

Was ist nur mit den Zombies los?

Spam auf Rekordtief, aber Zombies vermehren sich wieder - jedoch nicht in Deutschland

Ein Report der Pallas GmbH, Brühl

Autor: Dr. Kurt Brand, Geschäftsführer der Pallas GmbH

August 2011

1. Einleitung

Im ersten Halbjahr 2011 waren einige sehr ungewöhnliche Trends in der Internet-Sicherheit zu beobachten:

- Die weltweite Zahl der Computer-Zombies brach in Q4 2010 signifikant ein, steigt aber seitdem wieder kontinuierlich.
 - Dennoch verharrt der Spam in 2011 nachhaltig auf dem niedrigsten Niveau seit Jahren.
 - Die Zombies in Deutschland allerdings verschwinden ganz gegen den Trend.
- Der vorliegende Report beschreibt diese Trends und versucht Erklärungen zu liefern.

2. Die drei Spamphasen der letzten 5 Jahre und warum der Spam jetzt nur noch tröpfelt

Verseuchte, illegal in Botnetzen ferngesteuerte Rechner, üblicherweise (Computer-) Zombies genannt, sind seit Jahren verantwortlich für den größten Teil der Massenbedrohungen im Internet. Etwa 85 % des Spam werden aus Botnetzen versandt und fast alle Viren und andere Malware, die per Email hereinkommen. Der bei Pallas gemessene Postfachspam, das ist der Teil des Spam, der korrekt adressiert und direkt auslieferbar ist, ist ab 2007 bis Mitte 2008 zunächst kontinuierlich und deutlich gewachsen, das ist die Phase 1. In den Jahren 2009 und 2010 stieg der Spam dann im Durchschnitt nicht weiter, sondern sank sogar etwas. In dieser Phase 2 waren zunächst Quartalswellen zu beobachten, schließlich hohe und kurzfristige Volumenschwankungen. Die Phase 3 liegt in 2011: Der Spam ist drastisch gefallen und macht nur noch ein Viertel des Spam-Mittelwertes von 2007 aus.

Diese deutliche Absenkung ist zunächst auf viele erfolgreiche Maßnahmen gegen Botnetze und ihre Betreiber zurückzuführen, das veranschaulicht die Abbildung 1.

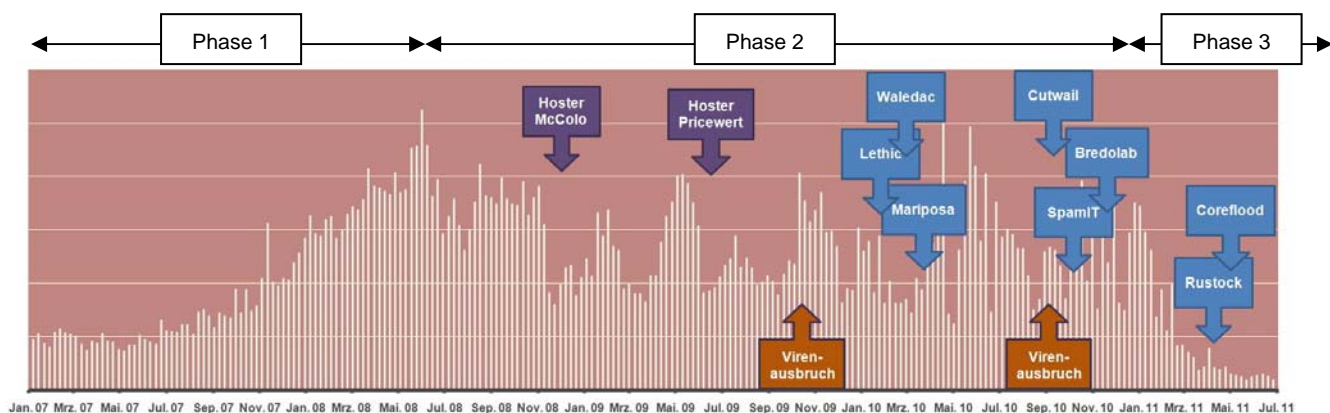


Abb. 1: Postfach-Spam in Pallas Spamsammler seit 2007; Quelle: Pallas

Zunächst wirkten Maßnahmen gegen verschiedene Rechenzentren der Spamversender (McColo, Pricewert), die Spamflut kam in 2009 aber regelmäßig immer wieder zurück. Dann gab es viele er-

folgreiche Maßnahmen gegen einzelne Botnetze, in Abbildung 1 blau gekennzeichnet. Die Ausschaltung vieler Botnetze ist der Grund für die erstaunliche Spam-Abnahme. Da die Zombies sich weltweit jedoch schon wieder stark vermehrt haben (siehe unten), stellt sich die Frage, warum die Spam-Aussendungen nicht wie in der Vergangenheit wieder stark zugenommen haben. Hierfür bieten sich zwei Erklärungsmuster an:

1. Die Zombies sind zwar zurück, aber das kriminelle Geschäftsmodell funktioniert (noch) nicht wie in der Vergangenheit. Entweder sind die Zombies noch kopflos, oder aber die kriminellen Geschäftsbeziehungen wurden empfindlich gestört.
2. Die modernen traffic-basierten Zombie-Erkennungsverfahren, zum Beispiel die bei Pallas eingesetzten IP-Reputations-Mechanismen von Commtouch, sind so genau und schnell geworden, dass Zombies ihren Spam immer schlechter ausgeliefert bekommen. Die Zombies werden deshalb vermehrt genutzt, um über echte Email-Accounts Spam mit besserer Reputation abzusetzen. Von dort kann aber viel weniger Spam versandt werden. Siehe dazu auch den Bericht von Commtouch Software Ltd. (Netanya, Israel) "Internet Threats Trend Report" von Juli 2011, siehe http://www.pallas.com/pub/Commtouch_Trend_Report_2011-July__Pallas.pdf.

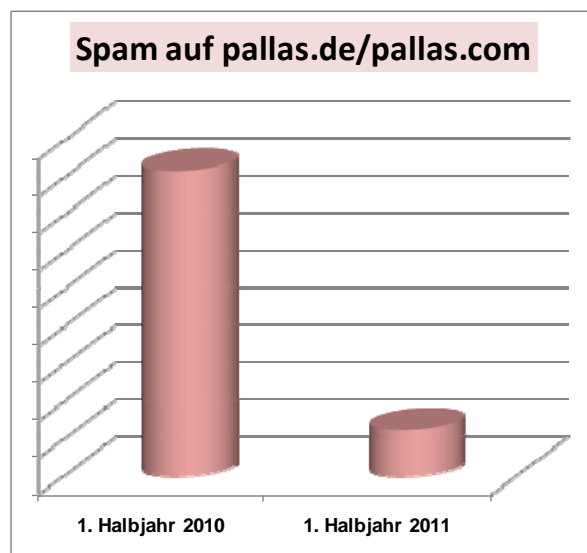


Abb.2: Gesamtspam bei Pallas; Quelle: Pallas

Auch der Gesamtspam auf Pallas-Domains - das ist etwa die zwanzigfache Menge des Postfach-Spam, sie umfasst neben korrekt adressierten Emails auch viel Müll an nicht vorhandene Empfänger - ist im ersten Halbjahr 2011 im Vergleich zum gleichen Zeitraum des Vorjahres sehr deutlich auf nur noch 15 % gesunken, siehe die Abbildung 2. Allerdings bedeutet das nicht, dass wir nun bald vom Spam gänzlich befreit sind: Auch beim derzeitigen Niedrigstand sind mindestens 3/4 des Email-Aufkommens immer noch Spam.

3. Wie die Zombies sich weltweit wieder vermehren - nur nicht in Deutschland

Commtouch identifiziert und zählt die weltweiten, aktiven Zombies durch Klassifikation der sendenden IP-Adressen nach ihren Aktivitäts- und Trafficmustern. In Q4 2010 wurde dabei eine gravierende Verringerung der Zombies weltweit um fast 50 % gegenüber dem Vorquartal festgestellt. Das ist den oben geschilderten Anti-Botnetz-Maßnahmen geschuldet (siehe Abbildung 1). In

Deutschland verschwanden sogar mehr als 60 % der Zombies und - eine zusätzliche erstaunlich positive Entwicklung - sie kamen in Q1 und Q2 2011 auch nicht mehr zurück. Erstaunlich, weil die Botnetz-Betreiber weltweit inzwischen schon wieder für deutliche Vermehrung gesorgt haben. Diese große Schere zwischen den deutschen Zombies (blau) und den Zombies weltweit (grau) veranschaulicht die Abbildung 3. Dabei wurde die Anzahl der weltweiten Zombies zur besseren Veranschaulichung auf den Stand der deutschen Zombies in Q3 2010 herunterskaliert. Nur noch 27 % der deutschen Zombies aus Q3 2010 sind aktiv, weltweit aber schon wieder 87 %.

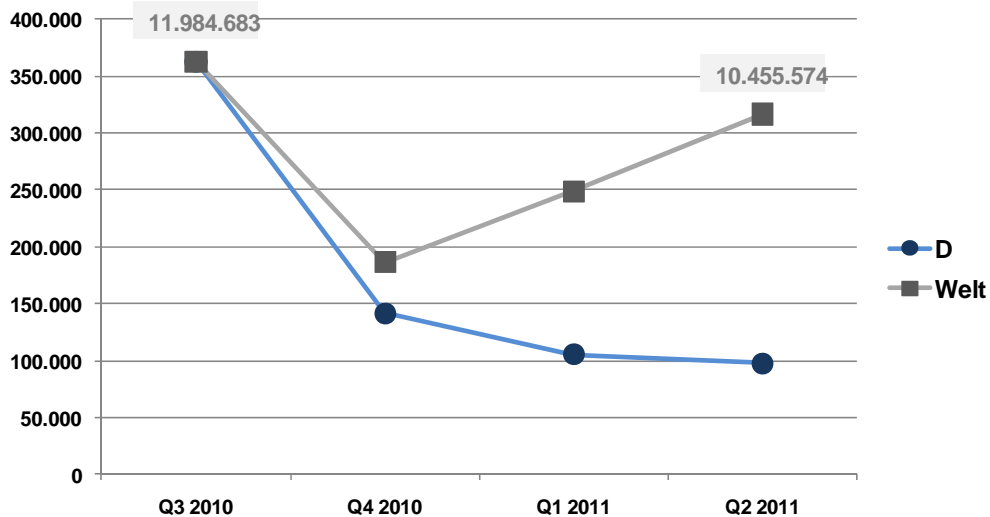


Abb. 3: Weltweit wieder Wachstum bei den Zombies - Deutschland (D) aber sinkt gegen den Trend; Quelle: Commtouch, Grafik: Pallas

Auch hier drängt sich die Frage nach dem Warum auf. Dass Zombies nach Verlusten wieder zurückkommen, ist ein genereller, schon vielfach beobachteter Trend. Saisonale Ausschläge - z.B. ein Abflauen um das Jahresende durch die im Weihnachtsgeschäft mitsamt ihren Zombies verschwindenden Altrechner - und nachfolgende Reaktivierungen sind üblich. Commtouch hat auch Ende März 2011 wieder ein eindrucksvolles Beispiel für einen solchen Zombie-Rückgewinnungsprozess beobachtet. Kurzzeitig wurden massiv virenverseuchte Emails verschickt, siehe die Abbildung 4.

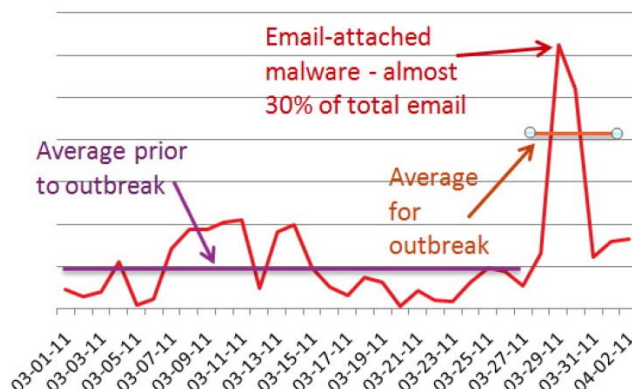


Abb.4: Massiver Ausbruch von Virenmails Ende März 2011; Quelle: Commtouch

Fünf Tage nach diesem Ausbruch stiegen dann tatsächlich die beobachteten neu aktivierten Zombies signifikant an, siehe Abbildung 5. Für das zweite Quartal 2011 insgesamt wurden weltweit

durchschnittlich 377.000 neu aktivierte Zombies gezählt, das ist der Spitzenwert der letzten drei Jahre.



Abb. 5: Neu aktivierte Zombies Anfang 2011, Peak kurz nach Virenausbruch Ende März;
Quelle: Commtouch

Das dadurch ausgelöste weltweite Wachstum machten aber die deutschen Zombies nicht mit, die PCs widerstanden offensichtlich auch dem heftigen Virenausbruch. Es liegt nahe, hier einen originär deutschen Grund zu suchen, wofür sich die Initiative www.bottfrei.de anbietet. Unter dieser Adresse agiert das Anti-Botnet-Beratungszentrum, getragen vom eco - Verband der deutschen Internetwirtschaft e.V. mit Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Das Angebot dieser Initiative wurde seit Q4 2010 hunderttausendfach erfolgreich genutzt. Zu vermuten ist, dass nicht nur sehr viele PCs gereinigt werden konnten, sondern auch ein neues, erhöhtes Sicherheitsbewusstsein mit verbesserten Sicherheitsstandards erreicht wurde.

Im Ergebnis ist Deutschland als einstiger (Q1 2008) unrühmlicher Zombie-Weltmeister, der auch in Q2 2010 noch an vierter Stelle rangierte, ein Jahr später auf Rang 26 der Zombie-Nationen zurückgefallen. Damit liegen die deutschen Zombies nun erfreulicherweise weit hinter Italien (Rang 14) und Großbritannien (Rang 18), die im vergangenen Jahr noch deutlich negativ übertroffen wurden.

Über die Pallas GmbH

Pallas ist Dienstleister für Managed Security Service und Secure Hosting: Schutz gegen alle Bedrohungen aus dem Internet, Beratung zur IT-Sicherheit und performanten Betrieb von Internet-Servern, TÜV-zertifiziert und auf Datenschutzkonformität geprüft. Unsere Kunden sind namhafte Unternehmen aus allen Branchen, für Referenzen siehe www.pallas.com/referenzen.html.

Weitere Informationen:

Pallas GmbH

Dr. Kurt Brand

Hermülheimer Str. 8a

50321 Brühl

Tel.: 02232-1896-0

Fax: 02232-1896-29

Email: [kurt.brand \(at\) pallas.de](mailto:kurt.brand@pallas.de)