



# **Current Threats and Open Document Formats**

Thomas Caspers

Oliver Zendel

Federal Office for Information Security

6<sup>th</sup> ODF Plugfest  
Berlin, July 15<sup>th</sup>, 2011



# Targeted Attacks via Email

- ❑ On average between 4 and 5 targeted emails with malicious attachments are detected within German governmental networks per day
- ❑ The attacker sends an email containing direct references to the victim's occupation and function
- ❑ Points of origin for producing the malicious attachments are
  - ❑ documents that are available on public websites
  - ❑ official letters from governmental organizations
  - ❑ internal documents of working groups



Einladung filetype:pdf site:bund.de



Ungefähr 974 Ergebnisse (0,03 Sekunden)

[Google.com in English](#)

[Erweiterte Suche](#)

- Alles
- Bilder
- Videos
- News
- Shopping
- Bücher
- Places
- Blogs
- Diskussionen
- Mehr

#### Bonn

[Standort ändern](#)

#### Das Web

[Seiten auf Deutsch](#)  
[Seiten aus Deutschland](#)  
[Übersetzte Seiten](#)

[Mehr Optionen](#)

#### [PDF] [Einladung - BMVBS](#)

[www.bmvbs.bund.de/cae/servlet/.../200-jahre-hydrologie-einladung.pdf](http://www.bmvbs.bund.de/cae/servlet/.../200-jahre-hydrologie-einladung.pdf)

Dateiformat: PDF/Adobe Acrobat - [Schnellansicht](#)

**Einladung.** Panta Rhei. Hydrologie für eine sich verändernde Welt. Internationales hydrologisches Symposium. Eine Veranstaltung des Bundesministeriums ...

#### [PDF] [Einladung zum 7. Werkstattgespräch Kunst am Bau und ihre ...](#)

[www.bmvbs.bund.de/cae/.../einladung-zum-7-werkstattgesprach.pdf](http://www.bmvbs.bund.de/cae/.../einladung-zum-7-werkstattgesprach.pdf)

Dateiformat: PDF/Adobe Acrobat

**Einladung** zum 7. Werkstattgespräch. Donnerstag, 27. August 2009, 19.00 Uhr. Bundesministerium für Verkehr, Bau und Stadtentwicklung ...

#### [PDF] [Einladung zum 53. ZEBET Seminar](#)

[www.bfr.bund.de/cm/343/seminar53.pdf](http://www.bfr.bund.de/cm/343/seminar53.pdf)

Dateiformat: PDF/Adobe Acrobat - [Schnellansicht](#)

**Einladung** zum 53. ZEBET Seminar. Auszeichnung der ZEBET-Datenbank über Alternativmethoden mit dem. Herbert-Stiller-Preis 2000 der Vereinigung „Ärzte gegen ...

#### [PDF] [Einladung zum 61. ZEBET-Seminar](#)

[www.bfr.bund.de/cm/343/einladung\\_zum\\_61\\_zebet\\_seminar.pdf](http://www.bfr.bund.de/cm/343/einladung_zum_61_zebet_seminar.pdf)

Dateiformat: PDF/Adobe Acrobat - [Schnellansicht](#)

**Einladung** zum 61. ZEBET-Seminar. (Q)SARs in der Risikobewertung: Einsatzmöglichkeiten von Struktur-Wirkungs-Beziehungen im BfR ...

#### [PDF] [Einladung des BfR zu einem Vortrag von Hubert W Vesper, Ph.D ...](#)

[www.bfr.bund.de/.../einladung\\_zu\\_einem\\_vortrag\\_von\\_hubert-vesper\\_...](http://www.bfr.bund.de/.../einladung_zu_einem_vortrag_von_hubert-vesper_...)

Dateiformat: PDF/Adobe Acrobat - [Schnellansicht](#)

**Einladung** des BfR zu einem Vortrag von. Hubert W Vesper, Ph.D. National Center for Environmental Health,. Centers for Disease Control and Prevention (CDC), ...

#### [PDF] [Einladung zum 64. ZEBET-Seminar - BfR](#)

[www.bfr.bund.de/cm/343/einladung\\_zum\\_64\\_zebet\\_seminar.pdf](http://www.bfr.bund.de/cm/343/einladung_zum_64_zebet_seminar.pdf)

Dateiformat: PDF/Adobe Acrobat - [Schnellansicht](#)

**Einladung** zum 64. ZEBET-Seminar. Inhalationstoxikologie: Bedarf an Forschung und Entwicklung von in vitro. Methoden ...



filetype:odt site:bund.de

Ungefähr 46 Ergebnisse (0,12 Sekunden)

[Google.com in English](#)

[Erweiterte Suche](#)

- Alles
- Bilder
- Videos
- News
- Shopping
- Bücher
- Places
- Blogs
- Diskussionen
- Mehr

## Bonn

[Standort ändern](#)

## Das Web

[Seiten auf Deutsch](#)  
[Seiten aus Deutschland](#)  
[Übersetzte Seiten](#)

[Mehr Optionen](#)

[\[ODF\] 2007\\_10\\_25\\_Beratungsanfrage\\_V\\_1.0.doc](#)

[www.oss.bund.de/sites/default/files/3PM\\_Beratungsanfrage\\_Formular.odt](http://www.oss.bund.de/sites/default/files/3PM_Beratungsanfrage_Formular.odt)

Dateiformat: OpenDocument - [HTML-Version](#)

Datum: Ressort / Behörde: Hausanschrift: Ansprechpartner(in): Organisationseinheit: Telefon:  
Fax: E-Mail: Wie sind Sie auf den Rahmenvertrag auf-merksam ...

[\[ODF\] Muster für die Umsetzungsprüfung eines Basis-Sicherheitscheck](#)

[https://www.bsi.bund.de/.../Muster\\_Verifikation\\_Basissicherheitscheck.odt?...](https://www.bsi.bund.de/.../Muster_Verifikation_Basissicherheitscheck.odt?...)

Dateiformat: OpenDocument - [HTML-Version](#)

30. März 2011 – Für Rückfragen zu diesem Dokument können Sie sich gerne wenden an:  
gszertifizierung@bsi.bund.de.

[\[ODF\] Muster Auditbericht](#)

[https://www.bsi.bund.de/SharedDocs/.../Muster\\_Auditbericht.odt?\\_\\_blob...](https://www.bsi.bund.de/SharedDocs/.../Muster_Auditbericht.odt?__blob...)

Dateiformat: OpenDocument - [HTML-Version](#)

17. März 2011 – Für Rückfragen zu diesem Dokument können Sie sich gerne wenden an:  
gszertifizierung@bsi.bund.de.

[\[ODF\] EVB-IT Überlassungsvertrag Typ A Langfassung](#)

[www.cio.bund.de/.../evb\\_it\\_ueberlassungsvertrag\\_typ\\_a\\_langf\\_odf\\_...](http://www.cio.bund.de/.../evb_it_ueberlassungsvertrag_typ_a_langf_odf_...)

Dateiformat: OpenDocument - [HTML-Version](#)

Vertrag über die zeitlich unbefristete Überlassung von Standardsoftware. gegen  
Einmalvergütung. Zwischen. – im Folgenden „Auftraggeber“ genannt – ...

[\[ODF\] EVB-IT Überlassungsvertrag typ A Kurzfassung](#)

[www.cio.bund.de/.../evb\\_it\\_ueberlassungsvertrag\\_typ\\_a\\_kurzf\\_odf\\_...](http://www.cio.bund.de/.../evb_it_ueberlassungsvertrag_typ_a_kurzf_odf_...)

Dateiformat: OpenDocument - [HTML-Version](#)

Vertragsnummer/Kennung Auftraggeber . Vertragsnummer/Kennung Auftragnehmer . Vertrag  
über die zeitlich unbefristete Überlassung von Standardsoftware gegen ...

[\[ODF\] Konzeptvorlage IT-Beratung und CCVBPO](#)

[www.bit.bund.de/.../20080521\\_bit2\\_vorlage\\_konzeptvorlage\\_odt.odt](http://www.bit.bund.de/.../20080521_bit2_vorlage_konzeptvorlage_odt.odt)

Dateiformat: OpenDocument - [HTML-Version](#)

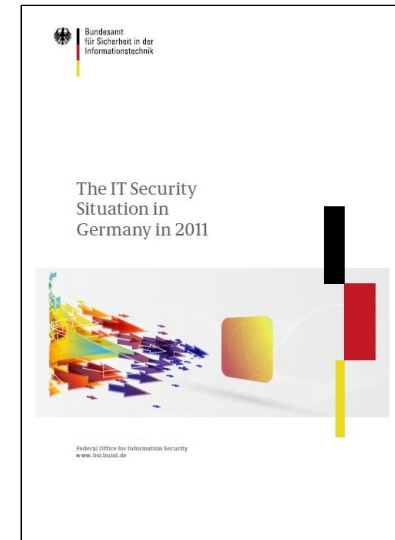
IT-Beratung, Kompetenzzentrum Vorgangsbearbeitung, Prozesse und Organisation (CC  
VBPO). < Name Dokument > für. < Name Behörde >. Version < 0.1 > ...

# Senders of Malicious Emails

- ❑ The sender is chosen *meaningfully*
  - ❑ The sender's name has a direct connection to the document that was found on a public website beforehand
  - ❑ The sender's name can be put in the context of a governmental organization easily
  - ❑ The sender's name can be found on a members list of a working group
- ❑ The way the email displays the sender's address is *plausible*
  - ❑ A real email account is compromised
  - ❑ A new email account is registered with a free webmail service using the sender's name
  - ❑ The sender's address is counterfeit

# BSI Status Report on IT Security 2011

- ❑ “Large waves of malware like Sasser or Loveletter are no longer being observed. A typical malicious program only lasts for a few days and is only targeted at a small group of victims.”
- ❑ “Targeted attacks for sabotage and espionage purposes increased significantly in the period under review and were carried out with a hitherto unknown professionalism.”
- ❑ “The BSI is concerned about the ever more widespread use of mobile devices for writing and reading e-mails, as these are often poorly protected due to a lack of suitable protection programs.”



Source: BSI, The IT Security Situation in Germany 2011

# Defense against Targeted Attacks

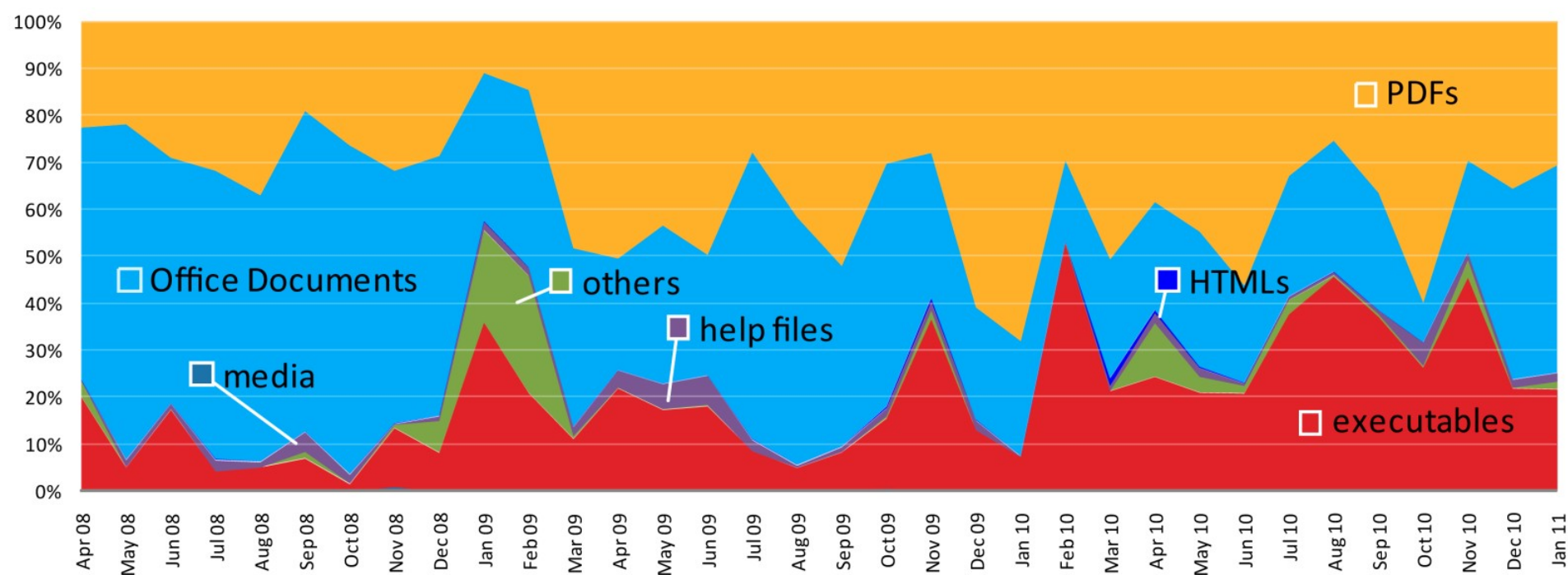
- ❑ Antivirus solutions generally do not come with appropriate signatures that are able to protect from targeted attacks

	AV solution 1	AV solution 2	AV solution 3	AV solution 4
.pdf	65%	85%	80%	55%
.doc	90%	20%	10%	5%
.xls	50%	65%	15%	10%

Source: Christoph Fischer, Effektivität von gängigen Malwarescannern bei dokumentenbasierten Schadprogrammen, 2011



# File Types Used in Targeted Attacks

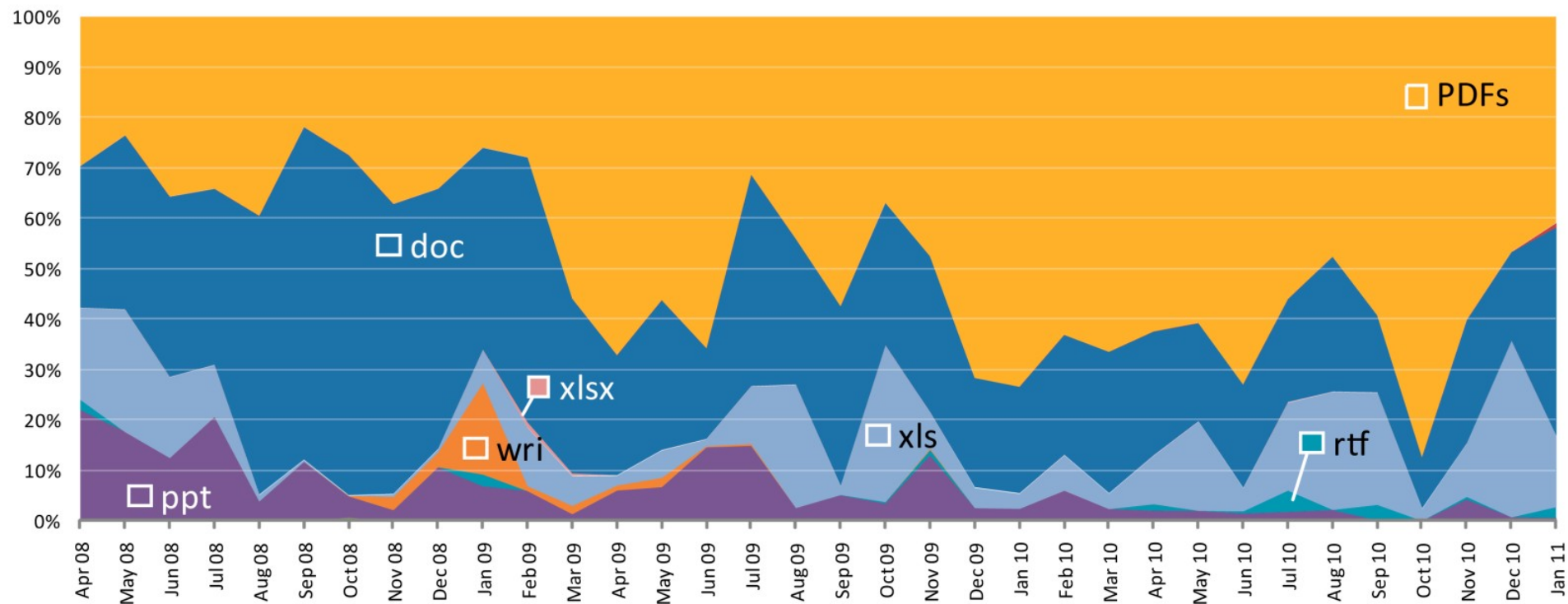


Source: Symantec MessageLabs Intelligence, February 2011 Intelligence Report





# Document File Types Used in Targeted Attacks



Source: Symantec MessageLabs Intelligence, February 2011 Intelligence Report



# Challenges: Weaknesses in the Standard Itself

- ❑ Exploitation of the PDF *Launch Action* (Didier Stevens)

```
7 0 obj
<<
  /Type /Action
  /S /Launch
  <<
    /F (cmd.exe)
  >>
>>
...
```

- ❑ *Launch Actions* are specified under section 12.6.4.5 in ISO PDF 32000-1:2008 „Document management — Portable document format“

- ❑ [http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PDF32000\\_2008.pdf](http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PDF32000_2008.pdf)



# Possibilities: Enabling the Analysis of Attacks

## ☐ Obfuscating malicious code in PDFs using filters

- ☐ ASCIIHexDecode
- ☐ ASCII85Decode
- ☐ LZWDecode
- ☐ FlateDecode
- ☐ RunLengthDecode
- ☐ CCITTFaxDecode
- ☐ JBIG2Decode
- ☐ DCTDecode
- ☐ JPXDecode
- ☐ Crypt

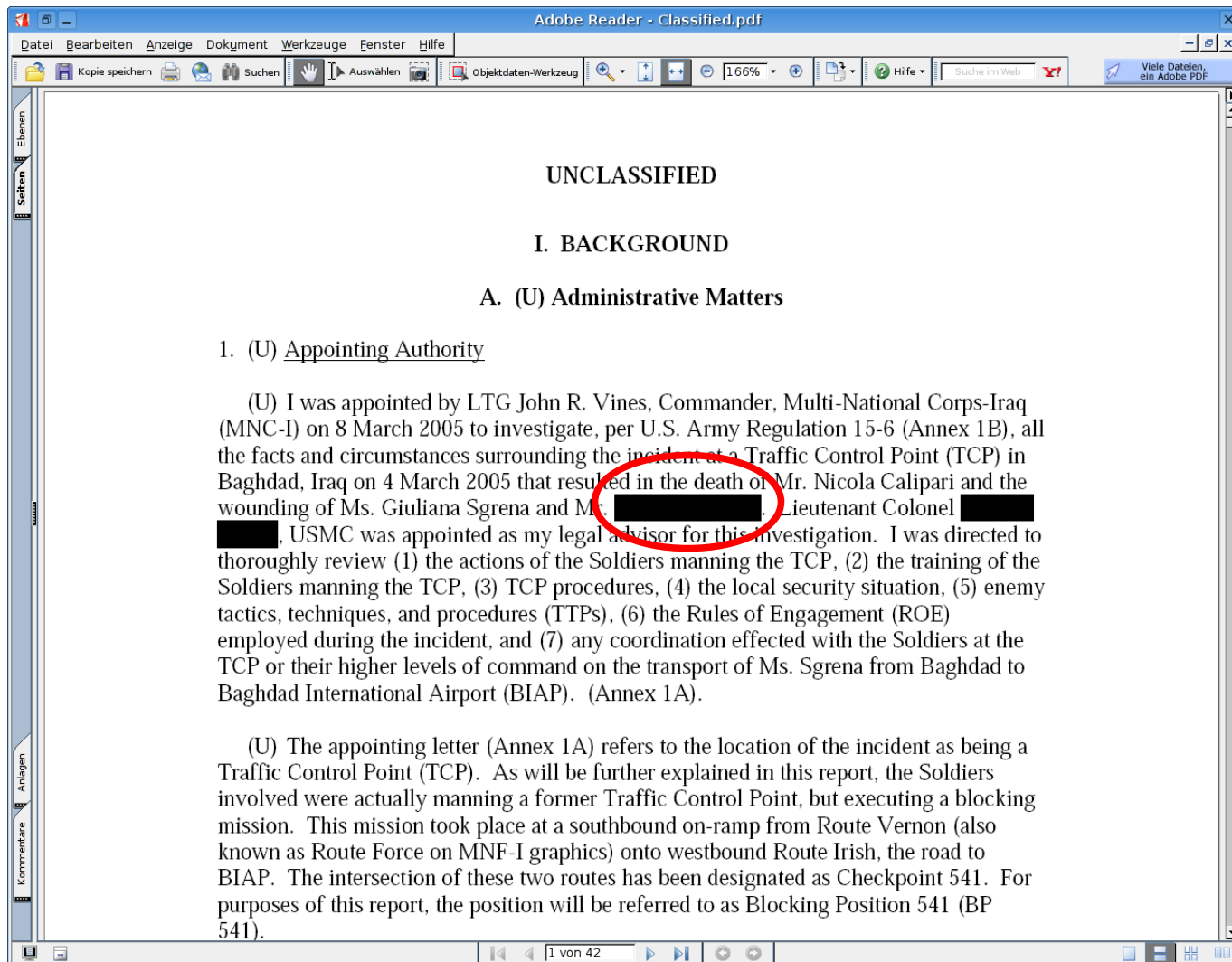
## ☐ Specified under 7.4 in ISO PDF 32000-1:2008 „Document management — Portable document format“

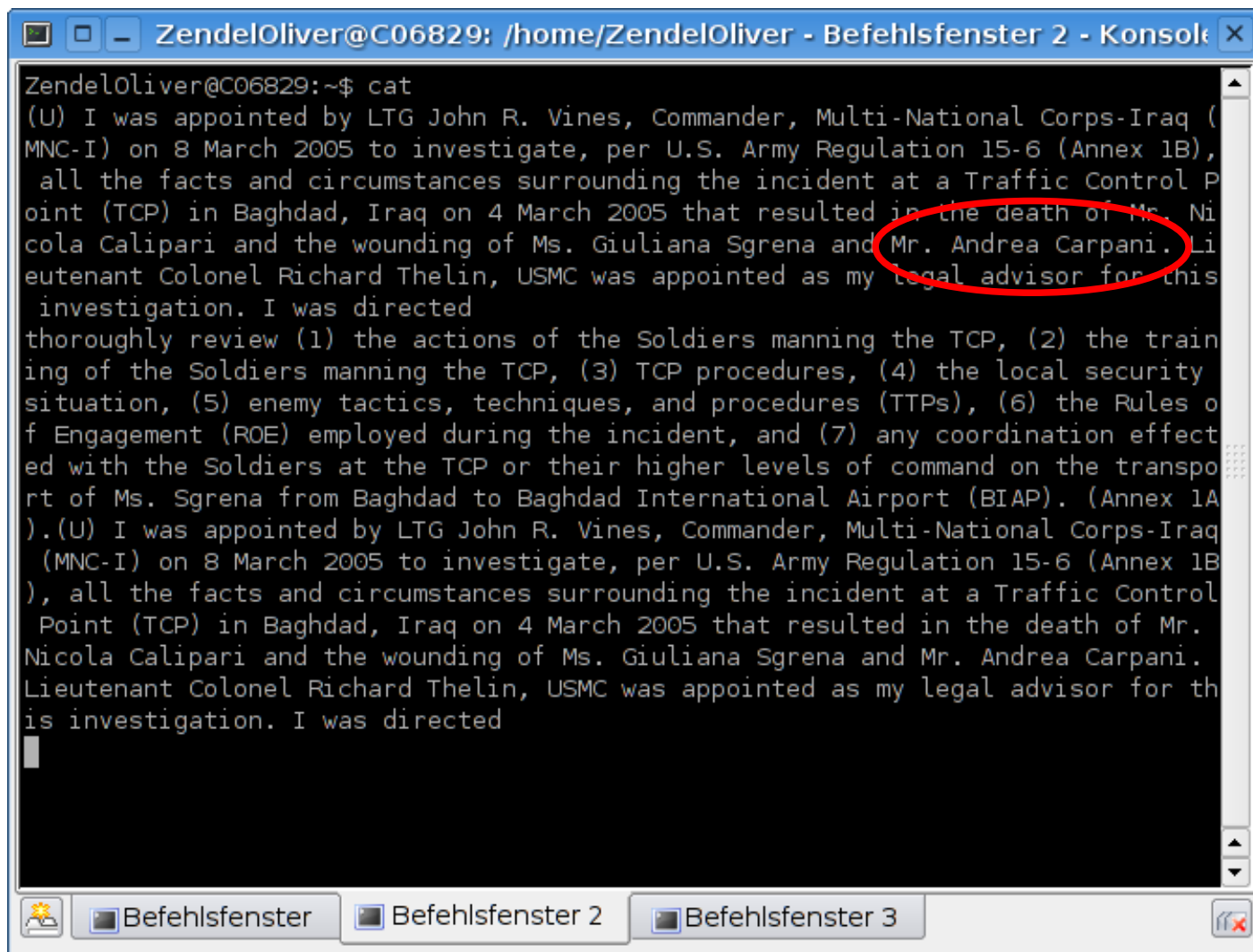
# IT Security Advantages of Open Document Formats

- ❑ Open Discussions about weaknesses in document formats
- ❑ Enabling a deeper analysis of techniques used in attacks
- ❑ Development of custom mechanisms to detect attacks
- ❑ Adapting Free Software that is used for rendering and processing of document formats to individually specific purposes – also independently from the vendor
- ❑ Prerequisite for software diversity
- ❑ Promotion of a competitive environment for vendors

**→ Strengthening IT Security**



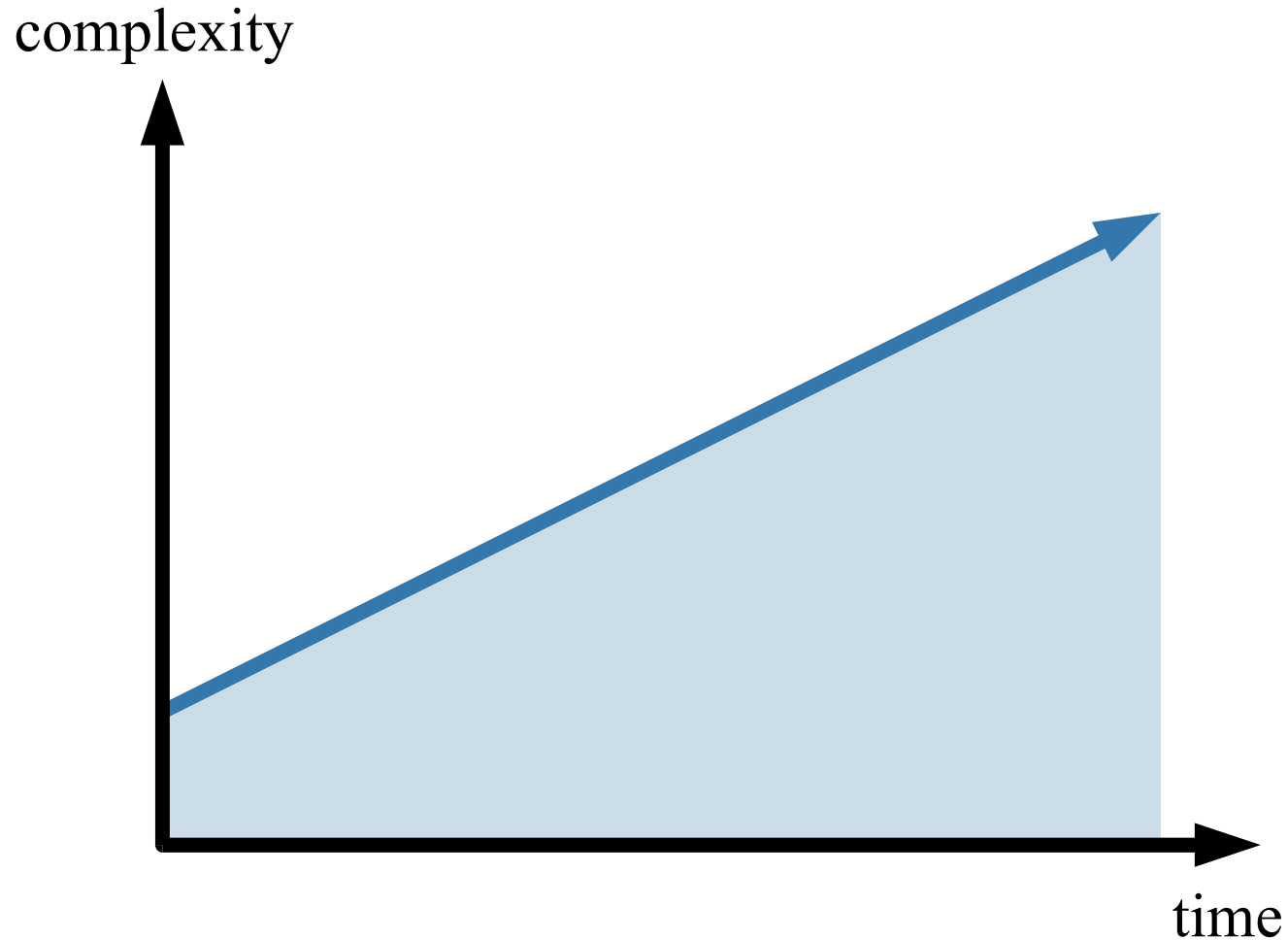




```
ZendelOliver@C06829:~$ cat
(U) I was appointed by LTG John R. Vines, Commander, Multi-National Corps-Iraq (MNC-I) on 8 March 2005 to investigate, per U.S. Army Regulation 15-6 (Annex 1B), all the facts and circumstances surrounding the incident at a Traffic Control Point (TCP) in Baghdad, Iraq on 4 March 2005 that resulted in the death of Mr. Nicola Calipari and the wounding of Ms. Giuliana Sgrena and Mr. Andrea Carpani. Lieutenant Colonel Richard Thelin, USMC was appointed as my legal advisor for this investigation. I was directed
thoroughly review (1) the actions of the Soldiers manning the TCP, (2) the training of the Soldiers manning the TCP, (3) TCP procedures, (4) the local security situation, (5) enemy tactics, techniques, and procedures (TTPs), (6) the Rules of Engagement (ROE) employed during the incident, and (7) any coordination effected with the Soldiers at the TCP or their higher levels of command on the transport of Ms. Sgrena from Baghdad to Baghdad International Airport (BIAP). (Annex 1A). (U) I was appointed by LTG John R. Vines, Commander, Multi-National Corps-Iraq (MNC-I) on 8 March 2005 to investigate, per U.S. Army Regulation 15-6 (Annex 1B), all the facts and circumstances surrounding the incident at a Traffic Control Point (TCP) in Baghdad, Iraq on 4 March 2005 that resulted in the death of Mr. Nicola Calipari and the wounding of Ms. Giuliana Sgrena and Mr. Andrea Carpani. Lieutenant Colonel Richard Thelin, USMC was appointed as my legal advisor for this investigation. I was directed
█
```



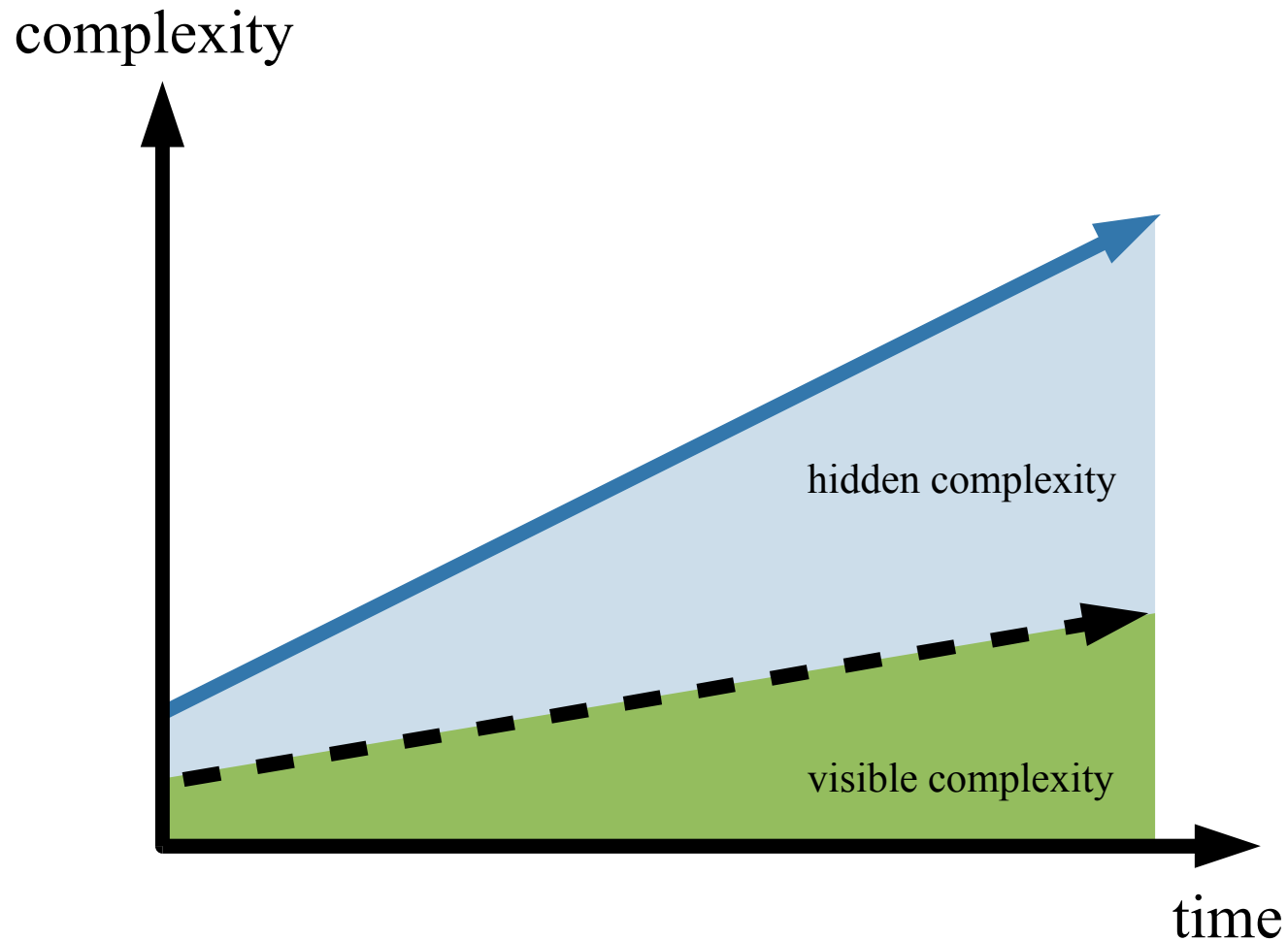
# Complexity of IT Systems







# Hiding Complexity (Usability)





# Complexity within Document Formats

Document Format	# Elements
Office Open XML	1792
WordprocessingML	780
OASIS Open Document	530

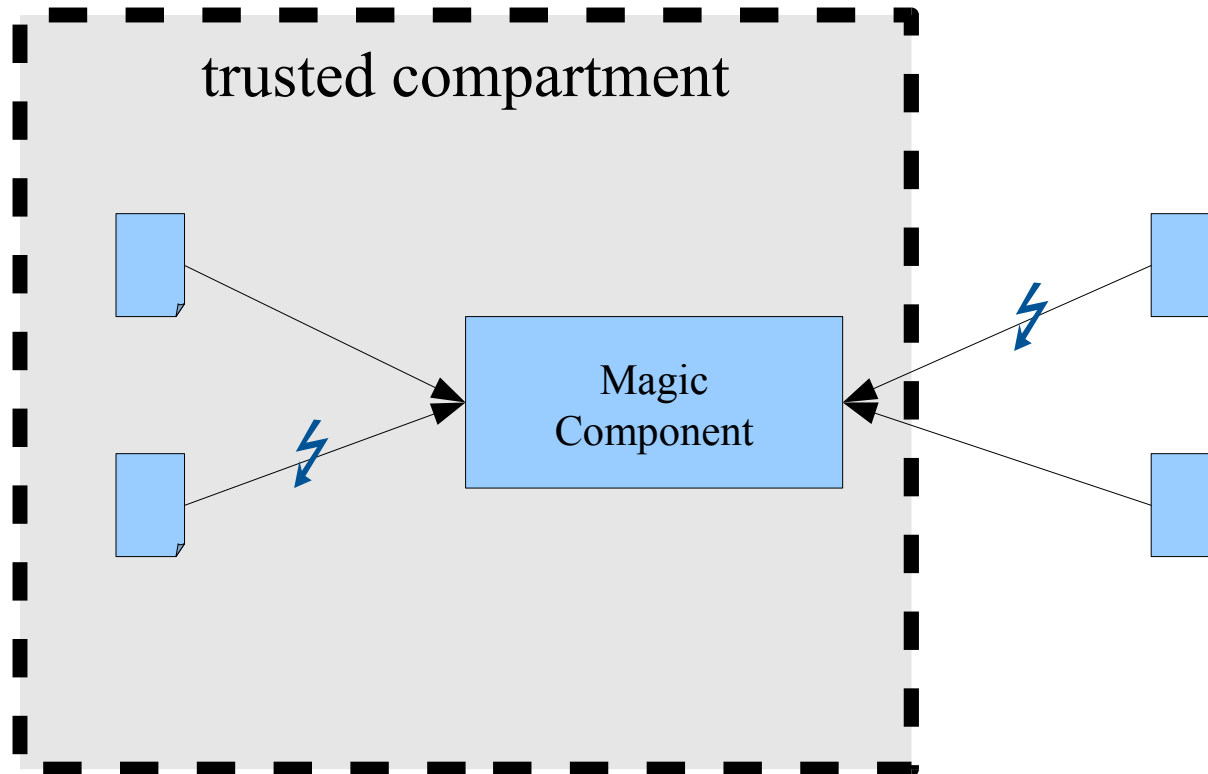
As of 2006



# Mitigating the Threats

- ❑ Goal: Sanitization of Office Documents
  - ❑ Check for weak removal of sensitive information
  - ❑ Check for hidden content
  - ❑ Check for malicious content
  - ❑ Remove unneeded or potential dangerous parts
- ❑ Requirements
  - ❑ Fully documented
  - ❑ Low complexity (format and semantics)
  - ❑ Easy to integrate in 3<sup>rd</sup> party products
  - ❑ Separation of static and dynamic parts
  - ❑ Possibility to remove dynamic parts

# Magic Component



# Contact



Federal Office for Information Security  
(BSI)

Thomas Caspers

Section C 13

Email [thomas.caspers@bsi.bund.de](mailto:thomas.caspers@bsi.bund.de)

Oliver Zendel

Section K 14

Email [oliver.zendel@bsi.bund.de](mailto:oliver.zendel@bsi.bund.de)

Godesberger Allee 185-189  
53175 Bonn

[www.bsi.bund.de](http://www.bsi.bund.de)