Deutscher Sicherheitsspezialist 8ack klärt Botnet-Angriffe auf und stellt Frühwarnsystem vor

Gewappnet gegen Botnet-Attacken

Der FBI-Botnet-Bericht aus dem letzten Jahr belegt: Auf das Konto von Botnets gehen allein in den Staaten über 9 Milliarden Dollar an Verlusten. Weltweit sollen es nach Schätzungen sogar rund 110 Milliarden Dollar an monetären Einbußen sein, die eine Armada an infizierten Rechnern verursacht. Die genaue Zahl liegt im Dunkeln. Doch laut dem FBI kommen jährlich über 500 Millionen infizierte Computer weltweit neu hinzu, so dass davon ausgegangen wird, dass jede Sekunde 18 Unternehmen weltweit Opfer einer Botnet-Attacke werden.

Heerschaaren von Cyberkriminellen und zahlreiche organisierte Cyber-Ringe, die aus den Attacken massiv Gewinn schlagen beziehungsweise gezielt für Schäden bezahlt werden, sorgen dafür, dass diese Bedrohung stetig zunimmt.

Botnets können jeglichen Dienst oder jede Anwendung im Web koordiniert und massiv angreifen. Das Problem: ist ein Botnet eliminiert, keimt schon das nächste noch raffinierter ausgelegte auf. Von der Vielzahl an infizierten Rechnern, von denen fast alle Besitzer -- ob privater Endanwender oder Mitarbeiter in Unternehmen -- nicht einmal wissen, dass sie kompromittiert sind, geht eine immense Bedrohung aus. Denn durch die globale Verteilung der einzelnen Rechner, die bei einer geplanten Attacke ein gemeinsames Angriffssystem bilden, ist eine individuelle Abwehr durch das Opfer kaum möglich. Das Verhältnis zwischen organisiertem Cyber-Verbrechen und den "Guten" kippt durch die Botnetze massiv auf die Seite der Hacker.

"Botnetze sind das Rückgrat der Internetkriminalität", erläutert Daniel Schattke, Geschäftsführer des deutschen Sicherheitsspezialisten 8ack aus Kiel. Deshalb hat sich 8ack darauf konzentriert, Mechanismen zu entwickeln, die die weltweit agierenden Botnetze in einem Frühwarnsystem erkennen, die Angriffsaktivitäten auf der eigenen "Global-Attack-Map" sichtbar machen und mit ihrem eigenentwickelten "Threat Intelligence Feed" und einem Scoring-Modell zuverlässig aufklären und vermeiden helfen. "8ack ist als einziges deutsches Unternehmen in der Lage, Botnet-Aktivitäten bis auf Einzelrechnerebene zu analysieren", erklärt Schattke.

Um Botnet-Aktivitäten zuverlässig aufzuklären und die richtigen Maßnahmen zur Vermeidung von Schäden auf Webseiten und Diensten der Unternehmen zu empfehlen, kommen die beiden Produkte "Global-Attack-Map" und der IP-Reputation-Service von 8ack zum Einsatz.

Global-Attack-Map

Die Global-Attack-Map ist Teil des umfassenden Services von 8ack gegen Cyber-Attacken für Carrier, Service-Provider und Unternehmen. Basis für die Daten der Hacker-Aktivitäten sind weltweit verteilte Sensoren, die als Honeypot in Rechenzentren jeglicher Couleur agieren sowie der "IP-Reputation-Service".

Die zahlreichen Sensoren von 8ack aggregieren die Hacker-Aktivitäten auf der Global-Attack-Map. Brute-Force-, Web-, Vulnerability-Attacken und -Scans werden grafisch auf einer globalen Karte dargestellt und zeigen das aktuelle Angriffsverhalten in den Regionen dieser Welt. Zudem visualisiert die 8ack-Global-Attack-Map Informationen über die IP-Adresse mit den meisten Angriffen, aus welchen Rechenzentren das Gros der Angriffe stammt oder welcher Provider die meisten kompromittierten Server zu verzeichnen hat.

IP-Reputation-Service

Während die Honeypots den "Bösewichtern" potenziell interessante Sites vorgaukeln, erfasst der IP-Reputation-Service mit seinem "Threat Intelligence Feed" deren Aktivitäten. Dieser Dienst protokolliert die vorliegenden Attacken wie Brute-Force-, Web-,Vulnerability-Attacken sowie -Scans und wertet sie entsprechend aus.

Dazu werden die Rohdaten aus dem weltweit verteilten Sensorennetz über verschiedene Algorithmen korreliert und jeder Angreifer-IP wird ein Score zugewiesen, um False-Positives auszuschließen und um echte Angreifer zuverlässig zu identifizieren. 8ack stellt dazu den Kunden als Service eine stetig aktualisierte Kopie dieser Angreifer-Datenbank lokal zur Verfügung, damit diese erkannte und bekannte Angreifer blocken können. Die Angreifer-Datenbank basiert auf über 10.000.000 erkannten Angriffen je Monat und über 500.000 identifizierten Unique-IPs. Standardmäßig ist eine Integration in Apache- und Nginx-Webserver vorgesehen. Zudem lässt sich die Angreifer-Datenbank in Firewalls, IDS/IPS- sowie SIEM-Produkte integrieren, um den ganzheitlichen Schutzwall zu komplettieren, den Carrier-, Service-Provider und Unternehmen dringendst benötigen.

8ack bietet die Services entweder einzeln oder als Paket im Rahmen von Serviceverträgen an und berät Carrier-, Service-Provider und Unternehmen generell zur IT-Sicherheitsthematik.

Pressekontakt

New Technology Communication

Herr Uwe Scholz
Albrechtstr. 119
12167 Berlin

uscholz.com
uscholz@uscholz.com

Firmenkontakt

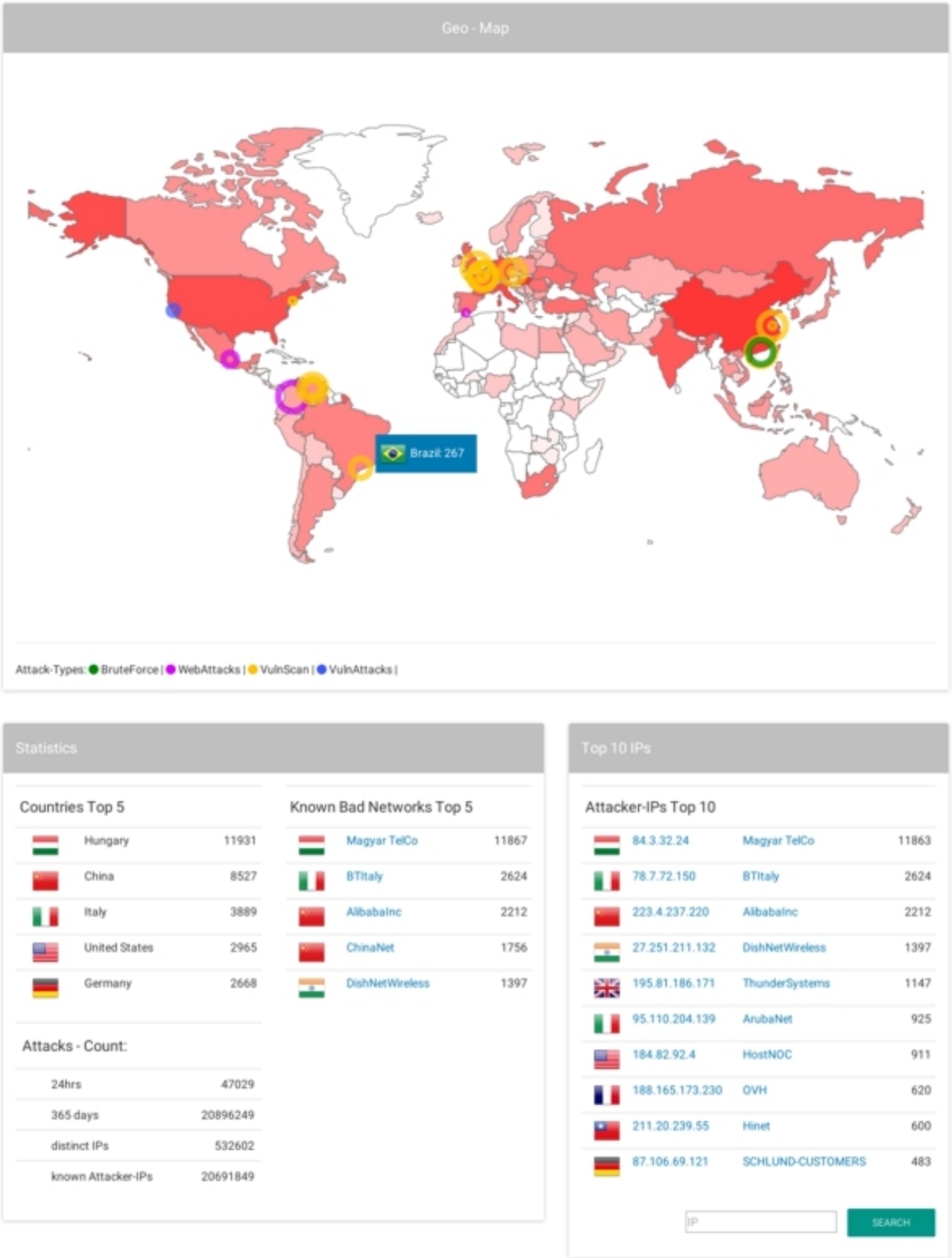
8ack

Herr Björn Christiansen
Werftbahnstr. 8
24143 Kiel

http//:8ack.de
mail@8ack.de

Das Unternehmen 8ack aus Kiel hat sich auf IT-Security-Lösungen "Made in Germany" spezialisiert. Es offeriert als einziges deutsches Unternehmen sensorgestützte Internet-Security-Lösungen. 8ack wurde mit dem Innovationspreis IT 2015 ausgezeichnet und ist Partner der Allianz für Cybersicherheit, Mitglied im TeleTrust - Bundesverband IT-Sicherheit e.V. und Unterstützer des Qualitätssiegels "IT Security Made in Germany".

Anlage: Bild


Geo - Map
Brazil: 267
Attack-Types: BruteForce | WebAttacks | VulnScan | VulnAttacks |
Statistics
Countries Top 5
Hungary 11931
China 8527
Italy 3889
United States 2965
Germany 2668
Known Bad Networks Top 5
Magyar TelCo 11867
BTItaly 2624
AlibabaInc 2212
ChinaNet 1756
DishNetWireless 1397
Attacks - Count:
24hrs 47029
365 days 20896249
distinct IPs 532602
known Attacker-IPs 20691849
Top 10 IPs
Attacker-IPs Top 10
84.3.32.24 Magyar TelCo 11863
78.7.72.150 BTItaly 2624
223.4.237.220 AlibabaInc 2212
27.251.211.132 DishNetWireless 1397
195.81.186.171 ThunderSystems 1147
95.110.204.139 ArubaNet 925
184.82.92.4 HostNOC 911
188.165.173.230 OVH 620
211.20.239.55 Hinet 600
87.106.69.121 SCHLUND-CUSTOMERS 483
IP
SEARCH