EASYSOLUTIONS

PROTECTION AGAINST PHARMING AND PHISHING ATTACKS

SUMMARY

The intention of this whitepaper is to provide a general view of phishing and pharming as electronic fraud techniques and to show how Easy Solutions, an innovative IT security company, approaches this problem providing a solution oriented to end-users who want to access transactional and confidential websites safely

TABLE OF CONTENTS

CURRENT SITUATION

1

Although the IT security industry's attention is currently focused on the evolution of malware (Botnets, spam, mobile devices, among others) [1] - [2], it has deliberately neglected the only element that can't be technically controlled: the end-user.

Meanwhile, IT crime has become a formally established business in which its members are mainly in it for the economic benefits [1]. Keeping in mind these two realities, the IT criminals are currently focusing on attacking the end-user using deceptive techniques (social engineering) to carry out electronic fraud. This is what generally is known as phishing.

According to the Anti-Phishing Working Group (APWG), phishing is a "criminal mechanism that uses social engineering techniques, as much as technological know-how, to obtain personal information and/or financial credentials." [3]. In other words, phishing happens when a user is tricked into accessing a malicious website, giving personal and financial information which is obtained by the phisher who owns the site.

Phishing attacks have been increasing over the last years. According to a study conducted by the Gartner consulting firm, more than 5 million people in the United States lost money due to phishing attacks as of September, 2008 which represents an increment of 39.8% with regards to the previous year. Additionally, the average amount of money lost due to phishing attacks in 2008 was US$351 increasing US$95 with regards to 2005 (US$256) [4].

Meanwhile, more recent data provided by the Anti-Phishing Working Group (APWG) shows that in the second semester of 2008, in the month of October, there was a peak of 27,739 reported phishing websites (fraudulent pages that are an identical copy of a legitimate transactional site) having a sustained growth from July to October as shown here [3]:

CURRENT SITUATION

1

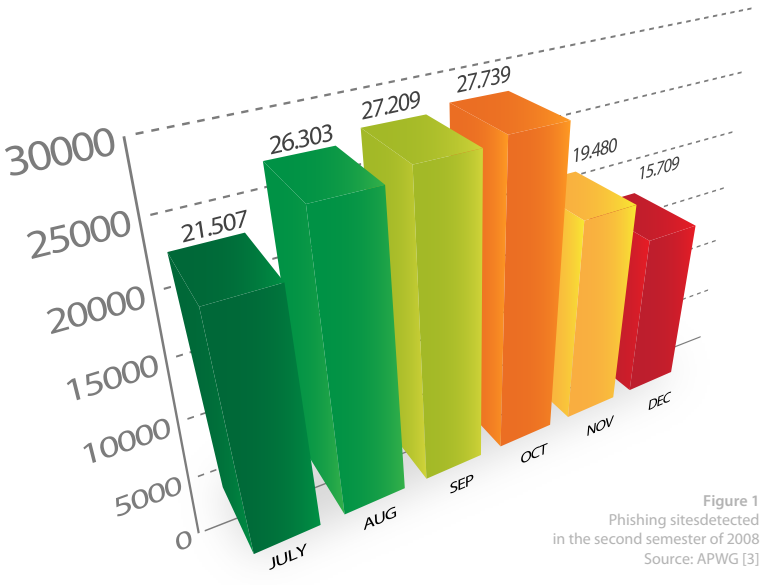


Figure 1
Phishing sitesdetected
in the second semester of 2008
Source: APWG [3]

Finally, PhishTank provides the most recent statistics on phishing. According to this entity, a total of 24,311 reports of suspicious activity were sent in for analysis in the month of June, 2009 alone giving a result of 2,911 valid phishing attacks and 199 false flags which show that the majority of threats turn out to be real [5]. Also, PhishTank provides the top targeted entities for phishing according to the data obtained:

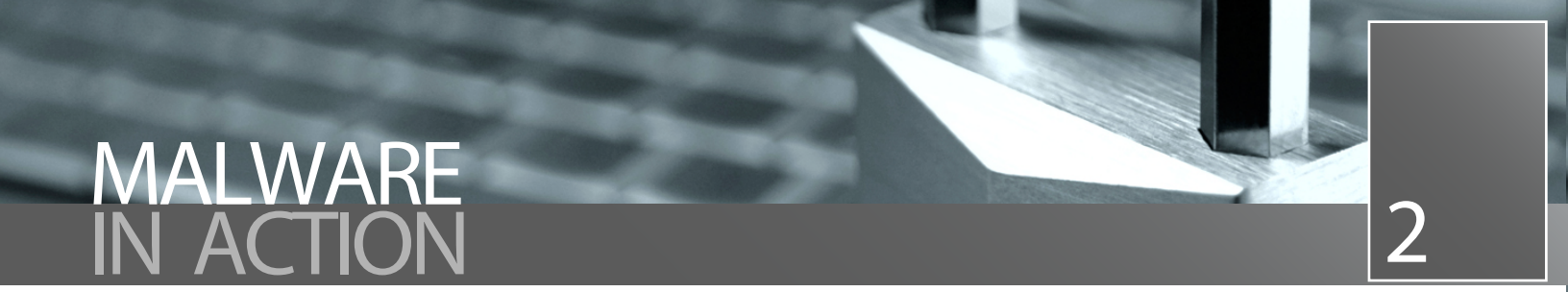
	Top 10 Identified Targets	Valid Phishes
1	PayPal	12,775
2	JPMorgan Chase and Co.	897
3	Bank of America Corporation	561
4	Google	369
5	HSBC Group	292
6	Internal Revenue Service	227
7	eBay, Inc.	184
8	Sulake Corporation	152
9	Facebook	123
10	Poste Italiane	51

Figure 2
Top 10 phishing targets
during the month June 2009
Source: PhishTank [5]

The above mentioned shows that the main objective of phishing attacks is electronic fraud for financial gain (PayPal, JPMorgan, Bank of America). However, social networks such as Facebook are increasing for which phishing can shift to more sophisticated attacks such as identity theft.

Evaluating the recent trends, it can be expected that phishing and malware attacks continue to rise during 2010 considering it's still a lucrative business for IT criminals.

To learn how to be protected from these threats, it's important to analyze a phishing attack in detail.



MALWARE IN ACTION

2

According to SANS, pharming is a sophisticated technique that allows automatically re-directing a user to a malicious site [6]. In other words, a user that has been attacked by means of pharming when entering www.easybank.com will be automatically re-directed to a fraudulent site identical to the legitimate one allowing the theft of credentials.

There are several ways of carrying out a pharming attack. One of the simplest and less sophisticated ways is to modify the hosts file. This file allows storing IP - domain names to speed up surfing and avoid consulting a DNS server [7]. For example, if the hosts file contains:

xxx.xxx.xxx.xxx easybank.com

Every time that the user enters easybank.com into the browser, the PC won't consult a DNS but rather it will consult the hosts file first and, if it finds this domain name, it will take the IP address XXX.XXX.XXX.XXX which is a counterfeit website where the attacker steals the credentials effecting a phishing attack.

To carry out a pharming attack, three things are needed:

1. A batch script to write the malicious IP and domain names onto the hosts files.
2. A joiner to join this batch file onto another file (image, video, music, etc.) in an executable EXE along with the appropriate icon to do social engineering and trick the user.
3. A code obfuscator or any other software in charge of making the generated executable undetectable to the anti-viruses.

The first point is necessary because it is the essence of the attack. The other two points consist on making the user fall blindly into the trap by complementing it.

The batch script is really simple, it can be done in a text editor and saved with the BAT extension:

```
@echo off
echo xx.xxx.xxx.xx www.easybank.com >>
%windir%\system32\drivers\etc\hosts
echo xx.xxx.xxx.xx easybank.com >>
%windir%\system32\drivers\etc\hosts
exit
```

To test it, it just has to be executed and then the hosts file can be checked in the following path:

```
%windir%\system32\drivers\etc\hosts.
```

It should appear like this:

```
127.0.0.1 localhost
xx.xxx.xxx.xx www.easybank.com
xx.xxx.xxx.xx easybank.com
```

Next, we enter the address www.easybank.com in any browser and it should automatically redirect to the IP xx.xxx.xxx.xx. The following steps consist of adding an additional file (an image, for example) to make it look like a postcard, changing the icon of the executable and confusing the code to make it undetectable to the anti-viruses.

EASY SOLUTIONS' PROPOSAL

3

The Detect Safe Browsing software provided by Easy Solutions gives the necessary mechanisms to safely access sites you wish to visit. Among the functionalities that this tool contains is the search for malicious entries in the Hosts file, which avoids pharming attacks like the example of the previous section:

Additional to the search, Detect Safe Browsing allows seeing a historical record of the suspicious activity found during the last 60 days. After the scan, the software allows solving the problems found using the "Quick Fix" button as shown here:

Figure 4 - Detect Safe Browsing finding suspicious activity and solving the inconveniences found

Next, the user can safely access the protected sites that he/she defined and configured in Detect Safe Browsing. The search of anomalous activity is not only carried out on a

Figure 3 - Detect Safe Browsing before surfing in a safe way

local level but also remotely because it protects against attacks such as DNS Poisoning which consists in that the server names configured in the client has its table modified in such a way that if the petition is www.easybank.com, the answer will be a malicious IP. The way that Detect Safe Browsing detects this type of attack is by verifying the IP address that the DNS server sends to the Easy Solutions servers located in the United States by way that, if the IP addresses don't match, Detect Safe Browsing warns the user with an alert.

Additionally, Detect Safe Browsing strives to be the only reliable means to access websites where confidential information (personal and financial) can be compromised.

Detect Safe Browsing allows accessing social networks and transactional sites in a safe way, avoiding becoming a victim of phishing and pharming attacks.

RESOURCES

4

More information about Detect Safe Browsing, including its Datasheet, can be found on:

http://www.easysol.net/newweb/Products/Detect-Safe-Browsing

REFERENCES

[1] GTISC. "Emerging Cyber Threats Report for 2009". Georgia, United States. Available at: http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf

[2] Sophos. "Security threat report: 2009". Available at: http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf

[3] APWG. "Phishing Activity Trends Report". 2nd Half 2008. Available at: http://www.apwg.org/reports/apwg_report_H2_2008.pdf

[4] GARTNER. "The War on Phishing Is Far From Over". 2008. Available at: http://www.gartner.com/DisplayDocument?id=927921

[5] PhishTank. "Stats June 2009". Available at: http://www.phishtank.com/stats/2009/06/

[6] SRIVASTAVA Tushar. "Phishing and Pharming – The Deadly Duo". 2007. SANS Institute. Available at: http://www.sans.org/reading_room/whitepapers/privacy/phishing_and_pharming_the_evil_twins_1731

[7] Anti-Phishing. "So what is hosts file and how to use hosts file?" Available at: http://www.anti-phishing.info/what-is-hosts-file.html

ABOUT EASY SOLUTIONS

5

Easy Solutions is the only security vendor focused exclusively on fraud prevention; providing anti-phishing services and research, multifactor authentication and anomaly transaction detection.

We deliver an integrated and comprehensive approach to multichannel fraud prevention and works in alliance with industry leaders in other security disciplines supporting a wide range of heterogeneous platforms.

Our software solutions are simple to manage and easy to deploy. Our proprietary technologies provide accurate identification of devices with unprecedented accuracy while protecting users by monitoring transaction behavior for activity associated with fraudulent activity.

Working closely with the leading security companies and leading financial enterprises with large online customer communities, Easy Solutions continuously collect and understands the latest methods used by online criminals.

The capacity to react to new threats in the antifraud protection field is based on our proprietary technology and in the methodology to face each threat in an integral way implemented through Easy Solutions' Total Fraud Protection Strategy.

EASYSOLUTIONS

Headquarters:
1401 Sawgrass Corporate Parkway, Sunrise, FL 33323 - Phone: +1-866-524-4782
Latin America:
Calle 93A No. 14 – 17 Of. 506 Bogota, Colombia - Phone: +57 1- 2362455.
www.easysol.net