



Sebastian  
Kübeck

# Web-Sicherheit

Wie Sie Ihre Webanwendungen  
sicher vor Angriffen schützen

# Teil I

## Grundlagen der Informationssicherheit

### In diesem Teil:

- **Kapitel 1**  
Wie konnte es nur so weit kommen? – Eine kurze Geschichte der Computerkriminalität . . . . . 21
- **Kapitel 2**  
Auswirkungen von Sicherheitsvorfällen auf Unternehmen und Organisationen . . . . . 41
- **Kapitel 3**  
Warum sich keiner betroffen fühlt und niemand etwas dagegen tut. . . . . 47
- **Kapitel 4**  
Grundprinzipien der Informationssicherheit . . . . 55
- **Kapitel 5**  
Authentifizierung und Autorisierung. . . . . 69
- **Kapitel 6**  
Sichere Nachrichtenübermittlung und -speicherung. . . . . 81



# Wie konnte es nur so weit kommen? – Eine kurze Geschichte der Computerkriminalität

Da viele Bezeichnungen im Bereich der Computerkriminalität, wie zum Beispiel »Hacker«, historische Wurzeln haben und sich ihre Bedeutung laufend verändert, ist es sinnvoll, wenn wir uns erst einmal einen kurzen Überblick verschaffen, wie es eigentlich so weit kommen konnte mit der Computerkriminalität. Die Kenntnis der Geschichte der Computerkriminalität ist zwar für das Verständnis der folgenden Kapitel nicht zwingend notwendig, es erleichtert allerdings das Verständnis heutiger Angriffsmethoden oft ungemein, wenn man weiß, wie sich diese im Laufe der Zeit entwickelt haben.

Das Erstaunliche an dieser Geschichte ist, dass die wenigsten aktuellen Angriffstechniken wirklich neu sind. Warum das so ist und warum wir uns immer noch mit Problemen herumschlagen, die seit 40 Jahren bekannt sind, werden wir im nächsten Kapitel näher beleuchten.

## 1.1 Frühe Computer

Bis in die Sechzigerjahre des vorigen Jahrhunderts war Computerkriminalität nicht wirklich ein Problem, da es bis dahin keine Rechnernetze gab. Computer waren damals riesige, unsagbar teure und kompliziert zu bedienende Maschinen, welche Daten über Lochkarten oder Ähnliches mit der Außenwelt austauschten.

Die Computer der damaligen Zeit arbeiteten im Übrigen im Batch-Betrieb, das heißt, dass sie eigentlich gar keine Benutzerschnittstelle im heutigen Sinn hatten. Man belud sie mit einer Unzahl von Lochkarten und startete die Verarbeitung. Das Ergebnis wurde nach dem Ende der Berechnung üblicherweise auf Papier ausgedruckt. Das alles bot keine brauchbare Angriffsfläche für Kriminelle.

## 1.2 Telefonnetze und Phreaker

Es gab allerdings schon ein elektronisches Kommunikationsnetzwerk, lange bevor es Computer gab: das Telefonnetz. Als Konrad Zuse im Jahr 1941 den ersten Computer überhaupt baute, war das Telefonnetz bereits sechzig Jahre alt.

In den USA wurde das Telefonnetz schon manipuliert, lange bevor dies mit Computern möglich war. Joe Engressia gilt heute als der Vater dieser Art von Manipulationen, die den Zweck hatten, kostenlose Ferngespräche führen zu können. Personen, die diese Manipulationen anwendeten, wurden *Phreaker* genannt und das Ganze funktionierte so:

Joe Engressia war in den Fünfzigerjahren ein blindes Kind. Er fand zu dieser Zeit heraus, dass er durch Pfeifen eines gewissen Tons das System zurücksetzen konnte, das für die Erzeugung des Tons zuständig war, welcher erklang, nachdem eine Verbindung zwischen Gesprächsteilnehmern getrennt wurde. Die Frequenz von 2.600 Hertz, die er durch sein Pfeifen nachahmte, war genau jene, die auch das amerikanische Telefonsystem verwendete. Obwohl er das nicht gleich realisierte, war er so in der Lage, einen wichtigen Teil des öffentlichen Telefonsystems zurückzusetzen, wodurch der Weg für kostenlose Ferngespräche frei war.

Später entwickelte sich eine regelrechte Phreaker-Szene, die sich dann in den Achtzigerjahren zu der Hacker-Szene weiterentwickelte, wie wir sie heute kennen.

### 1.3 Time-Sharing

Mit *Time-Sharing* wird das Aufteilen der Rechenzeit eines Computers auf unterschiedliche Benutzer bezeichnet. Der erste Computer, der Time-Sharing beherrschte, war die PDP-1 (von Programmed Data Processor) der Digital Equipment Corporation (DEC, heute ein Teil von HP). An die PDP-1 waren mehrere Terminals angeschlossen. Terminals waren Geräte mit Bildschirm und Tastatur, die allerdings nur eine ziemlich einfache Technik besaßen.

So wurde meist jeder Tastendruck an den Computer gesendet, woraufhin dieser Zahlensequenzen an das Terminal schickte, welches diese wiederum als Zeichen am Bildschirm darstellte. Der Computer selbst bediente alle Terminals quasi parallel, indem er eine gewisse Zeit lang für jeden Benutzer bereitstand und reihum alle bediente, so dass bei jedem Benutzer der Eindruck entstand, der Computer kümmere sich ausschließlich um seine Anfragen.

Durch den Zugriff unterschiedlicher Benutzer auf gemeinsame Ressourcen und Dateien war natürlich schon prinzipiell die Möglichkeit geschaffen, auf Daten anderer Benutzer zuzugreifen, was dann auch letztlich geschah. Da heute zum Beispiel Webserver nach demselben Prinzip funktionieren, ergibt sich hier dieselbe prinzipielle (und oft faktische) Verwundbarkeit wie damals.

Die erste Hacker-Gruppe formierte sich 1961 am MIT (Massachusetts Institute of Technology), kurz nachdem das Institut seine erste PDP-1 bekam. Diese Gruppe, die sich *Tech Model Railroad Club* nannte, bestand aus Leuten, die großen Spaß am Programmieren fanden. Ursprünglich war ja mit dem Begriff *hacken* keine krimi-

nelle Tätigkeit gemeint. Es war ein Wort für die Beschäftigung mit der Technik aus Freude an der Sache, also ohne kommerzielle oder sonstige Absicht.

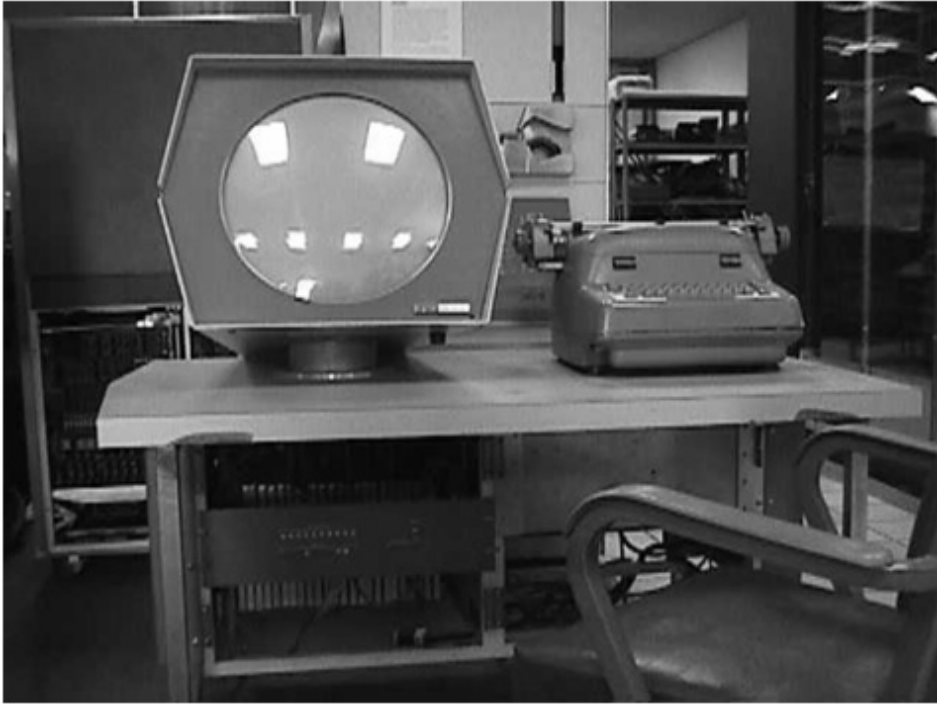


Abb. 1.1: PDP-1 aus dem Jahre 1960. Quelle: Wikipedia

## 1.4 Die Bedeutungen des Wortes »Hacker« im Laufe der Zeit

In den Sechzigerjahren des vorigen Jahrhunderts wurde jemand als *Hacker* bezeichnet, der wirklich etwas vom Programmieren verstand, der sich mit den Computern dieser Zeit auskannte und Programme so manipulieren konnte, dass sie mehr leisteten als das, wofür sie ursprünglich geschrieben worden waren. In den späten sechziger und frühen Siebzigerjahren wurde das Hacken dann mehr und mehr mit radikalen Untergrundaktivitäten in Verbindung gebracht, welche sich gegen das damalige Gesellschaftssystem richteten (»yippie«).

Zu dieser Zeit begannen Behörden in den USA, gegen *Phreaker* vorzugehen, die das Telefonnetz manipulierten, um Gratis-Ferngespräche führen zu können. In den Achtzigerjahren wurden mehrere hochkarätige Computer-Hacker vom FBI festgenommen, zu denen auch Kevin Mitnick gehörte, der daraufhin in der Hacker-Community zum Märtyrer avancierte. Die Filme *WarGames – Kriegsspiele*

(John Badham, 1993), Sneakers – Die Lautlosen (Phil Alden Robinson, 1992) und Hackers – Im Netz des FBI (Iain Softley, 1995) machten den Begriff *Hacker* schließlich als Synonym für eine Art Robin Hood mit überragenden technischen Fähigkeiten populär.

Obwohl die Hacker-Community wie der deutsche *Chaos Computer Club (CCC)* immer zwischen dem »Hacker« in seiner ursprünglichen Bedeutung und dem »Cracker« – die Bezeichnung für jemanden, der mit böser Absicht Sicherheitssysteme umgeht um in Computer einzudringen – unterschied, wurden diese Begriffe in der öffentlichen Wahrnehmung zunehmend vermischt und der Begriff »Hacker« behielt seinen schlechten Ruf.

Mit dem »Hacker« wurden aber in jedem Fall immer außergewöhnliche technische Fähigkeiten verbunden, die eingesetzt werden, um Schwachstellen von Systemen aufzuzeigen und Dinge mit Computern und Programmen anzustellen, zu denen kein normaler Computerbenutzer fähig ist. Die Bedeutung des Begriffs »Cracker« hat sich ebenfalls gewandelt: Er wird heute eher als Kurzform für *Password Cracker*, also für einen Spezialisten auf dem Gebiet des Aufspürens von fremden Passwörtern verwendet.

Bei den Hackern wird inzwischen oft zwischen *White-Hats* und *Black-Hats* unterschieden. »White-Hats« attackieren Netzwerke und Computer im Auftrag der Eigentümer selbst. Sie werden beauftragt, Sicherheitslücken zu finden und dem Eigentümer gegebenenfalls bei deren Behebung zu helfen. »Black-Hats« dagegen sind kriminelle Hacker, die in Netzwerke und Computer einbrechen, um beispielsweise Daten zu stehlen. Daneben gibt es noch sogenannte »Gray-Hats«. Diese Hacker attackieren widerrechtlich fremde Infrastruktur, allerdings zu dem Zweck, auf Sicherheitslücken aufmerksam zu machen und Black-Hats zuvorzukommen.

## 1.5 Computernetze

In den späten Siebzigerjahren war die Geburtsstunde der *Personal Computer* gekommen, also kleiner, billiger Computer, die auch für kleine Firmen und Privatpersonen erschwinglich waren. Einer der ersten Vertreter dieser Gattung war der Altair 8800, den man allerdings erst einmal zusammenbauen musste, bevor man ihn verwenden konnte. Auch hatte er noch keine Tastatur und keinen Bildschirm. Das änderte sich mit dem Aufkommen des Apple I und II sowie der weiteren PCs dieser Zeit wie dem Commodore 64 und dem IBM PC.

Für diese Computer gab es vorerst noch keine Netzwerke, wie wir sie heute kennen. Der Datenaustausch erfolgte durch die Weitergabe von Datenträgern wie Kassetten und Disketten (dies wurde auch als *Pantoffelnetzwerk* bezeichnet). Trotz dieser Einschränkungen wurde damals bereits Schadsoftware entwickelt, vornehmlich Viren. Diese Viren brachten befallene Computer dazu, ihren eigenen

Code auf alle Datenträger zu schreiben, auf die die verseuchten Computer zugriffen. Griff nun ein nichtbefallener Computer auf einen dieser Datenträger zu, wurde er ebenfalls »angesteckt«. So konnten sich diese Viren schnell verbreiten. Ein Virus ist eine Schadsoftware, die sich selbsttätig, also ohne die Hilfe eines anderen Programms, verbreiten kann.

Der erste bekannte Virus dieser Art für MS-DOS war der *Pakistani-* oder *Brain-Virus*, der erstmals 1986 auftauchte. Seine Schöpfer Basit und Amjad Farooq Alvi wollten damit laut eigenen Angaben das unerlaubte Kopieren ihrer Software verhindern und ahnten zu diesem Zeitpunkt noch nicht, was sie damit auslösen würden. Schon zwei Jahre später war es mit dem »Virus Construction Kit« möglich, Computerviren nach Bedarf zusammenzustellen, ohne tiefgreifende Kenntnisse in der Virenprogrammierung zu besitzen.

In den darauf folgenden Jahren entwickelten sich unterschiedliche Varianten von Viren. Es gab harmlose Viren, die einfach nur lästig waren und zum Beispiel bunte Figuren über den Bildschirm springen ließen (sogenannte *Fun-Viren*). Es gab aber auch böartige Viren, die zum Beispiel nach einer gewissen Zeit Disketten löschten oder unbrauchbar machten. Autoren dieser Viren waren meist äußerst versierte und erfahrene Programmierer, die es offenbar genossen, andere Computerbenutzer in Angst und Schrecken zu versetzen und ihre überragenden technischen Fähigkeiten zu demonstrieren.

Das Ethernet wurde – wie so vieles andere auch – in den Siebzigerjahren im Xerox Palo Alto Research Center erfunden, es erreichte allerdings erst ab den Achtzigerjahren große Beliebtheit bei PC-Benutzern. Mit ihm war es erstmals möglich, Computer halbwegs erschwinglich zu vernetzen. Bis heute ist das Ethernet die dominierende Technologie bei der Vernetzung, speziell von PCs.

Diese Netzwerke hatten aber zunächst keinen so großen Einfluss auf die Computerkriminalität wie die WANs (Wide Area Networks) in der Form des Telefonnetzes und später des Internets.

## 1.6 Die unselige Verbindung von Computern und Telefonnetz

Beginnend mit den Achtzigerjahren wurden Mailboxen – im englischsprachigen Raum *Bulletin Board Systems* oder kurz *BBS* genannt – sehr beliebt. Man benötigte ein Modem oder einen Akustikkoppler, um sich über das Telefonnetz mit der Mailbox zu verbinden.

Einschub zum Begriff *Akustikkoppler*: In Deutschland und Österreich war das Telefonnetz damals noch im Besitz der jeweiligen staatlichen Post, die nur eigene, sündhaft teure Endgeräte in ihrem Netz erlaubte, daher kamen Akustikkoppler in Mode, die das Monopol teilweise umgingen. Akustikkoppler sind Geräte, die ähnlich wie ein Modem funktionieren. Man verbindet sie allerdings nicht direkt mit

dem Telefonnetz, sondern steckt sie auf den Telefonhörer, wie in der folgenden Abbildung zu sehen ist.

Ein Akustikkoppler besaß einen Lautsprecher und ein Mikrofon. Er erzeugte Töne, die vom Mikrofon des Telefonhörers entgegengenommen wurden und sein eigenes Mikrofon nahm wiederum Töne aus dem Lautsprecher des Telefonhörers entgegen. Das Ganze war zwar billiger als ein Modem, dafür aber äußerst störanfällig und die Übertragung war quälend langsam, wodurch diese Geräte im Zuge der späteren Liberalisierung der Telefonnetze schnell wieder aus der Mode kamen.



**Abb. 1.2:** Akustikkoppler. Quelle: [www.benser.net](http://www.benser.net)

Mailboxen waren eine Art Vorläufer des Internets. Obwohl sie rein textbasiert waren, stellten sie viele Dienste zur Verfügung, die heute das Internet bietet. Dazu gehörten das Verschicken von E-Mails, das Herunterladen und Tauschen von Dateien sowie *schwarze Bretter*, die ähnlich wie heutige Newsgroups funktionierten und auf denen Benutzer für alle sichtbare Nachrichten hinterlassen konnten. Darüber hinaus gab es auch schon Onlinespiele, bei denen unterschiedliche Benutzer mitmachen konnten und vieles mehr.

Mailboxen entwickelten sich schnell zu Tummelplätzen für Hacker und Phreaker. Sie boten ihnen eine perfekte Plattform, um Gleichgesinnte kennenzulernen, mit denen sie Angriffstechniken und Tricks austauschen konnten. Mailboxen waren für diese Leute auch ein praktisches Medium, um geackte Software auszutauschen, also Software, deren Kopierschutz entfernt worden war.



Abb. 1.3: Mailbox. Quelle: Wikipedia

Gecrackte Programme, die illegal verbreitet werden, werden im Szene-Jargon bis heute als *Ware* bezeichnet. Natürlich waren Mailboxen auch äußerst aktiv an der Verbreitung von Viren beteiligt, genau wie das heute im Internet der Fall ist.

## 1.7 Der BTX-Hack

Eine besondere Form von Mailbox war BTX (Bildschirmtext), ein System, das ähnlich aussah und funktionierte wie Videotext (Teletext), allerdings war es ein interaktiver Onlinedienst, der über das Telefonnetz bereitgestellt und von der Post betrieben wurde. Benutzer konnten zunächst auch nicht ihre eigenen Computer für BTX verwenden, sondern mussten spezielle Endgeräte der Post, sogenannte *BTX-Terminals*, verwenden.

Im November 1984 entdeckten Steffen Wernéry und Wau Holland vom Chaos Computer Club eine Sicherheitslücke im Bildschirmtextsystem (BTX) der Bundespost. Diese Lücke erlaubte es den Angreifern, 134.000 DMark von einer Filiale der Hamburger Sparkasse zu entwenden, wobei dieser Angriff lediglich als Demonstration gedacht war.

Die Angreifer wollten Schwachstellen im Onlinesystem aufdecken und an die Öffentlichkeit bringen, um Banken und ihre Kunden, die BTX verwendeten, zu schützen [Schönherr 1999]. Es war der erste öffentlich bekannte Fall in Deutsch-

land, bei dem es einem Angreifer gelungen war, durch Manipulation eines Online-systems an Geld zu kommen.



Abb. 1.4: Das österreichische BTX-Terminal »mupid«. Quelle: IICM, TU Graz

## 1.8 Das Internet

Die Geschichte des Internets beginnt im Jahr 1957 als Reaktion auf den ersten Satelliten *Sputnik*, den die Sowjetunion in diesem Jahr in eine Erdumlaufbahn schoss. Dieses Ereignis löste in den USA einen regelrechten Schock aus. Als Reaktion wurde die *ARPA* (*Advanced Research Projects Agency*) gegründet, deren Aufgabe es war, neue Technologien im Bereich Kommunikation und Datenübertragung zu entwickeln, um den USA einen technischen Vorsprung gegenüber der UDSSR zu verschaffen. Ein Projekt der ARPA bestand darin, ein überregionales Computernetzwerk, später *ARPANET* genannt, zu errichten.

Es dauerte allerdings noch bis zum Ende der Sechzigerjahre, bis die ersten Computer über das ARPANET kommunizieren konnten und bis in die Siebzigerjahre, bis eine nennenswerte Anzahl an Computern über das ARPANET verbunden waren. Der endgültige Durchbruch gelang dem Internet (das ARPANET wurde zum *Internet*, als sich die ARPA in den Siebzigerjahren von diesem Projekt zurückzog) erst, als es in den Neunzigerjahren für jeden interessierten Benutzer geöffnet wurde. Davor hatte nur ein eingeschränkter Benutzerkreis – vornehmlich Angehörige einiger ausgewählter Universitäten – Zugriff darauf.

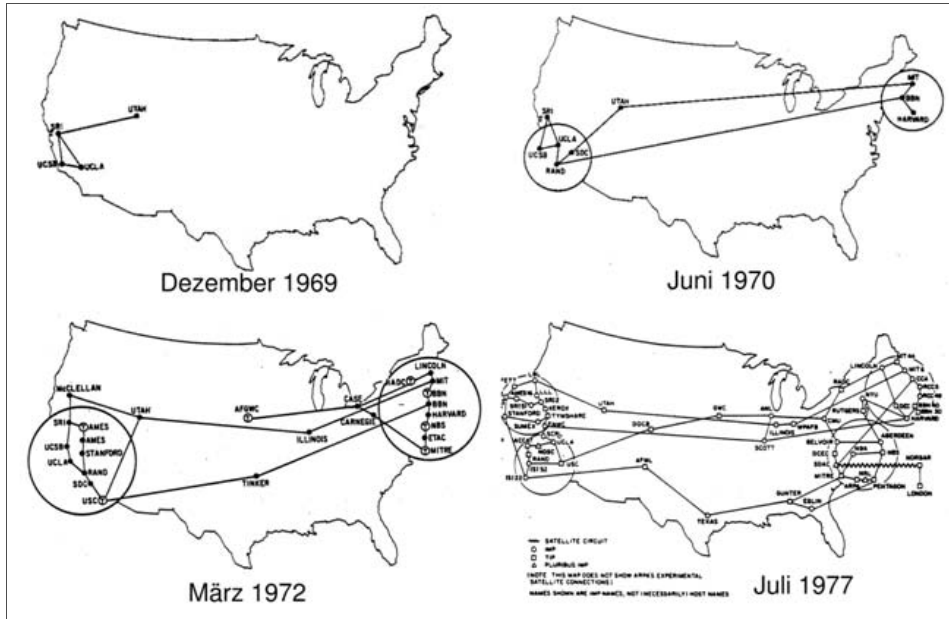


Abb. 1.5: Entwicklung des ARPANET in den USA. Quelle: [linux.fiebel.org](http://linux.fiebel.org)

Dennoch tauchte schon zu dieser Zeit, genauer 1979, die erste Schadsoftware im Internet auf. Es war der *Morris-Wurm*, benannt nach seinem Schöpfer Robert Morris, der schon in den ersten Stunden nach seiner Freisetzung über 6.000 Computer infizierte. Ein Wurm ist im Gegensatz zu einem Virus eine Schadsoftware, die andere Programme für ihre Verbreitung benötigt.

Der Morris-Wurm nutzte zahlreiche Schwachstellen im Betriebssystem UNIX, um sich auf fremden Computern einzunisten und Kopien seines Codes an andere Computer zu verschicken, welche ihrerseits für die weitere Verbreitung des Wurms sorgten [Daswani 2007]. Die Verbreitung über das Internet war naturgemäß um Größenordnungen schneller, als dies durch den Austausch von Disketten möglich gewesen wäre. Der Morris-Wurm war ein Vorgeschmack darauf, was sich

über zwanzig Jahre später während der Massenepidemien, die das ganze Internet bedrohten, geschehen würde.

In den Neunzigerjahren verschwanden die Mailboxen allmählich und gingen im Internet auf. Damit verlagerten sich auch die Hacker-Aktivitäten ins Internet, wodurch die Sicherheit in dem damals neuen Medium erstmals zu einem ernststen Problem wurde.

## 1.9 Vom Wurm zum Bot-Netz

Im Jahr 2001 tauchte ein Wurm namens *Code Red* auf. Er nutzte einen *Pufferüberlauf*, um sich in das Wirtssystem – in diesem Fall Server mit Microsofts Windows NT und laufendem Internet Information Server (IIS) – einzunisten und zu verbreiten. Ein Pufferüberlauf ist eine Schwachstelle, die es einem Angreifer ermöglicht, fremden Code in ein System einzuschleusen und zur Ausführung zu bringen (siehe Kapitel 13).

Das Interessante an diesem Wurm war die Geschwindigkeit, mit der er sich im Internet ausbreitete. In seinen besten Zeiten war es ihm möglich, über 2.000 Server pro Minute im Internet zu infizieren. Ähnlich wie der Morris-Wurm erzeugte auch Code Red ein unheimliches Datenvolumen, welches die reibungsfreie Kommunikation im gesamten Internet bedrohte.

Die Verbreitungsstrategie des Wurms war dabei eigentlich sehr einfach: Er generierte mit einem simplen Algorithmus IP-Adressen und attackierte diese der Reihe nach, bis er ein passendes System fand, in das er sich einnisten konnte. Der Wurm selbst veränderte keine Dateien, er lief lediglich im flüchtigen Speicher des Wirtsrechners. Wurde der Wirtsrechner heruntergefahren und neu gestartet, war der Wurm verschwunden – allerdings dauerte es nicht lange, bis der Rechner wieder infiziert wurde. Der unangenehme Nebeneffekt dieses Verhaltens war, dass Code Red nicht von Antivirus-Software entschärft werden konnte, da diese ja nur Dateimanipulationen erkannten.

Im Gegensatz zum Morris-Wurm verfügte Code Red auch über eine *Schadroutine*. Mit Schadroutine ist jener Teil einer Schadsoftware gemeint, der nicht zur Verbreitung selbst dient, sondern vom Autor gewollte Aktivitäten ausführt. Im Fall von Code Red attackierte diese Schadroutine in einem gewissen Zeitraum (20.-27. des jeweiligen Monats) die Webseite des Weißen Hauses.

Eine Unzahl von infizierten *Zombie-Rechnern* begannen nun alle gleichzeitig, die Server des Weißen Hauses zu attackieren, wodurch dessen Webseite zeitweise nicht mehr erreichbar war (Attacken dieser Art werden *Distributed Denial of Service*- oder DDoS-Attacken genannt).

```
GET /default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090
%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u53
1b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

**Listing 1.1:** Angriffssignatur des Code-Red-Wurms. Der letzte Teil vor HTTP 1.0 ist der eigentliche Schadcode – das Programm default.ida enthielt die Schwachstelle, die attackiert wurde.

In den folgenden Jahren wurde das Internet von weiteren Schadsoftware-Attacken geplagt, die in Wellen darüber hereinbrachen. Die bekanntesten von ihnen waren wohl die Würmer *Nimda*, *Blaster* und *SQL-Slammer*. Nahezu kein Internetdienst (*World Wide Web*, *E-Mail*, zahlreiche anwendungsspezifische Protokolle) wurde von ihnen verschont, um ihre oft epidemische Ausbreitung zu gewährleisten.



**Abb. 1.6:** Der Wurm »Blaster« befahl Rechner mit Windows NT, 2000 und XP über eine Schwachstelle im Windows-RPC-Dienst. Hatte sich der Wurm erst einmal eingeknistet, schaltete er den RPC-Dienst nach einer gewissen Zeit ab, wodurch der Benutzer gezwungen war, den Rechner neu zu starten.

Ihnen allen ist gemein, dass ihre Autoren keine kommerziellen Ziele verfolgten. Vielmehr wollten sie die Öffentlichkeit auf ihre ihrer eigenen Meinung nach über-ragenden technischen Fähigkeiten aufmerksam machen. Das sollte sich jedoch schon bald ändern, als die Verfasser von Schadsoftware herausfanden, wie sich diese zu Geld machen lässt. Dies führte dann zur Entstehung sogenannter *Bot-Netze*.

Der Grundbaustein eines Bot-Netztes ist wiederum eine Schadsoftware (der *Robot* oder kurz *Bot* genannt), die sich automatisch im Internet verbreitet. Zusätzlich lässt sich diese Art Schadsoftware jedoch vom Angreifer direkt fernsteuern. Das gelingt dadurch, dass sich die Schadsoftware nach erfolgreicher Infektion mit einem zentralen Server (*Steuerungsserver* oder *Command and Control Server* genannt) verbindet und fortan dessen Befehle entgegennimmt und ausführt. Das ganze System aus Steuerungsserver und infizierten Computern (*Zombies*) wird Bot-Netz genannt.

Bot-Netze entwickelten sich in den frühen Neunzigerjahren des vorigen Jahrhunderts parallel zur bereits besprochenen Schadsoftware aus sogenannten *Hintertüren* (*Back Doors*). Hierbei handelt es sich um eigene Dienste, die ein Angreifer auf dem übernommenen Server startet, um ihn über das Internet fernsteuern zu können. Ursprünglich tauchten sie in IRC-Netzen auf (der *Internet Relay Chat* ist der Urahn aller Chats sowie der Instant-Messaging-Software wie ICQ, Microsoft Messenger etc.), später verbreiteten sie sich über unterschiedlichste Internetprotokolle und -dienste.

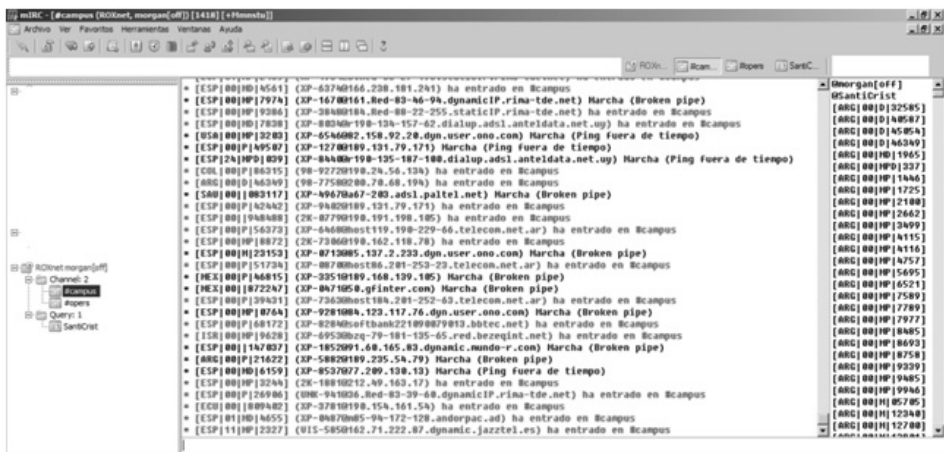


Abb. 1.7: IRC-Kommunikation eines Bots [Ester 2009]

Solche Bot-Netze mit Zigtausenden bis Hunderttausenden Zombies werden heute gegen Entgelt im Internet angeboten. Wie sich diese Netze von den kriminellen »Kunden« wiederum kommerziell verwerten lassen, werden wir in Kapitel 3 noch ausführlicher erläutern.

Eine andere Art, mit Schadsoftware Geld zu verdienen, ist die Verbreitung von Software, die Zugangsdaten ausspäht wie der Trojaner *Zeus* [Westmoreland 2010] (ein *Trojaner* ist eine Schadsoftware, die sich als nützliches Programm tarnt, aber unbemerkt vom Benutzer eine andere Funktion ausführt) oder die sogenannte *Scareware* auf infizierten Rechnern installiert, die dem Benutzer einen Virenbefall

vorgaukelt, um ihn dazu zu bringen, die Vollversion eines vermeintlichen Viren-scanners käuflich zu erwerben. Wir werden uns im Abschnitt 1.10 noch näher mit diesem Thema beschäftigen. Den bekanntesten Fall dieser Art von Schadsoftware stellte wohl der *Conficker-Wurm* dar [Ziegler 2009].

Nachdem er im Oktober 2008 erstmals aufgetaucht war, verbreitete er sich in Windeseile im gesamten Internet. Millionen von PCs und Servern wurden infiziert, darunter auch solche von Krankenhäusern und militärischen Einrichtungen. Lange wurde gerätselt, welchen Zweck seine Schöpfer mit ihm verfolgen, bis er im April 2009 schließlich begann, das Scareware-Programm *SpywareProtect2009* (siehe Abschnitt 1.10.3) auf den infizierten Rechnern zu installieren.



Abb. 1.8: Scareware »SpywareProtect2009«, welche vom Conficker-Wurm verbreitet wurde

## 1.10 Social Engineering

Bisher wurden vornehmlich Verfahren erörtert, mit denen Computer zu kriminellen Zwecken missbraucht werden. Es ist jedoch auch möglich, Menschen derart zu täuschen, dass sie sich für kriminelle Aktivitäten missbrauchen lassen, ohne dass ihnen das bewusst ist. Diese Art der Täuschung ist älter als die Menschheit selbst. In der Tier- und Pflanzenwelt und sogar bei Einzellern und Bakterien sind Täuschungen weit verbreitet.

Sind Menschen das Ziel dieser Täuschungen, spricht man meist von *Social Engineering*.

Hier ist anzumerken, dass der Begriff Social Engineering im Englischen unterschiedliche Bedeutungen haben kann. In Wikipedia ist der Begriff wie folgt definiert:

- Social Engineering (Politikwissenschaft), Anstrengungen zur Veränderung oder Verbesserung gesellschaftlicher Strukturen.
- Social Engineering (Sicherheit), zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Informationen oder technische Infrastrukturen zu gelangen.

Wir beziehen uns in diesem Buch lediglich auf die Bedeutung im Zusammenhang mit *Sicherheit*, dabei kann ich mir allerdings nicht verkneifen, auf die Ironie hinzuweisen, die sich aus der Gleichsetzung von *Politikwissenschaft* und *Täuschung* ergibt.

Das Telefon und erst recht vernetzte Computer machen Täuschungen relativ einfach, da die Identität und die Absichten von Kommunikationspartnern viel schwieriger auszumachen sind, als wenn sich Täter und Opfer physisch gegenüberstehen. Hacker können sich zu Computersystemen Zugang verschaffen, indem sie Schwachstellen in Software gezielt ausnutzen; es ist allerdings oft einfacher, Menschen dazu zu bewegen, Zugangsdaten zu verraten oder Zugänge zu schaffen. Kriminelle nutzen dabei oft den Umstand aus, dass Menschen von Natur aus hilfsbereit sind. So reicht oft ein vorgetäuschter Anruf eines vermeintlich neuen Mitarbeiters aus, um beispielsweise Administratoren dazu zu bringen, Zugangsdaten preiszugeben.

Eine inzwischen weit verbreitete Art der Täuschung sind automatisch versendete E-Mails, die die Opfer veranlassen sollen, dem Täter in irgendeiner Form Geld zukommen zu lassen. Der Grund, warum diese Art von Attacken funktioniert, ist der Umstand, dass es mithilfe des Internets so einfach ist, große Mengen an E-Mails automatisiert zu verschicken. Es genügt häufig, dass weniger als ein Prozent der Benutzer auf den Schwindel hereinfallen, um dem Täter ein nicht unbedeutendes Einkommen zu sichern.

### 1.10.1 Spam- oder Junk-Mails

*Spam-* oder *Junk-Mails* sind unerwünschte Werbe-E-Mails, die in Massen versendet werden. Die Bezeichnung *Spam* ist im Gegensatz zu *Junk* (englisches Wort für Abfall oder Plunder) etwas irreführend, da dies ursprünglich eine Marke für Dosenfleisch war (*SPiced hAM*). Erst der Spam-Sketch der englischen Comedy-Serie Monty Python's Flying Circus, in dem das Wort *Spam* 132 Mal vorkommt, verhalf diesen Werbe-E-Mails zu ihrem Namen.

Mittlerweile machen Spam-Mails den Großteil der weltweit versendeten E-Mails aus. Kunden von Spam-Produzenten (Spammer) sind oft dubiose Händler von

gefälschten Arzneimittelprodukten. Spam-Mails werden auch dazu verwendet, den Preis für gewisse Aktien hochzutreiben. Es ist dabei wichtig zu verstehen, dass Spammer professionell agierende Individuen oder Gruppen sind, die ihre Dienste offen im Internet anbieten.

Get HYWI First Thing on Monday, This stock Going To Explode for at least 30%

Check out for Hot News!

Hollywood Intermediate, Inc.

Symbol: H Y W I - H Y W I - H Y W I - H Y W I - H Y W I - H Y W I

Current price: \$1.30 , but will increase at least 20-25 % on Monday!

About the company:

Hollywood Intermediate provides a proprietary technology of Digital Intermediate services to feature filmmakers for post-production for film mastering and restoration. This technology gives the filmmakers total creative control over the look of their productions. Whether shooting on film or acquiring in HD or SD video, Hollywood Intermediate puts a powerful cluster of digital tools at the director's disposal to achieve stunning results on the big screen. Matchframe Digital Intermediate, a division of Hollywood Intermediate, Inc., packages a full array of post-production services with negative handling expertise and cost-effective 2K digital intermediate and 35mm film out systems. stock purchase recommendations and short term trading tips stock coverage highlighting booming markets The Digital Intermediate process eliminates current post-production redundancies by creating a single high-resolution master file from which all versions can be made, including all theatrical and H!

High Definition formats. By creating a single master file with resolution higher than the current High Definition broadcast standards, the DI master file enables cinema and television distributors to extract and archive all current and future cinema and television formats including Digital Cinema, Television and High Definition. Improve your yearly gains with expert stock advice Premium stock recommendation services to

to allow earning more

Don't forget to include this stock to your bag!

Mutual benefit by reliable stock information stock recommendation boosting stock performance

Read great news on this stock

Beauty without grace is like a hook without bait. . April is the cruellest month You have to be in it to win it The older the fiddler, the sweeter the tune. A person who can smile when things go wrong has found someone to blame it on. Wherever you may be let your wind go free A gentle heart is tied with an easy thread.

Blood is thicker than water The longest rope has an end

One good turn deserves half the blankets If Wishes Were Horses, Beggars Would Ride A penny always turns up. A soft answer turneth away wrath. Little Strokes Fell Great Oaks

Is better to light a candle than to curse the darkness A man is known by the company he keeps. Good broth may be made in an old pot Virtues all agree, but vices fight one another There are always ears on the other side of the wall Don't bite the hand that.. looks dirty.

**Listing 1.2:** Beispiel für eine typische Spam-Mail, welche für eine Aktie wirbt. Die Tippfehler sind beabsichtigt. Sie dienen dazu, Spam-Filter zu verwirren.

Spam-Aktivitäten beschränken sich mittlerweile nicht mehr nur auf E-Mails. Inzwischen werden auch auf Webseiten, die Benutzer mitgestalten können (Foren, Blogs, Wikis, Newsgroups etc.), automatisiert Spam-Nachrichten platziert.

### 1.10.2 Verbreitung von Phishing-Mails

*Phishing* ist ein Kunstwort, das aus den Worten *Password* und *Fishing* zusammengesetzt ist. Es geht dabei – wie der Name vermuten lässt – darum, arglose Benutzer solcherart zu täuschen, dass sie beispielsweise Benutzerdaten an einer Stelle angeben, wo sie eigentlich nicht hingehören. Damit ist es einem Angreifer beispielsweise möglich, den Benutzer ohne sein Wissen dazu zu bringen, Geldbeträge mittels Telebanking auf das Konto des Angreifers zu überweisen.

Zu diesem Zweck bekommt er zum Beispiel eine E-Mail mit der Aufforderung, seine Zugangsdaten über einen in die E-Mail eingebetteten Link zu ändern. Geht der Benutzer auf diese Aufforderung ein, wird er nicht auf die Seite der Bank, sondern auf eine speziell präparierte Seite des Angreifers verwiesen. Dieser braucht dann nur noch zu warten, bis arglose Benutzer ihre Zugangsdaten bei ihm eingeben.

Banken sind zwar inzwischen vorsichtig geworden und fordern den Kunden auf, eine TAN (Abkürzung für *Transaktionsnummer*) für jede Transaktion einzugeben. Es hat jedoch nicht lange gedauert, bis Angreifer diesen Sicherheitsmechanismus umgangen hatten. Leider wurden auch schon die Nachfolgeverfahren iTAN und das jüngere mTAN-Verfahren, welches das Mobiltelefon als vermeintlich sicheren Weg für die Übertragung von TANs benutzt, erfolgreich umgangen [Bachfeld 2005] [Kirsch 2009].



Abb. 1.9: Phishing-Mail. Quelle: Wikipedia

Leider machen es viele Unternehmen Phishern leicht, Benutzer in die Irre zu führen, indem sie selbst E-Mails verschicken, die nur äußerst schwierig von Phishing-Mails zu unterscheiden sind. Das hat folgende Gründe:

- Die Unternehmen beauftragen externe Dienstleister, in ihrem Namen E-Mails zu verschicken, weshalb die E-Mails dann nicht von der eigentlichen Firma kommen, sondern von einem Dienstleister, der aber seinerseits dem Benutzer nicht bekannt ist.
- Die Unternehmen verschicken selbst HTML-E-Mails mit zahlreichen Links darin – genauso, wie das auch Phisher tun.

Sie können Ihre eigenen Fähigkeiten zur Erkennung von Phishing-Mails mithilfe des Quiz von SonicWall (<http://www.sonicwall.com/phishing/>) testen. Darüber hinaus gibt es auch ein Trainingsprogramm namens *Anti-Phishing Phil*, mit dem man das Erkennen von Phishing-Mails spielerisch erlernen kann ([http://cups.cs.cmu.edu/antiphishing\\_phil/](http://cups.cs.cmu.edu/antiphishing_phil/)).

### 1.10.3 Scareware

Mit *Scareware* (zu Deutsch etwa »Schrecksoftware«) werden Programme bezeichnet, die Benutzern einen Virenbefall vortäuschen und sie dazu auffordert, die Vollversion eines vermeintlichen Virenschanners käuflich zu erwerben. Scareware ist

so erfolgreich, dass sich inzwischen eine Art von Industrie rund um die Herstellung und Verbreitung dieser Programme etabliert hat.

Damit Scareware funktioniert, muss natürlich der Benutzer mitspielen, aber wie im Fall von Phishing-Mails genügt es, wenn nur ein geringer Prozentsatz darauf hereinfällt, um dem »Hersteller« lukrative Einnahmen zu bescheren.

## 1.11 Die Schattenwirtschaft im Internet

Zweifelsohne war die Globalisierung ein treibender Faktor für das Wachstum der Weltwirtschaft in den letzten Jahrzehnten. Noch stärker als dieses Wachstum war jedoch das Wachstum der globalisierten Schattenwirtschaft. Das jährliche Wachstum der Schattenwirtschaft entsprach im Jahr 2008 wahrscheinlich dem Doppelten des Wachstums der *regulären* Wirtschaft [Gilman 2009].

Die Internetkriminalität ist inzwischen ein fester Bestandteil dieser Schattenwirtschaft. Mit ihr werden heute 10 bis 80 Milliarden US-Dollar weltweit illegal eingenommen. Waren es in der Anfangszeit der Informationstechnologie noch technisch versierte Einzeltäter, die ihre technische Überlegenheit demonstrieren wollten, sind heute lose Netzwerke von Kriminellen mit vornehmlich wirtschaftlichen Interessen für die meisten illegalen Aktivitäten verantwortlich.

Dieser Wandel hat unterschiedliche Ursachen. Eine davon ist sicher der Umstand, dass Programmierer in vielen Ländern mit illegalen Aktivitäten um Größenordnungen mehr verdienen können als mit legaler Programmierertätigkeit. Auch sorgen unterschiedliche nationale Gesetzgebungen dafür, dass es äußerst schwierig ist, Internet-Kriminelle aus gewissen Ländern vor Gericht zu bekommen. Im Zusammenhang mit diesen kriminellen Netzwerken wird oft der Begriff *organisierte Kriminalität* genannt.

Hier gilt es jedoch, einem Missverständnis vorzubeugen: Diese Netzwerke sind nicht wie die Mafia organisiert (auch wenn Mafia-Organisationen sicher auch hier ihre Hand im Spiel haben), wie man sie im Film *Der Pate* (Francis Ford Coppola, 1972) beschrieben bekommt. Es gibt gar keinen Paten. Die Beteiligten kennen sich nicht einmal persönlich. Vielmehr dient das Internet als Marktplatz für kriminelle Produkte und Dienstleistungen [Holz 2008].

Es gibt Marktteilnehmer, die zum Beispiel Kreditkartendaten entwenden und diese zum Kauf anbieten. Andere Teilnehmer sorgen dafür, dass mit den Kreditkartendaten illegale Zahlungen durchgeführt werden und dass das Geld auf den Konten der Kriminellen ankommt. Handelt es sich um physische Produkte, müssen diese natürlich ebenfalls irgendwie in den Besitz des Kriminellen gelangen.

Er wäre natürlich äußerst unvorsichtig, wenn er sich diese Produkte an seine eigene Heimatadresse schicken ließe, deshalb bedient er sich Anbietern sogenannter *Drop-Zones*. Das sind Personen in anderen Ländern, die gegen ein gewis-

ses Entgelt Waren entgegennehmen und an den eigentlichen Adressaten weiterschicken. Der Leidtragende ist dann in der Regel der Händler des Internet-Shops, in dem der Kriminelle eingekauft hat, denn er wird weder die Ware noch das Geld jemals zurückbekommen.



Abb. 1.10: Webshop für Kreditkarten, PayPal-Accounts und vieles mehr

## 1.12 Aktivitäten von Geheimdiensten im Internet

Nach dem Ende des kalten Krieges standen viele Länder mit einem aufgeblähten Geheimdienstapparat da, für den sie vorerst keine Verwendung mehr hatten. Es fand sich aber schon bald ein neues Betätigungsfeld: die *Industriespionage*. In vielen Ländern ist es Geheimdiensten nicht nur erlaubt, Betriebsgeheimnisse von ausländischen Firmen auszuspähen, sie sind auch explizit beauftragt, nicht nur Spionageaktivitäten anderer Länder abzuwehren, sondern der heimischen Wirtschaft durch ihre Aktivitäten, die im betroffenen Land natürlich als illegal angesehen werden, einen Vorteil zu verschaffen.

Für diese Art der Informationsbeschaffung bot es sich natürlich an, das Internet zu verwenden. Das ist in der Regel günstiger, da man nicht erst Mitarbeiter des auszuspionierenden Unternehmens mit Geld dazu überreden muss, Betriebsgeheimnisse zu verraten. Auch kommt man schneller zu Ergebnissen.

Für diese Art von Spionage wird häufig Schadsoftware speziell auf das auszuspiönierende Unternehmen zugeschnitten. Diese Programme verhalten sich meist extrem unauffällig. Sie versuchen, sich möglichst in alle Computer einzuschleusen und warten dann auf spezielle Informationen, die sie nach außen weiterleiten. Als Übertragungsweg sind übrigens auch wieder Speichermedien in Mode, wie das in den Achtzigerjahren weit verbreitet war.

Diesmal handelt es sich allerdings nicht um Disketten, sondern um USB-Sticks. Das hat natürlich einen guten Grund: Speziell größere Unternehmen verwenden Spam-Filter, um mit Schadcode infizierte E-Mails auszusondern. Auch trennen sie vom Internet her erreichbare Webserver bis zu einem gewissen Grad von internen Netzen, weshalb dieser Weg für die Angreifer oft umständlicher ist, als USB-Sticks in die Firma einzuschmuggeln. In einem solchen Fall (der allerdings nicht an die Öffentlichkeit gelangte) bestellte eine Firma zu Werbezwecken USB-Sticks aus China und verteilte diese an ihre Kunden. Diese Sticks waren mit Schadsoftware infiziert, die speziell darauf programmiert wurde, interne Informationen weiterzugeben (sogenannte *Spyware*).

Diese Verwendung von USB-Sticks als bevorzugtem Übertragungsweg kann sich jedoch rasch wieder ändern; beispielsweise wenn die Firmen reagieren und USB-Ports deaktivieren, wenn Angreifer neue Angriffskanäle, wie beispielsweise Mobiltelefone, entdecken oder neue Angriffstechniken für »alte« Angriffskanäle wie das Internet finden. Geheimdienste gehen bei ihren Aktivitäten in der Regel so vor, dass ihre Urheberschaft nicht entdeckt werden kann. Die einfachste Möglichkeit ist, Hacker anzuheuern und für entsprechende Aktivitäten zu bezahlen.

Fliegt die Sache auf, glaubt die Öffentlichkeit, es handle sich beispielsweise um Studenten, die ihre technischen Fähigkeiten unter Beweis stellen wollen. Es liegt in der Natur digital gespeicherter Informationen, dass sich ihr Urheber nicht nachweisen lässt, wenn er nicht irgendwo in den Informationen Hinweise auf seine Urheberschaft hinterlässt – ganz im Unterschied zu einem Brief zum Beispiel. Hier finden sich zahllose Spuren wie Fingerabdrücke, DNA-Spuren, die Handschrift oder der verwendete Drucker, chemische Spuren, die Art und Beschaffenheit des Papiers und so weiter. Deshalb ist es für Behörden auch besonders schwierig, die tatsächliche Urheberschaft von Schadsoftware nachzuweisen – zumindest wenn der Urheber dafür sorgt, dass er keine Spuren hinterlässt.

Angriffe dieser Art sind besonders heimtückisch, da man es sozusagen mit der Elite der Hacker zu tun hat. Inwieweit eine Organisation Ziel solcher Angriffe sein kann, ist äußerst schwer zu sagen, da man ja nicht weiß, auf welche Informationen genau es die Geheimdienste abgesehen haben. Es passiert allerdings nicht selten, dass, wenn ein Hersteller in unseren Breiten ein neues Produkt herausbringt, plötzlich ein nahezu identisches Modell aus Fernost auftaucht. Natürlich haben Betroffene kein gesteigertes Interesse daran, dass diese Vorfälle an die Öffentlichkeit gelangen; den Behörden zufolge treten sie allerdings in zunehmenden Maße auf.