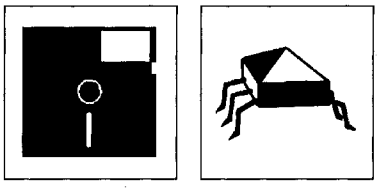


Viren und Internet

Fridrik Skúlason

Dieser Artikel beschäftigt sich mit dem gegenwärtigen Zustand der Virus-Verteilung im Internet. Er betrachtet verschiedene Methoden der Verteilung, gefolgt von einer Analyse, wie das Internet dazu verwendet wird, Anti-Virus Software und Virus-Informationen bereitzustellen.

Einleitung
Ich beginne mit zwei grundsätzlichen Annahmen:

Zwei Grundannahmen

1. Die unkontrollierte Verteilung von Computer-Viren ist unerwünscht.
"Unerwünscht" bedeutet nicht "illegal", obwohl dies auf manche Länder sicherlich zutrifft. Auf jeden Fall ist die Verteilung sowohl unmoralisch als auch unverantwortlich. Das gleiche gilt für die Verteilung ähnlicher Gegenstände, wie z.B. von Viren-Quellcode und von Informationsschriften über die Herstellung von Viren.

2. Die Verteilung von Anti-Virus-Programmen und zuverlässigen Informationen über Viren ist wünschenswert und sollte gefördert werden.
Es gibt verschiedene "Grauzonen": Die Beschreibung von Virus-Techniken, besonders von neuen und fortentwickelten, könnten für die Hersteller von Viren wie auch für das beabsichtigte Publikum nützlich sein. Eine andere "Grauzone" besteht im Austausch von Virus-Material zwischen legitimierten Forschern und Anti-Virus-Entwicklern über das Internet.
Diese beiden Grundannahmen sollten bei der Lektüre dieses Artikels stets präsent sein.

Das Internet und der "Anarchie-Faktor"

Ich betrachte das Internet als ein Medium, das Leute dazu in die Lage versetzt, Informationen auszutauschen und dies in einer schnellen und effektiven Weise – funktional ähnlich dem Telefon, postalischen oder Amateurradiosystemen; es kann als solches dazu verwendet werden, nützliche Informationen zu verteilen und Unterstützung zu gewähren. Es kann auch dazu mißbraucht werden, bösartige Propaganda und anderes "unerwünschtes" Material zu verteilen.
Aus dieser Perspektive betrachtet, besteht ein bedeutender Unterschied zwischen dem Internet und ähnlichen Medien, den ich den "Anarchie-Faktor" nenne. Dem Internet fehlt eine gewisse Autorität, ein "code of conduct", und in den meisten Ländern haben die Rechtssysteme kaum Erfahrung mit "Cyberspace".
Mit anderen Worten, weil eine Autorität fehlt, die den Leuten sagen würde, was im Internet erlaubt ist, kommt es dazu, daß man macht, was man will. In den meisten Fällen, tatsächlich in den allermeisten Fällen, ist das kein Problem. Die meisten Leute neigen gewöhnlich dazu, sich verantwortungsvoll zu verhalten. Die Betonung liegt hier auf "die meisten". Es gibt aber immer einige Personen, die jede Freiheit oder jeden Spielraum für ihren eigenen Profit oder Vorteil mißbrauchen, ungeachtet aller Nachteile oder Schäden für andere.
Das Internet ist da keine Ausnahme.
Trotz der allgemeinen Übereinstimmung, daß Computer-Viren schädlich sind und eine Verschwendung von Zeit und Ressourcen darstellen, nimmt ihre Verteilung im Internet in immer schnellerem Tempo zu.

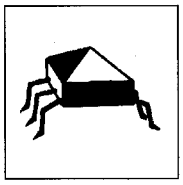
Virenverteilung im Internet

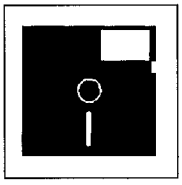
Verteilmedien

Die unkontrollierte Verteilung von Computer-Viren und ähnlichem Material spielt sich im Internet in verschiedenen Formen ab. Zu nennen sind:

- Dedizierte FTP-Rechner
- Reguläre Internet-Provider
- Alt.comp.virus
- Der Kaos4-Vorfall
- Mailing-Listen
- Internet Relay Chat (IRC)

Fridrik Skúlason ist Autor des Virenschutzprogramms F-Prot.





Dedizierte FTP-Rechner

So viel ich weiß, gibt es nur zwei Rechner im Internet, die direkt von virus-schreibenden Organisationen betrieben werden: Nuke und Phatcom/Skism.

Glücklicherweise bieten diese Rechner keine große Virus-Sammlung an – wenigstens nicht zu dem Zeitpunkt, in dem die Viren geschrieben werden, aber sie bieten doch Material an, das zur Virusentwicklung in Beziehung steht.

Der Kooperationsvorsprung der Virus-Entwickler

Diese Rechner sind gegenwärtig kein großes Problem. Sie sind außerhalb der virusschreibenden Gemeinschaft nicht weit bekannt, aber ihre Gegenwart erinnert daran, daß in gewisser Hinsicht die Virusentwickler besser organisiert sind und stärker kooperieren als die Anti-Virus Industrie.

Diese Rechner scheinen gegennwärtig in ihren Aktivitäten zu expandieren, einschließlich der Einrichtung eines WWW-Servers. Mir ist nicht ganz klar, warum die Manager dieser beiden Rechner nicht mehr Reklame machen und mehr Virus-Material anbieten als zur Zeit. Es ist offensichtlich, daß die gegenwärtigen Gesetze – um das mindeste zu sagen – ineffektiv sind.

Reguläre Internet-Provider

Einige Anbieter von Internet-Zugängen stellen die Bedingung, daß auf ihren Rechnern die Verteilung bestimmten Materials nicht erlaubt ist. Dies umfaßt normalerweise illegales Material, wie z.B. raubkopierte Software, in einigen Fällen Pornographie und zum Haß aufstachelndes Material, wie neo-nazistische Propaganda. In manchen Fällen wird dieser Bann auch auf Computer-Viren ausgedehnt.

Zunehmend: Provider-Passivität

Es ist jedoch mehr als üblich geworden, daß Anbieter sich weigern, etwas zu unternehmen, wenn ihre Kunden Viren ohne jede Einschränkung verteilen. Selbst auf den Hinweis, daß entweder Virus-Quellcode zu "Newsgroups" gepostet wurde oder Viren via FTP zur Verfügung gestellt wurden, wird mit der Bemerkung geantwortet, daß man in keiner Weise eingreifen wolle – Virus-Verteilung sei vollständig legal. Bis sich das ändere, wollten sie nichts unternehmen.

Es mag legal sein, zumindest in einigen Teilen der Welt, aber was mich betrifft, so finde ich diese Einstellung unmoralisch und unverantwortlich.

Kommerz vor Moral

Wie auch immer, es scheint, daß moralisches und verantwortliches Verhalten offenbar weniger wichtig ist, als die Möglichkeit, Gewinn zu erzielen, indem man den Virus am Leben läßt – für die Virusentwickler und ihre Unterstützer (als Kunden).

Die traurige Tatsache ist die, daß absolut kein Druck auf Netcom.com, Kaiwan.com oder andere Internet-Provider ausgeübt wird, die gegenwärtige Virusverteilung zu stoppen. Es scheint aus schwer zu verstehenden Gründen so zu sein, daß die Virus-Verteilung von der Geschäftswelt und der allgemeinen Nutzergemeinschaft nicht als ein Problem betrachtet wird.

Tatsächlich stellt sich die Situation sogar als das genaue Gegenteil dar – man denke z.B. an die sehr große Zahl verkaufter Exemplare der Mark Ludwig CD-ROM.

Ich habe versucht, gegen die unkontrollierte Verteilung von Viren zu kämpfen, aber irgendwie habe ich das Gefühl, auf einem Ein-Mann-Kreuzzug zu sein. Trotzdem werde ich den Kampf weiterführen, und im Falle von Netcom (oben als Beispiel angeführt) und einigen anderen Anbietern, habe ich einige Schritte eingeleitet. Ich werde damit anderen vergleichbaren Anwendern gegenüber fortfahren.

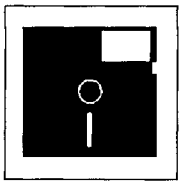
Gegenmaßnahmen

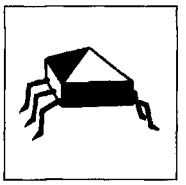
1. Ich fordere insbesondere die auf, die mit der Computer-Sicherheitsindustrie in Beziehung stehen, ihre Ablehnung auszudrücken, und jeglichen möglicherweise bestehenden Netcom-Account zu kündigen.

2. Ich verweigere Netcom-Kunden Zugang zu meinem Rechner, meinem (bald freigegebenem) WWW-Server und meinem automatischen Anti-Virus E-Mail Service. Jede Anfrage von Netcom-Kunden wird mit dem Standard-Satz beantwortet, daß wir Verbindungen von Servern ablehnen, die Viren transportieren.

3. Ich füge jeder E-mail Korrespondenz mit Netcom-Kunden eine Bemerkung hinzu, die die Situation erklärt und erläutert, warum sie zu unseren Diensten nicht zugelassen sind.

4. Die Verteilung meines Anti-Virus Programms ist auf Netcom-Maschinen strikt untersagt. Das gleiche gilt für jeden anderen Rechner, der Viren und gefährliches Zusatzmaterial zur Verfügung stellt.





Die einzige Wirkung, die diese Aktionen eventuell haben, ist der Verlust einiger Geschäfte, aber damit habe ich wenigstens meine Position klar gemacht.

Alt.comp.virus

Dies ist eine Newsgroup, die sich anscheinend speziell zu dem Zwecke gebildet hat, Viren und ähnliches Material zu verteilen. Ich habe nur einen Bruchteil von dem Material gesehen, das an diese Newsgroup geschickt wurde, und zwar aus dem einfachen Grunde, weil sie in Island nicht verteilt wird. Das wenige, das ich gesehen habe, macht den Eindruck, daß es sich bei einem großen Teil der Virus-Schreiber um inkompetente Dummköpfe handelt. Wie auch immer, selbst wenn alt.comp.virus keine weit verteilte Newsgroup ist, bewirkt sie doch zwei große Probleme. Das eine Problem ist offensichtlich, das andere nicht.

Die Multiplikationswirkung (auch für "Laien")

Das erste Problem besteht darin, daß anders als bei der FTP-Verteilung, wo die Nutzer aktiv Viren suchen müssen, Newsgroup-Verteilung bedeutet, daß der Nutzer die Viren ohne Anfrage erhält. Mit anderen Worten dürfte das bedeuten, daß eine große Anzahl von Viren in der Hand von Leuten landet, die nicht die leiseste Idee davon haben, wie sie sie sonst auf andere Weise erhalten könnten. Diese Leute können dann entweder fahrlässig oder vorsätzlich diesen Virus weitergeben.

Der Vorsprung der unmoderierten Newsgroup

Das andere Problem besteht darin, daß vom Namen her "alt.comp.virus" nicht offensichtlich ist, daß es sich dabei um eine hauptsächlich virus-verteilende Newsgroup handelt, so daß sich eventuell Leute mit Virus-bezogenen Fragen mit der Bitte um Hilfe an diese Newsgroup wenden. Sie mögen natürlich auch zur gleichen Zeit eine Nachricht an "comp.virus" adressieren, aber anders als bei "alt.comp.virus" wird diese Newsgroup moderiert, so daß die Antwort erst später erfolgt.

Was mir Sorge macht ist, daß – betrachtet man die durchschnittliche technische Qualität der Nachrichten an "alt.comp.virus" – jede Erwiderung auf tatsächliche Probleme unvollständig, ungenau oder regelrecht schädlich sein kann.

Der Kaos4-Vorfall

Dieser Vorfall wurde dadurch ausgelöst, daß ein infiziertes Programm an eine weit verbreitete Newsgroup gesandt wurde. Das könnte ein Zufall gewesen sein, aber es gibt einige Indizien, die darauf schließen lassen, daß es sich um einen vorsätzlichen Versuch handelte, den Virus zu verteilen.

Drei Indizien für den strategischen Hintergrund

Erstens handelte es sich bei dem fraglichen Virus um einen neuen, vorher noch nie gesehenen Virus. Er war zudem sehr primitiv, und es war unwahrscheinlich, daß er sich ohne irgendwelche unterstützende Maßnahmen weit verbreiten würde. Deshalb ist es unwahrscheinlich, daß das gesendete Programm während einer "normalen" zufälligen Infektion infiziert wurde.

Zweitens war die sexbezogene Newsgroup, zu der das infizierte Programm gesendet wurde, wohl ausgesucht worden, um den Versuch zu erschweren, dem Virus auf die Spur zu kommen. Als die ersten Berichte der Kaos4-Infektion erschienen, wußte man nicht, woher der Virus kam. Einige Tage vergingen, bevor es möglich wurde, berichteten Vorfällen zu diesem speziellen Posting nachzugehen. Einige von diesen so infizierten erschienen nicht besonders begeistert, zugegeben zu müssen, daß sie ein Programm dieser sexbezogenen Newsgroup gestartet hatten.

Drittens gibt es einige Hinweise, daß der Sender des infizierten Programms, dieselbe Person war wie der Autor des Virus, der sich selber "Köhntark" nennt.

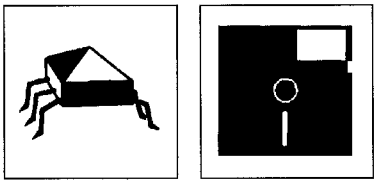
Alles in allem stellte sich heraus, daß dieser Vorfall nur Anlaß für mäßige Unruhe sein mußte. Trotzdem hätte es viel schlimmer kommen können. Wenn der Virus weiter entwikkelt gewesen wäre, wenn es sich z.B. um einen ganz neuen und hoch polymorphen Stealth-Virus gehandelt hätte, dann hätte dies zu einer großen Epidemie führen können, anstatt zu einigen isolierten Vorfällen, die man schnell in den Griff bekommen hat.

Dies war nicht der erste Fall eines infizierten Programms, das zu einer Newsgroup gesendet wurde und wird wahrscheinlich auch nicht der letzte sein. Wir können nur hoffen, daß künftige Vorfälle genauso schnell und einfach behoben werden können, wie dieser.

Mailing-Listen

Genaues weiß man nicht.

Es gibt wahrscheinlich verschiedene geschlossene Mailing-Listen von Virus-Schreibern, aber man weiß nichts Sicheres darüber. Die meisten von den bekannten Virus-schreibenden Gruppen begannen in der Mailbox-Szene und sind wahrscheinlich bis jetzt noch nicht vollständig in die traditionellen Internet-Wege der Kommunikation integriert.



Kein bedeutsamer Faktor.

Internet Relay Chat (IRC)
Der letzte und gegenwärtig am wenigsten bedeutsame Weg, Virus-Material im Internet zu verteilen, geschieht durch IRC-Systeme. In der Vergangenheit gab es einige Virus "mailing bots". Der Großteil der Aktivität dort besteht aber im "chat" (vielleicht verbunden mit der Aufforderung, Viren zu übersenden). Jedenfalls hat, soweit festgestellt werden konnte, das IRC keine entscheidenden Auswirkungen im Sinne des hier betrachteten Problems.

Die Anti-Virus Koalition und das Internet

Gerade als die Virus-Schreiber in der Mailbox-Szene aktiv waren, fand sich die Anti-Virus Koalition bei CompuServe und anderen Online-Diensten zusammen. Dieser Artikel beschäftigt sich jedoch nur mit dem Internet, wo beide Gruppen zu einem großen Anteil die gleichen Methoden und Ressourcen verwenden.
Die Anti-Virus Koalition nutzt das Internet hauptsächlich für drei verschiedene Zwecke.

- Verteilung von Anti-Virus Software
- Produkt-Unterstützung
- Verteilung zuverlässiger Virus-Informationen

Die am meisten genutzten Kanäle sind die folgenden:

- FTP-Dienste
- WWW-Server
- Usenet Newsgroups
- E-mail

FTP-Dienste
Heute gibt es einige Stellen, die dazu bestimmt sind, Anti-Virus Software und ähnliches Material zu verteilen. Einige dieser Dienste werden von Anti-Virus Entwicklern betrieben und bieten nur deren eigene Software an, während andere alle frei verteilbaren Anti-Virus Programme und darauf bezogenes Material vorhalten.
Der größte Nutzen der von Herstellern betriebenen Dienste besteht darin, daß man Originalversionen der Programme erhält, man sich also keine Sorgen über trojanische Versionen machen muß.

oak.oakland.edu
garbo.uwase.fi

Zusätzlich zu diesen ausgewiesenen Anti-Virus Stellen, haben die meisten größeren FTP-Dienste (wie z.B. oak.oakland.edu und garbo.uwase.fi) besondere Abteilungen für Anti-Virus Material. Einige dieser Stellen sind fast so sicher wie die Verkaufsstellen der Autoren, da die betreffende Software direkt von den Autoren eingespielt wird.

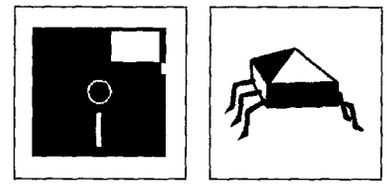
Das Problem des Altmaterials

Da ist nur ein Problem. Diese Stellen haben zwar eine große Sammlung von Anti-Virus Programmen, aber die meisten dieser Sammlungen bestehen aus altem und uneffektivem Material. Es scheint, als ob diese Software niemals zum angemessenen Zeitpunkt von diesen Stellen entfernt worden sei, woraus eine Mülleimer füllende Virus-Abteilung entstanden ist. Diese unnützen Programme schaden mehr als daß sie nutzen, weil sie den Anwender in falscher Sicherheit wiegen. Was hier nötig ist, ist ein gründliches Aufräumen, aber die Verwalter dieser Stellen sind keine Virus-Experten und die meisten der qualifizierten Leute arbeiten für die Anti-Virus Entwickler, so daß man ihnen Interessenkollision vorwerfen könnte, wenn sie daran gingen, die Programme nach "nutzlos" und "nützlich" zu klassifizieren.

WWW-Server
Bis jetzt gibt es nur wenige WWW-Server, die Anti-Virus bezogenes Material anbieten, aber ihre Zahl wird bestimmt – mit der Popularität des WWW – in naher Zukunft steigen. Folgendes Material ist dort gegenwärtig verfügbar:

1. Virus-Information
2. Anti-Virus Produkt Informationen
3. Der comp.virus FAQ und ähnliches Material

Alles läßt darauf schließen, daß wahrscheinlich im Internet auf dem WWW die Anti-Virus Aktivität in naher Zukunft am stärksten zunehmen wird.



Die frühen Tage von comp.virus ...

Usenet Newsgroups

1989 war die comp.virus Newsgroup die wichtigste Quelle, die der Anti-Virus Koalition im Internet zur Verfügung stand. Diese Situation hat sich heute geändert.

In den frühen Tagen waren neue Viren selten. Jeder neue Virus wurde von einer Anzahl Leute begeistert unter die Lupe genommen, die seine Merkmale miteinander verglichen oder wenigstens den Virus diskutierten. Aktuelle Virus-Berichte waren nur ein Bruchteil der Mitteilungen – das haupsächliche Thema war allgemeine Neugierde.

Heute ist die Situation ganz anders. Viele von den "Alten" sind ausgeschieden, entweder aus Frustration oder aus Zeitmangel.

Die populärsten Themen scheinen heutzutage Fragen zu sein wie "Hilfe, ich habe den Form Virus" und ähnliche Mitteilungen (von Leuten, die sich offensichtlich nicht die Mühe gemacht haben, die FAQ's – frequently asked questions – zu lesen) oder unendlich langweilige Argumentationen über die Ethik der Virus-Verteilung.

... und die Jetztzeit.

Die "alte" comp.virus Newsgroup ist dahin, aber glücklicherweise haben andere ihren Platz eingenommen. Es gibt einige andere Newsgroups, die aus der Anti-Virus Perspektive von Interesse sind. Alt.security und comp.security haben gelegendich Virus-bezogenes Material, comp.sys.ibm.pc.hardware und comp.os.msdös behandeln manchmal Virus-Probleme. Comp.binaries.ibm.pc verteilt regelmäßig die populärsten Shareware und Freeware Anti-Virus Programme.

E-Mail

Im Zentrum der Ereignisse

E-Mail wird gebraucht, um Produkt-Unterstützung bereitzustellen, aber die große Zahl von virus-orientierten "mailing lists" ist für die Anti-Virus Koalition von noch größerer Bedeutung. Das letzte Mal, als ich gezählt habe, stellte ich elf verschiedene Listen fest. Einige von ihnen sind geschlossen, ihre Existenz und die Namen ihrer Mitglieder bleiben geheim, und beizutreten ist ein langer Prozeß, der eine Abstimmung der bereits vorhandenen Mitglieder einschließt. Andere Listen sind halb offen: Jeder, der kein bekannter Virus-Autor ist und der einen bestimmten Grad von technischem Wissen hat, ist eingeladen teilzunehmen.

Diese Listen dienen verschiedenen Zwecken, darunter dem Austausch von verschlüsselten Virus-Beispielen zwischen etablierten Virus-Forschern sowie technischer Diskussion.

Heutzutage sind diese Mailing-Listen (zumindest von meinem Standpunkt aus) der einzig bedeutsame Weg, virus-bezogenes Material zwischen Teilnehmern einer Anti-Virus Koalition auszutauschen. Ohne diese Mailing-Listen würden wir signifikant schwächer organisiert sein als unsere Viren schreibenden Gegenspieler.