

# Früher war alles besser ...



Früher gingen virtuelle Ganoven mit relativ einfach gestrickten Methoden vor, um ihre finsternen Ziele zu erreichen. In den letzten Jahren aber hat sich die kriminelle Online-Branche zunehmend kommerzialisiert und ihre Angriffsversuche sind dabei immer professioneller und ausgefeilter geworden. Das macht es umso schwerer, sie zu bekämpfen.

# W

enn die Altvorden ein Loblied auf vergangene Zeiten anstimmen, fällt es, zumindest wenn es um das Thema IT-Sicherheit geht, schwer, ihnen zu widersprechen: Vergleicht man die Bedrohungslage früherer Jahre mit heutigen Zuständen, wirken die damals benutzten Angriffsmethoden noch relativ naiv und amateurhaft. So war zum Beispiel ein kleines Script in einer ansonsten praktisch leeren E-Mail bereits völlig ausreichend, um dem „I-love-you-Virus“ zu einem durchschlagenden Erfolg zu verhelfen. Mittlerweile reichen die Strategien der Cyberkriminellen von der gefälschten Antivirus-Software bis zum ebenso gefälschten Schreiben der Staatsanwalt-

schaft. Cybercrime ist persönlicher geworden, immer häufiger suchen sich die Verantwortlichen eine recht genau definierte Zielgruppe aus. Angriffsmedium und Inhalte sind optimal auf den Empfänger zugeschnitten.

## GEFÄLSCHTE SOFTWARE

Mit Malware Geld zu verdienen, ist kein neuer Trend mehr. Und auch 2009 fanden die Cyberkriminellen wieder neue Variationen des Themas. Auffallend häufig wurde versucht, gefälschte Antivirus-Software an den Mann zu bringen. Die Programme funktionierten immer nach dem gleichen Muster: Zunächst nutzen sie entweder Sicherheitslücken im Browser oder Betriebssystem aus, um auf

dem Computer aktiv zu werden, manchmal bieten auch gehackte legitime Webseiten die Programme als echte Antivirus-Software an. Einmal auf dem PC aktiv, täuschen sie einen Systemscan vor und finden dabei selbstverständlich haufenweise Schadprogramme – außer sich selbst, versteht sich. Dass die Meldungen allerdings gefälscht sind, merkt der Benutzer nur in seltenen Fällen. Er soll zur Desinfektion seines Computers eine Lizenz der Software erwerben. Der Hersteller von Antivirus-Software Kaspersky Lab stellte in einer Analyse fest, dass die Verbreitung solcher gefälschten Antivirus-Programme im Vergleich zu 2008 um etwa 600 Prozent gestiegen ist. Allerdings gehen die Analysten von Kaspersky Lab davon aus, dass diese >

>

The image shows the Spyware Protect 2009 interface. The main window has a blue header with the product name and logo. On the left, there is a sidebar with buttons for 'Perform scan', 'Adjust settings', 'Get updates', 'Activate now', and 'Help & support'. The main area is titled 'Performing scan' and shows the current state as 'Scanning computer'. It displays the file path 'C:\WINDOWS\inf\net559ib.inf' with a total of 1811 items and 22 threats. The malware database status is 'Up to date' with 11345 signature entries. A warning message states: 'Activate Spyware Protect 2009 now to be sure that maximal protection is applied.' Below this is a table of detected threats:

Threat name	Severity	Description (click on item for more information)
L4Pinch V	Critical	A variant of the Key Logger that captures passwords as it
Advanced Stealth Email	Critical	Advanced Stealth Email Redirector (Advanced SER) is a pr
VMalun AWS	High	Trojan: Any program with a hidden intent. Trojans are one
CNNIC Update U	Very high	A program that downloads and may execute or install soft
Bancoos DMD	Critical	A variant of the Key Logger that captures passwords as it

At the bottom of the main window, a progress bar shows 'Scan progress' at 41% completed. A warning box at the bottom left states: 'Your PC is currently unprotected and may be exposed to spyware adware, trojans and viruses. Get full real-time protection.' A dialog box titled 'AntiMalware 2009' is overlaid on the bottom, asking 'Do you want to activate AntiMalware 2009?'. It has two buttons: 'Yes activate AntiMalware 2009 (Recommended)' and 'No, continue unsecure (Dangerous)'. The 'No' button has a red background and contains the text: 'Continue to web site and allow to virus to send your credit cards details to remote host.'

FALSCHER FUZZIGER: Einmal auf dem PC aktiv, täuscht eine gefälschte Antivirus-Software einen Systemscan vor und findet dabei haufenweise Schadprogramme – außer sich selbst.