AV-Test: Test von Anti-Virus-Software

Andreas Marx
AV-Test GmbH
(www.av-test.de)

Inhalt

- Kurzvorstellung AV-Test GmbH
- Tests von Sicherheitssoftware
- Hauptteil: Wie testet man einen Scanner?
- Vorstellung eines aktuellen Projektes
- Fragen und Antworten

Kurzvorstellung AV-Test GmbH

- Gründung zum 01.01.2004
  - vormals bekannt als GEGA IT-Solutions GbR
- Firmensitz: Magdeburg, Klewitzstr. 6
  - ca. 205 m², 50+ PCs und 10 Server (15+ TB)
- Malware-Sammlung mit über 2 Mio. Dateien (95 GB)
- Momentan 4 feste und 10 freie Mitarbeiter
- Kunden: ca. 45 Zeitschriften weltweit (Tests), sowie große Unternehmen (Beratung)
- Zusammenarbeit mit dem TÜV Saarland (Tekit)

Testvorraussetzungen

- Man muss vorher wissen, was man tun will → detaillierter Testplan
- Man benötigt eine sichere, von allen externen Netzwerken (wie dem Internet) getrennte Testumgebung → Testnetzwerk
- Detaillierte Kenntnisse über Malware erforderlich → „Reverse Engineering Skills“
- Malware ist kein Spielzeug!

Wie testet man einen Scanner? (I)

- Der Klassiker: Erkennungsraten
  - Virenscanner sollen Viren erkennen…
  - Einfachste Testmethode: Man scannt eine vorher zusammengestellte Malware-Datenbank durch
  - Unterscheidung nach WildList- und Zoo-Tests
  - On-Demand (Scanner) vs. On-Access (Wächter)
  - Kaum noch aussagekräftig (99,5 vs. 99,7%)
  - Malware-Datenbanken oft schlecht gewartet

Wie testet man einen Scanner? (II)

- Das Gegenstück: Fehlalarm-Tests
  - Eher selten berücksichtigt, obwohl Scanner mit vielen Fehlalarmen nicht für die Praxis taugen
  - Möglichst große Datenbank an „bekanntermaßen guten/ harmlosen Dateien“
  - Quellen: CDs, DVDs, Spiegel von FTP-Servern
  - Sortiert nach Priorität (Schweregrad eines Alarms, z.B. bei einer Windows-Systemdatei)

Wie testet man einen Scanner? (III)

- In den heutigen Tagen wichtig: Reinigung
  - Kaum endender Malware-Strom
  - Malware mit Selbstschutz-Techniken, die besser sind als die gleichen Funktionen der AV-Produkte
  - System infizieren und Reinigungsfunktion testen
  - Wichtig: Werden alle Dateien und die Windows-Registry korrekt behandelt?
  - Extrem aufwendiger und zeitintensiver Test

Wie testet man einen Scanner? (IV)

- Noch wichtiger: Vorbeugung (Prävention)
  - Welche Techniken bieten die Produkte, um die Infektion durch eine dem Scanner noch unbekannte Malware zu verhindern?
  - Stichwort: Anwendungskontrollmechanismen
  - Prinzip: Malware starten und „beobachten“
  - Wichtig: Die Testumgebung muss für die Malware möglichst „real“ aussehen (Internet-Simulation)

Wie testet man einen Scanner? (V)

- Outbreak-Reaktionszeitmessungen
  - Frage: Ab wann war ich geschützt?
  - Aufbau eines Archiv mit allen AV-Updates (Signaturen, Engines, Programmdateien)
  - Multi-Scanner-System (über Skripte)
  - Test aller archivierten Updates gegen die verschiedenen Scannerversionen
  - Heuristische Erkennungen, Reaktionszeiten und Namensänderungen feststellbar

Aktuelles Projekt: Cross-Referenzlisten von Virennamen

Dateiname	AVG	AntiVir	BitDefender
MYTBAB.EXE	I-Worm/Mytob.Z	Worm/Mytob.AB	Win32.Worm.Mytob.S
MYTBAE.EXE	I-Worm/Mytob.BB	Worm/Mytob.BM	Win32.Worm.Mytob.FE
MYTBAH.EXE	I-Worm/Mytob.AE	Worm/Mytob.AH	Win32.Worm.Mytob.X
MYTBAL.EXE	I-Worm/Mytob.AL	Worm/Mytob.BF	Win32.Worm.Mytob.AC
MYTBAM.EXE	I-Worm/Mytob.AC	Worm/Mytob.BF	Win32.Worm.Mytob.V
MYTBAN.EXE	I-Worm/Mytob.AM	Worm/Mytob.BF	Win32.Worm.Mytob.AN
MYTBAR.EXE	I-Worm/Mytob.AP	Worm/Mytob.BA	Win32.Worm.Mytob.AA
MYTBAU.EXE	I-Worm/Mytob.AK	Worm/Mytob.AU	Win32.Worm.Mytob.Y
MYTBAW.EXE	I-Worm/Mytob.AQ	Worm/Mytob.AW	Win32.Worm.Mytob.AB
MYTBAX.EXE	I-Worm/Mytob.AR	Worm/Mytob.AX	Win32.Worm.Mytob.AA
MYTBBB.EXE	I-Worm/Mytob.AU	Worm/Mytob.BG	Win32.Worm.Mytob.AE
MYTBBD.EXE	I-Worm/Mytob.AS	Worm/Mytob.BE	Win32.Worm.Mytob.AB
MYTBBI.EXE	I-Worm/Mytob.FW	Worm/Mytob.ED.1	Win32.Worm.Mytob.BC
MYTBBJ.EXE	I-Worm/Mytob.AI	Worm/Mytob.AS	Win32.Worm.Mytob.T
MYTBBL.EXE	I-Worm/Mytob.BF	Worm/Mytob.BR	Win32.Worm.Mytob.M
MYTBBM.EXE	I-Worm/Mytob.BO	Worm/Mytob.BW	Win32.Worm.Mytob.AF

Fragen & Antworten

- ???

- Literaturhinweis:
  - http://www.av-test.de → Tests → Papers