Würmer angeln

Immer mehr Zero-Day-Exploits machen den Security-Admins das Leben schwer. Wer auf Nummer sicher gehen will, wartet nicht auf Warnmeldungen von Sicherheitsanbietern, sondern stellt eine eigene Wurmfalle auf. Zum Beispiel mit Nepenthes.

ACHIM WAGENKNECHT

Die Existenz von so genannten Zero-Day-Exploits zeigt deutlich, dass es immer wieder Zeitfenster gibt, in denen ein System anfällig für Attacken ist – trotz des regelmäßigen Einspielens von Patches. Je schneller und aggressiver die Cracker angreifen, desto wichtiger werden wirksame Frühwarnsysteme. Dazu gehört Nepenthes. Das Programm ist nach einer fleischfressenden Pflanze benannt und so wie diese Insekten in die Falle lockt, fängt Nepenthes Computerwürmer ein. Die gespeicherten Schadprogramme können dann mit aktuellen Virenscannern überprüft werden. Ist ein Wurm keinem der verfügbaren Antivirenprogramme bekannt, sollten Sie ihn zwecks Analyse an den Hersteller Ihrer Antiviren-Software schicken – verschlüsselt, versteht sich. Alternativ können Sie sich an die Firma Norman wenden. Die stellt nämlich ihre automatische Analyse-Sandbox im Web unter *http://sandbox.norman.com/live_4.html* bereit. Hier können Sie Ihre Würmer zur Analyse hochladen.

Virenscanner testen

Umgekehrt können mit Nepenthes gesammelte Schadprogramme auch dazu dienen, die Erkennungsleistung von Antivirenprogrammen zu testen. Was Nepenthes fängt, stammt definitiv aus freier Wildbahn und ist mit sehr hoher Wahrscheinlichkeit schädlich. Was sonst außer Malware sollte an eine Schwachstelle andocken und sich auf den Zielrechner kopieren? So ist es mit Hilfe einiger ungefilterter E-Mail-Accounts und einiger Nepenthes-Rechner heute nicht schwierig, Viren und Würmer, die sich nachweislich »in the wild« befinden, zu sammeln. Die von einem internationalen Team von Antivirenexperten mühevoll zusammengestellte Wildlist ITW könnte dadurch überflüssig werden *(www.wildlist.org)*.

Antivirenhersteller stellen die Wildlist gerne als wichtigste Messlatte für die Erkennungsleistung ihrer Produkte dar. Da jedes Antivirenprogramm, das etwas auf sich hält, aber hundert Prozent der Wildlist-Viren erkennt, sind Tests auf dieser Basis nicht wirklich aussagekräftig. Aber dank Nepenthes sind Sie ja auch nicht mehr darauf angewiesen, solchen Tests zu vertrauen. Wer Antivirenprogramme mit Hilfe von Nepenthes testet, kann zu ganz anderen Ergebnisse kommen. Das Nepenthes-Team selbst hat das gemacht und bezeichnet die Ergebnisse als »erstaunlich oder schockierend«. Statt durch die Bank hundert Prozent zu erkennen, lagen die tatsächlichen Erkennungsraten zwischen 64 und 99 Prozent. Bei einem ähnlichen Test des Luxemburger Computer Security Research and Response Teams lagen die Erkennungsraten sogar nur zwischen 34 und 71 Prozent *(www.csrrt.org)*. Wenn Sie Nepenthes eine Zeitlang einsetzen, können Sie mit dem gesammelten Material die Erkennungsraten der Virenscanner testen.

Sicher unter Linux

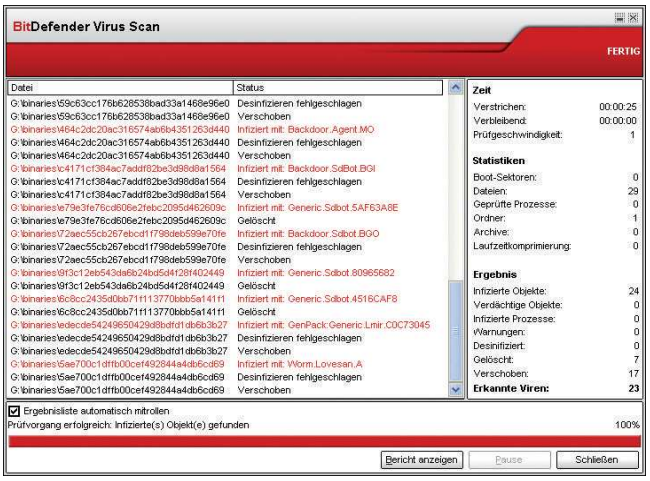
Nepenthes emuliert bekannte Schwachstellen, die es über offene Ports im Internet bereitstellt. Für einen Wurm sieht das aus wie eine willkommene Gelegenheit, einen Computer zu kompromittieren und sich darauf fortzupflanzen. Um sich zu verbreiten, muss der Wurm sich selbst in das RAM oder auf die Festplatte des angegriffenen Rechners kopieren. Nepenthes mimt das arglose Opfer und lässt das ohne Widerstand geschehen. Ist der Programmcode des Wurms aber vollständig übertragen, schnappt die Falle zu: Der Wurmcode wird abgespeichert, der Angriff protokolliert – der Schadcode aber natürlich nicht ausgeführt.

Nepenthes ist Open-Source-Software und läuft unter Linux. Da die meisten Würmer Windows befallen und auf Linux nicht lauffähig sind, kann Nepenthes auf einer Linux-Maschine relativ sicher betrieben werden. Spannend ist allerdings die Frage, wo diese Maschine platziert werden soll. Ein sinnvoller Aufbau ist zum Beispiel folgender: Vor

Nepenthes-Voraussetzungen

Die Wurmfalle simuliert bekannte Schwachstellen. Versucht Malware, diese auszunutzen, wird das Schadprogramm heruntergeladen und auf der Festplatte gespeichert. Dort steht es für Analysen bereit. Folgende Voraussetzungen müssen erfüllt sein, um die Falle aufzubauen:

- Nepenthes (*nepenthes.mwcollect.org*)
- Internet-Zugang ohne Firewall
- Gnu-C++-Compiler, falls Sie Nepenthes selbst kompilieren möchten.
- Folgende Pakete müssen installiert sein: libadns, libadns-devel, file-devel, pcre, pcre-devel, curl, curl-devel



Überführt: Bitdefender identifiziert über 80 Prozent der heruntergeladenen Dateien als Schadprogramme

Mit Google Maps und dem Nepenthes-Modul Geolocation zeigt das CSRRT Luxemburg den Ursprung der Würmer an

der Firewall direkt am Internet-Zugang wird ein Switch angeschlossen, der einerseits zum Nepenthes-Rechner und andererseits zur Firewall verzweigt. An dieser Stelle kann Nepenthes alle Würmer fangen, die in der offenen Wildnis des Internets kursieren. Hinter der Firewall wird ein zweiter Nepenthes-Sensor installiert. Dieser dient zur Intrusion Detection. Auf dieser inneren Nepenthes-Instanz sollten überhaupt keine Würmer ankommen. Tun sie es doch, sollte sofort Alarm ausgelöst werden.

Wer so viel Aufwand nicht treiben möchte, kann stattdessen umstöpseln: Nach Feierabend wird die Firewall vom Netz getrennt und stattdessen der Nepenthes-Rechner angeschlossen. Damit kann zwar nicht der zeitliche Verlauf der Wurmaktivität über 24 Stunden erfasst werden, aber um Samples von Schadcode zu sammeln, reichen Nachtschichten allemal aus.

Aus Sicherheitsgründen ist es sinnvoll, einen eigenen Rechner oder zumindest eine dedizierte Installation auf einer eigenen Partition zu verwenden. Denn die Linux-eigene Firewall muss deaktiviert werden, damit Nepenthes funktioniert, der Rechner ist damit ungeschützt. Obwohl es reizvoll ist, zu diesem Zweck einen alten Rechner wiederzuverwenden, raten die Nepenthes-Entwickler davon ab: Heftige Wurmausbrüche könnten den Rechner in die Knie zwingen.

Schlechte Dokumentation

Wenn Sie Nepenthes installieren und damit arbeiten wollen, machen Sie sich auf eine miserable Dokumentation gefasst. So enthält die Online-Version der Readme-Datei mehrere Buttons mit der Aufschrift »Fix me« – reparier mich. Immerhin scheinen die Entwickler gemerkt zu haben, dass hier Verbesserungsbedarf besteht. Im Troubleshooting-Abschnitt wird als Problem genannt: »Es funktioniert nicht!« (Gliederungspunkt 7.1). Dass darauf als Lösung vorgeschlagen wird: »Finden Sie heraus, warum es nicht funktioniert«, werden viele Benutzer nicht als hilfreich empfinden. Netter ist da schon der Vorschlag, die Sicherheitswirkung von Nepenthes-Sensoren bei einem Bier zu besprechen, der sich in den FAQ findet (Punkt 8.9). Sie glauben nicht, dass diese Dinge in der Nepenthes-Dokumentation stehen? Überzeugen Sie sich selbst unter *http://nepenthes.mwcollect.org/ documentation:readme*

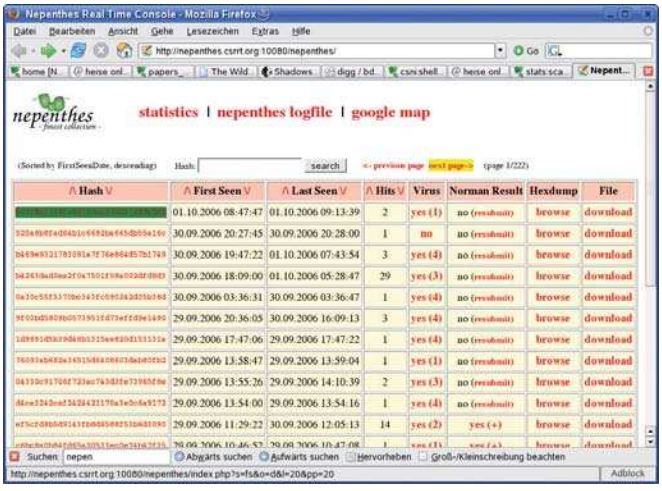
Installation

Trotz dieser Hindernisse ist es den Experten von Linux Professionell gelungen, Nepenthes zu installieren und damit Würmer zu fangen. Vorkompilierte Nepenthes-Pakete gibt es für Gentoo, Debian, FreeBSD und OpenBSD. Das Debian-Paket sollte auch unter Ubuntu laufen.

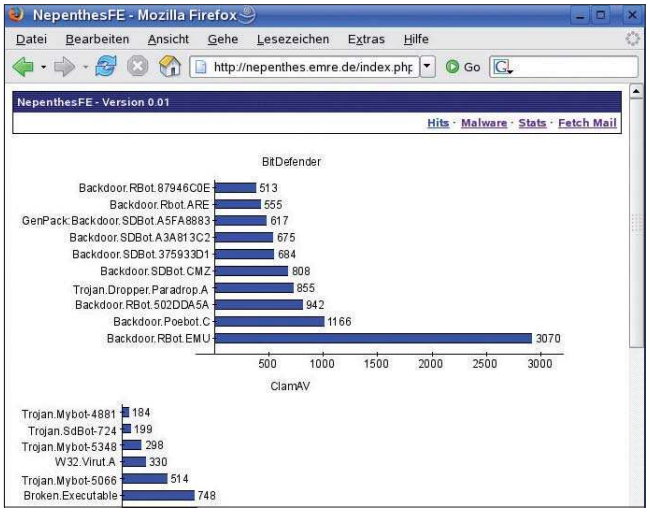
Den Quellcode können Sie aus dem SVN-Repository der Entwickler entnehmen. Dieser Quellcode enthält aber keine Dateien für die automatische Konfiguration. Einfacher ist es, ein fertiges Release zu verwenden. Zum Redaktionschluss war Version 0.17 aktuell. Taucht in einem Release ein kleinerer Fehler auf, erstellen die Entwickler kein neues Release, sondern einen Patch. Für die Version 0.1.7 wurden zum Testzeitpunkt zwei Patches angeboten. Einer davon behebt einen Fehler, durch den die Würmer Mydoom und Bagle den Nepenthes-Prozess in eine Endlosschleife schicken konnten. Wenn Sie diesen Patch ins Hauptverzeichnis des Nepenthes-Quellcode-Pakets geladen haben, wenden Sie ihn mit folgendem Befehl an:

```
cat mydoom_bagle_endless_
  loop.patch | patch -p0
```

Der andere Patch ist als *optional* gekennzeichnet. Das ist nicht ganz richtig. Unter Umständen müssen Sie den Patch nämlich unbedingt aufspielen. Es kommt dabei darauf an, ob man das Intrusion-Detection-Framework namens Prelude zusammen mit Nepenthes einsetzt. Der Patch sorgt für ein reibungsloses Zusammenspiel dieser beiden Komponenten. Setzt man Prelude nicht ein, führt der Patch zu Fehlern. Nepenthes kann



Einblick: Was der Nepenthes-Honeypot beim CSRRT Luxemburg an Würmern fängt, wird in Echtzeit publiziert



Kriminell: Der größte Teil des Fangs besteht aus Trojanern und Backdoors, die Angreifern Tür und Tor öffnen können

dann ein wichtiges Shellcode-Modul nicht laden. Das wiederum führt dazu, dass der Sensor zwar Hexdumps von Angriffen speichert. Die eigentlichen Honeypot-Funktionen, die die Malware herunterladen, funktionieren aber nicht, so dass die Wurmsammlung leer bleibt.

Sie haben den Quellcode entpackt, den Patch angewendet und die Pakete installiert, die Nepenthes benutzt? Dann können Sie das Programm installieren:

```
./configure --prefix=/opt/
  nepenthes
make
make install
```

Die Kompilierung kann mehrere Minuten dauern. Wenn die Installation fehlerfrei abgeschlossen ist, muss noch die Konfiguration angepasst werden. Zu dem Zweck haben die Entwickler im Ordner *etc/nepenthes* 43 Konfigurationsdateien hinterlegt. In der Dokumentation findet sich der Hinweis, dass Sie davon die folgenden drei mit einem Editor anpassen sollen: *nepenthes.conf*, *submit-norman.conf* und *log-irc.conf*. Diese ließen die Linux-Professionell-Tester aber unangetastet. Stattdessen fand sich in der Datei *download-nepenthes.conf* eine absolute Pfadangabe, die auf dem Testrechner nicht existierte und auf das Programmverzeichnis von Nepenthes */opt/nepenthes* gesetzt wurde. In der Datei *download-ftp.conf* wurde ein dynamischer DNS-Account beim Anbieter *dyndns.org* für den Testrechner eingetragen. Mit diesen Änderungen gelang der Würmerfang.

Jetzt können Sie Nepenthes starten und anfangen, Würmer zu angeln. Im Test an einem DSL-1000-Anschluss wurde der Nepenthes-Sensor durchschnittlich alle zwei Minuten angesprochen. Nicht bei jedem Angriff auf eine Schwachstelle wird aber ein Wurm heruntergeladen. Das geschah im Test im Durchschnitt nur viermal pro Stunde.

Shellcodes und Würmer

Wenn ein Hacker oder ein Wurm eine Schwachstelle angreift, so geschieht das meist über sogenannte Shellcodes. Ein Shellcode besteht aus einer Reihe von Bytes, die über eine Schwachstelle in einen Computer geschleust werden. Dort werden sie dank der Schwachstelle vom Prozessor ausgeführt. Meist wird dabei eine Shell gestartet, und in dieser werden weitere Befehle platziert. Damit sind Shellcodes wesentliche Bestandteile von Exploits. Nepenthes speichert die Shellcodes, die bei einem Angriff übermittelt werden, hexadezimal im Verzeichnis *var/hexdumps*. In der Logdatei verzeichnet das Programm parallel dazu, welche Lücke der Shellcode auszunutzen versuchte, wie lang der Dump ist und unter welchem Dateinamen er gespeichert wurde. Auf dieser Grundlage können Hexdumps analysiert und neue Exploits entdeckt werden.

Nicht jeder Exploit, der bei Nepenthes eintrifft, führt zum Download eines Schadprogramms. Im Test lag das Verhältnis bei einem Wurm auf neun Shellcodes. Die Würmer, die Nepenthes fängt, landen im Ordner *var/binaries*. ClamAV erkannte 41 Prozent der Dateien als Schadprogramme, Bitdefender identifizierte mit 83 Prozent mehr als das Doppelte. Von den hundert Prozent, die bei Wildlist-Tests üblicherweise herauskommen, ist das aber immer noch weit entfernt.

Weitere Funktionen

Über das Sammeln von Shellcodes und Würmern hinaus bietet Nepenthes dem Anwender viele weitere Funktionen. Das Programm ist modular aufgebaut und kann beliebig erweitert werden. Außerdem kann das Programm sich in IRC-Kanäle einklinken, über die Botnetze meist gesteuert werden, und die Kommunikation protokollieren. Weitere Funktionen dienen dazu, Malware-Samples auszutauschen und die Angriffe statistisch detailliert auszuwerten. ■

Weitere Informationen

Auf Webseiten rund um Nepenthes finden sich unter anderem Hintergrundinformationen zu Shellcodes sowie Statistiken und Analysen zum gesammelten Schadcode.

Das Luxemburger Computer Security Research and Response Team stellt die Echtzeit-Daten eines Nepenthes-Honeypots unter *http://nepenthes.csrrt.org:10080/nepenthes/* zur Verfügung. Hier ist auch auf einer Google-Landkarte zu sehen, woher die Angriffe kommen. Der Kölner Emre Bastuz hat ein Web-Frontend für Nepenthes entwickelt, das die Logdateien auswertet. Er hat damit seinen Nepenthes-Sensor drei Monate lang laufen lassen und stellt die Ergebnisse inklusive statistischer Auswertung und Schadcode-Analyse unter *http://nepenthes.emre.de/* bereit.

Was es mit einem Shellcode auf sich hat und wie Sie selbst einen solchen schreiben, hat ein Hacker mit dem Pseudonym bitmuncher notiert und veröffentlicht: *www.hackerwiki.org/index.php/Erstellen_eines_Shellcode.*