Kaspersky bittet um Mithilfe zum Knacken eines RSA-Schlüssels

Eine neue, bereits kursierende Version des Verschlüsselungstrojaners GPGCode verwendet RSA mit 1024 Bit zur Verschlüsselung von Dateien. Kaspersky will mit Hilfe der Internet-Gemeinde den Schlüssel faktorisieren, um betroffenen Anwendern zu helfen.

News die Meldung vom 09.06.2008

Eine neue Version des Verschlüsselungstrojaners "GPCode" kursiert nach Angaben von Kaspersky derzeit und bereitet den Spezialisten Kopfzerbrechen. (http://www.viruslist.com/en/weblog?weblogid=208187524)

Er verschlüsselt auf einem infizierten Windows-System Dateien mit den Erweiterungen DOC, TXT, PDF, XLS, JPG, PNG, C und viele andere mit dem Verschlüsselungsalgorithmus RC4. Der dafür benutzte Schlüssel ist allerdings mit RSA 1024 geschützt. Betroffene Anwender haben die Wahl, mit dem Autor des Trojaners respektive dem Erpresser Kontakt aufzunehmen und eine Entschlüsselungssoftware zu kaufen oder den richtigen Schlüssel selbst zu finden. Genau das will Kaspersky tun und ruft deshalb in seinem Blog zum Cracken beziehungsweise Faktorisieren des Keys auf.

Nach Meinung der Spezialisten benötige man 15 Millionen moderne PCs und ein Jahr, um den Schlüssel zu finden. Man hoffe auf die Hilfe von Kryptograhpen, Instituten, anderen Antivirenspezialisten und unabhängigen Forschern. In einem eigens der Aufgabe gewidmeten Forum wird derweil schon eifrig diskutiert, wie man am besten vorgeht, denn abgesehen vom Aufruf "Stoppt GPCode" hat Kaspersky selbst noch nicht viel unternommen. Weder gibt es einen Client, einen Server oder eine Bibliothek zum Einbinden, die sich Freiwillige auf den Rechner laden können. Einzig die zwei Public Keys des Trojaner stehen zum Verfügung.

Auch der Einsatz von Grafikkarten zum Berechnen des Schlüssels werden schon diskutiert. Nivida-Karten unterstützen in der aktuellen Generation das Framework Compute Unified Device Architecture (CUDA), mit dem die Grafikkarte parallelisierbare Aufgaben übernehmen kann. Der Hersteller Elcomsoft nutzt diese Möglichkeit in seiner Distributed Password Recovery (DPR), um Windows-NTLM-Passwörter bis zu 25 Mal schneller zu knacken.

Ob Kasperskys Ansinnen von Erfolg gekrönt sein wird, darf man bezweifeln. Zuletzt wurde Ende des Jahres 2005 ein RSA-Schlüssel mit 640 Bit faktorisiert. Ohnehin dürften die wenigsten Betroffenen ein Jahr Zeit haben, um auf die Entschlüsselung ihrer Daten zu warten. Vorherige Versionen von GPGCoder ließen sich relativ leicht knacken, Kaspersky konnte damals schnell Entschlüsselungsroutinen zur Verfügung stellten. Bleibt zu hoffen, dass es sich wirklich um einen Schlüssel handelt, der nur im Trojaner zum Einsatz kommt und nicht eventuell zu einem Server oder einem anderen geschütztem System gehört – bei dem die Teilnehmer unwissentlich mithelfen, es auszuhebeln.

Glücklicherweise scheint der neue Trojaner aber nur vereinzelt aufzutreten. Virenscanner mit aktuellen Signaturen sollten den Schädling schon beim Eindringversuch erkennen. Wie er genau auf den Rechner gelangt, ist bislang aber noch ungeklärt, Kaspersky bittet Anwender, eine genaue Schilderung der Vorgänge kurz vor der Infektion zu schicken.