



Allgemeine Hintergrundinformation über Viren

Allgemeine Hintergrundinformation über Viren

1. Was ist ein Virus?

Ein Computervirus ist ein Programm oder eine Folge von Anweisungen, mit dem Ziel sich zu verbreiten, bevor es entdeckt ist. Die Programm- oder Anweisungsfolge besteht aus ausführbaren Codes, die in der Lage sind, Kopien zu generieren, selbst eine Routine zu enthalten, die im allgemeinen Schaden verursacht.

2. Definitionen

Wurm: Ein "Wurm" ist ein Programm, das dafür entworfen ist, sich überall in weitreichenden Computernetzen zu verbreiten. Im allgemeinen ist das Ziel eines Wurms die Operation von Netzen zu einem Stillstand durch Überladen ihrer Ressourcen zu bringen. In der Pandavirusliste beginnt die Nomenklatur der meisten Würmer mit I-Worm oder Worm.

Trojanisches Pferd: Ein "trojanisches Pferd" ist ein Programm, das die im Computer gespeicherte Information modifiziert oder zerstört. Der Name "trojanisches Pferd" kommt von der Tatsache, das in der Regel dieses Art Virus dem Benutzer als ein Computerspiel oder Textverarbeitungsprogramm verkleidet übergeben wird, das den zerstörerischen Code enthält. Durch Definition hat ein trojanisches Pferd nicht die Fähigkeit der Autovervielfältigung. In der Pandavirusliste beginnt die Nomenklatur der meisten Trojaner mit TROJAN.

Virus: Ein "Virus" ist ein kleines Programm, das Merkmale von "Würmern" und "trojanischen Pferden" erhalten hat. Es kann sich wie ein Wurm selbst kopieren und kommt auch getarnt auf den PC. Ein Virus hat darüberhinaus die Fähigkeit durch Dateimanipulation Daten zu vernichten.

3. Merkmale

Damit ein Programm als einen Virus betrachtet wird, muß es die folgenden Merkmale haben:

- ? Es muss ein kleines Computerprogramm sein, dessen Zweck es ist sich zu verbreiten und in einigen Fällen, Dateien und Systeme zu beschädigen.
- ? Es muss die Kapazität der Autovervielfältigung haben, Dateien und PCs infizieren und eine Weile versteckt bleiben.

4. Lebenszyklus eines Computervirus

Ursprung und Übertragung

Jemand programmiert es und plaziert es innerhalb der Reichweite der Öffentlichkeit. Ein Benutzer führt es aus, und der Virus installiert sich im Computer.

Die Kette der Verteilung des neuen Virus wird initiiert, wenn eine Person die sich für das Programm interessiert, es ausführt und auf diese Art sein System infiziert. Sobald der Computer des ersten Opfers infiziert ist, kann der Virus sich in den Programmen reproduzieren, die auf seiner Festplatte oder auf Diskettenlaufwerken gespeichert sind. Wenn dieser Benutzer mit anderen Computern dadurch, das er einem anderen Benutzer ein kontaminiertes Programm leiht, das er in seinem oder ihrem Arbeitsplatzrechner ausführt, steigert der Virus exponentiell seine Aussichten auf Verbreitung.

Schlaf und Aktivierung

Ein Virus wird immer schlafend übertragen. Er wird erst dann aktiv wenn das Programm das den Virus transportiert ausgeführt wird.

Die einfachsten Viren führen eine Kopie von sich in die ausführbaren Datei ein, die innerhalb ihrer Reichweite sind. Dadurch steigt die Größe der Datei leicht. Diese ausführbaren Dateien schließen jede Datei ein, deren Erweiterung "EXE", "COM", "OVL", "SYS" oder "BIN" ist. Andere Viren verwenden freien Platz auf der Festplatte, um sich zu installieren.

Viele vorhandene Viren installieren sich als "memory resident", wenn ein infiziertes Programm ausgeführt wird. Von dieser Position im Speicher können die Viren sich in normale Computeroperationen einmischen. Von den Moment, wenn ein Virus in Speicher ansässig ist, hängt es von der Ausführung anderer Programmen ab, wann sie infiziert werden.

Es gibt bestimmte Systemdateien, die jedes Mal ausgeführt werden, wenn der Computer gebootet wird. In Folge sind viele Viren dafür entworfen, sie direkt zu infizieren, da diese Dateien für das Funktionieren vom System entscheidend sind. Deshalb wirkt die Tatsache, daß diese Dateien infiziert sind, als eine Garantie für die zukünftige Fortpflanzung des Virus. Die Dateien, die am häufigsten an dieser Dynamik beteiligt werden, sind command.com, und die Windows win.com. Leider wird die entgegengesetzte Variante auch genutzt: es gibt viele andere Viren, die es vermeiden, diese Systemdateien auf jeden Fall zu infizieren, da sie die Dateien sind, die am meisten Aufmerksamkeit erregen.

Viren schließen im allgemeinen eine zerstörerische Routine ein, die aktiviert wird, wenn eine vorherbestimmte Bedingung erfüllt wird. Zum Beispiel wird der spanische Virus "Barrotes" (Bars) am 5. Januar aktiviert, zeigt dicke Striche auf dem Bildschirm an und blockiert die Festplatte zum weiteren Gebrauch.

Ein anderes Beispiel ist der "Anti Telefónica" Virus, der aufgeführt ist, als anti-CTNE Boot, in der Pandavirusliste.

Dieser Virus integriert einen Bootzähler, so dass, wenn der infizierte Computer eine gewisse Anzahl der Starts erreicht hat, in diesem Fall 333, der Virus die Festplatte mit zufälligen Informationen überschreibt und die auf der Platte enthaltenen Daten zerstört.

Einige andere Viren sind weniger zerstörerisch und beschränken sich darauf, Nachrichten oder Abbildungen auf dem Bildschirm anzuzeigen oder Geräusche durch den Systemlautsprecher zu emittieren, während andere einfach programmiert werden, um den Computer zu infizieren und nicht mehr, da sie das Aktivierungsmerkmal nicht haben.

Entdeckung

Diese Phase beginnt in dem Moment, wenn der Benutzer bemerkt, dass ihr Computer von einem Virus infiziert ist, das jederzeit geschehen kann, obwohl die Entdeckung normalerweise auftritt, wenn der Virus aktiviert wird.

Entfernen

Wenn Sie das richtige Antivirus Programm zu Ihrer Verfügung haben, gibt es Ihnen die Möglichkeit, den Virus aus ihren Dateisystemen zu entfernen.

5. VIRUS TYPEN UND IHRE INFEKTIONSMETHODEN

? BOOT VIRUS

Bootviren infizieren den Bootsektor und /oder die Partitionstabelle, um sich auszuführen und jedes Mal die Kontrolle zu übernehmen, wenn der Computer von einer infizierten Platte bootet. Der einzige Weg, ihn nicht zu aktivieren, ist das Booten des Systems von einer nicht infizierten Platte oder Diskette .

Der typische Prozess, der von dieser Art des Virus folgt wird, um sich in einem Computer zu installieren :

Nehmen Sie an, dass Sie eine Diskette haben, deren Bootsektor von einem Bootvirus infiziert ist. Die Verwendung der auf der Diskette enthaltenen Dateien beeinflusst auf keinsten Weise die Verwendung Ihres Computers; das heißt, Sie können sie kopieren oder ausführen, und der Virus, der sich im Bootsektor befindet, wird nicht in der Lage sein, sich auszuführen.

Der Virus beginnt nicht Probleme zu verursachen, bis Sie zum Beispiel vergessen, die Diskette aus dem Diskettenlaufwerk heraus zu nehmen.

? Wenn es eine Diskette in Laufwerk A ist: wenn der Computer neu gebootet wird, versucht das System, damit zu booten. Ohne Rücksicht darauf, ob die Diskette eine Bootplatte ist, wird ihr Bootsektor ausgeführt, das bedeutet, dass der Viruscode in der infizierten Diskette ausgeführt wird.

- ? Wenn der Bootvirus die Kontrolle übernimmt, hat er mehrere Gelegenheiten dazu sich zu Öffnen :
1. Das erste, was ein Bootvirus normalerweise macht ist, es belegt den Speicherbereich den es braucht, so dass niemand anderes ihn verwenden kann. Es infiziert dann die Festplatte, so dass es die Kontrolle übernehmen kann, wenn der Computer von der Festplatte gebootet wird.
 2. Es bewegt sich dann, von der Position in die es das Betriebssystem geladen hat, zum Bereich des Speichers, den es für sich reserviert hat.
 3. Die dritte Stufe ist, sobald er in seinem definitiven Standort installiert ist, soll er bestimmte Betriebssystemdienste abfangen und wirkt als ein Filter zwischen dem Betriebssystem und der Computerhardware. Der Dienst, der am häufigsten von Bootviren abgefangen wird, ist der Lese- und Schreib-Dienst.
 4. Jedes Mal wenn auf eine Diskette im Diskettenlaufwerk zugegriffen wird, überprüft der Virus den Speicher. Wenn die Diskette, die verwendet wird, sauber ist, infiziert der Virus diese einer Kopie von sich.

Wenn der Sektor sauber ist, startet der Virus den Infektionsprozess. Das erste was er tun wird ist, eine Stelle auf der Diskette suchen, wo er ein Kopie des original Bootsektors anlegen kann. Einige Viren tun dieses in freien Clustern, die sie dann als fehlerhaft kennzeichnen. Andere speichern es auf die letzten Position der Diskette und zerstören die Information, die dort gespeichert sind, wenn die Diskette voll ist.

Nach dem Sichern des Original Bootsektors schreibt der Virus seinen Code in den Bootsektor der Diskette und erhält die Information über seine Struktur. Da diese Schreiboperation nach dem Lesen sofort auftritt, nimmt der Benutzer nicht an, das die Aktivität vom Diskettenlaufwerk anormal ist. Außerdem ist die Zeit, die es braucht, um in einen Sektor zu schreiben sehr kurz.

Die beste Art, eine Diskette vor einer Virusinfektion zu schützen, ist sie Schreibzuschützen, da diese Art des Schutzes alle daran hindert, Daten auf ihr zu sichern und die Platte zu infizieren.

Es gibt drei Punkte in diesem Abschnitt, die sich hervorheben lassen:

1. *Es ist unmöglich, eine Diskette mit einem Bootvirus oder einem Dateivirus zu infizieren, wenn die Diskette schreibgeschützt ist. Kein Virus kann diesen Schutz umgehen, da es die Diskettenlaufwerks Hardware ist, die das angeforderte Schreibverfahren blockiert.*
2. *Ein Bootvirus kann eine Festplatte infizieren, wenn Sie versuchen, von einer infizierten Diskette zu booten, selbst wenn die Diskette keine Bootdiskette ist*
3. *Es gibt Viren, die sowohl Bootsektoren als auch ausführbare Dateien infizieren. Diese Viren werden "multipartite" Viren genannt; das heißt, sie sind gemischte Viren, die simultan Dateien- und Bootviren sind. Es kann sein, dass ein infizierter Bootsektor bewirkt, dass der Festplattenbootsektor infiziert wird.*

? DATEI VIRUS

Dateiviren verwenden ausführbare Dateien als Mittel, um sich zu übertragen. Eine mit einem Dateivirus infizierte ausführbare (Programm) Datei ist völlig harmlos, solange Sie es nicht ausführen.

Ein typischer Dateivirus installiert sich und infiziert folgendermaßen einen Computer:

1. Ein infiziertes Programm ist ausgeführt und als Ergebnis wird der Virus aktiv. Zum Beispiel, Makroviren (in Word, Excel usw.) „erwachen“, wenn ein Dokument, das ein virusbeladenes Makro enthält, geöffnet wird.
2. Wenn der Virus im Speicher ansässig ist, führt er sich im Speicher durch Abfangen der Dateiöffnung und der Ausführungsdienste ein. Auf diese Art, wird jedes Mal wenn das System diese Funktionen aufruft, um eine Datei zu öffnen oder auszuführen, der Virus in der Lage sein, diese Datei zu infizieren.

Entsprechend der Art, wie ein Dateivirus Dateien infiziert, kann die folgende Klassifizierung gemacht werden:

- ? Resident file viruses
- ? Direct action file viruses
- ? Overwrite viruses
- ? Companion viruses
- ? Macro viruses

Resident file viruses

Sobald diese speicherresidenten Viren aktiviert werden, prüfen Sie ob die Bedingung für Ihre Ausführung gegeben sind (Datum Bootzähler...)

Daraufhin lädt sich das Virus in den Speicher des PC von wo aus es seine Angriffe startet.

Diese können vielfältig sein. Ein Virus kann sich verbreiten, das Arbeiten am PC verhindern oder andere Aktivitäten ausführen.

Bevor eine Datei angegriffen wird prüft ein Virus folgende Punkte:

- ? Ob die Größe des Programms innerhalb des richtigen Bereichs liegt. Wenn die Summe der Originalgröße der Datei plus des Viruscodes diesen Bereich übertrifft (z.B. 64kb für COM Dateien), kann die Datei nicht infiziert werden oder sollte wenigstens nicht infiziert werden.
- ? Ob die Datei zu der Dateart gehört, die es infizieren kann, (COM, EXE, SYS, usw.)
- ? Ob die Datei zuvor infiziert wurde. Einige Viren infizieren Dateien wieder, die zuvor infiziert wurden, während andere Zeichen in die Dateien stellen, um zu vermeiden, sie wieder zu infizieren. Diese Zeichen können die Erstellungszeit einer Datei in einem falschen Format, aus einer gewissen Folge von Bytes in eine bestimmte Position in der Datei oder einer anderen Änderung bestehen.

Wenn ein Virus eine Datei infiziert, fügt es dem Code der Datei normalerweise seinen eigenen Code hinzu. Die Positionen, wo sich Viren normalerweise in infizierten Dateien unterbringen, sind:

- ? Am Anfang einer Datei
- ? Am Ende der Datei. Dies ist die gebräuchlichste Position.
- ? In die Mitte der Datei.

Wichtig: Eine " read only " Datei bildet keine Barriere gegen Infektion durch eine große Mehrheit von Viren.

Direct action Datei Viren

Dieser Virus reproduziert sich direkt bei seiner Ausführung und lädt sich nicht in den Speicher.

Es kann dann auch nach neuen Dateien suchen, die entweder im gegenwärtigen Verzeichnis oder im Systempfad liegen und diese infizieren.

Wenn seine Selbstfortpflanzung durchgeführt ist, gibt der Virus die Kontrolle an das Virustransportprogramm zurück, so daß alles ganz normaler zu funktionieren scheint.

Überschreibende Viren

Diese Art des Virus ist durch das nicht Respektieren des Inhalts der Datei charakterisiert, die es infiziert. Eine andere von seinen Eigenschaften ist, das, wenn es eine Datei infiziert, die Datei nie an Größe zunimmt, es sei denn, der Viruscode nimmt zufällig mehr Platz als sein Opfer ein.

Obwohl das Originalprogramm zerstört ist, funktioniert die Kopie des in die Datei eingefügten Virus perfekt; das heißt, wenn der Benutzer versucht, die Datei auszuführen, zeigt der Virus eine anormale Fehlermeldung an, die vortäuscht, das ein Fehler am Originalprogramm vorliegt.

Der einzige Weg, eine so kontaminierte Datei zu desinfizieren ist sie zu löschen. Sie muß dann durch eine Kopie des Originalprogramms ersetzt werden.

Begleitende Viren

Diese sind durch nicht Modifizieren der Dateien die sie infizieren **charakterisiert**. Sie nutzen ein Merkmal des DOS Befehlssystems aus: wenn das Betriebssystem zwei ausführbare Dateien findet, mit demselben Namen, aber mit verschiedenen Erweiterungen: (.COM und .EXE) führt es die Datei mit der .COM Erweiterung immer zuerst aus.

Wenn ein Begleitervirus eine .exe Datei infiziert, das einzige was er tut, ist eine neue Datei mit dem selben Namen wie der infizierte zu erstellen, aber die mit der .com Erweiterung beinhaltet den Viruscode

Um diesen Virus zu bekämpfen reicht es also die infizierte COM Datei zu löschen.

? MACRO VIRUSES

Makros sind Folgen von Anweisungen, oder Miniprogramme in Dokumenten, die durch Microsoft Büroprogramme erstellt wurden. Makroviren sind eine relativ neue Art des Virus, der mit Version 6,0 von Microsoft Word und Version 5,0 of Microsoft Excel erschien. Gegenwärtig erscheinen täglich neue Makroviren in jedem Teil der Welt.

Makroviren sind äußerst leicht zu schreiben.

Ohne Rücksicht auf das Betriebssystem können Makroviren ohne Änderungen der Plattform von jeder der unterstützten Anwendungen funktionieren, die das Macro interpretiert. Zum Beispiel, ein Microsoft Word Makrovirus kann auf

jeder Plattform arbeiten, für die es eine Version des Programms gibt: Windows 3.x, Windows 95/98, Windows NT, usw..

Folgen Effekte sind einige der bösartigen Wirkungen, die Makroviren haben können:

- ? Löschen von Dateien und Dokumenten von der Festplatte
- ? Umbenennen von Dateien
- ? Das Verschieben von persönlichen Dateien an unbekannte Stellen
- ? Sendet Daten von der Festplatte zu einer E-mail Adresse

In einigen Stunden kann ein Makrovirus alle Computer eines Netzes infizieren, da es die Übertragung und den Informationsaustausch in der Form von Dokumenten über elektronische Post benutzt.

Makroviren sind normalerweise nicht wirklich gefährlich, und sie sind lange darauf beschränkt gewesen, lustige Nachrichten auf Bildschirm anzuzeigen. Wir können jedoch nicht darauf vertrauen, daß ein Makrovirus nicht unser System beschädigt, da das Niveau des hohen Entwicklungsstands, der im Entwurf dieser Art des Virus erreicht wird, Infektion durch einen Makrovirus in ein wirkliches Problem für die Stabilität der Information der Gesellschaften umwandelt.

Die folgenden Punkte sollten Sie sich in Bezug auf Makroviren merken:

- ? **Die Tatsache, daß ein Dokument Makros enthält, bedeutet nicht, daß IT infiziert ist.** Viele der in Dokumenten gefundenen Makros sind Makros, die von Benutzern erstellt wurden, um bestimmten Aktionen zu ermöglichen.
- ? **Makroviren sind nicht Speicheransässig.** Sie können einen Makrovirus im latenten Zustand auf einer Festplatte haben, ohne andere Daten zu infizieren. Solange Sie Word nicht öffnen, kann ein einfacher Makrovirus nicht fortfahren, andere Dateien zu infizieren.
- ? Wenn Sie, während Word geschlossen ist, die infizierte Normal.dot löschen und wieder Word öffnen, generiert das Programm automatisch eine neue, normal.dot die virenfrei ist.

Macroviren in der Panda Virus Liste:

- WM/ - Word 6.0 macro virus
- W97M/ - Word 97 macro virus
- W2000M/ - Word 2000 macro virus
- XM/ - Excel 6.0 macro virus
- X97M/ - Excel 97 macro virus

A97M/ - Access 97 macro virus

5. TECHNIKEN VON VIREN

Um es zu vermeiden, entdeckt werden, können Viren diverse Methoden verwenden:

- ? Stealth
- ? Tunneling
- ? Self-Encryption
- ? Polymorphic Mutation
- ? Armoring

Stealth

Diese Methode besteht daraus, die sichtbaren Symptome einer möglichen Virusinfektion zu verbergen, um seine Entdeckung zu vermeiden. Nur speicheransässige Viren können diese Methode verwenden.

Wenn ein Virus eine ausführbare Datei infiziert, läßt es immer Beweise seiner Gegenwart zurück. Diese Anhaltspunkte sind die Zunahme der Größe der Datei, Änderungen im Datum oder der Zeit der Erstellung der Datei.

Viele ansässige Viren verwenden Tarnungsmethoden, um diese Änderungen oder den Virus selbst daran zu hindern, wahrgenommen zu werden. So kann ein Virus z.B. das Lesen von Dateien verhindern oder diese sogar unsichtbar machen indem es die Dateibewegungen filtert

Es ist klar, daß ein Virus nur in der Lage sein wird, solche Methoden zu verwenden, wenn es Speicheransässig ist.

Tunneling

Diese Methode wurde dafür entworfen, ansässige Schutzprogramme zu umgehen. Wie Viren fangen diese Programme die Systemdienste ab, um die Erkennung zu verhindern, die Viren oder der Mißbrauch von anderen Programmen verursachen können. Zum Beispiel verhindern sie, in Bootsektoren, die Änderung von ausführbaren Programmen oder die Formatierung von Festplatten.

Die „einen Tunnel grabende“ Methode erlaubt Viren, die Originalspeicheradressen der Systemdienste zu erhalten. Dies ermöglicht ihnen, auf diese Dienste direkt zuzugreifen, ohne von anderen ansässigen Programmen abgefangen zu werden.

Glücklicherweise gibt es Arten wahrzunehmen, wenn ein Virus versucht, die Originaladressen zu erhalten. Deshalb warnt ein AV Programm vor diesem Umstand.

Self-Encryption

Heutzutage sind die meisten Viren dazu fähig sich, jedes Mal wenn sie eine Infektion ausführen, auf eine andere Weise zu verschlüsseln. Auf diese Art behindern sie die Arbeit von Antivirusprogrammen durch Ändern ihres Musters nach jeder Infektion.

Polymorphic Mutation

Polymorphe Viren gehen in ihren Verschlüsselungsmethoden ein Schritt über Self-Encryption-Viren hinaus. Viren, die diese Methode verwenden, werden nicht nur verschlüsselt, sondern sind in der Lage, ihre Verschlüsselungsroutine von einer Infektion zur Nächsten zu ändern. Dies bedeutet, daß zwischen zwei Mustern von demselben Virus es nichts gemeinsames, nicht einmal ihre Verschlüsselungsroutine gibt.

Diese Methode macht die traditionelle Methode nach Virusstrings zu suchen fast unmöglich und erfordert die Implementierung von algorithmischen Suchverfahren.

Armoring

Einige Viren verwenden Methoden zur Vermeidung, durch Debugger geprüft zu werden. Damit wird es schwieriger, sobald sie wahrgenommen und isoliert worden sind, ihre Anatomie und ihr Ziel zu studieren um die passende desinfizierende Routine vorzubereiten.