks as soon as they are detected.
- Interaction with global databases, which will contain the list of all phished sites.
- Detect phished websites which look exactly the same as original and genuine sites.
- Detect phished websites with some degree of similarity.

Business Case

Problem Statement

There exist numerous ways in which phishing can be used by individuals to social engineer unsuspecting individuals. Phishing attacks spread across social network websites and most of the attacks spread via email.

For starters, an individual with a malicious intention can modify or manipulate a website's address in such a way so as to provide the impression that a user is being directed to the authentic, genuine website, when in fact the user is being directed to a website hosted by the attacker. Any phishing process involves five steps: planning, setup, attack, collection and identity theft and fraud (Ramya et. al, 2011).

Phishing Industry Overview

Financial services (Fig. 1) continued to be the most targeted industry sector in the fourth quarter of 2012 with payment services close behind (APWG, 2012).

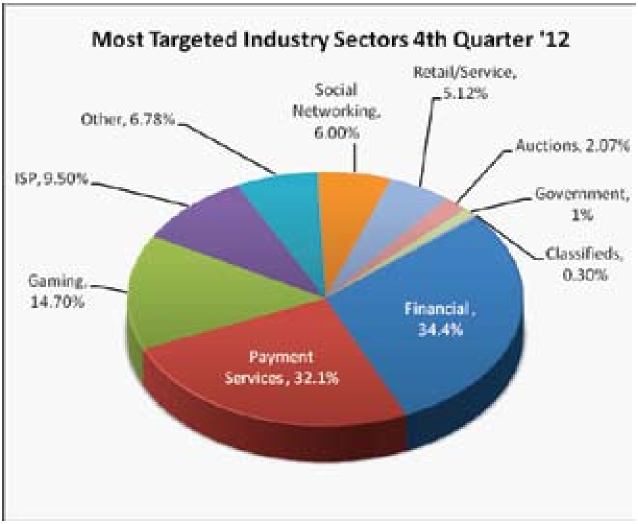


Figure 1. Phishing Targeted Industries Q4'2012

Anti-Phishing Working Group (APWG) counted 720 unique target institutions during the period, up significantly from the 611 found in 2H'2012 (APWG, 2013).

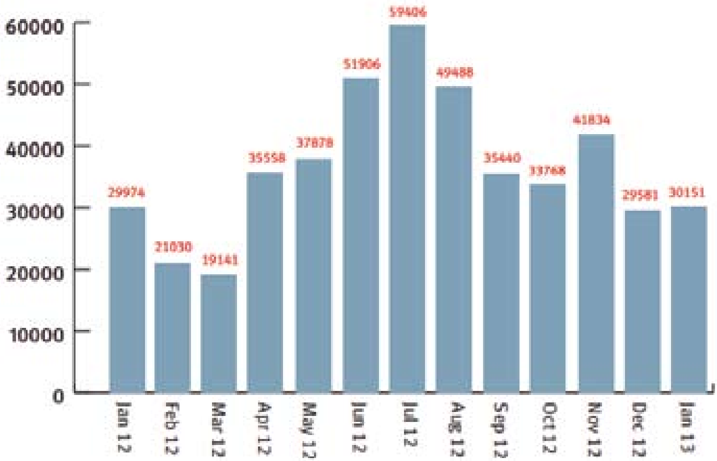
Phishing Figures

Phishing is defined as “a kind of attack in which victims are tricked by spoofed emails and fraudulent websites into giving up personal information” (Zhang et. al, 2007, p. 639). Below are figures reported from computer security agencies:

- More than $1.5 billion of worldwide losses from phishing attacks in 2012 (RSA, 2013)
- 70% of nationwide banks are targets of phishing campaigns (RSA, 2013)
- Number of phishing websites increased by 600% (Websense, 2013)
- 62% of users in UAE are unable to recognise forged web pages (Kaspersky Lab, 2012)

Phishing Scale

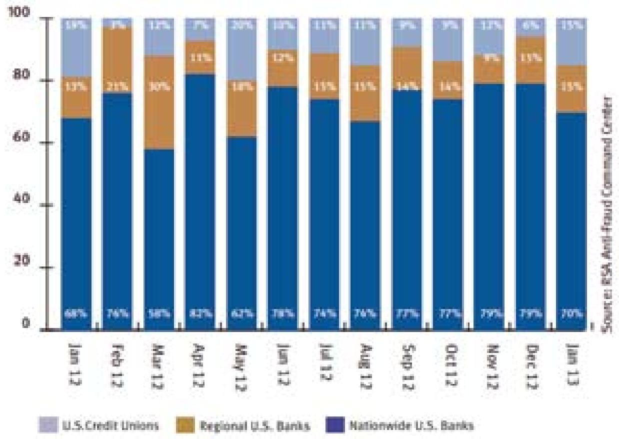
1. In January 2013, RSA identified 30,151 attacks launched worldwide, a 2% increase in attack volume from December 2012. Considering historical data, the overall trend in attack numbers in an annual view shows slightly lower attack volumes through the first quarter of the year (RSA, 2013).



Source: RSA Anti-Fraud Command Center

Figure 2. Phishing attacks statistics Jan 2012 - Jan 2013

2. A survey conducted in May 2012 by O + K Research at the request of Kaspersky Lab demonstrated that it is not always easy to recognise a phishing message. The survey found that 62% of users in UAE claimed they are incapable of recognising a phishing message or a forged website. The overwhelming majority of phishing messages are delivered through email or social networks, where much of the region's online activity takes place (Gulf Business, 2012).
3. Websense Security Labs measured 600% increase in use of malicious web links, representing 100 million global malicious websites. More than 85% were found on legitimate hosting providers had been compromised (Websense, 2013).
4. Nationwide banks continue to be the prime target for phishing campaigns targeted by 70% of the total phishing volume in January 2013. Regional banks' attack volume remained steady at 15%, while attacks against credit unions increased by 9%. (RSA, 2013).



Source: RSA Anti-Fraud Command Center

Figure 3. Phishing Statistics for Bank Industry Jan 2012 - Jan 2013

APD.3 Solution

The advantage of APD.3 comparing to other vendors is that it comes as a browser extension. Most of the alternative software is hard to remove and removing some of them is almost impossible for regular users. This makes APD.3 easy-to-install and easy-to-remove. Processing and analysis is done at server side, so the application doesn't consume your computer resources.

Architecture and Method

In order to be effective, it is vital that a modern anti-phishing solution integrates three characteristics:

1. Provide an easy-to-use interface, which can help the user understand what is going on, so that appropriate steps may be taken if needed
2. Use a detailed set of heuristics for comparing possible phished sites against their legitimate counterparts
3. Low reliance on blacklists, which need to be verified by humans (thereby increasing the amount of resources used). APD.3 meets those criteria.

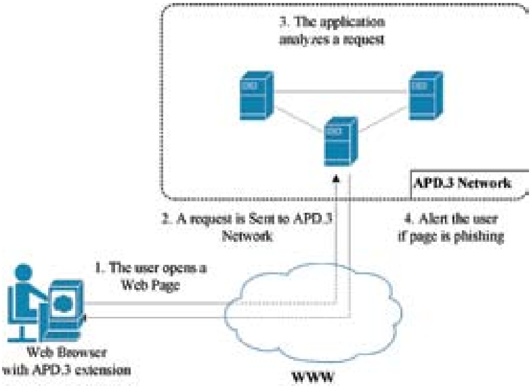

3. The application analyzes a request
APD.3 Network
2. A request is Sent to APD.3 Network
4. Alert the user if page is phishing
1. The user opens a Web Page
Web Browser with APD.3 extension
WWW

Figure 4 illustrates the structure of the application. Once the user opens a web page, the request is sent to the application. APD.3 analyses the request. Depending upon whether the website is categorised as a phished website or not, the user will be alerted if the page is forged.

Figure 4. Proposed Solution

Features

- Detects most known type of phishing attacks
- Tracks possible defacements originating from difference sources
- Reports phishing attack in real time
- Knowledgebase of all known phishing websites
- Offered as a browser extension
- Doesn't consume resources
- Easy to Install

About the Developers

Khalid Al-Najjar

Bachelor of Computer Science in Digital Systems Security, UOWD
KhalidAlnajjar@apd3.net

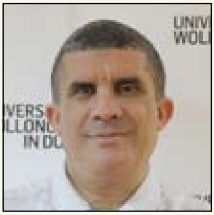
Ali Payani

Bachelor of Computer Science in Digital Systems Security, UOWD
AliPayani@apd3.net

Marlen Bissaliyev

Graduate student of IT Management, Bachelor of Computer Science, UOWD
MarlenBissaliyev@apd3.net

Coordinator



Dr Halim Khelalfa

MSc American University, PhD Illinois Institute of Technology
Halimkhelalfa@uowdubai.ac.ae

Acknowledgements

We would also like to acknowledge the kind support of Dr Farhad Oroumchian, Dr Abdelghani Benharref, Prof Mohamed-Vall M. Salem and the Faculty of Computer Science and Engineering of the University of Wollongong in Dubai.

www.apd3.net
info@apd3.net