

Malware-Prognose für das Jahr 2010

Kaspersky Lab prognostizierte für das Jahr 2009 eine Reihe an globalen Malware-Attacken. Leider wurde diese Vorhersage bestätigt: Denn 2009 war geprägt von Rootkits, dem Kido/Conficker-Wurm, Web-Attacken und Botnetzen, SMS-Betrügereien sowie speziellen Attacken auf soziale Netzwerke. Im Jahr 2010 erwartet der IT-Sicherheitsexperte mehr Angriffe auf Filesharing- oder P2P-Netzwerke, raffiniertere und komplexer programmierte Schadprogramme sowie verstärkt Angriffe auf mobile Geräte.

Die Analysten von Kaspersky Lab gehen davon aus, dass Cyberkriminelle im kommenden Jahr neuartige Angriffe auf Internetanwender starten werden. Dabei wird es weniger um Angriffe auf Webseiten und Anwendungen, sondern auf Filesharing- beziehungsweise Peer-to-Peer-Netzwerke (P2P-Netze) gehen. Bereits im Jahr 2009 gab es eine Reihe von Malware-Attacken, bei denen schädliche Dateien zum Beispiel über Torrent-Portale verbreitet wurden. Durch diese Angriffsart wurden Schadprogramme wie TDSS und Virut sowie der erste Backdoor-Trojaner für Mac OS X verbreitet. Kaspersky Lab geht daher davon aus, dass Cyberkriminelle im Jahr 2010 vor allem P2P-Netzwerke angreifen werden.

„Legale“ Botnetze und Rückgang gefälschter Antiviren-Programme

Cyberkriminelle werden weiterhin versuchen, sich gegenseitig Internet-Traffic abzujagen. Die aktuelle Cybercrime-Szene lässt nichts unversucht, um sich einen legalen Anstrich zu verpassen und mit dem durch Botnetze generierten Traffic kann viel Geld verdient werden. Aktuell sind Botnetz-Dienste vor allem auf dem Schwarzmarkt gefragt. Kaspersky Lab geht aber davon aus, dass in Zukunft halblegale Plätze im Internet entstehen werden, über die Botnetz-Dienstleistungen angeboten werden. So genannte "Partner-Programme" werden es Botnetz-Betreibern ermöglichen, mit Spam-Versand, DDoS-Attacken oder Malware-Verbreitung Geld zu verdienen – ohne offiziell ein Verbrechen zu begehen.

Die Kaspersky-Analysten gehen zudem davon aus, dass die Zahl der gefälschten Antiviren-Programme im kommenden Jahr wieder abnehmen wird, ähnlich wie der Rückgang der Gaming-Trojaner im Jahr 2009. Gefälschte Antiviren-Programme traten zum ersten Mal verstärkt im Jahr 2007 auf, 2009 gab es dann den absoluten Höhepunkt (siehe auch <http://www.viruslist.com/de/analysis?pubid=200883672>). Der Grund für den Rückgang: Da der Netzwerk-wurm Kido/Conficker unter anderem ein gefälschtes Antiviren-Programm auf infizierten Computern installiert, ist der Markt an gefälschter Antivirus-Software so gut wie

gesättigt. Daher fallen die Gewinne für Cyberkriminelle in diesem Bereich geringer aus. Außerdem wird diese Betrugsmethode mittlerweile sowohl von IT-Sicherheitsunternehmen als auch von den Strafverfolgungsbehörden verstärkt überwacht. Es wird also immer schwieriger, mit gefälschten Antiviren-Programmen Geld zu verdienen.

Komplexere Schädlinge sowie Angriffe auf Webservices und Smartphones

"Cyberkriminelle werden im Jahr 2010 ihre Schadprogramme noch raffinierter programmieren und einsetzen. Zahlreiche Antiviren-Programme werden daher nur sehr langsam auf die komplexer werdenden, schädliche Dateien und verfeinerten Rootkit-Technologien reagieren können", sagt Alex Gostev, Director des Global Kaspersky Lab Research & Analysis Team. "IT-Sicherheitsunternehmen werden diesem Phänomen mit der Entwicklung von noch komplexer funktionierenden Schutz-Mechanismen begegnen."

Bei Angriffen auf Web-Services werden Cyberkriminelle im Jahr 2010 wohl Google Wave im Visier haben. Angriffe auf diesen neuen Google-Service werden dabei höchstwahrscheinlich wie folgt ablaufen: Zuerst werden Spam-Mails verschickt, dann folgen Phishing-Attacken, abschließend werden Schwachstellen in Programmen missbraucht und Malware verbreitet. Obwohl die geplante Einführung des Netzwerk-basierten Betriebssystems Google Chrome im kommenden Jahr eines der wichtigsten Ereignisse in der IT-Welt sein wird, gehen die Experten von Kaspersky Lab nicht davon aus, dass Chrome in naher Zukunft von Cyberkriminellen massiv angegriffen wird.

Allerdings erwartet Kaspersky Lab im kommenden Kalenderjahr vermehrt Angriffe auf das iPhone und das Android-Betriebssystem für Mobiltelefone. Die ersten Schadprogramme für diese Plattformen wurden bereits im Jahr 2009 entdeckt – ein sicheres Zeichen dafür, dass diese verstärkt in den Fokus der Cyberkriminellen rücken werden. Im Gegensatz zu iPhone-Benutzern, die nur bei infizierten Geräten gefährdet sind, laufen Android-Anwender ständig Gefahr, sich mit Malware zu infizieren. In China wird das Betriebssystem Android immer beliebter, allerdings ist Fremdsoftware auf diesen mobilen Endgeräten in der Regel nicht adäquat geschützt. Die Folge: Cyberkriminelle werden es verstärkt auf Smartphones abgesehen haben, auf denen Android läuft.

Die Hauptursache für Malware-Attacken im Jahr 2010 werden Sicherheitslücken in beliebten Programmen sein. Diese Lücken werden sowohl in Fremdsoftware, wie den Programmen von Adobe oder Apple, als auch bei Windows 7, dem neuen Betriebssystem von Microsoft, auftauchen.