Federal Office
for Information Security

# Fighting targeted attacks on Government Networks

Robert P Krawczyk

DIMVA / 2013-07-19

# Protecting Government Networks

The Task

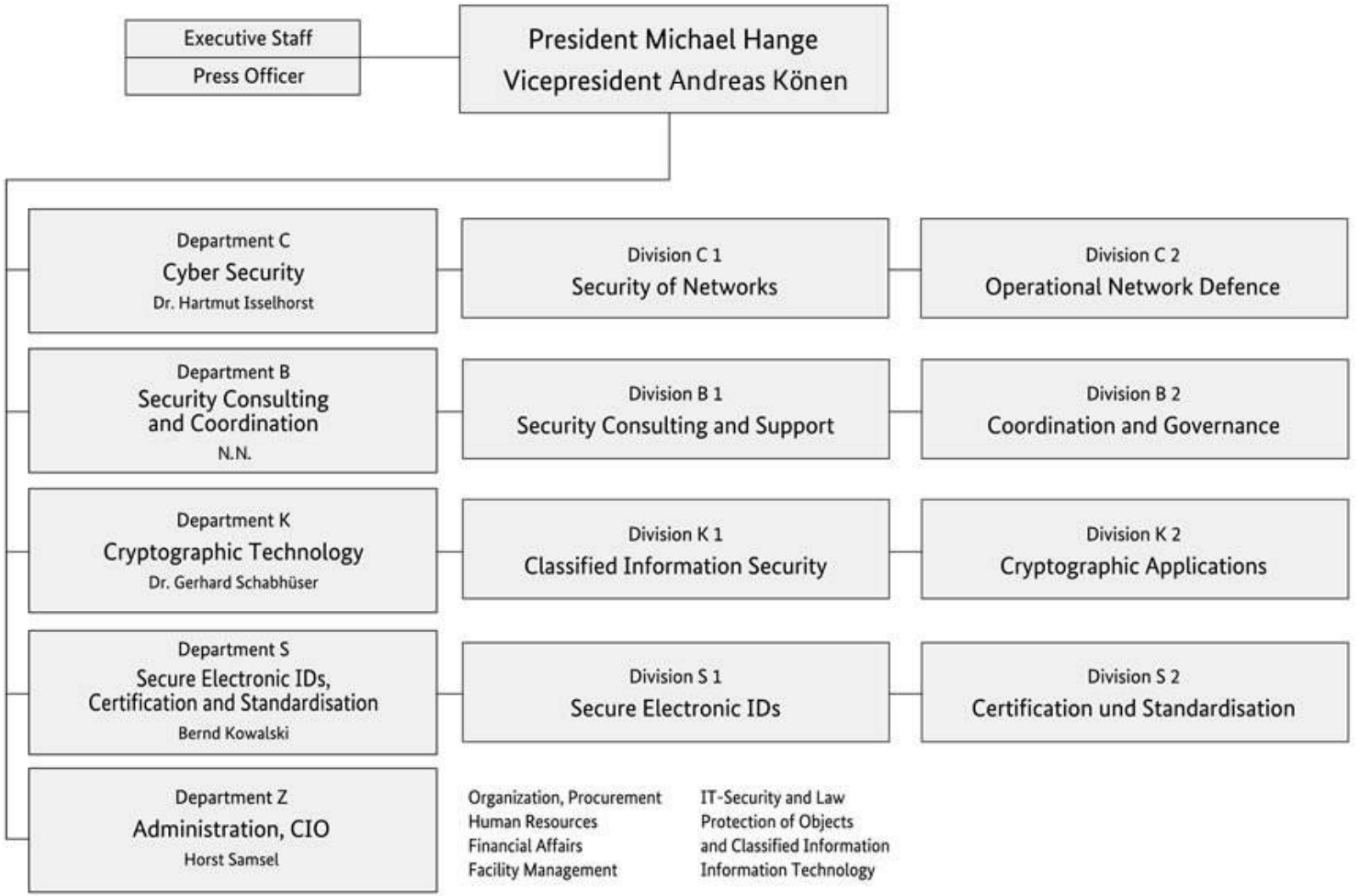
Successes

Challenges

# Who are we?

- Established on the 17th December 1990
- Promotes IT security in Germany
- Provides information on risks and threats
- IT security testing and assessment of IT systems
- BSI advises
  - agencies
  - manufacturers
  - distributors
  - users of information technology
- Analyses development and trends in IT
- BSI standards, IT-Grundschutz Catalogues

# Organisation



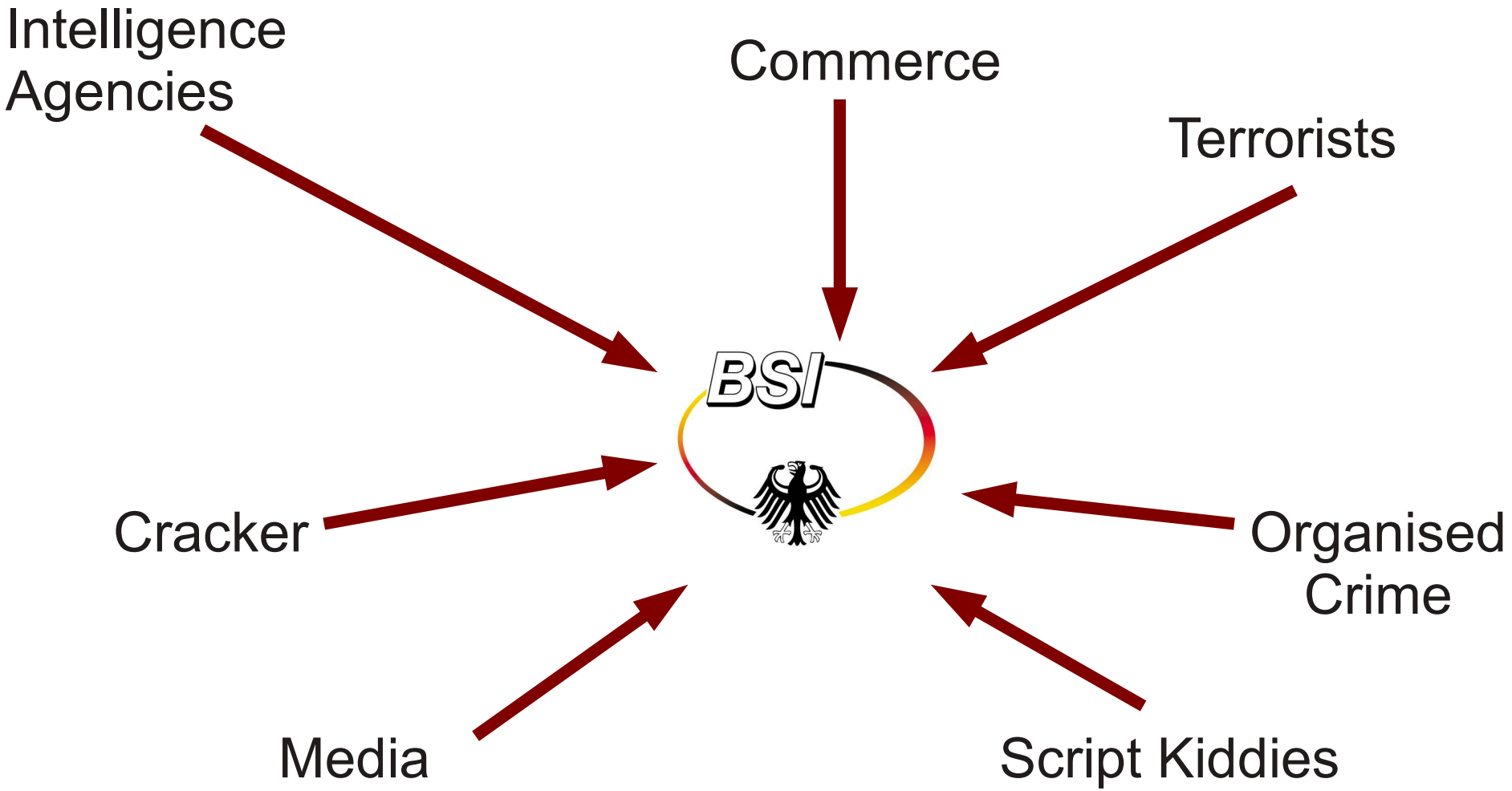
# In the media


BSI warnt vor unseriöser E-Mail-Werbung
Bonn, 14. August 2006. Vor aktuellen, unerwünschten E-Mails mit der Absenderangabe "Germany Online Consult" bzw. "Consult-Online-AG" warnt das Bundesamt für Sicherheit in der I
Der angebliche Versender von E-Mail-Werbung verspricht die Überweisu
unterschriebenes Formular mit Name, Adresse, Bankverbindung ausgefü
zugeschickt wird. Eine Überweisung auf das angegebene Konto solle un
- Bürger-CERT-Newsletter informiert über Sicherheitslücken
Bonn, 31. August 2006. Über neue Sicherheitslücken und
Bürger-CERT-Newsletter "Sicher Informiert".
In seiner aktuellen Ausgabe warnt der 14-tägliche Information
Satellitentelefonummern, vor gefährlichen Phishing-Mails, die s
Meldung vom 02.05.2005 18:
Sober-Wurm tarnt sich
-Ticket-Auslosung
news 30.05.2005 17:05
<< Vorige | Nächste >>
Trojaner spionierte israelische Unternehmen aus
Ein umfangreicher Fall von Industriespion
einem eigens entwickelten Trojaner wurd
Konkurrenten belauscht. Zu den Auftragg
unter anderem die Mobilfunk-Provider C
Mineralwasserabfüller Tami-4
ZDFheute.de computer
"IT-Sicherheit kostet Geld"
Verfassungsschutz-Vize-Chef Remberg
über chinesische Hacker-Angriffe
Bundesamt
für
Verfassungsschutz
heise Security
Meldung vom 03.07.2007 12:07
Gezielte Trojaner-Angriffe auf PCs von Führungskräften
Das obere Management und einzelne Führungskräfte sind ins Visier der Cyber-Kriminellen gerückt, schreibt der Anbieter von Sicherheitsdienstleistungen MessageLabs in seinem Intelligence Report für Juni 2007. So seien Mails mit bösartigen Word-Dokumenten im Anhang besonders zielgerichtet gewesen, die den richtigen Namen und Jobtitel des Empfängers enthielten. Mittels Trojaner wollen die Wirtschaftsspione wichtige Geschäftsinformationen auf dem Unternehmens-PC ausspionieren.
Wirtschaftsspionage
in Baden-Württemberg und Bayern
DATEN-FAKTEN-HINTERGRÜNDE
Fakten
Daten
Hintergründe
Terrorists Turn to the Web as
Base of Operations
By Steve Coll and Susan B. Glasser
Washington Post Staff Writers
Terror on the Internet
PalestineWay.com
DER SPIEGEL
DIE GELBEN SPIONE
Wie China deutsche Technologie ausspäht
Computer-Spionage!
Chinesen bespitzeln Kanzlerin
Bild am Sonntag
Botnet operation controlled 1.5m PCs
Largest zombie army ever created
Tom Sanders in California, vnunet.com 21 Oct 2005
A recently foiled botnet operation has turned out to be 15 times larger th
initially thought.
On further investigation, authorities found that the operation had put ab
million computers and servers under its control. The crime ring was thoug
created a botnet of 100,000 systems, which they claimed was the largest
detected.
Viruses, spyware cost users $7.8 billion
Sunday, August 13, 2006
By Kim Hart, The Washington Post
Consumers paid as much $7.8 billion over two years to repair or replace computers that got infected with viruses and spyware, a Consumer Reports survey found.

# Defining the Problem

- Attacks by different entities
- Virus scanners cannot cope anymore
  - Number of viruses is increasing rapidly
  - Signatures require a lot of work
  - Sometimes virus scanners are the source of problems
- Use of off-the-shelf/standardised operating systems, applications, and other components makes institutions more vulnerable
- Security is usually not considered when new processes are implemented
- Attitude: Security does not pay!
- Hindsight is a wonderful thing...

# Attackers


Intelligence Agencies
Commerce
Terrorists
BSI
Cracker
Organised Crime
Media
Script Kiddies

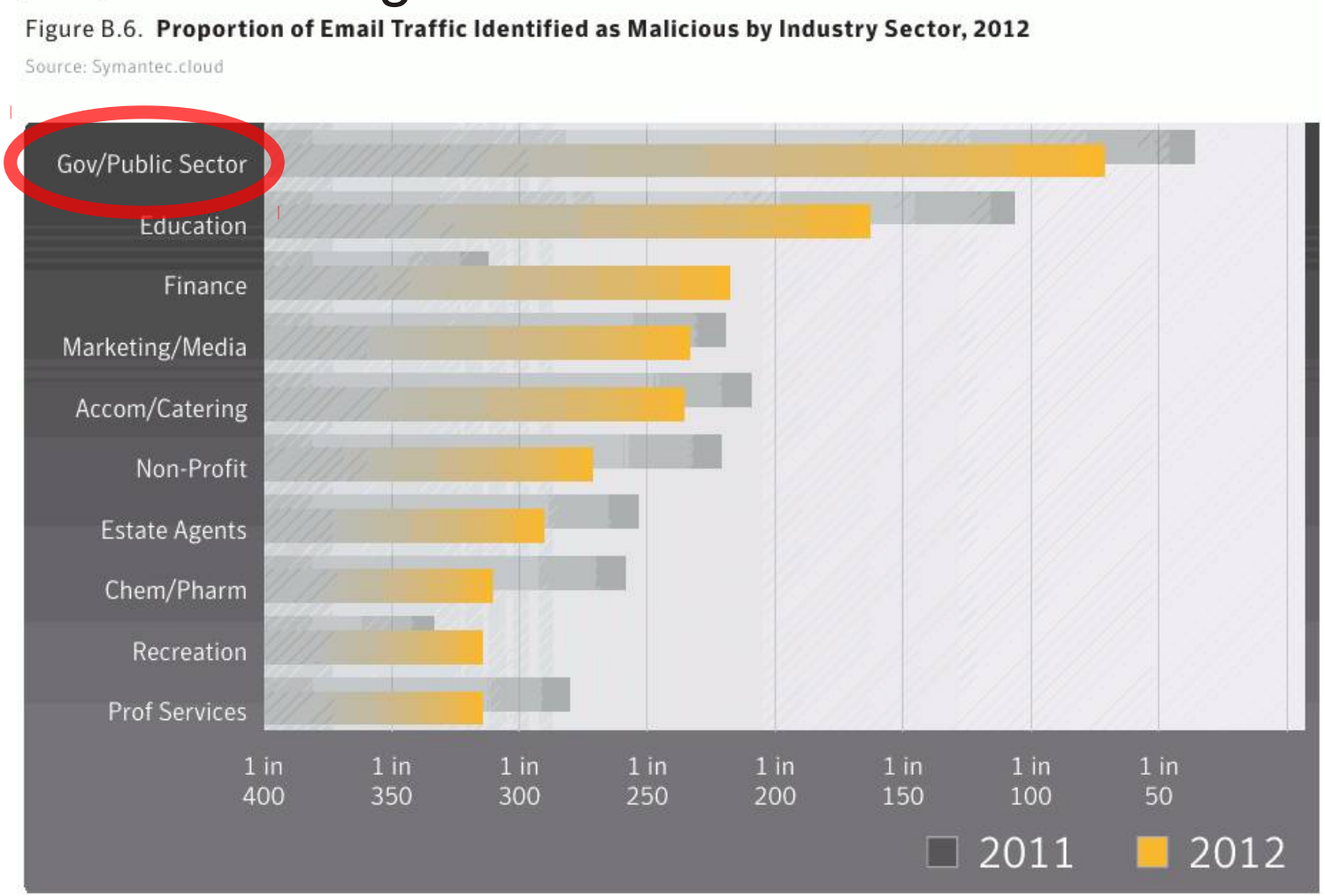
# And... sometimes your own employees

- 39 % believe in-house IT will protect them from Spyware and Phishing
- In Germany: 76 % of employees will open suspicious emails or web pages at work
  - security software is installed at work
  - it is much too dangerous to do this at home...
- 29 % just do not care because the computer is the company's property

Quelle: [TrM] http://de.trendmicro-europe.com/enterprise/about_us/spresse.php?id=183

# Malicious Emails

- Organisations in the Government and Public sector were subjected to the highest level of email attacks



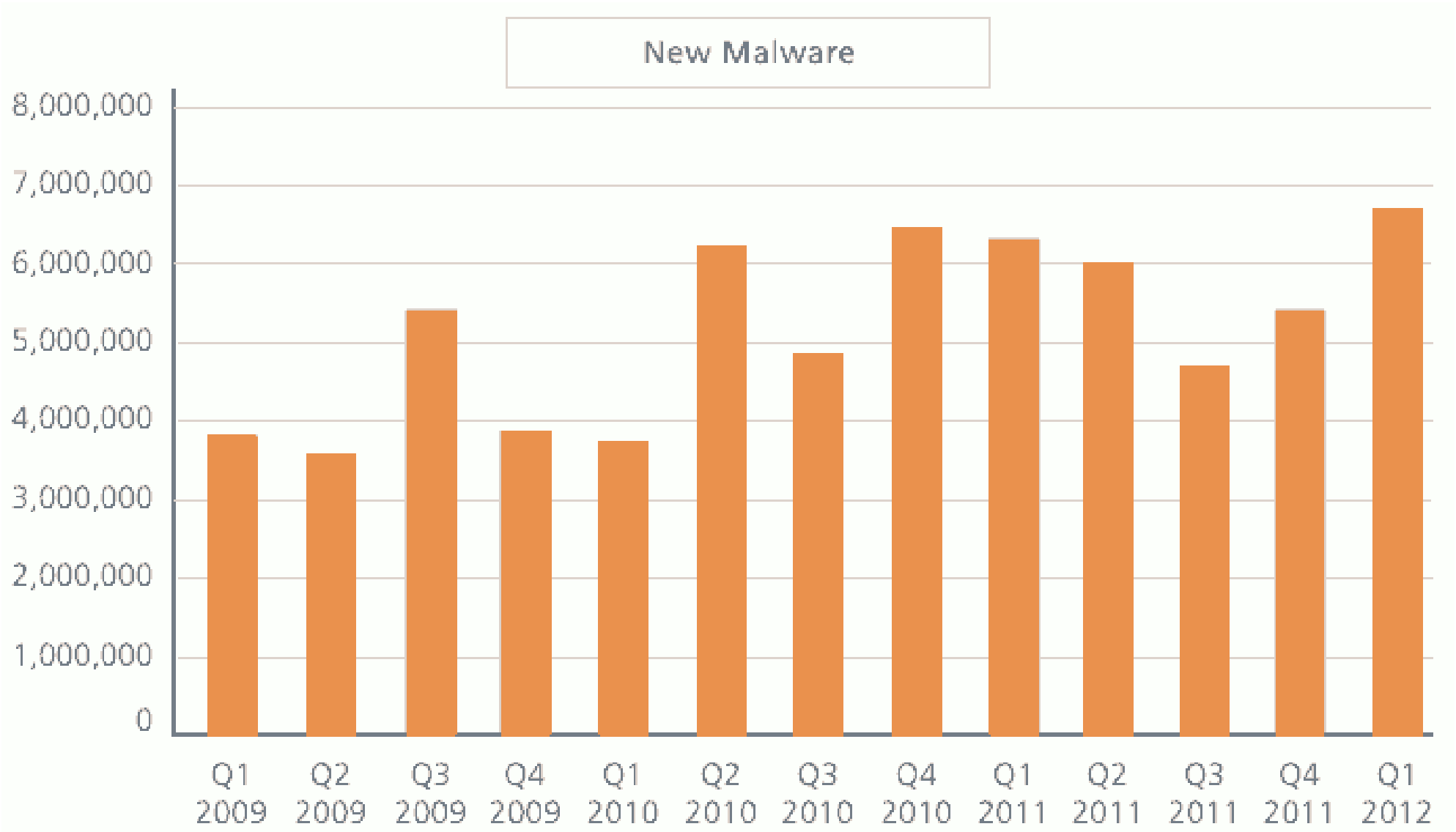
# File Formats

Figure B.13. **Breakdown of Document Types Being Attached to Targeted Attacks, 2012**

Source: Symantec.cloud

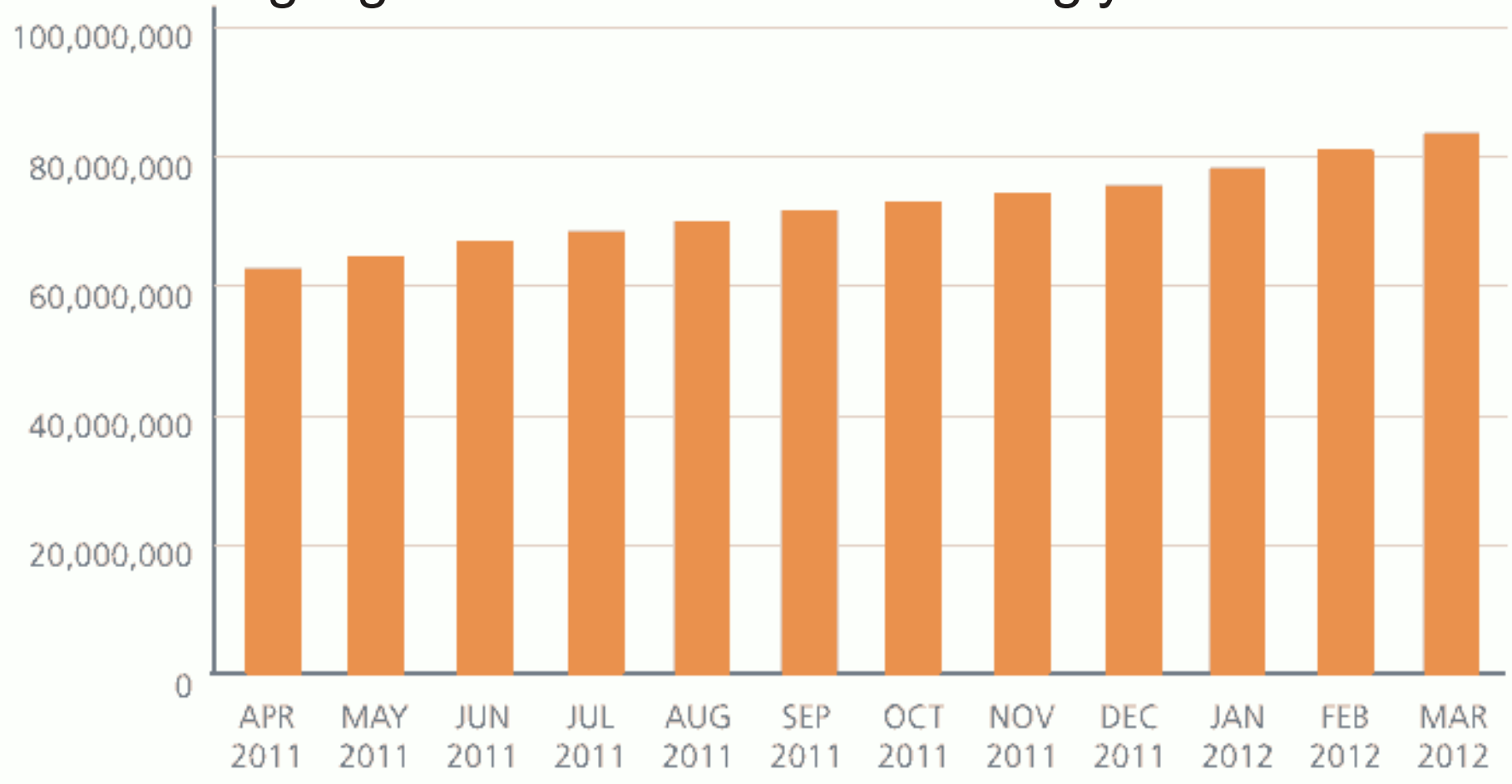
Attackers are still using EXEs?
(Succesfully?)

# Virus Numbers
# McAfee report 2012Q1

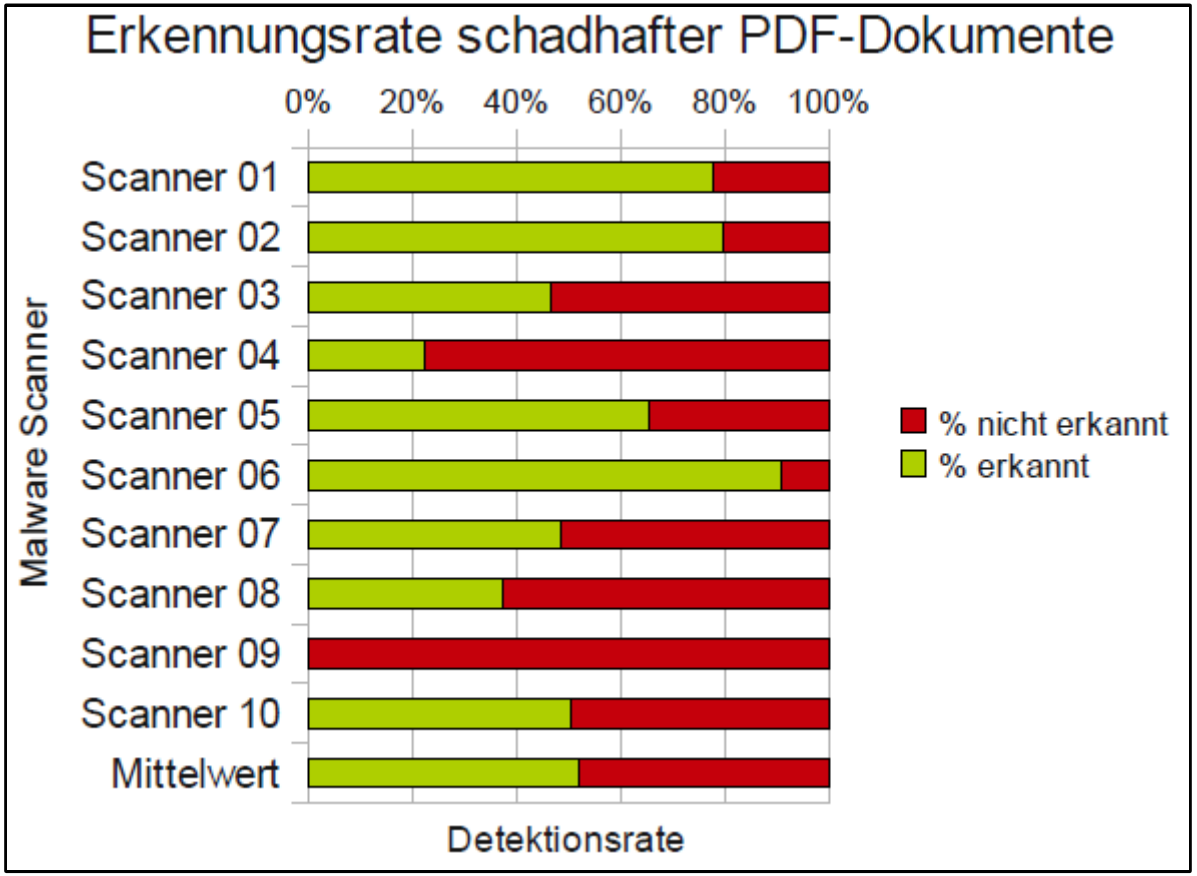


# Virus Numbers
# McAfee report 2012Q1

- Total number ever increasing
- Generating signature becomes increasingly difficult

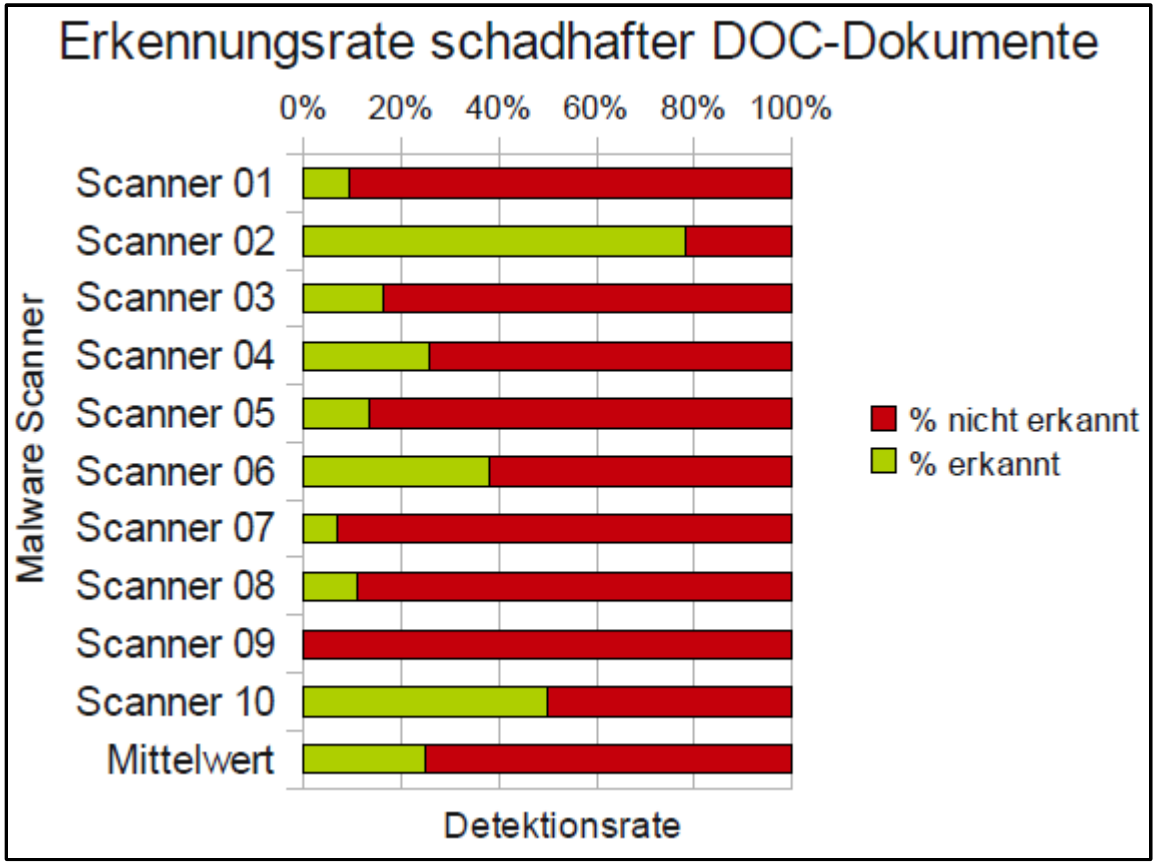


# Detection rate for PDFs




Average: 52%

# Detection rate for DOCs




Average: 25%

# Virus-scanner failures

- Getting signatures is hard
- Only already known threats can be found
  - Oh yeah... heuristics...
- False positives are problematic
- Vendors have difficulties with newest Windows

- Sometimes too eager...

04.06.2013 15:48 « Vorige | Nächste »

**G Data: 2014-Update legt Rechner lahm**

vorlesen / MP3-Download

In der vergangenen Woche hat das Bochumer Sicherheitsunternehmen G Data begonnen, Installationen der 2013-Generation automatisch auf die 2014-Generation zu aktualisieren. Dieser Vorgang geht offenbar nicht immer gut: Leser berichteten heise Security, das Update verlangsame einige Systeme derart, dass sich nicht mehr sinnvoll damit arbeiten lässt. Bisherigen Rückmeldungen zufolge tritt das Problem nur bei 32-Bit-Versi
AntiVirus als au

Zur Linderung d
in den Einstellu
unter "Allgemei
die Option "Lan
aktivieren – dies
deutlich. Ein be
über die System
Vorversion von
darin die Produ
abzuschalten.

Die beste Optio
2014 über die V
zu deinstallierer
Programmreste
eine ausführlich
dann eine saub

G Data konnte
Ursache aber n

March 15th, 2013, 07:40 GMT · By Bogdan Popa

BLOG

**AVG Anti-Virus Breaks Down Windows XP Due to False Positive**

SHARE: Tweet Adjust text size:



ENLARGE - AVG fixed the issue with a definition update

**The popular AVG Anti-Virus software incorrectly flagged a vital Windows system file as Trojan horse, causing a failed boot in case the user opted to remove the "infection."**

# What now?

- We need a new protection mechanism
- As a government institution we are bound by the law in our choice of methods
- Therefore...

# I am The Law

- In 2009 a new law was passed
- § 5 contains specific rights for the BSI to defend the government network
  - *Protokolldatenauswertung*
    - Collecting and analysing data logged by government network infrastructure and systems
  - *Abwehr von Schadprogrammen*
    - Ability to operate a system that detects network-based attacks

# BSIG

- http://www.gesetze-im-internet.de/englisch_bsig/index.html

**Section 5: Protection against harmful software and threats to federal communications technology**

(1) In order to protect federal communications technology against threats, the Federal Office may

1. use automated processes to gather and evaluate protocol data generated by operating federal communications technology as necessary to recognize, contain or remedy disruptions to or problems with federal communications technology or attacks on federal communications technology;

2. use automated processes to evaluate data generated at interfaces of federal communications technology as needed to recognize and protect against harmful software.

# BSIG

(2) Protocol data as referred to in subsection 1 first sentence no. 1 may be stored longer than specified in subsection 1 first sentence no. 1, but no longer than three months, if there are concrete indications that, if suspicion is substantiated under subsection 3 second sentence, these data could be needed to protect against threats arising from the harmful software found or to recognize and protect against other harmful software. Organizational and technical measures shall be used to ensure that data stored on the basis of this subsection are evaluated only using automated processes. The data shall be depersonalized, where this is possible using automated processes. Non-automated evaluation or use of data which allows the identification of the person to whom the data pertain shall be allowed only in accordance with the following subsections. If doing so entails repersonalizing depersonalized data, this process must be ordered by the president of the Federal Office. A record is to be kept of the decision.

# BSIG

(3) Use of personal data beyond the restrictions specified in subsections 1 and 2 shall be permitted only when certain facts substantiate suspicion that

1. they could contain harmful software,
2. they could have been transmitted using harmful software, or
3. they could provide information about harmful software,

and when the data must be processed in order to substantiate or dispel suspicion. If suspicion is substantiated, the further processing of personal data shall be permitted as necessary

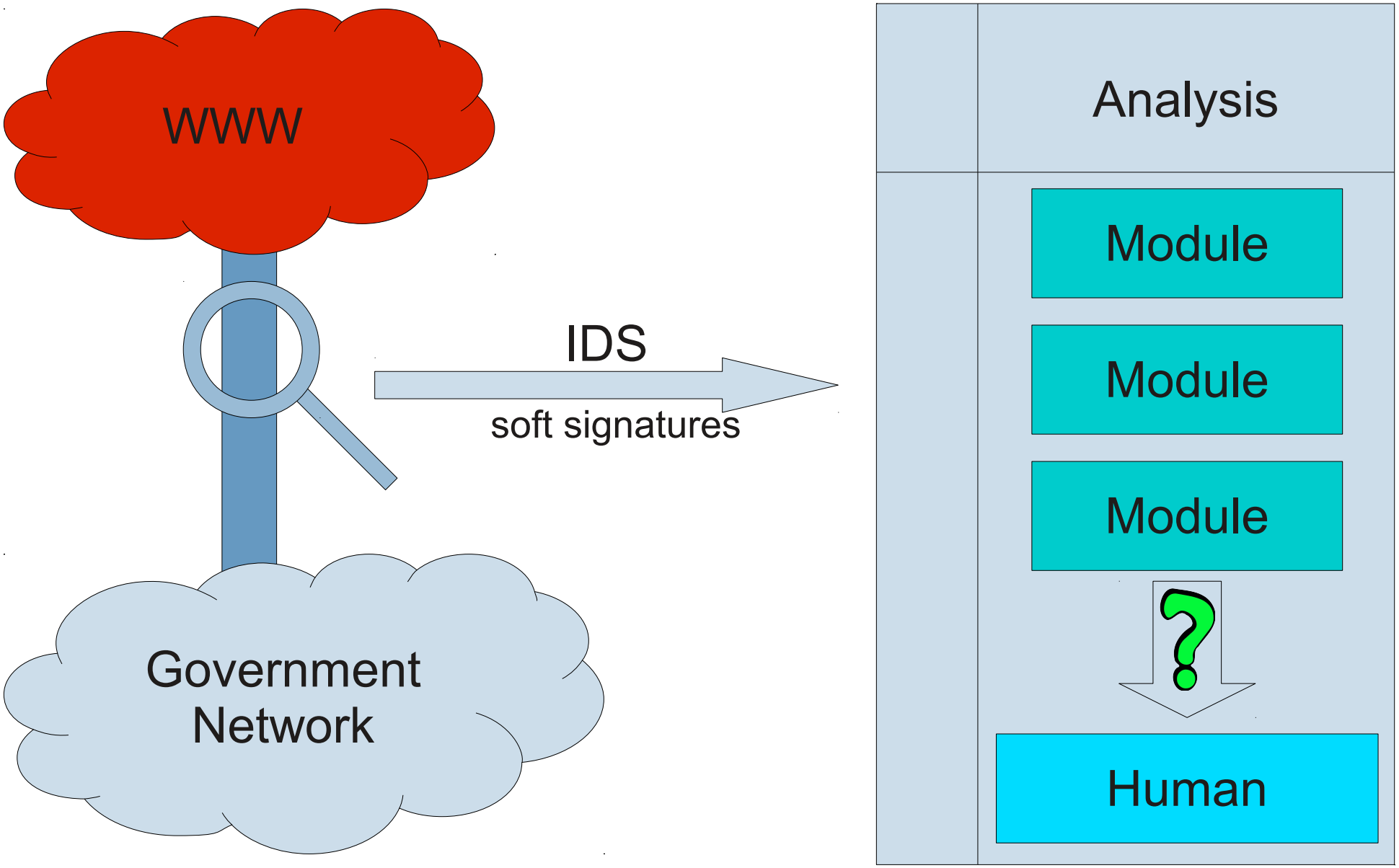
1. to protect against harmful software,
2. to protect against threats arising from the harmful software found, or
3. to recognize and protect against other harmful software.

Harmful software may be removed or disabled. Non-automated use of data in accordance with the first and second sentences may be ordered only by a Federal Office employee who is qualified to hold judicial office.

# The Strategy

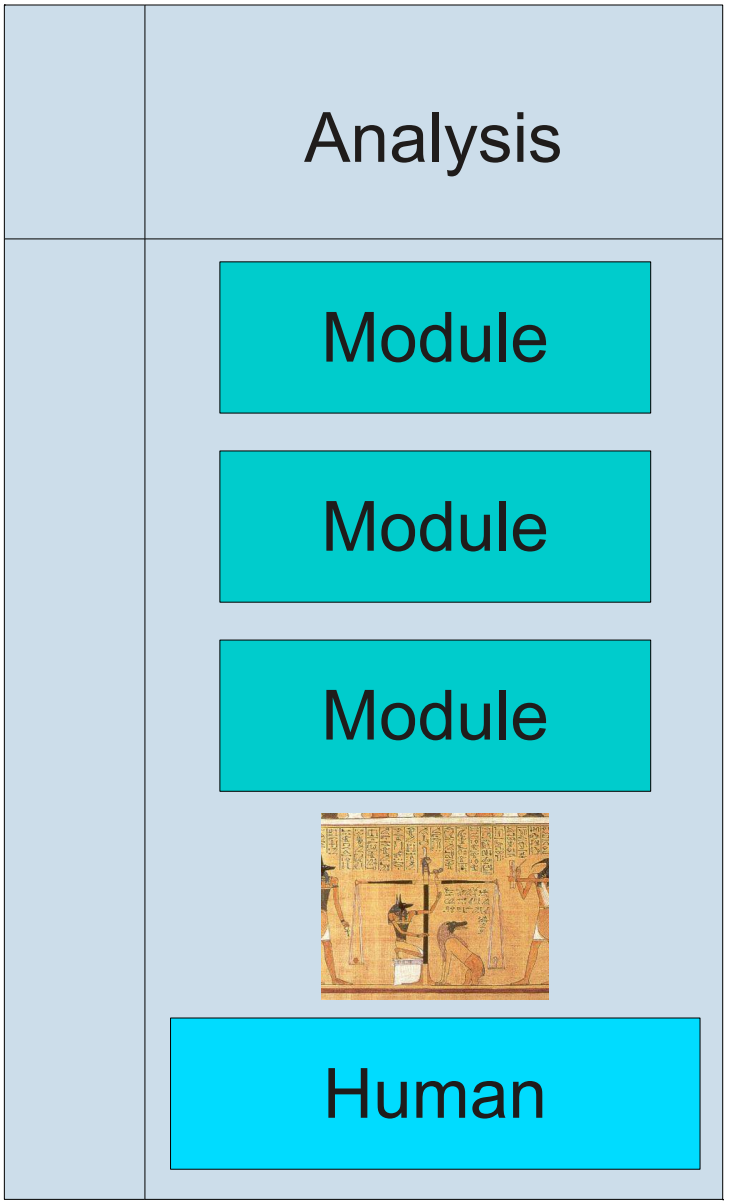
- We do not rely on a single tool
  - Buy and forget does not work
  - Still true: security is a process
- Multiple Systems
  - central connection to the WWW
  - traditional virus scanners
  - blocking of unwanted connections
  - SES (Schadprogramm-Erkennungssystem)
  - etc.

# The System


WWW
IDS
soft signatures
Government Network
Analysis
Module
Module
Module
?
Human

# The System

- Each suspicious communication is analysed with multiple modules
- Communication is separated / unpacked into files
- Analysis based on identified file type
- Each module rates the files
- Based on the rating it is decided if a manual analysis is needed
- Humans ultimately decide
  - Expertise
  - Intuition



# Modules

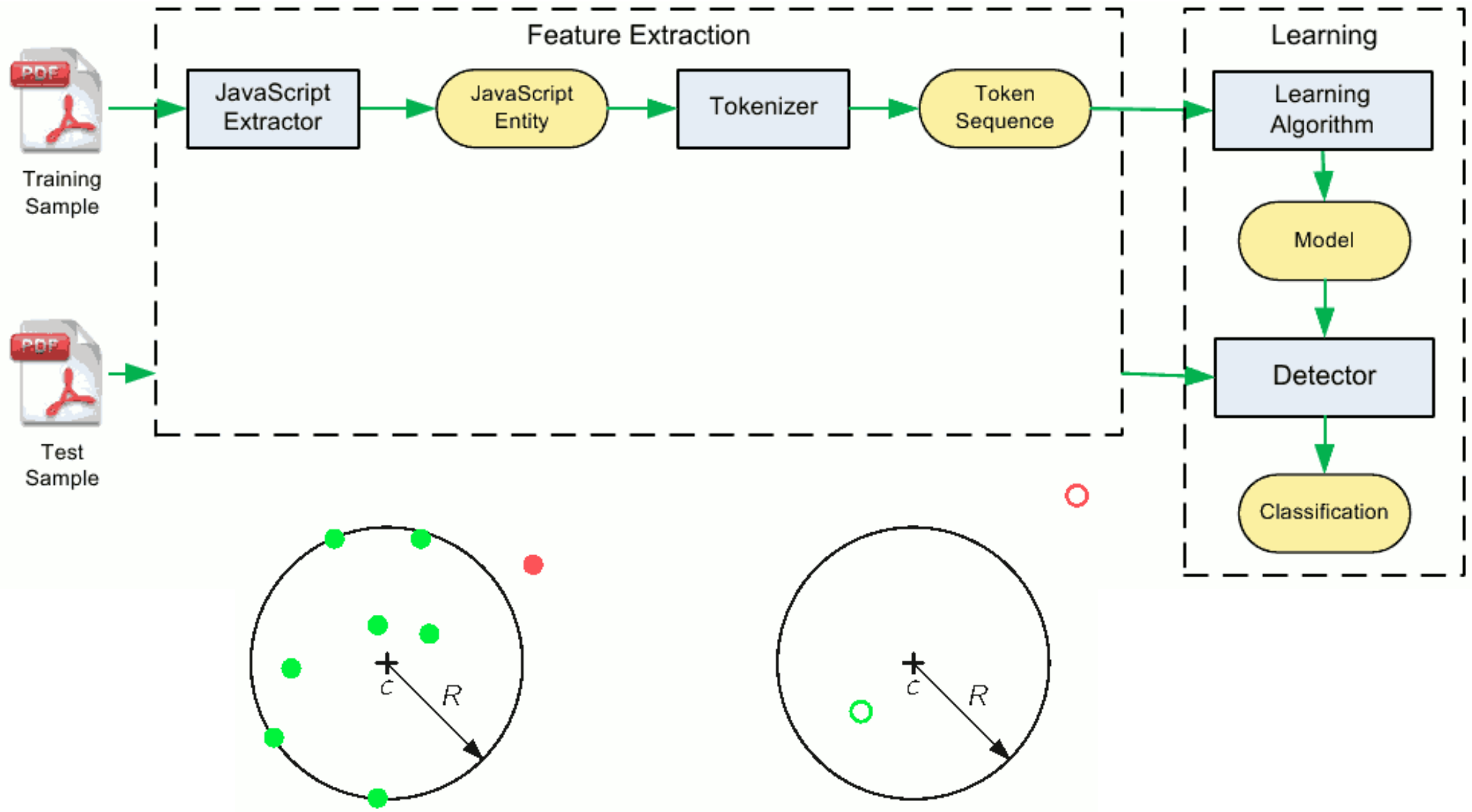
- Processing is automated
- Nearly all modules are homebrew
- Modules are:
  - Decryptor
  - VMs
  - Multiple virus scanners
  - Machine Learning Techniques
  - Lexical analyser
  - sorry, can not tell
  - sorry, can not tell
  - ...

# Example: PJScan

- One of many modules
- Often malicious PDFs contain JavaScript
  - Exploiting weaknesses in the JS engine
  - Preparing the exploit (e.g. heap spray)
- JavaScript in PDF is analysed
  - JS is extracted
  - tokenised
  - 4-grams are collected
  - SVM decides

```
1 0 obj <<
  /Type /Catalog
  /Pages 2 0 R
  /OpenAction <<
    /S /JavaScript
    /JS (alert('Hello World!');)
  >>
>>
endobj
```

# PJScan Overview



# PJScan results

- Acceptable detection rates
- Acceptable false-positives rates
- Module is extremely fast
- Works only for PDFs with JavaScript
- Sometimes malicious PDFs are thoroughly broken so that JavaScript can not be extracted
- False-positive rate is too high for most other systems
  - It is acceptable in our system, though
  - Analysts can cope with this

# Success

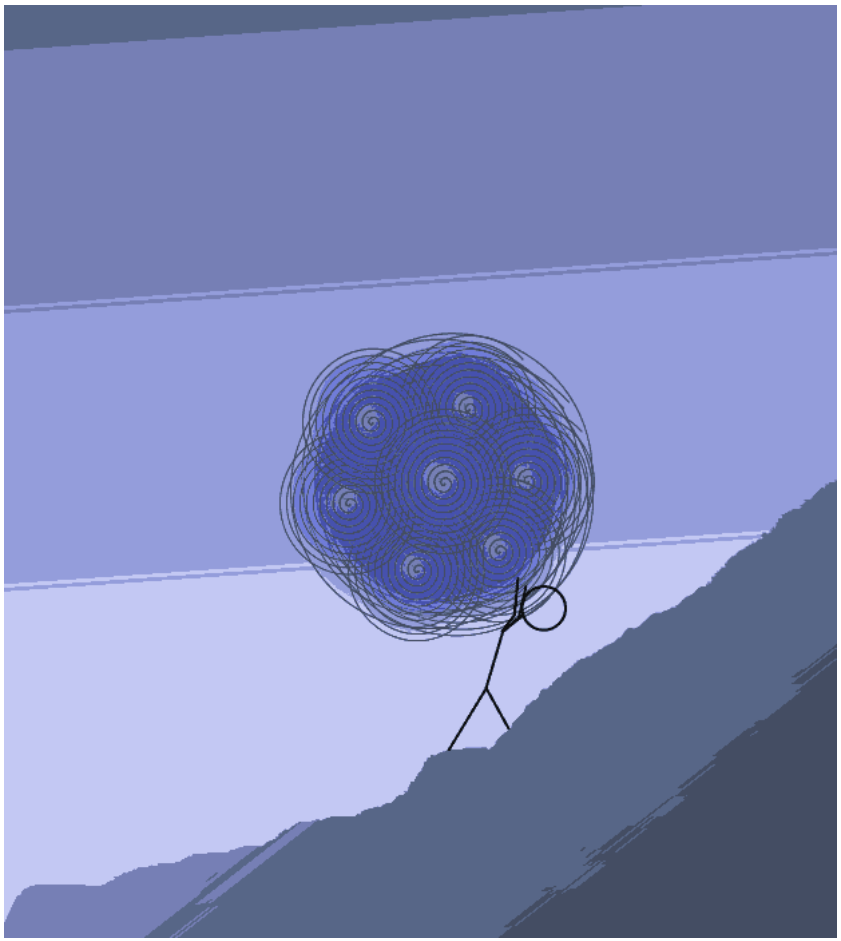
- Good overall detection rates
  - We do not detect everything, though (honestly)
- System under continuous development
  - Quickly adapts to new threats
  - We are able to use non-standard techniques
  - Binds a lot of resources
- We warn affected agencies
  - Asynchronous process
  - Agencies often have trouble coping with the attack

# Challenges

- New …
  - Operating Systems
  - Applications
  - Devices
  - User behaviour
- Constant battle for resources (who hasn't?)
- Ongoing professionalisation of attackers
  - Ressources comparable to or *exceeding* government/company resources
- Not all infection vectors are covered
- Pervasive/Ubiquitous computing

# Summary

- The system is successful as a *part* of an overall CADS (Cyber-Attack Defence-Strategy)
- Components
  - “soft”/diffuse signatures
  - automatic analysis
  - manual processing necessary
- Mostly developed in house
- APT
  - Advanced Persistent Threat
  - **Arduous Protection Task**



# Congratulations!

Ten Years of DIMVA!

# Thank you for your attention!

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Robert Krawczyk
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228-9582-5475
Fax: +49 (0)228-10-9582-5475

robert.krawczyk@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de