mark semmler
Security Services

Blockieren Sie diese Netze!

Eine einfache und elegante Möglichkeit, die Sicherheit Ihres Netzes mit wenig Aufwand nachhaltig zu stärken

Donerstag, 04.12.2008

Mark Semmler Security Services I Tel: +49 . 6151 . 42 85 68 . 0 I E-mail: kontakt_mse@mark-semmler.de

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Was erwartet Sie?

- Wir werden „Ross und Reiter“ nennen: Auf den folgenden Seiten werden Sie die schlimmsten Netze des Internets kennen lernen (ich übertreibe hier leider nicht).
- Indem Sie rigoros sämtlichen Verkehr von und zu den hier genannten Netzen blockieren, werden Sie die Sicherheit Ihres Firmennetzes bzw. Ihres privaten Rechners sehr effektiv steigern.
- Unterstützen Sie den Kampf gegen die schlimmsten Kriminellen im Netz und machen Sie mit:

Block! These! Networks!

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Kriminelle brauchen Server...

- Wenn ein Krimineller mit dem Internet Geld verdienen möchte, steht er vor einem Problem: Er benötigt (mindestens) einen Server, den er für seine kriminellen Machenschaften verwenden kann:
  - ✗ Wer mit Kinderpornos Geld verdient, braucht Server, auf denen er diese Ungeheuerlichkeiten anbieten kann.
  - ✗ Wer mit Phishing das Geld anderer Leute stiehlt, der benötigt Server, auf denen gefälschte Bankseiten gehostet werden, auf denen der arglose Benutzer seine Bankdaten eingeben soll.
  - ✗ Wer mit Spyware fremde Benutzer ausspioniert, benötigt Server, an die die geklauten Daten übertragen werden.
  - ✗ ...

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Die Server sind die Achillesferse der Kriminellen

- Diese Server sind also vital für den Kriminellen. Sie müssen zuverlässig arbeiten, da er sonst die Früchte seiner kriminellen Tätigkeiten nicht ernten kann.
- Der Kriminelle kann keine gekaperten Systeme für seine Zwecke einsetzen – gehackte Systeme können entdeckt und vom Eigentümer gesäubert bzw. geschlossen werden.
- Der Kriminelle benötigt also eine eigene IT-Infrastruktur (eigene Server). Diese Systeme sind seine Achillesferse.
- Problem für den Kriminellen:
  Welcher Provider spielt das dreckige Spiel mit und hält seine schützende Hand über die bösen Server, selbst wenn er explizit dazu aufgefordert wird, diese vom Netz zu nehmen?

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Kriminelle helfen Kriminellen…

- Mehrere spezielle Provider bieten an dieser Stelle ihre Dienste an. Sie offerieren ihren kriminellen Kunden ein so genanntes „Bullet-Proof-Hosting“ - sie garantieren ihnen unbehelligtes Arbeiten und stellen unter anderem speziell für illegale Aktivitäten konfigurierte Systeme und Infrastruktur zur Verfügung.
- Die Infrastruktur dieser Provider ist in Ländern beheimatet, die keine (funktionierenden) Gesetze gegen Cyber-Kriminalität oder keine funktionierende Justiz besitzen (Beispiel: Panama, Russland, China, …).
- Der größte kriminelle Organisation in diesem Bereich nennt sich „RBN“. RBN steht für „Russian Business Network“. Hinter dieser Bezeichnung verbergen sich kriminelle aus St. Petersburg.
- Weitere prominente Vertreter ihrer Art sind Intercage, Inhoster, McColo, Nevacon, GoEast und andere, wohl bekannte Provider.

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Beispiel RBN: Was wird bei RBN gehostet?

- Auf den Systemen von RBN tummeln sich die miesesten Kriminellen, die das Internet kennt:
  - ✗ RBN hostet Kinderpornografie der absolut allerübelsten Sorte.
  - ✗ RBN stellt Server für das Versenden von SPAM zur Verfügung.
  - ✗ RBN stellt die Infrastruktur für das Verbreiten von Viren, Würmern, Add- und Spyware sowie Server für gefälschte Webseiten bereit.
  - ✗ RBN macht nichts anderes
- **So gut wie jede bedeutende kriminelle Internet-Attacke der letzten vier Jahre hatte auf irgendeine Weise (meistens ganz direkt) mit den Netzwerken von RBN zu tun.**

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Es wird gehandelt – leider zu zögerlich!

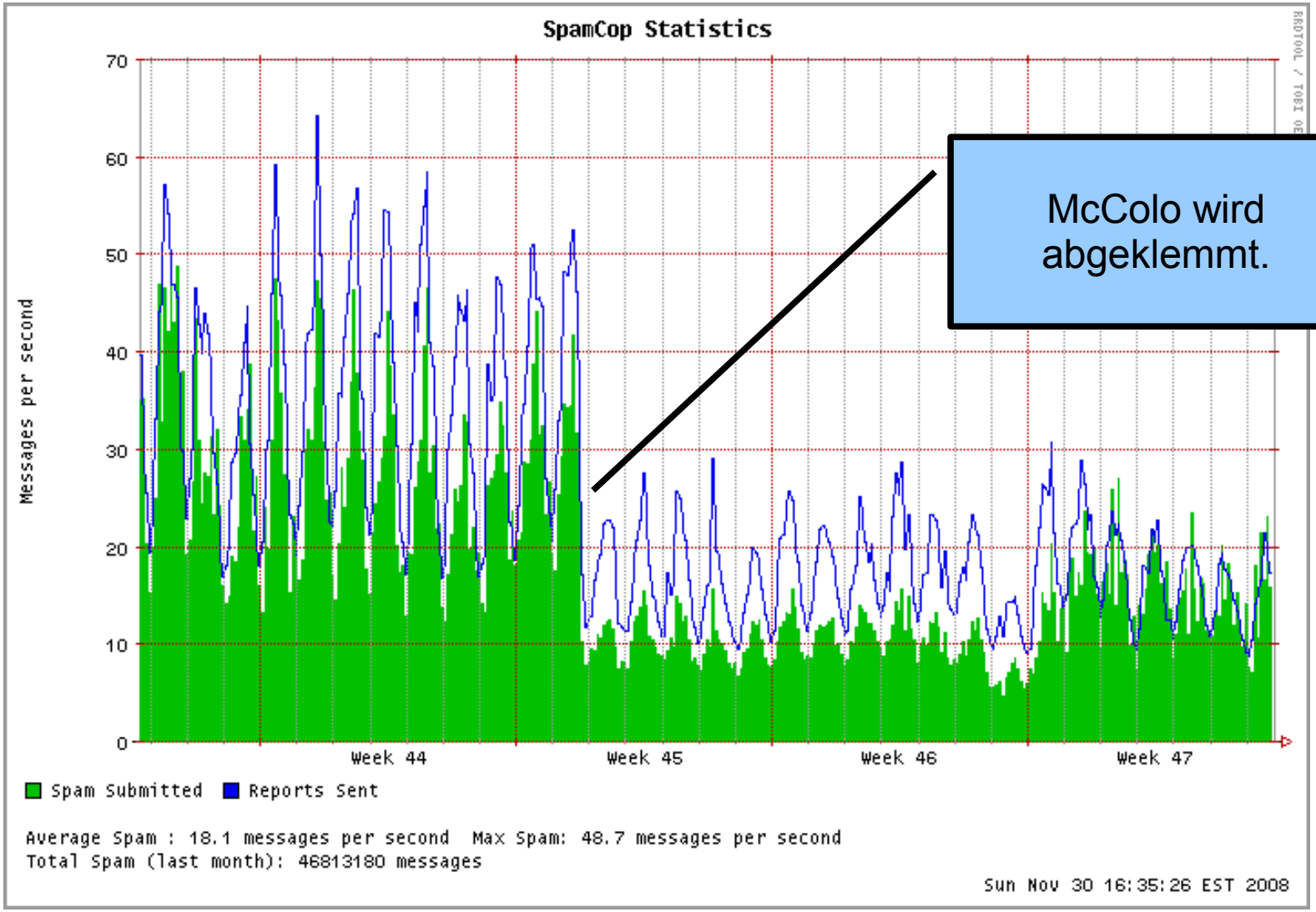
- In der Vergangenheit sind bereits einige der „schwarzen Netze“ vom Internet abgeklemmt worden.
- Am 06.11.2007 ist ein Kern-Netz von RBN offline gegangen - die Upstream-Provider haben ganz einfach die Stecker gezogen.
- Am 20.09.2008 ist der Provider Atrivo/Intercage (Sitz: California, USA) offline gegangen und am 12.11.2008 ist der Provider McColo (ebenfalls USA) offline gegangen. Auch hier haben die Upstream-Provider nach massiven Protesten gehandelt und die Leitungen gekappt!
- Natürlich verfügen (vor allem die großen) kriminellen Provider über ein weit verzweigtes Netz, dass über eine recht hohe Dynamik verfügt.
- Dennoch haben Stilllegungen von kompletten Netzen empfindliche Einbußen bei den Kriminellen zur Folge…

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Ein Beispiel: McColo Shutdown!

- Im Netz von McColo wurden unter anderem die zentralen Verwaltungsserver (C&C-Server) von verschiedenen Botnetzen gehostet. Unter anderem vom Botnetz „Srizbi“.
- Srizbi ist derzeit eines der größten Botnetze (mehr als 300.000 Mitglieder) und einer der Hauptverantwortlichen für die globale Spamflut (gemäß Marshal Limited werden 39% aller Spammails via Srizbi versendet).
- Auf der nächsten Seite betrachten wir das Aufkommen von SPAM-Mails im November 2008 (Quelle: http://www.spamcop.net).

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de



PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Über das Blockieren von kompletten Netzen...

- ...lässt sich trefflich streiten! Wer will entscheiden, wann Netze blockiert werden sollen und wann nicht? Unsere Regierung? Die UNO? Die Provider?
- Aktuelles Beispiel: Familienministerin Ursula von der Leyen (CDU) möchte, dass Provider Webseiten mit Kinderpornos sperren.
- „Tolle Gelegenheit" dachte sich Vertreter der hessischen Landesregierung und der Staatlichen Lotterieverwaltung in Bayern und fordern nun ganz unverholen, dass die Provider auch gleich illegale Glücksspielseiten sperren müssen, um so das staatliche Glücksspielmonopol zu schützen.
  Quelle: Focus Online vom 29.11.2008
  (http://www.focus.de/digital/internet/internet-gluecksspielseiten-droht-sperrung_aid_351940.html)

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Schließen Sie selbst die Pforten zur Hölle!

- Warten Sie nicht auf andere. Handeln Sie selbst!
- Die schwarzen Netze sind bekannt. Es gibt Freiwillige, die kostenlose Regelwerke herausgeben, mit deren Hilfe Sie jeden Verkehr zu und von diesen Netzen sperren können!
- Diese Regelwerke sind tagesaktuell und liegen in Formaten vor, die Sie einfach in Ihre Infrastruktur einfügen können.
- Die Folge:
  Weniger SPAM und (fast) keine Probleme mehr mit Malware!

Block! These! Networks!

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Blockieren der schwarzen Netze via DNS

- Stellen Sie durch geeignete Regeln in der Firewall sicher, dass alle Ihre Systeme nur Ihren internen DNS-Server zur Namensauflösung verwenden können (Schadsoftware modifiziert oftmals die DNS-Einstellungen befallener Systeme, um Benutzer beim Browsen im Netz auf Malware-Domains umzuleiten oder Anti-Viren-Updates zu verhindern).
- Nutzen Sie die DNS-Zonefiles der Organisation „Malwaredomains“ (http://malwaredomains.com/) für Ihren internen DNS-Server. Diese Zonefiles führen dazu, dass die Namensauflösung bekannter Malwaredomains erfolglos bleiben. Benutzer können sich nicht mehr infizieren und Schadsoftware nicht mehr „nach Hause telefonieren“.
- Führen Sie ein tägliches Update dieser Dateien durch (wget und PERL sind Ihre Freunde – auch unter Windows!).

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Blockieren der schwarzen Netze in der Firewall

- Die Organisation „Emerging Threats“ stellt auf ihrer Webseite http://www.emergingthreats.net umfangreiche, tagesaktuelle Regelwerke für folgende Firewalls zur Verfügung:
  - ✔ IPFilter (Free-, Net-, OpenBSD, Linux, SunOS, Solaris, HP-UX, Tru64. IRIX, QNX, Mac OS X)
  - ✔ Netfilter/iptables (Linux)
  - ✔ Packet Filter (Open-, Free-, Net-, DragonFly-BSD, Core force)
  - ✔ CISCO PIX
- Pflegen Sie diese Regelwerke in Ihre Firewall ein und halten Sie diese aktuell. Mit ein wenig Scripting können auch kommerzielle Firewalls mit diesen Regelwerken versehen werden!
- Sprechen Sie notfalls mit dem Hersteller Ihrer Firewall!

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Blockieren der schwarzen Netze via IDS/IDP

- Auch hier stellt die Organisation „Emerging Threats“ auf ihrer Webseite http://www.emergingthreats.net umfangreiche, tagesaktuelle Regelwerke für folgende IDS zur Verfügung:
  - ✔ snort (http://www.snort..org, verfügbar für Linux und Windows, verwendet in vielen kommerziellen Firewalls wie z.B. der Astaro)
  - ✔ Bro IDS (http://www.bro-ids.org, verfügbar für alle Betriebssysteme der UNIX-Familie)
- Pflegen Sie diese Regelwerke in Ihre Firewall ein und halten Sie diese aktuell. Mit ein wenig Scripting können auch kommerzielle Firewalls mit diesen Regelwerken versehen werden (sofern sie snort oder Bro als IDS verwenden)!
- Sprechen Sie notfalls mit dem Hersteller Ihrer Firewall!

PGP fingerprint
EF81 A404 19C9 C350 2B9B 7F8D CF85 7D93 117D 8335
www.mark-semmler.de | kontakt-mse@mark-semmler.de

Vielen Dank
für Ihre Aufmerksamkeit
&
allzeit sicheres Arbeiten!