

## Der Stand der Internet-Sicherheit

Dr. Kurt Brand, Pallas GmbH

Erschienen in: eco Jahrbuch 2008 "Beyond the Borders", eco - Verband der deutschen Internetwirtschaft e.V.

Nie war es so schlimm wie heute. Wenn man denkt, der Kampf verlagert sich gerade von Email zu Web, wird man mit einer richtig bösen Emailwelle eines anderen belehrt. Zehn Millionen Computer-Zombies sind täglich (und nächtlich) arg lebendig und sorgen für Nachwuchs im sechsstelligen Bereich. Jeden Tag wechseln sie ihre IP-Identität, um einen neuen Hinterhalt zu legen. Sie sprechen gutes Deutsch mit dem User und fallen mit perfiden Tricks über ihn her. Das ist kein Spiel mehr, es geht um sehr viel Geld. Blitzschnell muss die Abwehr erfolgen, in Real-Time und weltweit. Weil alles so still abläuft, wurde unser Bewusstsein lange nicht gepatcht und weist Sicherheitslücken auf. Da kommt es gut, dass nun auch tiefenpsychologische Methoden bei der Abwehr helfen.

Email ist vom Lebensalter her seit Jahren volljährig, Viren und Spam haben immerhin auch schon die Zeit der Pubertät hinter sich. Ist damit auch die Internet-Sicherheit aus dem Gröbsten heraus? Mitnichten, wir hängen mitten im Groben fest. Denn auch die Skriptkiddies wurden erwachsen und trachten nicht mehr nach Ehre, wenn sie einen Rechner hacken, sondern nach schnödem Profit. Je nach persönlicher Disposition sind sie heute zurück in der Rechtsgesellschaft und machen ihr Geld als Pentester, oder sie stecken im Cybercrime von Betrug, Erpressung, Diebstahl "over" IP.

Ein großer Teil der Cyberkriminellen kümmert sich seit dem vergangenen Jahr

verstärkt um Ausbau und Nutzung von Botnetzen, die aus infizierten Computer-Zombies bestehen. Botnetze bieten heute die wohl größte illegale Einnahmequelle im Internet. Das ist der Grund, warum der Spam bis Mitte 2008 deutlich gestiegen ist. Zwar hat das Abschalten eines Providers in Kalifornien im November zu einer signifikanten Entlastung geführt, gleich darauf wuchs die Spammenge aber schon wieder an (siehe Abb. 1).

### Die Botnetze sind schuld

Botnetze sind für 85 % des Spam, fast 100 % aller Malware (Viren, Trojaner, Würmer usw.), sowie die meisten sonstigen Internet-Angriffe (z.B. Phishing und Denial-

of-Service-Attacken) verantwortlich. Botnetze sorgen dafür, dass seit Monaten etwa 80 % des internationalen Emailaufkommens Spam ist. Unternehmen mit langer und bekannter Internet-Historie sind meist noch weitaus schlechter dran, viele bringen es auf weniger als 5 % Nutzlast auf dem Email-Kanal, der Rest ist rauschender Spam.

Da lohnt es sich, auch auf geringfügige Unterschiede bei der sicheren Spamerkennung zu achten (sicher heißt hier: ohne Falscherkennung). Eine Erhöhung der Erkennungsquote um 1 % klingt erst mal nicht sehr beachtlich, bedeutet aber bei 1.000 Spams, die über die Hauptbetroffenen pro Tag hereinbrechen, 10 weniger, über die man sich ärgern muss.

### Real-Time-Schutz tut not

Die Botnetze haben dafür gesorgt, dass der Real-Time-Schutz zur wichtigsten Aufgabe bei der Malware-Abwehr geworden ist. Die Zeiten, in denen wir in der Tagesschau vor einem Virusausbruch in Asien gewarnt wurden und uns am nächsten Tag immer noch ausreichend schützen konnten, sind lange vorbei. Neu freigesetzte Malware

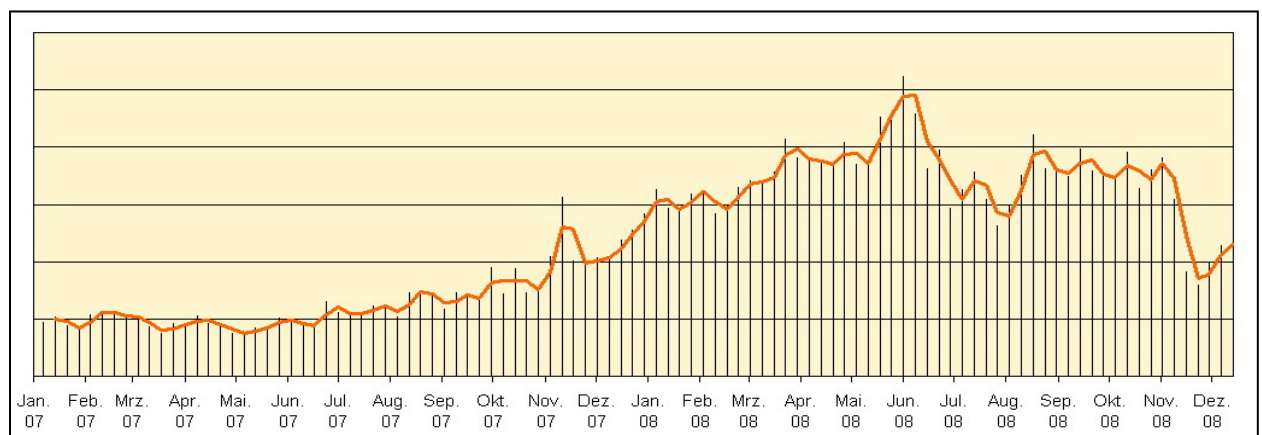


Abb. 1: Spam 2007/2008 in Pallas-HoneyPot mit Trendlinie

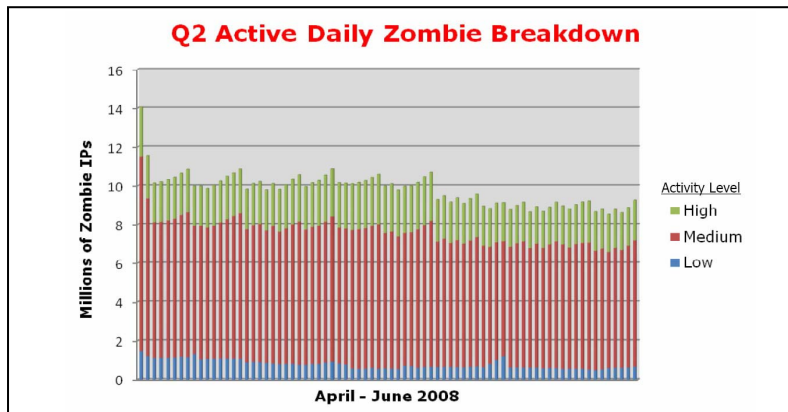


Abb.2: Anzahl aktiver Zombies in Q2/2008 nach Commtouch (www.commtouch.com)

erreicht heute Unternehmen mit hohem Mailvolumen innerhalb von Minuten. Tagtäglich werden etwa 10 Millionen Zombies beobachtet - davon jeweils einige hunderttausend neue (siehe Abb. 2). Sie senden meist nur wenige Stunden, dann wird der Angriff schon wieder variiert. Damit unterlaufen sie die klassische Abwehr, die bedingt durch die Herstellung und Verteilung von Erkennungsmustern nach

gerade noch einmal eine Renaissance der Email-Viren, es ist aber doch anzunehmen, dass sich der generelle Trend hin zur Ansteckung über Blended Threats (kombinierte Angriffsmethoden) fortsetzen wird, z.B. indem man per Email auf befallene Webseiten gelockt wird. Es ist außerdem zu erwarten, dass die Botnetz-Angriffe auch vor Smartphones nicht haltmachen werden. Der nächste Januar wird wie schon in den

(Manipulationen, die auf sozialer Interaktion aufsetzen) jemanden hereinzulegen, werden immer ausgefeilter, und (richtiges) Deutsch sprechen die Angreifer inzwischen auch.

### Der Mensch macht's

Ein gerade erlebter Angriff tarnte sich mit dem Namen eines bekannten Inkasso-Unternehmens und behauptete, einen größeren Betrag beim Empfänger der Email abgebucht zu haben. Wer jetzt entrüstet auf den Dateianhang klickt und technisch nicht hochversiert ist, glaubt an das angebliche Sicherheitszertifikat, bekommt aber perferweise einen Schädling installiert.

Folgerichtig muss die Psychologie auch auf der Seite der Guten, der für die IT-Sicherheit Verantwortlichen, helfen (siehe Abb. 3). Thema des Arbeitskreises Sicherheit beim eco Verband der deutschen Internetwirtschaft e.V. war deshalb in diesem Jahr eine tiefenpsychologische Security-Studie von known\_sense zu Selbstbild und Wirkungsanalyse des CISO (Chief Information Security Officer). Drei CISO-Basistypen hat die Studie herausgearbeitet: den zentralen Kontrolleur, den unauffälligen Helfer und den beweglichen Streetworker. CISOs sollten eine Marke in ihrem Unternehmen bilden, um Sicherheit lebendig zu halten und ein hohes Involvement zu erreichen.

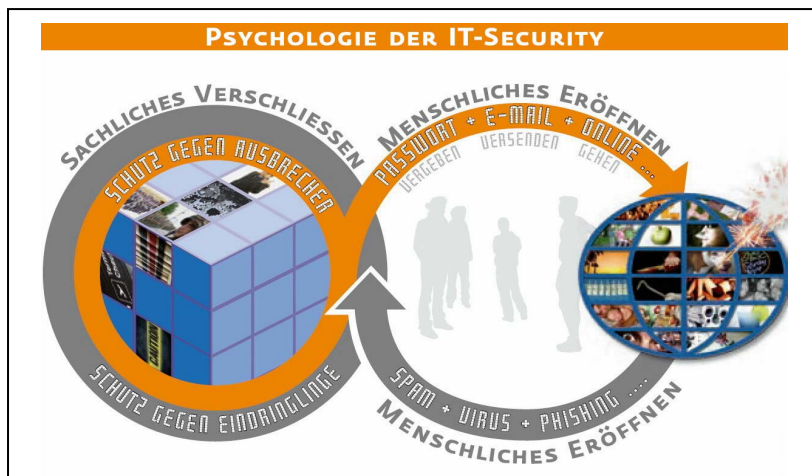


Abb.3: Psychologie der IT-Security nach known\_sense (www.known-sense.de)

einem Neuausbruch Stunden braucht, um Schutz liefern zu können. Real-Time-Schutz setzt bei der Analyse von Internet-Traffic an und erzielt über IP-Reputation, Spam- und Virenerkennung sehr gute Ergebnisse innerhalb von ein oder zwei Minuten nach einem Neuausbruch. Traffic lässt sich außerdem mit wesentlich weniger Rechenaufwand analysieren als Content, Traffic-basierte Verfahren sparen deshalb erhebliche Ressourcen ein.

Real-Time-Schutz wird verstärkt auch für Webtraffic benötigt. Zwar erlebten wir

letzten Jahren spannend, wenn die Botnetz-Betreiber den "Schaden" durch das Weihnachtsgeschäft wettmachen und die frischen PCs möglichst schnell zu Zombies machen wollen.

Letztlich entscheiden aber nicht die Kisten über die Sicherheit, sondern die Nasen. Alle Technik nützt nicht viel, wenn die Menschen, die damit umgehen, nicht aufpassen und mitdenken. Denn sie bleiben die größte Schwachstelle durch Sorglosigkeit, Naivität und manchmal auch Gier. Die Versuche, per "Social Engineering"

Pallas Managed Security Service: Vom Mailschutz bis hin zur umfassenden mehrstufigen Sicherheitslösung, TÜV-zertifiziert und mehrfach ausgezeichnet. Sicherheitsberatung und Betrieb abgesicherter Internet-Server.

**Dr. Kurt Brand**  
Geschäftsführer Pallas GmbH

#### Weitere Informationen

Dr. Kurt Brand  
Pallas GmbH  
Hermülheimer Straße 10  
50321 Brühl  
Tel: 02232-1896-0  
Fax: 02232-1896-29  
kurt.brand (at) pallas.de  
www.pallas.de