Analyse und Erkennung von Phishing-E-Mails mit Delphish

Robert Krzeminski

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

Abstract

In diesem Dokument wird die Antiphishing-Lösung Delphish vorgestellt. Delphish ist als Schutz- und Analyse-Werkzeug konzipiert und kann als Erweiterung über eine bereitgestellte Schnittstelle in bestehende E-Mail-Clients integriert werden. Delphish ist zurzeit in Form eines Add-Ins für MS Outlook verfügbar. Zur Identifizierung von Phishing-Attacken verwendet Delphish eine Kombination aus signaturbasierter und heuristischer Analyse. Das Ziel dieser Lösung ist nicht nur eine automatische Erkennung der Phishing-E-Mails, sondern auch ausreichende Hilfestellung für den Benutzer, falls er mit einer neuen, bisher nicht bekannten Attacke konfrontiert wird. Dank der graphischen Darstellung der in einer E-Mail befindlichen Links und deren Risiko sowie der Anzeige der Ergebnisse von Reputationstests und anderer relevanter Informationen, wie z.B. WHOIS-Datensätze zu der hinter jedem Link liegenden Domäne, wird der Anwender in die Lage versetzt, selbst über das Gefahrenpotenzial der verdächtigen Nachricht zu entscheiden. Dadurch wird er mit der Zeit für den bewussteren und sichereren Umgang mit E-Mails sensibilisiert.

1. Einführung

Phishing ist ein Versuch vertrauliche Daten des Anwenders durch Täuschung zu stehlen. Mit den auf diese Weise erworbenen Informationen können die Kriminellen im Namen des Opfers böswillig handeln und ihm und Dritten sowohl wirtschaftlichen als auch immateriellen Schaden (z.B. Rufschädigung) zufügen. Die ersten Betrugsversuche dieser Art wurden im Internet Mitte der 1990er Jahre notiert. Seit dieser Zeit ist die Anzahl der Phishing-Attacken dramatisch gestiegen und erreichte im Juni 2006 laut Angaben der Anti-Phishing Working Group (APWG) 28.571 unterschiedliche betrügerische E-Mails. Im Vergleich zu Juni 2005 ist die Anzahl der einzelnen Phishing-Attacken um ca. 90% gestiegen. Auch die Anzahl der Phishing Web-Sites steigt kontinuierlich und war im Juni 2006 (9.255) mehr als doppelt so hoch wie im gleichen Monat des Vorjahres (4.280) [2, 3].

Die Phishing-Attacken werden in der Regel mit einer E-Mail initiiert. Der Angreifer schickt dem Opfer eine Nachricht, die wie eine offizielle E-Mail der vorgetäuschten Organisation aussehen soll. Durch Anwendung von Social-Engineering-Techniken versucht er den Empfänger zu einer Aktion zu motivieren, wie z.B. eine bestimmte Website zu besuchen oder Zugangsdaten direkt in das eingebettete Formular einzugeben. Um das Vertrauen der Benutzer in die E-Mail zu stärken, nutzen die Angreifer sehr oft die bekannten Sicherheitslücken im SMTP-Protokoll und fälschen die From-Header. Der Empfänger der E-Mail sieht dann eine offizielle Absenderadresse in seinem E-Mail-Client und kann falsche Schlüsse über die Herkunft der Nachricht ziehen.

Die meisten Anti-Phishing Desktop-Lösungen [15, 6, 10, 11, 16] setzen in den Web-Browsern an und informieren den Benutzer mithilfe von verschiedenen Sicherheitsindikatoren, wenn er bekannte Phishing-Seiten besuchen will. Die Klassifizierung erfolgt in der Regel automatisch. Der Benutzer ist aber auf sich allein gestellt, falls er mit einer neuen, unbekannten Phishing-Seite konfrontiert wird. In einem solchen Fall werden ihm auch keine Indizien angezeigt, die darauf hinweisen, dass die von ihm besuchte Seite ein Betrugsversuch sein könnte, und kann somit falsche Schlussfolgerungen ziehen und annehmen, dass er sich auf einer ungefährlichen Seite befindet. Auch bei richtig erkannten Phishing-Seiten wird der Anwender mit einem fertigen Analyse-Ergebnis konfrontiert und kann somit kein Gefühl für den sicheren Umgang mit E-Mails und im Web entwickeln. Die Sensibilisierung des Anwenders ist aber das effektivste und in der Literatur meistempfohlene Mittel im Kampf gegen Phishing. Der bewusste Benutzer wird an jede E-Mail, die ihn auffordert, persönliche Daten preiszugeben, mit gesundem Misstrauen herangehen und sie sorgfältig prüfen, bevor er die darin enthaltenen Anweisungen ausführt. Er braucht aber Werkzeuge, die ihm bei der Analyse der verdächtigen E-Mail helfen.

1.1. Vision

Wir stellen eine Lösung namens Delphish vor, die die Vorteile der automatischen Erkennung nutzt und gleichzeitig den Benutzer für einen sicheren und verantwortlichen Umgang mit E-Mails sensibilisiert. Delphish ist als zusätzliche Toolbar für E-Mail-Clients konzipiert und ist zurzeit als Add-In für MS Outlook implementiert. Die Analyse einer E-Mail mit Delphish beginnt erst, wenn der Benutzer einen Verdacht schöpft, dass es sich um einen Betrugsversuch handeln könnte. Er drückt auf eine Schaltfläche in der Delphish-Toolbar und damit wird die Analyse der vermeintlich gefährlichen Nachricht gestartet. Delphish versucht zuerst, die E-Mail automatisch einzustufen. Unabhängig davon, ob sie automatisch als Betrugsversuch erkannt wird oder nicht, wird eine Risiko-Analyse der in der E-Mail befindlichen Links vorgenommen. Die Ergebnisse der Untersuchungen werden in einem übersichtlichen Fenster angezeigt, in dem die potenziell gefährlichen Links hervorgehoben werden. Der Benutzer kann sich jetzt selbst von der Gefährlichkeit eines jeden Links überzeugen, indem er sich zu jedem Link ausführliche Informationen, wie tatsächliches Ziel, Typ, Popularität, Alter, Domainbesitzer etc., anzeigen lässt. Da die Link-Informationen auch bei den als Phishing entlarvten E-Mails zur Verfügung stehen, lernt der Anwender im Laufe der Zeit die von Phishern

angewendeten Techniken kennen, was sich später in seiner erhöhten Wachsamkeit beim Umgang mit E-Mails widerspiegelt.

2. Mail-Analyse

Delphish bietet einen zweischichtigen Phishing-Schutz, der aus signaturbasierter und proaktiver heuristischer Analyse besteht. Die reaktive Komponente wehrt alle bekannten Phishing-E-Mails und ihre Varianten ab. Von der Entdeckung einer Phishing-Attacke bis zur Erstellung einer entsprechenden Signatur vergeht aber Zeit, in der die neuen Angriffe eine Bedrohung für die Benutzer darstellen. Um diesen unbekannten Gefahren vorzubeugen, enthält Delphish eine zweite Schutzschicht, die dem Leser anhand von Risiko- und Reputationstests die Gefahren in der E-Mail aufzeigt. Auf diese Schutzschichten wird eine dritte Schicht, die Informationsschicht, aufgelegt, die zusätzlich zu den Ergebnissen der beiden Analysen relevante Daten für jeden Link liefert, um es dem Benutzer zu ermöglichen, das Gefahrenpotenzial einer E-Mail selbst einzuschätzen.

2.1. Signaturbasiertes Scanning

Im ersten Schritt wird die verdächtige E-Mail von einem Virenscanner untersucht. Bei dieser Prüfung werden bereits bekannte Phishing-Attacken identifiziert. Der Erfolg der signaturbasierten Technologie wird durch die Aktualität ihrer Datenbasis bestimmt. Diese ist besonders bei den kurzlebigen Phishing-Attacken sehr wichtig. Eine auf dem Rechner des Anwenders installierte AV-Software ist in vielen Fällen inaktuell, da sich viele Benutzer nur unregelmäßig oder gar nicht um Updates kümmern. Aus diesem Grund haben wir uns für eine serverbasierte Lösung entschieden, die zentral und automatisch verwaltet wird. Wir setzen zurzeit die Open-Source-Lösung Clam AntiVirus ein. Delphish ist aber von der verwendeten AV-Lösung nicht abhängig, wodurch ein Wechsel der AV-Software jederzeit möglich ist. Die Kommunikation mit dem AV-Server erfolgt verschlüsselt über ein SSL-basiertes HTTP-Protokoll (HTTPS).

2.2. Link-Risiko-Bewertung

Die potenziell gefährlichen Elemente einer E-Mail sind Links, Formulare, Anlagen und aktive Inhalte, soweit sie von dem verwendeten Client ausgeführt werden. Zwar können Phishing-E-Mails den Empfänger auch ohne diese Elemente mithilfe eines entsprechend formulierten Textes verleiten, eine bestimmte Seite aufzurufen bzw. eine kostenpflichtige Telefonnummer anzurufen, jedoch sind diese Fälle zurzeit als marginal zu bezeichnen und sie können einfach durch eine musterbasierte Analyse erkannt werden. Die meisten E-Mail-Clients verfügen über eigene Mechanismen, mit den potenziell gefährlichen Anlagen umzugehen, weshalb wir auf deren zusätzliche Analyse verzichtet haben.

Im Kapitel 3 wird die Link-Risiko-Bewertungs-Engine beschrieben, die wir für die Risiko-Einschätzung der in der E-Mail enthaltenen Links entwickelt haben.

2.3. Geolocation

Die geographische Lage eines Servers, der hinter einem Link „steckt“, spielt für die Risiko-Analyse eine beträchtliche Rolle. Die seit Jahren auf dem Markt verfügbaren Geolocation-Technologien erlauben anhand der IP-Adresse die Ortung von fast jedem Computer auf der Welt.

Die geographische Herkunft der hinter einem Link liegenden Website wird von Delphish in Form des Ländernamens bzw. des dazugehörigen Fähnchens angezeigt. Zwar befinden sich über 40% [3] der Phishing-Websites in den USA, jedoch kann diese Information wertvolle Hinweise liefern, wenn die Angreifer Rechner in exotischen Ländern benutzen bzw. wenn die gefälschte Seite in einem völlig anderen Land gehostet wird, als legitime Links, die sich in der betrügerischen E-Mail auch befinden.

2.4. WHOIS

WHOIS ist ein Protokoll zur Abfrage eines verteilten Datenbanksystems, das Informationen über Internet-Domänen und deren Besitzer enthält. In der Regel beinhaltet ein WHOIS-Eintrag Angaben zum Eigentümer, zum administrativen und technischen Kontakt sowie zum Registrierungsdatum der Domäne.

In der manuellen E-Mail-Analyse liefern die Informationen zu der Domäne aus dem WHOIS-Datensatz meistens den entscheidenden Beweis dafür, dass es sich bei einem Link und somit bei der untersuchten Nachricht um einen Betrugsversuch handelt. Aus diesem Grund wird in Delphish zu jeder Domäne, die in einem Link in der E-Mail vorkommt, eine WHOIS-Abfrage ausgeführt. Um die WHOIS-Dienste nicht unnötig zu belasten, wird die einmal abgefragte Information über eine definierte Verweilzeit für spätere Zugriffe in einem lokalen Cache gehalten. Um den ungeübten Anwendern das Studieren der WHOIS-Daten zu erleichtern, haben wir uns entschieden, die Besitzerdaten einer Domäne in Form einer Adresse anzuzeigen. Da die Struktur der zurückgelieferten Daten keinen Standards unterliegt, haben wir eine Reihe von Parsern für die meistbenutzten WHOIS-Server implementieren müssen, um dies zu bewerkstelligen.

3. Link-Risiko-Analyse

In der ersten, signaturbasierten Stufe der E-Mail-Analyse versucht Delphish, eine E-Mail automatisch einzustufen. Falls aber eine solche Klassifizierung nicht möglich ist, weil die E-Mail bisher unbekannt war, erfolgt in zweiter Stufe eine Link-Risiko-Bewertung mittels der von uns für diesen Zweck entwickelten Link-Risiko-Bewertungs-Engine DelLink. DelLink ist eine Sammlung von Tests, die für jeden in der E-Mail vorkommenden Link durchgeführt werden. Auf Grundlage dieser Tests wird für jeden Link ein Risiko-Wert (RiskScore *RS*) gebildet. Um den unterschiedlichen Stellenwert der Tests festzulegen, haben wir zusätzlich eine Gewichtung w_i eingeführt. Es gibt zwei Arten von Tests: Risiko- und Reputationstests. Der Risiko-Wert *RS* eines Links ist die Differenz zwischen seinem Risiko *RISK* und seinem Renommee *REP*.

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

Die Risiko-Tests sind heuristische Tests, die den Risiko-Wert *RS* eines Links steigern. Sie untersuchen die Links auf das Vorhandensein von Techniken, die in den bisherigen Phishing-Attacken zur Verschleierung des tatsächlichen Link-

Ziels verwendet wurden. Jeder Test liefert einen Risiko-Wert V_i zwischen 0 und 1. Das Risiko *RISK* eines Links ist die Summe der einzelnen Test-Ergebnisse multipliziert mit ihrer Gewichtung:

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

Die Reputationstests sind risikomindernde Tests. Sie versuchen mithilfe der externen Services das Renommee der hinter einem Link liegenden Domäne zu ermitteln. Sie liefern ebenfalls einen Wert R_i zwischen 0 und 1. Die Reputation *REP* eines Links ist die Summe der einzelnen Reputationswerte multipliziert mit ihrer Gewichtung:

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

Überschreitet der aus der Analyse resultierende Risiko-Wert eines Links die in DelLink empirisch festgelegte Schwelle, wird er auf der Delphish-Oberfläche als gefährlich hervorgehoben.

Abhängig davon, welches Link-Element und in welchem Kontext untersucht wird, haben wir die Test-Routinen in vier Klassen unterteilt: URL-, Link-, Kontext- und Renommee-Analyse. Im Folgenden werden diese Test-Klassen genauer erläutert.

3.1. URL-Analyse

Das Ziel von E-Mail-Phishing-Attacken ist es in der Regel, den Benutzer dazu zu bewegen, einem in der Nachricht enthaltenen Link zu folgen oder einen Anhang mit einem gefährlichen Programm zu öffnen und auszuführen. Das Link-Ziel wird in den meisten E-Mail-Clients in der Statuszeile, mitunter aber auch gar nicht (wie z.B. im Microsoft Outlook 2002) angezeigt. Die Spezifikation der URL ermöglicht es den Angreifern, URLs zu bilden, die das eigentliche Ziel für den Benutzer schwer erkennbar machen können. Im Folgenden werden die URL-Verschleierungstechniken kurz erläutert, die durch DelLink zur Risiko-Bewertung mit einbezogen werden.

3.1.1. Gespoofte Domainnamen

Eine der beliebtesten und trivialsten Methoden, die die Phisher benutzen, um dem Leser vorzugaukeln, dass er es mit einem legitimen Server zu tun hätte, ist die Registrierung eines der gefälschten Domäne ähnlichen Namens. Es wird z.B. eine Domäne paypa1.com registriert, die sich auf den ersten Blick von der legitimen Domäne von PayPal, paypal.com, nicht unterscheidet.

3.1.2. „Friendly login"-URLs

Es ist möglich, Links zu bauen, die die Authentifizierungsdaten enthalten, um dem Benutzer die lästige Eingabe von Kennung und Passwort abzunehmen. Diese Möglichkeit wird von den Phishern missbraucht, um das eigentliche Link-Ziel zu verschleiern. Angenommen eine E-Mail enthält einen Link in der Form http://www.paypal.com:money@phisher.com. Der ungeübte Leser muss nicht unbedingt bemerken, dass es sich hier um eine gefälschte Seite handelt.

3.1.3. Verschleierung des Hostnamens

Eine andere Methode, den Hostnamen des tatsächlichen Ziels zu verschleiern, ist die Benutzung von IP-Adressen anstelle von Hostnamen. Jedes Programm, das über das Internet kommuniziert, muss die für die Internet-Benutzer üblichen Hostnamen in die dazugehörigen numerischen Adressen auflösen. Der Phisher kann einen Link in der Form http://www.postbank.de@123.100.200.2 bauen, um das Link-Ziel zu verstecken.

3.1.4. Untypische Ports

Die gefälschten Seiten werden sehr oft auf von den Angreifern gehackten Servern gehostet. Auch die kompromittierten Rechner der Privatanwender (sog. Bot-Netzwerke) werden für diese Zwecke benutzt. Ein typisches Merkmal für solche Server ist die Verwendung von untypischen Ports, wie z.B. 680, 85, 4443 etc. [2].

3.1.5. Verschleierung der URL

Die meisten E-Mail-Clients und Webbrowser unterstützen die Kodierung von speziellen Zeichen in der URL. Das ist notwendig, um Zeichen zu repräsentieren, die in der URL als solche nicht vorkommen können, oder zur Unterstützung von speziellen Zeichen anderer Sprachen. Es ist trivial für den Phisher, eine URL mithilfe dieser Kodierungsschemen zu verschleiern. Zum Beispiel eine URL, die wie folgt aussieht http://%77%77%77%2E%70%61%79%70%61%31%2E%63%6F%6D, ist eine Escape-kodierte Version von http://www.paypa1.com.

3.2. Link-Analyse

Diese Klasse von Tests untersucht einen oder mehrere Bestandteile eines Links mit dem Ziel, dessen verdächtige bzw. gefährliche Eigenschaften, Merkmale und Inhalte ausfindig zu machen.

3.2.1. Diskrepanz zwischen Link-URL und Link-Text

Die Phisher nutzen die Tatsache, dass die meisten Mail-Clients in HTML kodierte Inhalte darstellen können. In dem Inhaltsteil eines Links wird oft eine andere URL als in dem HREF-Attribut angegeben. Da der Benutzer in der Regel nur auf den Inhalt achtet, bleibt das eigentliche Link-Ziel für ihn verborgen.

3.2.2. Skripte

Da sich aktive Inhalte wie JavaScript oder VBScript wunderbar zur Verschleierung des tatsächlichen Link-Ziels eignen, erhöhen wir bei der Analyse das Risiko von Links, die in ihren Attributen und Ereignisbehandlungsroutinen Skript-Anweisungen enthalten.

3.3. Kontext-Analyse

Im Laufe der Analyse der in den bisherigen Phishing-Attacken angewendeten Techniken und Tricks haben wir festgestellt, dass es sinnvoll ist, die Links im Kontext der anderen Links zu untersuchen. Dadurch lassen sich die Verweise herausfinden,

die durch ein bestimmtes Merkmal aus der Menge herausstechen.

3.3.1. Überdeckte Links

Eine andere Methode zur Verschleierung des gefälschten Link-Ziels haben wir in einer Phishing-Attacke auf die Kunden der Volksbanken Raiffeisenbanken gefunden:

```
<A HREF="http://www.volksbank.de/__C1
256B56003097E2.nsf/X851A68E4F14128EFC1256C
670055579C">
<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>
```

In dem aufgeführten Beispiel wird ein Bild, das im Anker steht, durch einen linksensitiven Bereich überdeckt. Somit zeigt der dadurch entstandene Link nicht auf die durch das HREF-Attribut des Ankers (http://www.volksbank.de/__C1256B56003097E2.nsf/X851A68E4F14128EFC1256C670055579C) definierte URL, sondern auf eine Phishing-Seite, die auf dem Server mit der IP-Adresse 210.68.8.180 liegt. Die Verwirrung des Lesers kann durch den Angreifer noch gesteigert werden, indem er nur einen Teil des Bildes durch einen linksensitiven Bereich überdeckt.

3.3.2. Bildlinks

Die von Spammern benutzten Techniken, um die zur Identifizierung von ungewollten E-Mails eingesetzten Filter zu umgehen, werden auch bei der Erstellung von Phishing-E-Mails angewendet. Schließlich wollen die Angreifer, dass ihre E-Mails auch eine größtmögliche Menge von Lesern erreichen. Eine beliebte Methode, die auch oft in Phishing-Attacken zu finden ist, ist die Verwendung eines Bildes bzw. von Bildern anstelle von Text. Solche Nachrichten enthalten in der Regel ein Bild, das gleichzeitig ein Link ist. Delphish erkennt solche Bild-Links und erhöht für diese Links das Risiko bei der Analyse. Im Laufe der Entwicklung haben wir uns entschieden, diese Maßnahme auf alle Bild-Links in der E-Mail auszuweiten, falls sie ausschließlich solche enthält. Wir sind der Meinung, dass der Leser dieser Art von Links bei der E-Mail-Verifikation eine größere Aufmerksamkeit schenken soll, auch wenn dadurch die False-Positive-Rate unserer Lösung steigt.

3.3.3. Host-Lokalisierung

Damit die Nachricht einer echten E-Mail der gefälschten Organisation/Institution täuschend ähnlich sieht, werden Original-Bilder und -Logos verwendet. Um bei dem Leser den Eindruck der Echtheit der gefälschten E-Mail zu verstärken, werden auch richtige Links in den Text eingebettet. Sehr oft ist nur ein Link gefälscht, der den Benutzer zu einer gefährlichen Seite führen soll. Die von Delphish eingesetzte Geo-Datenbank ermöglicht die Lokalisierung des Standortes des Servers, auf welchen der in der E-Mail befindliche Link zeigt. Diese Information haben wir auch mit in die Risiko-Bewertung einbezogen. Damit können die Links entdeckt werden, die zu Seiten führen, die auf einem anderen Server als dem, zu dem die restlichen Links führen, gehostet werden.

3.4. Renommee-Analyse

Die Reputationstests gehören zu den das Link-Risiko mindernden Tests und werden mittels Abfrage von externen Internet-Diensten durchgeführt.

3.4.1. Popularität der Link- Domäne

Die Popularität der Domäne ist ein Wert, der die Anzahl der externen Seiten widerspiegelt, die auf diese Domäne verlinken. Sie ist ein Indikator dafür, wie oft der Inhalt der Website von anderen inspiziert wurde. Das ist ein Maß für die Vertrauenswürdigkeit einer Domäne.

3.4.2. Alter der Domäne

Die von Phishern verwendeten Domains sind in der Regel kurzlebig (laut der letzten Statistiken der Anti-Phishing Working Group 4.8 Tage), da eine Phishing-Attacke ziemlich schnell entdeckt wird. Außerdem kann es für den Betrüger wegen der Verfolgung gefährlich sein, sie eine längere Zeit zu betreiben. Deswegen kann eine Information über das Alter einer Domäne bei der Analyse eine große Hilfe sein. Eine Domäne, die vor einem Monat registriert oder im Internet noch nie gesehen wurde, soll die besondere Aufmerksamkeit des Anwenders wecken.

4. Architektur und Implementierung

Die Architektur von *Delphish* ist in der Abbildung 1 dargestellt.

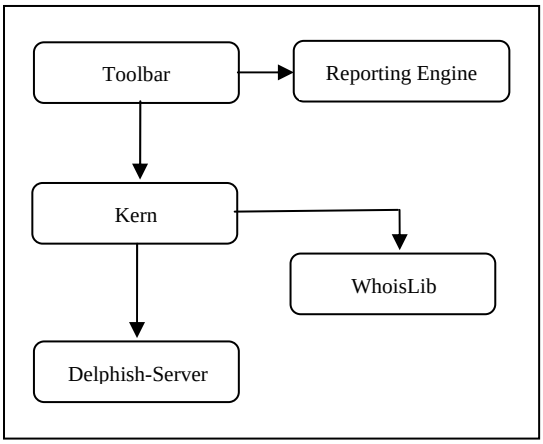


Abbildung 1: Delphish-Architektur.

4.1. Delphish-Komponenten

- Kern, der unabhängig von dem verwendeten E-Mail-Client entworfen wurde. Der Kern kommuniziert mit dem Delphish-Server, um die E-Mail mit bekannten Signaturen von Phishing-E-Mails zu vergleichen. Hier befindet sich auch die Link-Risiko-Bewertungs-Engine DelLink.
- Reporting-Engine, die für die graphische Ausgabe der Einstufung und Analyse verantwortlich ist.

- WHOIS-Bibliothek, die aus einem WHOIS-Client und den dazugehörigen Parsern besteht.
- Toolbar, eine Client-abhängige Komponente, die dem Anwender den Zugriff auf die Delphish-Funktionen in dem von ihm verwendeten E-Mail-Programm ermöglicht.
- AV-Server, der die signaturbasierte Analyse der verdächtigen E-Mail durchführt. Er sorgt für die Aktualität der verwendeten Signatur-Datenbank.

4.2. Implementierung

Delphish wurde komplett in C++ implementiert. Die einzelnen Client-Komponenten kommunizieren miteinander mittels klar definierter Schnittstellen. Das Add-In für Microsoft Outlook haben wir als ATL-COM Komponente implementiert. Damit der Einsatz von Delphish in anderen Programmen ohne Probleme möglich ist, haben wir uns entschieden die restlichen Delphish-Bibliotheken als reguläre Windows-DLLs zu entwerfen. Bei der Entwicklung des GUI haben wir auf Frameworks von Drittanbietern (wie z.B. MFC) bewusst verzichtet, um die Installation von Delphish nicht unnötig durch zusätzliche Dateien, die mitgeliefert werden müssen, zu belasten. Für die Datenhaltung haben wir die schlanke und in der Handhabung einfache SQLite Engine genommen, die ohne zusätzliche Installation von Datenbankservern in das Programm eingebunden werden kann. Die Parser für WHOIS-Informationen sind als einzelne Module konzipiert (mehrere Parser in einer Bibliothek möglich), wodurch eine einfache Erweiterung von Delphish um weitere Parser möglich ist.

Um die geographischen Daten zu ermitteln, wie das Land, wo die jeweilige verlinkte Seite gehostet wird, haben wir uns für GEO-IP von MaxMind entschieden.

Das Programm wurde mit einer einfachen Update-Schnittstelle ausgestattet, die in regelmäßigen Intervallen für Aktualisierungen sorgt.

4.3. Benutzer-Interface

Es war uns wichtig, dass der Benutzer durch unsere Lösung in seiner gewohnten Umgebung nicht behindert wird. Da die Prüfung der E-Mail und die Anfragen an externe Reputations-Services eine von der Art des Internetanschlusses und Auslastung der kontaktierten Server abhängige Verarbeitungszeit benötigen, haben wir uns entschieden die Prüfung asynchron durchzuführen. Das ermöglicht dem Anwender das störungsfreie Fortsetzen seiner Arbeit mit seinem E-Mail-Programm, während die gewünschte E-Mail untersucht wird.

Nachfolgend werden kurz die Bestandteile der Delphish-Benutzeroberfläche beschrieben.

4.3.1. Delphish-Toolbar

Nach der Installation wird im E-Mail-Client eine Toolbar angezeigt, die in der Abbildung 2 dargestellt wird. Über diese Symbolleiste erhält der Benutzer Zugang zu den wichtigsten Funktionen und Optionen von Delphish.

Abbildung 2: Delphish-Toolbar

4.3.2. Statusberichtsfenster

Das Statusberichtsfenster (Abbildung 5) stellt die Ergebnisse der von Delphish durchgeführten Analysen graphisch dar. Wir haben uns entschieden diese Informationen in einem Popup-Fenster (Systray-Popup) über dem Taskleisten-Infobereich zu zeigen. Der Status der ausgewählten E-Mail wird zusätzlich mittels eines Icons in der Delphish-Toolbar symbolisiert.

4.3.3. Details-Dialog

Der Details-Dialog ist eine andere Ansicht des Statusberichtsfensters. Er ist für die Benutzer gedacht, die lieber mit einer Listen-basierten als einer graphischen Darstellung der Links arbeiten. Er ist auch bei solchen E-Mails nützlich, bei denen die graphische Variante durch die große Anzahl der Links unübersichtlich werden kann.

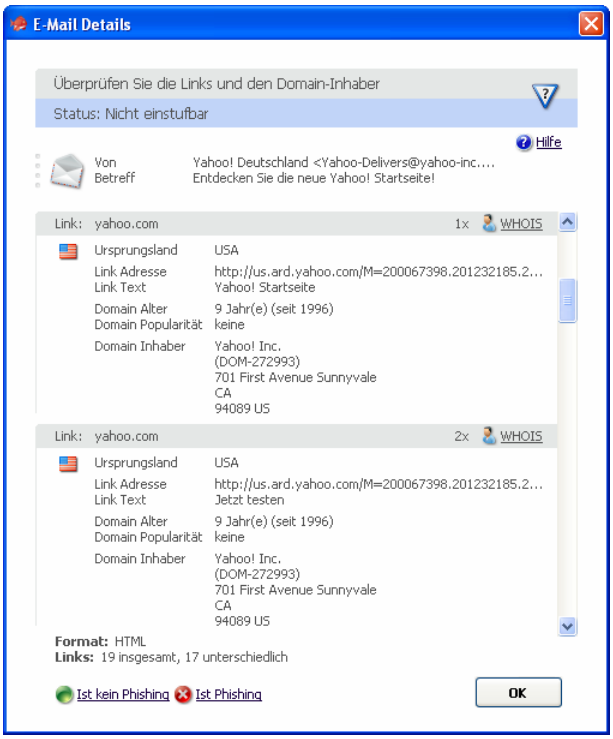


Abbildung 3: Details-Dialog.

4.3.4. WHOIS-Dialog

Die zurückgelieferten WHOIS-Informationen werden in ihrer Original-Form in einem separaten Fenster (Abbildung 6) angezeigt. Je nach WHOIS-Server sind sie unterschiedlich formatiert.

4.3.5. Statistik und Einstellungen

Delphish verfügt über zahlreiche statistische Auswertungen, die über die Toolbar abgerufen werden können. Sie werden in

einem speziell entworfenen Statistik-Fenster übersichtlich präsentiert.

Die Einstellungen über Sprachauswahl, verwendeten Proxy-Server etc. sind über einen Konfigurationsdialog möglich.

5. Evaluierung

Auf die Evaluierung der ersten Stufe der Delphish-Analyse haben wir verzichtet, weil sie von der eingesetzten Antiviren-Software abhängt. Da sie und die dazugehörige Signatur-Datenbank regelmäßig und automatisch aktualisiert werden, muss die Erkennungsrate dem aktuellsten Stand der AV-Software entsprechen. Wir haben uns auf die Evaluierung der Link-Risiko-Analyse konzentriert, die dem Benutzer behilflich sein soll, wenn er auf eine bisher unbekannte Phishing-Attacke stößt. Die in der Risiko-Analyse verwendeten Heuristiken können folgende Fehleinschätzungen produzieren:

- *False Positive*, falscher Alarm, falls ein untersuchter Link unter Verwendung von bekannten Phishing-Tricks gebaut wurde, aber trotzdem ungefährlich ist. Zum Beispiel könnte eine E-Mail einen Link auf eine Seite im Google-Cache enthalten, der eine IP-Adresse anstatt von Hostnamen benutzt.
- *False Negative*, trügerische Sicherheit, wenn der untersuchte Link mit keiner der bisher bekannten Täuschungs-Techniken gebaut wurde und dazu keine Merkmale aufweist, die ihn von den anderen unterscheiden.

Für die Bewertung der Link-Risiko-Engine haben wir zwei Gruppen gebildet, die jeweils über dreihundert E-Mails enthielten:

- Phishing-E-Mails, die durch unseren Dienst SaferSurf [12] aussortiert worden waren. SaferSurf ist ein Proxy-basierter Dienst, der die Web- und E-Mail-Inhalte filtert. Die Erkennung der gefährlichen Inhalte erfolgt dabei durch den Einsatz von Virenscannern.
- Normale E-Mails, die ebenfalls über SaferSurf abgeholt worden waren.

Dank dieser Vorsortierung durch die Antivirus-Software konnten wir die Fehlklassifikationsrrate bei der Gruppenbildung auf ein Minimum reduzieren. Die E-Mails aus beiden Gruppen wurden mithilfe von DelLink analysiert. Die Ergebnisse wurden dann manuell ausgewertet. Anschließend haben wir Testpersonen, die über Kenntnisse der Internet-Grundkonzepte (wie Links, URLs, Domänen etc.) verfügen, gebeten, Phsihing-E-Mails nur anhand der von Delphish in der zweiten Analysestufe gelieferten Informationen zu klassifizieren, ohne sie die Ergebnisse der AV-basierten Bewertung wissen zu lassen.

Table 1: Auswertung der Link-Risiko-Analyse-Ergebnisse

Calculations	Phishing	Nicht Phishing
False Positive Rate	1%	4%
False Negative Rate	32%	-
Korrektklassifikationsrate	83%	96%
Fehlklassifikationsrate	17%	4%

In der Phishing-Gruppe lag die Korrektklassifikationsrate bei 83%. Die ungefährlichen Links in den untersuchten E-Mails waren „korrekt“ ohne Anwendung von Phishing-Techniken aufgebaut, was sich in der minimalen (1%) False Positive Rate widerspiegelte. Das ist darauf zurückzuführen, dass die Angreifer die Nachrichten so weit wie möglich wie die Originale gestalten wollen und dazu richtige Links nutzen. Die Fehlklassifikationsrate lag bei 17% und war bis auf wenige Ausnahmen durch False negatives bestimmt. Zwar hat DelLink in 32% aller positiven Ergebnisse die Links fälschlicherweise als ungefährlich eingestuft, jedoch waren die Testpersonen in nahezu allen Fällen in der Lage, diese Links mithilfe der mitgelieferten WHOIS- und Renommee-Informationen als Betrugsversuche zu entlarven. Das stimmte auch mit unserem Grundkonzept überein, DelLink lediglich als Hilfe zu betrachten, die den Anwender auf die offensichtlich gefährlichen Links aufmerksam machen soll. In jedem Fall soll der Anwender alle Links genau inspizieren, bevor er einer Nachricht sein Vertrauen schenkt.

Nachfolgend wird die Delphish-Analyse anhand von zwei ausgewählten Beispielen aus der Praxis vorgestellt.

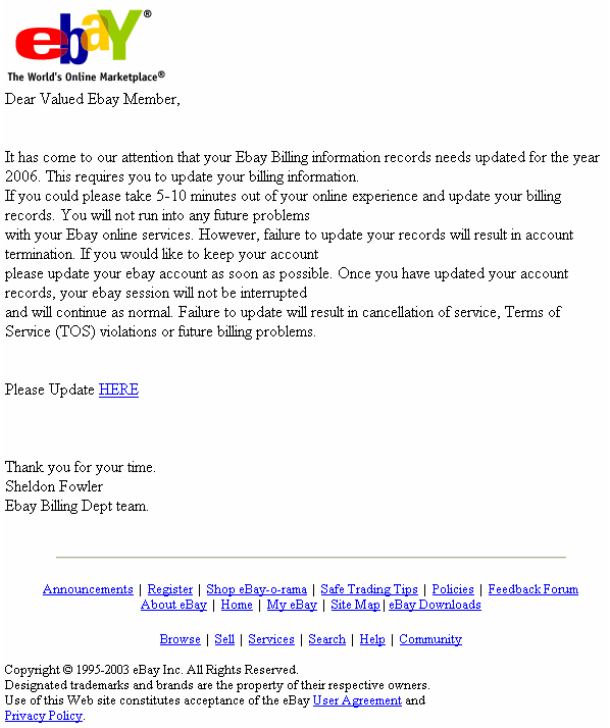
5.1. „Account suspended“ Attacke

Das ist eine klassische Phishing-Attacke, die den Leser auffordert seinen Account zu aktualisieren, um zu verhindern, dass der gesperrt wird. Abbildung 4 zeigt eine echte E-Mail, die sich an Ebay-Benutzer richtet und Ende 2005 verschickt wurde.

Die von uns eingesetzte Antiviren-Software konnte diese E-Mail in der ersten Analyse-Stufe nicht automatisch einordnen. Die Link-Risiko-Analyse hat unter den 21 unterschiedlichen Links, die in dieser Nachricht vorkamen, einen Link („HERE“) als potenziell gefährlich eingestuft, was in Abbildung 5 zu sehen ist.

Wie man in dem Statusberichtsfenster von Delphish sehen kann, zeigt der markierte Link auf eine Seite, die auf einem Server (202.224.236.250) in Japan gehostet wird. Die Reputationstests haben ergeben, dass diese Adresse im Internet noch nicht gesehen wurde („Domain Alter“) und dass es sich um eine unbekannte Domäne handelt.

Aus den WHOIS-Informationen in Abbildung 6 geht hervor, dass diese IP zu einem ISP namens Mashito Outa gehört. Es existiert kein sichtbarer Bezug zu Ebay. Anhand dieser Indizien sind wir zu dem Entschluss gekommen, dass es sich bei dieser Nachricht um einen Betrugsversuch handelt.



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

Copyright © 1995-2003 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

Abbildung 4: ”Account suspended” Attacke

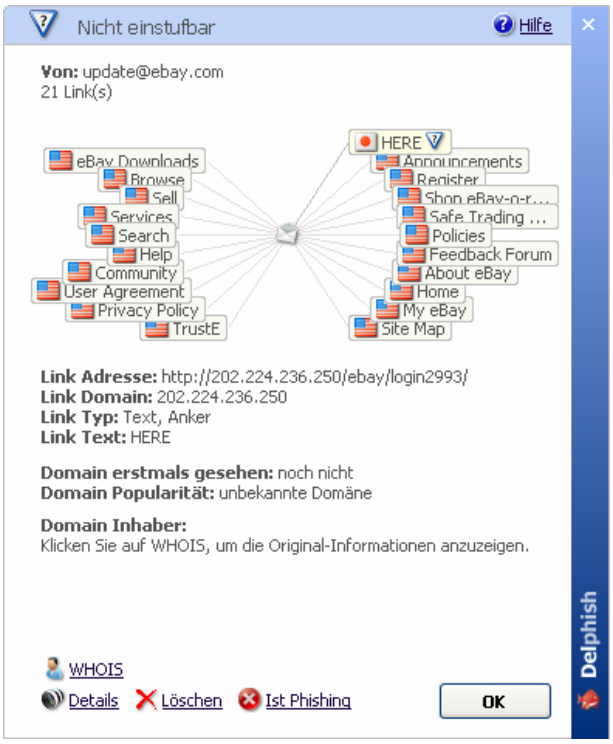


Abbildung 5: Nicht einstufbar

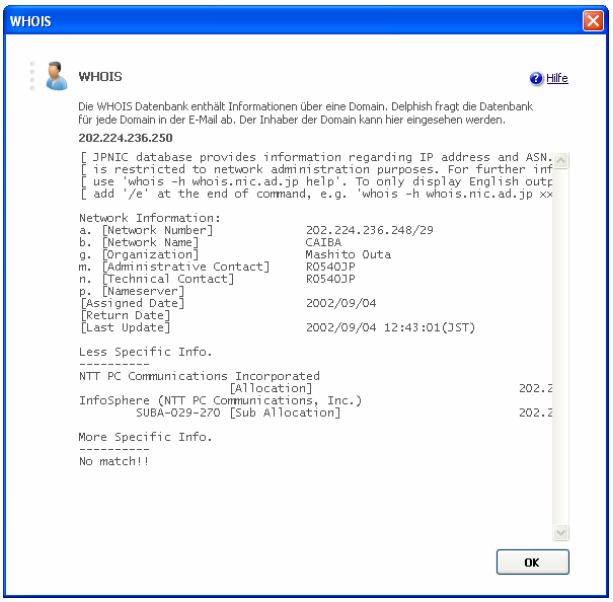


Abbildung 6: WHOIS-Informationen

5.2. PayPal Attacke

Die E-Mail in Abbildung 7 zeigt eine typische Attacke auf Kunden von PayPal. Sie informiert den Kunden darüber, dass es Login-Versuche auf sein Konto gegeben hätte, die von ausländischen IP-Adressen ausgeführt worden wären. Er wird gebeten, seine Identität zu verifizieren, indem er den in der Nachricht aufgeführten Link benutzt. Damit er die ganze Angelegenheit ernst nimmt, wird ihm mit der Suspendierung seines Accounts gedroht.

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should **never** give your PayPal password to anyone, including PayPal employees.

Abbildung 7: PayPal-Attacke

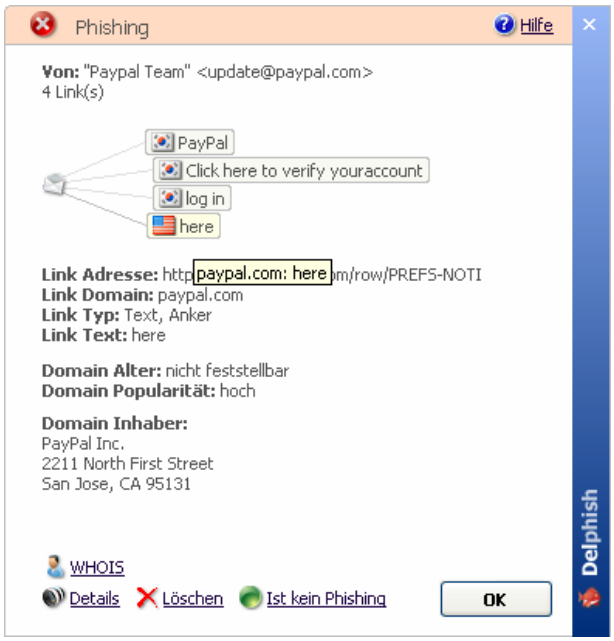


Abbildung 8: Statusberichtsfenster für die PayPal-Attacke

Die E-Mail enthielt insgesamt vier Links. Die signaturbasierte Analyse hat sie als Phishing identifiziert. Die Gründe dafür lieferte uns die Durchsicht der übrigen von Delphish zur Verfügung gestellten Informationen. Die Link-Risiko-Bewertungs-Engine konnte zwar keine Links als gefährlich erkennen, aber bereits ein Blick auf das Statusberichtsfenster in der Abbildung 8 zeigt, dass drei der Links zu einer Website führen, die sich in Korea befindet (der vierte Link zeigt auf PayPal). Da der Domain-Alter-Test ergab, dass diese Website bereits seit 3 Jahren existierte, konnten wir davon ausgehen, dass sie entweder von Angreifern übernommen oder kompromittiert wurde. Aus dem WHOIS-Datensatz konnten wir entnehmen, dass die dazugehörige Domäne einer Firma aus Seoul gehörte und es bestand keine erkennbare Verbindung zwischen ihr und PayPal.

5.3. Schlussfolgerung

Unsere Lösung hat sich in der Praxis bewährt, wie die Evaluierung zeigt. Die bekannten Phishing-E-Mails werden bereits in der ersten Analyse-Stufe mithilfe von Antiviren-Software identifiziert. Die zusätzlichen Analysen und Hilfen, die Delphish zur Verfügung stellt, wie Link-Risiko- und Reputationsanalyse sowie WHOIS-Informationen, liefern dem Benutzer ausreichend Hilfe, um neue, bisher unbekannte Attacken abzuwehren. Der Anwender lernt mit der Zeit, die Tricks der Phisher und verdächtige Muster in den Links zu erkennen.

6. Zukünftige Erweiterungen

Wir betrachten Delphish keineswegs als ein vollendetes Werk, sondern als ein Tool zur Bekämpfung von Phishing, das sich ständig auf neue Tricks und Techniken, die von den Kriminellen erfunden und angewendet werden, einstellen muss. Dazu gehört eine kontinuierliche Weiterentwicklung des Programms. Wir planen, Delphish um weitere hilfreiche Analysen und Berichte zu erweitern, die bestehende Technologien und Informationen nutzen, mit dem Ziel, Auskünfte über die E-Mail und ihre Herkunft zu liefern. Es sind u.a. folgende Erweiterungen geplant.

- Analyse des zur Übertragung einer E-Mail verwendeten Weges mittels SMTP Path Analyse
- Erkennung von IDN-Spoofing-Angriffen
- Prüfung, ob der angegebene Link zu einem Free-Web-Hoster führt
- Prüfung, ob die E-Mail von einem Free-E-Mail-Provider-Konto abgeschickt wurde
- Ausarbeitung und Implementierung von Mechanismen zur Phishing-Target-Erkennung
- Prüfung der SSL-Zertifikate
- Verwendung von Blacklists, die die bekannten Spam- und Phishingrechner identifizieren
- Erkennung von dynamischen IP-Adressen in Links

7. Nutzwerk GmbH

Die Nutzwerk GmbH ist ein Anbieter von Sicherheitslösungen, überwiegend für Privatkunden. Sie betreibt den Proxy-basierten Dienst SaferSurf (http://www.safersurf.com).

8. Literatur

[1] Amir Herzberg, Ahmad Gbara, *TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks*, 2004: Cryptology ePrint Archive: Report 2004/155.

[2] Anti-Phishing Working Group, *Phishing Activity Trends Report*, Juli 2006.

[3] Anti-Phishing Working Group, *Phishing Activity Trends Report*, Juli 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 Attakcs: 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