

Legendäre Gruppe von Virenprogrammierern aufgelöst

Da die Kontakte zwischen den Mitgliedern der berühmt-berüchtigten Gruppe 29A abgebrochen sind, werde die Gruppe nun aufgelöst. Bekannt wurde 29A durch ihre Viren, die die Machbarkeit für verschiedene Plattformen und Betriebssysteme bewiesen.

29A, die berühmt-berüchtigte Gruppe von Virenschreibern, hat sich offenbar aufgelöst. Laut einem Posting des langjährigen Mitglieds Virusbuster auf der 29A-Webseite sind die Kontakte zu den anderen Mitgliedern abgebrochen. Daher werde die Gruppe nun vom letzten Mitglied aufgelöst. Schon im Juli 2007 wurden alle Aktivitäten eingestellt, nachdem es mehrere Austritte aus der Gruppe gab und nur noch drei Virenspezialisten verblieben.

Als einer der Gründe für den Niedergang der Gruppe vermuten Antivirenspezialisten zum einen die fast vollständige Kommerzialisierung der Malware-Szene, die einige der Virenautoren in die Arme der Internet-Mafia treibt. Zudem geschehe es immer häufiger, dass Virenautoren und Botnetz-Betreiber für ihre Aktivitäten ins Gefängnis müssten, was die Attraktivität einer Mitgliedschaft in einer so genannten vX-Gruppe nicht gerade fördere – selbst wenn es sich wie bei 29A (hexadezimal für 666) nur um Amateure handele.

Die Demo-Viren von 29A waren in der Regel wegweisend, da sie die Machbarkeit von Viren für bestimmte Betriebssysteme und Techniken vorführten. Der Smartphone-Virus Cabir beispielsweise wurde von 29A-Mitgliedern programmiert. Ebenso stammten die ersten Viren für Windows 2000, für die 64-Bit-Versionen von Windows und die Alternate Data Stream in NTFS von 29A.

Auch Win32.Winux, ein Schädling, der Windows und Linux befallen konnte, entstand in der Gruppe. Die Schädlinge hatten allesamt keine Schadroutinen, sondern zeigten nur Verbreitungswege und Infektionsmöglichkeiten. Während des Bestehens gab die Gruppe mehrere Online-Magazine mit verschiedenen Artikeln rund um die Programmierung von Viren heraus. Allerdings landete unter anderem das Mitglied Marek "Benny" Strihavka für einen Hack im Gefängnis.