



Kommentar

Blühendes Geschäft

Das Prinzip ist einfach: „make money fast“ – dies hat in den letzten Jahren wohl zum prägendsten Motivwandel geführt. Waren es früher Neugier oder Geltungsdrang, so hat sich mittlerweile eine effektive Cybercrime-Community gebildet, die sich auch erstaunlich „arbeitssteilig“ organisiert hat. Neben Daten und Informationen werden ganze Infrastrukturen, Software und „Dienstleistungen“ angeboten. Wirft man einen genaueren Blick auf die Infrastrukturen, erkennt man sehr schnell, dass es sich dabei um ein florierendes Geschäft handeln muss – zumal mehrere tausend Server betrieben und unzählige Domains von den Großen der Cyber-Kriminalität kontrolliert werden. Einer modernen Hydra gleich bringt es wenig, eine einzelne Site, einen einzelnen Server oder gar eine Domain zu sperren, da sofort fünf neue statt dessen online gehen.

Eine Konsequenz dieser Entwicklung ist, dass viele Attacken nur mehr teilweise oder gar nicht registriert werden und den potentiellen Angreifern damit „Erfolge“ bescheren, die wiederum zu weiteren Angriffen führen. Ein Kreislauf, der



„Der Kreislauf beginnt sich immer schneller zu drehen.“

Josef Pichlmayr
Ikarus Software

sich immer schneller zu drehen beginnt.

Diese Masse an neuen Malcodes macht es unmöglich, ein „big-picture“ zu zeichnen – also ein Lagebild der Gesamtsituation zu erstellen, zu erkennen, welche Trojaner-Systeme miteinander interagieren oder mit welchen Code-Teilen sie zusammenarbeiten.

So darf es auch nicht verwundern, wenn die Qualität der Attacken um ein Vielfaches gestiegen ist. Neben professionellerer Infrastruktur zeichnen sich die Attacken des vergangenen Jahres durch zunehmende Komplexität aus und sind für Laien in vielen Fällen nicht mehr erkennbar. Ein weiterer guter Grund, seine eigene Sicherheit auch in die Hände von Spezialisten zu legen. Mehr Infos unter

www.myMailwall.at