Risiken der Nichterkennung von Malware in komprimierter Form

DIMVA 2004
6./7. Juli 2004
Dortmund

Michel Messerschmidt, Fabian Müller & Jan Seedorf
antiVirusTestCenter, Universität Hamburg

Risiken der Nichterkennung von Malware in komprimierter Form

(1) Vorstellung aVTC

(2) Risiken durch Malware in komprimierter Form

(3) Testen der Erkennung von komprimierter Malware durch Anti-Malware-Software

(4) Testergebnisse

(1)
Vorstellung aVTC

Vorstellung aVTC

- Ein Projekt des Arbeitsbereichs AGN im Fachbereich Informatik der Universität Hamburg unter Leitung von Prof. Brunnstein
- Unabhängiges Testen von Anti-Malware-Produkten seit über 10 Jahren
- Offengelegte Methodik sichert Nachvollziehbarkeit der Ergebnisse
- Beteiligung von Studenten im Rahmen ihres Studiums

(2)
Risiken durch Malware in komprimierter Form

Risiken durch Malware

Risiken durch Malware bestehen bei:

- Aktivierung
  - Wesentliche Maßnahme: On-Access Scanner
- Weiterverbreitung / Distribution
  - Wesentliche Maßnahme: Schutz auf Gateway- und Server-Rechnern
  - Für mobile Geräte sind zusätzliche Schutzmaßnahmen notwendig

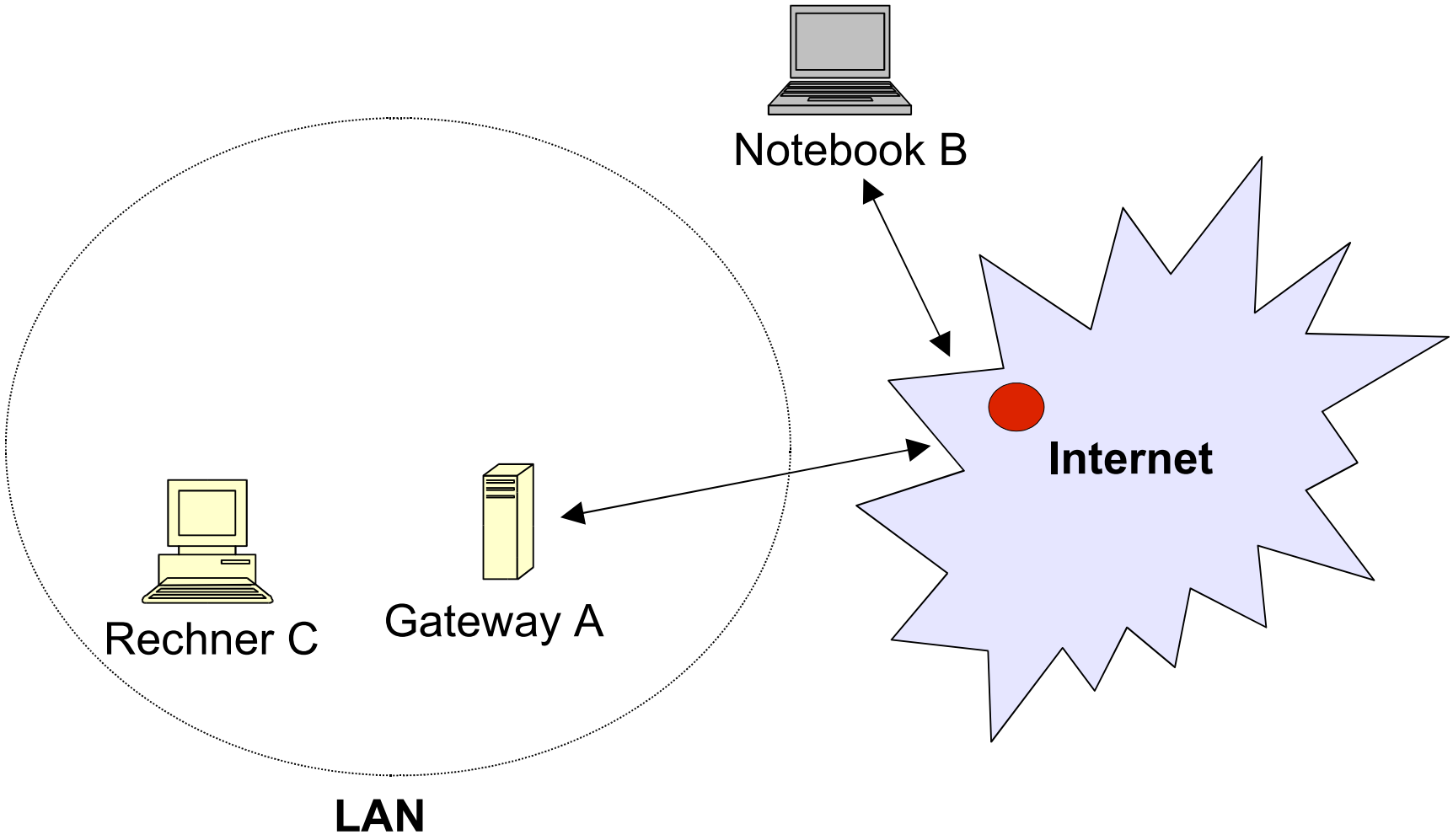
Aktivierung von komprimierter Malware

- Nicht laufzeit-komprimierte Malware
  - On-Access Modus schützt auch ohne gesonderte Maßnahmen für komprimierte Objekte
- Laufzeit-komprimierter Malware
  - Auch im On-Access Modus sind zusätzliche Maß-nahmen erforderlich:
    - Scannen in laufzeit-komprimierten Objekten erfordert effiziente Unterstützung vieler Kompressionsformate
    - Code-Emulation

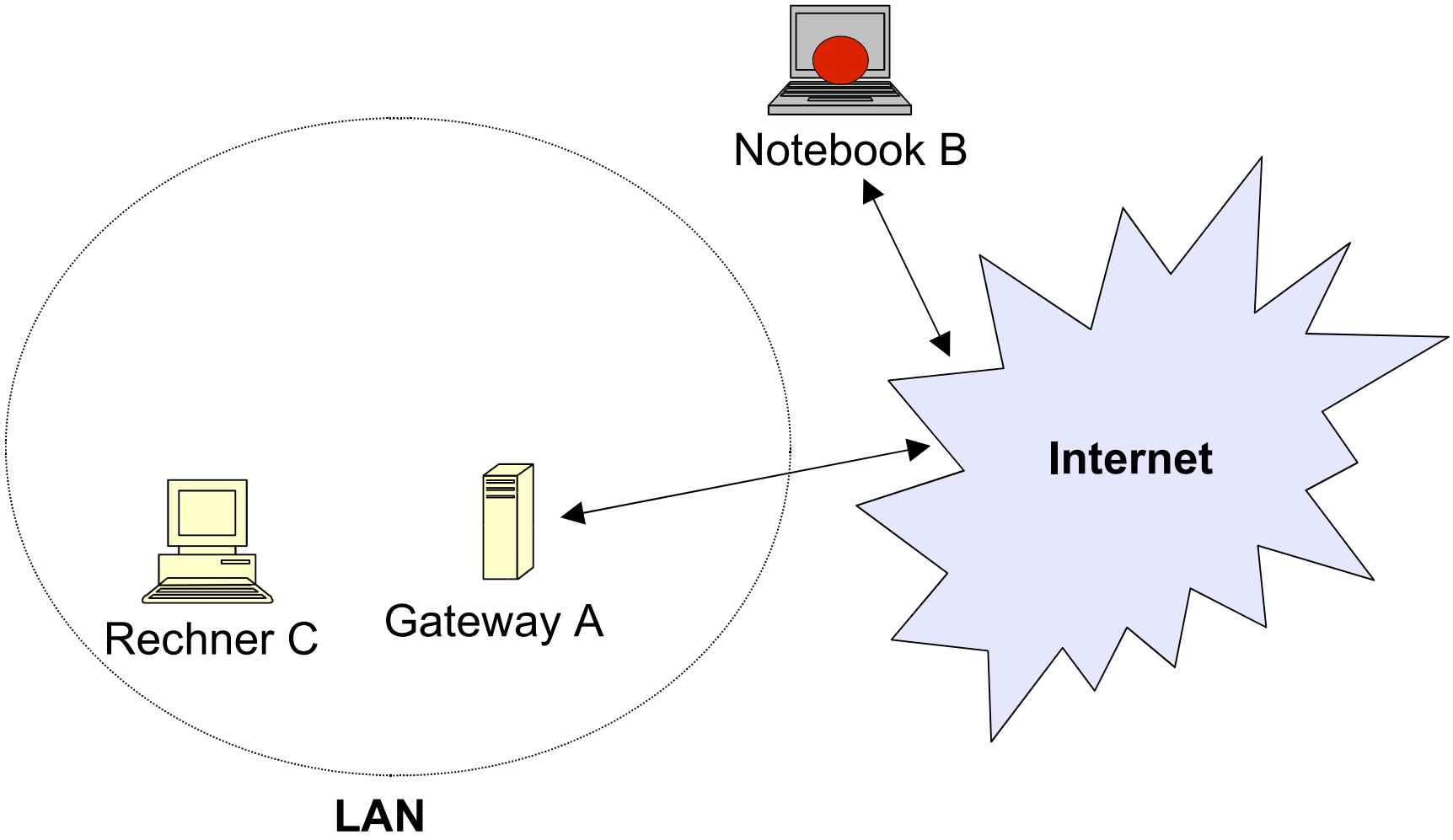
Weiterverbreitung von komprimierter Malware

- Typischer Schutz der Client-Systeme ist nicht ausreichend
  - On-Access Modus kann unzureichend sein:
    - Objekte müssen bei allen Dateizugriffen gescannt werden (nicht nur bei Ausführung)
    - Die Unterstützung verbreiteter Kompressionsformate ist erforderlich
    - Evtl. Code-Emulation
  - Oft ist nicht jedes System im lokalen Netz ausreichend geschützt
  - Komprimierte Malware kann auf eigentlich geschützte Systeme (z.B. Fileserver) gelangen und von ungeschützten Systemen aufgerufen werden

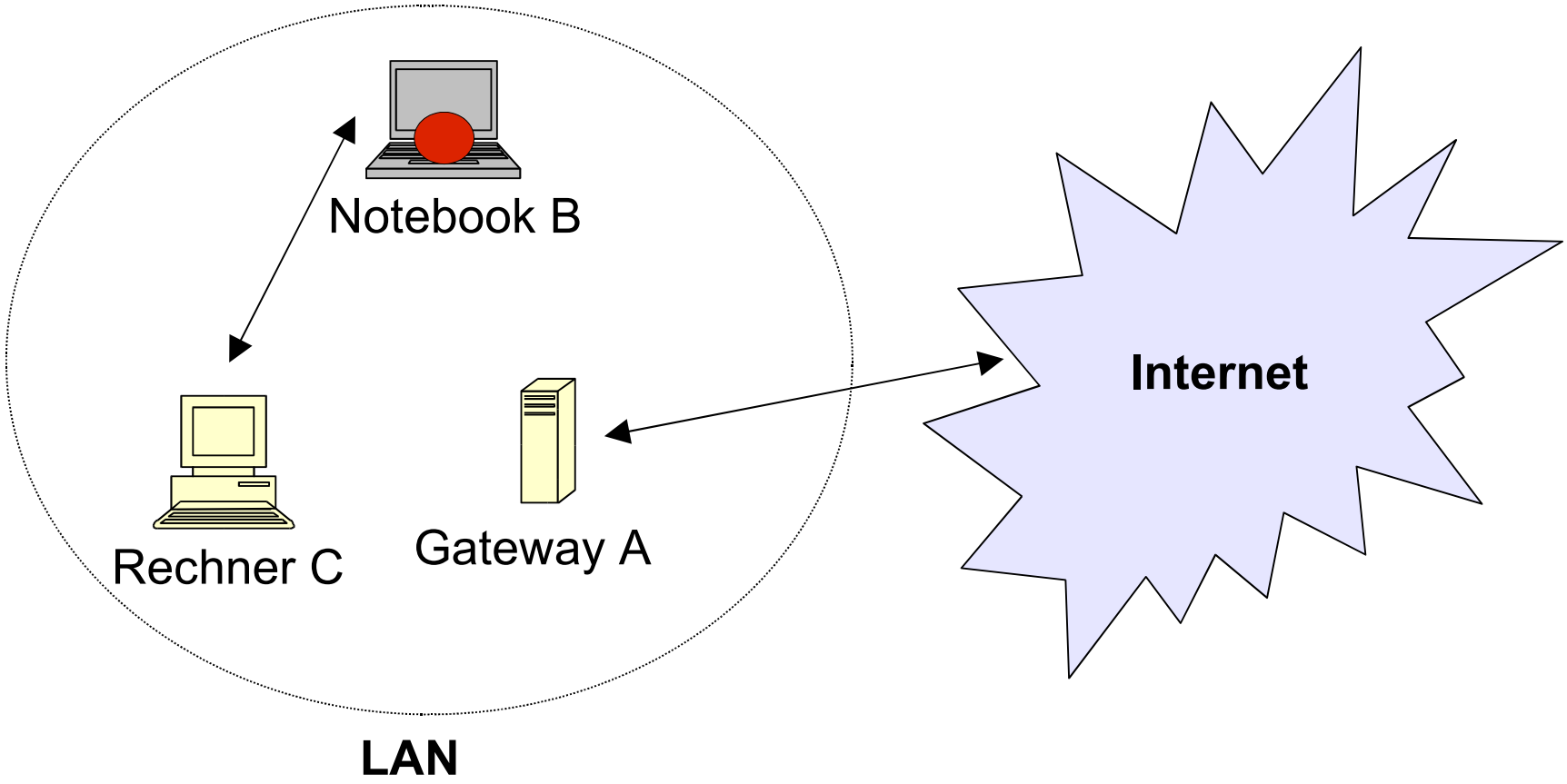
Beispiel-Szenario



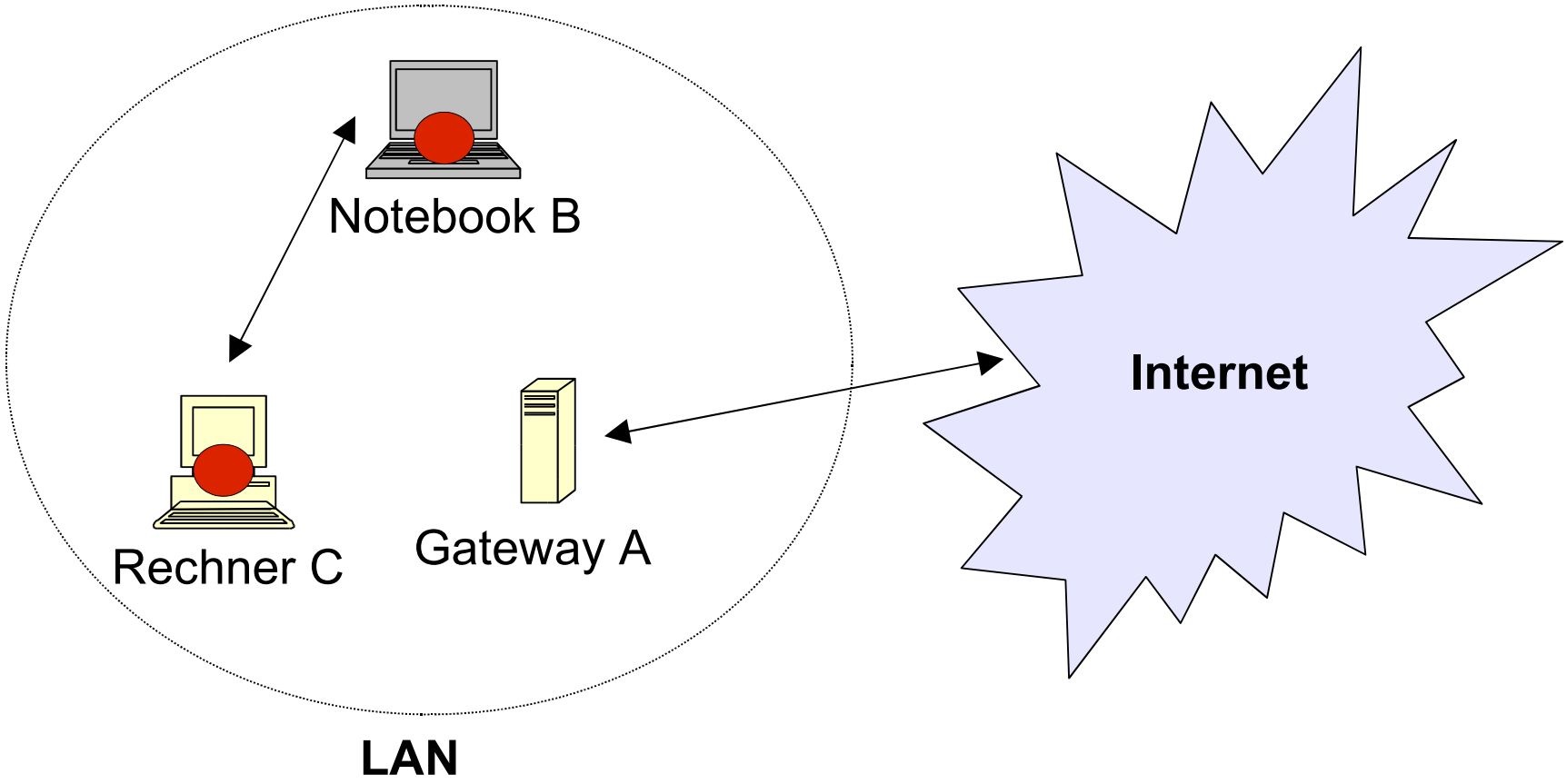
Beispiel-Szenario



Beispiel-Szenario



Beispiel-Szenario



(3)
Testen der Erkennung von komprimierter Malware durch Anti-Malware-Software

Testen der Erkennung von komprimierter Malware durch Anti-Malware-Software

- Standard-Schutz gegen komprimierte Malware

  -> Anti-Malware-Software

- Frage:

  Wie gut schützt Anti-Malware-Software vor komprimierter Malware ?

- Ansatz:

  Anpassung der aVTC-Testmethodik, um speziell die Erkennung von komprimierter Malware zu testen

Fragestellungen, die der Test beantworten soll

- Welches Produkt unterstützt welche Komprimierungsformate ?
- Mit welcher Güte werden die Formate unterstützt ?
- Werden alle Versionen eines Archivformates unterstützt ?
- Unterstützen die getesteten Programme auch alle Modi eines Komprimierungsverfahrens ?

Fragestellungen, die der Test beantworten soll (2)

- wird auch Malware in (mehrfach) rekursiv gepackten Archiven erkannt ?
- wie reagieren die getesteten Programme bei Problemen mit komprimierten Dateien ?

aVTC Testmethodik

- Tests in einem von der Außenwelt abgeschottetem Netzwerk
- Testmenge wird auf Server bereitgestellt, getestete Produkte greifen per Netzwerkfreigabe im ***on-demand*** Modus auf die Testmenge zu
- Durch Auswertung der dabei erzeugten Logdateien werden folgende Werte gemessen:
  - Erkennungsrate
  - Erkennungsgenauigkeit
  - Erkennungszuverlässigkeit

aVTC Testmethodik

- Vergleichbarkeit:
  - festgelegter Stichtag zum Einreichen der Produkte
- Nachvollziehbarkeit durch Dokumentation und Veröffentlichung von:
  - verwendeter Hardware
  - Einstellungen
  - Testumgebung
  - Testmethodik

aVTC Testmethodik

- Auswertung von Protokolldateien (Perl-Skripte):

  1) Protokolldatei in einheitliches Format umwandeln

  2) Protokolldatei aufteilen
     - infiziert gemeldete Dateien
     - nicht infiziert gemeldete Dateien
     - übrige Zeilen

  3) Erkennungsrate und andere Kriterien ermitteln

  4) Überprüfung des Protokolls

- Bis zu 2 „Nachscans“ pro Produkt und Testmenge

aVTC Testmethodik - für Komprimierungstest angepasst

- Nicht die Erkennungsrate, sondern der Einfluss der getesteten Kompressionsformate ist von Interesse
- Test von File-itw Viren sowohl unkomprimiert (als Referenzmenge) als auch unter verschiedenen Formaten komprimiert

aVTC Testmethodik - für Komprimierungstest angepasst

- Qualität der Unterstützung eines Kompressionsformates durch ein Testprodukt:
  - Differenz zwischen der Erkennungsrate unter Anwendung der jeweiligen Kompression und der Erkennungsrate der unkomprimierten Referenzmenge

$$\text{Minderung der Erkennungsrate}_{\text{Produkt, Format}} = \text{Erkennungsrate Referenztestmenge}_{\text{Produkt}} - \text{Erkennunngsrate}_{\text{Produkt, Format}}$$

aVTC Testmethodik - für Komprimierungstest angepasst

- Durchgeführter Test:
  - 25 AntiMalware Produkte
  - Erkennung von 32 Kompressions-/Archivformaten
  - Referenztestmenge: file-itw (Wildlist Okt 2001)
  - Betriebssystem: Windows 2000

aVTC Testmethodik - verschiedene Testarten

- Testen der Kompressionsformate*:
  - Einfache Kompression (ein Archiv pro Verzeichnis)
  - Gesamte Referenztestmenge in einem Archiv
  - Archive ohne Dateiendung
  - Selbstextrahierende Archive
  - Passwort-geschützte Archive
  - Rekursive Archive (2-fach und 9-fach)

(*soweit vom Format unterstützt)

(4)
Testergebnisse

Getestete Produkte

ANT	Antivir
AVA	Avast!
AVG	AVG Antivirus System
AVK	Antiviren Kit
AVP	Kaspersky Antivirus
BDF	BitDefender
CMD	Command Antivirus
DRW	Dr. Web
FIR	Fire Anti-virus Kit
FPR	F-Prot for Windows
FSE	F-Secure
GLA	Gladiator Antivirus
IKA	Ikarus Virus Utilities
INO	eTrust Antivirus
NAV	Symantec Antivirus
NVC	Norman Virus Control
PAV	Power Antivirus
PER	Per Antivirus
PRO	Protector
QHL	QuickHeal
RAV	RAV Antivirus
SCN	McAfee ViruScan
SWP	Sophos Anti Virus
VBR	VirusBuster
VSP	VirScanPlus

Getestete Komprimierungsformate

7Z_	7-Zip
AC2	Ace v2
ACE	Ace v1
ARC	Arc
ARJ	Arj
B64	MIME Base64
BH_	Black Hole
BZ2	Bzip2
CAB	MS Cabinet File
CMS	MS Compress
GZ_	Gzip
HA_	Ha
JAR	Jar
JAV	Java Archive
LHA	Lha
PAK	Pak
RA1	Rar v1
RA2	Rar v2
RA3	Rar v3
RAR	Rar v3 (solid compression)
SHA	Shell Archive
SQZ	Squeeze It
TAR	Tape Archive
UC2	Ultra Compressor 2
UUE	UUEncode
ZI2	PkZip 6.0 (zip2.04 compatible)
ZI6	PkZip 6.0
ZIB	PkZip 6.0 (bzip2 comp.)
ZID	PkZip 6.0 (DCLimplode comp.)
ZIE	PkZip 6.0 (Deflate64 comp.)
ZIP	InfoZip 2.3
ZOO	Zoo

Testergebnisse

- Alle Testergebnisse im Internet unter

www.avtc.info

- Für jede getestete Kompressionsart eine Matrix (Produkte x Kompressionsformate),
  Inhalt der Zellen ist jeweils die Minderung der Erkennungsrate

Testergebnisse - Auffälligkeiten

- Archive ohne Dateiendung:
  - Probleme bei der Erkennung (AVG, CMD, FPR)
- Passwort-geschützte Archive:
  - Meldung des Testproduktes interessiert
  - Viele Produkte melden passwortgeschützte Archive als „ok“ (das Archiv ist ok), sehr irreführend für den Benutzer
  - Meldung „passwort-protected“ und „unable to scan“ eher selten
- Rekursiv komprimierte Archive:
  - Stabilitätsprobleme der Testprodukte (FSE, NVC, PRO, SCN)

	ANT	AVA	AVG	AVK	AVP	BDF	CMD	DRW	FIR	FPR	FSE	GLA	IKA	INO	NAV	NVC	PAV	PER	PRO	QHL	RAV	SCN	SWP	VBR	VSP
_A_	26,9		23,6										87,2					53,3	25,6						98,3
7Z_																									
AC2																				0,9	92,1				
ACE																				0,9	6,6				
ARC				30,3																	32,8				
ARJ																				0,9					
B64		0,2											34,0						97,7						
BH_																									
BZ2																					2,9				
CAB																				0,9					
CMS							0,9			0,9															
GZ_	99,8																								99,2
HA_																					69,2				
JAR																									
JAV															60,0					0,9					
LHA														6,3	0,7		0,5								
PAK						97,9																			
RA1							95,0			95,0				99,5						0,9					
RA2																				0,9					
RA3																				0,9					
RAR																				0,9					
SHA					55,2		89,3			89,1				55,7		56,2	55,2						55,3		
SQZ																									
TAR		0,5				8,9																	2,7		
UC2																									
UUE														0,7											
ZI2			1,4																	0,9					
ZI6			1,4																	0,9					
ZIB		97,5	97,5	97,5		97,4						72,2			97,5			99,3	97,5		97,5	97,5	97,5		
ZID		82,0	82,0	81,7	90,5	81,1	90,9	90,5		90,5	90,5	54,4		90,5	81,7	82,3	90,5	86,0	82,2	91,3	81,7	81,7	82,3		
ZIE			99,5	99,5											80,1				99,5		99,5	99,5	99,5		
ZIP			2,3												22,2					0,9					
ZOO																									

Loss of detection (in percent): 0,0% 0,1% – 99,9% 100,0%