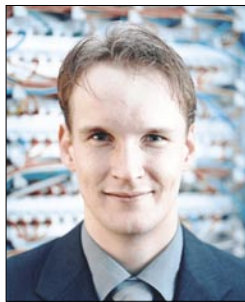




Interview

Interview mit Dirk Kollberg



Dirk Kollberg

Dirk Kollberg arbeitet als Research Lead im McAfee Avert und bearbeitet verdächtige Dateien die von Kunden eingesendet werden oder aus anderen Quellen stammen. Entsprechend werden die Signaturen für die McAfee Produkte aktualisiert. Des Weiteren ist er an der Qualitätssicherung der Signaturen und der technischen Teamleitung in der europäischen Zeitzone beteiligt.

hakin9: Herr Kollberg, wo sehen Sie derzeit die größten Probleme, warum sich Würmer nach wie vor im Internet ausbreiten können?

Dirk Kollberg: In den letzten Jahren haben wir eine deutliche Verschiebung bei den Gefahren aus dem Netz gesehen. *Script Kiddies* schrieben früher einfache Schädlinge, um ideologische Gedanken zu verbreiten. Vor einigen Jahren noch waren E-Mail Würmer das Hauptproblem und es fand ein Wettstreit zwischen verschiedenen Autoren statt. Netsky und Bagle sind zum Beispiel zwei Würmer, bei denen die Autoren sogar versuchten, den jeweils anderen Schädling von einem infizierten System zu entfernen, so dass sich der *eigene* optimal verbreiten konnte. Doch die Zeiten und die Motive haben sich geändert - finanzielle Interessen stehen jetzt im Vordergrund. Es gibt kriminelle Gruppen, die selber die Schädlinge programmieren, mit denen sie anschließend versuchen ihre Opfer auszunutzen - aber auch die ergaunerten Daten werden über das Internet zum Verkauf angeboten. Man findet leicht im Netz Angebote für gültige Kreditkarten Informationen für unter 10 €. Eine Liste von 30.000 aktuellen Email Adressen kostet ca.

5€. Ältere Adresslisten werden teilweise auch *verschenkt*. Zugangsdaten zu *Paypal* Konten werden auf dem Schwarzmarkt im Bereich von 30-300 € gehandelt. Aber auch Zugangsinformationen zu *Skype* oder Onlinespielen wie *World of Warcraft* werden angeboten.

Auch Erpressung ist eine mögliche Einnahmequelle. So können kompromittierte Rechner genutzt - bzw. *gemietet* werden - um große Datenmengen an eine Firma zu senden, um diese durch die Datenflut lahmzulegen. Sind diese Firmen über das Internet nicht mehr erreichbar, entsteht für diese ein großer Schaden. Zahlt das Opfer eines solchen *Deny of Service* Angriffs, ziehen die Angreifer zum nächsten.

Andere Gruppen entwickeln nur die Schadsoftware und verkaufen diese über das Internet. Selbst eine *Garantie* auf die Software wird teilweise geboten... Wird der Schädling durch AV Software erkannt, erhält der Käufer innerhalb eines gewissen Zeitrahmens kostenlos eine neue Version. Eine Schadsoftware kommerziell zu verbreiten, ist in vielen Ländern nicht strafbar.

Die einen produzieren die Waffen, die anderen nutzen sie, um die Bank auszurauben.

Seit knapp einem Jahr macht der Storm Wurm die Runde - auch bekannt als *W32/Nuwar@MM* oder *W32/Zhelatin@MM*. Hierbei handelt es sich um einen Schädling, der nicht von einem Server aus gesteuert wird, sondern der selber ein Peer-to-Peer Netzwerk aufbaut. Über dieses Netzwerk kann sich der Schädling selber aktualisieren, erhält aber auch seine Befehle. So kann er *Deny of Service* Angriffe ausführen - unter denen auch schon einige Anbieter von Sicherheitssoftware leiden mussten - aber auch Spam versenden oder weitere Dateien auf dem Rechner des Opfers installieren.

Um der Erkennung von Anti-Virus Software zu entgehen, werden die Schädlinge im Minutentakt neu generiert. Die Funktionalität bleibt hierbei gleich, jedoch werden polymorphe Packer genutzt, die den Code des Schädlings verschleiern. Zusätzlich werden mehrfach pro Tag diese Packer gewechselt, so dass die Dateien jeweils andere Strukturen aufweisen.

Dies ist eine große Herausforderung für die Hersteller von Sicherheitssoftware, der man nicht nur mit traditionelle AV Signaturen begegnet. Weitere Funktionen wie eine *Buffer Overflow Protection* verhindern das Ausnutzen von Exploits, *Access Protection* die schädliche Zugriffe auf Systembereiche schützt und auch verhaltensbasierte Analysemethoden werden in die Sicherheitsprodukte mit aufgenommen, um diese Gefahren abzuwehren.

Doch auch der gesunde Menschenverstand sollte geschult werden und die Neugier sollte bei den Nutzern nicht im Vordergrund stehen. Ohne Sicherheitsupdates für das Betriebssystem, sowie die installierten Programme, und ohne aktuelle AntiVirus Software/Firewall sollte sich kein Nutzer mit dem Internet verbinden.

Wird ihr Rechner kompromittiert, übernimmt der Angreifer die Kontrolle, und Sie werden zum Gast.

h9: In Hakin9 (06/2007) haben wir bereits über mobile Schädlinge berichtet. Wie sehen Sie die realistischen Bedrohungen dieser Art von Schädlingen?

DK: Derzeit befinden wir uns noch in der Phase, in der die Autoren versuchen zu zeigen, was möglich ist. Verglichen mit den Schädlingen auf Computern, sind wir hier noch im *Hobby* Bereich. Zwar gibt es einige Schädlinge, die einem Opfer viel Geld kosten, wie zum Beispiel der Comwarrior. Da dieser sich per MMS an alle Einträge im Adressbuch versendet, kommen hier schnell hohe Kosten auf das Opfer zu.

Jedoch stellt sich bei den mobilen Geräten eine völlig andere Situation da - es gibt eine große Vielfalt an Betriebssystemen für die Geräte und unterschiedliche Versionen dieser, so dass es nicht möglich ist, einen Schädling zu entwickeln, der auf allen Geräten funktioniert.

Mit derzeitigen Schädlingen oder Tools die Schwachstellen ausnutzen, kann man noch nicht das

große Geld verdienen. Sicherlich kann ein Angreifer bei einem Opfer sensitive Daten wie SMS, Kalender oder das Adressbuch auslesen und diese ggf. zu Geld machen. Jedoch erfordert dies einen hohen manuellen Aufwand für jedes einzelne Opfer, daher ist dies noch kein lohnender Anreiz für die Autoren, die damit Geld verdienen wollen.

h9: Was meinen Sie in Hinblick auf die Zukunft, was uns an Schädlingen erwarten wird?

DK: Sobald diese mobilen Geräte kompatibler mit einander werden, und die Geräte auch für finanzielle Transaktionen genutzt werden, wird das Thema interessant für kriminelle Autoren.

In Japan können schon seit Jahren Telefone genutzt werden, um an der Kasse im Supermarkt die Rechnung vom Konto abbuchen zu lassen. Homebanking ist auch ein Service, der in Europa derzeit über den PC und das Internet abgewickelt wird. Der Markt der Schädlinge ist dynamisch und wird sich möglichen *Einnahme-Quellen* schnell anpassen.

h9: In der letzten Zeit hat man den Eindruck, dass Schädlinge vermehrt eingesetzt werden um gezielt Internetuser auszuspionieren. Können Sie das in der Form bestätigen?

DK: Dieser Trend hat sich fortgesetzt. Nehmen wir das Beispiel Spam: Wir würden nicht das ständig steigende Volumen von Emails die für blaue Pillen sehen, wenn es sich nicht lohnen würde. Der Verkauf von - bei uns verschreibungspflichtigen - Medikamenten ist in vielen Ländern nicht verboten. Daher gibt es viele Anbieter von Medikamenten im Internet, die auch in das Ausland liefern. Durchaus ist diesen Firmen bekannt, dass ihr Service nicht in allen Ländern legal ist.

In einem Fall hatte ich über Google Zugangsinformationen zu einem SQL Server im Internet gefunden, der von einem neuen Schädling genutzt wurde. Als ich mich auf den SQL-Server verbunden hatte, sah ich eine Datenbank von einem Händler für Medikamente. Enthalten war die Kundendatenbank mit kompletten Datensätzen die Name, Vorname, Adresse, Telefon, Email und alle Kreditkarten Informationen enthält.

Ebenfalls waren die *Partner* zu sehen, also die Personen, die der Firma die Kunden vermitteln. Hierfür erhalten diese eine Prämie, die bei manchen bei über 5.000€ pro Woche lag. Von diesen *Partnern* waren natürlich keine Namen oder Adressen hinterlegt, jedoch Nicknames und ICQ Nummern. Weitere Untersuchungen haben schnell gezeigt, dass es sich hierbei um Spammer handelt.

Interessant war ein Teil der Datenbank, in dem die Fragen und Antworten von den Endkunden gespeichert wurden. So war ein Nutzer aus Europa sehr verwundert, dass er eine Lieferung aus Asien erhalten hat, obwohl er doch in Amerika bestellt hatte. Zudem waren die Pillen nicht in einer Original-Verpackung, sondern in einem Buch, in das ein Loch geschnitten



war. Die Pillen sahen auch nicht so aus wie das Medikament, das er gewohnt war. Grund sich Sorgen zu machen?

Die Antwort war, dass der Kunde sich keine Sorgen machen sollte, und dass die *generischen Medikamente* zwar anders aussehen, jedoch die selben Wirkstoffe enthalten.

Wenn man Glück hat erhält man Traubenzucker.

Spam ist nur eine Möglichkeit Geld zu verdienen. Nach fast dem gleichen Prinzip funktioniert der Bereich Adware. Auch hier kann jemand Geld verdienen, wenn er Adware auf Rechnern installiert. Wird so die Werbung dem Nutzer angezeigt, erhält der Vermittler eine Provision. Auch hierbei gibt es legale Anwendungsgebiete, bei denen der Nutzer eine Software zum Beispiel kostenlos nutzen kann, wenn er hierfür die Werbung in Kauf nimmt.

Wird jedoch über ein Bot-Netz eine Million Rechnern diese Adware untergeschoben, ist dies sicherlich nicht im Sinne des Erfinders, aber sehr lukrativ für den Bot-Netz Betreiber.

Phishing Angriffe sind ein Wettlauf mit den Banken. Die Banken versuchen einfache Lösungen für ihre Kunden finden, jedoch können sie dem Rechner des Kunden nicht trauen. Befindet sich der Rechner unter der Kontrolle eines Hackers, können Informationen abgefangen und misbraucht werden. Je nutzerfreundlicher die Dienstleistung wird, desto einfacher ist es auch für Angreifer hier Missbrauch zu betreiben. Sichere Wege zum Homebanking existieren, aber es kostet die Banken deutlich mehr, diese mit dem Kunden zu betreiben.

Nutzer, die Homebanking mittels einer einfachen TAN Liste machen, sollten mit Ihrem Institut sprechen und auf eine sichere Methode umsteigen.

h9: Welche Bedrohungen stellen denn konkret Rootkits dar, von denen ja immer öfter berichtet wird?

DK: Rootkits sind Programme oder *Treiber*, die sich tief im Betriebssystem verankern. Sie können somit das, was der Nutzer auf der Oberfläche sieht, beeinflussen. So verstecken Rootkits schädliche Prozesse im Taskmanager und auch im Explorer - auch in der DOS Konsole sind die Dateinamen nicht sichtbar. Es ist auch möglich, dass Rootkits Treiber installieren, die den Netzwerkverkehr überwachen und einzelne Pakete verändern.

Spam-MeSpam zum Beispiel überprüft Aufrufe der WSOCK32.DLL, die von Programmen genutzt werden, die Daten über das Netzwerk versenden. Handelt es sich hierbei um eine Email, also eine SMTP Verbindung, fügt der Schädling weitere Zeilen in die Email ein. Es ist dabei nicht relevant welcher Email-Client genutzt wird, da alle Email Programme ihre Daten über die WSOCK32.DLL versenden. Der MeSpam Trojaner erhält über eine Command & Control (C&C) Webseite seine Befehle und kann so bestimmte Nach-

richten an eine Mail anhängen - z.B. einen Link zu einer schädlichen Datei.

Der Empfänger, der den Sender vermutlich kennt und auch traut, wird dann selbst infiziert, wenn er die Datei ausführt. Zusätzlich ist der MeSpam auch in der Lage, Zusätze in ICQ, Yahoo, AOL, Webmail Verbindungen einzufügen.

Mit den Mitteln, die Windows bereitstellt, sind diese Schädlinge für Nutzer manuell nicht zu finden und nicht zu entfernen.

In den AV-Produkten finden daher immer stärker Funktionen zur Erkennung solcher Rootkits einzug, da sich ein Rootkit auch vor traditionellen AV-Scannern verstecken kann. Das McAfee Avert stellt für Nutzer, die ihren Rechner überprüfen wollen hierzu eine kostenlose Version des Rootkit Detective zur Verfügung. Im Unterschied zu einem AV Scanner, sucht der Rootkit Detective nach den Ansatzpunkten, an denen Rootkits sich einklinken könnten. Kürzlich wurde die Version 1.1 veröffentlicht, die neue Funktionen zur Erkennung enthält:

<http://download.nai.com/products/mcafee-avert/McafeeRootkitDetective.zip>

h9: Sehen Sie eine Gefahr durch immer mehr zunehmende Technik in mobilen Geräten, wie beispielsweise die Ausbreitung von Schädlingen über Bluetooth?

DK: Über Bluetooth werden wir wohl auch in Zukunft keine Epidemien haben. Auf Grund der geringen Reichweite wäre eine Verbreitung sehr schleppend, verglichen mit dem Internet. Wenn sich jemand aber auf den Hauptbahnhof stellt und versucht über ein Laptop alle möglichen Geräte auszulesen, kann er schnell an fremde Daten gelangen. Derzeit ist es noch nicht üblich zwischen Bekannten, Programme für das Telefon als MMS zu versenden, zumeist werden Bilder der Klingeltöne getauscht, die keinen ausführbaren Code enthalten.

Wir sind jetzt noch am Anfang - das Telefon wird auch bei uns an Bedeutung zunehmen und wird stärker in das tägliche Leben einfließen. Walkman, MP3-Player, Kamera, GPS Navi-System, Fernbedienung, Onlinebanking, Internet, Kreditkarte - alles in einem ist möglich. Kommt jedoch ein Angreifer über eine Schwachstelle rein, hat er Zugriff auf alle Daten.

Mit Dirk Kollberg sprach
Marko Rogge