Für Einsteiger

VX – The Virus Underground

Marcell Dietl

Schwierigkeitsgrad

Immer wieder liest man in den Medien von neuen Viren und Würmern, welche in Umlauf kommen und großen Schaden anrichten. Doch kaum einer weiß, dass es eine kleine Gruppe von Leuten gibt, welche so genannte Malware programmiert, da sie es als eine Kunst des Hackings ansieht. Dieser Gruppe von Menschen und deren Ideologie wollen wir uns im Folgenden widmen.

Wenn die Schlagzeilen in Zeitschriften und Fernsehen wieder von einem neuen Virus oder Wurm geprägt sind, läuft es vielen kalt über den Rücken, sie befürchten eine neue Infektionswelle und entwickeln einen Zorn auf die Autoren solcher Programme, welche wir im Weiteren als Malware klassifizieren werden. Kaum einer bedenkt dabei jedoch, dass solche Programme auch durchaus aus positiven Beweggründen entstehen können. Leider wird das oft nicht erwähnt, da nur solche Malware die Schlagzeilen füllt, welche meist aus Profitgier entsteht. Die kleine Szene von vielleicht fünfzig Leuten, welche sich zum Ziel gesetzt hat, immer neue und kreative Programme zu erstellen, leidet unter dieser negativen Verallgemeinerung und wird in vielen Ländern mittlerweile genauso bekämpft wie die Kriminellen selbst. Im nachfolgenden Artikel wollen wir uns jedoch genau dieser Gruppe von Menschen widmen und lernen ihre Denkweise zu verstehen und erkennen, dass Viren durchaus auch eine Kunst des Hacking sein können, wenn auch eine komplett andere, als viele denken. Lassen Sie uns also einen Blick auf diese kleine Gruppe, ihre Idole, ihre Ideologie und Szenestruktur werfen und vielleicht werden Sie Ihre Meinung auch ein wenig ändern, wenn Sie das nächste Mal von einem neuen Virus oder Wurm lesen, welcher wieder einmal nur aus Geldgier entstanden ist.

Wichtige Gruppen der Szene

Später werden wir noch genauer die Probleme der VX Szene betrachten, doch hier sei schon

In diesem Artikel erfahren Sie...

- Wie die Virenszene aufgebaut ist;
- Welche Fachbegriffe es bei Virenschreibern gibt;
- Welche wichtigen Personen, Gruppen etc. es in der Szene gibt;
- Welche Verbindung zwischen Virenschreibern und Anti-Viren Firmen besteht;
- und vieles mehr...

Was Sie vorher wissen/können sollten...

- Außer einem Interesse an der Materie ist kein Vorwissen nötig.

einmal erwähnt, dass eines der Probleme eine ständige Veränderung der Gruppen- und Szenekonstellation ist. So gibt es ständig neue Virusautoren und Virusgruppen, doch nur wenige bleiben auf längere Sicht gesehen aktiv, was es durchaus erschwert genau festzulegen, welche Gruppen und Autoren es derzeit gibt und inwieweit diese noch aktiv sind. Nichtsdestotrotz möchte ich Sie hier mit einigen Namen von Gruppen vertraut machen, die zumindest nach jetzigem Stand der Dinge als aktiv gelten können. Ob sie es in Zukunft weiterhin bleiben ist fraglich. Lassen Sie uns mit den zwei wichtigsten Gruppen anfangen, die eine trägt den Namen Ready Rangers Liberation Front (rRlf) und ist eine deutsche Gruppe, welche es seit nunmehr sieben Jahren gibt. Sie haben viele Veröffentlichungen in den letzten Jahren hervogebracht und es ist unwahrscheinlich, dass sie in nächster Zeit inaktiv werden. Die andere und wohl bekannteste Gruppe der ganzen Szene ist 29A, was den Hexcode von 666 darstellt. Es ist eine internationale Gruppe, welche ebenso vor vielen Jahren zu Beginn des VX (Virus Coding) gegründet wurde. Sie brachte viele Veröffentlichungen heraus und ist auch heute noch aktiv, jedoch hat sich die Struktur leicht verändert. Um Ihnen eine gute Basis zu geben, seien hier noch die Gruppen DoomRiderz aus Amerika (wo es mittlerweile als Verbrechen gilt Viren zu schreiben), Purgatory aus dem Iran, F-13 Labs und das EOF-Project(.net), welches ich im Jahre 2006 gründete und das seit 2007 unter neuer Leitung steht, genannt. Natürlich kann ich Ihnen hier nur einen groben Überblick geben, da es ständig zu Veränderungen der Szenestruktur kommt, aber zumindest sind Ihnen jetzt schon einige Begriffe geläufig. Alle Gruppen bestehen meist aus Mitgliedern verschiedener Staaten, so ist etwa der Leader (=Anführer/Organisator) des amerikanischen Teams selbst nicht aus Amerika, jedoch wurde diese Gruppe ursprünglich in Amerika gegründet, hat sich jedoch mittlerweile stark gewandelt. Auch das EOF-Project besteht aus Mitgliedern der verschiedensten Staaten dieser Welt, eine typische Eigenart der Szene, da es meist nicht länderspezifisch organisiert ist. Ich hoffe, dass Ihnen dieser Abschnitt schon einmal einen kleinen Einblick in die wichtigsten Gruppen der Szene gegeben hat.

Die Ideologie der Autoren

Im letzten Absatz haben Sie eine kleine Einführung in einige wichtige Gruppen der Szene erhalten, nun wollen wir uns der Ideologie der Autoren widmen, denn nicht alle programmieren Viren aus den gleichen Grundsätzen heraus und es gibt enorme Unterschiede. Natürlich könnte man hier als erstes solche nennen, welche Malware nur erstellen, um damit Geld zu verdienen. Sei es, weil sie etwas VCKs (Virus Creation Kits) weiterverkaufen oder weil sie Rechner infizieren, um sensible Daten auszuspähen. Doch denen wollen wir uns gar nicht weiter widmen, denn mit diesen Kriminellen hat ein VXer nichts zu tun. Ansonsten könnte man die Virenschreiber in zwei große Gruppen einteilen, die Hobbyisten und die Ideologen. Gängiger Definition nach versteht man unter der Hobbyisten solche Programmierer, welche gelegentlich einen Virus schreiben oder auch nur ein einziges bis einige wenige Male, um das als kreative Herausforderung zu sehen. Daher kommt auch die ständige Umstrukturierung der Szene, da es ständig neue Autoren gibt, welche jedoch nach wenigen Viren meist wieder verschwinden. Hobbyisten sehen das Programmieren eines Virus als interessante Herausforderung, aber widmen sich schnell wieder anderen Themengebieten. Dann gibt es noch die Ideologen. Sie programmieren Viren und sonstige Malware, da es für sie eine künstlerische Herausforderung darstellt. Sie wollen ständig neue Techniken erlernen und umsetzen und suchen neue Möglichkeiten, etwa neue Verbreitungswege. Man kann schwer sagen, wer in welche Gruppe einzuordnen ist, meist ist die Grenze recht fließend, doch lässt es sich ganz gut zeitlich festlegen. Wer lange in der Virenszene war und immer aktiv blieb, gehört eher zu den Ideologen als den Hobbyisten. Als ein Beispiel sei hier der Autor Roy G Biv von 29A genannt, welcher heutzutage als einer der längsten und aktivsten in der Szene tätig ist. Er gehört eindeutig zu den Ideologen. Er ist zwar nicht der einzige, doch ein sehr gutes Beispiel dafür. Einen entscheidenden Unterschied gibt es schließlich noch, nämlich VXer, welche ihre Viren in die *Wildbahn* aussetzen und solche, welche Viren zwar veröffentlichen, jedoch nicht, um damit destruktiv Schaden anzurichten. Würde man es mit Hackern vergleichen, könnte man bei den meisten VXern von Whitehats sprechen, da sie alles im gute Sinne programmieren und bei solchen, welche Schaden anrichten wollen von Blackhats. Doch dies nur als kleine Parallele zu der Welt des Hacking (was ja VX auch bedingt ist).

Abbildung 1. *Das Logo der Gruppe Ready Rangers Liberation Front*

Vergangenheit – Gegenwart – Zukunft

Nachdem wir uns zuerst mit einigen Namen und der Ideologie der Szene vertraut gemacht haben, wollen wir jetzt einen Blick auf die Entwicklung der Virenszene vom Beginn bis heute und auch zukünftig werfen. Den Anfang von Malware, damals vor allem simple Viren, kann man etwa auf den Beginn der achtziger Jahre datieren. Erste Viren tauchten zum Beispiel 1982 für den Apple II Computer auf und waren mehr scherzhaft als wirklich destruktiv. Im Laufe der achtziger Jahre tauchten immer neue Viren auf, später vor allem für Windows, das Betriebssystem von Microsoft, welches sich immer weiter verbreitete. Ziel der damaligen Autoren war es vor allem möglichst interessante neue Techniken aufzuzeigen, teilweise indem die Viren immer destruktiver wurden oder einfach in ihrer Art immer einfallsreicher. Seien es scherzhafte Fehlermeldungen oder das Formatieren der kompletten Festplatte, viele Virenschreiber wollten Aufmerksamkeit und Anerkennung. Nachdem die ersten Viren noch über Disketten verbreitet wurden, kam zu Beginn der neunziger Jahre beziehungsweise Ende der achtziger Jahre das Internet immer mehr auf. Viel mehr Computer wurden internetfähig und boten somit auch ein immer interessanteres Ziel für VXer, vor allem da es mittlerweile zum Standard gehörte Windows zu nutzen. So kam es schließlich zu den ersten größeren Wurminfektionen, angefangen bei Würmern, wie dem Morris-Wurm bis hin zu dem I LOVE YOU-Wurm. Dieser Trend der Würmer erreichte seinen Höhepunkt schließlich zu Beginn des 21. Jahrhunderts mit Würmern wie Sasser, MyDoom, Netsky und weiteren, welche noch heute in vielen Varianten aktiv sind (Anmerkung: Netsky führt auch heute noch immer die Wurmstatistiken an, basierend auf Analysen verschiedener Antivirenfirmen über den prozentualen Anteil an verseuchten Emails. Außerdem sei hier noch der StormWorm genannt, welcher mit bis zu 12 Millionen Infektionen einen der größten, wenn nicht den größten, Wurm darstellt. Als Botnet eingerichtet stellt er den leistungsstärksten Rechner der Welt dar). Blickt man zurück könnte man sagen, dass es zuerst die Viren waren, teilweise sogar als Studentenarbeiten geschrieben, welche Aufsehen erregten, später waren es die Würmer.

Wie sieht es heute aus? Betrachtet man die aktuelle Lage der Virenszene geht der Trend eindeutig zu Trojanern, also solche Programme, welche sich unter einem falschen Vorwand auf dem System einnisten und dem Autor eine Backdoor (=Hintertür) öffnen, durch die er immer wieder Zugriff auf den Computer erhalten kann. Im gleichen Zuge werden Botnets immer populärer und haben ihren Höhepunkt erreicht oder streben ihn zumindest immer weiter an. Bots sind solche Programme, welche trojanerähnlich aufgebaut sind, sich jedoch zum Beispiel via IRC zu einem kompletten Netzwerk zusammenschließen, welches dann von einer kleinen Gruppe von Leuten administriert wird. Das wohl derzeit bekannteste Beispiel ist der StormWorm, welcher Millionen von Rechnern infiziert hat und welcher dazu dient das wohl größte Botnet aller Zeiten aufzubauen. Im Vordergrund steht heute also immer häufiger Geld und Diebstahl sensitiver Daten. Im Kontrast zu früher, als es eher eine kreative Herausforderung darstellte Viren und Würmer zu programmieren. Doch vergessen Sie eines hierbei nie: Auch wenn immer mehr Malware heutzutage zu Geldzwecken geschrieben wird, gibt es eine kleine Gruppe von Leuten, die diesem Trend strikt entgegenwirkt und weiterhin Viren nur als kreative Herausforderung schreibt, denen widmen wir uns schließlich hier.

Betrachten wir als letztes noch, welchen Trend es wohl in der Zukunft geben wird. Zwar ist das reine Spekulation, doch scheint es derzeit so, dass Handyviren immer weiter an Popularität gewinnen werden. Schon heute gibt es verschiedene Proof-of-Concept Viren, welche beweisen, dass es möglich ist ein Handy zu infizieren und wie es früher mit einigen wenigen Viren begann, welche einfach nur beweisen sollten, dass es geht, wird es sich vielleicht auch mit den Handyviren verhalten. Dies war natürlich nur ein grober Überblick und er kann gewiss nicht alle Faktoren abdecken, bedenken Sie das bitte immer.

Plattformübergreifende Malware

Ein Trend, der eben noch nicht angesprochen wurde, der jedoch derzeit in der VX Szene auch immer populärer wird ist das Schreiben von Malware, welche sich plattformübergreifend verbreiten kann. Lassen Sie uns also einen Blick auf verschiedene Möglichkeiten werfen, wie dies derzeit realisiert wird und das Ganze auch beispielhaft betrachten. Es gibt natürlich die verschiedensten Möglichkeiten plattformübergreifende Programme, in unserem Fall Viren, Würmer und Trojaner (zusammenfassend Malware), zu schreiben und es wäre schwierig jede Möglichkeit abzudecken, doch lassen Sie uns hier zumindest die typischsten Varianten betrachten. Ein Trend, welcher erst vor kurzem für großen Wirbel gesorgt hat, ist die Möglichkeit Viren zu schreiben, welche als Makroprogramme in Drittprogrammen ausgeführt werden. Klingt erst einmal sehr komplex, ist jedoch recht

Abbildung 2. *Das Logo von 29A*

simpel. Jedes größere Office Paket enthält heutzutage die Möglichkeit bestimmte Programmroutinen zu automatisieren, es enthält also eine eigene kleine Programmiersprache, mit der man Zusatzkomponenten erstellen und diese in sein Dokument auch einbinden kann. Diese Programmteile, welche man in ein Dokument einbinden kann, sind Makros, kleine Programmroutinen also. Der Vorteil eines Makrovirus ist es, dass die großen Office Pakete meist auf verschiedenen Betriebssystemen lauffähig sind. So ist es also möglich einen Makrovirus zu schreiben, in ein Dokument einzubinden und schließlich zu versenden. Für den Makrovirus ist es egal auf welchem Betriebssystem er ausgeführt wird, da die Interpretierung seiner Routinen dem jeweilig eingesetzten Office Paket überlassen wird.

Lassen Sie uns das ganze an einem populären Beispiel betrachten, um Ihnen das Ganze besser verständlich zu machen. Zusammen mit dem Team DoomRiderz, welches ich Ihnen vorhin kurz vorgestellt habe, begann ich vor etwa einem Monat einen großen Proof-Of-Concept Wurm zu programmieren, der sich über OpenOffice installierte und etwa über IRC verbreitete. Der Wurm wurde als Makrovirus gestaltet und in der für OpenOffice üblichen Programmiersprache StarBasic programmiert. Diesen Teil übernahm Necronomikon von DoomRiderz. Nun war es an der Reihe dieses Konstrukt mit den jeweils für die Betriebssysteme Windows, Linux und Mac OS X gestalteten Droppern zu versehen. Ein Dropper stellt dabei ein kleines Programm dar, welches für das jeweilige Betriebssystem geschrieben ist und auf diesem als Datei abgelegt wird, um dann zur Ausführung zu kommen. Meine Aufgabe bestand nun darin, einen Dropper für Mac OS X zu programmieren, welchen ich in Ruby verfasste. Weitere Dropper wurden schließlich noch für Windows und Linux geschrieben. Alles zusammen entstand schließlich ein StarBasic Wurm, der erkannte auf welchem Betriebssystem er lief und dementsprechend eine Datei ablegte, welche ausgeführt wurde. Genau das ist das Prinzip eines Makrovirus. Ich hoffe, dass Ihnen dieses kleine Beispiel ein besseres Verständnis der Materie vermitteln konnte. Genannt haben wir den Wurm BadBunny, passend zu seinem Payload (Begriff wird später noch genauer betrachtet). Sie können unter Google genügend Material dazu finden. Eine weitere Möglichkeit, einen plattformübergreifenden Virus zu erstellen, stellt das Benutzen von zur Verfügung gestellten Frameworks dar. Hierbei wäre das wohl typischste Beispiel das .NET Framework von Microsoft, welches es mittlerweile dank der Arbeit vieler Freiwilliger auch auf anderen Betriebssystemen gibt. Programmiert man einen Virus etwa in der für dieses Framework typischen Programmiersprache C#, so muss der Code nicht aufwendig angepasst werden, um die gleiche Wirkung auf anderen Betriebssystemen zu haben, allein die Pfadangaben und andere Kleinigkeiten können natürlich variieren. Einen sehr guten Artikel hat Paul Sebastian Ziegler zu diesem Thema in Hakin9 4/2007 verfasst, auch mit gutem Beispielcode. Ähnlich dieser Technik funktioniert die nächste Möglichkeit Viren für verschiedene Systeme zu erstellen: Das Schrei-

Abbildung 3. *Das Logo der DoomRiderz Gruppe*

ben von Programmen in Skriptsprachen. Bekannte Beispiele wären etwa PHP, Perl, Python oder Ruby. Codes, welche in solchen Sprachen erstellt werden, sind wieder insoweit plattformunabhängig, dass sie von einem Programm, dem Interpreter, auf dem jeweiligen Betriebssystem ausgeführt werden. Ein Programm, welches zum Beispiel die Funktion enthält den aktuellen Ordner zu löschen, wird dabei auf jedem System laufen, welches den passenden Interpreter installiert hat. Wenn Sie Interesse an so etwas haben schauen Sie sich zum Beispiel den sehr einfachen Beispielvirus Cyanotic an, welchen ich auf meiner Webseite (*www.smash-the-stack.net*) zur Verfügung stelle. Er ist in Java geschrieben und macht nichts anderes als die Dateien des aktuellen Ordners, in dem er sich befindet mit einem String (ein aus mehreren Zeichen bestehender Satz) zu überschreiben. Jedes System, was über Java verfügt kann diesen Virus auch zur Ausführung bringen, es bedarf keinerlei Anpassungen. Eine letzte, jedoch eher seltener genutzte Möglichkeit ist es einen Virus zum Beispiel in einer LowLevel Programmiersprache zu erstellen, etwa Assembler und den Code so zu gestalten, dass er sich dem jeweiligen Betriebssystem entsprechend verhält. Der Aufwand ist demnach enorm, sollten Sie es dennoch sehr interessant finden und weitere Informationen wünschen, die diesen Artikel und Abschnitt sprengen würden, so empfehle ich eine Suche nach dem wohl bekanntesten Beispielcode, mit dem Namen Winux, eine Anspielung auf die Kombination der Wörter Windows und Linux (Anmerkung: Der Virus ist unter verschiedenen Bezeichnungen zu finden: Linux.PEElf.2132, W32.Winux, Linux.Winux, W32/Lindose).

Abbildung 4. *Das Logo des iranischen Purgatory VX Teams*

Genutzte Verbreitungswege

Die letzten Abschnitte ermöglichten Ihnen nun schon einen kleinen Einblick in die VX Szene und ihre Entwicklung über die letzten Jahre hinweg. Mit was wir uns bisher nicht beschäftigt haben, ist das Thema, wie typische Viren aufgebaut sind und welche Fachbegriffe oder Techniken häufig eingesetzt werden. Dem wollen wir uns jetzt widmen. Lassen Sie uns einen Blick darauf werfen, welche typischen Verbreitungswege VXer bei ihren Viren einsetzen. Natürlich gibt es mehr Möglichkeiten, als die, welche ich Ihnen hier vorstellen werde, aber es ist zumindest ein kleiner Einblick in typische Wurmtechniken. Wie wir vorhin schon erfahren haben, wurden die ersten Viren noch als kleine Projekte von vorwiegend Studenten geschrieben, verbreitet wurden sie zumeist über Freunde und Disketten. Man reichte die Datei untereinander weiter und so entstanden die ersten *Würmer*, obwohl sie es im eigentlich Sinne noch nicht waren. Heute greift man auf andere Techniken zurück. Eine Möglichkeit, die häufig genutzt wird, stellt es dabei dar, von der Autostart Funktion einer CD oder DVD ROM Gebrauch zu machen. Nur wenige Nutzer von Windows haben diese deaktiviert und so ist es ein Leichtes einen Virus zu schreiben, welcher sich auf ein Medium kopiert, um von dort andere Rechner zu infizieren. Eindeutiger Nachteil dieser Methode ist erneut, dass es eines Anfangs bedarf, also etwa einem Nutzer, welcher absichtlich eine CD mit dem Virus beschreibt und weiterreicht. In neuerer Zeit werden USB Sticks immer mehr genutzt und erste USB Sticks enthalten eine Autostart Funktion von Programmen. Auch diese Möglichkeit eignet sich gut, um den eigenen Virus schnell an andere zu verbreiten und dort eine automatische Ausführung zu provozieren. Doch auch dies Bedarf der Tatsache, dass ein USB Stick eingesteckt ist und weitergereicht wird. Welche Möglichkeiten gibt es noch und welche sind vor allem hiflreicher einen Wurm schnell zu verbreiten? Diese Frage lässt sich nicht eindeutig beantworten, jedoch zeichnen sich einige Trends ab, die man hier benennen kann. In den letzten Jahren wurden so genannte Peer-To-Peer- oder kurz P2P-Netzwerke immer beliebter. Sie erlauben es beliebige Dateien und Ordner des eigenen Rechners anderen zur Verfügung zu stellen, damit diese darauf zugreifen können. Viele solcher Tauschprogramme enthalten Standardordner, in denen diese Freigaben gespeichert werden und so ist es unter VXern sehr beliebt ihren Virus mit interessanten Dateinamen zu versehen – etwa ein Crack für Windows – und in diesem Ordner abzuspeichern. Diese Methode funktioniert ähnlich bei Tauschseiten, so genannten Sharehostern, wie etwa Rapidshare oder ähnlichen. Man stellt seinen Virus möglichst anonym online, gibt ihm einen interessanten Inhalt und wartet, bis er sich verbreitet. Man könnte sich nun noch vorstellen, dass man automatisiert in ungeschützten Foren oder Blogs Werbung für diese Datei macht und hofft, dass so mehr Leute das Programm herunterla-

den und ausführen werden. Diese Methode funktioniert erwiesenermaßen ziemlich gut und wird zum Beispiel auch von dem aktuellen StormWorm eingesetzt, welcher sich unter anderem über Blogs verbreitet. Doch nichtsdestotrotz bleibt die beliebteste Verbreitungsvariante weiterhin die Email. Viele Nutzer benutzen noch immer Outlook zum Versenden von Emails und es gibt genügend Beispielcodes, wie man es schafft seinen eigenen Virus beziehungsweise Wurm an alle Emails weiterzuversenden, welche im Adressbuch eingetragen sind. Auch der eben schon genannte StormWorm nutzt Emails als Hauptverbreitungsweg und verweist darin auf infizierte Websseiten, welche den Virus enthalten. Wie man sieht: Es funktioniert. Ich hoffe, dass Ihnen dieser Abschnitt einen kurzen Überblick über beliebte Verbreitungswege der Würmer gegeben hat, von früher bis zur Gegenwart. Betrachtet man die Zukunft wird wohl eine Verbreitung über MMS oder SMS Würmer oder Bluetooth Malware immer häufiger anzutreffen sein, letztendlich bleibt es jedoch vorerst reine Spekulation. (Anmerkung: Erste Konzepte liegen bei Bluetooth Malware schon vor, wie der Artikel von Marko Rogge in Ausgabe 9/2007 zeigt)

Payloads

Allein schon die Überschrift dürfte bei manchen Fragen aufgeworfen haben. Was ist ein Payload überhaupt? Genau dieser Frage wollen wir uns nun widmen und auch der Fragestellung, welche unterschiedlichen Typen von Payloads es gibt. Der Payload ist wohl der wichtigste Teil, den ein VXer bei seiner Arbeit an einem Virus bedenken muss; er

Abbildung 5. *Das Logo der Gruppe Electrical Ordered Freedom (EOF)*

beschreibt sozusagen den Kern des Virus. Allgemein könnte man sagen, dass der Payload der Teil des Codes ist, welcher zur Ausführung kommt, wenn der Virus aktiviert wird (etwa das Löschen eines Ordners etc.). VXer ordnen dabei die Art eines Virus entsprechend ihres Payloads in mehrere Kategorien ein. Die Oberkategorien wären Overwriter, Appender und Prepender. Wenn Ihnen diese Begriffe nichts sagen, so seien Sie beruhigt, wir werden sie nun genauer betrachten. Will man diese Kategorien verstehen, hilft es schon, wenn man die Namen aus dem Englischen übersetzt. Ein Overwriter stellt hierbei die simpelste Form eines Virus dar. Der Virus überschreibt einfach nur spezifische Dateien, entweder mit einem bestimmten Inhalt oder aber in vielen Fällen mit seinem eigenen Code. Ein Overwriter könnte also etwa so aussehen, dass ein Perl Virus im aktuellen Ordner nach Perl Dateien sucht und deren Inhalt so manipuliert, dass er deren Inhalt mit dem seinigen ersetzt. Führt der Anwender nun seine Perl Skripte aus, wird er in Wahrheit den Virus zur Ausführung bringen. So entsteht ein simpler Overwriter Virus. Die Begriffe Appender und Prepender sind von ihrer Struktur her recht ähnlich, nur der Code ist leicht angepasst. Im Prinzip bezeichnen sie das Voranstellen (Prepend) oder Hintenanstellen (Append) des Viruscodes an eine andere Datei. Klingt erst einmal sehr komplex, ist jedoch sehr leicht zu verstehen. Stellen sie sich wieder eine Perl Datei vor, welche eine Umrechnung von Grad in Fahrenheit vornimmt und einen Virus, welcher alle Dateien im aktuellen Verzeichnis infiziert, etwa einen Appender. Der Virus wird den Code des Perl Skriptes insofern nicht löschen, dass er nicht, wie bei einem Overwriter den kompletten Inhalt löscht. Vielmehr wird er sich hinten an den Code anhängen. Was dann passiert ist folgendes: Das Programm ist in seiner eigentlichen Funktion als Umrechnungsinstrument weiter nutzbar, führt jedoch am Anfang einen Jump (=Sprung) zum Viruscode aus, um anschließend wieder den Originalcode auszuführen. Ein Prepender tut in etwa das Gleiche, führt jedoch erst den Viruscode aus, um mit einer anschließenden Verzögerung ein Backup des Programmes zur Ausführung zu bringen. Wie sie sich denken könnten, waren dies nur wieder einige wenige Möglichkeiten eines Payloades, die typischsten sozusagen. Natürlich gibt es auch weitere, der Fantasie ist dabei keine Grenze gesetzt. Ein Payload wäre es auch, wenn etwa der aktuelle Hintergrund des Systems mit einer Signatur des Autors versehen wird oder aber wenn bestimmte AntiViren Seiten gesperrt werden. Zu unterscheiden gilt es hierbei noch einmal zwischen zwei Gruppen von Payloads: Den auffälligen und unauffälligen Payloads. Auffällige Payloads sind solche, die den Anwender eindeutig spüren lassen, dass er mit einem Virus infiziert wurde, etwa durch ein *merkwürdiges* Verhalten des Computers. Unauffällige Payloads sind solche, welche etwa bei einem Trojaner zum Einsatz kommen. Der Anwender soll von der Infektion keine Kenntnis nehmen und möglichst keinen Verdacht schöpfen. Ein gutes Beispiel sind hierbei die Codes von Joanna Rutkowska, welche gezeigt hat, wie es mit Virtualisierungstechniken möglich ist, das komplette System in eine Virtuelle Maschine zu versetzen, sodass der Anwender nicht merkt, dass er infiziert wurde. Auch aktuelle Anti-Viren Programme sind dann meist machtlos den Übeltäter überhaupt erst aufzuspüren. Bei Würmern stellen die Payloads meist zustäzlich die eingesetzte Verbreitungsroutine dar, etwa das Versenden via Email oder P2P-Netzwerk. Auch wäre es möglich Würmer über Netzwerkfreigaben zu verbreiten oder ähnliches. Bei Trojanern widerum stellt der Payload die Routinen dar, welche zur Verschleierung des Trojaners gedacht sind, etwa das Aktivieren des Trojaners als Linux Kernel Modul.

Kommunikation unter VXern

Mittlerweile sollten Sie schon einen großen Einblick in die Welt der Virusprogrammierung gewonnen haben, doch ein paar wenige Aspekte stehen noch aus. Denen wollen wir uns nun abschließend noch widmen. Da wäre zum einen die Frage, wie VXer miteinander kommunizieren und ihre Informationen untereinander austauschen. Wie die meisten Szenen im Internet betreiben fast alle Virenschreiber ihre eigenen Webseite, auf denen Sie ihre Kunst, ihre Viren, zur Schau stellen und anderen Einblicke in den Quellcode ermöglichen. In den seltensten Fällen liegen den Quelldateien die kompilierten Versionen bei, das liegt an der Ideologie, die sie nun schon kennengelernt haben. Es geht darum Wissen zu verbreiten, nicht aber Schaden anzurichten. Ein erster Anlaufpunkt für VXer stellt dabei die Seite vx.netlux.org (mittlerweile verlinkt diese auf vx.org.ua) dar, welche ein Riesenarchiv an Texten und Quellen enthält, über die man sich grundlegendes bis sehr spezifisches Wissen aneignen kann. Viele VXer Seiten sind direkt von dort auch verlinkt. Weiterhin lässt sich sagen, dass die meisten Seiten in Englisch gehalten sind. Wie auch im Berufsleben stellt Englisch die wichtigste Sprache zum Informationsaustausch dar, auch wenn manche Gruppen länderspezifisch organisiert sind. Nächstes Mittel der Kommunikation sind Emails, welche vorwiegend dann genutzt werden, wenn Informationen gezielt untereinander ausgetauscht werden, etwa über ein neues Projekt oder eine Technologie, welche bisher noch geheim gehalten werden soll. Ähnlich verhält es sich hier mit diversen Instant Messengern wie ICQ, MSN und Yahoo. Eines der wohl wichtigsten Kommunikationskanäle für VXer stellt das Undernet dar. Ein auf IRC basierendes Chatnetzwerk, in dem die wichtigsten VX Channels anzutreffen sind und über die die meisten Leute Einstieg in die Szene gewinnen und Kontakte knüpfen. IRC ist DAS Chatmedium unter VXern, wenngleich es nicht zu den sichersten gehört, ist es doch das beliebteste. Eine Hierarchie gibt es dabei kaum, jeder Fremde wird meist freundlich empfangen und nach seinen Interessen gefragt. Hilfe wird meist schnell und konkret geboten. Das Undernet stellt eine perfekte Anlaufstelle für jeden Interessierten dar. Von anderen Chattechnologien wie SILC halten sich Vxer bislang fern, auch wenn diese sicherheitstechnisch betrachtet sinnvoller erscheinen könnten. Doch all diese Mittel erscheinen erst einmal trivial, es bleibt jedoch noch eine letzte und wohl die wichtigste Kommunikationsart offen, die E-Zines. Der Begriff bedeutet nichts anderes als elektronisches Magazin. Im Normalfall ist damit eine auf HTML basierende Dateiensammlung gemeint, welche Quellcodes und Texte enthält und über den aktuellen Stand einer Gruppe oder über die Szene allgemein informiert. Diese E-Zines werden von verschiedenen Gruppen in regelmäßigen Abständen herausgegeben und werden dabei immer von der ganzen Szene mit Spannung erwartet, da im Vorfeld meist nicht bekannt ist, welche neuen Viren und Techniken veröffentlicht werden. Immer häufiger wird anstatt auf E-Zines auch auf Foren zurückgegriffen, doch hat sich diese Technik noch nicht genügend bewährt und wird eher weniger genutzt. Wie man sieht, nutzen auch VXer ganz normale Kommunikationswege, wie jeder andere auch, greifen jedoch auch auf szenetypische Eigenarten zurück.

Zusammenarbeit zwischen VXern und AntiViren Firmen

Auf den ersten Blick mag diese Überschrift sehr merkwürdig erscheinen. Welchen Grund sollte auch nur eine der beiden Parteien haben mit der anderen in irgendeiner Weise zusammenzuarbeiten, sind sie doch das komplette Gegenteil und kämpfen immer darum, dass sie die Oberhand gewinnen? Doch betrachtet man das ganze intensiver, wird deutlich, dass es eine Verbindung zwischen beiden gibt. Sie ist bei Weitem nicht mit der unter VXern zueinander zu vergleichen, aber es gibt sie. Eine Eigenart von VXern ist es zum Beispiel ihre Viren in ausführbarer Form (also etwa als *.exe Datei) an AntiViren Firmen zu schicken, damit diese die Viren untersuchen und eine Diagnose auf-

Über den Autor

Unter seinem Nicknamen SkyOut arbeitet Marcell Dietl seit 2007 an seiner Projektseite *www.smash-the-stack.net*, auf der er Programme und Texte rund um IT Security (VX eingeschlossen) veröffentlicht. Ebenso führt er dort seinen Blog und ist unter *skyout@smash-the-stack.net* zu erreichen. Derzeit bildet er sich persönlich im Bereich IT Security immer weiter und strebt nächstes Jahr eine Lehre oder ein Studium zum Informatiker an.

Im Internet

- *http://www.29a.net* – Die Seite der berühmten Gruppe 29A;
- *http://www.rrlf.de.vu* – Die Seite der deutschen Ready Rangers Liberation Front;
- *http://www.doomriderz.co.nr* – Die Seite des amerikanischen DoomRiderz Teams;
- *http://www.freewebs.com/purgatory-vx/* – Die VX Seite des iranischen Purgatory Teams;
- *http://www.eof-project.net* – Das EOF-Project;
- *http://vx.eof-project.net* – Das VX Forum des EOF-Projects;
- *http://vx.netlux.org* – Zentrale Anlaufstelle rund um Viren – mit Texten, Quellcodes und Links.
- *http://vxchaos.official.ws* – Datensammlung rund um VX und Security

stellen. Für beide Seiten bietet diese Verhaltensweise Vorteile. Die Firmen werden über Viren informiert, bevor diese in Umlauf kommen und können ihre Kunden besser sichern, die VXer entwickeln mit jedem mal ein wenig mehr Stolz. Unter VXern ist eine Virus Beschreibung seitens einer AntiViren Firma wie Sophos oder F-Secure, wie eine Trophäe, mit der man anderen imponieren kann und sein eigenes Selbstwertgefühl steigern kann. Eine weitere Verbindung, die zwischen VXern und Mitarbeitern bei Firmen, wie auch Symantec, besteht, ist die Tatsache, dass sich eben diese Mitarbeiter auch immer mit der Virusszene auseinandersetzen müssen. So hat mittlerweile fast jede große Firma einen eigenen Blog, in dem sie Neuigkeiten über die Szene niederschreibt. Es besteht also ein ständiges Interesse seitens der Firmen über die Szene auf dem Laufenden zu bleiben. Das schafft in gewisser Weise eine ironische Verbindung, trotz der gegensätzlichen Positionen, haben sie doch einiges gemein. Sie arbeiten zwar auf zwei verschiedenen Seiten, doch sind sie auch voneinander abhängig oder wie sollte eine Firma weiter bestehen, wenn es nichts mehr zu schützen gäbe, weil keine Gefahr mehr bestünde? Interessanterweise lässt sich hier noch anmerken, dass es zwei Arten von Firmenmitarbeitern gibt. Solche, die eher friedlich gegenüber der Szene eingestellt sind und solche, welche die Szene mit allen Mitteln zu bekämpfen versuchen, wenngleich dies komplett kontraproduktiv erscheint. Namen sollen hier nicht fallen, doch sind unter den VXern einige Analysten sehr in Verruf geraten, da sie sich zum Beispiel versuchten in die Szene einzuschleußen, um sie dann im Kern zu zerschlagen. Zum Glück ist ihnen das nie gelungen.

Abbildung 6. *Das Logo eines der größten Fileserver rund um VX*

Programmiersprachen der Szene

Abschließend wollen wir noch einen Blick auf typische Programmiersprachen der VX Szene werfen. Es gibt gewisse Sprachen, welche mehr vertreten sind und gewisse Trends, die sich in den letzten Jahren abgezeichnet haben. So lässt sich zum Beispiel sagen, dass Sprachen, welche plattformübergreifende Malware ermöglichen in letzter Zeit an Bedeutung gewonnen haben. So wird immer häufiger auf C# und das .NET Framework zurückgegriffen. Doch auch andere Sprachen dieses Frameworks werden immer wichtiger, etwa VB .NET. Weiterhin lässt sich sagen, dass vor allem Sprachen sehr beliebt sind, welche unter Windows funktionieren, da Windows noch immer die auch bei VXern meistgenutzte Plattform darstellt. Viele VXer programmieren zum Beispiel in Visual Basic, eine typische Programmiersprache für das Windows Betriebssystem. Als Trend zeigt sich hier vor allem eines: Skriptsprachen werden immer beliebter, hingegen sind LowLevel Sprachen immer weniger vertreten. So gibt es immer weniger Viren in Sprachen wie C, jedoch immer häufiger welche in Perl oder ähnlichen Skriptsprachen. Als Königsdisziplin gilt unter VXern jedoch das Programmierern in einer bestimmten Sprache: Der Assemblersprache. Welche Assemblervariante, sei es AT&T oder Intel Syntax, ist dabei erstmal zweitrangig. Die wichtigsten Viren der Szene wurden meist in ASM geschrieben und etwa die berühmte Gruppe 29A programmierte beeindruckende Viren in ASM, teils mit Quellcodes von bis zu 10 000 Zeilen. Auch sehr beliebt sind Makrosprachen, etwa für das produzieren von Viren für Word oder, wie wir gesehen haben, auch OpenOffice. Was lässt sich hier also zusammenfassend sagen: LowLevel Sprachen gelten weiterhin als Königsdisziplin eines jeden VXers, wenngleich Skriptsprachen immer beliebter werden, ebenso wie Sprachen für das .NET Framework.

Probleme der VX Szene

Als letzten Aspekt der Szene wollen wir noch einmal auf die Probleme dieser eingehen. Hier lassen sich vor allem zwei Dinge anmerken: Die Größe und die Dezentralisierung. Was stellt man sich aber darunter nun vor? Größe soll hier einfach nur verdeutlichen, dass die Szene in den letzten Jahren immer kleiner geworden ist und es teilweise an vielversprechendem Nachwuchs fehlt. Immer mehr VXer betreiben das Coden von Viren nur als ein nebensächliches Hobby und bleiben auch nur kurz in der Szene, das schafft einen ständigen Wandel der Konstellation von Gruppen und Autoren. Ein enormes Problem mittlerweile, da es kaum Gruppen beziehungsweise Autoren gibt, welche über viele Jahre in der Szene bleiben. Ständig kommen Neue hinzu und Alte verschwinden. Schätzungsweise gibt es derzeit etwa fünfzig VXer weltweit, wobei davon nicht alle gleichermaßen aktiv sind. Das zweite Problem, welches gewissermaßen aus dem ersten resultiert ist die Dezentralisierung der Szene. Es ist ganz einfach zu erklären: Jede neue Gruppe versucht ihr eigenes Projekt zu gründen und ruft etwa ein Forum ins Leben, viele dieser Foren sterben schnell wieder aufgrund der Inaktivität der Benutzer. Anstatt also alle an einem Strang zu ziehen, versucht jeder seinen Weg alleine zu gehen. Zwar gibt es zentrale Anlaufstellen, wie etwa vx.netlux.org, doch sind diese eher die Ausnahme. So gibt es derzeit etwa eine handvoll Foren in der Szene, das wohl aktivste ist das von EOF-Project, welches unter vx.eof-project.net zu erreichen ist. Meiner Meinung nach sollten VXer mehr zusammenarbeiten, anstatt *gegeneinander.* Gerade in einer solch kleinen Szene würde dies eine gewisse Stabilität schaffen. Wie die Entwicklung weitergehen wird, wird sich in den nächsten Monaten und Jahren zeigen. ●