



Threat Deception - Zusätzlicher Schutz gegen Hackerangriffe

Kiel, 11.11.2015



1

Einleitung

Threat Deception – Extern

Threat Deception – Intern

Hackeraktivitäten florieren – dank des attraktiven Business Cases



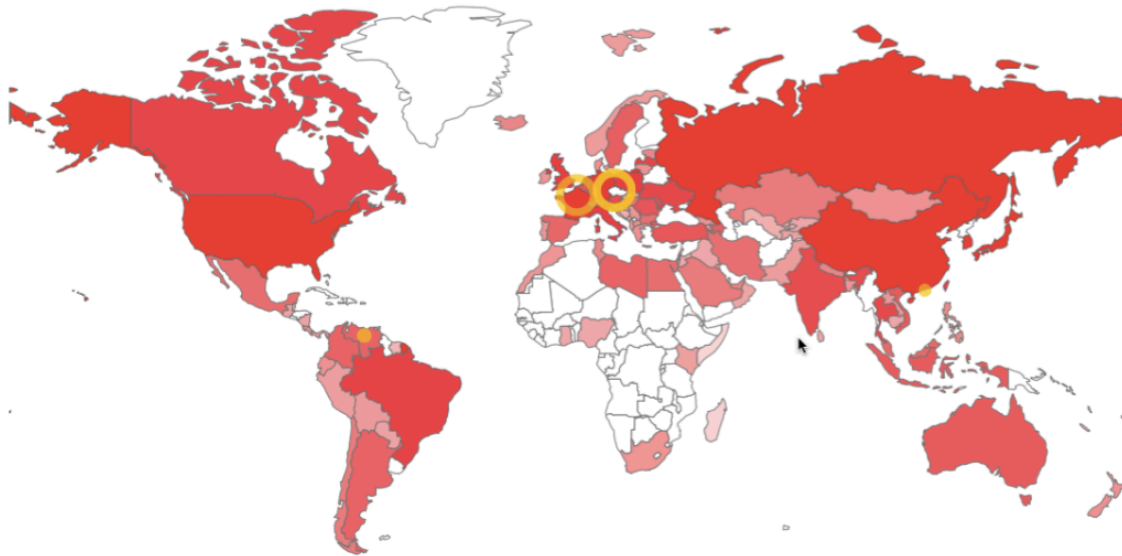
Einflussfaktoren für „Wachstums-case Internet-Kriminalität“



Threat Deception Made in Germany



8ack registriert 1,5 Mrd. Hackerangriffe pro Jahr



Attack-Types: ● BruteForce | ● WebAttacks | ● VulnScan | ● VulnAttacks |

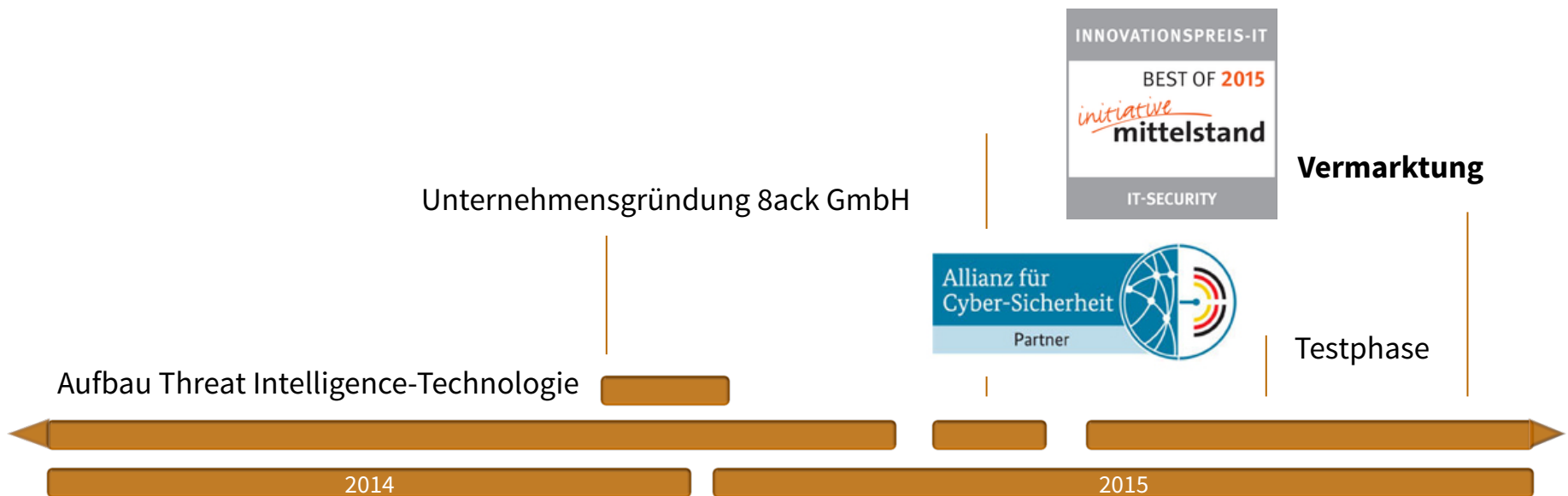
- Verhaltensbewertung als Ergänzung zur Mustererkennung (Antivirus, etc.) in Echtzeit verfügbar
- Bewertung/Scoring ermöglicht zuverlässig den Ausschluss automatisierter Hacker-Angriffe
- Interner Einsatz der Technologie ermöglicht Aufspüren dedizierter Hacker Angriffe (Spear-Phishing, etc.)

Das Unternehmen – Auszeichnungen unterstreichen Innovationsstärke von 8ack



Historie

- Einziger europäischer Anbieter von Threat Intelligence / Threat Deception Produkten
- Mitarbeiterwachstum auf mittlerweile 10 Mitarbeiter in 2015, Stetiger Aufbau Kundenbasis
- Gut vernetzt in diversen Interessensvereinigungen: Teletrust, BSI, IT Security Made In Germany
- Ausgezeichnet mit dem Innovationspreis „Best of 2015“ der Initiative Mittelstand





Einleitung

②

Threat Deception – Extern

Threat Deception – Intern

■ Problem

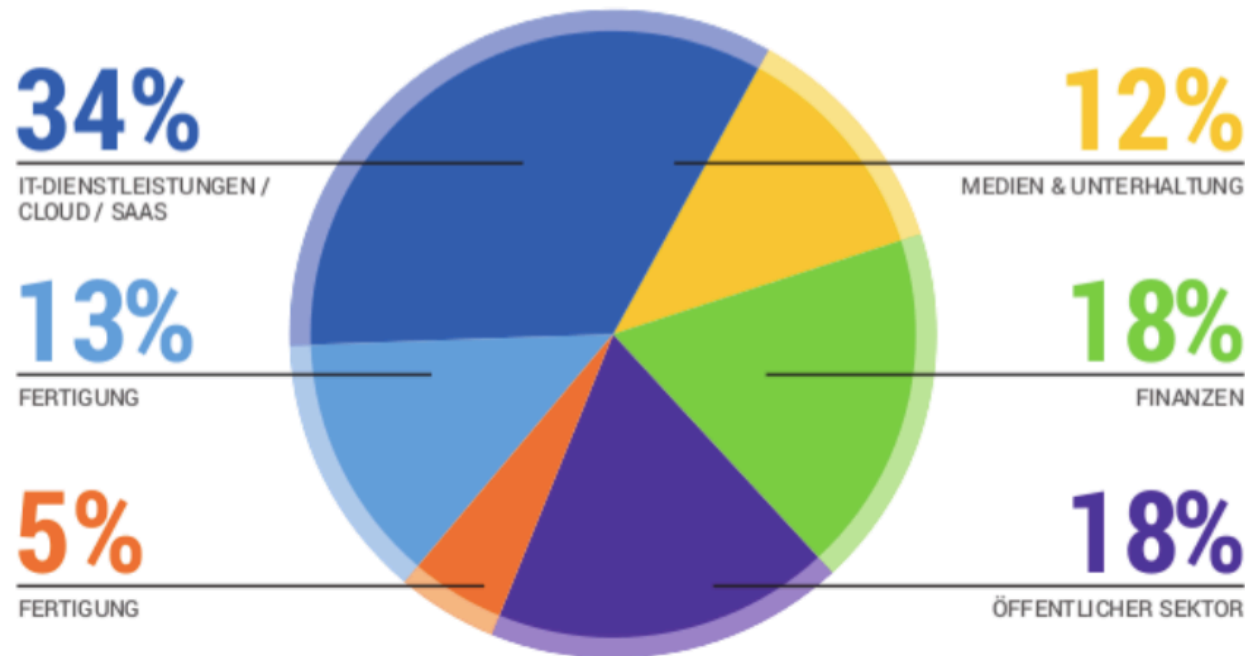
- Abhängigkeit von digitaler Kommunikation
- Bedrohungslage hochdynamisch
- Exploits vor Patches
- Scanner-Techniken
- Shodan.io
exploit-db.com
- Botnetz-Angriffe

■ Lösung

- Kontinuierliche Aufklärung
- Abgleich der Schutzmechanismen an Bedrohungslage
- Dynamische (aktive) Verteidigung



Jede Branche ist eine Zielgruppe



Quelle: Verisign

Remote Exploits

This exploit category includes exploits for remote services or applications, including client side exploits.

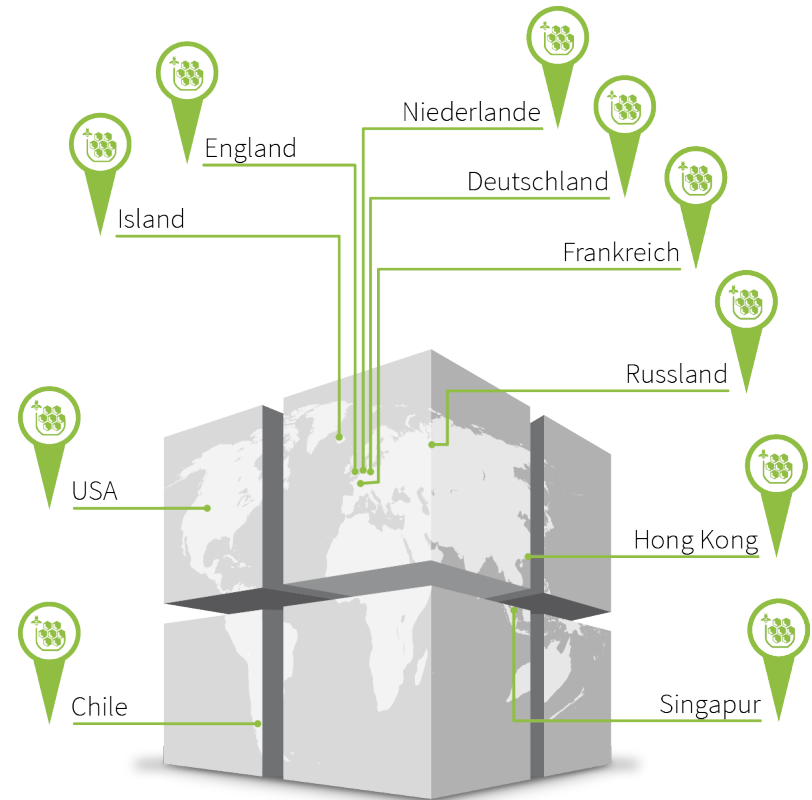
Date	D	A	V	Title	Platform	Author
2015-11-10	↓	-	🔒	Huawei HG630a and HG630a-50 - Default SSH Admin Password on ADSL Modems	hardware	Murat Sahin
2015-11-09	↓	📄	✅	Wordpress Ajax Load More PHP Upload Vulnerability	php	metasploit
2015-11-07	↓	-	✅	Cryptocat Arbitrary Script Injection Vulnerability	multiple	Mario Heideric.
2015-11-06	↓	-	🔒	Solarwinds Log and Event Manager/Trigeo SIM 6.1.0 - Remote Command Execution	windows	Chris Graham
2015-11-02	↓	-	✅	Symantec pcAnywhere 12.5.0 Windows x86 - Remote Code Execution	win32	Tomislav Paska.
2015-10-28	↓	-	✅	Samsung SecEmailUI Script Injection	android	Google Securit.
2015-10-27	↓	-	✅	Th3 MMA mma.php Backdoor Arbitrary File Upload	php	metasploit

Web Application Exploits

This exploit category includes exploits for web applications.

Date	D	A	V	Title	Platform	Author
2015-11-07	↓	-	🔒	Google AdWords API PHP client library <= 6.2.0 - Arbitrary PHP Code Execution	php	Dawid Golunski
2015-11-07	↓	-	🔒	eBay Magento CE <= 1.9.2.1 - Unrestricted Cron Script (Potential Code Execution / DoS)	php	Dawid Golunski
2015-11-07	↓	-	🔒	Google AdWords <= 6.2.0 API client libraries - XML eXternal Entity Injection (XXE)	php	Dawid Golunski
2015-11-10	↓	-	🔒	Jenkins 1.633 - Unauthenticated Credential Recovery	java	The Repo
2015-11-10	↓	-	🔒	YESWIKI 0.2 - Path Traversal Vulnerability	php	HaHwul
2015-11-09	↓	-	🔒	Arris TG1682G Modem - Stored XSS Vulnerability	hardware	Nu11By73
2015-11-09	↓	📄	🔒	TestLink 1.9.14 - CSRF Vulnerability	php	Aravind C Ajay.

- Weltweites Sensornetzwerk
- Tracking und Korrelation von Angriffen
- Echtzeit-Datafeed schützt Infrastruktur, Server und Dienste










Per 10.11.2015

Statistics

Countries Top 5

	China	480577
	United States	219498
	Japan	147529
	France	128279
	Russian Federation	58970

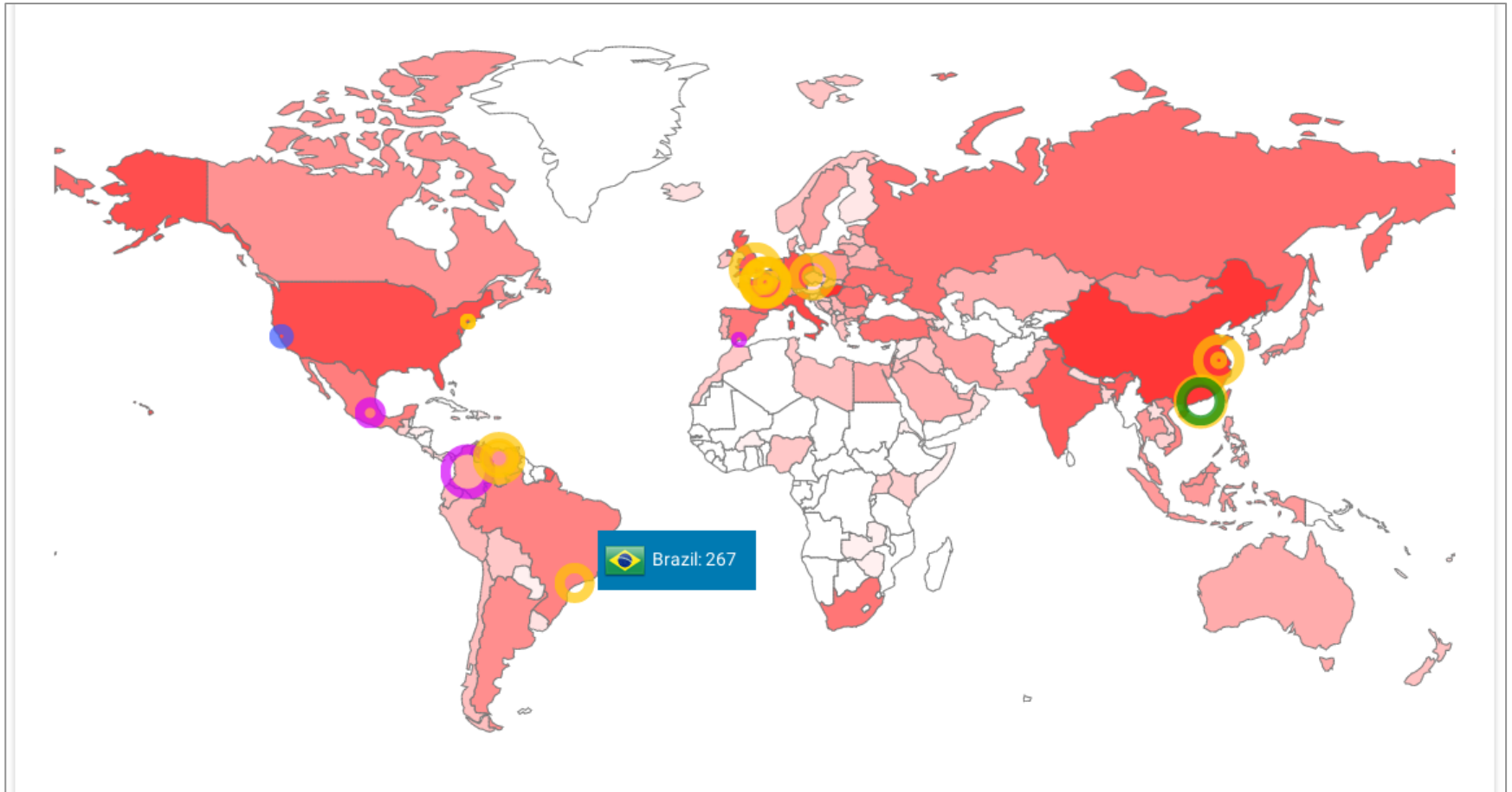
Known Bad Networks Top 5

	ChinaNet	298558
	HotNet Ltd	146739
	OVH	76897
	Iliad Datacenters	73173
	UNIFIEDLAYER	59701

Attacks - Count:

24hrs	1556750
365 days	239935069
distinct IPs	3537730
known Attacker-IPs	86771902

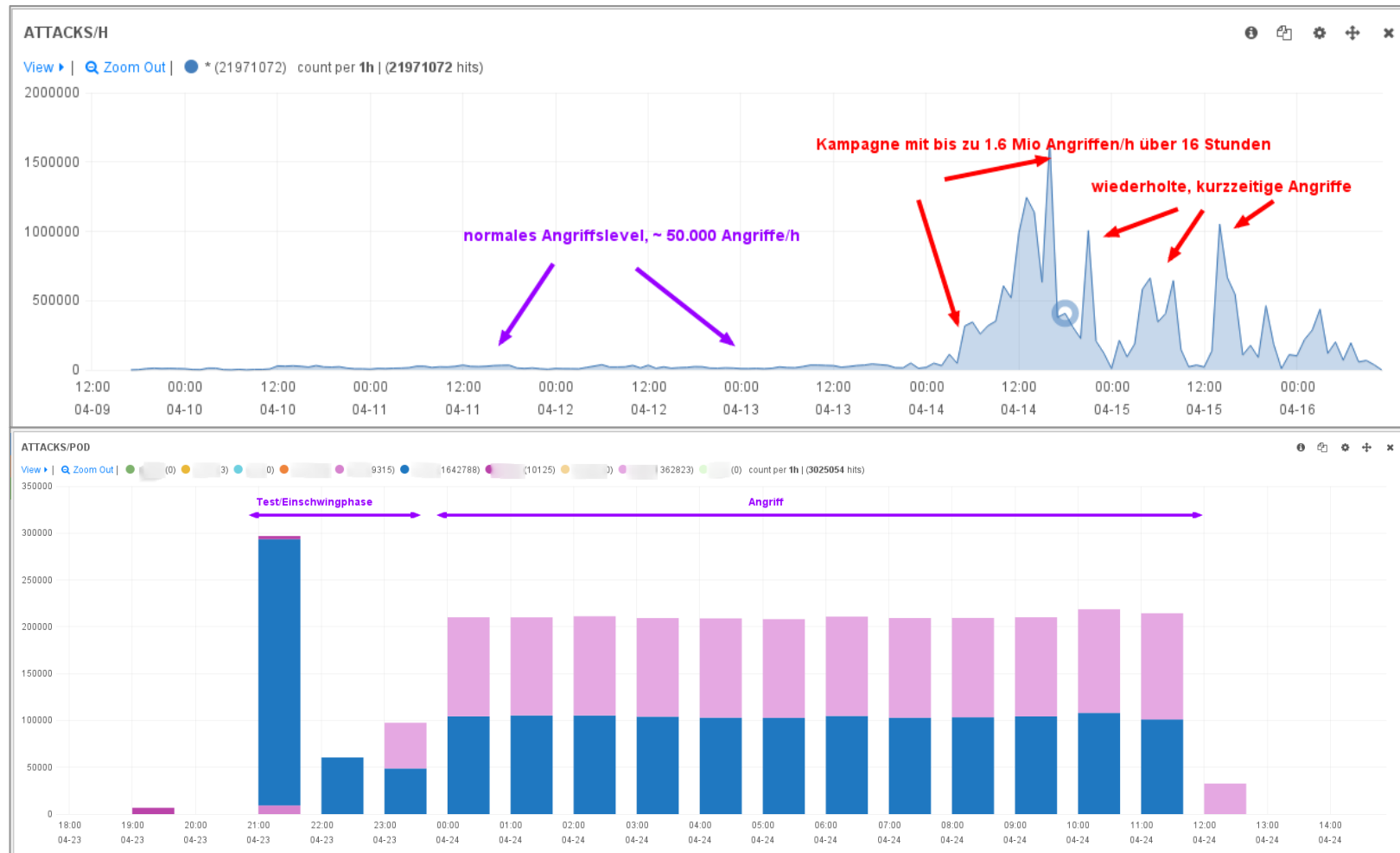
Übersichtskarte der weltweiten Angriffe aus 8acks Perspektive



Botnetzangriffe aufgeklärt (1/2)



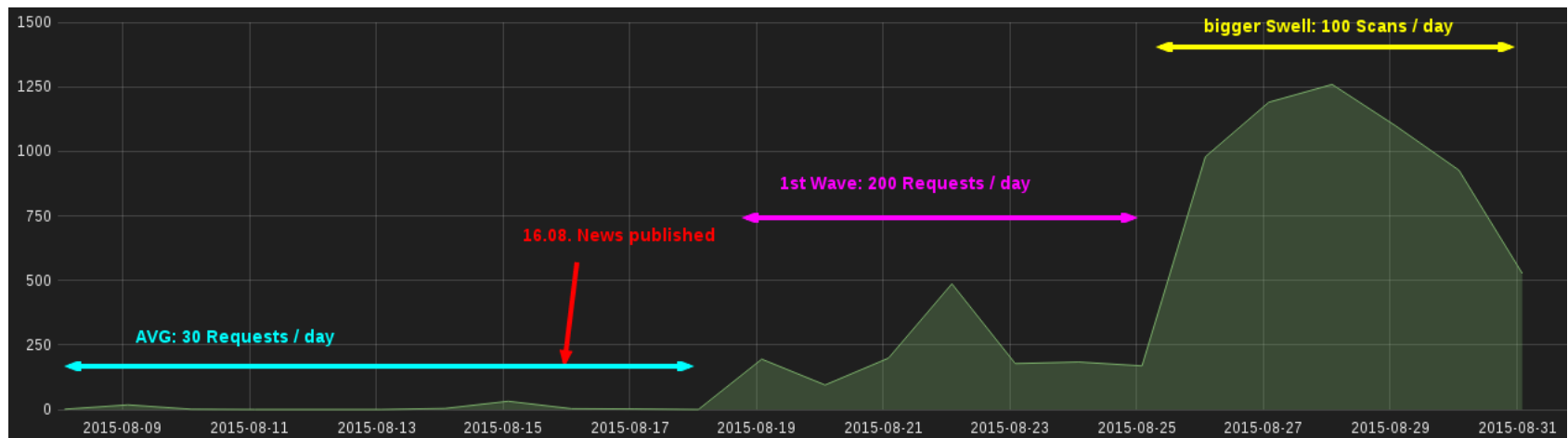
Dashboard



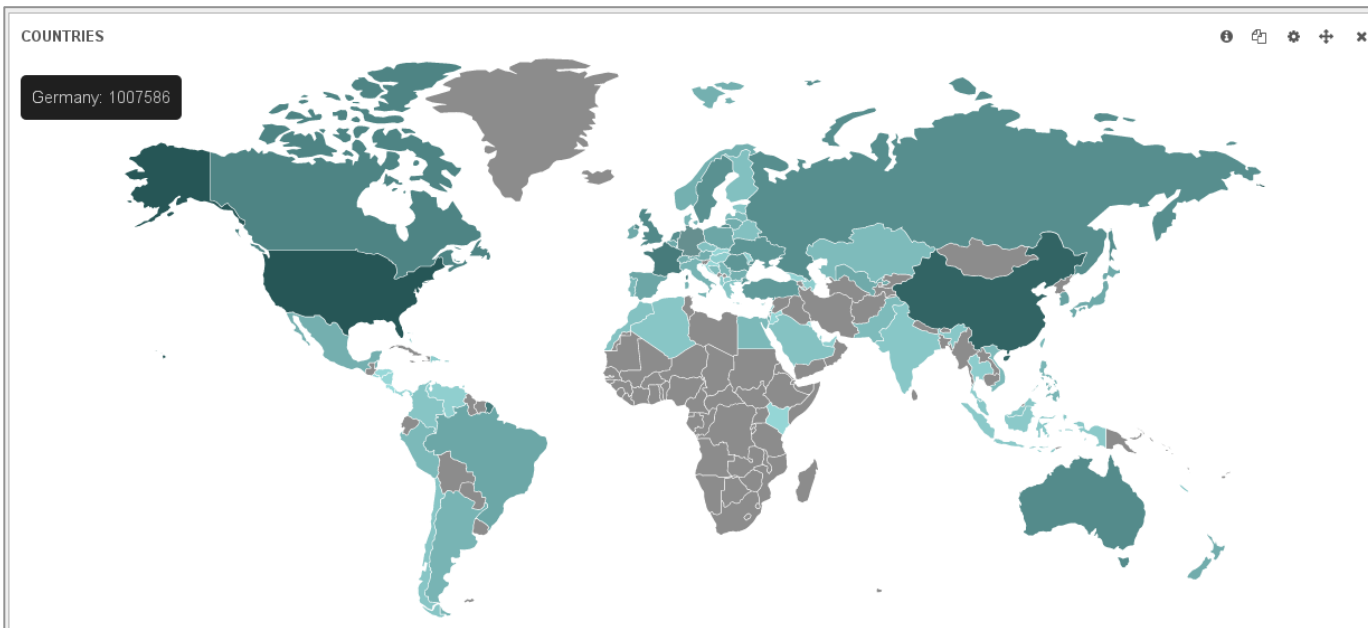
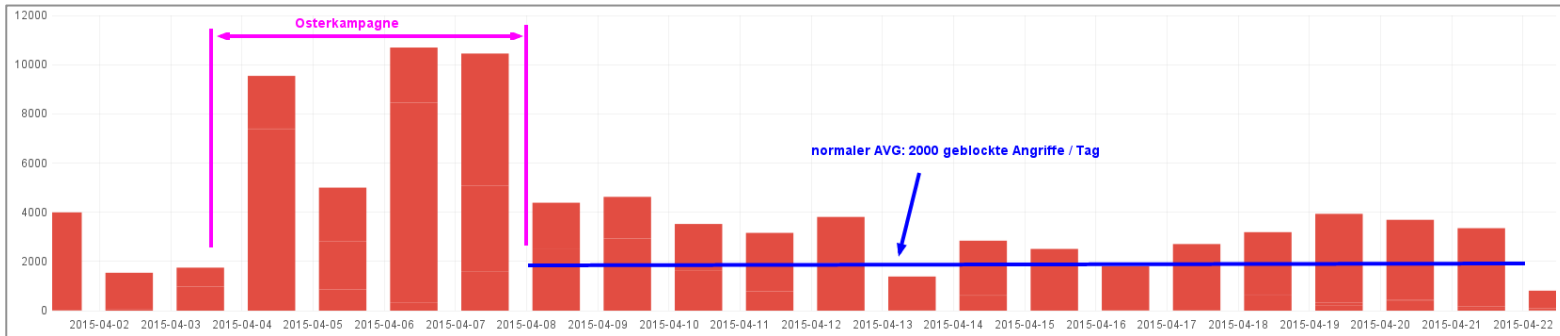
Botnetzangriffe aufgeklärt (2/2)



- 24h nach Publizieren einer Lücke wird aktiv danach gescannt



Features





Einleitung

Threat Deception – Extern

3

Threat Deception – Intern

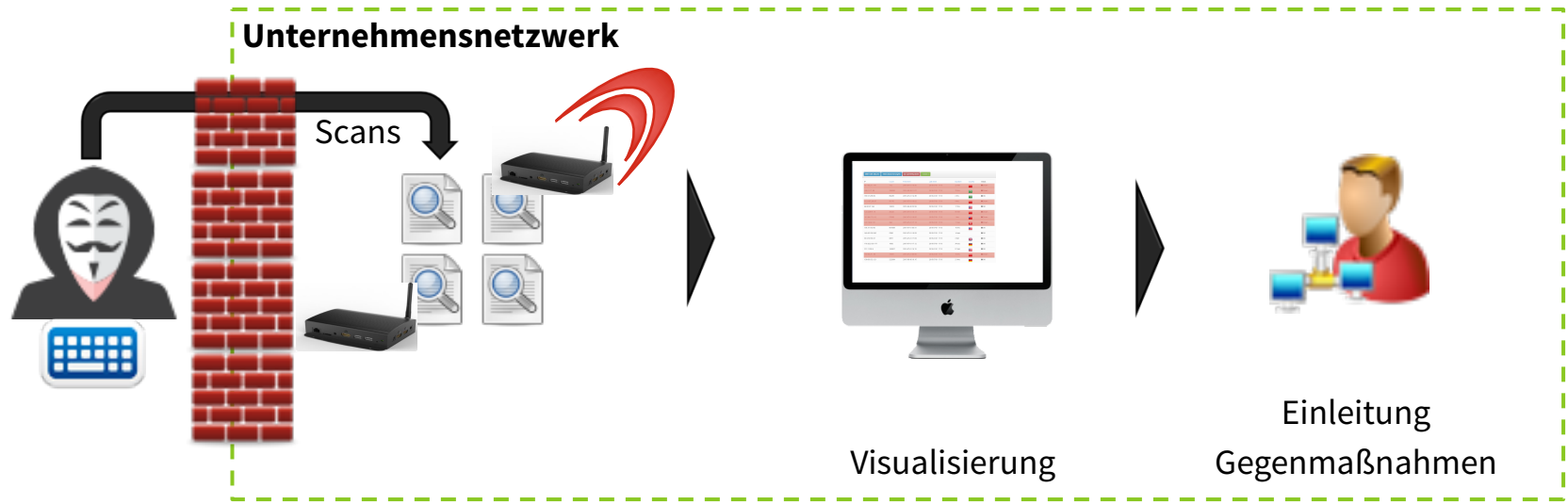
■ Problem

- Layer-8
- Social Engineering
- SpearPhishing, APT
- Grenzen für signaturbasierte Systeme
- Google, Facebook, Bundestag, RSA, Apple ...
- 200 Tage unerkant
- Smokescreening, Ausleitetechniken



The screenshot shows a news article from Spiegel Online. The main headline is "Hackerangriff auf den Bundestag: Das entblößte Parlament". Below the headline is a photograph of the Reichstag building in Berlin. The article text below the photo reads: "Wie dramatisch ist der Spähangriff auf den Bundestag? Die Abgeordneten fühlen sich alleingelassen, die Arbeit im Parlament leidet. Noch heute soll eine Entscheidung über das weitere Vorgehen fallen."

Funktionsweise



- Erkennen der Aufklärungsphase
- Ablenkung der Eindringlinge
- Verlangsamung des Angriffs
- Zeitgewinn für Gegenmaßnahmen



8ack GmbH
Werftbahnstr. 8
24143 Kiel

t: 0431 55 68 3481
m: mail@8ack.de