CYBERCRIME COMPETENCE CENTER NEWS
INFORMATIONEN · TIPPS · RECHERCHEN · BERICHTE

- **Sollte dieser Newsletter bei Ihnen nicht einwandfrei angezeigt werden, beachten Sie bitte die beigefügte Version als PDF.**

BitCryptor und Coinvault: Möglichkeit der Entschlüsselung von betroffenen Daten

Art der Bedrohung

Mit Erpressersoftware wie BitCrypter und CoinVault (inklusive Cryptographic Locker, CryptoWall, CryptoDefense, CryptorBit und Cryptolocker) über infizierte E-Mail Nachrichten, Exploit Kits und gefälschte Downloads wie bösartige Videoplayer oder gefälschten Flash Aktualisierungen verschlüsselte Dateien.

Modus Operandi

Wie in einer Online-Aussendung von heise.de berichtet, besteht nunmehr die Möglichkeit, dass durch die Ransomware BitCryptor und Coinvault verschlüsselte Daten wieder hergestellt werden können.

Dies ist dem Umstand zu verdanken, dass die Autoren des Verschlüsselungstrojaners am 14.09.2015 in Holland verhaftet wurden. Im Zuge der Ermittlungen gelangten Sicherheitsforscher von Kaspersky in den Besitz der für die Entschlüsselung notwendigen Keys. Die über 14.000 Keys wurden nunmehr in das Tool „Ransomware Decryptor“ von Kaspersky integriert, welches mittels BitCryptor und Coinvault verschlüsselte Dateien automatisch entschlüsseln soll.

Für eine erfolgreiche Wiederherstellung bzw. Entschlüsselung der Daten ist es erforderlich, dass sich der Ihre Daten betreffende Schlüssel unter den aufgefundenen befindet. Weitere Informationen zur Entschlüsselung sowie der Download des Tools können auf der Webseite von Kaspersky (in englischer Sprache) abgerufen werden. Der Link hierfür kann dem rot markierten Artikel über die Programmierung des Decryption-Tools auf securelist.com in der Quellenangabe entnommen werden (To see if you can decrypt your files for free, please go to https://noransom.kaspersky.com).

Empfohlene Vorgangsweisen:

- Die Möglichkeit der Entschlüsselung der Daten bezieht sich vor allem auf jene, welche vor dem 14.10.2015 mit der genannten Ransomware verschlüsselt wurden
- Beachten Sie die Sicherheitshinweise und Tipps, für einen Sicheren Umgang mit dem Internet

und Schutz vor IT-Kriminalität der Kriminalprävention: http://www.bmi.gv.at.

Quelle: Kaspersky.com

Quellen:

- Artikel auf heise.de über „Das Ende von Bitcryptor und Convault“: http://www.heise.de/security/meldung/Das-Ende-von-Bitcryptor-und-Coinvault-Alle-Schluessel-in-Tool-verfuegbar-2866862.html
- Artikel über die Programmierung des Decryption-Tools auf securelist.com: https://securelist.com/blog/research/69595/challenging-coinvault-its-time-to-free-those-files/
- Artikel und Beschreibung der BitCryptor Erpressersoftware und Entfernungsanleitung auf pcrisk.de: https://www.pcrisk.de/ratgeber-zum-entfernen/7806-bitcryptor-virus
- Link zum Ransomware Decryptor von Kaspersky: https://noransom.kaspersky.com/?utm_source=securelist&utm_medium=text&utm_campaign=chttps://noransom.kaspersky.com/?utm_source=securelist&utm_medium=text&utm_campaign=com-securelistom-securelist

HERAUSGEBER: Bundesministerium für Inneres
Bundeskriminalamt
A-1090 Wien, Josef Holaubek Platz 1
Tel.: +43 1 24836 986500

FEEDBACK

NEWSLETTER AN-/ABMELDUNG