Würmer: Gefahr im Internet?

Jens Tölle

Rheinische Friedrich-Wilhelms-Universität Bonn
Institut für Informatik IV
Römerstraße 302
53117 Bonn
toelle@cs.uni-bonn.de

Abstract: Dieser Bericht beschreibt eine aktuelle Bedrohung von Rechnern im Internet, die mittlerweile nicht mehr nur von Fachleuten wahrgenommen wird. Die Berichterstattung über sogenannte Würmer hat bereits den Sprung in die Hauptnachrichtensendungen und die Tagespresse geschafft. Wie stark ist die aktuelle Bedrohung tatsächlich? Wie könnte sich diese Situation in Zukunft verändern? Welche Maßnahmen und welche Verhaltensweisen sind sinnvoll?

1 Einleitung und Definition

„Ein Computerwurm ist eine selbständige Programmroutine, die sich selbst reproduziert, indem sie über ein Computernetzwerk an Computerprogrammen oder Betriebssystemen anderer Computer Manipulationen vornimmt." – Dieses Zitat aus [1] gibt eine der zahlreichen Definitionen des Begriffes Wurm wieder.

Der wesentliche Aspekt dieser Definition ist die selbsttätige Ausbreitung eines Wurmes ohne (oder mit wenig, i.d.R. unfreiwilliger) Hilfe der Benutzer der betroffenen Computersysteme. Unter Berücksichtigung dieses Aspektes erscheint es sinnvoll zu sein, Würmer in zwei Kategorien einzuteilen.

Diese beiden groben Kategorien sind Mail-Würmer und aktive Würmer. Ein Mail-Wurm nutzt zur Verbreitung E-Mails. Ein empfangender Rechner muss durch Ausnutzung von nicht geschlossenen Sicherheitslücken in der Mail-Software zur automatischen Weiterleitung der Mail an möglichst viele weitere Empfänger gebracht werden. Zur Erstellung der Liste der weitere Empfänger bedient sich der Wurm im Regelfall aus dem persönlichen Adressbuch des Rechnernutzers. Alternativ muss die Wurm-Mail so verfasst sein, dass der Leser der Mail dazu gebracht wird, ein mitgesendetes ausführbares Programm zu starten. Wurmautoren täuschen hierbei beispielsweise falsche Dateiendungen vor, behaupten, dass die angehängte Datei wichtige Informationen enthält oder versprechen kostenfreien Zugang zu normalerweise kostenpflichtigen Inhalten.

Im Regelfall sind die Methoden raffiniert genug, um eine nennenswerte Nutzerzahl zur Ausführung der mitgesendeten Datei zu verleiten. In letzter Zeit ist zudem eine deutliche Zunahme der Kreativität der Wurmautoren zu bemerken, um Nutzer zur Ausführung der entsprechenden Wurminstanzen zu verleiten.

Aktive Würmer versuchen sich ohne Nutzung des Mediums E-Mail zu verbreiten. Genutzt werden beliebige Dienste und Protokolle des Internets, sofern die Verbreitung ausreichend ist und potentielle Schwachstellen bekannt sind.

2 Geschichte – Würmer damals...

Ein Blick zurück auf die Geschichte der Ausbreitung von Würmern im Internet zeigt einige Eigenschaften von Würmern, die auf für das Verständnis der heutigen Situation lehrreich sind.

Der erste Wurm ist der im Jahre 1988 aus freigesetzte und nach seinem Programmierer benannte Morris-Wurm. [2]. Eine Analyse des damaligen Vorfalls zeigte folgende Besonderheiten: Der Wurm war unsauber programmiert und hat sich deshalb sehr aggressiv vermehrt, ist durch die dadurch aufgetretene Überlast früh bemerkt worden und konnte deshalb schnell bekämpft werden. Trotzdem befiel er ca. 10% aller damals an das Internet angeschlossenen Systeme. Weiterhin nutzte der Wurm längst bekannte Sicherheitslücken. Es bestand somit keine besondere Leistung darin, neue Lücken und Methoden zu deren Ausnutzung zu finden, sondern es handelte sich lediglich um die automatisierte Ausnutzung von Profis bekannten Angriffsmustern.

Weiterhin war es schwer bis unmöglich, verlässliche Informationen über angerichtete Schäden zu beziehen. Alle diese Eigenschaften sind auch bei heutigen Würmern zu finden.

3 ...und Würmer heute

Auch heute gibt es bei Würmern unsaubere Programmierung: Erste Versionen des Code-Red-Wurms 2001 [3] enthielten einen fehlerhaften Mechanismus zur Bestimmung neuer Angriffsziele. Dadurch verzögerte sich die Ausbreitung drastisch. (Alle Wurm-Instanzen starteten einen Pseudozufallszahlengenerator mit dem gleichen Startwert, so dass diese Instanzen versuchten, von anderen Wurminstanzen bereits besuchte Systeme zu infizieren, die entweder bereits infiziert waren oder sich nicht infizieren ließen.). Erst eine zweite Version, die kurze Zeit später in Umlauf gebracht wurde, war mit einem verbesserten Ausbreitungsmechanismus versehen. Inzwischen wurden aber bereits einige der verwundbaren Systeme abgesichert, so dass dieser Wurm zwar beachtlichen Ausbreitungserfolg hatte, aber bei sauberer Programmierung noch einiges erfolgreicher (aus der Sicht des Programmierers) und gefährlicher (aus der Sicht der Internet-Nutzer) hätte sein können.

Es ist auch heutzutage nicht schwer, Sicherheitslücken und auch Programmcode zur Ausnutzung dieser Lücken zu finden. Es erfordert also keine exzellenten Systemkenntnisse mehr, einen solchen Wurm zu erstellen.

Weiterhin ist es auch heute schwierig, zuverlässige Schätzungen von durch Würmern verursachten Schäden zu erhalten. Die Auskunftsfreudigkeit von Betroffenen ist entweder sehr gering, da die Netzwerke und Rechner der betroffenen nicht als schlecht gewartet und gesichert dargestellt werden sollen, oder Schadenssummen werden drastisch übertrieben, beispielsweise um damit den Absatz von Schutzsoftware oder Consulting-Leistung zu erhöhen.

Viele der bisher in freier Wildbahn aufgetretenen Würmer hatten bis jetzt keine „ernsthaften“ Schadroutinen, so dass beispielsweise die Schäden durch Datenverluste bis heute auch deutlich höher hätten ausfallen können!

Alle diese Punkte sind Grund genug, sich die aktuellen Stand der Dinge im Internet anzusehen. Die „Qualität“ der Würmer nimmt sowohl in Bezug auf die Fähigkeit zur Ausnutzung von bekannten Sicherheitslücken als auch in Bezug auf die Gefährlichkeit der Schadroutinen zu.

4 Und was kommt dann...?

Tatsache ist, dass Wurm-Programmierer noch „geschicktere“ Würmer implementieren können und werden.

Folgende Aspekte sind dabei wichtig: Durch steigende Rechnerzahl (und die damit einhergehende Anzahl verwundbarer Rechner) steigt die potentielle Ausbreitungsgeschwindigkeit, da es für eine Wurminstanz leichter wird, einen neuen verwundbaren Rechner zu finden. Standardinstallationen enthalten immer mehr Dienste, die für Angriffe genutzt werden können. Patches zum Schließen von Sicherheitslücken werden oft verspätet oder gar nicht installiert. Gerade eine große Zahl an Heimanwendern sorgt sich wenig um ein sicheres System. Selbst sicherheitsbewussten Anwendern wird das Absichern Ihres Systems nicht leicht gemacht. In [4] berichtet ein Anwender vom Versuch, ein frisch installiertes System durch Nachladen von Updates aus dem Internet abzusichern. Die Versuche wurden jedoch mehrfach durch einen Angriff des Blaster-Wurms [5] auf den zu diesem Zeitpunkt noch nicht geschützten Rechner unterbrochen.

Ein Trend sind Wurmbaukästen, die gleich mehrer Verwundbarkeiten ausnutzen und eine Auswahl an Schadroutinen bieten. Damit ist ein sehr aggressiver Wurm auch durch absolut unkundige Angreifer zu erstellen. [6] ist ein Beispiel für einen im Quellcode verbreiteten Wurm. Weiterhin zeigen Forschungen wie in [7] beschrieben, dass die Ausbreitungsgeschwindigkeit von Würmern durch geschicktere Verfahren noch gesteigert werden kann.

Wie üblich wird es auf einen Wettlauf zwischen Wurm-Autoren und Verteidigern hinauslaufen. Ein Beispiel für diesen Wettlauf ist der E-Mail-Wurm Bagle/Beagle [8], der in manchen Versionen eine Schadroutine in einem verschlüsselten Anhang enthielt und das notwendige Passwort zur Verschlüsselung im Mailtext mitlieferte. Durch die Verschlüsselung mit einen zufälligen Passwort wurde eine automatische Erkennung und Filterung der Mails erschwert. Nachdem entsprechende Scanner das Passwort aus dem Mail-Text extrahieren und damit den gefährlichen Anhang erkennen konnten, wurde das Passwort in späteren Wurmvarianten als Grafik übertragen, um eine automatische Texterkennung zu verhindern.

5 Maßnahmen

Zusammenfassend lässt sich feststellen, dass die üblichen Sicherheitsmaßnahmen (aktuelle Patches, Firewalls mit restriktiven Filterregeln, aktuelle Virenscanner,...) im Regelfall zwar wirksam sind und deshalb keinesfalls vernachlässigt werden sollten.

Trotzdem besteht Forschungsbedarf im Bereich der automatischen Erkennung und Abwehr von Wurmausbreitungen. Basis für unter Beteiligung des Insituts für Informatik IV der Universität Bonn entwickelte Verfahren [9] zur automatischen Erkennung von Wurmausbreitungen sind Systeme, die von Würmern verursachte ungewöhnliche Verkehrsmuster im Inneren überwachter Netze sowie an Netz-Außenanbindungen erkennen können und davor warnen. Durch den Einsatz graph-basierter Methoden ist es möglich, wurm-typische Aktivitäten (Suche nach verwundbaren Rechnern, Durchmusterung von Adressräumen, auch in verschleierter Weise, Zugriffsversuche auf von Wurminstanzen installierte Hintertüren,...) zu entdecken, von der normalen Systemnutzung zu unterscheiden und frühzeitig zu warnen.

Literaturverzeichnis

[1] Wikipedia – Die freie Enzyklopädie, de.wikipedia.org, Stichwort Computerwurm

[2] Internet Engineering Taskforce, "The Helminthiasis of the Internet" – RFC 1135, www.ietf.org/rfc/rfc1135.txt

[3] CERT-Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL, www.cert.org/advisories/CA-2001-19.html

[4] www.techuser.net/index.php?id=47

[5] Bundesamt für Sicherheit in der Informationstechnik – www.bsi.de/av/vb/blaster.htm

[6] Symantec – http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.gen.html

[7] Harald Schmidt, „Simulation und Erkennung der Ausbreitungsstrukturen von Würmern", Univ. Bonn, Diplomarbeit, 2002

[8] Bundesamt für Sicherheit in der Informationstechnik – www.bsi.de/av/vb/beaglex.htm

[9] Marko Jahnke, Martin Lies, Sven Henkel, Michael Bussmann, Jens Tölle: Komponenten für kooperative Intrusion-Detection in dynamischen Koalitionsumgebungen. Erscheint in: Proc. Detection of Intrusions and Malware & Vulnerability Assessment, DIMVA 2004