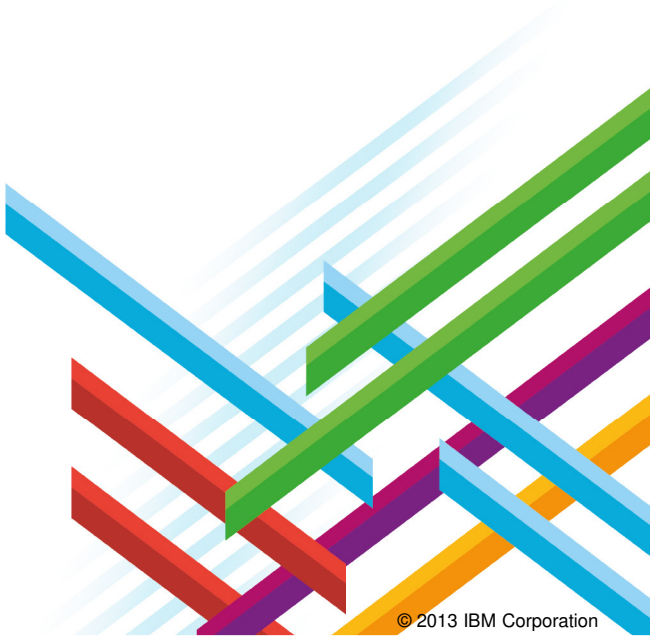
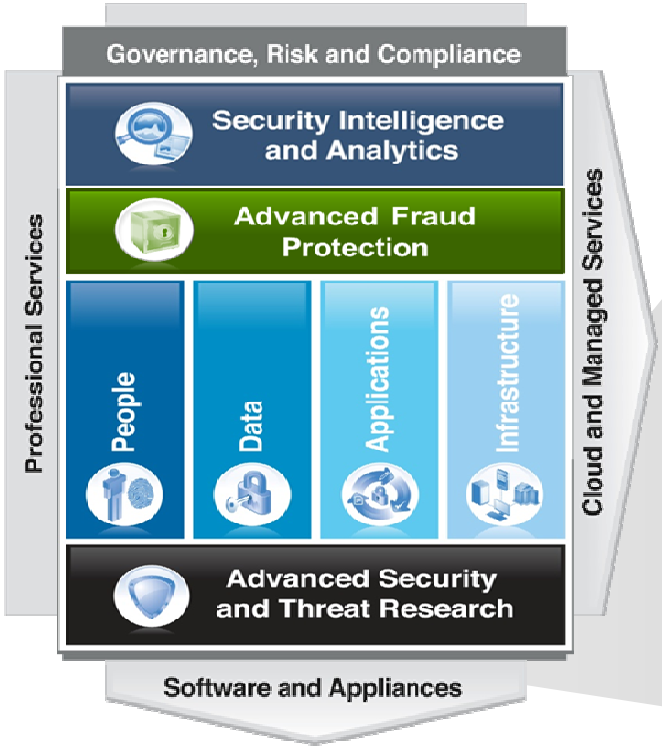
Security

IBM X-Force 2013 Mid-Year Trend and Risk Report

Carsten Dietrich



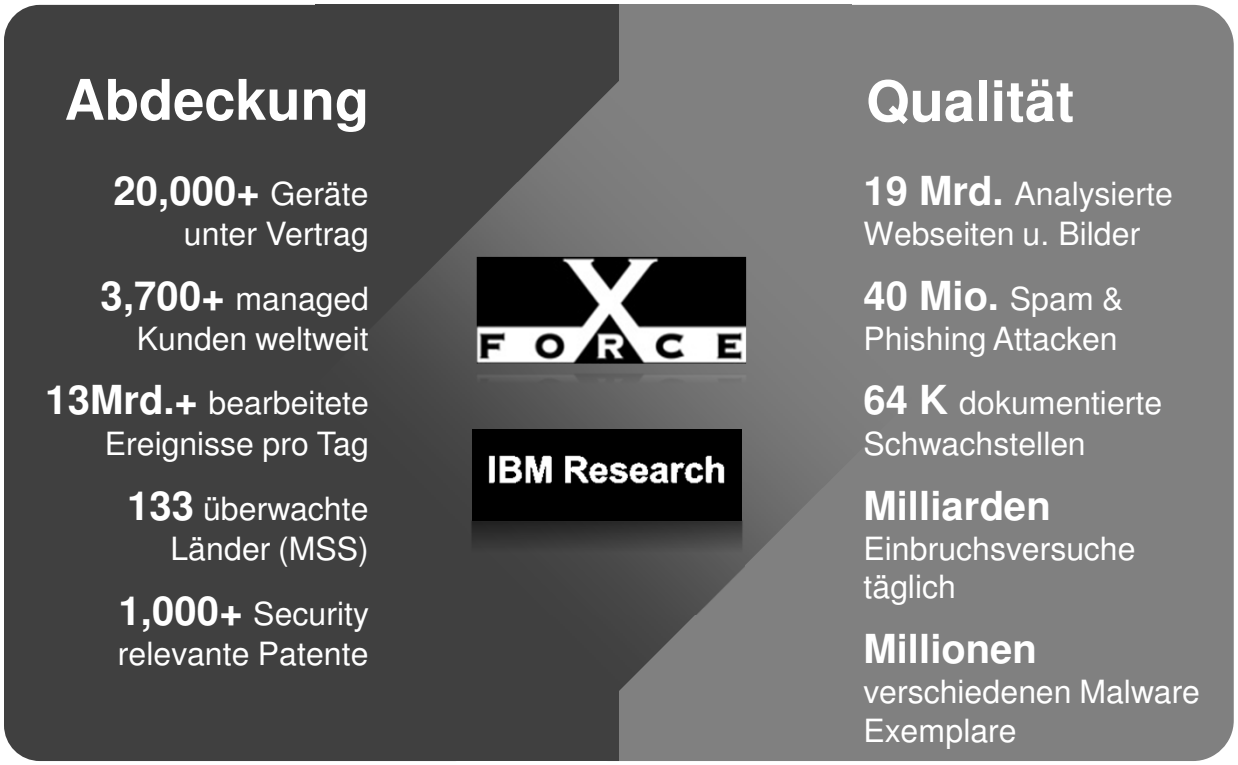
X-Force bildet die Basis für „Advanced Security and Threat Research“ für das IBM Security Framework



Die Mission der X-Force:

- **Überwachung** und Auswertung der sich schnell ändernden Angriffs-Landschaft
- **Erforschung** neuer Angriffs-Techniken und Entwicklung von Schutzvorkehrungen für die Herausforderungen von Morgen
- **Schulung** unserer Kunden u. der Öffentlichkeit

Verteilte IBM-Teams überwachen und analysieren die neusten Sicherheitsvorfälle weltweit



Die wichtigsten Ergebnisse des Trend Report 2013 H1

Threats and Activity

- 40% mehr Einbrüche (Datendiebstahl) in 2012 – Trend setzt sich in 2013 fort
- Raffinesse ist nicht immer eine Frage der Technologie
- Mit Java so viele Systeme wie möglich infizieren

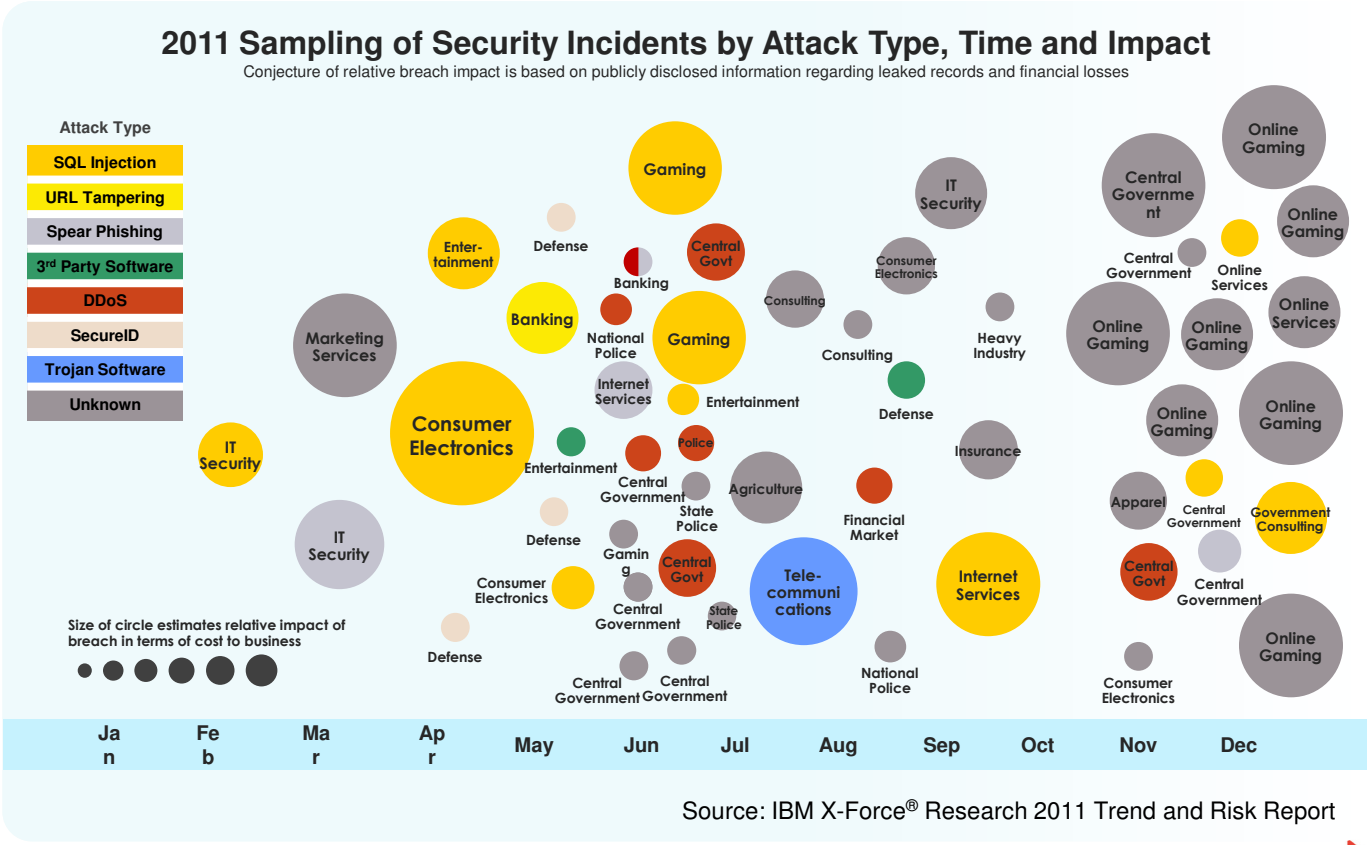
Operational Security

- Schwachstellen in Web Applikationen steigen an
- Plug-Ins für Content Management Systeme bieten ein leichtes Ziel

Emerging Trends

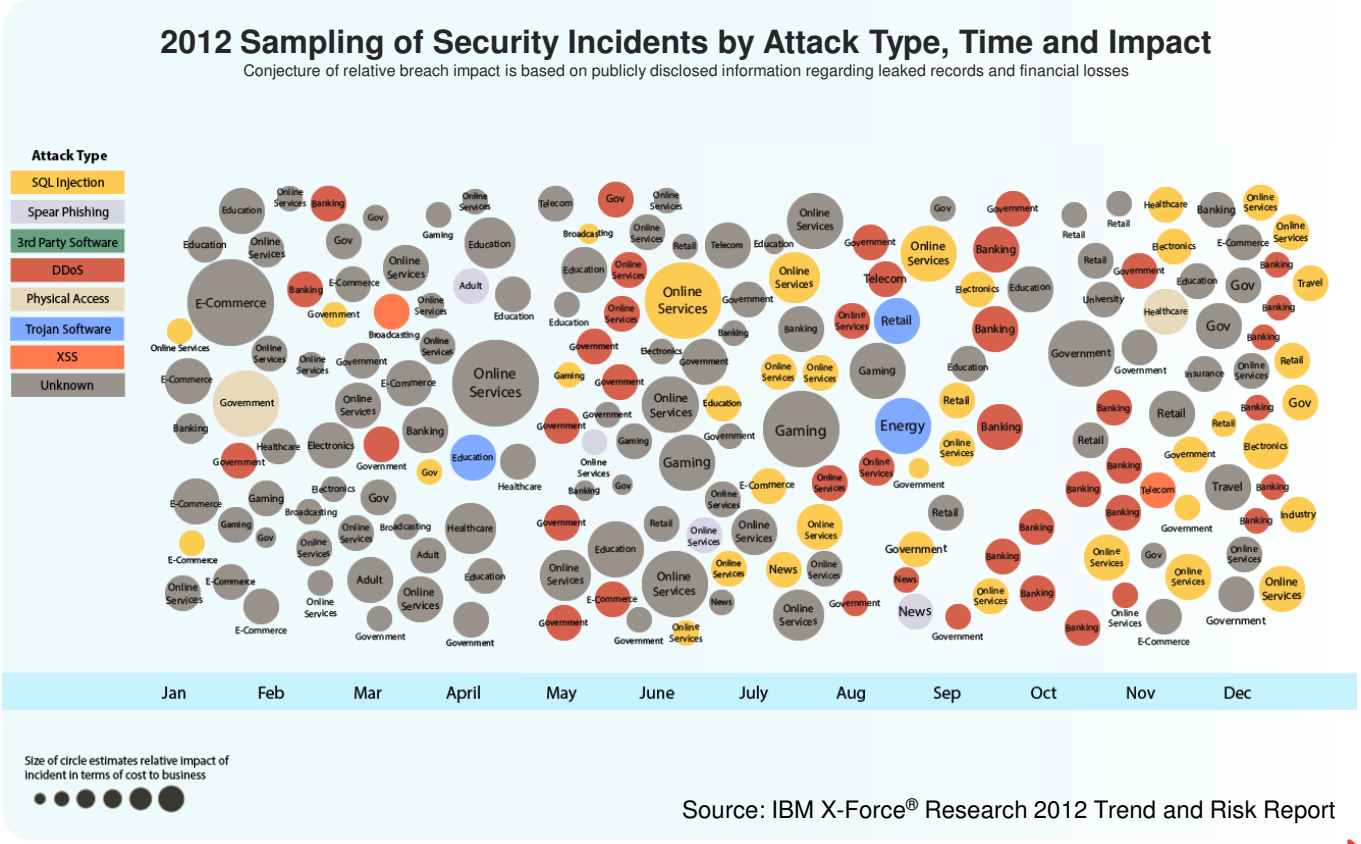
- Soziale Netzwerke werden zunehmend für Spear-Phishing und das Sammeln von Informationen für Angriffe genutzt

2011: “The year of the targeted attack”



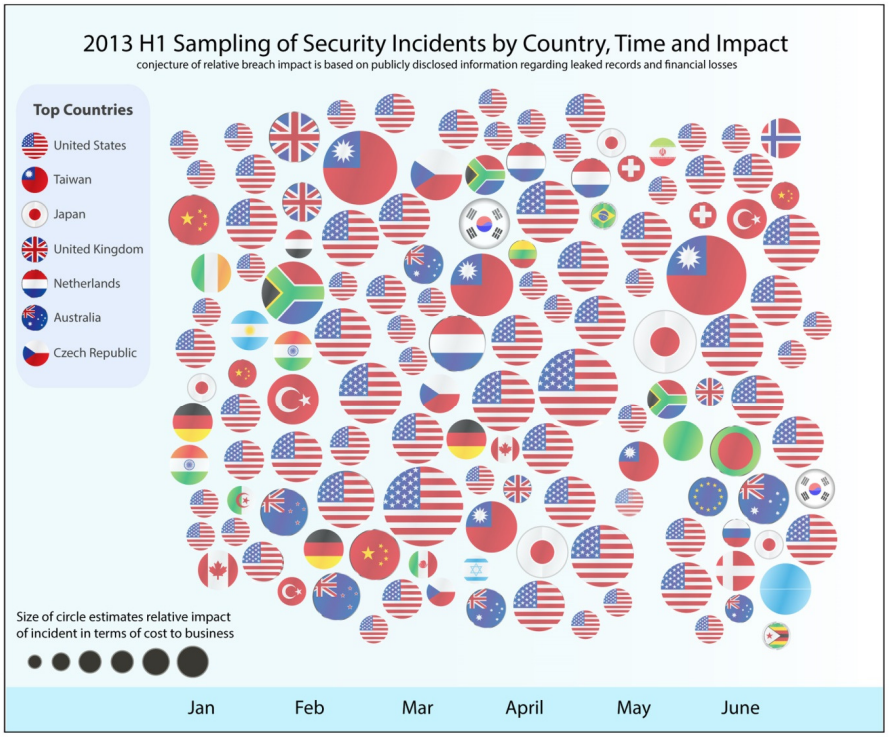
Source: IBM X-Force® Research 2011 Trend and Risk Report

2012: Die Anzahl der Einbrüche explodiert!



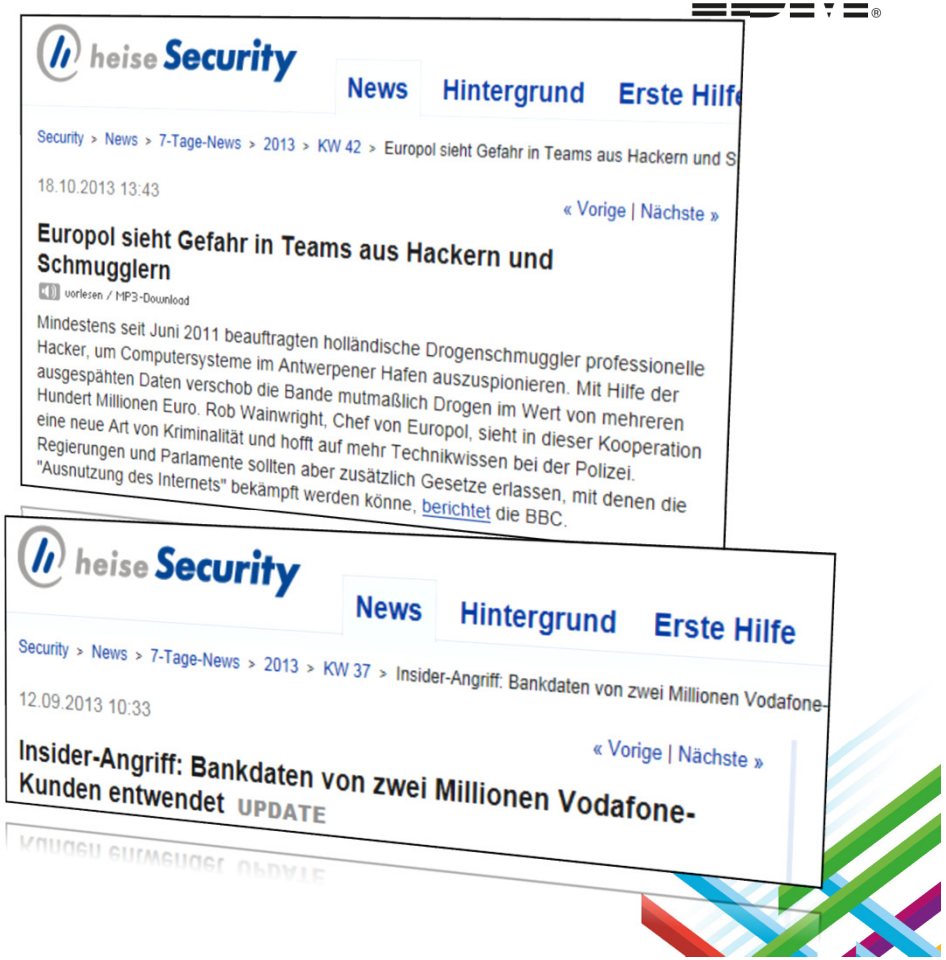
Source: IBM X-Force® Research 2012 Trend and Risk Report

2013: The explosion of breaches continues!



Source: IBM X-Force® Research and Development

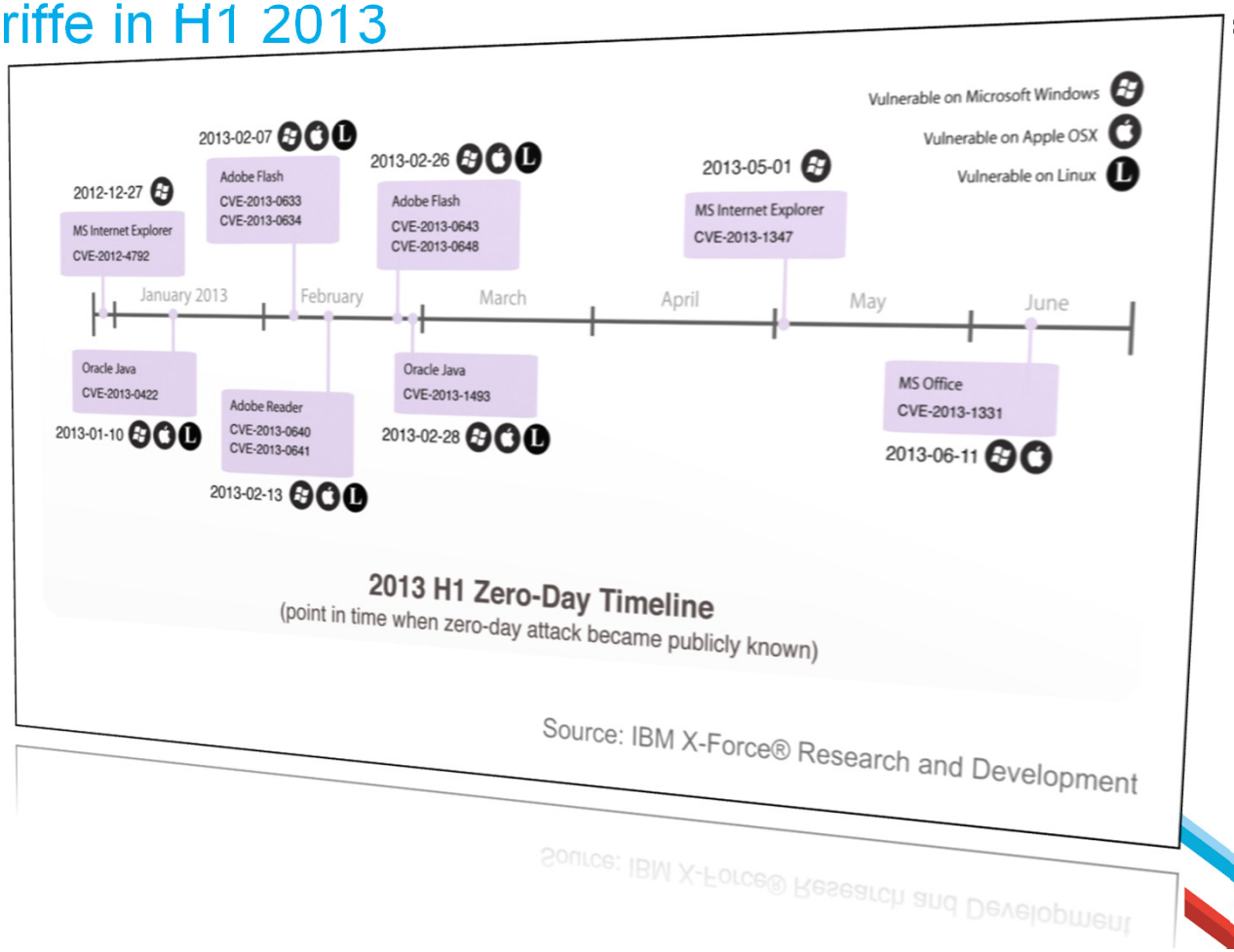
Aktuelle Beispiele



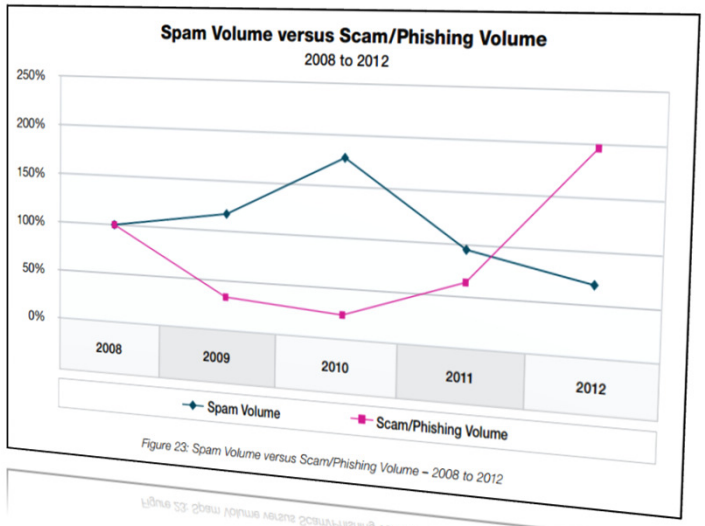
Zero-day Angriffe in H1 2013

Viele Angriffe wurden zunächst als "**Targeted Attacks**" durchgeführt.

Angriffe sind zunehmend **plattform-unabhängig**

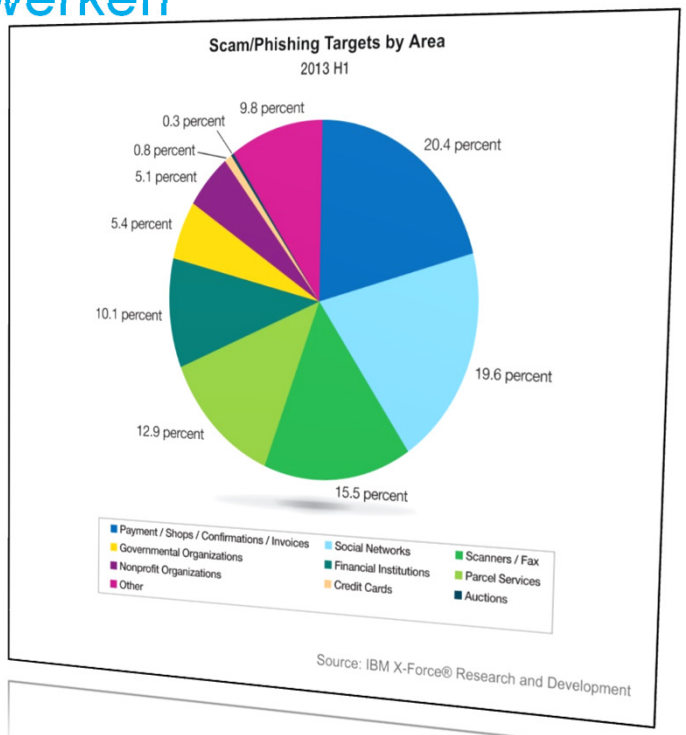


Spear-Phishing „mit“ Sozialen Netzwerken



Spam Volumen ist rückläufig, aber

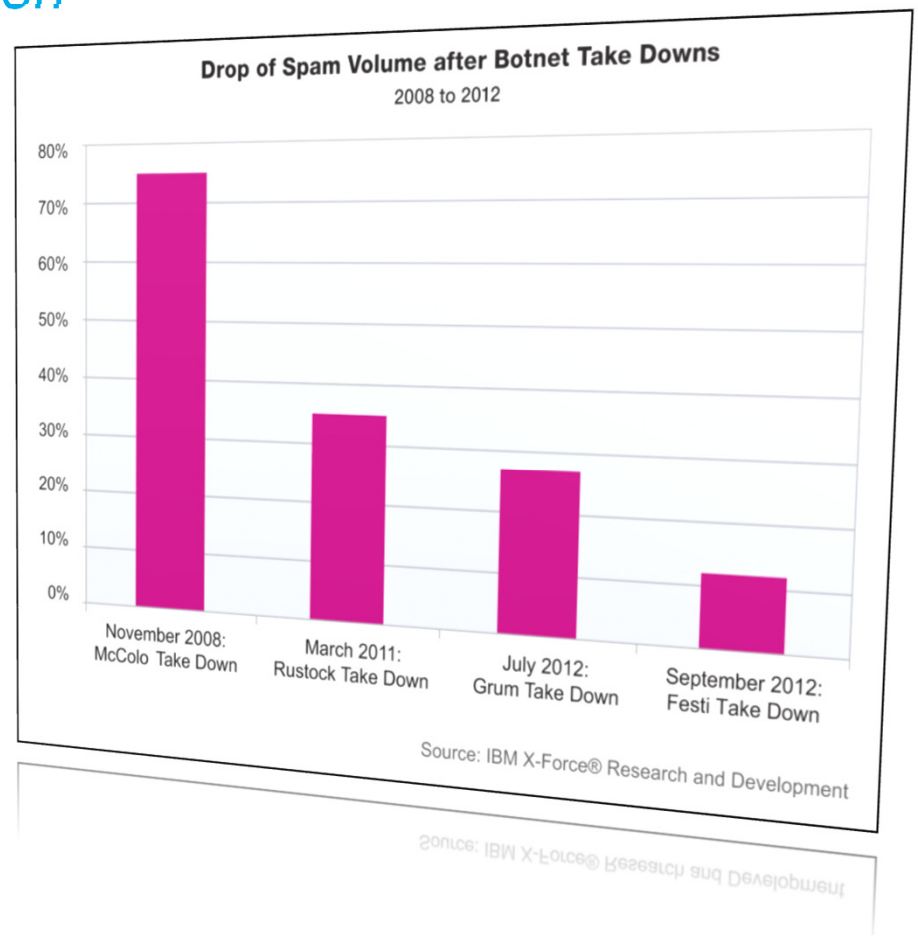
Spams mit bösartigen Attachments steigen an!



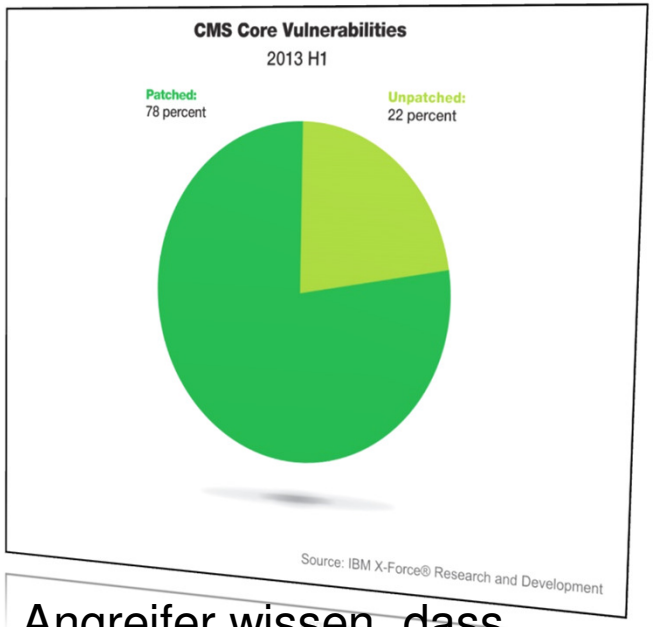
Scammers rotieren ihr “Karusell der Ziele”

Robustheit von Botnetzen

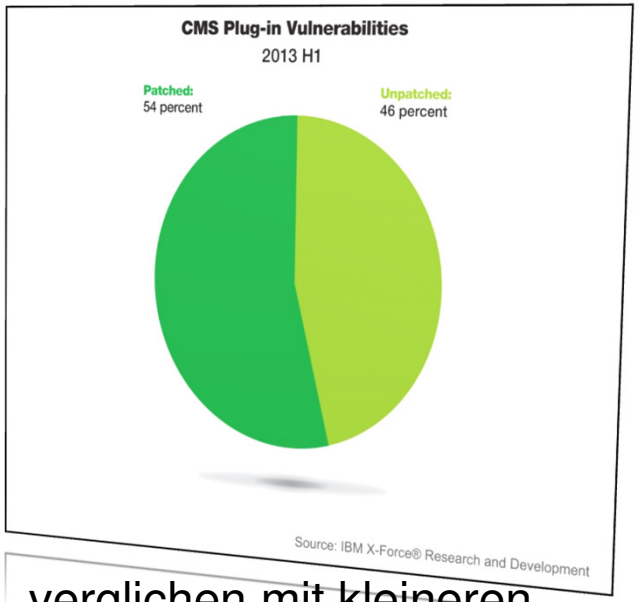
Wenn C&C-Server von Botnetzen ausgeschaltet werden, wird die Funktionalität schneller als jemals zuvor kompensiert.



Content Management Systeme



Angreifer wissen, dass CMS-Hersteller besser patchen

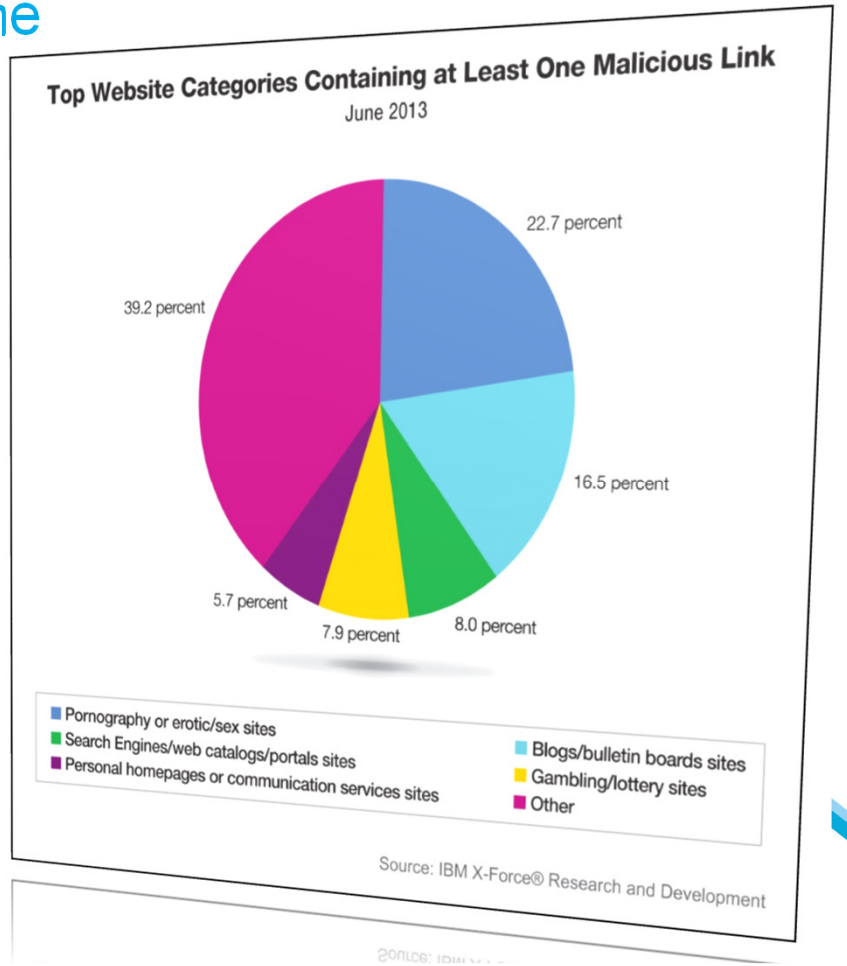


… verglichen mit kleineren Herstellern und Einzel-Entwicklern von Add-Ons und Plug-Ins

Links auf Schad-Programme

Vorsicht!

beim Besuch von „seriösen“ Webseiten

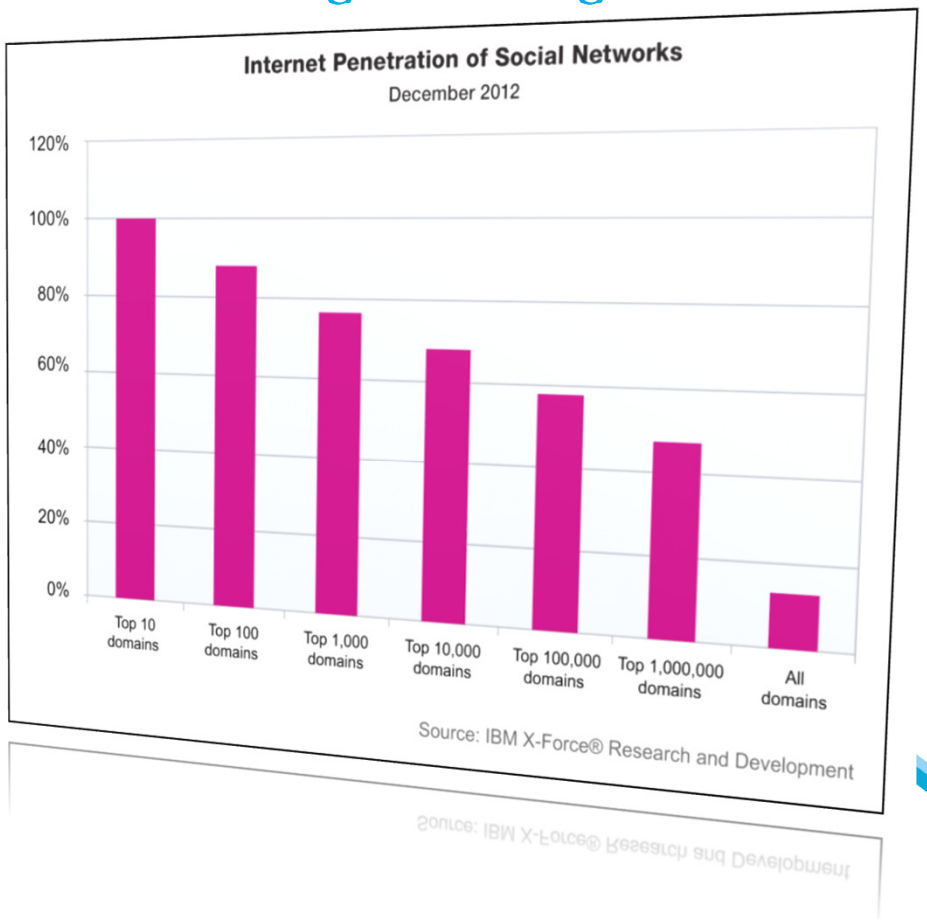


Soziale Netzwerke und Informationsgewinnung

50%

aller Webseiten haben Verbindungen zu Sozialen Netzwerken

Moderne Spear-Phishings scheinen von Freunden oder Kollegen zu kommen



Einfluss sozialer Netze auf die Börse

60 Zeichen kosten den U.S. Aktienhandel **200.000.000.000 $** - ja, 200 Mrd.

Durch nur **einen Tweet**

Bleiben Sie mit IBM X-Force Research and Development in Kontakt

Security Intelligence Blog

http://securityintelligence.com/

Download X-Force security trend & risk reports

http://www.ibm.com/security/xforce/

Subscribe to X-Force alerts at http://iss.net/rss.php or X-Force Security Insights blog at http://www.ibm.com/blogs/xforce

Follow us at #ibmsecurity and #ibmxforce

Thank You!