heise Security

Blurry Box: Anti-Raubkopierer-Dongle knacken - und Preisgeld kassieren

25.04.2017 10:53 Uhr – Uli Ries

(Bild: Screenshot)

Wibu Systems, Anbieter von Produkten zum Sofwareschutz, will Hackern drei Wochen lang Zeit geben, einen neuen USB-Dongle zu knacken. Fällt die Blurry Box genannte Verschlüsselungsmethode, winken 50.000 Euro Preisgeld.

Ab sofort und bis einschließlich 12. Mai können sich interessierte Sicherheitsspezialisten unter **www.blurrybox.com** [**1**] für den dreiwöchigen Hacker-Wettbewerb registrierten. Los geht es am 15. Mai.

Schafft es nur einer der Teilnehmer den Blurry Box getauften Schutzmechanismus auszuhebeln und das damit geschützte Computerspiel ohne den USB-Dongle zu starten, gehören ihm laut dem Ausrichter Wibu Systems 50.000 Euro Preisgeld. Gehen mehrere funktionierende Cracks ein, wird das Preisgeld geteilt. Auch für teilweise funktionierende Lösungswege soll es laut Wibu Systems Geld geben.

Zocken und cracken

Den ersten tausend Interessenten will der Veranstalter einen per Blurry Box geschützten USB-Dongle zuschicken. Die Lizenz zum Starten des eigens für den Wettbewerb in C++ programmierten Spiels ist inklusive. Das Spiel läuft unter Windows (32 Bit und 64 Bit).

Eine Jury bewertet die Einsendungen und will ab 16. Juni die Gewinner bekanntgeben. Zu den Preisrichtern gehört unter anderem **Prof. Dr. Thorsten Holz** [**2**], Vorstandsmitglied am Horst Götz Institut für IT-Sicherheit und Leiter des Lehrstuhls für Systemsicherheit an der Ruhr-Universität Bochum. Er war unter anderem an der Analyse des vom **Krypto-Messenger Signal** [**3**] verwendeten Protokolls beteiligt.

Entwickelt wurde das Blurry-Box-Verfahren von Wibu-Systems, dem Karlsruher Institut für Technologie (KIT) und dem FZI (Forschungszentrum Informatik). Es beruht nach Angaben der Entwickler auf dem Kerckhoffs' Prinzip, welches den Verschlüsselungsalgorithmus offenlegt und nur die im Dongle gespeicherten Schlüssel geheim hält. Der Ansatz ist somit das Gegenteil von Security through obscurity.

Fallen im Code sperren den Dongle

Blurry Box schützt den Programmcode durch insgesamt sieben miteinander verzahnte Maßnahmen. Grundsätzlich bricht es den Code in kleinere Funktionsblöcke auf und verwendet dabei jeweils eigene Schlüssel und AES, um diese Teile zu schützen. Der zum Codieren dieser sogenannten Variant Keys verwendete geheime Schlüssel ist auf dem Dongle gespeichert.

Um ein Entschlüsseln der einzelnen Blöcke durch Cracker zu verhindern, haben die Blurry-Box-Entwickler Fallen eingebaut: Decodiert ein Angreifer einen zu einer Falle gehörenden Variant Key, sperrt sich der Dongle und macht die Lizenz der Software ungültig. Weitere Details zum Verfahren hat Wibu Systems **auf seiner Webseite veröffentlicht** [**4**].

Der Wettbewerb hat das Ziel, Blurry Box auf ihre Standhaftigkeit zu testen. Besteht sie den Test, beziehungsweise sind eventuell gefundene Schwachstellen geschlossen, will Wibu Systems das Verfahren laut eigener Angabe seinen Kunden anbieten. (**des** [**5**])

URL dieses Artikels:
https://www.heise.de/security/meldung/Blurry-Box-Anti-Raubkopierer-Dongle-knacken-und-Preisgeld-kassieren-3693112.html

Links in diesem Artikel:
[1] https://blurrybox.com/enroll-now
[2] https://www.ei.rub.de/fakultaet/professuren/tho
[3] https://eprint.iacr.org/2016/1013.pdf
[4] http://www.wibu.com/de/protection-suite/blurry-box-kryptographie.html
[5] mailto:des@heise.de