Ulrich Flegel, Michael Meier (Eds.)

Detection of Intrusions and Malware & Vulnerability Assessment

GI Special Interest Group SIDAR Workshop, DIMVA 2004
Dortmund, Germany, July 6-7, 2004
Proceedings

Gesellschaft für Informatik 2004

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-46

ISBN 3-88579-375-X
ISSN 1617-5468

Volume Editors
Ulrich Flegel
University of Dortmund,
Computer Science Department, Chair VI, ISSI
D-44221 Dortmund, Germany
ulrich.flegel@udo.edu
Michael Meier
Brandenburg University of Technology Cottbus,
Computer Science Department, Chair Computer Networks
P.O. Box 10 13 44, D-03013 Cottbus, Germany
mm@informatik.tu-cottbus.de

printed by Köllen Druck+Verlag GmbH, Bonn

Risiken der Nichterkennung von Malware in komprimierter Form

Heiko Fangmeier, Michel Messerschmidt, Fabian Müller, Jan Seedorf

antiVirusTestCenter
Fachbereich Informatik, Universität Hamburg
Vogt-Kölln-Straße 30
22527 Hamburg
5fangmei@informatik.uni-hamburg.de
uni@michel-messerschmidt.de
9fmuelle@informatik.uni-hamburg.de
seedorf@informatik.uni-hamburg.de

Abstract: Maliziöse Software (Malware) gefährdet die Vertraulichkeit, Integrität und die Verfügbarkeit von Informatiksystemen auf verschiedene Art und Weise. In diesem Beitrag wird der Frage nachgegangen, inwiefern durch Malware in komprimierter Form Risiken entstehen. Ausgewählte Risiken werden anhand eines Szenarios veranschaulicht und analysiert.

Ein Standard-Schutzmechanismus vor Malware ist Anti-Malware-Software. Es wird eine Testmethodik vorgestellt, mit der systematisch die Güte der Erkennung von Malware in komprimierter Form durch Anti-Malware Software getestet werden kann. Abschließend werden mit dieser Methodik erlangte Testergebnisse vorgestellt.

1 Risiken durch Malware in komprimierter Form

1.1 Einleitung

Maliziöse Software (Malware) gefährdet die Vertraulichkeit, Integrität und die Verfügbarkeit von Informatiksystemen auf verschiedene Art und Weise. Ein etablierter Schutzmechanismus gegen Malware ist der Einsatz von Anti-Malware Software. Diese kann gegenüber einer Testmenge mit maliziöser Software getestet werden, um eine Aussage über den gewährten Schutz zu ermöglichen.

In diesem Beitrag wird der Frage nachgegangen, inwiefern Risiken der Umgehung des durch Anti-Malware Software gebotenen Schutzes durch Malware in komprimierter Form bestehen. Um die Risiken zu verdeutlichen, wird in einem Beispielszenario aufgezeigt, wie der Schutz durch komprimierte Malware umgangen werden kann. Im zweiten Abschnitt wird eine Testmethodik vorgestellt, mit der die Güte der Erkennung

komprimierter Malware von Anti-Malware Software gemessen werden kann. Abschließend werden Ergebnisse eines mit der vorgestellten Methodik durchgeführten Tests präsentiert.

Prinzipiell besteht ein Risiko der Umgehung einer Anti-Malware Software immer dann, wenn ein Anti-Malware Programm ein bestimmtes Kompressionsformat nicht unterstützt. Dann kann mit diesem Format komprimierte Software unerkannt auf einen eigentlich geschützten Rechner gelangen. Dieses Risiko kann allerdings dadurch gemindert werden, dass die Anti-Malware Software den Rechner im on-access Modus schützt[1]. Hierbei wird jeder ausführbare Code beim Zugriff durch eine im Hintergrund aktive Anti-Malware Software überprüft. So kann zwar komprimierte Malware unerkannt auf einen Rechner gelangen, aber bei der Ausführung (nach einer Dekompression) wird sie erkannt und eine Infektion verhindert.

Ein zusätzliches Risiko besteht bei laufzeit-komprimierter Malware[2], da diese erst während der Ausführung dekomprimiert wird. Wird das entsprechende Kompressionsformat von der Anti-Malware Software nicht unterstützt, kann die Aktivierung der Malware auch im on-access Modus in der Regel nicht verhindert werden. Im durchgeführten Test konnte die Erkennung von laufzeit-komprimierter Malware aus Komplexitätsgründen jedoch nicht getestet werden.

Es sind jedoch auch Szenarien denkbar, zum Beispiel in zentral administrierten Netzwerken, in denen nicht jedes Rechensystem durch eine lokal installierte Anti-Malware Software im on-access Modus geschützt wird. Hier besteht nicht nur das Risiko der Verbreitung von unerkannter maliziöser Software, sondern auch das Risiko der Ausführung und damit der Infektion des betroffenen Systems.

Ein weiteres Risiko besteht durch bestimmte, stark komprimierte Archive, die beim Entkomprimieren potentiell die Anti-Malware Software zum Absturz bringen und somit deren Verfügbarkeit gefährden [Bi03].

1.2 Ein Beispielszenario

Abbildung 1 zeigt ein beispielhaftes Szenario zur Veranschaulichung von potentiellen Risiken. In diesem Szenario als einzelne Rechner oder Server bezeichnete Symbole können entweder für einen einzelnen Computer dieses Typs oder aber für eine gesamte Gruppe dieser Rechner stehen (Cluster). Dieses ist für die Betrachtung in Bezug auf Malware nicht relevant, da ein Rechnercluster als infiziert betrachtet werden kann, sobald ein Rechner dieses Clusters infiziert ist.

[1] Anti-Malware Programme können bösartige Software (Malware) grundsätzlich in zwei verschiedenen Betriebsarten erkennen: Im on-demand Modus wird die Software bei Bedarf (engl. "demand") aktiviert und zur Überprüfung (Scannen) von Dateien oder Verzeichnissen eingesetzt. Im on-access Modus ist die Software im Hintergrund aktiv und überwacht die Aktivitäten auf dem Rechner. Sie überprüft bei jedem Dateizugriff (engl. "access") automatisch im Hintergrund die entsprechende Datei auf bösartige Software.

[2] Eine laufzeit-komprimierte (engl. „runtime compression“) Software besteht in der Regel aus einer kurzen Dekompressionsroutine gefolgt von dem komprimierten Code, der erst direkt vor der Aktivierung im Speicher dekomprimiert wird. Für die Erkennung von Malware sind dabei auch Verfahren zu berücksichtigen, bei denen der ausgeführte Code niemals komplett dekomprimiert vorliegt.

Rechner B, Rechner C und der Gateway-Server A befinden sich in einem lokalen Netzwerk (LAN). Rechner B ist ein Laptop, der sowohl gelegentlich im Firmennetz angeschlossen ist, als auch eine direkte Verbindung ins Internet haben kann (bei Einsatz außerhalb des betrachteten LANs). Rechner C entspricht einem typischen Büroarbeitsplatz. Er ist über das Gateway A an das Internet angeschlossen. Server/Gateway A ist der zentrale Punkt der Netzanbindung.

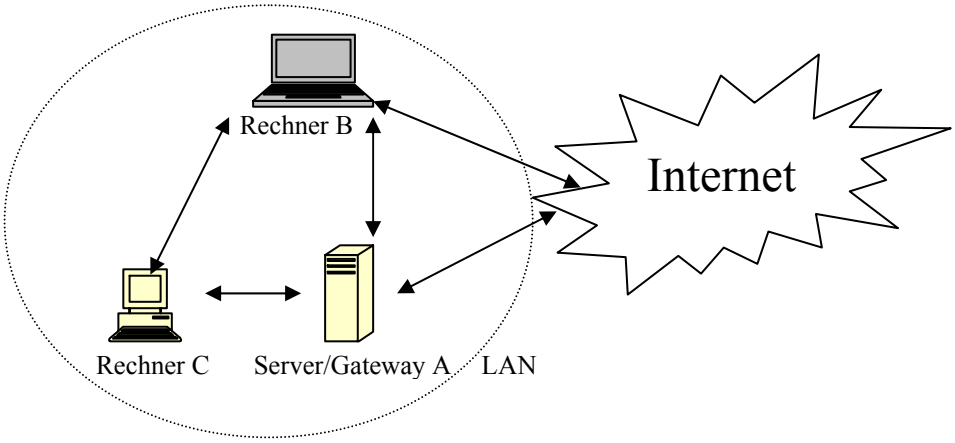

Abbildung 1: Beispielszenario

Generell besteht in einem lokalen Netzwerk das Risiko, dass auf einem mit Anti-Malware Software geschützten Rechner Malware in komprimierter Form abgelegt aber nicht ausgeführt wird (vgl. 1.1), und diese dann von einem nicht geschützten Rechner des Netzwerkes aufgerufen bzw. kopiert und ausgeführt wird. Genauso kritisch ist ein Ausfall eines Anti-Malware Produktes auf einem der Rechner. Im Einzelnen sind zum Beispiel folgende Möglichkeiten der Ausbreitung von maliziöser Software und der Infektion von Rechnern in einem lokalen Netzwerk denkbar:

Wird auf dem Gateway-Rechner A, der das Netzwerk schützen soll, ein Anti-Malware Produkt im on-access Modus eingesetzt, das ein bestimmtes Kompressionsformat nicht unterstützt, so kann mit diesem Format komprimierte Malware unentdeckt zu Rechner B und C gelangen. In diesem Fall würden alle Rechner ohne Anti-Malware Schutz infiziert. Selbst beim Einsatz eines Anti-Malware Produktes auf Rechner C im on-access Modus ist eine Infektion denkbar, falls dieses Produkt die (durchgelassene) Malware auch unkomprimiert nicht erkennt. Dies kann der Fall sein, wenn auf Rechner C ein anderes Produkt als auf dem Gateway eingesetzt wird, oder wenn die Software auf Rechner C aus anderen Gründen nicht schützt (veraltete Signaturen, Absturz, Fehlkonfiguration).

Ein weiteres Risiko ist denkbar, wenn Rechner B außerhalb des Netzwerkes eingesetzt wird (zum Beispiel auf Reisen), und komprimierte Malware auf den Rechner gelangt, deren Kompressionsformat von der auf Rechner B laufenden Anti-Malware Software nicht unterstützt wird. In diesem Fall kann die Malware auf Rechner C gelangen und

dort zur Infektion führen (weil gar kein Anti-Malware Schutz besteht oder aus in obigem Beispiel genannten Gründen). Dies kann sogar dann passieren, wenn die auf dem Gateway-Rechner eingesetzte Anti-Malware Software Malware und Kompressionsformat erkennen würde, da eine direkte Verbindung im Netzwerk von Rechner B zu Rechner C besteht.

Aus den obigen Ausführungen ist zu ersehen, dass sich kein Risiko durch komprimierte Malware manifestieren kann, solange jede Komponente des Netzwerkes durch Anti-Malware Software im on-access Modus geschützt ist[3]. Wenn allerdings, intentional oder unabsichtlich, mindestens eine Komponente im Netzwerk nicht geschützt ist (z.B. aus Performance-Gründen), kann eine Nichterkennung von komprimierter Malware zu einer Infektion des Netzwerkes führen.

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

Ein Standard-Schutzmechanismus - auch gegen komprimierte Malware - ist Anti-Malware Software. Es stellt sich die Frage, inwiefern aktuelle Anti-Malware Programme ausreichend guten Schutz gegen die aufgezeigten Risiken bieten, indem sie Malware auch in komprimierter Form erkennen. Im anti Virus Test Center (aVTC) der Universität Hamburg wird seit Jahren regelmäßig Anti-Malware Software getestet. Um die Frage der Güte von Anti-Malware Programmen hinsichtlich der Erkennung von Malware in komprimierter Form zu untersuchen, wurde die im aVTC eingesetzte Methodik so angepasst, dass im Rahmen eines Tests von Anti-Malware Software folgende Fragen beantwortet werden können:

- Welches Produkt unterstützt welches Komprimierungsformat ?
  Um eine Aussage zu machen, welches Anti-Malware Programm welchen Schutz hinsichtlich komprimierter Malware bietet, gilt es zu prüfen, welches Produkt welche Formate bei der Erkennung von maliziösem Code unterstützt.

- Mit welcher Güte werden die Formate unterstützt ?
  Es wird nicht nur getestet, welches Produkt welche Formate unterstützt, sondern auch die Qualität der von den Produkten jeweils eingesetzten Dekomprimierungsroutine[4], um nachzuprüfen, ob die getestete Anti-Malware Software auch zuverlässig alle Malware in einem von ihr unterstützen Format erkennen kann, so sie diese Malware denn auch unkomprimiert erkennt.

[3] sofern diese die Malware unkomprimiert erkennt und es sich nicht um eine Laufzeit-Komprimierung handelt

[4] Es wird davon ausgegangen, dass die getesteten Produkte im Regelfall die komprimierte Malware dekomprimieren und dann mit ihren Signaturen vergleichen. Dies muss nicht der Fall sein: die Produkte können auch für jede Kombination aus Malware und Kompressionsformat eine eigene Signatur erstellen.

- Werden alle Versionen eines Archivformates erkannt ?
  Erfahrungen zeigen [Br03], dass sich einige Komprimierungsformate substantiell in unterschiedlichen Versionen des jeweiligen Formats unterscheiden. Es gilt zu verifizieren, dass ein Produkt auch Malware in allen Versionen eines Formates erkennt. Ist dies nicht der Fall, entsteht die Gefahr, dass sich der Benutzer der Software zu Unrecht auf die Unterstützung eines bestimmten Komprimierungsformates durch die eingesetzte Anti-Malware Software verlässt.

- Unterstützen die getesteten Anti-Malware Programme auch unterschiedliche Modi eines Komprimierungsformates ?
  Neben unterschiedlichen Versionen bieten viele Komprimierungsprogramme auch die Kompression in unterschiedlichen Modi an (z.B. selbstextrahierende Archive, solide Archive, u.ä.). Damit sich der Benutzer auf die eingesetzte Anti-Malware Software verlassen kann, gilt es zu verifizieren, dass auch alle Modi eines Komprimierungsformates unterstützt werden.

- Wie reagieren die getesteten Anti-Malware Programme bei Problemen mit komprimierten Dateien ?
  Sollte ein Anti-Malware Programm nicht in der Lage sein, eine komprimierte Datei zu überprüfen, muss dies dem Benutzer gemeldet werden, damit dieser nicht fälschlicherweise die betreffende Datei als nicht-maliziös erachtet.

- Erkennen die getesteten Anti-Malware Programme auch Malware in mehrfach rekursiv gepackten Archiven ?
  Ein ausreichender Schutz durch Anti-Malware Software besteht nur dann, wenn diese auch mehrfach rekursiv gepackte Archive zuverlässig erkennt, da sonst der Schutz durch Anti-Malware Software leicht umgangen werden kann.

Im Rahmen der vorgestellten Testmethodik wird nicht systematisch geprüft, inwiefern die Verfügbarkeit der getesteten Produkte durch denial-of-service Attacken mit bestimmten Archiven gefährdet werden kann (vgl. 1.1, [Bi03]).

2.1 Angewandte Testmethodik

Im anti Virus Test Center (aVTC) der Universität Hamburg werden auf der Grundlage von ethischen Grundsätzen [Br01] in einer abgeschotteten Testumgebung Tests von Anti-Malware Software durchgeführt. Dazu wird eine Testmenge mit Malware auf einem Server bereitgestellt, an der die Testprodukte gemessen werden, indem per Netzwerkzugriff im on-demand Modus[5] die Testmenge überprüft wird. Durch Auswertung der dabei erzeugten Meldungen (Logdateien) werden die Erkennungsrate (Anteil der erkannten Malware), die Erkennungsgenauigkeit (gleiche Identifikation gleicher Varianten) sowie die Erkennungszuverlässigkeit (zuverlässige Erkennung aller infizierten Samples einer Malwarevariante) berechnet.

[5] Um die Güte der Kompressionsunterstützung zu testen, werden im Rahmen der vorgestellten Testmethodik Tests im on-demand Modus durchgeführt. [Si02] hat nachgewiesen, dass die so erzielten Ergebnisse auch für den Einsatz der Produkte im on-access Modus angenommen werden können.

Die Vergleichbarkeit der Produkte wird durch einen festgelegten Stichtag für die Produktversionen und Signaturen erreicht. Damit die erzielten Testergebnisse möglichst objektiv, nachvollziehbar und reproduzierbar sind, werden bei sämtlichen aVTC-Tests alle verwendeten Einstellungen, die verwendete Hardware, die Testumgebung und die Testmethodik ausführlich dokumentiert und veröffentlicht [AV04]. So können die erzielten Ergebnisse jederzeit reproduziert werden.

Die Verzeichnisstruktur im aVTC ordnet die Musterdateien hierarchisch: <Testmenge> \ <Plattform> \ <Bezeichnung> \ <Variante> \ <Objekt>. Zur automatischen Auswertung der von den Testprodukten erzeugten Protokolldateien wird im aVTC die Skriptsprache Perl verwendet. Die Verarbeitung einer Protokolldatei erfolgt in mehreren Schritten:

- Protokolldatei in einheitliches Format umwandeln (Trennung des Protokolls in Pfad des getesteten Objektes, Meldung des Testproduktes, gemeldete Malwarebezeichnung für getestetes Objekt)
- Protokolldatei aufteilen (infiziert gemeldete Dateien, nicht infiziert gemeldete Dateien, übrige Zeilen)
- Erkennungsrate und andere Kriterien ermitteln
- Überprüfung des Protokolls

Ergeben sich bei der Auswertung der Protokolldateien Unstimmigkeiten oder hat ein Produkt nicht alle Objekte der getesteten Testmenge im Protokoll gemeldet, werden diese Objekte bis zu zwei Mal erneut getestet und ausgewertet. Durch dieses wiederholte Testen haben die Testprodukte eine weitere Chance, auch auf diese Objekte zuzugreifen, und andere potentielle Fehlerquellen können minimiert werden.

Aufgrund der speziellen Fragestellungen (s.o.) zum Test von komprimierter Malware wurde die aVTC-Methodik angepasst. Statt der Erkennungsrate ist ausschließlich der Einfluss der Kompressionsformate auf die Erkennungsrate von Interesse, um Aufschluss über die Güte der Unterstützung von Kompressionsformaten zu gewinnen. Deshalb werden die als Testdaten verwendeten Malwaredateien sowohl unkomprimiert (Referenztestmenge) als auch in verschiedenen Kompressionsformaten überprüft. Aus der Differenz zwischen der Erkennungsrate unter Anwendung der jeweiligen Kompression und der unkomprimierten Referenzergebnisse ergibt sich die Qualität der Unterstützung des jeweiligen Kompressionsformats. Die Minderung der Erkennungsrate (in Prozentpunkten) pro Produkt und Kompressionsformat berechnet sich wie folgt:

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

Die Kompressionsformate werden (soweit möglich) auf folgende Arten verwendet, um auch weniger offensichtliche Schwächen der Anti-Malware Produkte zu identifizieren:

- Standard-Kompression[6]
- Die gesamte Referenztestmenge (inkl. Verzeichnisstrukturen) in einem Archiv
- Archivdateien werden umbenannt (generischer Name ohne Dateiendung)
- Erzeugung selbst-extrahierender Archive
- Erzeugung von passwort-geschützten Archiven
- Rekursive Archive: Jeder Komprimierungsvorgang wird 2x bzw. 9x durchgeführt

Unterschiedliche Formatversionen und Spezialmodi einzelner Kompressionsformate[7] werden im Rahmen des hier vorgestellten Tests als einzelne Kompressionsformate betrachtet.

2.2 Testdurchführung

Der Test wurde auf einem isolierten Rechner mit einer lokal verfügbaren Testmenge auf Windows 2000 durchgeführt. Auf die Hypothese, dass die erzielten Testergebnisse auf andere Win32-Betriebssysteme übertragen werden können (z.B. Windows XP), wird im Rahmen dieses Beitrags nicht eingegangen. Entsprechend der Testmethodik des aVTC wurde vor jedem Produkttest ein System-Image des frisch installierten Betriebssystems neu aufgespielt, um Wechselwirkungen der verschiedenen Anti-Malware Produkte auszuschließen.

Insgesamt wurden 25 Anti-Malware Produkte auf die Erkennung in 32 Kompressions- und Archiv-Formaten (inklusive verschiedener Format-Versionen) getestet. In dem hier beschriebenen Test wurden als Referenztestmenge „in-the-wild“ Fileviren[8] verwendet, die in der Wildlist für Oktober 2001 [We01] aufgeführt sind. Durch die Verwendung dieser sich seit 2001 „in-the-wild“ befindlichen Viren ist die Annahme gerechtfertigt, dass nahezu alle Anti-Malware Produkte diese Samples in unkomprimierter Form einwandfrei erkennen können (vgl. [Br02]).

3 Testergebnisse

Im Folgenden sollen einige Ergebnisse des durchgeführten Tests kurz vorgestellt werden. Eine komplette Auflistung aller erzielten Testergebnisse findet sich unter [AV04].

---

[6] Standardkompression des jeweiligen Formates, jeweils alle infizierten Samples einer Malwarevariante in einem Archiv

[7] z.B. Rar: solide Archive

[8] Die Gesamt-Testmenge des aVTC ist nach Plattformen, auf denen die maliziöse Software lauffähig ist, unterteilt. Dementsprechend gibt es Makro-, Skript-, File- und Bootviren als Testmenge. Für den vorgestellten Test von komprimierter Malware wurden File-in-the-wild Viren als Referenztestmenge verwendet. Dem liegt die nicht überprüfte Hypothese zugrunde, dass die getesteten Produkte die maliziöse Software zuerst dekomprimieren und die Dekomprimierungsroutinen sich bei anderen Testmengen (z.B. Skriptviren) ähnlich verhalten.

3.1 Unterstützung von Kompressionsformaten durch die getesteten Produkte

Abbildung 2 zeigt die getesteten Produkte und Kompressionsformate; Abbildung 3 zeigt einen Überblick über die Unterstützung von Kompressionsformaten durch die getesteten Produkte[9]. Eine weiße Zelle bedeutet keine Abnahme der Erkennungsrate gegenüber der unkomprimierten Malware in der Referenztestmenge, das heißt, das entsprechende Format wird ohne Fehler unterstützt und alle unkomprimiert erkannte Malware wird auch unter diesem Format komprimiert erkannt. Das Gegenteil ist bei den dunkelgrauen Zellen der Fall: hier ist die Erkennungsrate um 100 Prozentpunkte abgefallen, d. h. das entsprechende Format wird nicht unterstützt.

Produkte		Kompressionsformate	
ANT Antivir	PER Per Antivirus	7Z_ 7-Zip	RA1 Rar v1
AVA Avast!	PRO Protector	AC2 Ace v2	RA2 Rar v2
AVG AVG Antivirus System	QHL QuickHeal	ACE Ace v1	RA3 Rar v3
AVK Antiviren Kit	RAV RAV Antivirus	ARC Arc	RAR Rar v3 (solid comp.)
AVP Kaspersky Antivirus	SCN McAfee ViruScan	ARJ Arj	SHA Shell Archive
BDF BitDefender	SWP Sophos Anti Virus	B64 MIME Base64	SQZ Squeeze It
CMD Command Antivirus	VBR VirusBuster	BH_ Black Hole	TAR Tape Archive
DRW Dr. Web	VSP VirScanPlus	BZ2 Bzip2	UC2 Ultra Compressor 2
FIR Fire Anti-virus Kit		CAB Cabinet File	UUE UUEncode
FPR F-Prot for Windows		CMS MS Compress	ZI2 PkZip 6.0 (zip2.04 compatible)
FSE F-Secure		GZ_ Gzip	ZI6 PkZip 6.0
GLA Gladiator Antivirus		HA_ Ha	ZIB PkZip 6.0 (bzip2 comp.)
IKA Ikarus Virus Utilities		HAP Hap	ZID PkZip 6.0 (DCLimplode comp.)
INO eTrust Antivirus		JAR Jar	ZIE PkZip 6.0 (Deflate64 comp.)
NAV Symantec Antivirus		JAV Java Archive	ZIP InfoZip 2.3
NVC Norman Virus Control		LHA Lha	ZOO Zoo
PAV Power Antivirus		PAK Pak	

Abbildung 2: Getestete Produkte und Kompressionsformate

Bei den Ergebnissen in den hell- und mittelgrauen Zellen beträgt die Minderung der Erkennungsrate weder 0 noch 100 Prozentpunkte. Das bedeutet, dass diese Formate von den jeweiligen Produkten zwar prinzipiell unterstützt werden und auch damit komprimierte Malware erkannt wird. Allerdings werden in komprimierter Form weniger Dateien als unkomprimiert erkannt. Dies deutet auf eine schlechte Implementierung der Dekompression in den betroffenen Programmen hin und zeigt eine Schwäche in der Abwehr gegenüber so komprimierter Malware. Auffällig ist, dass kein Produkt im Test alle Modi des Zip-Formates vollständig unterstützt. Bei einigen Modi dieses Formates (ZIB, ZID) haben alle Produkte im Test Probleme bei der Dekompression.

[9] Standard-Kompression, Kompressionsformate in der linken Spalte, getestete Produkte in der ersten Zeile

Minderung der Erkennungsrate								
	0		0,1 - 20		20,1 – 99,9		100	

	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
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																									

Abbildung 3: Minderung der Erkennungsrate bei Standard-Kompression

3.2 Probleme und Auffälligkeiten

Beim Testen komprimierter Dateien ohne Dateiendung zeigte sich, dass einige Produkte Viren nicht erkennen, wenn die Archivdateien lediglich umbenannt wurden (betrifft AVG bei allen unterstützten Formaten sowie CMD und FPR bei „LHA"-Archiven). Bei den passwort-geschützten Archiven interessieren nicht die Erkennungsraten (die wie erwartet durchgängig bei 0% Erkennung liegen), sondern die Meldungen der Anti-Malware Produkte. Um eine realistische Einschätzung des Risikos zu ermöglichen, sollte zumindest ein Hinweis gegeben werden, dass diese Archivdateien nicht geprüft werden konnten (darüber hinaus ist auch eine Begründung wünschenswert, warum diese Dateien nicht geprüft werden konnten, etwa „password protected"). Ein erheblicher Anteil der getesteten Anti-Malware Produkte ist dazu aber nicht in der Lage und meldet jede dieser Dateien nur als „nicht infiziert" bzw. als „Ok" (betrifft ANT, AVG, GLA, IKA, INO, PER, PRO, RAV, SCN, VBR, VSP).

Zusätzlich zeigten sich technische Probleme. Viele Anti-Malware Produkte konnten Archivinhalte in der Log-Datei nicht vollständig benennen (ANT, BDF, FPR, GLA, INO, NAV, QHL, SCN). Diese Schwäche zeigte sich insbesondere bei Archiven, die Verzeichnisstrukturen enthielten sowie bei mehrfach rekursiv komprimierten Archiven. Bei einigen Produkten war dieses Verhalten generell zu beobachten (ANT, BDF, GLA, NAV).

Beim Überprüfen der rekursiv komprimierten Archive waren deutliche Stabilitätsprobleme festzustellen (FSE, NVC, PRO, SCN stürzten wiederholt ab). Von den wenigen Produkten die Archive im „HA"-Format unterstützen, benötigten einige sehr lange (in der Größenordnung mehrerer Stunden) zum Scannen eines „HA"-Archivs (betrifft RAV und AVK[10]).

4 Zusammenfassung

Durch Nichterkennung von maliziöser Software in komprimierter Form können Risiken entstehen, auch beim Einsatz von Anti-Malware Software im on-access Modus. Um eine Aussage über die Erkennungsgüte von Anti-Malware Produkten hinsichtlich komprimierter Malware machen zu können, wurde eine hierfür entwickelte Testmethodik vorgestellt.

Bei der Durchführung eines Tests von Anti-Malware Software mit der vorgestellten Methodik zeigt sich, dass erhebliche Schwächen bei fast allen getesteten Produkten bestehen. Insbesondere beunruhigen die Testergebnisse, bei denen ein Format von einem Produkt zwar unterstützt wird, jedoch eine Minderung der Erkennungsrate gemessen wurde. Zusätzlich wurden Mängel bei einem Großteil der getesteten Software bei der Meldung von nicht überprüften komprimierten Dateien festgestellt sowie diverse andere Schwachpunkte aufgezeigt (vgl. [AV04]).

[10] Da AVK intern u.a. die Scan-Engine von RAV verwendet, handelt es sich vermutlich um eine einzelne Schwäche dieser Scan-Engine.

Literaturverzeichnis

[AV04] anti Virus Test Center, Hompage, 2004, www.avtc.info

[Bi03] Bieringer, P.: bzip2 bomb vulnerability of antivirus decompression engines, 2003, http://www.aerasec.de/security/advisories/txt/bzip2bomb-antivirusengines.txt

[Br01] Brunnstein, K.: avtc code of conduct, 2001, ftp://agn-www.informatik.uni-hamburg.de/pub/CodeConduct/CoC-016.txt

[Br02] Brunnstein, K.: avtc test report 2002-12, 2002, http://agn-www.informatik.uni-hamburg.de/vtc/en0212.htm

[Br03] Brunnstein, K.: avtc test report 2003-04, Evaluation WinXP, 2003 ftp://agn-www.informatik.uni-hamburg.de/pub/texts/tests/pc-av/2003-04/7evalwxp.txt

[Si02] Siekierski, U.: methods and procedures for quality assessment of AntiMalware products, especially on access scanners, Diplomarbeit, Fachbereich Informatik, Universität Hamburg, 2002

[We01] Wells, J.: PC Viruses in the Wild – Sep/Oct 2001, http://www.wildlist.org/WildList/200110.htm