# *Cyberfahnder*

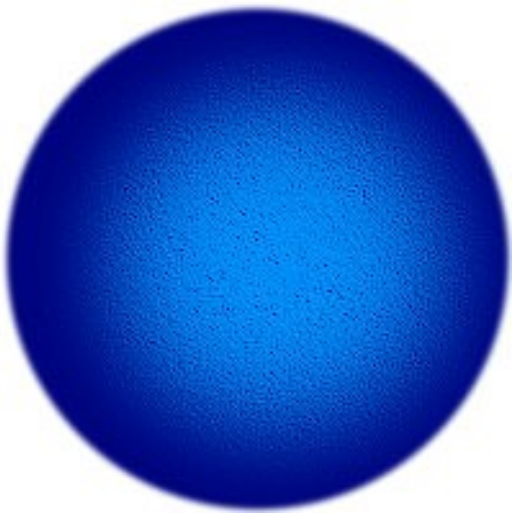
#001

***Wie funktionieren die Informationstechnik und das Internet?***

# Phishing

**Die Phisher nutzen alle Techniken des Angriffs, Ausspähens und Täuschens, die die Informationstechnik und das Marketing entwickelt haben.**
**Sie sind die Ersten, die sich ausschließlich darauf konzentrieren, die Netz- und Informationstechnik für einen Zweck zu missbrauchen: Zum Betrug.**

Version 1.1
Stand: 21.01.2007



## Cyberfahnder

In den Jahren 2000 bis 2006 stellte Cyberfahnders EDV-Workshop im Internet für die Ermittlungspraxis hilfreiche Adressen und Erklärungen vor. Die Website wurde im Herbst 2006 gelöscht, weil sie schon lange nicht mehr auf dem aktuellem Stand war.

Künftig möchte ich mich einzelnen Schwerpunkten widmen und keine breite Palette von Themen regelmäßig auf dem Laufenden halten.

Ziel ist es dabei, Ermittlerinnen und Ermittlern auf dem Hintergrund des Straf- und Strafverfahrensrechts einen Eindruck von den technischen Prozessen und Wirkungen zu vermitteln und in ihre rechtliche Beurteilung einzuführen. Mir geht es dabei nicht um tiefe juristische Auseinandersetzungen, sondern um das tatsächliche Wissen und Handwerkzeug, um das Recht anwenden zu können.

CyberHeft #001

Thema: **Phishing**
Autor: Dieter Kochheim
Hannover
Stand: 22.01.2007

Inhalt:



Abbildungen:



## Einleitung „Phishing“

Der Begriff leitet sich, so die überwiegende Meinung, von „Password Fishing“ ab, also von dem Ausspähen von Kontozugangsdaten mit dem Ziel ihres Missbrauchs.

Die Phisher nutzen dazu alle Erkenntnisse und Mechanismen des Einbruchs, des Überredens und des Missbrauchs der modernen Netz- und Informationstechnik. Sie agieren in aller Regel aus dem Ausland und bleiben dadurch weitgehend unerkannt und von der Strafverfolgung unbehelligt.

Kriminalistische Analysen über das Vorgehen und die Organisation der Phisher sind (mir) bisher nicht bekannt. Bei meiner Darstellung muss ich deshalb ganz überwiegend auf journalistische Quellen und eigene Recherchen zurückgreifen. Sie zeigen ein noch nicht geschlossenes Bild mit einigen Konturen.

Zum Verständnis des Phishings müssen eine Reihe anderer Themen und Phänomene angesprochen, aber nicht in ihren Einzelheiten vertieft werden. Dazu gehören besonders das Hacking, also das Eindringen und missbrauchen von fremden Computersystemen, und das Spamming, also der massenhafte Versand von elektronischen Nachrichten. Im Zusammenhang mit dem Spamming sind vorwiegend zwei Zielrichtungen hervorzuheben: Entweder sollen Kunden für Kaufgeschäfte geworben oder mit der Nachricht sollen schädliche Programme verteilt werden (Viren, Würmer, Trojaner), wobei nur die Einwahlprogramme für Umleitungen zu teuren Mehrwertdienstenummern (Dialer) nahezu vom „Markt“ verschwunden sind.

Eine systematische Auswertung der Absender von Spam-Nachrichten und der Urheber von Phishing-Aktionen für den deutschsprachigen Bereich fehlt bislang. Das ist im US-amerikanischen Bereich anders, wo sich eine Menge von privaten Initiativen um die Dokumentation auffälliger Internet- und Domainadressen kümmern und damit eine gewisse Öffentlichkeit gegen die Ohnmacht herstellen.

Im selben Maße haben auch die Strafverfolgung und die Rechtsprechung im Zusammenhang mit dem Phishing kaum eine öffentliche Resonanz gefunden. Der insoweit sehr rege Heise-Verlag, der den Meldungsdienst heise online betreibt, kennt nur drei Meldungen, bei denen die Suchworte „Phishing“ und „Anklage“ zusammen kommen. Die älteste vom 21.05.2006 berichtet von einem 23-jährigen US-Amerikaner, der wegen Betrugs im Zusammenhang mit Phishing zu einer Freiheitsstrafe von 21 Monaten verurteilt worden sei [1]. Die zweite berichtet davon, dass ein Finanzagent vom Amtsgericht Überlingen per Strafbefehl zu einer Geldstrafe von 30 Tagessätzen verurteilt worden sei [2] und die jüngste vom 15.12.2006 darüber, dass das Landgericht Frankfurt gegen sechs Litauern und einem Deutschen ein Strafverfahren wegen Kontomanipulationen führe, wobei zwischen Juli 2005 und März 2006 Trojaner zum Ausspähen von Kontozugangsdaten eingesetzt worden seien [3].

Spamming und Phishing sind Plagen, die die E-Mail-Konten der Anwender vollmüllen, Netze und Systeme belasten, Vermögensgefahren verursachen und die Öffentlichkeit verunsichern. Wegen des Phishings werden von ihr im Wesentlichen die Spamming-Aktionen wegen der Werbung von Finanzagenten und zur Auskundschaftung von Bankkunden sowie die gefälschten Webseiten bekannt, die zum Ausspionieren der Kontozugangsdaten dienen.

---

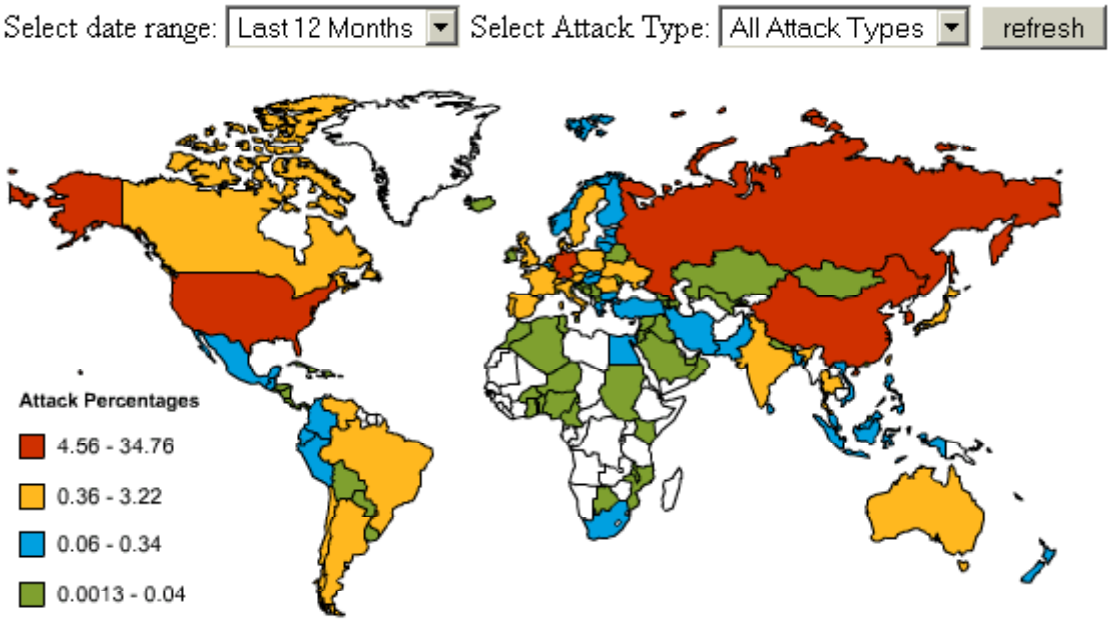
1 21 Monate Haft für Phishing, heise online 21.05.2006

2 Strafbefehl gegen "Finanzagenten" wegen Phishing-Beteiligung, heise online 27.09.2006

3 Prozess um Online-Phishing beginnt mit Verzögerung, heise online 15.12.2006

**Angriffe durch Phishing und „Crimeware“ im Jahr 2006**

Quelle: Phishing and Crimeware Map, 19.12.2006



Phishing ist die kriminelle Steigerung des Spammings, das allein schon mit seinem Aufkommen erhebliche wirtschaftliche Schäden verursacht. Ein Beispiel soll genügen: Das Informatikzentrum Niedersachsen – izn – wurde im November 2006 in Hochzeiten von mehreren Zehntausend Spam-Nachrichten pro Minute penetriert, so dass es kurzfristig auch zum Verlust von „normalen“ E-Mails kam [4].

Die geographischen Schwerpunkte für das Phishing bilden die USA, Deutschland und schließlich Russland [5]. Wegen der Verbreitung von Crimeware wird darüber hinaus Spanien lokalisiert. Ihnen folgen von West nach Ost Nord- und Südamerika, Europa einschließlich der Türkei, China und Japan.

Die von den Phishern verwendeten E-Mail-Texte, das Layout und die gefälschten Webseiten werden immer professioneller und damit auch gefährlicher, weil immer mehr Opfer auf sie hereinfallen können.

Dies zeigt, dass hinter den Phishing-Aktionen ein erheblicher Aufwand und eine beachtliche Logistik stecken.

## Formen des Phishings

Wegen des Ausspähens von Kontozugangsdaten lassen sch vier Erscheinungsformen des Phishings unterscheiden.

1. Die Täter greifen auf Daten zurück, die sie von anderen bekommen (gekauft) haben. Hierbei kommen zum Beispiel Daten von ausgelesenen und kopierten Kreditkarten zum Einsatz.
2. Die Täter verwenden eine E-Mail mit Formulareigenschaften, bei der die Kontodaten in die vorgegebenen Felder eingetragen werden sollen.
3. Die bekannteste Variante lockt die Opfer auf nachgemachte Webseiten, die so wie die Originalseite der betreffenden Bank gestaltet ist.
4. Die Täter setzen Malware, besonders Würmer oder Trojaner zum Ausspähen der Zugangsdaten ein.

In den folgenden Beispielen beschränke ich mich auf die unter Ziffer 3. bezeichnete Variante.

## Pharming

Das Pharming ist eine Weiterentwicklung im Zusammenhang mit dem Phishing. Es bewirkt, dass die Pfadangaben für eine Webseite manipuliert werden und der Angriff verschleiert wird. Hierzu gibt es mehrere Möglichkeiten:

1. Beim **DNS-Poisoning** werden die Webbrowser-Einstellungen im Computer des Opfers verstellt. Zur Auflösung einer DNS-Adresse greift der Computer zuerst auf eine eigene Tabelle zu, in der die am häufigsten benutzten Adressen verzeichnet sind. Dadurch werden Anfragen an DNS-Server im Internet vermieden.
2. Beim **Cross-Site-Scripting** werden in den Code der Originalseite korrumpierte Teile eingesetzt, die den Kunden unbemerkt zu einer manipulierten Seite führen.
3. Das **serverbasierte DNS-Poisoning** ähnelt der ersten Variante, nur dass hierbei die DNS-Tabellen eines Zugangsproviders korrumpiert werden.

4 Mail-Sperre durch irrtümlich gesetzten Spamfilter, heise online 26.11.2006

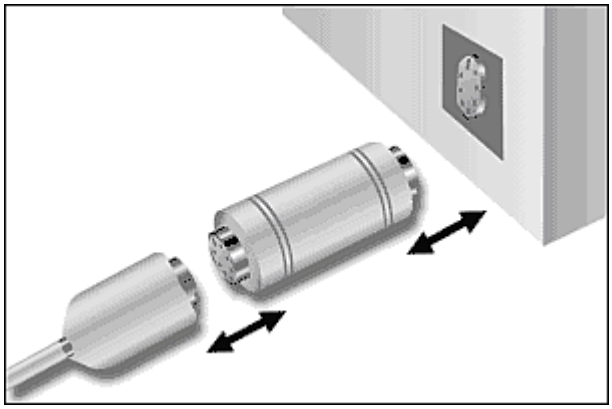
5 Zählung von Phishing and Crimeware Map, siehe Seite 6. Als „Crimeware“ werden dabei Keylogger, also Programme zur Protokollierung von Tastatureingaben, und Trojaner angesehen, die sich weiter verbreiten und missbräuchliche Aktionen ausführen können.

Links: Präparierter Bankautomat (Bild: LKA Bayern)

Mitte: Kartenleser als Aufsatz zum Originalteil (ohne Abbildung: Die Tastatureingaben werden von einer versteckten Kamera aufgezeichnet).

Unten: Hardware-Keylogger zum Protokollieren von Tastatureingaben (hier: Angebot von keylogger-hrd.com)

Dies ist ein falsches Teil, das auf dem Original angebracht ist (selbe Farbe, selber Aufkleber). Dieses Teil enthält einen Kartenlektor, der die auf der Karte enthaltenen Informationen kopieren kann und es damit ermöglicht, eine neue, identische Karte herzustellen!!!



## Ausforschung von Bankdaten

### Hardwarebasierende Methoden

Zur Ausforschung von Bankdaten sind in der Vergangenheit und werden noch heute verschiedene kriminelle Methoden verwendet. Eine traditionelle Methode ist das Auslesen und Kopieren von Kreditkartendaten, wobei es darauf ankommt, an die vollständigen Kreditkarteninformationen einschließlich der Prüfziffer für die Karte selber zu gelangen (Fachbegriff: CCV2). Sie ist meistens auf der Rückseite der Karte aufgedruckt.

Eine klassische Form des Angriffs ist auch die Täuschung durch (handwerklich gut gemachte) Fassaden. In ihrer ursprünglichen Form handelte es sich um Aufsätze vor Nachtbriefkästen und Einwurfschächten für Geldbomben. Diese wurden von den Tätern nach Feierabend vor die Originalinstallation einer Bank montiert und verhinderten, dass die Geldbomben oder Verrechnungsschecks in den Tresor (usw.) der Bank fielen, sondern in den Zwischenraum hinter der Fassade.

Ihre neuere Spielart verhält sich zunächst wie ein normaler Geldautomat und protokolliert die eingegebenen Geldkartendaten. Dann zieht die Fassade die Geldkarte ein und die Täter können noch in der Nacht eigene Geldabhebungen durchführen.

Solche Attacken sollen seit 2005 vorwiegend im Mittelmeerraum stattgefunden haben, wo vor allem die Touristen mit dem "normalen" Gebahren der dortigen Geldautomaten nicht vertraut sind. Dabei sollen bevorzugt unauffällige Aufsätze auf den Kartenleseinheiten der Geldautomaten und Miniaturkameras zum Einsatz gekommen sein, mit denen die Tastatureingaben aufgezeichnet wurden.

### Keylogger

Keylogger sind Adapter, die zwischen den Stecker der PC-Tastatur und der Tastatur-Buchse am PC eingestöpselt werden. Sie protokollieren alle Tastatureingaben mit und speichern sie. Während die älteren Varianten vom Täter wieder deinstalliert werden müssen ist auch von neueren Arten berichtet worden, die nach einem vorgegebenen Zeitpunkt oder nach einer bestimmten Datenmenge ihren Speicherinhalt per Funk dem Täter übermitteln. Dann können sie weitere Daten ausspähen.

Solche Hardware-Keylogger werden weniger für die Spionage nach Kontodaten, sondern eher für lange Texte eingesetzt. Aber das ändert nichts an ihrer prinzipiellen Gefährlichkeit.

Die moderne Malware realisiert Keylogger als Programme, die ebenfalls Tastatureingaben und andere Vorgänge im Computer protokollieren.

## Malware

Als Angriffspunkte für die Spionage sind viele Schnittstellen denkbar. Moderne Laptops und andere mobile Geräte sind mit verschiedenen von ihnen ausgestattet, die unterschiedliche Frequenzbereiche des Funks betreffen.

Sie beschränken sich aber nicht auf die üblichen Funknetze (Wireless LAN - WLAN), deren Gefahren beim unbedarften Umgang hinreichend bekannt sind, sondern können auch den "Nahfunk" betreffen. Die dazu etablierte Technik ist "Bluetooth". Kaum einem Anwender ist geläufig, dass sein Laptop permanent nach Gegenstellen suchen könnte, mit denen es einen Kontakt aufbauen und Daten austauschen könnte. Diese Gegenstelle könnte in dem Werbegeschenk eines Geschäftsfreundes eingebaut sein und z.B. die Eingaben in das Laptop protokollieren.

tecchannel, 20.01.2007

### Cyberattacke: Schwedische Bank um viel Geld erleichtert

**Die schwedische Bank Nordea wurde laut Theinquirer von Cyberkriminellen um zirka 928.000 Euro erleichtert.**

Es sollen sich mindestens 250 Kunden in den letzten drei Monaten Dateien heruntergeladen haben, welche die Backdoor „haxdoor.ki“ enthielten. Der Schadcode schaltete sich ein, sobald Kunden versucht haben, Online-Banking zu betreiben. Die Software hat persönliche Daten gestohlen. Danach erschien eine Fehlermeldung mit der Bitte, die Daten noch mal zu senden. Die Hacker hatten angeblich zwei Zugriffscodes, um Geld zu transferieren.

Die schwedische Polizei glaubt, dass die Angreifer in Russland sitzen. Man verfolgte eine Spur, die zunächst auf einen amerikanischen Server führte. Danach wurden die Daten nach Russland weitergeleitet. McAfee sagte, dass dieser Angriff einen beunruhigenden Trend aufzeige. (jdo)

Die am meisten unkalkulierbare Gefahr ist der Mensch, der aus Bosheit, Selbstüberschätzung, Bequemlichkeit oder Unbedarftheit Sicherheitsvorrichtungen oder -regeln umgeht, sie penetriert oder fatale Anwendungsfehler macht.

Die dazu entwickelten Angriffsmethoden werden als "social engineering" diskutiert. Sie reichen vom Durchstöbern von Abfällen nach interessanten Aufzeichnungen bis hin zu psychologisch geschickten Ausfragungen. Auch die Gestaltungen und Formulierungen von Spam-Mails und den Webseiten der Phisher sind geprägt von den "Überredungsstrategien" des social engineering. Dabei handelt es sich um klassische Methoden der Detektiv- und Spionagearbeit, die an die heutigen Bedürfnisse angepasst werden.

## Superwürmer und Trojaner

Datenspionage ist nicht nur mit Spam-Methoden oder einem aufwändigen Hardwareeinsatz möglich, sondern auch Software-basierend mit Malware, also mit schädlichen Programmen in verschiedenen Spielarten.

Viren als die älteste bekannte Form der Malware sind zumeist kleine Programmsequenzen, die sich in andere Programme einnisten, ihre ungewollte Wirkung ausführen und sich schließlich vermehren und verbreiten. Sie brauchen ein Trägermedium, in das sie sich einfügen. Dazu können sie Teile des Trägers überschreiben, damit ihre Existenz weniger auffällt, oder sich schlicht an eine Programmsequenz anschließen. Sie "leben" davon, dass ihr Wirt als unschädliches Programm vom Anwender oder seinem Computer aktiviert wird.

Die gefährdetste Phase, die Viren bevorzugt ausnutzen, ist der Boot-Vorgang, also das Starten eines Computers. Zuvor ist das Betriebssystem noch nicht aktiv, sondern muss erst geladen und ausgeführt werden.

Dazu müssen definierte physikalische Bereiche von Datenträgern gelesen werden, wobei es sich um Disketten, Festplatten und beliebige andere Datenträger handeln kann, die vom BIOS dazu angesprochen werden.

Im Gegensatz dazu treten Würmer bevorzugt als Anhänge an anderen Dateien auf. Sie nutzen nicht die Aktivität des Trägers aus, sondern die Einstellungen des Systems, wie mit bestimmten Dateien zu verfahren ist (Umgebungen). Ihre Wirte sind deshalb Dateien mit Formaten, die anwenderfreundlich und bequem von verbreiteten und großen Programmen verwendet werden und dabei bevorzugt im Zusammenhang mit elektronischen Nachrichten und Büroanwendungen.

Deshalb können Würmer umfangreichen Programmcode enthalten, weil sie sich durch ihr Erscheinungsbild tarnen und nicht durch die Eigenschaften des Wirts.

Ihre Funktionalitäten sind beliebig und vielfältig. Sie können weitere Funktionen aus dem Netz installieren, ihr Erscheinungsbild ändern und alle denkbaren Ereignisse steuern.

Trojaner schließlich bieten sich mit mit ihren Diensten und Funktionen an und verdecken dabei ihre schädlichen Eigenschaften, die sie unbemerkt ausführen. Sie müssen also eine begehrte Funktionalität haben, die den Anwender zu ihrem Einsatz reizt.

## IP-Würmer

Die Ur-Würmer verbreiteten sich ausschließlich als Anhänge zu anderen Dateien und dabei bevorzugt im Zusammenhang mit E-Mails. Sie nutzten in aller Regel die bequemen Runtime-Umgebungen der Browser (Java for Applications, activeX) oder von Office-Anwendungen aus (Visual Basic for Applications für Word und Excel aus dem Office-Paket von Microsoft), wobei sie entweder selbständig starten konnten oder vom Anwender unbedarft aktiviert werden mussten.

Dort nisten sie sich ein, ändern die Systemeinstellungen, verbreiten sich, laden weitere Programmteile aus dem Netz und entfalten die ihnen eingegebenen Aktivitäten.

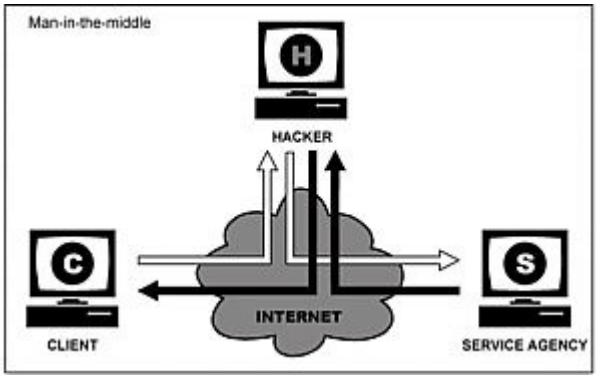
Dabei verwenden sie verschiedene Techniken zur Tarnung. Sie sind vereinzelt in der Lage, ihren Programmcode zu aktualisieren, ihr Erscheinungsbild zu ändern und sich immer wieder an aktualisierte Virenscanner und Firewalls anzupassen. Von einigen wurde bekannt, dass sie diese Schutzware gezielt angreifen und deaktivieren.

Eine neuere Variante sind IP-Würmer, die kein Trägermedium benötigen, sondern sich selbsttätig verbreiten und agieren können. Dazu detektieren sie voreingestellte oder zufällige Adressen im Internet auf der Suche nach einer aktiven Gegenstelle, die gleichzeitig bestimmte Sicherheitslücken aufweist, die von dem Wurm ausgenutzt werden können.

Findet er eine solche Adresse, dann nutzt er die Sicherheitslücke, setzt sich in dem angegriffenen System fest und führt die ihm einprogrammierten Funktionen aus. Die wichtigsten davon sind, wieder auf den „Horchposten“ zu gehen und sich weiter zu verbreiten.

Zu Seite 13:

## The Man in the Middle




Quelle: e.govt.nz/services/.../m-i-m.gif

### ... im Einsatz

Spionageaufgaben lassen sich aber nicht nur mit den angesprochenen Hardwarekomponenten ausführen, sondern grundsätzlich auch mit Programmen und deshalb auch mit Malware.

Wegen der Kontodaten des Opfers ist folgendes Szenario vorstellbar (es wird diskutiert, sein Vorhandensein behauptet, aber nicht belegt).

Das Opfer wird mit einem Wurm penetriert; dafür gibt es haufenweise Beweise. Der Wurm nistet sich ein und das heißt in aller Regel, dass er seine Aktivierungsparameter in der Registry oder anderen Systemdateien hinterlegt, Kommunikationskomponenten aus dem Internet lädt (besonders FTP-Server) und weitere Änderungen an den Systemeinstellungen und -programmen unternimmt.

Dann entfaltet er aber keine auffälligen Aktivitäten, sondern lauert und wartet. Bis der Anwender z.B. seine Homebanking-Software oder die dazu genutzte Internetseite aufruft.

Den Homebankingvorgang protokolliert der Wurm vollständig. Wenn der Anwender nach der Eingabe einer Transaktionsnummer einen Bezahlvorgang abschließen will, wird der Wurm aber besonders aktiv. Er blockiert den Return-Befehl (Absatzvorsprung), blockiert die Standard-Zugangsdaten zum Internet und zum Homebanking, öffnet eine besondere Spezifikation für den Internetzugang und übermittelt die von ihm protokollierten Kontodaten.

Der Angreifer muss jetzt handeln und die ausgeschnüffelten Daten missbrauchen. Der Anwender jedoch bekommt keine Vollzugsmeldung für seine Homebanking-Aktion und kann sich auch nicht mehr in das Internet einloggen, weil die Zugangsdaten vom Wurm gesperrt wurden.

Dieses Szenario lässt sich auf andere Situationen und Angriffsziele beliebig übertragen.

## The Man in the Middle

Im Anschluss an die Sicherheitsmaßnahmen der Banken, zum E-TAN-Verfahren zu wechseln und nur gesicherte https-Verbindungen zwischen der Bank und dem Kunden aufzubauen, gibt es nur zwei Methoden für ein erfolgreiches Phishing: Entweder man erlangt von den Bankkunden haufenweise TANs und erhöht damit die Wahrscheinlichkeit, dass eine darunter ist, die von der Bank auch angefordert wird, oder man agiert als "Man in the Middle".

Hierzu benötigt der Angreifer zunächst einmal die Kontozugangsdaten, die ihm sein Wurm beschafft hat. Darüber hinaus hat der Wurm z.B. die DNS-Tabelle im PC des Bankkunden abgeändert, so dass er beim Homebanking nicht mit der IP der Bank, sondern mit dem Angreifer verbunden wird.

Auf seinem Computer simuliert nun der Angreifer die Homebanking-Umgebung der Bank und nimmt seinerseits Kontakt zur Bank auf, um die von ihm gewollte Transaktion vorzubereiten.

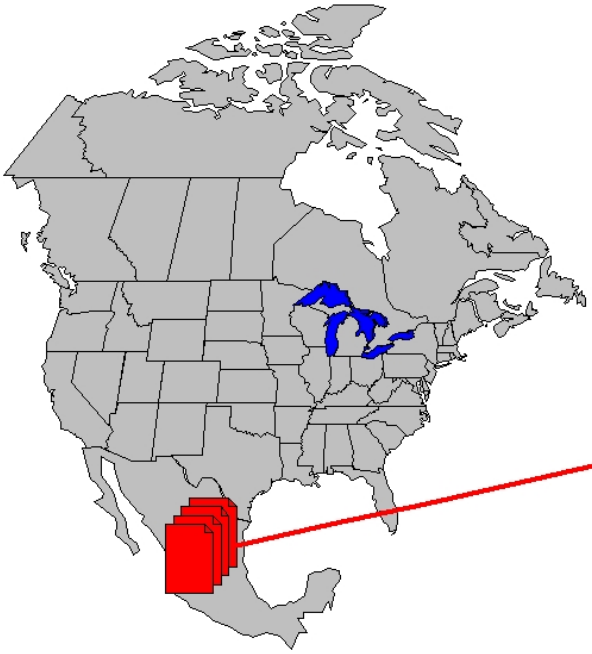
Während der Session vollzieht der Angreifer alle Bewegungen des Bankkunden nach und simuliert auf seinem Computer die Meldungen der Bank über Kontostände, Daueraufträge und andere Bestandsdaten.

In dem Moment, in dem der Bankkunde eine Transaktion durchführt, für die er eine TAN benötigt, ändert sich das Verhalten des Angreifers. Während er bislang alle Bewegungen des Bankkunden nachvollzogen und die Meldungen der Bank weitergegeben hat, führt er jetzt unbemerkt eine Überweisung auf ein von ihm bestimmtes Konto aus.

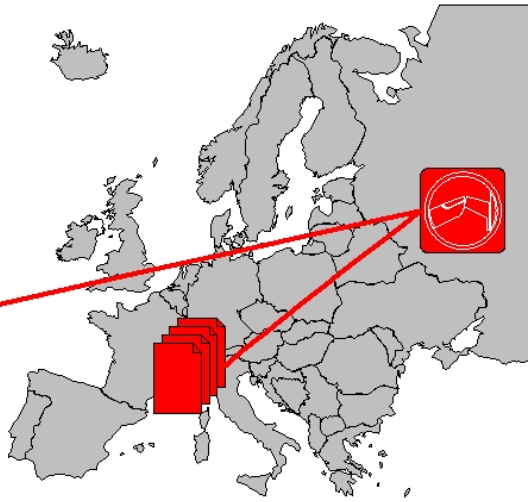
Die Bank meldet dem Angreifer die Position der TAN, die sie zur Legitimation benötigt und genau diese Anfrage reicht der Angreifer zum Bankkunden weiter. Der Bankkunde meint, die Legitimation beträfe seine, nur in der simulierten Umgebung stattfindende Überweisung, und übermittelt die angeforderte TAN. Diese gibt der Angreifer an die Bank weiter und löst damit seine Überweisung aus.

Das lässt sich beliebig fortsetzen je nach dem, wie gut und anpassungsfähig die Simulationsumgebung ist.

Phishing in Aktion



Phishing in Aktion
Vorbereitungen
Adressenlisten beschaffen



## Ablauf eines Phishing-Angriffs

### Vorbereitung des Angriffs

Nehmen wir an, dass die Phishing-Organisation in Osteuropa angesiedelt ist und am Schalter sitzt, also die Aktivitäten gestaltet. Jetzt ist sie noch inaktiv.

Nach den bekannten journalistischen Quellen ist davon auszugehen, dass die wesentlichen Phishing-Aktivitäten in Europa einschließlich Russland und Nordamerika und dort vor allem in den USA stattfinden. Darauf sollen sich die hier gezeigten Beispiele beschränken.

### Beschaffung von Adressen

Für eine vollständige Phishing-Aktion werden zwei Spam-Aktionen benötigt, die der Werbung von Finanzagenten und zur Täuschung von Bankkonteninhabern dienen. In der Anfangsphase sind wahrscheinlich die Finanzagenten noch direkt und im persönlichen Kontakt geworben worden. Seit Ende 2005 häufen sich jedoch die Spam-Mails, in denen Interessenten mit besten Verdienstmöglichkeiten bei geringer Arbeitszeit gelockt werden (konzentriertes Ansprechen einer Zielgruppe, Spear-Phishing).

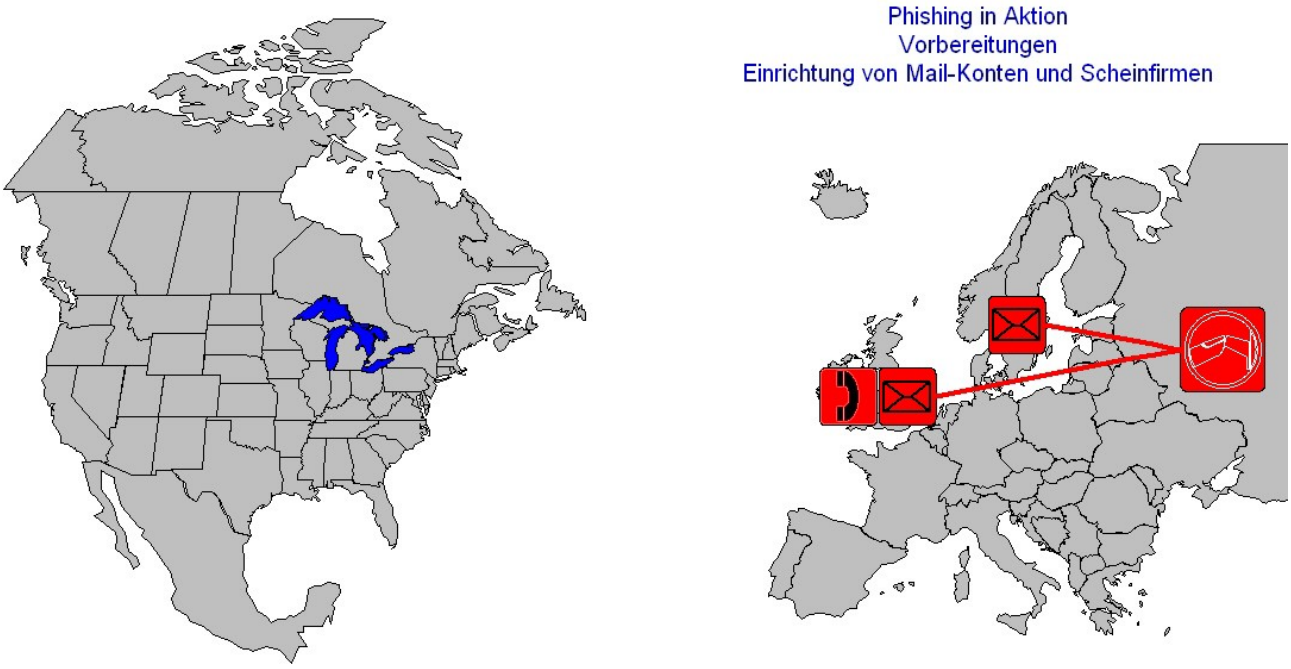
Für die Spam-Aktionen werden Adressenlisten benötigt, die möglichst viele "gute" Kontakte versprechen. Das bedeutet nicht nur, dass die Adressen wirklich bestehen, sondern möglichst auch zu solchen Leuten führen, die für den jeweiligen Zweck benötigt werden.

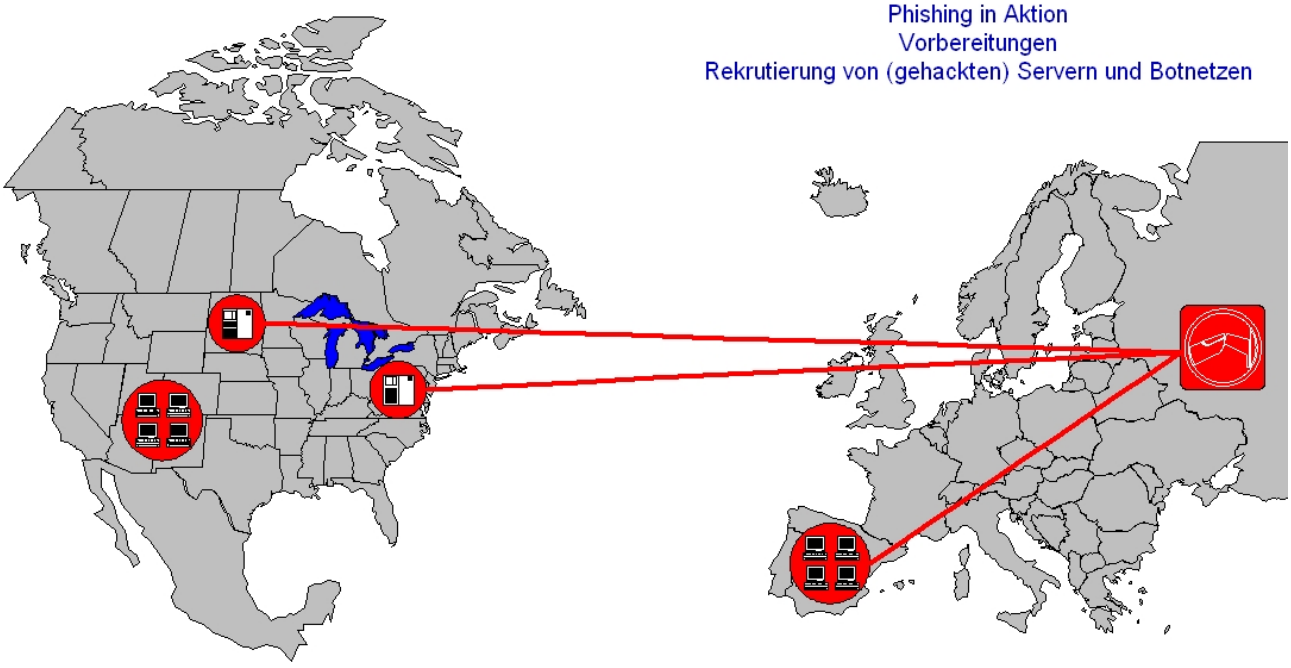
Es gibt mehrere Möglichkeiten, um an Adressen zu kommen. Entweder man durchsucht selber mit Suchrobotern das Internet nach E-Mail-Adressen oder man greift auf Sammlungen zurück, die entweder von kommerziellen Adressenhändlern oder von Hakkern als Kopien von Kundenverzeichnissen aus penetrierten Systemen verkauft oder veröffentlicht werden.

Auch Kontozugangs- und Kreditkartendaten sind im Internet frei oder gegen Entgelt erhältlich.

Die Adressenqualität - Erreichbarkeit und für den Werbezweck geneigt - ist zwar wichtig, fällt aber in der Bedeutung gegenüber dem Grundsatz "Masse statt Klasse" zurück. Beim professionellen Spamming, das sich gerne als "Direktmarketing" versteht und die Grenzen zwischen beiden verschwimmen lässt, gilt wegen der geringen Kosten, die beim gewerblichen Versand massenhafter E-Mails entstehen, der Grundsatz, dass es sich bereits lohnt, wenn ein Tausendstel Promille (0,0001 %) der Adressaten auf die Offerte reagiert.

Für das Phishing werden inzwischen durchweg oder überwiegend gehackte Systeme verwendet, so dass die Kosten für den Versand gar keine Rolle spielen. Deshalb sind die Adressenlisten die besten, die entweder ein gezieltes Publikum ansprechen oder einfach nur riesengroß sind.


Phishing in Aktion
Vorbereitungen
Einrichtung von Mail-Konten und Scheinfirmen


Phishing in Aktion
Vorbereitungen
Rekrutierung von (gehackten) Servern und Botnetzen

### Einrichtung von E-Mail-Konten und Scheinfirmen

Im Zusammenhang mit der Anwerbung von Finanzagenten ist ein gewisser stetiger Kontakt zwischen den Agenten und dem Auftraggeber nötig. Inzwischen sind nicht nur die Werbetexte erheblich professioneller geworden, sondern auch Meldungen dazu bekannt, dass regelrechte Anstellungsverträge mit komplexen Regelungswerken vereinbart werden, die einen durch und durch seriösen Anschein erwecken.

Für das Phishing gilt aber: Finanzagenten haben nur eine Funktion, sie sollen das ertrogene Geld weiterreichen.

Normalerweise reicht es deshalb, dass der Auftraggeber über irgendeine, kostenfreie oder seriös wirkende E-Mail-Adresse erreichbar ist und über sie an die Kontaktdaten des Finanzagenten kommt und ihn dadurch dazu veranlassen kann, den illegalen Gewinn zu transferieren.

Aufgrund der Veröffentlichungen in der Presse und in anderen Medien sind die potentiellen Opfer gewarnt und müssen die Legenden für die Aktivierung der Finanzagenten immer seriöser wirken.

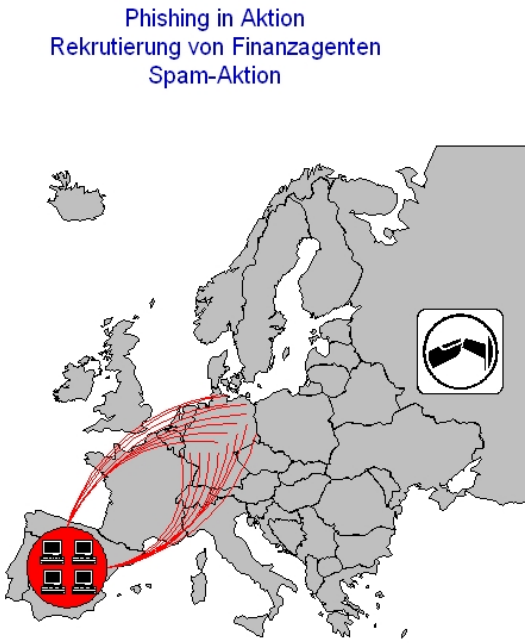
Ich habe deshalb die Vermutung, dass immer mehr auch vorübergehend Scheinfirmen eingerichtet werden, um dieses Ziel zu erreichen.

### Rekrutierung von gehackten Servern und Botnetzen

Für die Platzierung einer Website, die wie die Original-Seite einer Bank aussehen soll, brauchen die Phisher - jedenfalls vorübergehend - eine stabile Adresse auf einem Webserver. Diese Adresse soll nur kurze Zeit erreichbar sein und wird dann wieder aufgegeben, so dass es sich anbietet, keinen Serverdienst zu mieten, sondern diesen entweder selbst zu hacken oder sich von anderen beschaffen zu lassen.

Auch für die Anwerbung von Finanzagenten und die Täuschung der Bankkunden werden entweder Server mit einem Maildienst oder Botnetze benötigt, die für den massenhaften Versand von Spam eingesetzt werden sollen. Bei den Botnetzen handelt es sich um eine Vielzahl mit Malware infizierter PCs, die dadurch zentral ferngesteuert werden können.


Phishing in Aktion
Rekrutierung von Finanzagenten
Spam-Aktion


Phishing in Aktion
Rekrutierung von Finanzagenten
Spam-Aktion

## Rekrutierung von Finanzagenten.

### Spam-Aktion

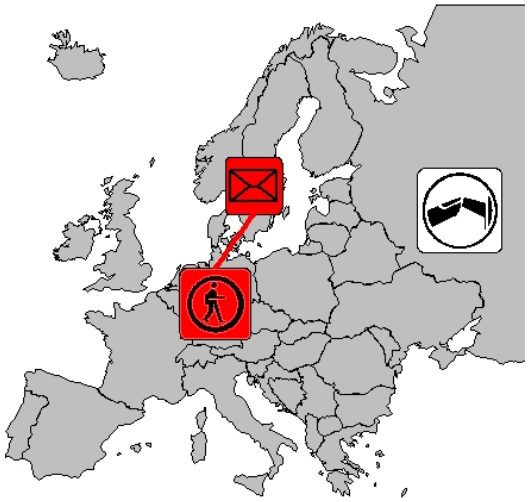
Zunächst gilt es, Finanzagenten zu werben. Diese sollen entweder ihre laufenden Girokonten zur Verfügung stellen oder neue Bankkonten einrichten, auf die dann die Gelder von den missbrauchten Konten überwiesen werden.

Die Aufgabe der Finanzagenten ist es dann, das Geld von ihrem Konto abzuheben, eine angemessene Provision für sich abzuziehen und den Restbetrag mittels eines Auslandszahlungsdienstes, z.B. Western Union, an ihre Auftraggeber zu übersenden.

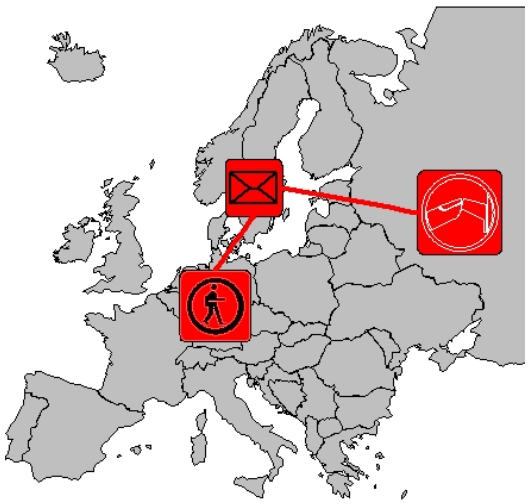
Nachdem die Phisher die vorgesehene Adressenliste und den Werbetext in das Botnetz geladen und dieses dann gestartet haben, können sie einfach abwarten. Das Botnetz überschwemmt die angegebenen Adressen mit einer Nachricht.

Jetzt kommt es auf die inhaltliche Qualität des Werbetextes an und darauf, ob sich genügend Interessenten melden.

Phishing in Aktion
Rekrutierung von Finanzagenten
Kontaktaufnahme



Phishing in Aktion
Rekrutierung von Finanzagenten
Verhandlungen

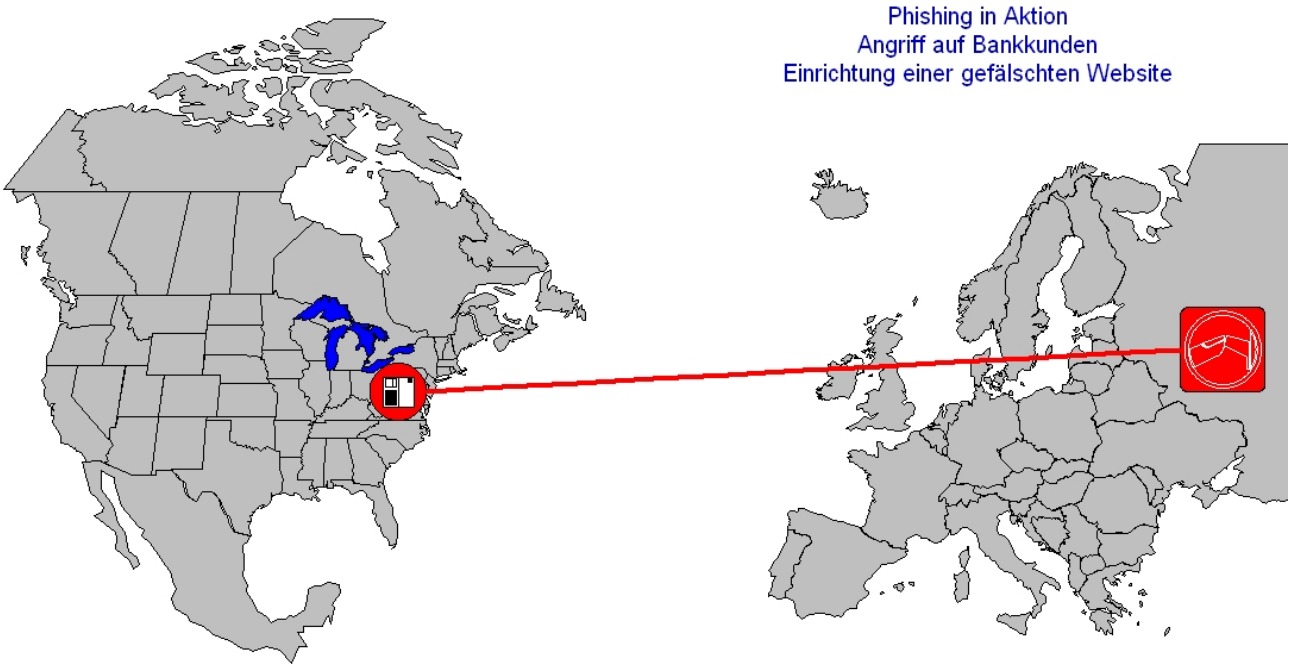


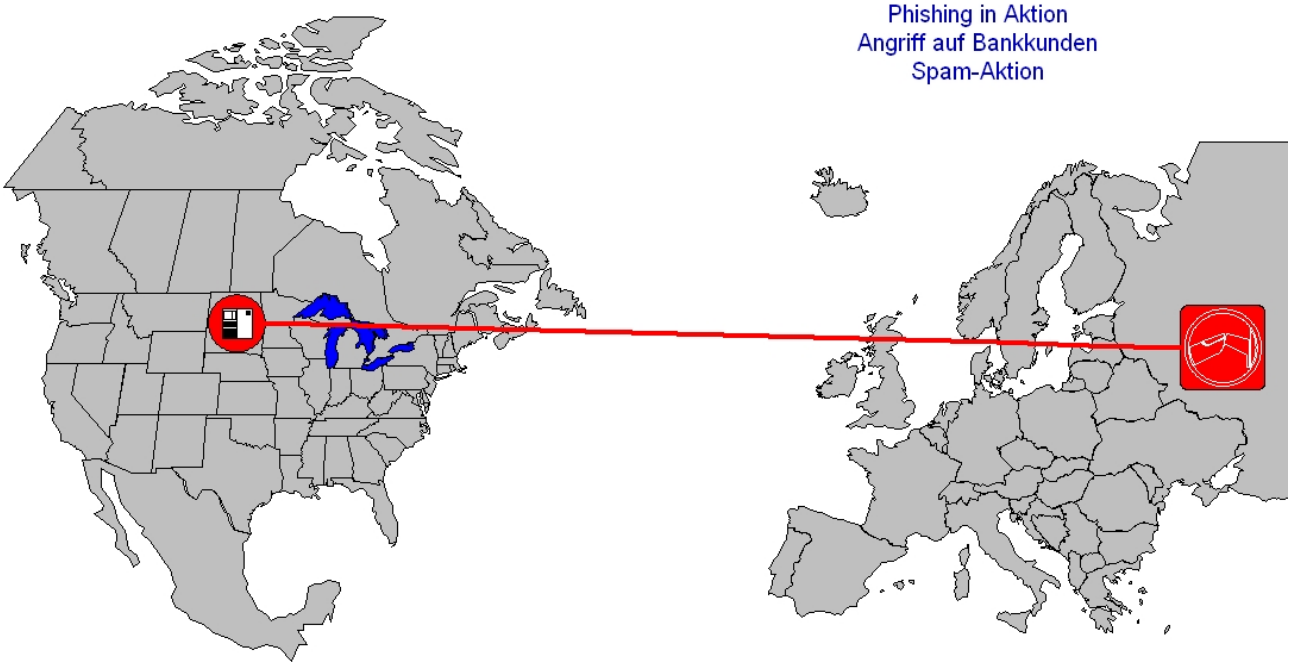
Das Botnetz hat seine Schuldigkeit getan. Es kann warten auf seinen nächsten Einsatz, wobei sich seine Struktur nach und nach ändern wird: Einzelne Anwender werden Anti-Viren-Programme einsetzen und ihre Systeme reinigen oder sich neue Rechner anschaffen, die zunächst einmal immun sind. Doch die Malware verbreitet sich weiter und neue Rechner werden in den Verbund des Botnetzes aufgenommen.

Der erste Interessent meldet sich bei den Phishern.

Jetzt kommt es darauf an, den Interessenten dazu zu bewegen, sich als Finanzagent zur Verfügung zu stellen. Die Phisher brauchen seine Bankverbindung und seine Bereitschaft, eingehende Gelder an sie weiter zu leiten.

Das beste Lockmittel der Phisher ist: Profit. Eine Entlohnung, die mit normaler Arbeit nicht zu erzielen ist, einfach dafür, sein Konto zur Verfügung zu stellen und eine Überweisung vorzunehmen.


Phishing in Aktion
Angriff auf Bankkunden
Einrichtung einer gefälschten Website


Phishing in Aktion
Angriff auf Bankkunden
Spam-Aktion

## Angriff auf Bankkunden

### Einrichtung einer gefälschten Website

Die Phisher wollen an die Konto- oder andere sensible Daten von Kontoinhabern gelangen. Sie müssen dazu gebracht werden, ihre Kontonummer, ihr Kennwort (PIN) und ihre Transaktionsnummern zu offenbaren (TAN).

Die beste Zeit dafür beginnt jeden Freitag Mittag. Die Banken sind geschlossen, die Bankkunden erledigen ihre Bankgeschäfte von zuhause aus und haben erst wieder am Montag die Gelegenheit, Auffälligkeiten und Störungen mit ihrer Bank anzusprechen.

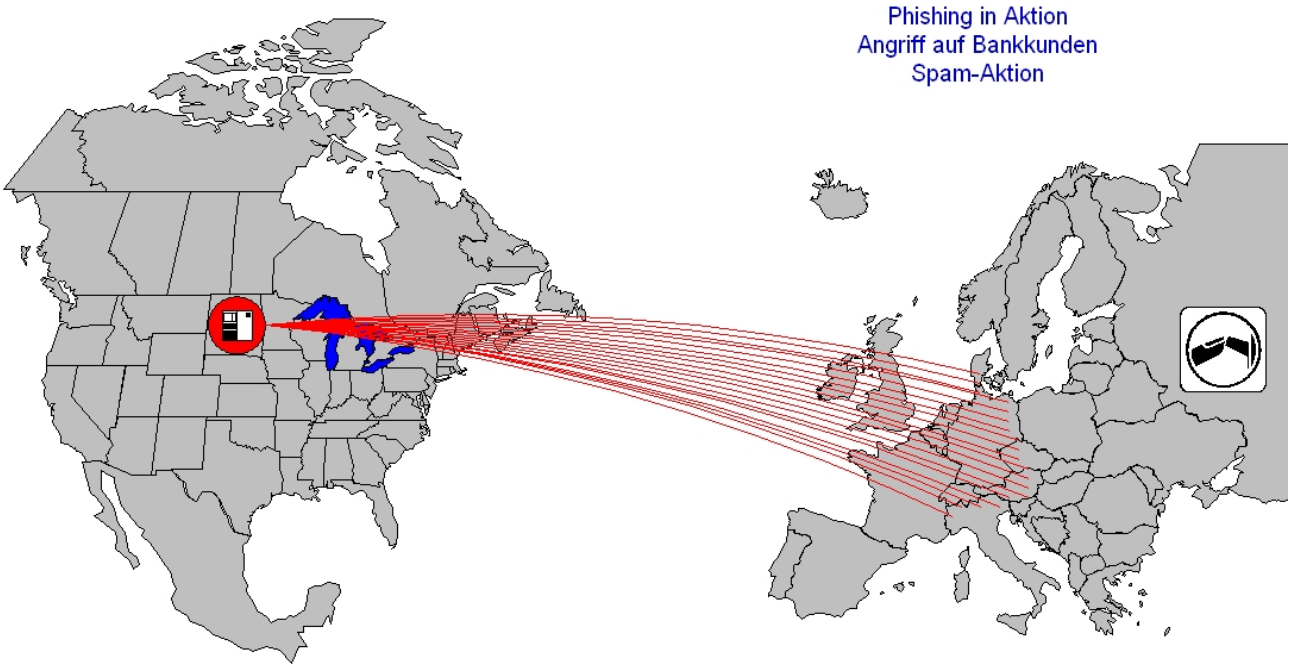
Die Phisher haben deshalb ein Wochenende lang Zeit, ihre Aktivitäten zu entfalten.

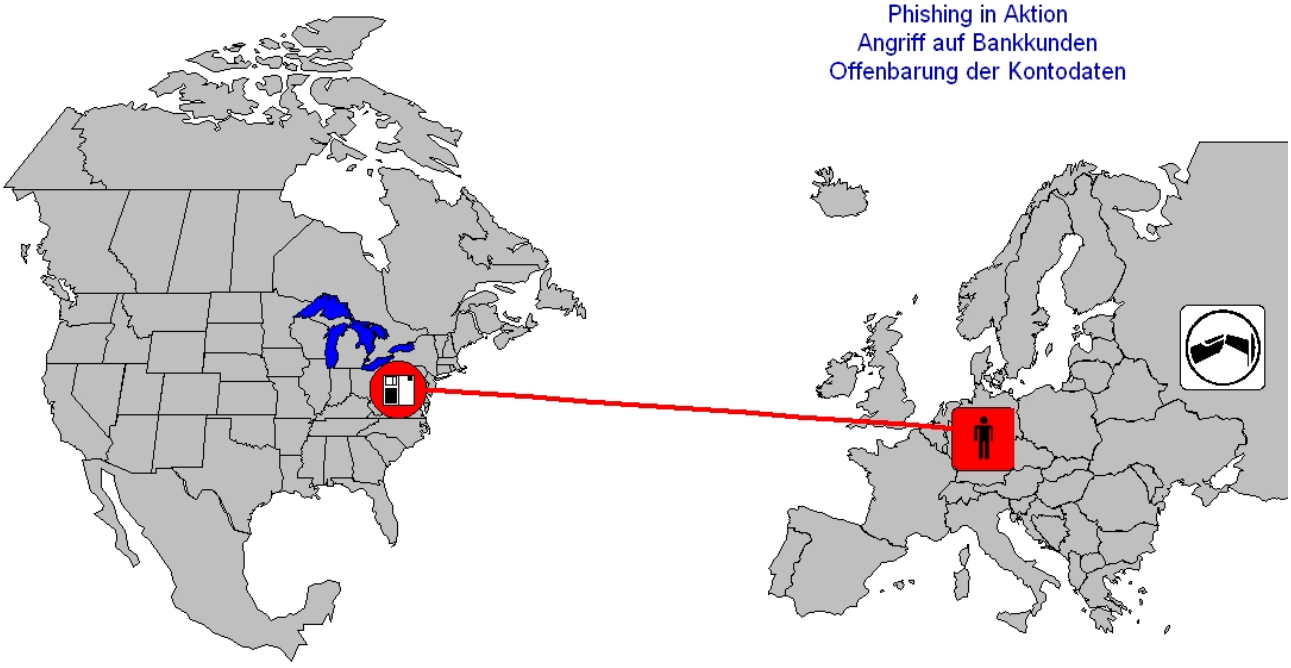
Beim alten TAN-Verfahren reichte es, sich **eine** TAN zu verschaffen, weil der Bankkunde bestimmen konnte, welche Nummer er aus seiner Liste auswählt. Im neueren eTAN-Verfahren gibt die Bank vor, welche Nummer an welcher Position sie genannt bekommen will. Die Phisher müssen deshalb versuchen, so viele TANs zu bekommen wie möglich. Nur so können sie erwarten, dass eine der bekannten Transaktionsnummern die ist, die die Bank auch wirklich im Homebanking-Verfahren anfordert.

Die gefälschte Website muss deshalb überzeugen und so perfekt sein, dass der arglose Bankkunde seine intimen Kenntnisse übermittelt. In einem Fall soll sich ein Kunde erbost an seine Bank gewandt und eine neue TAN-Liste gefordert haben, nachdem er die Hälfte seiner Nummern auf diese Weise weitergegeben hatte.

### Spam-Aktion

Jetzt muss sich erweisen, wie gut die Vorbereitungen waren. Die zweite Spam-Aktion wird gestartet. Wichtig dabei ist, dass ein anderer Mail-Server benutzt wird als bei der ersten Aktion (wenn auch dabei ein gehackter Server und kein Botnetz benutzt wurde), weil der "alte" längst als "Junk-Sender" bekannt ist und deshalb vielfach ignoriert wird.


Phishing in Aktion
Angriff auf Bankkunden
Spam-Aktion

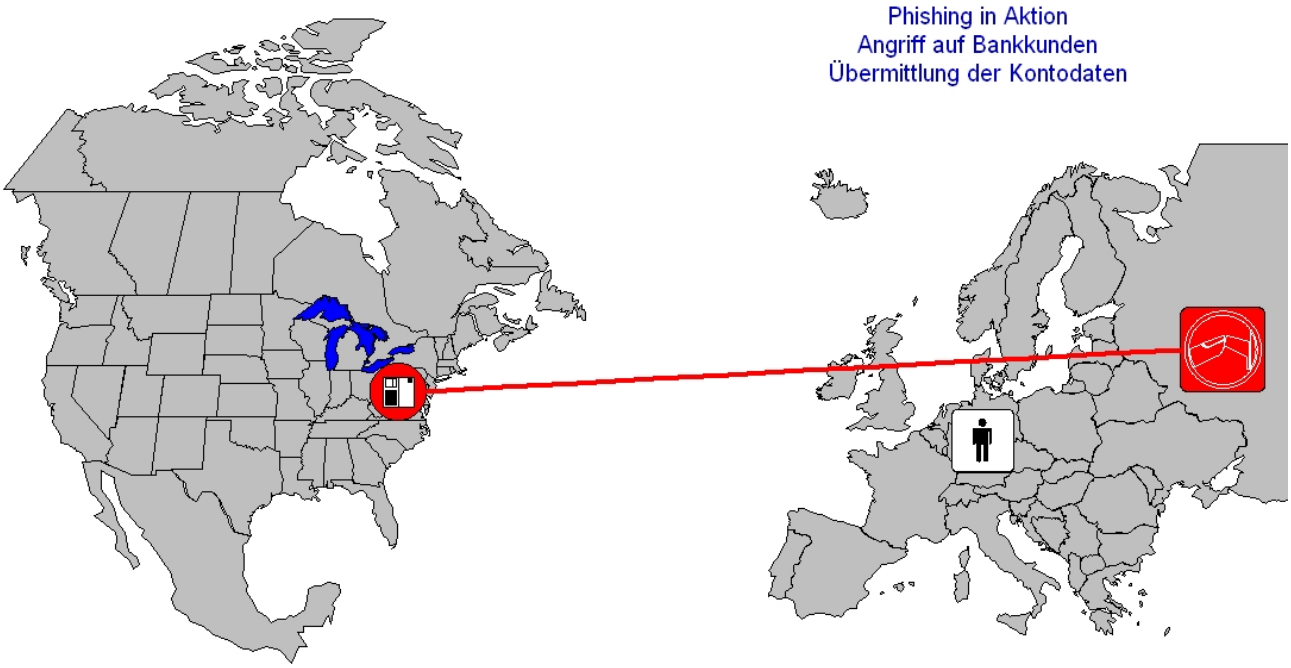

Phishing in Aktion
Angriff auf Bankkunden
Offenbarung der Kontodaten

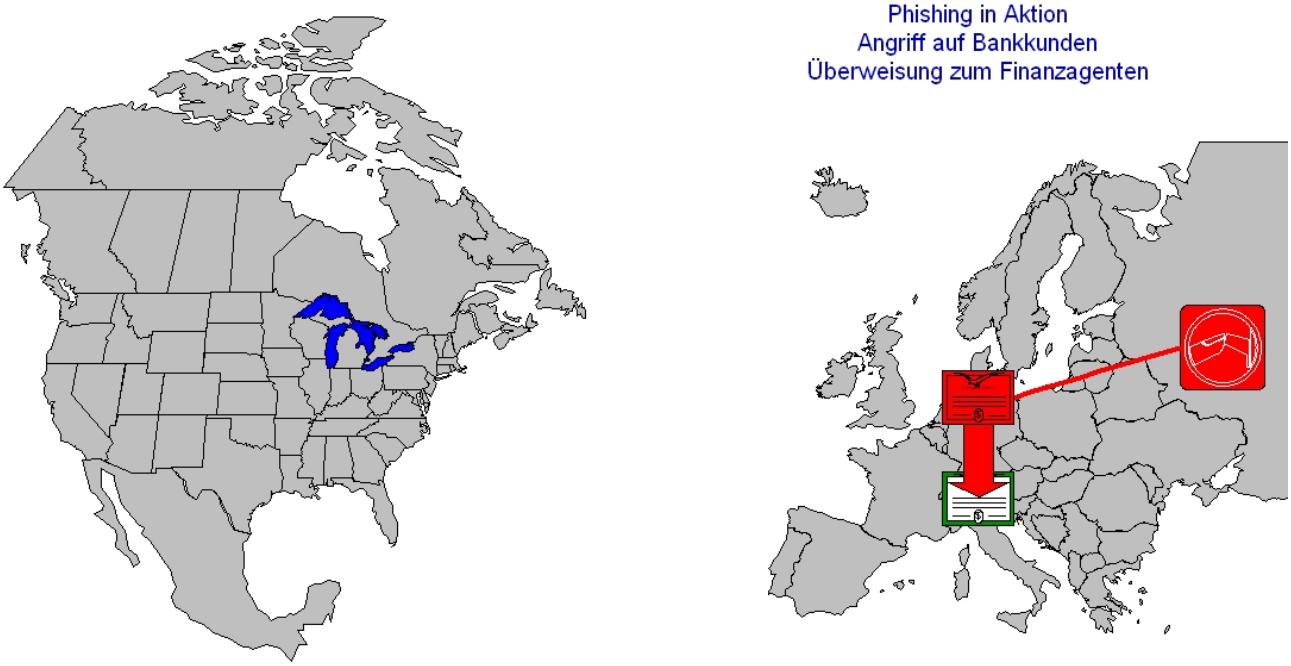
Die neuesten Adressenlisten und ein grammatisch und formal immer besserer Werbetext werden verwendet.

Wieder einmal müssen die Phisher einfach nur warten. Der korrupte Server versendet massenhaft E-Mails und ist dadurch "verbrannt". Das haben schon viele seriöse Internetdienste zu spüren bekommen, weil sie missbraucht wurden und wegen dieses Missbrauchs in schwarzen Listen als Spammer oder Phisher gelangt sind und von Zugangsprovidern gesperrt wurden.

Es folgt die erste entscheidende Aktion, auf die die Phisher keinen Einfluss nehmen können. Der Bankkunde offenbart seine Kontozugangsdaten, nachdem er die präparierte Website aufgerufen hat.

Die Vorbereitungen zur Täuschung der Bankkunden waren erfolgreich.


Phishing in Aktion
Angriff auf Bankkunden
Übermittlung der Kontodaten


Phishing in Aktion
Angriff auf Bankkunden
Überweisung zum Finanzagenten

Das Warten hat ein Ende. Der korrupte Server sendet die ausgehorchten Kontodaten (oder sie müssen von den Phishern erst noch abgeholt werden).

Jetzt kann die eigentlich geplante kriminelle Aktion beginnen - das Abräumen der Bankkonten.

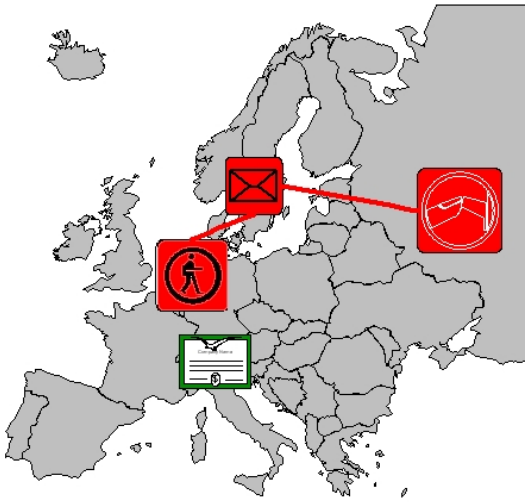
## Angriff auf Bankkunden.

### Verwendung der Kontodaten

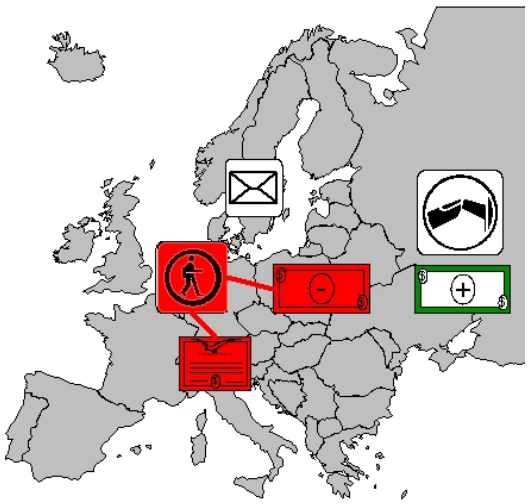
Die Phisher verwenden nun die Kontozugangsdaten, orientieren sich über das Guthaben und räumen das Konto ab, wozu sie die ausgespähten Transaktionsnummern verwenden (TAN).

Das Geld wird auf das Konto des Finanzagenten überwiesen. Die Summe bleibt immer schön innerhalb der Grenzen des Geldwäschegesetzes, damit die Transaktion nicht zu früh auffällt.

Phishing in Aktion
Finanztransaktion
Aktivierung des Finanzagenten



Phishing in Aktion
Finanztransaktion
Kontobelastung und Einzahlung bei Western Union



## Aktivierung des Finanzagenten

Die Phisher müssen ein letztes Mal aktiv werden. Sie beauftragen den Finanzagenten mit der Transaktion.

Der Finanzagent wird aktiv, hebt von seinem Konto das eingegangene Geld ab, nach Abzug seiner angemessenen Vergütung, und überweist den Betrag per Auslandsdienst zum Empfänger (meistens per Western Union).

Aufgrund der Vereinbarungen über den Lastschriftverkehr im deutschen Kreditwesen wird der missbräuchlich angewiesene Betrag aber wieder dem Konto des Finanzagenten belastet. Verfügt er über genügend Guthaben oder eine ausreichende Kreditlinie, so bleibt er auf dem Schaden sitzen. Ist das nicht der Fall, so trägt seine Bank den Schaden.

Darüber hinaus hat er sich wegen Geldwäsche strafbar gemacht, wie verschiedene bekannt gewordene Verurteilungen belegen.

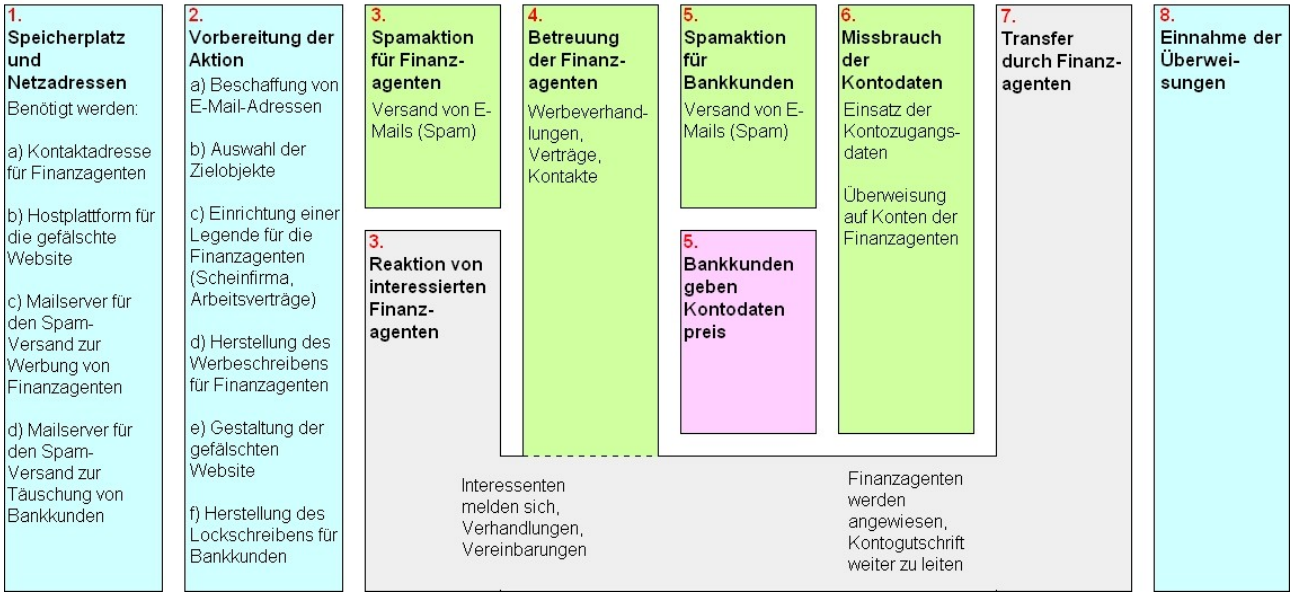
Wenn man es insgesamt betrachtet ist es meistens der "gierige" Finanzagent, der die Opferlasten eines Phishing-Angriffs trägt. Er handelt in der Öffentlichkeit und ist für die Strafverfolgungsbehörden greifbar.

Das angewiesene Geld wird schließlich für die Filiale im Ausland gutgeschrieben.

Das vom Finanzagenten angewiesene Geld steht den Phishern dann zur Verfügung. Die Hintermänner sind nicht öffentlich in Erscheinung getreten, können nur schwer oder gar nicht ermittelt werden und brauchen deshalb auch keine rechte Strafverfolgung befürchten.

Der einzige, der bestraft werden kann ist der Finanzagent.

Die Arbeitsschritte beim Phishing



## Die Arbeitsschritte beim Phishing

Erhebliche Teile einer Phishing-Aktion bleiben von der Öffentlichkeit unbemerkt (blaue Säulen) und dienen besonders der logistischen Vorbereitung. Der erste Arbeitsschritt dient zu Beschaffung der benötigten Technik, wobei klassische Hackermethoden zum Einsatz kommen. Vermutlich kommt es in diesem Bereich zu einer regen Zusammenarbeit zwischen der Hakker- und der Phisherszene.

Die Vorbereitung der Aktion ist die eigentlich typische Phase für das Phishing. Aufbauend auf den Erfahrungen der Spammer müssen wirksame und überzeugende Werbetexte sowie eine täuschend echt wirkende Website erstellt werden. Die zunehmende Professionalität ihrer Schreiben und ihrer Auftritte zeigen, dass sie nicht nur viel dazu gelernt haben, sondern dass sie auch sehr viel Aufwand damit betreiben, den richtigen Sprachstil zu treffen, korrekte Übersetzungen zu fertigen und ein wirksames Webdesign zu schaffen.

Zum Einsatz kommen alle Erfahrungen, die im Zusammenhang mit der Werbewirtschaft und dem Social Engineering entwickelt wurden, um die Finanzagenten zu werben und die Kontoninhaber zur Offenbarung ihrer geheimen Daten zu veranlassen.

Die "grünen" Handlungsphasen müssen in der Öffentlichkeit ausgeführt werden, wobei die Phisher vermeiden, identifiziert und angreifbar zu werden. Sie nutzen alle Manipulationsmöglichkeiten, die die Internettechnik bietet, und schaffen es damit, fast ganz unsichtbar zu bleiben.

Den geringsten Handlungsanteil haben die ausgeforschten Bankkunden selber, die einmal, gezielt und kurzfristig dazu gebracht werden, ihre Kontodaten zu offenbaren. Den Rest erledigen die Phisher (Kontomissbrauch) und die Finanzagenten.

Der Markt für die Werbung von Finanzagenten scheint nahezu leergefischt zu sein. Es häufen sich die Hinweise, dass zwar massenhaft ungebrauchte Kontozugangsdaten der Szene bekannt sind, aber die Absatzwege mittels Finanzagenten nicht mehr funktionieren. Insoweit haben die Strafverfolgung und die Berichterstattung über sie gut funktioniert.

## Strafbarkeit in Deutschland

Einzelne Handlungsschritte einer Phishing-Aktion sind auch im deutschen Strafrecht strafbewehrt. Die Strafverfolgung wird jedoch dadurch erschwert und meistens ausgeschlossen, dass die Handlungen im Ausland begangen werden.

Das gilt zunächst für das Hacking von Servern und die Errichtung von Botnetzen, die häufig mit einem Ausspähen von Daten (§ 202a StGB) und immer mit einer Datenveränderung verbunden sind (§ 303a StGB), die sich zu einer Computersabotage qualifizieren kann (§ 303b StGB).

Die Spammingaktionen erfolgen in aller Regel so, dass die Absenderangaben in den Headern der Nachrichten verfälscht werden. Nach der jüngeren Diskussion erfüllt dies den Tatbestand der Fälschung beweiserheblicher Daten (§ 269 StGB).

Der "Nachbau" von Bankseiten mit den grafischen Gestaltungselementen der Originale verstößt gegen die Urheber- und Markenrechte dieser Unternehmen (Markengesetz, Urhebergesetz).

Die beiden Spamming-Aktionen stellen im übrigen Vorbereitungshandlungen zur Anstiftung zur Geldwäsche (§ 261 StGB) wegen der Finanzagenten und zu einem späteren Computerbetrug (§ 263a StGB) dar, sind also nicht für sich alleine strafbar.

Der Missbrauch der Kontodaten ist verbunden mit einem Computerbetrug. Die übrigen Computerstraftaten - Ausspähen und Datenveränderung - scheitern in aller Regel daran, dass die Kontodaten "ungeschützt" herausgegeben werden und der Phisher keine Kontodaten neben der Transaktion verändert.

Die Weiterleitung des missbräuchlich erlangten Geldes durch den Finanzagenten ist nach gefestigter Rechtsprechung eine Geldwäsche, wobei unterschiedliche Meinungen darüber bestehen, ob der Finanzagent als Täter oder Beihilfetäter handelt.

## Phishing und Strategien zur Geldwäsche

Aus den Erfahrungen mit Phishing-Aktionen wissen wir, dass es zwei grundlegend unterschiedliche Kontaktversuche gibt. Der eine richtet sich an den Bankkunden mit dem Ziel, dessen Kontozugangsdaten auszuspähen. Der andere geht ihm meist voraus. Mit ihm sollen Finanzagenten geworben werden, die das ertrogene Geld zum Täter transferieren.

Für die "Pflege" der Finanzagenten ist ein gewisser Aufwand nötig, der es gleichzeitig erforderlich macht, dass der Kontakt vorübergehend stabil, unverdächtig und als Dialog ausgeführt werden kann.

Unter diesen Voraussetzungen ist es wahrscheinlicher, gesicherte Aussagen aus solchen E-Mails abzuleiten, die sich der Werbung von Agenten widmen.

Zur Sicherung eines "Absatzweges" gibt es mehrere Möglichkeiten. In der Anfangsphase haben die Phisher versucht, das Geld von den gehackten Konten direkt ins Ausland zu überweisen. Sie sind wahrscheinlich meistens dabei gescheitert, weil die Beträge entweder nach Maßgabe der Geldwäschevorschriften oder wegen ihrer ungewöhnlichen Überweisungsziele aufgefallen sind und storniert wurden.

Beim Einsatz von Finanzagenten sind die Phisher auf deren guten Glauben angewiesen. Aufgrund der restriktiven und öffentlich berichteten Rechtsprechung, die sowohl eine Rückbelastung gegen das Konto des Finanzagenten wie auch dessen Verurteilung wegen Geldwäsche zulässt, dürfte der Markt für Finanzagenten zusammen gebrochen sein.

Die Täter sind aber nicht zwingend darauf angewiesen, Werte in Form von Geld zu erlangen. Werthaltig sind auch Warensendungen, die von Mittelsmännern weitergeschickt werden.

In den weiteren Entwicklungsstufen dürften auch "Drops" zum Einsatz kommen, also sichere Bankkonten und andere Depots, die als Zwischenläger dienen.

Wenn die Täter auf stabilen sozialen und kulturellen Gruppenbeziehungen aufbauen können, dann können auch Transfers nach dem Vorbild der Hawala entwickelt werden [6].

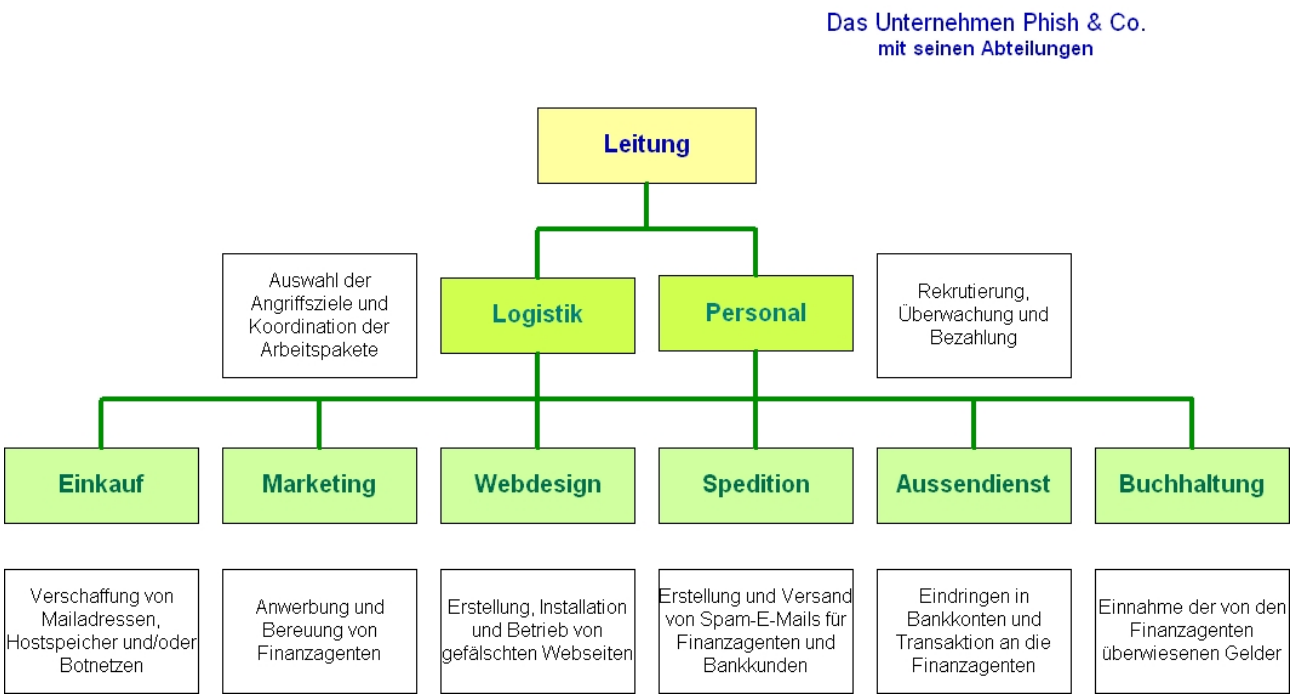
Dabei werden gegenseitige Forderungen privat verrechnet und von den Angehörigen der Gemeinschaft an verschiedenen Orten eingenommen und wieder ausgekehrt. Die Logik dieses Systems erinnert an die Praxis der norditalienischen Kaufleute im Mittelalter, die ebenfalls ein gegenseitiges Verrechnungssystem entwickelten, auf dem das bürgerlich-rechtliche Institut der Anweisung beruht.

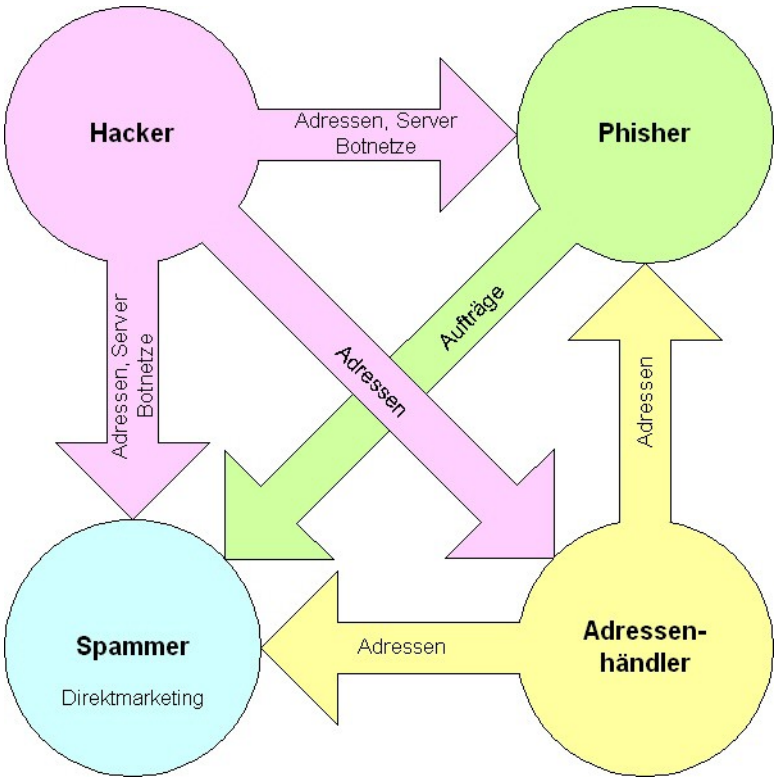
Das Verrechnungssystem lässt sich mit den Methoden der Geldwäsche noch weiter verfeinern. Nötig sind dazu Partner- oder Scheinfirmen mit Niederlassungen in verschiedenen Ländern, die ihre Forderungen mit Hilfe von Rechnungen und ihre kaufmännische Verbuchung umverteilen.

Denkbar sind auch internettypische Spielarten von Drops, bei denen entweder Bezahlsysteme ausgenutzt werden oder Scheinkonten in gehackten Systemen von Banken, Warenhäusern oder anderen Unternehmen verwendet werden. Besonders interessant könnten solche Unternehmen sein, die Niederlassungen in verschiedenen Ländern und gleichzeitig ein umfangreiches Buchungsaufkommen haben, so dass "geschleuste" Transaktionen unbemerkt bleiben könnten.

Auch die angesprochenen neuen Bezahlsysteme könnten genutzt werden. Das Beispiel "click and buy" zeigt, dass sie sich von reinen Inkassostellen wandeln zu Bankinstituten, die auch Debitkonten verwalten, also nicht nur Forderungen sammeln, einziehen und gebündelt überweisen, sondern auch Guthabenkonten führen.

6 Thomas **Pany**, Auf der Jagd nach den Schätzen von Terror, Inc., Telepolis 18.03.2004


Das Unternehmen Phish & Co.
mit seinen Abteilungen
Leitung
Auswahl der Angriffsziele und Koordination der Arbeitspakete
Logistik
Personal
Rekrutierung, Überwachung und Bezahlung
Einkauf
Marketing
Webdesign
Spedition
Aussendienst
Buchhaltung
Verschaffung von Mailadressen, Hostspeicher und/oder Botnetzen
Anwerbung und Bereuung von Finanzagenten
Erstellung, Installation und Betrieb von gefälschten Webseiten
Erstellung und Versand von Spam-E-Mails für Finanzagenten und Bankkunden
Eindringen in Bankkonten und Transaktion an die Finanzagenten
Einnahme der von den Finanzagenten überwiesenen Gelder


Hacker
Adressen, Server Botnetze
Phisher
Adressen, Server Botnetze
Aufträge
Adressen
Adressen
Spammer
Direktmarketing
Adressen
Adressen-händler

## Das Unternehmen Phish & Co.

Es gibt Hinweise darauf, dass Phishing-Organisationen arbeitsteilig aufgestellt sind und ihre einzelnen Abteilungen unabhängig voneinander arbeiten. Dadurch wirken sie wie moderne Wirtschaftsunternehmen mit hochgradig spezialisierten Mitarbeitern, deren Hinterleute zwar die Aktionen koordinieren, aber völlig unerkannt und verdeckt bleiben können.

Das Phänomen "Phishing" ist deshalb ein anschauliches Beispiel dafür, wie sich die moderne Kriminalität aufstellt, organisiert und alle Möglichkeiten der Technik und des Marketings nutzt.

## Zusammenarbeit der Szenen

An dieser Stelle sollen ein paar Vermutungen angestellt werden, für die es zwar Hinweise, aber keine gerichtsfesten Beweise gibt. Sie pauschalieren und betreffen nur einen Teil der Hacker und der Werbewirtschaft.

Das Spamming hat seinen Ursprung im Direktmarketing und nutzt einen Teil seiner Methoden. Es sind Unternehmen bekannt geworden, die sich im offiziellen Werbegeschäft betätigen und gelegentlich mit Spam-Aktionen auffallen. Die eingesetzte Technik ist kostengünstig zu betreiben und wird noch billiger, wenn man mit illegalen Methoden arbeitet und die verwendeten Systeme hackt und korrumpiert.

Beim Direktmarketing ist es besonders wichtig, über "gute Adressen" zu verfügen, um die Werbung gezielt und wirksam einsetzen zu können. Insoweit gibt es einen Zusammenhang mit dem Markt der gewerblichen Adressenhändler, bei denen man nach sozialem Status und Neigungen ausgewählte Adressen kaufen kann.

Im Zusammenhang mit dem Spamming hat sich der Adressenhandel gewandelt, weil es in allererster Linie darauf ankommt, erreichbare Adressen zu verwenden, ohne dass es besonders auf die Bildung, das Vermögen oder die Interessen der Adressaten ankommt. Angesichts der kostengünstigen Versendetechnik zählt Masse statt Klasse.

Einer der Zulieferer der Adressen ist die Hackerszene, die die korrupte Technik und Adressenbestände von Banken und Handelsunternehmen liefert. Ergänzt werden die Adressenbestände durch automatische Suchläufe im Internet, in Foren und Chats.

Es gibt Hinweise auf eine enge Zusammenarbeit zwischen Spammern und Hackern, bei der die Hacker richtig Geld verdienen [7].

Auf den Erfahrungen und "Handelswaren" der Hacker, Spammer und Adressenhändler setzen die Phisher auf. Ihre Marketingmethoden entstammen aus den Erfahrungen der Spammer, so dass eine Zusammenarbeit zwischen beiden Szenen nahe liegt. Womöglich werden einzelne Spam-Aktionen der Phisher gar nicht von ihnen selber durchgeführt, sondern sind Auftragsarbeiten von Spammern.

Die Hacker bedienen sich vereinzelt krimineller Methoden, sind aber eine heterogene Szene mit unterschiedlichen Moralvorstellungen. Das ist bei den Phishers anders. Sie organisieren sich ausnahmslos mit dem Zweck, Straftaten zu begehen.

7 Alfred **Krüger**, Kampf gegen Windmühlen. Herkömmliche Strategien versagen bei der Spambekämpfung, Telepolis 13.12.2006

## Fachworte

In der Phisher-Szene haben sich Fachbegriffe entwickelt (aus: tecchannel Compact 1/2007, S. 173).

**CCV2:** Eine komplette Kreditkarteninformation. Der Begriff bezieht sich auf die Prüfziffer der Karte, die meist auf der Rückseite abgedruckt ist.

**Dump:** Kompletter Satz gefälschter Kreditkarten.

**Drop:** ein sicherer Ort, etwa ein Lieferplatz für mit gestohlenem Geld bestellte Güter oder ein sicheres Bankkonto.

**Mule** oder **Mule-Account:** Sicheres Bankkonto, auf dem sich Geld zwischenlagern lässt. Die Accounts müssen vertrauenswürdig wirken, indem sie etwa bereits längere Zeit existieren und aktiv genutzt werden.

**Ripper:** Ein enttarnter Angestellter einer Sicherheitsfirma oder einer Behörde. Alternativ auch ein Schwindler, der die angebotene Ware nicht liefert oder gelieferte Ware nicht bezahlt.

**Skimmer:** Scanner, der die Informationen aus dem Magnetstreifen von EC- oder Kreditkarten ausliest, beispielsweise als Aufsatz für einen Geldautomaten.

## Journalistische Quellen

Über die Möglichkeiten im Internet Adressenbestände zu erhalten und gehackte Computer zu mieten, hat zuletzt Moritz Jäger sehr anschaulich berichtet [8].

Er beschreibt, dass sich zahlreiche Onlinebörsen, bevorzugt Forensysteme, entwickelt hätten, in denen der "zahlungswillige Käufer nahezu alle illegalen Dienstleistungen erhalten (kann), die das Internet bietet". Sie reichen von kompletten Personendaten über Kreditkartendaten bis hin zu Geräten, mit denen gefälschte Ausweise und Karten hergestellt werden können.

Dazu gehören auch "Drops", also sichere, möglichst langjährig bestehende Bankkonten, auf denen das ertrogene Geld zwischengelagert werden kann, und Lieferadressen für Warenbestellungen. Zusätzlich werden auch Treuhanddienste für die sichere Abwicklung von Waren-Geld-Transaktionen angeboten.

Zum Angebot gehören auch alle Spielarten der Malware (Viren, Würmer, Trojaner, Keylogger) einschließlich sechsmonatigen Support, wenn gewünscht. Ihre Programmierung kann so ausgerichtet sein, dass sie besonders auf TANs reagieren und zum Beispiel melden, dass die eingegebene TAN bereits verbraucht ist und der Kunde bitte eine andere verwenden möge.

Die von Jäger anhand von Screenshots gezeigten Foren schotten sich in aller Regel ab und lassen nur zugelassene Mitglieder in den tiefen Bereich des Forums.

Er weist auch darauf hin, dass in den Subszenen bevorzugt als Zahlungssysteme Micro-payment nach dem Muster von E-Gold (Verrechnungseinheit: Edelmetall) benutzt werden, deren Betreiber auf den Karibikinseln vor dem Zugriff der Strafverfolgungsbehörden sicher sind.

8 Moritz Jäger, Das Netz der Phisher: Wie Online-Betrüger arbeiten, tecchannel 20.09.2006

Über die Zusammenarbeit der Spammer, Hacker und Virenschreiber hat die c't wiederholt berichtet [9].

9 Holger Bleich,Trojaner-Sümpfe. DDoS- und Spam-Attacken gegen Bezahlung, c't 1/05, Seite 43
Ferngesteuerte Spam-Armeen. Nachgewiesen: Virenschreiber lieferten Spam-Infrastruktur, c't 5/04, Seite 18

Stellenangebot: Arbeitswillige, zuverlässige, motivierte und leistungsfähige Mitarbeiter gesucht

**WOWOWO® 2006** – Shopping Over The World For Everyone

Ihre grenzenlosen Möglichkeiten beim Online-Shopping in jedem Land der Welt mit unserer Hilfe

Haben Sie einen Wunsch eine interessante Tätigkeit, als Nebenjob, von Zuhause zu tätigen und dafür auch einen guten Lohn zu bekommen?
Mit WOWOWO® 2006 haben Sie nun eine solche Möglichkeit!

Seit unserer Gründung im Jahre 2004 bieten wir im Bereich Internet-Shopping sichere und erfolgreiche Dienste für Menschen aus der ganzen Welt an.

Wir haben uns darauf spezialisiert den Menschen aus verschiedensten Ländern die Möglichkeit zu geben, in den Ländern ihre Bestellungen vorzunehmen, in denen es normalerweise aus verschiedensten Gründen unmöglich wäre. Viele Online-Shops verschicken aus eigenen Ansichten die Waren nicht ins Ausland, oft auch aus politischen Gründen. Vor allem sind hier die Länder benachteiligt, die in die EU nicht eingehen. Durch uns hat jeder Mensch, nach Wunsch, in jedem Land der Welt Waren online zu bestellen und sie auch preiswert und schnell zu bekommen.

Zurzeit beträgt unser deutsches Partnerportal (www.wowowo.de) über 800 Online-Shops aus Deutschland, in denen nun jeder durch uns die Möglichkeit dazu hat. Zu unseren Kundenkreis gehören nicht nur Menschen, sondern auch verschiedene Firmen.

Da wir unseren Hauptsitz in Portugal haben, und unsere Geschäfte und Bestellungen auch von hier aus vornehmen, brauchen wir Mitarbeiter in verschiedensten Ländern der Welt, um die Warenlieferung an die Kunden zu ermöglichen. In letzter Zeit hatten wir viele Bestellungen in den Online-Shops aus Deutschland, deshalb suchen wir nun in Deutschland zusätzliches Personal.

Wir bieten mehrere freie Stellen als Order-Controller an.

Zu Ihren Aufgaben wird es zählen die bestellten Waren unserer Klienten zu empfangen, verpacken und schließlich an die Besteller, aus verschiedenen Ländern, weiterzusenden.

Es ist eine Interessante Beschäftigung, die ca. 1-2 Stunden täglich einnehmen wird.

Wir garantieren Ihnen eine gute Entlohnung (durchschnittlich ca. 35.00 ˆ pro vorgenommene Bestellung, hängt auch von dem Wert der Bestellung und dem Zielland ab).Alle entstandenen Versandkosten werden von uns zusätzlich beglichen.

**Vorraussetzungen**

**- Mindestalter von 21 Jahren**
**-Grundkenntnisse in Englisch**
**- Wohnsitz in Deutschland**
**- Möglichkeit Pakete zu verschicken und zu empfangen**
**- Max. 1-2 Stunden Zeit täglich**
**- Telefonische Verbindung**
**- Einen Willen zu arbeiten**
**- Vollkommene Zuverlässigkeit**

Ihre Onlinebewerbung schicken Sie bitte an:
support@wowowo-support.com

oder besuchen Sie uns im Internet www.wowowo-support.com
Dort finden Sie nähere Informationen zu der Tätigkeit.

Wir hoffen auf eine erfolgreiche Zusammenarbeit!

# E-Mail von Gay Hubbard

## Auswertung von Sprache, Headerprotokoll und Kontakthinweise in einer Phishing-E-Mail

Am 15.12.2006 ging mir die links wieder gegebene E-Mail zu.

## E-Mail-Schau. Förmlichkeiten

Die oberflächliche Betrachtung zeigt:

- Die E-Mail ist frei von Rechtschreibfehlern.
- Ihre Grammatik weist ebenfalls keine gravierenden Fehler auf.
- Die Wortwahl und der Satzbau klingen etwas ungewöhnlich, aber angesichts ihrer scheinbaren Herkunft aus den USA akzeptabel und unauffällig.

Die Nachricht scheint mit einem anderen als den in Westeuropa gebräuchlichen Zeichensatz verfasst worden zu sein, weil das Währungszeichen verfälscht ist:

... durchschnittlich ca. 35.00 ˆ pro vorgenommene Bestellung ...

Um „Dollar“ kann es sich dabei nicht handeln, weil das $-Zeichen in allen üblichen Zeichensätzen bekannt ist, das €-Zeichen hingegen noch nicht.

## Herkunft

Als Absender wird Gay Hubbard angezeigt. Der Betreff lautet Stellenangebot!

Der Absender stellt sich als seit 2004 weltweit tätiger Online-Shop vor, der unter dem Markenzeichen WOWOWO® 2006 und dem Slogan Shopping Over The World For Everyone agiert. Sein Hauptsitz soll in Portugal sein.

Als Kontaktadresse wird genannt:
support@wowowo-support.com

Die Top Level-Domain .com verweist ursprünglich auf ein kommerzielles Angebot aus den USA, kann aber inzwischen weltweit registriert werden.

Für weitere Informationen werden zwei www-Adressen angegeben. Der Absender präsentiert sich danach unter

www.wowowo-support.com

und hat einen deutschen Partner unter

www.wowowo.de

## Inhalt: Was soll ich tun?

Hubbard will mich als zuverlässigen und arbeitswilligen Order-Controller werben. Ich soll Waren in Empfang nehmen, neu verpacken und per Post weiter senden.

## Warum soll ich Order-Controller werden?

Dazu muss ich mindestens 21 Jahre alt sein, in Deutschland wohnen, über Grundkenntnisse in Englisch verfügen und über einen Telefonanschluss verfügen. Meine tägliche Arbeitszeit soll von 1 bis 2 Stunden reichen. Dafür soll ich einen guten Lohn erhalten, der durchschnittlich 35 - Euro muss ich meinen - pro Bestellung, aber je nach Warenwert betragen soll.

## Was ist der Grund?

Es geht um die Freiheit des Warenverkehrs, der von verschiedenen nationalen Restriktionen behindert wird.

Darunter sollen besonders die Bewohner von Nicht-EU-Ländern leiden.




## Kritische Bewertung der förmlichen Aussagen

Die Werbeaussagen klingen recht plausibel und reizen den Robin Hood in mir. Sie versprechen Freiheit für den Handel und jedem seinen Profit.

Das Gewinnversprechen ist weder marktschreierisch noch besonders überzogen. Ich soll richtig 'was tun (Waren empfangen, neu verpacken und bei der Post aufgeben) und erhalte dafür einen Lohn, dessen Höhe aber unbestimmt bleibt.

Hinweise auf die Herkunft und die Art der empfangenen Waren und die Zielorte, an die sie weiter gesandt werden sollen, fehlen jedoch.

Wenn meine Tätigkeit im Durchschnitt mit 35 € bezahlt werden soll und WOWOWO auch noch die Versandkosten übernimmt, so muss es sich jedoch um recht wertvolle Waren handeln, denn sonst machen diese Kosten keinen wirtschaftlichen Sinn. Sie müssen es dem Empfänger wert sein, sie zu bezahlen.

Mit etwas Böswilligkeit könnte man vermuten, dass irgendetwas an den Waren illegal sein könnte. In der Öffentlichkeit ist bekannt, dass man kein Rauschgift schmuggeln darf, dass besonders Musikträger (CDs) und Filme wegen der verwendeten Ländercodes nicht frei importiert werden dürfen, dass sich die Behörden wegen Arzneimittel und die freie Meinungsäußerung von rechtsradikalen Inhalten anstellen, ganz besonders im Zusammenhang mit Kinderpornographie, und dass die USA jede Einfuhr von Nahrungsmitteln verbietet.

Schließlich kann es auch noch Ärger mit dem Zoll und der Steuer geben.

Mit dem Blick auf das Phishing und die Verfolgung von Finanzagenten könnte sich vielleicht auch der Eindruck aufdrängen, dass hier neue Absatzwege erschlossen werden sollen.

Die mir zugelieferten Waren könnten mit ausgespähten Kontodaten bezahlt worden sein und der Order-Controller macht nichts anderes, als den kriminellen Gewinn in Form von werthaltigen Waren an den Täter zu übermitteln.

Dagegen sprechen aber das sprachliche Auftreten von WOWOWO, die deutsche Referenzadresse und die persönlichen Anforderungen an den Order-Controller, die insgesamt seriös wirken.

### merkwürdige Adressen

Die E-Mail-Adresse von Gay Hubbard hat aber nichts mit diesem Namen zu tun. Sie lautet auf hawkins@ricoche.net.

Gerichtet ist die Nachricht an contact@edv-workshop.de. Der EDV-Workshop hat jedoch kein Postfach mit der Bezeichnung contact. Die E-Mail ist zu mir gelangt, weil ich der Inhaber und Webmaster der Second Level Domain EDV-Workshop bin und mein Hostprovider (Strato) nicht zustellbare Nachrichten an mich weiter leitet.

### wowowo.de

Auch die deutsche Kontaktadresse scheint nicht ganz glücklich mit ihrer Aufgabe zu sein.

Dort wird behauptet, sie werde von wowowo-support.com seit dem 09.12.2006 missbraucht, habe mit den dort gemachten Jobangeboten nichts zu tun und es handele sich hier offensichtlich um Betrüger.

### wowowo-support.com

Auch der Webauftritt von wowowo-support.com überrascht etwas. Er erinnert weder an eine portugiesische noch an eine US-amerikanische Herkunft. Der Zeichensatz ist merkwürdig und nur wenige Worte erscheinen verständlich zu sein:

Firewall ist ein geläufiger englischsprachiger Begriff, ebenso Colocation für angemietete Serverstandorte.

АнтиSpyWare scheint auf AntiSpyware hinzudeuten, also auf Programme zur Abwehr von Spionageangriffen, und Торговля auf Trojaner.

Besonders auffällig ist, dass die Website nicht unter dem Namen WOWOWO firmiert, sondern unter **AGAVA**. Wir sind irgendwo im russischen Sprachraum gelandet - und ich habe nur einen schnellen Screenshot (Bildschirmabzug) gemacht, bevor alle Grafiken (und was sonst noch) geladen wurden.

Erstes Fazit: Da stimmt etwas nicht. Der Text der E-Mail von Gay Hubbard kann nicht richtig sein.

## Recherchen zur Mail-Adresse

Aufgefallen war uns, dass die E-Mail-Adresse von Gay Hubbard auf hawkins@ricoche.net lautet.

Um darüber genaueres zu erfahren verwenden wir ein Allzweckwerkzeug zur Auswertung von DNS-Namen und IP-Adressen: dnsstuff.com .

**Betreff:** **Stellenangebot!**
**Von:** Gay Hubbard <hawkins@ricoche.net>
**Datum:** 09:24
**X-Account-Key:** account2
**X-UIDL:** 1132761413.1563
**X-Mozilla-Status:** 0001
**X-Mozilla-Status2:** 00000000
**Return-Path:** <hawkins@ricoche.net>
**Received:** from mailin18.aul.t-online.de (mailin18.aul.t-online.de [172.20.26.73]) by mhead25 with LMTP; Fri, 15 Dec 2006 06:24:15 +0100
**X-Sieve:** CMU Sieve 2.2
**Received:** from natfruni.rzone.de ([81.169.145.180]) by mailin18.sul.t-online.de with esmtp id 1Gv5YA-1uy7tl0; Fri, 15 Dec 2006 06:24:02 +0100
**Received:** from mail.lesjofors.com ([212.220.76.82]) by mailin.webmailer.de (8.13.7/8.13.7) with ESMTP id kBF5O07f000389 for <contact@edv-workshop.de>; Fri, 15 Dec 2006 06:24:01 +0100 (MET)
**Received:** from 65.98.57.213 (HELO ricoche.net) by edv-workshop.de with esmtp (>L34FPA*= T*8L0+) id CJ0932-Q/3/87-=3 for contact@edv-workshop.de; Fri, 15 Dec 2006 05:24:07 -0300
**Message-ID:** <01c72009$3e177e30$6c 822ecf@hawkins>
**MIME-Version:** 1.0
**Content-Type:** multipart/alternative; boundary="----=_NextPart_000_0006_01C72033.26ED8630"
**X-Priority:** 3 (Normal)
**X-MSMail-Priority:** Normal
**X-Mailer:** Microsoft Outlook, Build 10.0.3416
**X-MimeOLE:** Produced By Microsoft MimeOLE V6.00.2900.2180
**Importance:** Normal
**X-TOI-SPAM:** u;0;2006-12-15T05:24:15Z
**X-TOI-VIRUSSPAM:** unchecked
**X-TOI-MSGID:** 41ddb698-8cf6-4e67-90c0-bac58dcae878
**X-Seen:** false
**X-ENVELOPE-TO:** <Kochheim.user@T-Online.de>

### ricoche.net

Der **WHOIS Lookup** verrät uns, dass hinter der Second Level Domain eine Firma GO DADDY steckt.

```
Registrar:      GO DADDY SOFTWARE, INC.
Status:         clientRenewProhibited
Dates:          Created 04-apr-2002
Updated 14-jul-2006  Expires 04-apr-
2007
DNS Servers:    NS1.RICOCHENETWORK.COM
NS2.RICOCHENETWORK.COM
```

Die dazu gehörige Adresse godaddy.com firmiert, so der **Reverse DNS lookup**, in Scottsdale, Arizona, USA.

Bei ricoche.net handelt es sich laut **Free E-mail Lookup** um keinen Freemailer. Dasselbe gilt für godaddy.com. Die genannte Adresse wäre nicht kostenlos erhältlich gewesen, wenn sie denn zutreffend ist. Kostenpflichtige E-Mail-Dienste bietet hingegen godaddy.com an.

An der Authentität der E-Mail-Adresse von Gay Hubbard sind hingegen Zweifel angebracht, weil es sich bei ricoche.net um eine Modeseite handelt, die das Barbie-Publikum anspricht.

## Header-Einträge

Dass uns die E-Mail-Adresse von Gay Hubbard nicht weiter geholfen hat, ist nicht weiter verwunderlich. Sie ist - ebenso wie der Name des Absenders, der Betreff, der Zeitstempel und die meisten anderen Angaben im Kopf einer E-Mail - frei manipulierbar und sagt nichts über den tatsächlichen Urheber der Nachricht aus. Schauen wir uns die anderen Angaben im Header der E-Mail von Gay Hubbard an.

### Aussagen der Header-Einträge

Die Angaben zum Absender haben uns nicht weiter geholfen. Sie übernehmen die Angaben des Versenders, die er selber auswählt.

Das Datum ist ebenfalls manipulierbar. Mein Browser weist nur die vom Absender angegebene Uhrzeit aus und lässt das heutige Datum aus.

Alle Angaben mit einem **X-**Vorsatz werden auf dem Übertragungsweg der E-Mail vermerkt und müssen nicht zwingend über ihre Herkunft aussagen.

Bei der Zehn-Ziffernfolge der X-UIDL links vom Punkt - 1132761413 - könnte es sich um eine dezimale IP-Adresse handeln, die die Original-Adresse verschleiert. Der **URL Deobfuscator** löst sie auf in die IP-Adresse 67.132.145.69. Sie wiederum verweist auf das ST. JOSEPH REGIONAL HEALTH CNTR in Bryan, Texas, USA.

Das UIDL (unique identifier listing) ist eigentlich eine Eintragung des Mailservers meines E-Mail-Kontos (bei T-Online). Also vergessen wir das Krankenhaus in Brian.

Die **X-Mozilla-Status** sind Eintragungen meines eigenen Browsers und geben keine Auskunft zur Herkunft.

Traceroute für ricoche.net mit bbox.ch


Traceroute für IP 212.220.76.82 mit bbox.ch


Traceroute mit dnsstuff.com

Der **Return-Path** wird zwar vom Absender gesetzt, ist aber manipulierbar und deshalb ohne feste Aussage. Er hilft nicht weiter, wie wir bereits festgestellt haben.

Danach folgen mehrere **Received**-Einträge, die tatsächlich Aussagen bergen, weil sie von den Servern vermerkt werden, über die die Nachricht zu mir gelangt ist. An erster Stelle erscheint der jüngste Eintrag und ihm folgen die jeweils älteren.

Das letzte Ereignis ist danach gewesen, dass sich innerhalb von T-Online der Posteingangsserver mailin18.aul.t-online.de am Freitag, dem 15.12.2006, um 06:24:15 MEZ, beim Postfachdienst mhead25 gemeldet und die Nachricht übergeben hat. Die Uhrzeit bezieht sich auf die Greenwich-Zeitzone (GMT). Der Zusatz +0100 besagt, dass eine Stunde hinzugezogen werden muss, also die Zeitzone nach Osten wechselt, also zur Mitteleuropäischen Zeitzone, in der auch Deutschland angesiedelt ist.

Auch der zweite **Received**-Eintrag hält keine Überraschungen bereit. Die IP 81.169.145.180 gehört zur Strato AG, bei der der EDV-Workshop und seine E-Mail-Postfächer betrieben (gehostet) werden. 13 Sekunden vorher hatte sich Strato bei T-Online gemeldet, um die Nachricht zu übergeben.

Erst der dritte **Received**-Eintrag führt uns nach außerhalb. Die Domain webmailer.de gehört zur Strato AG und löst deren Domain- und Postfachadressen auf. Ihr Server erhielt eine Sekunde vorher eine Anfrage von mail.lesjofors.com nach dem Postfach contact@edv-workshop.de.

Die Adresse lesjofors.com ließ sich zunächst nicht auflösen. Der DNS Report protokolliert aber den Weg zu dieser Adresse und führt schließlich zu der IP 62.20.13.197. Diese wiederum führt nach Schweden zu:

```
inetnum:        62.20.13.192 -
62.20.13.255
netname:        SE-LESJOFORSELECTRONIC
descr:          Lesjofors Electronic AB
country:        SE
...
org-name:       Lesjofors Electronic AB
org-type:       NON-REGISTRY
descr:          IT-bolag
address:        Bergsslagsgatan 105
address:        68096 Lesjofors
address:         Sverige
```

Lesjofors.com scheint nicht nur in Schweden ansässig zu sein. Zum DNS-Namen wurde auch die IP 212.220.76.82 protokolliert und die führt nach Russland.

```
descr:                Uralsviazinform OSPD
network

descr:           Ekaterinburg
descr:           Russia
...
person:         Igor V Semenov
address:        Russia
address:        Chapaeva 12
address:        Ekaterinburg
phone:          +7 3432 561256
e-mail:         ***@aoets.ru
...
person:         Andrew V. Shnir
address:        620067 Ekaterinburg
address:        4 Asbestowskij Lane
address:        Russia
phone:          +7 343 3761750
fax-no:         +7 343 3716099
e-mail:         *******@urtc.ru
```

Der vierte und letzte **Received**-Eintrag enthält die IP 65.98.57.213. Sie gehört einem Provider in Clifton, New Jersey, US. Das ist derselbe Ort, in dem auch ricoche.net ansässig ist:

```
OrgName:     FortressITX
OrgID:       FORTR-5
Address:     100 Delawanna Ave
City:        Clifton
StateProv:   NJ
PostalCode:  07014
Country:     US
```

FortressITX hat sich demnach bei (>L34FPA*= T*8L0+) id CJ0932-Q/3/87- über den Standort des Postfachs contact@edv-workshop.de erkundigt. Die Auflösung dieser Station übersteigt meine Fähigkeiten. Sie hat aber die IP 65.98.57.213 aufgelöst und als HELO ricoche.net identifiziert.

Verwirrend ist der Standort des Servers in Ekatarinburg am äußersten östlichen Rand von Europa.

Mit bbox.ch habe ich zwei Traceroutes [10] erstellt, eine für ricoche.net und eine für den Server 212.220.76.82 in Ekatarinburg. bbox.ch sitzt in Zürich. Deshalb werden die Verbindungen von der Schweiz aus zu den Zielorten angezeigt.

Mit einem weiteren Traceroutig mit dnsstuff.com habe ich festgestellt, dass ein ziemlicher Zickzackkurs auf dem Weg von den USA entstehen kann, der zunächst von Washington nach Großbritannien, von dort zurück nach Washington, dann aber direkt nach Moskau und von dort nach Ekatarinburg führt, dann aber noch einmal nach Chelybinsk am Ural, von dort nach Sochi am Schwarzen Meer und schließlich zur Zieladresse in Ekatarinburg führt.

Bei ricoche.net waren wir schon einmal und ich habe die Adresse als falsche Fährte angesehen.

Jetzt gibt es zwei Möglichkeiten: Entweder ist ricoche.net wirklich eine Finte oder der Server dieser Einrichtung wurde gehackt und missbraucht, um die E-Mail von Gay Hubbard zu versenden.

Eine vernünftige Antwort bekommen wir nicht aus der folgenden Message-ID, die zwar hawkins wiederholt, also die Postfachbezeichnung, die Gay Hubbard verwendet, aber ansonsten - mir jedenfalls - völlig unbekannte Notizen.

10 Mit einem Tracerouting werden die Strecke und die zwischengeschalteten Übergabepunkte für eine Nachricht protokolliert und ausgewertet (Ort, Reaktionszeit u.a.).


russland.RU
die Internet-Zeitung
XML Sch
Politik | Wirtschaft | Verschiedenes | Sport |
15-08-2004 SCHLAGZEILEN
Paradox auf Russisch: Mord an einem Richter gibt Zuversicht in den Sieg der Demokratie
Am vergangenen Montag holte ein Mann im Park der kleinen Stadt Dolgoprudny bei Moskau eine 34-jährige Frau ein, die zur Arbeit ging, riss den Stutzen, den er unter der Jacke trug, hervor und schoss ihr zweimal in den Bauch. Einige Stunden später verstarb das Opfer auf dem Operationstisch.

### was bleibt?

Als eher unwahrscheinlich können wir ausschließen, dass Gay Hubbards E-Mail aus dem Bereich von T-Online oder Strato stammt. Die Herkunftsdaten in Bezug auf ricoche.net, nach Schweden und schließlich nach Russland wären zwar sehr geschickt gewählt als verschleiernde Informationen, aber doch eher geeignet für Verschwörungstheorien.

Warum verweist uns der Weg der Nachricht nach Russland? Entweder befindet sich in Ekaterinburg der nächste DNS-Server, den der aussendende Mailserver erreichen kann, oder es ist Zufall, welcher DNS-Server aus dem europäischen RIPE-Verbund eine aus den USA stammende Anfrage aufnimmt und beantwortet.

Für beide Möglichkeiten sprechen die äußerst kurzen Reaktionszeiten im Sekundenbereich.

Somit kommt weiter richote.net als Absender der Nachricht in Betracht.

Web-Portale und -Shops mit einer permanenten Erreichbarkeit im Internet sind beliebte Ziele für missbräuchliche Hackingattacken und besonders dann, wenn der Missbrauch getarnt werden soll. Ihre Seriösität und offensichtliche Ungefährlichkeit sollen ausgenutzt werden - und ihre technischen Kapazitäten.

Um mehr Klarheit zu bekommen müssen wir noch einen Blick auf die Kontaktdaten aus Gay Hubbards E-Mail werfen.

## Gay Hubbards Kontaktdaten

Was uns bleibt ist, dass wir uns die Standorte der Domains wowowo-support.com und agava.-com etwas genauer anschauen.

Der **DNS Report** für die Domäne wowowo-support.com ermittelt deren Erreichbarkeit und zeigt gleichzeitig auf, welche IP-Adresse unter dem DNS-Namen aktiv ist. Diese Prüfung führt zu der IP 89.108.66.188.

Der **IPWHOIS Lookup** mit der IP 89.108.66.188 führt nach Russland und zeigt uns, dass diese IP von der Firma AGAVA JSC verwendet wird:

```
address: AGAVA JSC
address: Oruzheiniy per., 25/1, office
8
address: 125047 Moscow
address: Russia
phone: +7 495 4081790
phone: +7 495 4086755
fax-no: +7 495 4081790
```

Die Auflösung der Domain wowowo-support.com bringt ein ganz ähnliches Ergebnis:

```
Registrant:
Andrey Pavlov
Registered through: AGAVA Software
Domain Name: WOWOWO-SUPPORT.COM
Domain servers in listed order:
NS1.AGAVA.NET.RU
NS2.AGAVA.NET.RU
```

Dasselbe gilt für die Domain agava.net.ru:

```
person: VLADIMIR V PANFILOVICH
nic-hdl: VVP22-RIPN
address: Mendeleeva str.,12
address: 141700, Dolgopudniy, Russia
phone: +7 095 4081172
e-mail: **********@agava.com
changed: 2006.07.07
```

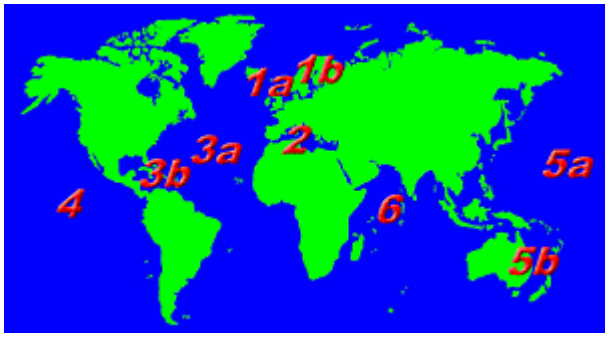
Richtig heißt die Stadt wohl Dolgoprudny.

Aus einer Meldung bei russlandonline.ru wissen wir, dass es sich um eine kleine Stadt bei Moskau handelt.

Nach Dolgoprudniy führt auch die Auflösung der Domain agava.com:

```
Administrative Contact
Contact ID: 07LSTRO-RU
Contact Name: AGAVA Software
Ltd.
Contact Organization: AGAVA llc.
Contact Street1: Pervomayskaya 1
Contact City: Dolgoprudny
Contact State: MO
Contact Postal Code: 141700
Contact Country: RU
Contact Phone: +7 495 4284200
Contact E-mail:
*******@agava.com
```


Links. Zonenverwaltungen für das Domain Name System – DNS




Links: Kabelregionen und -verbünde


Links: Satelliten und Kabelnetz von Teleglobe


Kabelnetz von IBM

## Fazit

Einige Informationen haben wir gewinnen können, um die die Herkunft der E-Mail von Gay Hubbard zu lüften.

Den ersten Hinweis gibt sie uns mit ihrer E-Mail-Adresse zur Kontaktaufnahme: support@wowowo-support.com

Sie führt uns zur Domain wowowo-support.com, die uns - ebenfalls wie die IP 89.108.66.188 zu der Firma Agava mit Sitz in Moskau führt. Eine weitere Niederlassung der Firma Agava ist offensichtlich in Dolgoprudniy in der Nähe von Moskau, die dort die Domains agava.net.ru und agava.com angemeldet hat.

Zwei Sackgassen haben sich uns aufgetan. Eine führte zur Domain ricoche.net, zu der Gay Hubbard eine passende E-Mail-Adresse angegeben hat, und eine zum DNS-Provider lesjofors.com mit Hauptsitz in Schweden und einer Niederlassung mit der IP 212.220.76.82, die wir in Ekaterinburg im tiefen Russland lokalisiert haben.

Waren das wirklich Sackgassen?

Gay Hubbards E-Mail war an die Domain EDV-Workshop.de adressiert. Um ihren Empfänger zu erreichen, musste diese DNS-Adresse von Rootservern aufgelöst und entweder unmittelbar in eine IP aufgelöst oder an einen DNS-Server weitergeleitet werden, der die DNS-Adresse in eine IP auflösen kann.

Die Länderdomain **de** wird von der in Deutschland ansässigen **DeNIC** verwaltet. Sie ist sozusagen eine Abteilung der europäischen DNS-Zone **RIPE** mit Sitz in Amsterdam. Sie verwaltet die Zonen 1a und 1b. 1a betrifft Großbritannien und West- und Mitteleuropa und 1b Nordeuropa, das Baltikum und das gesamte Russland.

Aus den Received-Einträgen der Nachricht wissen wir, dass der Erstkontakt zwischen einem nicht identifizierten Server mit der Lesjofors-Niederlassung unter der IP 212.220.76.82 in Ekaterinburg in Russland stattfand und Lesjofors die Anfrage ricoche.net zugeordnet hat.

Vielleicht stammt die E-Mail doch von ricoche.-net?

Schauen wir uns die Kabelverbindungen zwischen den USA und Europa anhand eines der größten weltweit tätigen Anbieter an, Teleglobe. Sie führen traditionell entlang den Handelsrouten der Schifffahrt und wurden zunächst von Irland aus durch den Nordatlantik zur Ostküste der USA geführt. Dort wurden sie auch besonders stark ausgebaut.

Aber auch die Westküste der USA hat starke Verbindungen durch den Pazifik hindurch nach Japan und von dort zum südlichen Asien.

Innerhalb der USA sind die Fernstreckennetze hervorragend ausgebaut, so dass unabhängig von der Tageszeit in den USA ein schneller Datenverkehr gesichert ist.

Die großen Telefongesellschaften sind darüber hinaus aus Kostengründen bestrebt, eine Verbindung in ihrem eigenen Kabelnetz zu führen. Sie unterhalten deshalb in aller Regel eine eigene Kabelverbindung zu den ausländischen Metropolen und in Übersee.

Clifton, der Sitz von ricoche.net, liegt in New Jersey in der Nähe von New York.

Einer der dominierenden Anbieter von Telekommunikationsleistungen im Ostküstenbereich ist IBM. Und IBM ist auch ein Unternehmen, das besonders leistungsstarke Kabelverbindungen nach Japan unterhält und darüber den südasiatischen Raum einschließlich einer starken Anbindung nach Australien.

Der Zeitstempel, der uns geliefert wurde, lautet: Fri, 15 Dec 2006 05:24:07 -0300. Wenn wir ihn entsprechend den Zeitzonen auflösen kommen wir zu folgenden Ortszeiten:

| | | | | |
|---|---|---|---|---|
| Kontakt | -0300 | = | 02:24 | Greenwich |
| Clifton | -0500 | = Vortag | 21:24 | Ortszeit |
| Westküste | -1000 | = Vortag | 16:24 | Ortszeit |
| Japan | +0900 | = | 11:24 | Ortszeit |
| Ekaterinburg | +0400 | = | 06:24 | Ortszeit |

Als der erste Kontakt stattfand war es in Clifton, New Yersey, abends um 21:24, also eine gute Zeit, um unbemerkt vom Personal eine Spam-Aktion durchführen zu können.

Lesjofors ist ein DNS-Server in der Zone 1, die von RIPE verwaltet wird. In Ekaterinburg war es früh morgens um 06:24. Dort herrschte noch finstere Nacht und es dürfte noch wenig Netzlast und Arbeitslast für den DNS-Server bestanden haben. Das spricht dafür, dass Ekaterinburg einfach nur der erste gut erreichbare DNS-Server in der europäischen Rootzone war.

Eine Bestätigung dafür ist auch das Tracerouting, das ich mit dnsstuff.com durchgeführt habe. Es führte u.a. nach Sochi am Schwarzen Meer. Dorthin verlaufen auch die Kabelstrecken der klassischen Überseekabel, die Europa mit Indien und China verbinden. Diese haben schließlich direkte Verbindungen mit dem Kabelnetz von IBM.

### Ergebnisse

Der Standort des ersten DNS-Servers in Russland, mit dem wegen der E-Mail von Gay Rubbard Kontakt in der Rootzone 1 aufgenommen wurde, muss nicht bedeuten, dass ihre Herkunft auch in Russland ist. Der DNS-Server hat die Anfrage jedenfalls aufgelöst und ricoche.net zugeordnet.

Das kann durchaus richtig sein, weil die Ortszeit am Sitz von ricoche.net äußerst günstig für eine illegale Spamaktion war. Unter der weiteren Annahme, dass die DNS-Anfragen von ricoche.net zunächst im Netz eines der führenden US-amerikanischen Netzanbieter transportiert wurde, muss sie nicht zwangsläufig über den Atlantik geführt worden sein, sondern kann auch über Japan, Südasien und dem Schwarzen Meer nach Russland gelangt sein, wo sich Lesjofors als erster und gut erreichbarer DNS-Server in der europäischen Rootzone anbot.

Ich gehe deshalb davon aus, dass der Server von ricoche.net für die Spamaktion missbraucht wurde, durch die Gay Hubbards E-Mail zu mir gelangte.

Dafür spricht auch, dass ricoche.net zwar nur in einer, aber immerhin als bekannter Spam-Versender bekannt ist, wie der **Spam Database Lookup** zeigt.

Gay Rubbards geschäftlichen Aktivitäten haben ihr Zentrum in und in der Umgebung von Moskau. Dort sind die Firmen und IP-Standortorte ansässig, die mit den Domains wowowwo-support.com und agava.com in Verbindung stehen.