Link: https://www.computerwoche.de/a/erpresser-viren-wieder-im-umlauf,2359285

Security

Erpresser-Viren wieder im Umlauf

Datum: 01.12.2010

Laut Sicherheitsexperten ist derzeit eine neue Welle an Erpresser-Trojanern unterwegs. Nutzer sollen zahlen, um Daten wieder zu entschlüsseln.

GpCode ist bei Windows-Nutzern berüchtigt und gefürchtet. Die Malware verschlüsselt Daten und will diese nur mittels Lösegeld wieder freigeben. Kaspersky-Mitarbeiter Vitaly Kamluk hat eine neue Variante - Trojan-Ransom.Win32.GpCode.ax - **gefunden**[1]. Diese funktioniert ähnlich, wie bisherige Versionen. Bestimmte Daten werden mit RSA-1024 und AES-256 verschlüsselt. Diese geben die Erpresser für ein Lösegeld von 120 US-Dollar dann wieder frei.

Kaspersky hat noch eine andere Version eines Erpresser-Virus - Trojan-Ransom.Win32.Seftad.a - entdeckt, die aber wesentlich weniger ausgeklügelt ist. Diese Malware kopiert sich lediglich in den MBR und startet den Rechner neu. Danach verlangt sie ein Lösegeld von 100 Euro. Die Behauptung, dass die Festplatte verschlüsselt ist, ist aber nur ein Bluff. Das gilt auch für die Lösegeldforderung. Anwender können den MBR mittels verschiedener Tools wieder herstellen. Ebenso ist es möglich, die Webseite zu besuchen und das Passwort aaaaaaciip benutzen. (jdo/**TecChannel.de**[2])

Links im Artikel:

[1] **http://www.securelist.com/en/blog/333/GpCode_like_Ransomware_Is_Back**
[2] **https://www.tecchannel.de/**
