Verschiebung der Bedrohungslage Cloud-basierte Malwareabwehr

aktuelle Entwicklungen – notwendige Änderungen im Sicherheitsmanagement

Matthias Jänichen
perComp-Verlag Hamburg

perComp Computer clever schützen

perComp-Verlag

- gegründet 1989 als Verlag für technische Dokumentation
- Gründungsmitglied des EICAR e.V. und CARO
- enge Zusammenarbeit mit dem Virus-Test-Center der Uni Hamburg
- heute Distributor, Systemhaus und Fachhändler für IT-Security Lösungen
- einzigartige Level-3-Hotline mit direktem Zugriff auf Hersteller-Ressourcen
- perComp betreut ca. 1.300 Kunden mit über 170.000 Endanwendern
- darunter Einzelanwender, aber auch Kunden mit 20.000 Arbeitsplätzen
- Ganzheitliche Betreuung durch
  - Konzeption
  - Rollout
  - Support
  - Schulung
  - Auditing


htc

perComp Computer clever schützen

Security Thread Forecast 2010

Here are **F-Secure's predictions for 2010** based on this year's threat analysis.

- **Windows 7 will gain market share** during 2010. **Windows XP will drop** below 50% market share overall and will thus reduce the amount of "low hanging fruit." This will **improve Internet security** in affluent countries and it will perhaps begin to create malware ghettos in less affluent countries as cyber-criminals concentrate their efforts on the remaining installed base of Windows XP. Whether attackers continue to focus on Microsoft Windows alone or whether they diversify to include OSX and mobile platforms remains to be seen.
- Real-time support in search engines such as Google and Bing will affect the frequency and manner of **Search Engine Optimization (SEO) attacks**.
- The **2010 FIFA World Cup** (soccer for those of you in the USA) **will generate** a good number of related trojans, fake ticket shops, spam, online shop hacking, and DDoS **attacks.** There could already be SEO attacks months before the matches actually take place in June. South Africa's mobile phone networks will be a hotbed of activity during the games.

Security Thread Forecast 2010

- Web search results leading to **"location based attacks"** using geo-location IP address techniques will increase. They will be localized in terms of language, current news events, and even regional banks that they target. ✓
- There will be more attacks against online banks with **tailor-made trojans**. ✓
- There will be more **iPhone attacks**, possibly also proof-of-concept attacks on **Android and Maemo**. We could also see a 0-day vulnerability used in a large scale exploit.
- **More** snowshoe **spamming**.
- At least **one large-scale DDoS attack** against a nation-state is likely.
- We may see a large-scale internal attack against a target such as Google Wave.
- There will be more **attacks on social networks** such as Facebook, Twitter, Myspace, LinkedIn, etc. Facebook has now reached 350 million accounts and its growth doesn't yet show signs of slowing. This concentration of people and data is a very tempting target for cyber-criminals to exploit. ✓

Security Thread Forecast 2010

- As Internet search engines and social networking sites work towards "social search results", we'll see **black hat social search optimization attacks**.
- As more people connect via mobile networks, the amount of traffic and activity such as banking, gaming, and social networking increases in step. With mobile banking and in-game purchasing gaining popularity, the financial motivation becomes stronger to spy on such transactions. Integrated social networking applications are also driving mobile phones users to be "always connected." **Cyber-criminals will use social engineering to exploit this trend**.
- **Attacks related to online games will continue**. Such sites and games are particularly popular in the Asia-Pacific region. Not enough focus is put on securing them and the problem will be further fueled by the fact that many users are younger and therefore more vulnerable to experienced cyber-criminals.
- There will be significant **data base compromises** that lead to tailored attacks. Cyber-criminals now have the resources to analyze, plan, and carry out mass-targeted attacks.

2008

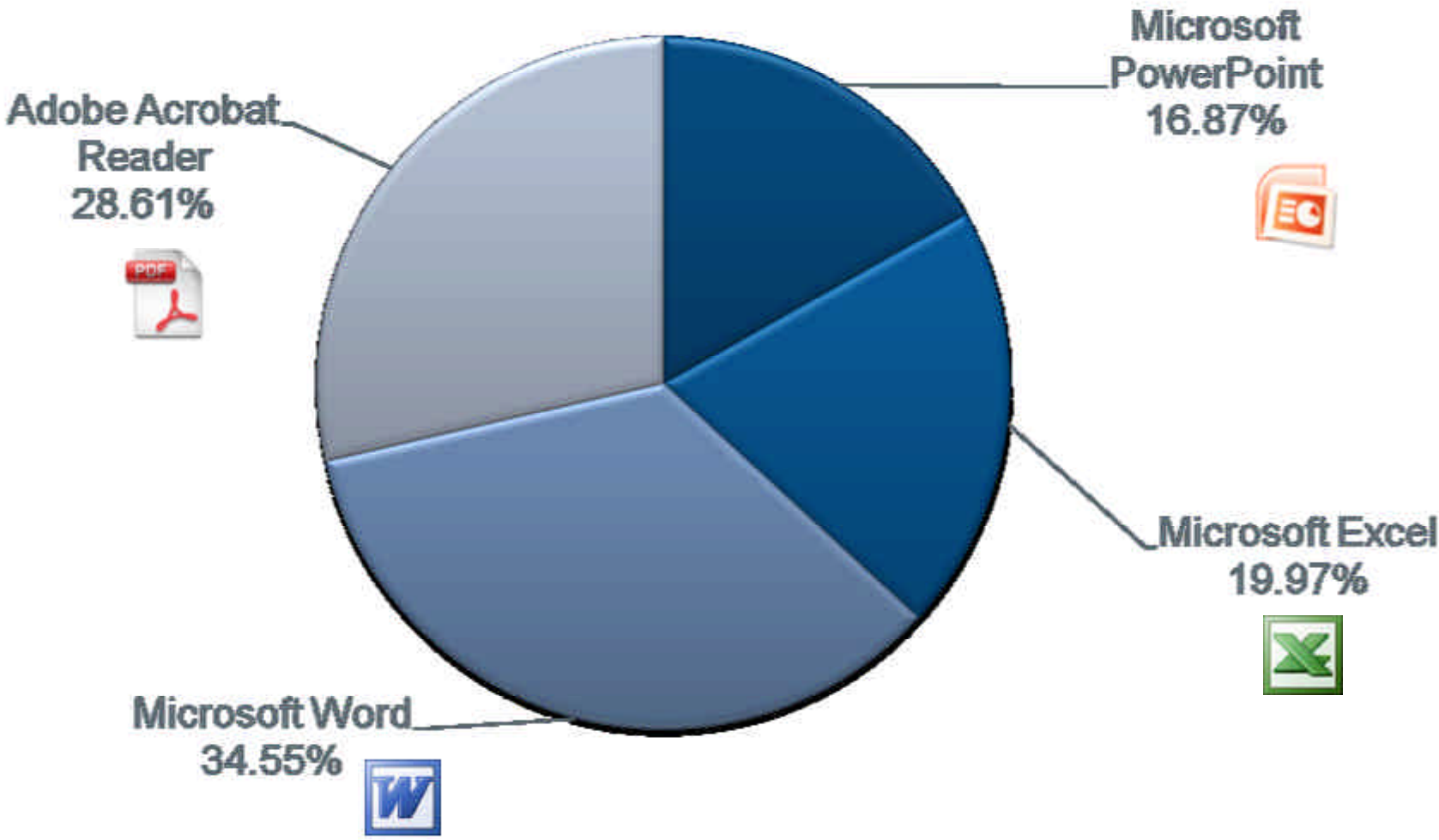
1968 attacks


2009
2195 attacks

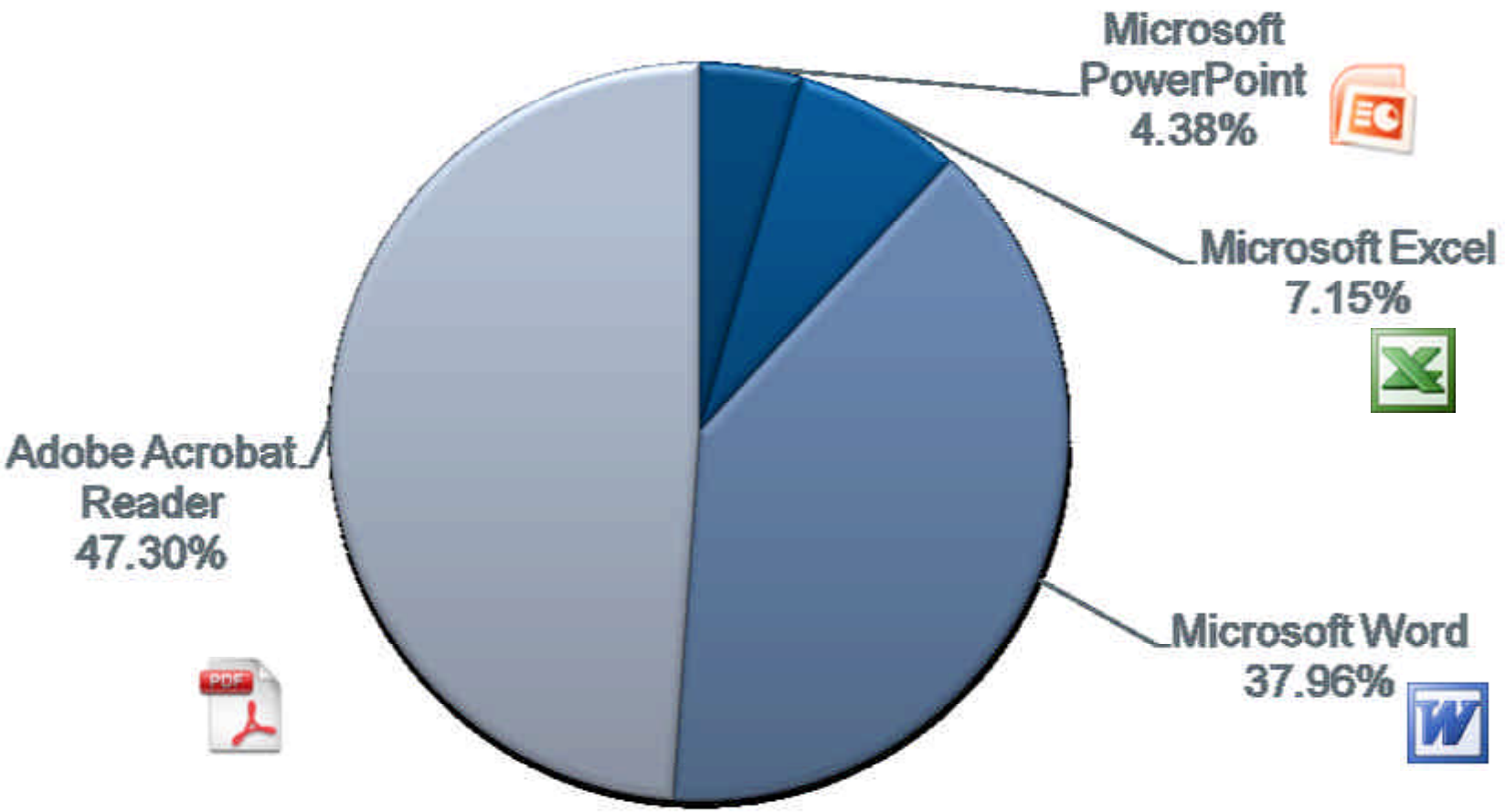

2010 (to date)
895 attacks
DC
AMPERES
4

Operation Aurora

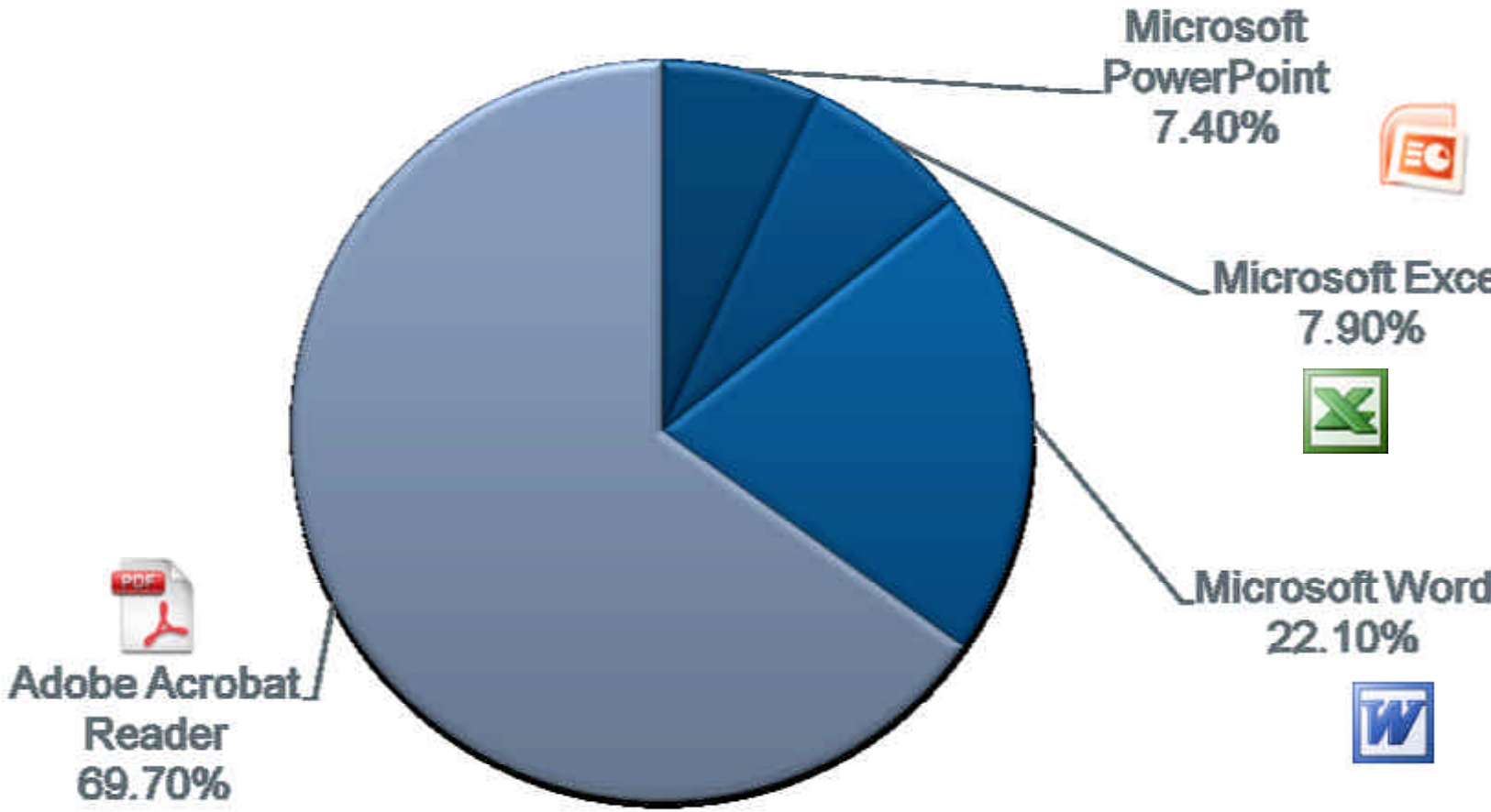
Targeted attacks 2008



Targeted attacks 2009



Targeted attacks 2010



AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The typical day in anti-malware industry

- In 2005
  - 114 Signature- and Program-Updates released per day
    - Thats over 3.400 per month and over 40.000 in a year
  - 1,2 GB of Updates downloaded by AV-Test per day
    - Thats 36 GB per month and about 400 GB in a year
  - Over 360 new unique samples received
    - Thats over 10.000 per month and nearly 130.000 in a year

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The typical day in anti-malware industry

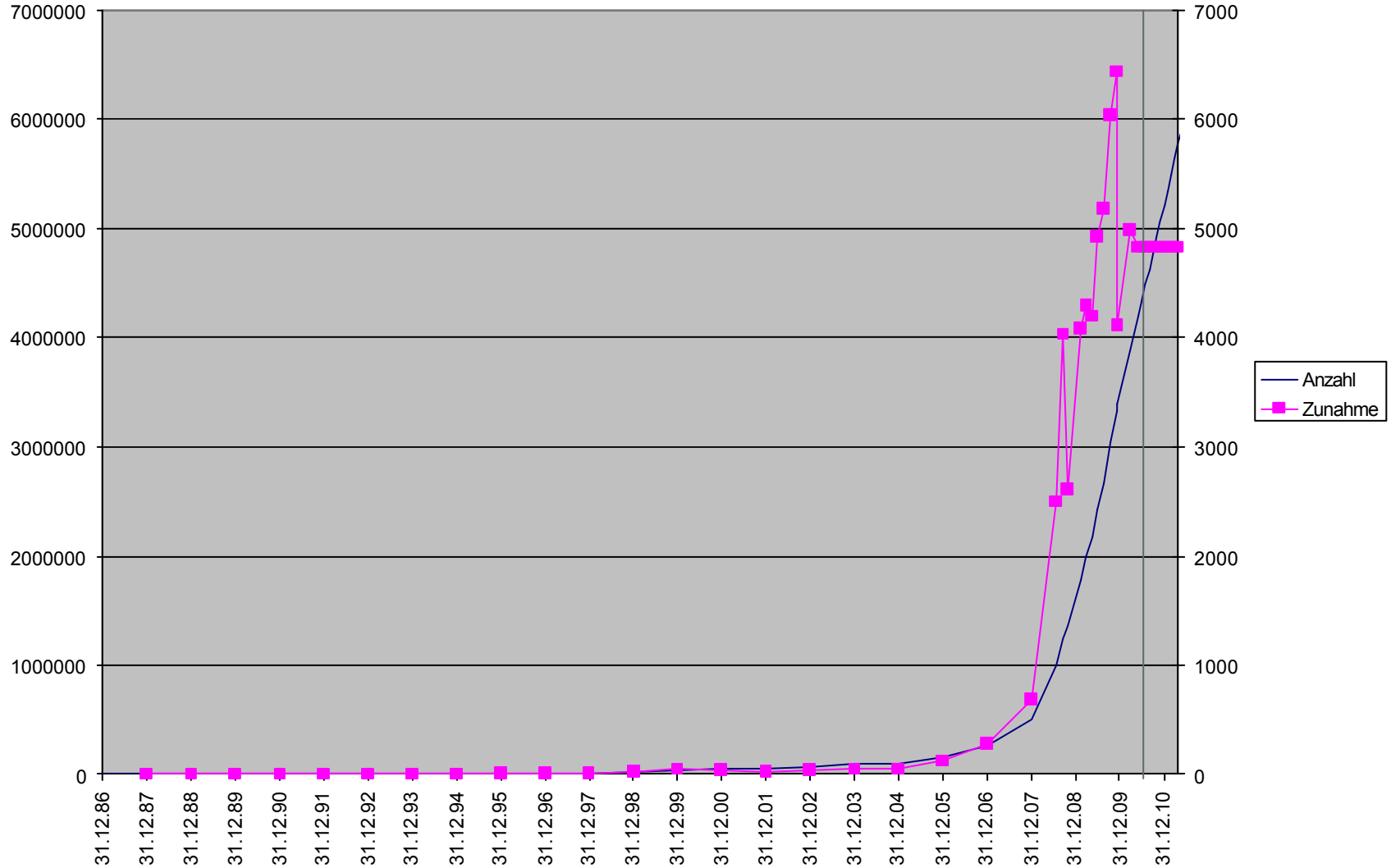
- In 2010
  - 574 Signature- and Program-Updates released per day
    - Thats over 17.000 per month and over 200.000 in a year
  - 17 GB of Updates downloaded by AV-Test per day
    - Thats over 510 GB per month and over 6120 GB in a year
  - Over 50.000 new unique samples received
    - Thats over 1.500.000 per month and nearly 20.000.000 in a year

Statistiken der Hersteller

- 100.000 Einsendungen pro Tag
- 50.000 Einsendungen sind Malware
- 40.000 „Unique Samples“ (80%)
- 5.500 neue Einträge

  7.200 neue Einträge am 09.06.2010
- 1.600 generische Signaturen

Anzahl der Records in den Datenbanken



Entwicklung der AV-Technologie

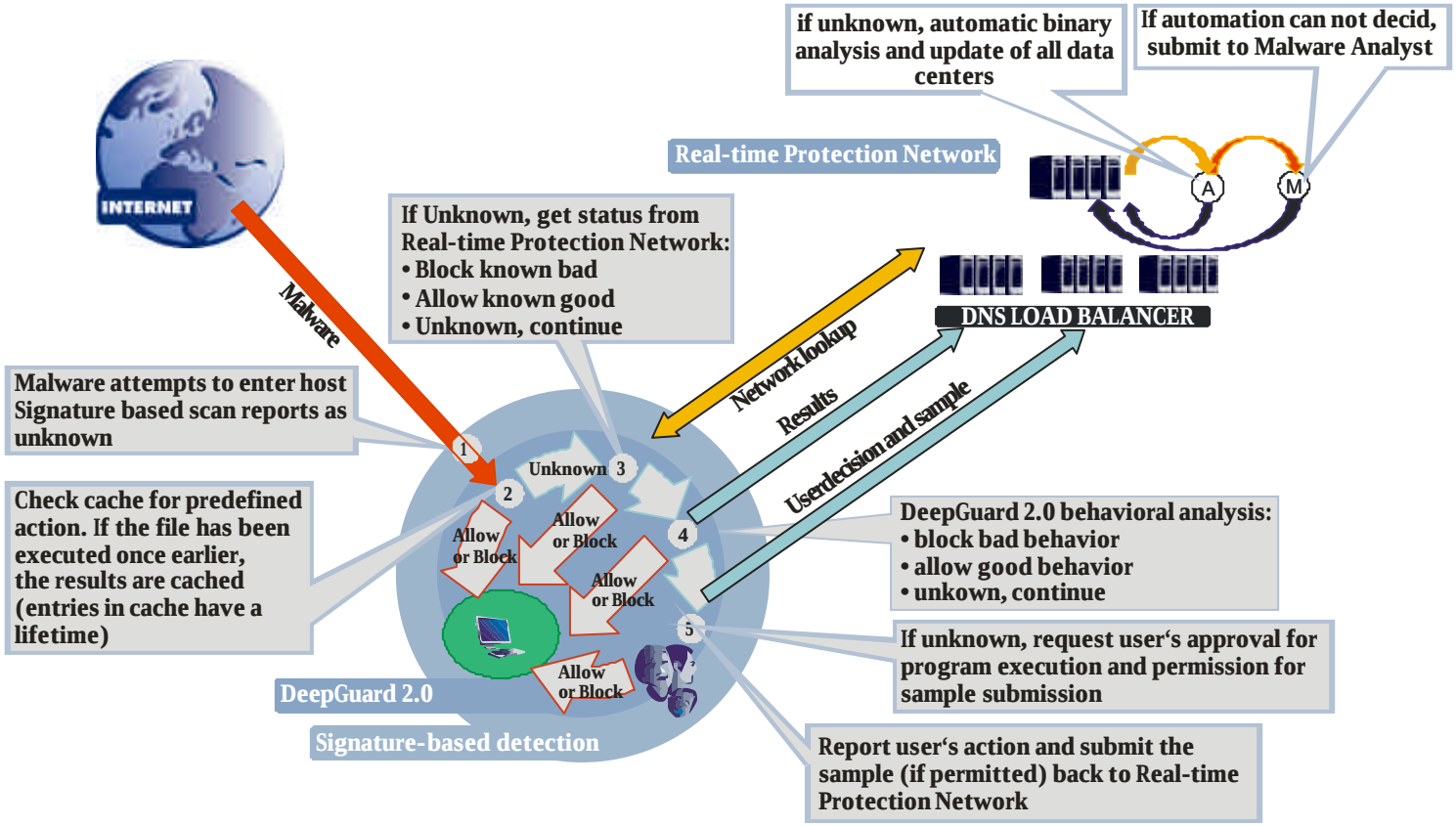
- **Angreifer**
- Dateiinfektoren (Viren)
- Mutationen
- Codeverschränkung
- Verschlüsselung
- Würmer
- Trojaner
- Kombinationen
- Angriffe auf das Betriebssystem
- Angriffe auf Anwendungen
- Angriffe auf Plugins

- **Abwehr**
- Zeichenketten
- Metacode
- Stepping
- Entschlüsselung
- lokale Firewalls
- Sandboxen
- Heuristiken
- Windows Update
- ?
- ?
- Verhaltens-Überwachung

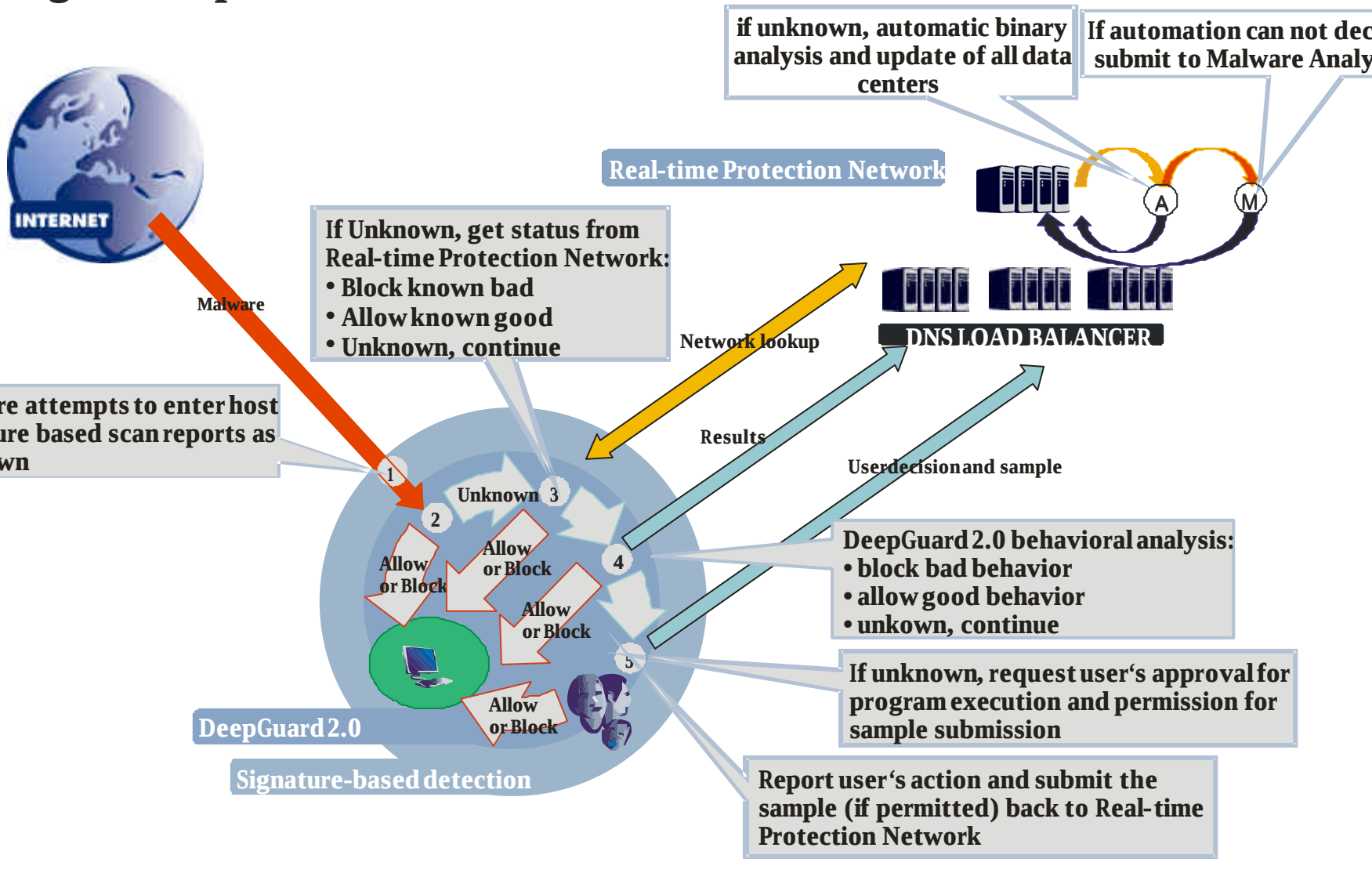
Cloud-basierte Erkennung

Cloud-basierte Erkennung

DeepGuard 2.0
Realtime Protection Network
Enabling fastest protection in the online world



eepGuard 2.0
ealtime Protection Network
nabling fastest protection in the online world



Vorteile der Cloud-basierten Erkennung

- Die **Signatur-Dateien** können durch generische Erkennungen wesentlich **kleiner** werden, unklare Ergebnisse können von der Cloud bestätigt werden. Dies führt zu **besserer Performance** und **weniger Speicherverbrauch**.
- **Signaturen** für Malware **stehen** jedem Anwender **sofort** nach der Analyse **zur Verfügung**. Er braucht nicht mehr auf das nächste Update zu warten.
- **Produktionsausfälle** durch False Positives in lokalen Applikationen **werden eliminiert**, da der Administrator die wichtigen Anwendungen selbst freigeben kann. FPs von Dateien, die aus dem Internet stammen, sind möglich und ärgerlich, aber stellen i.d.R. kein Problem dar.
- Rollbacks im Falle von False Positives waren schon immer problematisch, denn sie betreffen nicht nur die eine (falsche) Erkennung, sondern alle zuletzt zugefügten Signaturen. **Über die Cloud können False Positives schneller behoben werden** als durch ein Rollback der Signaturen. Das Sicherheitsniveau bleibt erhalten.

Fragen zur Cloud-basierten Erkennung

- Testmöglichkeit für Signaturen entfällt.
  - Die Cloud verändert sich ständig, daher ist ein Test nicht möglich. Auch die verhaltensbasierten Methoden können nicht sinnvoll überprüft werden.
- Datenschutz?
  - Welche Daten werden an den Hersteller übertragen? Sind diese zu schützen?
- Ist der Zugriff der Clients ins Internet möglich?
  - Die Antworten der Cloud müssen den PC schnell und ungefiltert erreichen.
- Wie hoch ist die zusätzliche Netzwerkbelastung?
  - 52 MB von 1.500 PCs in 24 h (0.05% der gesamten Netzlast am Gateway)
- Soll das Konzept der Cloud auch nach außen gelten?
  - Die Cloud lebt von aber auch nur durch die Gemeinschaft!
- Ist der Betrieb eines internen Cloud-Servers sinnvoll?
  - Nein. Durch den Betrieb eines internen Cloud-Servers entfällt die Aktualität. Weder neue noch korrigierte Erkennungen stehen zur Verfügung. Ein Proxy würde die Anfragen nur verzögern, denn 90% der Anfragen sind individuell.

Computer clever schützen

www. perComp .de

Matthias Jänichen
Holzmühlenstraße 84
22041 Hamburg
Tel.: 040 / 696 28 16-0
E-Mail: info@percomp.de