

## **PRESSEMITTEILUNG**

### **Effektivere Phishing- und Malware-Attacken mit Fast-Flux-Netzwerken – BullGuard beobachtet rasante Zunahme der Tarn-Technologie**

*Immer mehr Bot-Netz-Betreiber nutzen die Technologie um die Standorte ihrer Server zu tarnen*

München/Kopenhagen, 09. Oktober 2008 – Auch Cyber-Kriminelle arbeiten unablässig an der Verfeinerung ihrer Methoden und Technologien. So meldet BullGuard, Spezialist für benutzerfreundliche Sicherheitslösungen für PC und mobile Geräte, den immer häufigeren Einsatz der so genannten Fast-Flux-Netzwerke. Mit dieser Technologie lassen sich Phishing- und Malware-Attacken hervorragend hinter sich fortwährend verändernden Netzwerken von gehackten Computern verbergen. Ein Fast-Flux-Netzwerk nutzt dabei die Reports öffentlicher Domain-Name-Server, die sich im Minutentakt oder gar sekundlich ändern - und somit praktisch nicht mehr verfolgt und lahm gelegt werden können. Da die Internet-Kriminellen beim Hosting oder Versand von Malware die IP-Adresse der infizierten Computer ständig rotieren lassen, ist es extrem schwierig, die betreffenden Rechner zu blockieren.

#### **Bot-Netze von der Stange**

Das Storm-Botnet beispielsweise, dem Schätzungen zufolge zwischen einer und fünf Millionen kompromittierter Rechner angehören, ist eines jener Botnetze, die die Fast-Flux-DNS-Hosting-Technik für sich nutzen. Als eine Reihe von Phishing-Sites Domains nutzten, die eindeutig auf das Storm-Worm-Botnet zurückgeführt werden konnten, zeigte es sich, dass genau diese Domains zuvor von Internet-Kriminellen gekauft oder gemietet worden waren und damit eine wahre Welle von Fast-Flux-Phishing-Angriffen auslösten. Für Preise von 100.000 Dollar aufwärts konnten Spammer und andere Malware-Angreifer ihr höchsteigenes Storm-Worm-Botnet erwerben, Fast-Flux-DNS und Hosting-Möglichkeiten eingeschlossen.

---

#### **Kontakte für die Presse:**

Jürgen Rast  
Anne Andres  
Trademark PR GmbH  
Goethestr. 66  
D-80336 München  
Tel.: +49 (0)89 444 467-466  
BullGuard@trademarkpr.eu  
[www.trademarkpr.eu](http://www.trademarkpr.eu)

## **Tendenz weiter steigend**

Sicherheitsexperten ist diese Technik bereits seit 2006 bekannt, zu richtiger Berühmtheit gelangte aber erst eine Fast-Flux-Attacke vom Sommer 2007, bei der beinahe 100.000 MySpace-Seiten betroffen waren.

Im März 2008 deckte ein Sicherheitsanbieter auf, dass die Fast-Flux-Technik, die bis dahin nur als Instrument der Storm-Botnet-Betreiber betrachtet wurde, inzwischen von wenigstens drei weiteren kompromittierten Netzwerken verwendet wurde. So gelangte beispielsweise ein berüchtigtes organisiertes Hosting-Netzwerk aus Russland zu trauriger Bekanntheit, indem es Fast-Flux einsetzte um die Standorte der Server unkenntlich zu machen. Security-Forscher, ISPs oder Behördenvertreter hatten keine Chance, die Aktivitäten dieser Gruppe zu verfolgen. Die Superhirne hinter dem großen Asprox-Botnet haben 2008 ebenfalls schon mehrmals Fast-Flux-Techniken für ihre Zwecke eingesetzt.

PC-Anwender, deren Rechner als Mitglied eines Bot-Netztes unfreiwillig Anteil an dieser Entwicklung haben, sind mehr denn je aufgefordert, ihren PC zu schützen, indem sie verhindern, dass ihr Rechner durch Malware-Attacken überhaupt erst Teil eines solchen Bot-Netztes werden. Hersteller von Security-Lösungen wie beispielsweise BullGuard mit der Internet Security 8.5 bieten nachhaltig verbesserte Firewall- und Spamfilter-Funktionalitäten sowie Remote Access für den BullGuard-Support. In dem neuen Release wurden auch sämtliche klassischen Schutzmechanismen überarbeitet, um alle Bedrohungsszenarien sicher ausschließen zu können. Kontinuierliche Updates der Patches mit der derzeit schnellsten Aktualisierungsfrequenz auf dem Markt schützen Rechner ab sofort auch vor allen neuen Formen von Malware.

## **Über BullGuard**

BullGuard hat sich auf Sicherheitslösungen für PCs und mobile Geräte spezialisiert und richtet sich damit vor allem an Heimanwender und kleine Betriebe. Im Mittelpunkt stehen dabei die technische Expertise, das einfache Handling und ein umfassender persönlicher Kunden-Support. BullGuards Stärke liegt darin, einfach zu bedienende und preiswerte integrierte Sicherheitslösungen anzubieten, die die Nutzer mit erstklassigem Schutz vor Computerwürmern und anderer Malware versorgen.

Der Hauptsitz von BullGuard befindet sich in Kopenhagen, Dänemark, das Unternehmen unterhält Niederlassungen in Rumänien, Australien und in Großbritannien.