

.04 Viren-Jahresrückblick 2008 von Ikarus

Das Jahr 2008 hat geradezu eine Explosion neuer Schädlinge mit sich gebracht - über 10.000 Millionen "neuer" Files, die potentiell als schädlich bzw. gefährlich eingestuft werden mussten,



wurden von dem heimischen Spezialisten Ikarus Security gezählt. Alleine nackte Zahlen sprechen Bände: mussten im Jahr 2007 noch knappe 8.800 Malware-Codes pro Tag neu registriert werden, vervierfachte sich dieser Wert im abgelaufenem Jahr beinahe. Rund 31.000 neue Viren sind dabei der stolze Tagesdurchschnitt.

Absolute Spitzenreiter dabei sind Trojaner bzw. Trojaner-ähnliche Codes. Der Trend zu mehrstufigen Infektionsverfahren bringt für eine einzelne Attacke mittlerweile schon eine ganze Reihe an unterschiedlichen Modulen mit sich. Bestand ein Trojaner früher zumeist aus zwei Komponenten (einem Master und einem Slave) sind mittlerweile eine Vielzahl unterschiedlichster Programmteile involviert - der "Gewinner" der im vergangenen Jahr von Ikarus Security analysierten Trojanersysteme brachte es dabei immerhin auf stolze 34 Komponenten, was den Trend hin zu komplexen Trojaner-Systemen eindrucksvoll unterstreicht.

Die vielschichtige Motivlage und das "erschließen" immer neuer "Geschäftsfelder" beschert uns auch für das neue Jahr eine ungebrochene Flut an Malwareteilen und Komponenten. Eine genaue Analyse einzelner Systeme wird dabei immer öfter nur mehr anlassbezogen durchgeführt, was das erstellen eines Big-Pictures beinahe unmöglich macht.

Klar im Trend sind auch die Spezialisierung von Attacken. Weg von "unintelligenten" Massenattacken à la Loveletter, Sobig und Co. hin zu kleineren "überschaubaren" Angriffen mit Lokalkolorit. "Exploitbasierend" - also Angriffe unter Ausnutzung von Sicherheitslücken - stehen dabei hoch im Kurs, zumal derartige Attacken keine "direkte Userinteraktion" mehr benötigen und die Chance auf Entdeckung des Angriffes entsprechend verringert.

Immer bessere Tarnfunktionen bzw. die stark zunehmende Kombination von Trojanercode mit Rootkits bzw. genereller Rootkitfunktion lassen auch auf immer "nachhaltigere Bewirtschaftung" von infizierten Systemen schließen. Etwa durch Informations- ("keyword-searcher") und Identitätsdiebstahl. Mit "Mebroot" wurde 2008 dabei ein leistungsfähiges "Bootkit" auf den Markt geworfen, mit dem es möglich ist, jeden beliebigen Code fast unauffindbar auf Festplatten zu verstecken.

Neben PCs sind im vergangenen Jahr verstärkt Web- und MailServer ins Visier der Angreifer geraten. Cross-Site Skripting und SQL-Injektion basierende Attacken haben dabei ebenso rasant zugenommen wie DNS-Cache Poisoning basierende Angriffe - letztendlich aber alle mit dem Zweck Trojaner-Code auf potentiellen Besucher-Systemen auszubringen. "Geknackte" Mailserver hingegen eignen sich wieder sehr gut dafür, Spamfilter andere Nutzer zu unterlaufen.

In überschaubaren Grenzen hielt sich bis heute hingegen die Entwicklung von Trojanern für Handys, daran ändern auch die fleißigen Werbeversuche der Antivirenindustrie nichts. Knappe 450 "Handyviren" wurden überhaupt erst registriert und die Mehrheit davon funktioniert nur unter Laborbedingungen - keinen einzigen Fall wo ein Handy von einem Virus infiziert worden wäre, konnte Ikarus in Österreich registrieren.

Spam konnte trotz kurzfristiger Erfolge in der Eindämmung (einer der führenden Hostingpartner für Spammer wurde vom Netz genommen) nicht nachhaltig reduziert werden - das Gesamtaufkommen an Spammails liegt in Österreich durchschnittlich immer noch über 90 Prozent. Spannend dabei ist, dass rund acht Prozent dieser Mails mittlerweile ausschließlich URLs transportieren die für eine weiterführenden Viren/Trojanerattacke genutzt werden. (rnf/pi)