

1 Schnell, perfekt und destruktiv – Der Witty-Wurm greift an

Freitag, 19. März 2004

Der Angriff beginnt kurz vor neun Uhr abends US-amerikanischer Pacific Standard Time. Der Internetwurm, der bereits wenige Stunden später unter dem Namen »Witty« besonders in den USA für Furore sorgen soll, wird über einen Rechner irgendwo im alten Europa in die freie Wildbahn des Internets entlassen. Noch ahnt niemand etwas von den gefährlichen Datenpaketen, die gerade ihre Expressreise starten. Die Sicherheitsspezialisten in den Labors der großen Antivirenfirmen haben Witty noch nicht auf ihrem Radar. Sie haben in diesen Tagen vermeintlich Wichtigeres zu tun.

Im japanischen Tauschbörsennetzwerk WinNY ist gerade ein besonders hinterhältiger Schädling aufgetaucht. Antinny.G, so der Name des Schadprogramms, wird über WinNY verbreitet, eine in Japan beliebte Musiktaschbörse. Das Schadprogramm hat es in sich. Es sammelt auf den Festplatten seiner unfreiwilligen Gastgeber eine Reihe privater Informationen und macht einen Schnappschuss vom Bildschirminhalt. All diese Informationen sollen nach dem Willen des Antinny-Programmierers nicht nutzlos auf den Festplatten seiner Opfer schlummern, sondern der breiten WinNY-Tauschbörsenöffentlichkeit zugänglich gemacht werden. Zu diesem Zweck erstellt Antinny automatisch ein ZIP-Archiv, sammelt dort alle gefundenen Informationen, fügt als Appetithäppchen eine zufällige MP3-Datei hinzu und bietet diese brisante Mischung als Musikdatei im Tauschbörsennetzwerk an.

Seinen Namen trägt der Schädling nicht von ungefähr. **Anti(n)-NY** soll die Musiktaschbörse WinNY sabotieren, ihren Nutzern eine nachhaltige Lehre erteilen und jeweils am 10., 20. und 30. Tag eines Monats versuchen, sämtliche Dateien auf dem Laufwerk C: zu löschen – kein Wunder also, dass sich die Antivirenfirmen Mitte März 2004 gerade diesem Schädling widmen. Tauschbörsen sind in Japan wie überall auf der Welt beliebt. WinNY zählte damals rund 200.000 Nutzer, die nun als potenzielle Kunden mit der neuesten Virensignatur versorgt werden wollen. Und die Antivirenfirmen wetteifern

untereinander darum, mit einer brandaktuellen Antinny-Virensignatur als Erste auf dem Antivirenmarkt zu protzen. Dass sich gerade ein noch gefährlicherer Schädling auf Netzreise begeben hat, können sie zu diesem Zeitpunkt noch nicht ahnen.

20:45:36 Uhr Ortszeit

Das Internetteleskop im San Diego Supercomputer Center (SDSC) meldet ungewöhnliche Netzaktivitäten. Die ersten Spuren des Witty-Wurms werden gesichtet. Der Wurm verbreitet sich nicht via Email, sondern direkt übers Internet von Rechner zu Rechner. Zu diesem Zweck erzeugt ein im Wurmcode eingebauter Zufallsgenerator wahllos IP-Adressen von Rechnern, an die er sich verschicken kann. Die Datenpakete, mit denen sich der Witty-Wurm im Netz ausbreitet, werden in San Diego aufgefangen und gespeichert. Später dienen sie als Material, um die regionale Ausbreitung des Wurms und seine Verbreitungsgeschwindigkeit im Netz rekonstruieren zu können. An diesem Freitagabend aber kümmert sich noch niemand um die ungewöhnlichen Datenströme, die das Internetteleskop in San Diego auffängt.

Schon bei anderen Netzattacken haben die Rechner im SDSC hervorragende Arbeit geleistet. Sie sind so programmiert, dass mit ihnen der Datenverkehr in Teilbereichen des Internets beobachtet und aufgezeichnet werden kann. Alle zufällig eingehenden Datenpakete werden von den kalifornischen Uni-Rechnern automatisch auf ihre IP-Zieladressen hin überprüft. Dabei konzentrieren sich die Computerspezialisten am SDSC auf diejenigen Teilbereiche des Internets, die ungenutzt brachliegen, deren IP-Adressen also noch nicht vergeben wurden.

Kein Anschluss unter diesen Nummern

IP-Adressen sind die »Telefonnummern« des Internets. Die gesamte Internetkommunikation läuft über diese Nummern. Sie werden weltweit systematisch und blockweise vergeben. Oberstes Vergabegremium ist die Internet Assigned Numbers Authority (IANA), die je nach Bedarf Blöcke von IP-Adressen an die regionalen Internetregistrierungsstellen verteilt. Für Europa, den Mittleren Osten, Nordafrika und Teile von Asien ist das RIPE NCC (Réseaux IP Européens Network Coordination Centre) zuständig. RIPE teilt allen Internetprovidern im Zuständigkeitsbereich einen Pool von IP-Adressen zu. Jeder Rechner, der sich ins Internet einwählt, erhält von seinem Internetprovider aus diesem speziellen IP-Adress-Pool für die Zeit seiner Internetverbindung eine

eindeutige IP-Adresse zugewiesen. Anhand dieser weltweit einzigartigen Adresse ist der einzelne Nutzer somit stets zu identifizieren.

Eine IP-Adresse nach IPv4-Standard besteht aus 32 Bit, wodurch über vier Milliarden Zahlen dargestellt und ebenso viele IP-Adressen vergeben werden können. Als sich ab Anfang der 1990er Jahre das Internet langsam zu etablieren begann und die Nutzerzahlen ab 1995 vor allem in den entwickelten Industrienationen explosionsartig anstiegen, befürchteten Experten, dass der IP-Adressraum bei diesem rasanten Entwicklungstempo bald knapp werden könnte. Vergabeengpässe wurden bereits für 1995 prognostiziert. Diese Befürchtungen bestätigten sich nicht. Auch heute noch werden Teile des theoretisch möglichen IP-Adressraums nicht benötigt – und exakt das machen sich die Computerwissenschaftler in San Diego mit ihrem Internetteleskop zu Nutze.

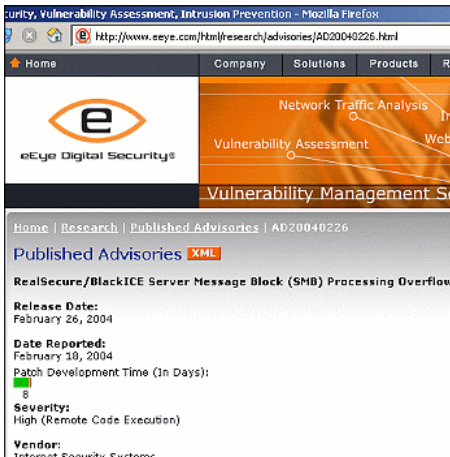
Telefonnummern, die es nicht gibt, werden in der Regel auch nicht angerufen. Entsprechendes gilt für die »Telefonnummern« des Internets. Wo keine IP-Nummern vergeben wurden, dürfte normalerweise auch kein Datenverkehr herrschen. Kein Internetnutzer surft IP-Adressen an, zu denen es keine Webseiten gibt. Wenn brachliegende IP-Adressbereiche dennoch plötzlich mit Anfragen und Datenpaketen überhäuft werden, kann die Ursache nur eine Anomalie sein. Der Internetwurm Witty produziert solch eine Anomalie. Er versendet sich automatisch und massenhaft an zufällig generierte IP-Adressen. Funktioniert der Zufallsgenerator einwandfrei, wird ein gewisser Prozentsatz der Datenpakete, mit denen sich der Wurm fortpflanzt, auch an brachliegende IP-Adressen verschickt. Diese Datenpakete »an niemanden« registriert das Internetteleskop in San Diego. »Kein Anschluss unter dieser IP-Nummer« – je häufiger die Analyseprogramme im SDSC solche Datenpakete pro Zeiteinheit aufspüren, desto größer ist die Aktivität des Wurms im Netz. Den kalifornischen Wissenschaftlern gelingt sogar noch mehr. Sie zerlegen das Witty-Wurmprogramm per »reverse engineering« in seine Einzelteile und analysieren vor allem seinen Zufallsgenerator. Es gelingt den Forschern, die automatisch generierten IP-Adressen zu rekonstruieren, sodass sie Wittys Spuren im Netz bis nach Europa zurückverfolgen können. Hier spüren sie am Ende gar jenen »Patient Zero« getauften Rechner auf, von dem aus das Wurmprogramm vermutlich freigesetzt worden war. Sein Angriffsziel: die Firewall-Software der Firma Internet Security Systems.

Drei Dinge braucht der sicherheitsbewusste Surfer: erstens einen Virenscanner, der Viren, Würmer und Trojaner zuverlässig identifiziert und beseitigt, zweitens regelmäßige Programm-Updates, die Sicherheitslücken in der verwendeten Software schließen und Schutzprogramme auf dem neuesten Stand halten, sowie drittens eine gute Firewall, die das System vor Angriffen von außen schützt. Diese Schutzsystem-Trias funktioniert nur so lange, wie sie

nicht selbst ins Visier von Angreifern gerät. Wurm Witty ist das erste Schadprogramm, das gezielt auf die Schutzsoftware einer ganz bestimmten Firma angesetzt wird. Er befällt ausschließlich Rechner, die durch eine bestimmte Sicherheitssoftware der Firma Internet Security Systems (ISS) vor Angriffen aus dem Netz eigentlich geschützt werden sollen. Eine Sicherheitslücke in dieser Schutzsoftware dient ihm als Einfallstor.

Hiobsbotschaften für ISS

Das erste Quartal 2004 läuft für das börsennotierte US-Sicherheitsunternehmen Internet Security Systems nicht sonderlich gut. Umsätze und Gewinne des Unternehmens mit Hauptsitz in Atlanta, Georgia, entwickeln sich schlechter als erwartet. Die Aktienkurse fallen von rund 20 Dollar zu Jahresbeginn auf einen Wert um 18 Dollar Ende März. Und nun auch noch das: Die agilen



eEye-Meldung 26.2.2004

Sicherheitsexperten der Konkurrenzfirma eEye entdecken in kurzen Zeitabständen zwei schwerwiegende Sicherheitslücken in verschiedenen ISS-Produkten. Die erste vertrauliche Warnung flattert ISS am 18. Februar 2004 ins Haus. Es dauert acht Tage, bis ISS diese Sicherheitslücke im Griff und einen Patch programmiert hat. Als eEye das Sicherheitsloch am 26. Februar schließlich publik macht, steht der Patch zum Schließen dieser Lücke schon bereit. Bis zur nächsten Hiobsbotschaft vergehen nur zehn Tage. eEye hat erneut eine gefährliche Sicher-

heitslücke in den so genannten Intrusion Detection Systems der Firma ISS entdeckt. Betroffen sind wiederum Schutzprogramme aus den ISS-Produktlinien »BlackICE« und »Real Secure«. Diese Produkte sollen Netzangriffe frühzeitig erkennen und abwehren. Zu diesem Zweck werden alle eingehenden Datenpakete von einem so genannten Protocol Analysis Modul (PAM) untersucht. Dieses Modul enthält eine Programmroutine zur Analyse von Datenpaketen, die mit dem beliebten Instant-Messaging-Programm ICQ verschickt werden. Sie werden erst freigegeben, wenn sie keinen schädlichen Code enthalten.

Am 8. März 2004 teilt eEye der ISS-Unternehmensleitung einen Programmfehler genau in diesem Modul mit. Durch speziell manipulierte Datenpakete können die betroffenen Schutzprogramme der Serie »BlackICE« und »Real Secure« selbst zum Ziel eines Angriffs werden. Noch hat sich diese neuerliche Sicherheitslücke in den einschlägigen Internetforen nicht herumgesprochen. Einen Exploit, der diese Lücke ausnutzt, gibt es noch nicht. Die Entdeckung wird deshalb vertraulich behandelt. Niemand soll etwas davon erfahren, bevor ISS nicht den entsprechenden Flicker zum Ausbessern der Sicherheitslücke parat hat.

Zehn Tage später, am 18. März, ist es so weit: Der Sicherheitsflicker ist fertig. eEye und ISS veröffentlichen gemeinsam Details zu den neuerlichen Sicherheitsproblemen bei ISS. Gleichzeitig legt ISS seinen Kunden das frisch programmierte Sicherheits-Update zur sofortigen Installation ans Herz. ISS könnte die leidige Angelegenheit nun abhaken. Die Firma hat rasch und richtig reagiert, das Update steht im Netz, geschäftsschädigende Negativschlagzeilen sind kaum noch zu erwarten. Im Gegenteil kann man sich rühmen, in nur knapp zehn Tagen ein funktionierendes Update produziert und seine Kunden informiert zu haben. Unternehmen wie Microsoft benötigen dafür schließlich manchmal Monate. Was die Manager bei ISS zu diesem Zeitpunkt noch nicht wissen können: Das Schlimmste steht ihnen und ihren Kunden noch bevor. Denn nur knapp 36 Stunden später wird Internetwurm Witty ausgesetzt, und Witty nutzt zu seiner Verbreitung im Internet exakt jene Sicherheitslücke in ISS-Produkten aus, die gerade eben erst bekannt geworden ist.

19. März 2004, 20:45:46 Uhr: Witty greift an

Witty kommt sekundenschnell auf Touren. Zehn Sekunden, nachdem das Internetteleskop in San Diego die ersten Witty-Datenpakete aufgefangen hat, sind bereits 110 Computer infiziert. Weitere zwanzig Sekunden später hat sich Witty erfolgreich an insgesamt 160 Systeme versendet. Diese Rechner dienen ihm als Ausgangsbasis. Von nun an schwächt sich seine Verbreitungsgeschwindigkeit ab und erreicht jene statistischen Normalwerte, die für Wurmprogramme seiner Art typisch sind. 45 Minuten nach seinem fulminanten Start ist Wittys Verbreitung bereits so gut wie abgeschlossen. 12.000 Rechner, auf denen die anfällige ISS-Schutzsoftware ohne Sicherheitsflicker installiert ist, sind durch Witty infiziert.

Witty ist ein schlanker Wurm. Die Datenpakete, mit denen er durchs Netz reist, sind nur rund 800 Bytes groß. Er gehört wie beispielsweise der Slammer-Wurm, der im Januar 2003 eine Windows-Sicherheitslücke ausnutzte und weltweit rund eine halbe Million Rechner infizierte, zur Klasse der dateilosen

Würmer, die sich in Form manipulierter Datenpakete direkt übers Internet verbreiten. Wittys Programmierer verzichtet in seinem Code auf jeden Ballast. Der einzige Programmluxus, den er sich leistet, ist die Zeichenkette »insert witty message here« (»witzige Nachricht hier einfügen«), von der der Wurm später seinen Namen bezieht. Trotz dieser Zeichenkette ist Witty (englisch für witzig, geistreich) alles andere als »witzig« gemeint. Die Nebenbedeutung der englischen Vokabel »witty« trifft den Kern des Wurms schon wesentlich genauer: Witty wurde »geistreich« programmiert. Sein Schöpfer ist ein Profi und programmiertechnisch ein Meister seines Fachs. Er arbeitete fehlerfrei. Anders als viele andere fehlerhaft bis dilettantisch programmierte Schadprogramme besitzt der Witty-Wurm keine »unerwünschten« Nebenwirkungen. Er erfüllt seine Aufträge korrekt, gründlich und exakt so, wie sie ihm sein Schöpfer aufgetragen hat.

Zwei Aufträge hat Witty von seinem Programmierer mit auf den Weg bekommen: »Infiziere möglichst viele Rechner, die mit der anfälligen ISS-Schutzsoftware ausgerüstet sind, und zerstöre anschließend die gastgebenden Systeme!« Witty führt diese Aufträge gewissenhaft aus. Zunächst aktiviert der Wurm seinen eingebauten Zufallszahlengenerator, liest die Systemzeit des befallenen Rechners aus und generiert 20.000 zufällige IP-Adressen, an die er sich umgehend versendet. Schadprogramme, deren Ziel es ist, weltweit möglichst viele Rechner anzugreifen, sind meist allein auf ihre eigene Verbreitung programmiert. Fortpflanzung, nicht Zerstörung ist ihr Daseinszweck. Sie richten sich in den befallenen Systemen häuslich ein, schalten Virens Scanner und Firewalls ab, verewigen sich in der Windows-Registrierung, kopieren sich in die entsprechenden Systemordner und sorgen dafür, dass sie bei jedem Systemstart ebenfalls gestartet werden. Durchschnittswürmer verhalten sich unauffällig. Der Gastgeber soll schließlich nicht bemerken, dass er einem blinden Passagier Asyl gewährt. Schadprogramme, die den Rechner ihres Gastgebers angreifen und seine Daten zerstören, gibt es äußerst selten. Witty gehört zu dieser gefährlichen Sorte. Hat er sich seinem einprogrammierten Fortpflanzungstrieb gehorchend an 20.000 zufällig generierte IP-Adressen versandt, widmet er sich dem Rechner seines Gastgebers. Er überschreibt zufällig ausgewählte Bereiche auf den Festplatten des Systems, was zu einem sofortigen Schaden führt, die Verbreitung des Wurms aber zunächst nicht gefährdet. Fortpflanzung und Zerstörung von Daten lösen sich dann im Wechsel ab, bis das System unbrauchbar wird und abstürzt. In einem Haus, das abgerissen werden soll, richtet sich kein Abrisskommando häuslich ein. Witty ist deshalb als speicherresidenter Wurm konzipiert. Er hält sich nur im Arbeitsspeicher der befallenen Systeme auf. Dort agiert er so lange, bis der Computer heruntergefahren wird oder auf Grund der angerichteten Zerstörungen am Ende abstürzt.

Wo ist Patient Zero?

Die Frage aller Fragen ist noch immer unbeantwortet: Wer hat den Witty-Wurm mit welcher Absicht programmiert? Der Computerwissenschaftler Abhishek Kumar vom Georgia Institute of Technology und seine beiden Kollegen Vern Paxson und Nicholas Weaver vom International Computer Science Institute haben sich dem Urheber des Witty-Wurms erstaunlich weit genähert. Sie werteten die Daten aus, die die Internetteleskope in San Diego und an der Universität von Wisconsin aufgezeichnet hatten, analysierten das Wurmprogramm per »reverse engineering« und konzentrierten sich dabei auf das Herz des Wurms, das ihm als Wegweiser durchs Internet diente: seinen (Pseudo-)Zufallszahlengenerator, mit dem die IP-Adressen erzeugt worden waren, die der Wurm mit seinem Besuch beehren wollte. Dabei stießen sie auf eine absichtlich programmierte Schwäche des Zufallsgenerators im ansonsten makellosen Wurmprogramm. Bestimmte IP-Adressbereiche ließen sich mit ihm nicht erzeugen. Diese Informationen genügten, um Wittys Weg durchs Netz zurückzuverfolgen bis zu jenem ersten System, dem »Patient Zero«, von dem aus der Schädling freigelassen worden war. Wittys Geburtsrechner stand in Europa. Seine Adresse gehörte zum IP-Adresskontingent eines europäischen Internetproviders. Damit nicht genug, fanden Kumar und Kollegen noch erheblich mehr heraus.

Witty wurde von »Patient Zero« aus nicht wahllos, sondern gezielt an 110 Erstverbreiter geschickt – erstaunlicherweise allesamt Rechner, auf denen die sicherheitsanfällige Version des ISS-Schutzprogramms BlackICE installiert worden war. Die IP-Adressen dieser Rechner lagen außerhalb des Bereichs, den der eingebaute Zufallszahlengenerator generieren konnte. Die ersten 110 Rechner müssen dem Urheber des Wurmprogramms also bekannt gewesen sein. Sie wurden bewusst zur Erstverbreitung eingesetzt. Kumar und Kollegen haben auch den Standort der Erstverbreiter lokalisieren können. Alle 110 Rechner befanden sich auf einer US-amerikanischen Militärbasis.

Die Frage nach dem Urheber des Witty-Wurms lässt sich somit auf einen ganz bestimmten engen Personenkreis eingrenzen. Witty muss von einer Person geschrieben worden sein, die erstens über hervorragende Programmierkenntnisse verfügte und zweitens die Möglichkeit besaß, ihre am Ende nahezu makellose Wurmkeure ungestört testen zu können. Drittens kommt als Autor nur eine Person in Frage, die frühzeitig die fragliche Sicherheitslücke in ISS-Produkten kannte und viertens wusste, dass das US-Militär in einer ganz bestimmten Militärbasis 110 Rechner betrieb, auf denen die angreifbare ISS-Schutzsoftware lief. Diese Schlussfolgerungen legen die Vermutung nahe, dass Witty von einem ehemaligen oder seinerzeitigen Mitarbeiter des US-Unterneh-

mens ISS geschrieben und verbreitet worden war – ein Verdacht, zu dem die Firma ISS bisher jeden Kommentar verweigert.

Auch die Sicherheitsindustrie kocht nur mit Wasser

Jede Softwarefirma reagiert gereizt, wenn es um Sicherheitsprobleme in den eigenen Programmen geht. Keine Software ist perfekt. Doch Sicherheitslücken sorgen – nicht nur in der informierten Fachwelt – für ein schlechtes Image, zumal dann, wenn sich die Probleme häufen. Die Sicherheitslücke der Firma A fungiert auf dem Softwaremarkt für Firma B als Wettbewerbsvorteil. Voraussetzung ist natürlich, dass der Wettbewerb über den Markt tatsächlich funktioniert. Aber selbst Unternehmen wie Microsoft, die im Bereich der Betriebssysteme ein Quasi-Monopol besitzen, können es sich auf die Dauer nicht leisten, mit periodisch wiederkehrenden, eklatanten Sicherheitsmängeln in die Schlagzeilen zu geraten. Sie laufen Gefahr, Marktanteile an die Konkurrenz speziell aus dem Open-Source-Bereich abgeben zu müssen. Verlorene Großaufträge der öffentlichen Hand oder aus der Wirtschaft, bei deren Vergabe Sicherheitsaspekte immer eine ganz besonders wichtige Rolle spielen, können rasch einen Flächenbrand auslösen, der die Dominanz eines marktbeherrschenden Softwareunternehmens wie Microsoft insgesamt zwar nicht beeinträchtigt, die Umsätze jedoch empfindlich schmälern kann. Nicht umsonst hat Bill Gates höchstpersönlich das Thema »Sicherheit« im Hause Microsoft zur Chefsache erklärt.

Was für marktdominierende Unternehmen wie Microsoft gilt, trifft die Hersteller von Sicherheitssoftware noch wesentlich härter. Sie müssen sich erstens auf einem relativ intakten Markt gegenüber der Konkurrenz mit ihren Produkten behaupten, und zweitens kratzt jede neue Sicherheitslücke am gern gepflegten Branchenmythos, Sicherheitsfirmen würden »Sicherheit« produzieren. Dass die Schutzsoftware, die die Sicherheitsindustrie herstellt und vertreibt, möglicherweise selbst unsicher ist, zum Ziel von Angriffen und damit zum Einfallstor für gefährliche Schadprogramme werden kann, kratzt am Image der betroffenen Firmen und passt der ganzen Branche nicht ins Werbe- und PR-Konzept. Der Witty-Wurm schädigte deshalb nicht nur das Unternehmen ISS, sondern konnte exemplarisch aufzeigen, dass die gesamte Sicherheitsindustrie bei ihren Schutzprogrammen letztlich nur mit Wasser kocht. Ihre Programme bieten keinen absoluten Schutz. Sie produzieren höchstens relative Sicherheit.

Besaß Witty also eine aufklärerische Funktion? War Witty ein »gutes« Wurmprogramm, das Computernutzern demonstrieren wollte, wie trügerisch die Versprechungen der Sicherheitsindustrie letztlich sind? Die Antwort ist ein

klares Nein. Witty sollte die Betreiber der angegriffenen Systeme weder informieren noch aufklären. Witty sollte gezielt angreifen und zerstören. Sein Schöpfer war ein Fachmann. Er wusste, was er tat. Er pflanzte seinem Wurmprogramm ein exakt kalkuliertes, todsicher funktionierendes Schadpotenzial ein und nutzte die ihm bekannte Sicherheitslücke in der ISS-Schutzsoftware bewusst aus, um in möglichst viele »ungeschützte« Systeme – egal ob in Krankenhäusern, Militärbasen oder bei Privatanwendern – einzudringen, dort schrittweise Daten zu löschen und die Systeme am Ende unbrauchbar zu machen. Sicherheitsexperten sehen hier den Beginn einer gefährlichen Entwicklung.

Witty hat bis dato keinen würdigen Nachfolger gefunden. Die meisten Wurmprogramme, die in die freie Wildbahn des Internets entlassen werden, nutzen immer noch hauptsächlich Sicherheitslücken in Microsoft-Programmen und Schwachstellen in Windows-Betriebssystemen aus. Auch dezidiert destruktive Würmer gibt es eher selten. Die allermeisten Schadprogramme wollen ihre gastgebenden Systeme nicht zerstören, sondern für weitere kriminelle Aktivitäten wie ferngesteuerten Spamversand oder Distributed-Denial-of-Service-Angriffe nutzen. Dennoch hat die Sicherheitsbranche nicht den geringsten Grund zum Aufatmen. Wie die US-amerikanische Unternehmensberatungsfirma Yankee Group herausgefunden hat, steigt die Zahl der Sicherheitslücken, die in Schutzsoftware entdeckt werden, seit Auftreten des Witty-Wurms überdurchschnittlich an. Es scheint, als habe der Wurm eine Vielzahl von Hackern, kriminellen Crackern und professionellen Sicherheitsspezialisten erst auf die Idee gebracht, die Produkte der Sicherheitsbranche genauer unter die Lupe zu nehmen. Was sie dort entdeckten, wirft auf die Branche kein besonders gutes Licht.

Schutzprogramme überwachen das System und haben regelmäßig uneingeschränkte Zugriffsrechte auf sämtliche wichtige Funktionen des Betriebssystems. Wer über eine unsichere Firewall in ein System einbricht, kann den Rechner also nach Lust und Laune manipulieren. Das macht Schutzprogramme für einen potenziellen Angreifer besonders attraktiv. Das allein schon müsste für die Sicherheitsfirmen eigentlich Grund genug sein, ihre Produkte besonders intensiv und penibel auf Bits und Bytes zu überprüfen, bevor sie auf den Markt geworfen werden. Das Gegenteil ist offenbar der Fall. Im Zeitraum von Januar 2004 bis Ende März 2005 zählten die Statistiker der Yankee Group 77 Sicherheitslücken in Schutzprogrammen, wobei die Zahl der entdeckten Risiken ab dem zweiten Quartal 2004, also nach dem Witty-Intermezzo, wesentlich stärker zunahm als die der Mängel etwa in Microsoft-Produkten, dem derzeitigen Marktführer in Sachen Sicherheitslücken und Schwachstellen. Betroffen waren insbesondere die großen Anbieter in Sachen Sicherheit. Große Ziele trifft man eben besser. 26 Prozent der gemeldeten

Sicherheitslücken wurden von Spezialfirmen wie eEye oder von konkurrierenden Unternehmen aufgespürt. Knapp die Hälfte wurde von unabhängigen oder anonymen Fachleuten beispielsweise in einschlägigen Internetforen publiziert. Die Sicherheitsfirmen selbst haben aus der Witty-Warnung offenbar wenig gelernt. Lediglich 16 Prozent aller Sicherheitslücken haben diese Firmen selbst entdeckt. Die Endkontrollen seien noch immer viel zu lasch, meinten die Analysten der Yankee Group. Die Sicherheitsfirmen sollten sich gefälligst endlich darum kümmern, die Qualität ihrer Software zu erhöhen. Neue Produkte sollten erst dann auf den Markt geworfen werden, wenn sie eine intensive Sicherheitsüberprüfung durchlaufen hätten. Solche Qualitätskontrollen werden umso dringlicher, als sich laut Yankee Group in den einschlägigen Internetforen längst ein schwarzer Markt auch für Exploits von Sicherheitssoftware herausgebildet hat. Es ist also nur eine Frage der Zeit, bis auf Wittys Spuren das erste destruktive Schadprogramm mit dezidiert kriminellem Hintergrund auf unsichere Schutzsoftware angesetzt wird. Experten sind sich sicher: Der nächste Witty kommt bestimmt.

Quellen

Andrew Jaquith: Fear and Loathing in Las Vegas: The Hackers Turn Pro.

http://www.yankeegroup.com/public/products/decision_note.jsp?ID=13157, letzter Zugriff am 22.01.2006.

Abhishek Kumar/Vern Paxson/Nicholas Weaver: Exploiting Underlying Structure for Detailed Reconstruction of an Internet-scale Event.

<http://www.cc.gatech.edu/%7Eakumar/witty-draft.pdf>, letzter Zugriff am 22.01.2006.

David Moore: Network Telescopes.

<http://www.caida.org/outreach/presentations/2003/dimacs0309/dimacs200309.pdf>, letzter Zugriff am 22.01.2006.

Colleen Shannon/David Moore: The Spread of the Witty Worm.

<http://www.caida.org/analysis/security/witty/>, letzter Zugriff am 22.01.2006.