Anhang C - Zeitreihen der Erkennungsrate

Zusätzlich zu den in Kapitel 7 (vgl. 7.3.1) dargestellten Zeitreihen der Erkennungsrate von nichtviraler Malware (File-Mal und Makro-Mal) werden in diesem Anhang weitere, durch die Datenbank VTED erstellte Zeitreihen von VTC-Testergebnissen wiedergegeben[1]. Die angegebenen Zeitreihen sind in dieser Form bisher nicht veröffentlicht worden und veranschaulichen die Entwicklung der Erkennungsrate einzelner Produkte auf den spezifischen Datenbanken. Im einzelnen werden folgende Zeitreihen der Erkennungsrate wiedergegeben:

Die Zeitreihen zu den Boot- und File-Datenbanken enthalten weniger Spalten, da diese Datenbanken nicht in jedem VTC-Test getestet wurden (ab dem Jahr 2000 nur noch einmal pro Jahr). Die Datenbanken Poly und VKit werden erst seit VTC-Test 1999-03 getestet, Skript-ITW erst seit Test 2001-04. Dementsprechend enthalten diese Tabellen noch weniger Spalten.

Die Zeitreihen betrachten alle die Ergebnisse unter dem Betriebssystem DOS, da dieses als längstes im VTC getestet wird. Es lassen sich mit der Datenbank VTED aber auch Zeitreihen der anderen getesteten Betriebssysteme beliebiger getesteter Datenbanken erstellen.

[1] Zur Erläuterung des Inhalts und der Aussage von Zeitreihen siehe Abschnitt 7.3.1

C.1 Zeitreihen der Erkennungsrate von Boot-ITW Viren unter DOS

Abkürzung	1997-02	1997-07	1998-02	1998-10	1999-03	1999-09	2000-04	2001-04
al4	93,4	93,6	89,4					
ANT			96,5	83,6			100	
AVA					98,7	100	100	
AVG	75,8	96,8	96,5	98,6	100	92,9		100
AVK				99	100			100
AVP	85,7	100	100	99,5	100	100	100	100
AVS	93,4	92,6		99,5				
CMD						100	100	
DRW	80,2	95,7	97,6	98,6	98,7	100	100	100
dsa	100	100						
DSS			100	100	100			
FPR	98,9	97,9	100	97,1	100	100	100	100
FSE			100	99,5	100	100	100	
IBM		97,9	100					
INO			100	99	100	100	100	100
IRI			68,2					
IRS					100			
ITM	11	5,3		91,8	97,4			
MR2						92,9		
NAV	96,7	96,8	100		98,7	100	100	100
NOD					100	100	100	
NVC	97,8	98,9	100	98,1	100	100	100	100
PAN			94,1					
PAV		100	100		100	100	100	100
pcv	79,1							
PRO					65,8			
RAV				85,5				
SCN	96,7	100	100	99,5	100	100	100	100
SWP	100	100	98,9	99		100	100	
TBA	97,8	98,9	100	97,1				
TNT	84,6							
TSC			88,2		96,1	92,9		
vb4		6,4						
VDS		93,6	96,5					
VET		6,4			6,6			
vht	62,6							
VSA			96,5					
VSP				62,3	63,2	92,9		
VSW			96,5					

Tabelle C.1: Zeitreihen der Erkennungsrate für Boot-ITW Viren unter DOS in VTC-Tests seit 1997

C.2 Zeitreihen der Erkennungsrate von Boot-ZOO Viren unter DOS

Abkürzung	1997-02	1997-07	1998-02	1998-10	1999-03	1999-09	2000-04	2001-04
al4	93,6	95,4	85,5					
ANT			71,3	63,3			93,7	
AVA					95,3	97,8		
AVG	70,9	70,4	74,4	81	81,6	73,9		85,2
AVK				99,5	99			99,1
AVP	64,8	99,3	96,9	99,9	98,2	99,9	100	99,2
AVS	60,9	71		98,2				
CMD						92,6	99,9	
DRW	44,3	74	76,9	91,5	93,4	97,3		
dsa	99,8	99,5						
DSS			96,8	99,9	99,1			
FPR	85	82,5	83,4	89,7	92,4	97,3	99,9	97,2
FSE			99	99,9	99	99,7	99,7	
IBM		94,5	91					
INO			20,3	92,7	96,7	94,1	98,1	97,2
IRI			23					
IRS					91,3			
ITM	12,9	38		75,6	61,7			
MR2						71,5		
NAV	66,9	67,1	93,4		94,3	96,4	89,2	95,9
NOD					99,1	98,5	100	
NVC	86	91,4	93,5	93,8	97,8	97	99,9	98,2
PAN			45,6					
PAV		99	96,9		99	98,5	99,8	99,4
pcv	40,5							
PRO					28,3			
RAV				58				
SCN	82,5	95,3	91	94,2	84,8	99,9	84,3	82,7
SWP	94,8	92,6	92,3	97,5		99,1	99,4	
TBA	78,6	77,4	72,5	86,7				
TNT	45,1							
TSC			60,1		62,2	55		
vb4		8						
VDS		45,5	42,5					
VET		9,7			12			
vht	36,4							
VSA			40,1					
VSP				50,2	58,9	71,3		
VSW			40,1					

Tabelle C.2: Zeitreihen der Erkennungsrate für Boot-Zoo Viren unter DOS in VTC-Tests seit 1997

C.3 Zeitreihen der Erkennungsrate von File-ITW Viren unter DOS

Abkürzung	1997-02	1997-07	1998-02	1998-10	1999-03	1999-09	2000-04	2001-04
al4	100	100	90,8					
ANT			94,9	93,4			89,7	
AVA					100	100	100	100
AVE		97,5						
AVG	85,6	98,3	93,9	99,2	100	100		100
AVK				100	79,3			100
AVP	100	100	100	100	100	100	100	100
AVS	94,9	95,8		99,2				
CMD						100	100	
DRW	97,5	100	100	99,2	100	100	100	100
dsa	100	100						
DSS			100	100	100			
FPR	99,2	100	100	99,2	100	100	100	100
FSE			100	100	100	100	100	
IBM		100	100					
INO			90,8	99,2	100	95,7	100	100
inv	36,4							
IRI			94,9					
IRS					82,8			
ITM		97,5	96,9	90,2	96,6			
MR2						87		60
NAV	99,2	100	100	97,5	92	100	100	100
NOD					100	100	100	
NVC	88,1	99,2	96,9	100	100		100	100
PAN			94,9					
PAV		100	100		78,2	100	100	100
pcv	72,9							
PRO					67,8			
RAV				97,5				
SCC		100						
SCN	98,3	100	100	98,4	100	100	100	100
SWP	100	100	100	100		100	100	
TBA	100	100	99	99,2				
TNT	91,5							
TSC			73,5	9,9	80,5	87		
vb4	73,7	87,3						
vbs	85,6			84,4				
VDS		87,3	82,7					
VET		99,2			93,1			
VIT							46,2	
VSA			96,9					
VSP				80,3	79,3	78,3	61,5	45
VSW			96,9					

Tabelle C.3: Zeitreihen der Erkennungsrate für File-ITW Viren unter DOS in VTC-Tests seit 1997

C.4 Zeitreihen der Erkennungsrate von Makro-ITW Viren unter DOS

Abkürzung	1997-02	1997-07	1998-02	1998-10	1999-03	1999-09	2000-04	2000-08	2001-04	2001-10
al4	100	89,2	66,7							
ANT			83,3	72			97,5	97,8		99,3
AS7		97,3								
AVA					100	100	98,8		99,3	99,3
AVE		81,1								
AVG	27,3	83,8	75,8	100	100	100			100	100
AVK				100	100			100	100	100
AVP	100	100	100	100	100	100	100		100	100
AVS	81,8	94,6		100						
CMD						100	100	100		100
DRW	95,5	100	100	100	100		100	99,3	100	100
dsa	100	100								
DSS			100	100	100					
FMA	100	100								
FPR	72,7	59,5	100	100	100	100	100	100	100	100
FSE			100	100	100	100	100			
FWI	100									
FWN		91,9	87,9	86,7						
HMV			98,5	100	100					
IBM	95,5	94,6	100							
IMS		86,5								
INO			98,5	100	100	100	100	100	99,3	
IRI			87,9							
IRS					92,8					
ITM	100		89,4	97,3	98,8					
MR2						66,1			10,2	
NAV	100	97,3	100	100	100	100	98,8	97,8	94,6	100
NOD					100	100	100			
NVC	9,1	94,6	100	100		100	100	100	100	
PAN			97							
PAV		100	100		100	100	100		100	100
PCC		97,3								
PRO					91,6	42,4				
RAV				100	100					100
SCN	100	100	100	100	100	100	100	100	100	100
SWP	95,5	100	100	100		100	100			
TBA	90,9	94,6	100	100						
TNT	90,9									
TSC			83,3	6,8	89,2	66,1				
VDS	27,3	21,6	19,7							
VET		94,6	100	100	100					
VIT	4,5						8,8			
VRX	13,6									
VSA			90,9							
VSP						0	0		0	0
VSW			90,9							

Tabelle C.4: Zeitreihen der Erkennungsrate für Makro-ITW Viren unter DOS in VTC-Tests seit 1997

C.5 Zeitreihen der Erkennungsrate von Skript-ITW Viren unter DOS

Abkürzung	2001-04	2001-10
ANT		100
AVA	100	94,7
AVG	100	100
AVK	100	100
AVP	100	100
CMD		100
DRW	100	100
FPR	100	100
INO	93,8	
MR2	87,5	
NAV	75	100
NVC	100	
PAV	100	100
RAV		94,7
SCN	100	100
VSP	87,5	89,5

Tabelle C.5: Zeitreihen der Erkennungsrate für Skript-ITW Viren unter DOS in VTC-Tests seit 2001

C.6 Zeitreihen der Erkennungsrate von polymorphen Viren unter DOS

Abkürzung	1999-03	1999-09	2000-04	2001-04
ANT			100	
AVA	100	100	100	100
AVG	100	100		100
AVK	100			100
AVP	100	100	100	100
CMD		100	100	
DRW	100	100	100	100
DSS	100			
FPR	100	100	100	100
FSE	100	100	100	
INO	100	100	100	100
IRS	100			
ITM	100			
MR2		100	83,3	100
NAV	100	100	100	100
NOD	100	100	100	
NVC	100	100	100	100
PAV	100	100	100	100
PRO	37,5			
SCN	100	100	100	100
SWP		100	100	
TSC	75	100		
VET	100			
VIT			66,7	
VSP	100	100	100	

Tabelle C.6: Zeitreihen der Erkennungsrate für polymorphe Viren unter DOS in VTC-Tests seit 1999

C.7 Zeitreihen der Erkennungsrate von VKit-generierten Viren unter DOS

Abkürzung	1999-03	1999-09	2000-04	2001-04
ANT			100	
AVA	100	100	100	100
AVG	83	92,1		94,7
AVK	100			100
AVP	100	100	100	100
CMD		100	100	
DRW	100	100	100	100
DSS	100			
FPR	100	100	100	100
FSE	100	100	100	
INO	100	100	100	100
IRS	94,5			
ITM	83,3			
MR2		100		100
NAV	44,8	99,9	99,9	99,9
NOD	98,1	99,8	100	
NVC	100	100	100	100
PAV	100	100	100	100
PRO	1,8			
SCN	100	100	100	100
SWP		100	100	
TSC	100	100		
VET	91,9			
VIT			1,8	
VSP	99,4	99,4	99,4	99,4

Tabelle C.7: Zeitreihen der Erkennungsrate für VKit-generierte Viren unter DOS in VTC-Tests seit 1999