Analysis and detection of Phishing emails with Delphish

Robert Krzeminski

Nutzwerk GmbH
Kohlgartenstr. 13, 04135 Leipzig, Germany
r.krzeminski@nutzwerk.de

Abstract

In this paper we present the Anti-Phishing solution Delphish. The idea behind Delphish is the creation of a protection and analysis tool, that allows integration into existing email clients through a provided interface. Delphish is currently available as an Add-In for MS Outlook. Delphish uses a combination of signature-based and heuristic analysis for the identification of Phishing attacks. The aim of this solution is not only the automatic detection of Phishing emails, but also to provide sufficient assistance to the user, in case he is subject to a new kind of attack. Due to the graphical display of the links in the email with their risk as well as the display of the result of reputation tests and other relevant information, like e.g. WHOIS records for the domain of each link, the user is enabled to judge the potential threat of the suspicious message on his own. This method sensitizes the user by and by for a more conscious and safer way of handling emails.

1. Introduction

Phishing is the attempt to steal confidential data from the user through deception. The criminals can act maliciously with the thereby obtained information, harming the user and third parties economically and also immaterially (e.g. bad reputation). The first fraud attempts of this kind were sighted on the internet in the mid-1990's. The number of Phishing attacks has dramatically increased since that time and it reached 28,571 different fraudulent emails in June 2006, according to the Anti-Phishing Working Group (APWG). That's an increase of 90% to the number of unique Phishing attacks in June 2005. The number of Phishing websites also increases continuously and was twice as high in June 2006 (9,255) as a year before (4,280) [2, 3].

The Phishing attacks are usually initiated through an email. The attacker sends a message to his victim, that is supposed to look like an official email of the faked brand. By using social engineering techniques, he tries to motivate the recipient for some kind of action, like e.g. visiting a specific website or entering credentials directly into the embedded form. To further increase the users confidence into the email, the attackers often use the known security holes in the SMTP protocol to fake the From-Header. The email recipient then sees an official sender address in his email client and he can draw wrong conclusions about the origin of the message.

Most Anti-Phishing Desktop solutions [15, 6, 10, 11, 16] focus on web browsers and inform the user through different security indicators, when he wants to visit known Phishing sites. The classification generally happens automatically. However, the user is on his own if the Phishing site is new and unknown. In that case he doesn't get any indices, advising him that the visited site may be a fraud attempt. So he can easily draw the wrong conclusion that the website is not dangerous. The user also faces a simple analysis result if the Phishing site was detected correctly, thus not giving him the chance to develop a feeling for the safe handling of emails and web surfing. The sensitization of the user is however the most effective, and most often recommended weapon against Phishing. The conscious user will approach any email, asking him to disclose personal data, with a good sense of distrust, and check it carefully before following the instructions. But he needs the appropriate tools, to help him with the analysis of the suspicious email.

1.1. Vision

We present a solution called Delphish, that uses the advantages of automatic detection and sensitizes the user for safe and responsible handling of emails at the same time. Delphish is designed as additional toolbar for email clients and it is currently implemented as an Add-In for MS Outlook. The analysis of an email with Delphish doesn't begin, until the user suspects that the email could be a fraud attempt. He clicks a button in the Delphish toolbar to initiate the analysis of the supposedly dangerous message. Delphish first attempts to automatically rate the email. A risk analysis of the links in the email is conducted, regardless of whether the email was automatically detected as a fraud attempt or not. The results of those tests are displayed in a concise window, where the potentially dangerous links are highlighted. The user can now judge the potential threat of each link on his own, by examining detailed information about each link, like the actual destination, type, popularity, age, domain owner etc. Since the link information is also available for emails that were detected as Phishing, the user gets accustomed to the techniques used by Phishers after a while. This will result in an increased alertness when handling emails.

2. Mail analysis

The Phishing protection offered by Delphish consists of two layers, the signature-based and the proactive heuristical analysis. The reactive component fends off all known Phishing emails and their variants. The time-frame between the detection of a Phishing attack and the creation of a respective signature however poses a threat, leaving the user vulnerable to the new attack. To obviate these unknown dangers, Delphish contains a second protective layer, pointing out dangerous elements in the email to the reader with the help of risk and reputation tests. A third layer, the information layer, is placed on top of these protective layers, providing relevant data for each link additionally to the analysis results, enabling the user to judge the potential threat of the email on his own.

2.1. Signature-based scanning

In the first step, the suspicious email is examined by an anti-virus scanner. Known Phishing attacks are already identified by this check. The success of the signature-based technology depends on the up-to-dateness of it's database. This is especially important for the short-lived Phishing attacks. An AV software that is installed on the users computer is often out of date, since many users update irregularly or even never. We therefore decided to use a server-based solution, providing a centralised and automatic administration. We currently utilize the open source solution Clam AntiVirus. Delphish is not dependent on the used AV solution though, allowing to switch the AV software in the future. The communication with the AV server is encrypted with a SSL-based HTTP protocol (HTTPS).

2.2. Link risk evaluation

The potentially dangerous elements in an email are the links, forms, attachments and active contents, as far as they are executed by the used client. Though Phishing emails can also induce the recipient to actions like visiting a specific website or calling an expensive phone number without these elements, through a carefully worded text, but these cases are currently marginal and they can simply be detected by a pattern-based analysis. Most email clients offer own mechanisms for handling potentially dangerous attachments, so we decided to refrain from an additional analysis in that respect.

Chapter 3 describes the Link Risk Analyzer, that we developed for the risk evaluation of the links in the emails.

2.3. Geolocation

The geographical location of a server, that is behind a link, plays a substantial role for the risk analysis. Geolocation technologies, which have been available on the market for several years, allow the location of almost any computer in the world by using it's IP address.

The geographical origin of the website behind a link, is shown in Delphish in the form of the country name and the corresponding country flag respectively. Though more than 40% [3] of the Phishing websites are located in the USA, this information can provide valuable hints if the attackers computer is located in exotic countries or when the faked site is hosted in an entirely different country as legitimate links, that are also placed in the deceptive email.

2.4. WHOIS

WHOIS is a protocol for querying a distributed database system, containing information about internet domains and their owners. A WHOIS entry normally contains information about the owner, the administrative and technical contact as well as the date of domain registration.

When conducting a manual email analysis, the domain information from the WHOIS record mostly provides the crucial proof for a link and thus for the entire message being a fraud attempt. Therefore Delphish conducts a WHOIS query for every domain, occurring in the links of the email. To reduce the load on the WHOIS services, the once requested information is stored in a local cache for later use for a predefined period of time. To ease the study of the WHOIS data for unexperienced users, we decided to display the owner data of a domain in the form of an address. Since the structure of the returned data underlies no standards, we had to implement a number of parsers for the most used WHOIS servers to properly achieve this.

3. Link risk analysis

In the first, signature-based step of the email analysis, Delphish tries to rate the email automatically. In case such a classification ist not possible, because the email was previously unknown, a link risk evaluation is conducted in the second step by the link risk analyzer DelLink, that we developed for this purpose. DelLink is a collection of tests, that are conducted for each link in the email. A risk score (RiskScore *RS*) is then generated based on these tests. To define the different significance of the tests, we introduced an additional weighting w_i. There are two kinds of tests: Risk and reputation tests. The risk score *RS* of a link is the difference between it's risk *RISK* and it's reputation *REP*.

$$RS(link) = RISK(link) - REP(link) \tag{1}$$

The risk tests are heuristical tests, that increase a links risk score *RS*. They examine the links for the existence of techniques, that were used in previous Phishing attacks to disguise the actual link destination. Every test delivers a risk score V_i between 0 and 1. The risk *RISK* of a link is the sum of the single test results multiplied with their weighting:

$$RISK(link) = \sum_{i=1}^{n} w_i V_i \tag{2}$$

The reputation tests are risk-lowering tests. They try to determine the reputation of the domain behind a link through the external services. They also deliver a value R_i between 0 and 1. The reputation *REP* of a link is the sum of the single reputation values mutiplied with their weighting:

$$REP(link) = \sum_{i=1}^{n} w_i R_i \tag{3}$$

If the analysis results in the risk score of a link to exceed the empirical threshold of DelLink, it will be highlighted as dangerous in Delphish.

Depending on the link element that is checked, and the context, we divided the test routines into four classes: URL-, Link-, Context- and Reputation analysis. These test classes are described in more detail below.

3.1. URL analysis

The purpose of email Phishing attacks is normally, to make the user follow a link in the message or to make him open and execute an attachment with a dangerous program. The link destination is shown in the status bar in most email clients, sometimes however it isn't shown at all (like e.g. in Microsoft Outlook 2002). The URL specification allows the attackers to create URLs, that make the real destination hard to recognize

for the user. The techniques for URL-disguising, that are included by DelLink for the risk evaluation, are briefly explained below.

3.1.1. Spoofed domain names

One of the favored and most trivial methods, that Phishers use to pretend the legitimacy of a server to the user, is registering a name that is similar to the one of the faked domain. They register for example the domain paypa1.com, which doesn't appear to differ from the legitimate PayPal domain, paypal.com, at first sight.

3.1.2. "Friendly login"-URLs

It is possible to build links containing authentication data, to relieve the user of the tedious entry of username and password. This possibility is abused by Phishers to disguise the actual link destination. Let's assume an email contains a link in the form http://www.paypal.com:money@phisher.com. The unexperienced reader won't necessarily notice that this is a fake site.

3.1.3. Disguising the host name

A different method for disguising the host name of the actual destination, is by using IP addresses instead of host names. Every program that communicates over the internet, needs to resolve the host names common to the internet users into their corresponding numerical addresses. The Phisher can build a link in the form http://www.postbank.de@123.100.200.2, to hide the link destination.

3.1.4. Untypical ports

The faked sites are very often hosted on servers, that were hacked by the attackers. The compromised computers of home users (so-called botnets) are used for this purpose. A typical characteristic of those servers is the usage of untypical ports, i.e. 680, 85, 4443 etc. [2].

3.1.5. Disguising the URL

Most email clients and web browsers support the encoding of special characters in the URL. This is necessary to be able to represent characters, that are not directly allowed inside a URL or to support special characters of other languages. It is trivial for the Phisher to disguise a URL using these encoding schemes. For example a URL that looks like this http://%77%77%77%2E%70%61%79%70%61%31%2E%63%6F%6D, is an escape encoded version of http://www.paypa1.com.

3.2. Link analysis

This class of tests examines one or more link components, with the purpose of finding it's suspicious or dangerous properties, characteristics and contents.

3.2.1. Mismatch between link URL and link text

Phishers use the fact that most mail clients can display HTML encoded content. The content part of a link often specifies a different URL than the HREF attribute. Since the user normally only pays attention to the content, the real link destination stays hidden from him.

3.2.2. Scripts

Since active content like JavaScript or VBScript is perfectly well suited for disguising the actual link destination, we raise the risk for links during analysis, if they contain script instructions in their attributes and event handlers.

3.3. Context analysis

During the analysis of the techniques and tricks used in the known Phishing attacks, we discovered that it's reasonable to examine the links in the context of the other links. That makes it possible to find the references, that stick out of the mass through a specific characteristic.

3.3.1. Overlapped links

We found a different method for disguising the faked link destination in a Phishing attack on the customers of the Volksbanken Raiffeisenbanken:

```
<A HREF="http://www.volksbank.de/__C1256B560030
97E2.nsf/X851A68E4F14128EFC1256C670055579C">
<map name="gfaV">
<area coords="0, 0, 788, 331" shape="rect"
href="http://210.68.8.180/rpm/"></map>
<img SRC="cid:part1.08070201.05030507
@support_ref_11@volksbank.de" border="0"
usemap="#gfaV"></A>
```

The example shows a picture inside an anchor being overlapped by a link-sensitive area. Thus the resulting link does not point to the URL specified in the HREF attribute of the anchor (http://www.volksbank.de/__C1256B560030 97E2.nsf/X851A68E4F14128EFC1256C670055579C), but to a Phishing site that is hosted on the server with the IP address 210.68.8.180. The readers confusion can be increased even more by the attacker, if he overlaps only a part of the picture with a link-sensitive area.

3.3.2. Image links

The techniques used by spammers to bypass the filters used for the identification of unsolicited emails, are also used when creating Phishing emails. Naturally the attackers want their emails to reach as many readers als possible. A preferred method, that is also often found in Phishing attacks, is using one or more images instead of text. Such messages normally contain an image, that is a link at the same time. Delphish detects these image links and raises the risk for these links during analysis. We later decided to extend this measure on all image links in the email, if it contains only image links. We think that the reader should pay more attention to this kind of links during the email verification, even though it raises the False-Positive-Rate of our solution.

3.3.3. Host localization

Original images and logos are used, to make the message look as much as possible like a real email from the faked organization/institute. To emphasize the readers impression of authenticity of the faked email, real links are also embedded into the text. Very often there is only one faked link, that shall lead the user to a dangerous site. The Geo-database used by Delphish allows the localization of the server, that the link in the email points to. We also included this information into the

risk evaluation. That makes it possible to detect links, that lead to sites that are hosted on a different server than the one for the rest of the links.

3.4. Reputation analysis

The reputation tests belong to the risk-lowering tests and they are conducted by querying external internet services.

3.4.1. Popularity of the link domain

The popularity of the domain is a value that reflects the number of external sites, that link to this domain. It is an indicator for the number of times, that the content of the website was inspected by others. That's a measure of trustability of a domain.

3.4.2. Age of the domain

The domains used by Phishers are normally short-lived (4.8 days, according to the latest statistics of the Anti-Phishing Working Group), since a Phishing attack is detected rather quickly. Furthermore it can be dangerous for the criminal to operate it for a longer period of time, due to possible prosecution. Therefore knowing the age of a domain can be a big help during the analysis. A domain that was registered a month ago, or maybe wasn't seen on the internet before at all, should highly alert the user.

4. Architecture and implementation

The architecture of *Delphish* is shown in figure 1.

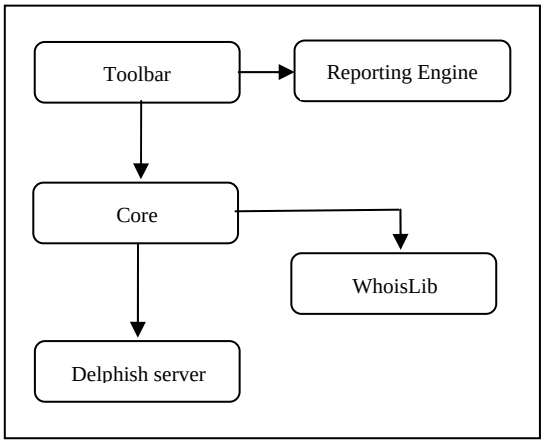

Figure 1: Delphish architecture.

4.1. Delphish components

- Core, which has been designed independently of the used email client. The core communicates with the Delphish server, to compare the email to the known signatures of Phishing emails. The link risk analyzer DelLink is also located here.
- Reporting engine, which is responsible for the graphical output of the classification and analysis.
- WHOIS library, which consists of a WHOIS client and the corresponding parsers.
- Toolbar, a client-dependent component, which allows the user to access the Delphish features in the email program of his choice.
- AV server, which conducts the signature-based analysis of the suspicious email. It ensures the up-to-dateness of the used signature database.

4.2. Implementation

Delphish was entirely implemented in C++. The individual client components communicate with each other using distinctly defined interfaces. We implemented the Add-In for Microsoft Outlook as an ATL-COM component. To simplify the adoption of Delphish for the use in other programs, we decided to design the remaining Delphish libraries as common Windows DLLs. During the development of the GUI, we deliberately refrained from using third-party frameworks (like e.g. MFC), to prevent the installation of Delphish to be unnecessarily bloated through additional files. The data management was implemented by using the slim and easy to handle SQLite engine, which can be embedded into the program without the need for installing database servers. The parsers for the WHOIS information are designed as individual modules (one library can contain multiple parsers), thus enabling us to easily add more parsers to Delphish.

For the determination of the geographical data, like the country hosting the linked site, we chose GEO-IP by MaxMind.

The program was equipped with a simple update interface, which ensures updates in periodic intervals.

4.3. User interface

It was an important aspect for us, that our solution does not impede the user in his accustomed environment. Since the email check and the queries to external reputation services take a period of time that is dependant on the kind of internet connection and the load of the contacted servers, we chose to conduct the check asynchronously. That allows the user to continue his work in the email program without interruption, while the designated email is being examined.

In the following, the elements of the Delphish user interface will be briefly described.

4.3.1. Delphish toolbar

After the installtion, a toolbar will be shown in the email client, as depicted in figure 2. This toolbar enables the user to access the most important features and options of Delphish.

Figure 2: Delphish toolbar

4.3.2. Status report window

The status report window (Figure 5) displays the results of the analyses, that Delphish conducted, in a graphical way. We decided to show this information in a popup window (systray popup) over the taskbar infotray area. The status of the

selected email is symbolized additionally through an icon in the Delphish toolbar.

4.3.3. *Details dialog*

The Details dialog is a different view of the status report window. It is intended for users, who prefer a list-based view over the graphical display of the links. It is also helpful in case the graphical display becomes cluttered, if the emails contain a large number of links.

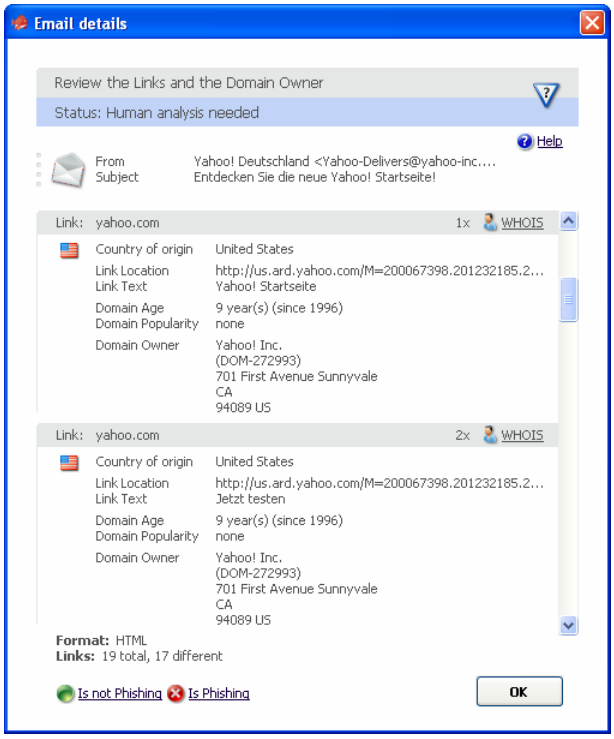

Figure 3: Details dialog.

4.3.4. *WHOIS dialog*

The obtained WHOIS information is shown in it's original form in a separate window (Figure 6). It's formatting varies, depending on the originating WHOIS server.

4.3.5. *Statistics and settings*

Delphish offers numerous statistical evaluations, that can be accessed through the toolbar. They are displayed in a purpose-built statistics window in a concise way.

The settings for language, the used proxy server etc. are available through a configuration dialog.

5. Evaluation

We refrained from evaluating the first step in the Delphish analysis, because it is dependent on the utilized anti virus software. Since it and the corresponding signature database are updated periodically and automatically, the recognition rate must comply to the latest version of the AV software. We focused on the evaluation of the link risk analysis, that shall help the user, in case he is subject to a previously unknown Phishing attack. The heuristics used in the risk analysis can produce the following misinterpretations:

- *False Positive*, is a false alarm, in case an examined link is safe even though it is built using known Phishing tricks. An email might for example contain a link to a site in the Google cache, which uses an IP address instead of a host name.
- *False Negative*, means treacherous confidence, in case the examined link was built using none of the known deceptive techniques and additionally doesn't show any characteristics to make it distinguishable from the others.

We created two groups for the evaluation of the link risk analyzer, each containing more than three hundred emails:

- Phishing emails, that were sorted out by our SaferSurf [12] service. SaferSurf is a proxy-based service, filtering the web- and email content. Dangerous contents are thereby detected by using anti virus scanners.
- Regular emails, that were also received through SaferSurf

Due to this presort by the anti virus software, we could reduce the inaccuracy rate when building the groups to a minimum. The emails from both groups were analyzed using DelLink. Afterwards the results were evaluated manually. Then we asked test persons with general knowledge about the internet concepts (like links, URLs, domains etc.), to classify Phishing emails only by the information provided by Delphish in the second analysis step, without letting them know about the results of the AV-based rating.

Table 1: Evaluation

Calculations	Phishing	Not Phishing
False Positive Rate	1%	4%
False Negative Rate	32%	-
Accuracy rate	83%	96%
Inaccuracy rate	17%	4%

The accuracy rate was 83% in the Phishing group. The safe links in the examined emails were "correctly" built without the use of Phishing techniques, what in turn resulted in the minimal (1%) False Positive Rate. The reason for this effect is the fact that the attackers wanted the design of the messages to resemble the original design as close as possible, therefor using correct links. The inaccuracy rate of 17% was a result of False Negatives, with a few exceptions. Even though DelLink rated the links in 32% of all positive results wrongly as safe, the test persons managed to reveal the fraud attempts of the links in almost all cases, with the help of the WHOIS and reputation information. This also corresponds to our basic concept of considering DelLink merely as a help, that should point the users attention to the obviously dangerous links. The user should inspect all links anyway, before trusting a message.

The Delphish analysis is presented in the following by means of two real-world examples.

5.1. "Account suspended" attack

This is a classic Phishing attack, requesting the reader to update his account, to prevent it from being suspended. Figure 4 shows a real email, that was addressed to eBay users in late 2005.

Our anti virus software couldn't rate this email automatically in the first analysis step The link risk analysis rated one ("HERE") of the 21 different links, that occurred in this email, as potentially dangerous, as shown in figure 5.

As can be seen in the status report window of Delphish, the marked link points to a site that is hosted on a server (202.224.236.250) in Japan. The reputation tests showed, that this address was never seen on the internet before ("Domain Age") and that this is obviously an unknown domain.

The WHOIS information in figure 6 reveals, that this IP belongs to an ISP called Mashito Outa. There is no visible reference to eBay. Based on these indices, we came to the conclusion that this message is a fraud attempt.

The World's Online Marketplace®

Dear Valued Ebay Member,

It has come to our attention that your Ebay Billing information records needs updated for the year 2006. This requires you to update your billing information.
If you could please take 5-10 minutes out of your online experience and update your billing records. You will not run into any future problems
with your Ebay online services. However, failure to update your records will result in account termination. If you would like to keep your account
please update your ebay account as soon as possible. Once you have updated your account records, your ebay session will not be interrupted
and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.

Please Update HERE

Thank you for your time.
Sheldon Fowler
Ebay Billing Dept team.

Announcements | Register | Shop eBay-o-rama | Safe Trading Tips | Policies | Feedback Forum
About eBay | Home | My eBay | Site Map | eBay Downloads

Browse | Sell | Services | Search | Help | Community

Figure 4: "Account suspended" attack

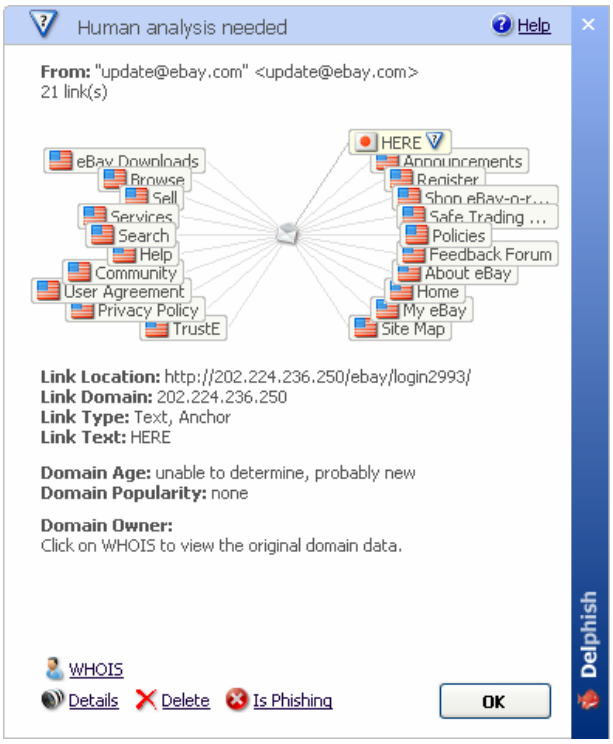

Figure 5: Not rateable

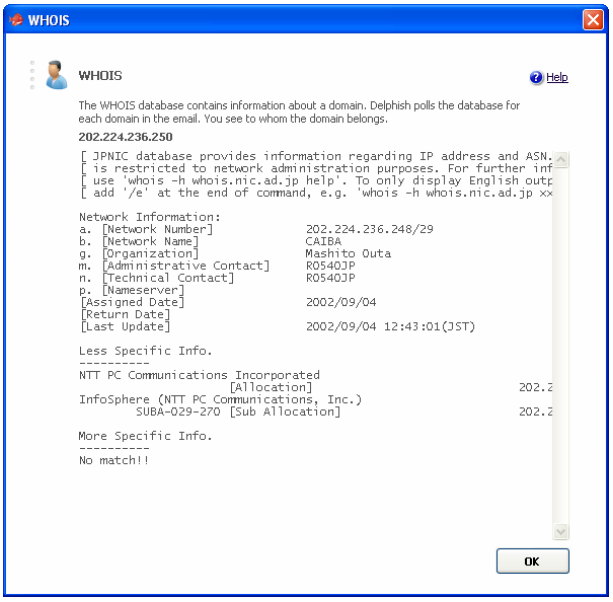

Figure 6: WHOIS information

5.2. PayPal attack

The email in figure 7 shows a typical attack on PayPal customers. It informs the customer about login attempts to his account, that had allegedly been conducted through foreign IP addresses. He is asked to verify his identity, by using the link in the message. To make sure he takes the whole matter seriously, the email threatens to suspend his account.

Figure 7: PayPal attack

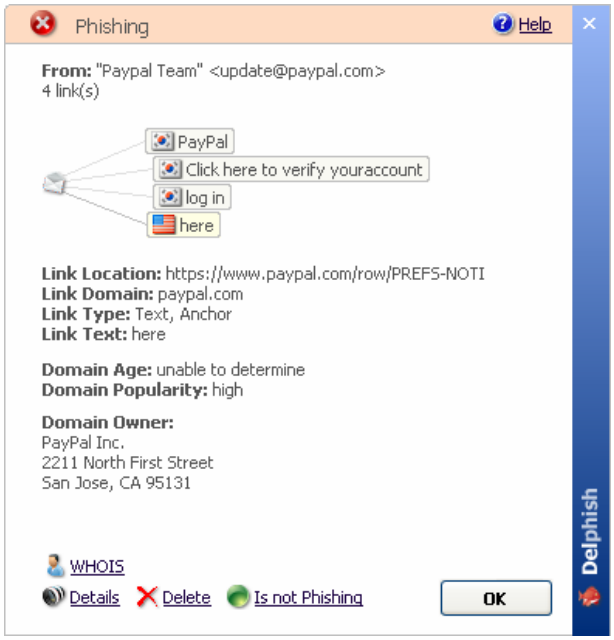

Figure 8: Status report window for the PayPal attack

The email contained four links in total. The signature-based analysis identified it as Phishing. We found the reasons for that, when we looked through the remaining information provided by Delphish. The link risk analyzer couldn't detect any links as being dangerous, but the status report window, shown in figure 8, revealed at a glance, that three of the links lead to a website in Korea (the fourth link pointed to PayPal). Since the domain age test showed that this website already existed 3 years ago, we could assume that the attackers either adopted the site or hacked it. The WHOIS record revealed, that the corresponding domain belonged to a company from Seoul and there existed no noticeable connection between it and PayPal.

5.3. Conclusion

As the evaluation clearly showed, our solution stood the test in practice. The known Phishing emails are already identified in the first analysis step, with the help of anti virus software. The additional analyses and facilities, provided by Delphish, like link risk- and reputation analysis as well as the WHOIS information, assist the user adequately to fend off previously unknown attacks. The user learns about the tricks of the Phishers by and by, and he is enabled to detect suspicious patterns in the links.

6. Future enhancements

We don't see Delphish as a finished work at all, but rather as a tool to fight Phishing, that constantly needs to adapt to new tricks and techniques, that the criminals invent and use. A continuous development of the program is part of this aim. We plan to extend Delphish with more analyses and reports, that use existing technologies and information, with the purpose of obtaining information about the email and it's origin. Here is a list of some of the planned enhancements.

- Analysis of the transmission route of the email through SMTP Path analysis
- Detection of IDN spoofing attacks
- Checking, if the specified link leads to free web hoster
- Checking, if the email was sent from a free email provider account
- Planning and implementation of mechanisms for Phishing target detection
- Checking of the SSL certificates
- Using blacklists, identifying the known spam- and Phishing computers
- Detection of dynamic IP addresses in the links

7. Nutzwerk GmbH

The Nutzwerk GmbH offers security solutions predominantly for home users. Nutzwerk operates the proxy-based service SaferSurf (http://www.safersurf.com).

8. Literature

[1] Amir Herzberg, Ahmad Gbara, *TrustBar: Protecting (even Naive) Web Users from Spoofing and Phishing Attacks*, 2004: Cryptology ePrint Archive: Report 2004/155.
[2] Anti-Phishing Working Group, *Phishing Activity Trends Report*, July 2006.
[3] Anti-Phishing Working Group, *Phishing Activity Trends Report*, July 2005.
[4] B. Leiba, J. Ossher, V. T. Rajan, R. Segal, M. Wegman, *SMTP Path Analysis*
[5] Core Street, Spoofstick, http://www.corestreet.com/spoofstick/
[6] eBay, *eBay Toolbar*, http://pages.ebay.com/ebay_toolbar/

[7] G. Ollman, *The Phishing Guide: Understanding and Preventing Phishing Attacks*, Next Generation Security Software Inc, 22. September 2004
[8] J. Tuliani, *The Future of Phishing*, HNS 5. April 2004.
[9] Min Wu, *Thesis Proposal: Fighting Phishing at the User Interface*, MIT. 2006.
[10] M. Wu, R. Miller, S. Garfinkel, *Do Security Toolbars Actually Prevent Phishing Attacks?*, CHI 2006-09-17.
[11] Netcraft, *Netcraft Toolbar*, 2004, http://toolbar.netcraft.com/.
[12] Nutzwerk, *SaferSurf*, http://www.safersurf.com
[13] Rachna Dhamija, J. D. Tygar, Marti Hearst, *Why Phishing Works*, 2005
[14] R. Dhamija, J. D. Tygar, *The Battle Against Phishing: Dynamic Security Skins*, SOUPS 2005.
[15] The Crystal Group: Steve Colucci, Vadim Dolt, David Fitzpatrick, Paul Firgens, *Phishing Attacks: A Survey of their History, Techniques and Possible Solutions*, 2005
[16] T. Sharif, *Phishing Filter in IE7*, 9. September 2006, http://blogs.msdn.com/ie/archive/2005/09/09/463204.aspx
[17] Wikipedia, *Phishing*, http://de.wikipedia.org/wiki/Phishing.
[18] Wikipedia, WHOIS, http://de.wikipedia.org/wiki/Whois