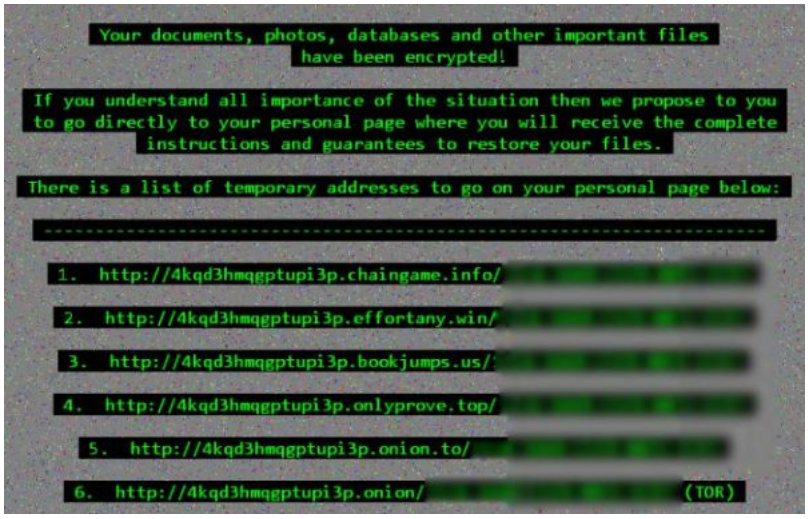
Cerber Ransomware bekommt Cerber-2 Erweiterung

08.08.2016, 16:35 | IT, New Media & Software

Pressemitteilung von: *Virus-Entferner*



Desktopmeldung Cerber 2 Ransomware

Cerber2 Ransomware ist das geänderte Erscheinungsbild vom Erpresser-Cerber-Virus, der Microsoft API CryptGenRandom nutzt, um die Verschlüsselung zu aktivieren und die Dateien, Fotos und Dokumente auf den Computern zu verschlüsseln. Man kann Cerber2 Virus durch Spammails mit einer schädlichen Anhängerdatei aus Versehen herunterladen.

Die kodierten Dateien und Dokumente sind leicht zu erkennen. Sie bekommen nach der Verschlüsselung eine .cerber2 Erweiterung und die Dateinamen werden bis zur Unkenntlichkeit verändert. Zum Beispiel magisterarbeit.doc wird plötzlich zu QsfTr35As.cerber2 geändert.

Nach dem Sie auf eine Fake-Anhänger Datei aus Versehen geklickt haben, fängt der Cerber Virus sich zu verbreiten. Am Anfang merken Sie das nicht. Erst nach dem Neustart wird der Virus sichtbar. Virus stellt sich so ein, dass er beim nächsten Computerstart wieder ausgeführt wird. Der Cerber2 Virus verwendet den sogenannten Doppelstart: zuerst sendet er eine Fehlermeldung und startet den Computer in den abgesicherten Modus mit Netzwerktreiben. Danach startet den Computer ein weiteres Mal, jedoch in den normalen Modus, um den Verschlüsselungsprozess zu beginnen.

Im Unterschied zum Cerber1 wurden im Cerber2 diverse Programmier-Fehler bei der Verschlüsselung beseitigt und der interne Packer ersetzt. Eine Anaylse des Quelltextes der Ransomware wird deutlich erschwert und die Erkennungsrate von installierten Sicherheitssystemen deutlich gesenkt. Es wird auch berichtet, dass Ransomware eine sog. schwarze Liste bei sich trägt, die nach dem Callblocker-Prinzip funktioniert. Das bedeutet, dass nach dem Ransomware ins System gelandet ist, erkennt der Virus die gängigen Antivirus Programme und blockiert sie. Hier werden: Arcabit, Arcavir, Avast, BitDefender, Bullguard, Emsisoft, ESET, eTrust, F-Secure, G Data, Kaspersky Lab, LavaSoft, TrustPort und sogar Vorgängerversionen-Ersteller Shadow Explorer genannt.

Portrait

Das Projekt Virus-Entferner macht es sich zur Aufgabe Computernutzer über Ransomware, Schadsoftware, Adware und andere im Internet kursierende gefährliche Programme zu informieren. Virus-Entferner ist eine grosse Quelle für sicherheitsorientierte Informationen, die für das Verhindern oder Entfernen von Viren wesentlich sind. Wir bieten klare und professionell geschriebene Parasitenbeschreibungen, ausführliche Entfernungsanweisungen, Beurteilungen für Anti-Spyware, Antivirensoftware und vieles mehr.

News-ID: 913929 • Views: 1080 (Stand: 23.05.2026)

Link zur Pressemitteilung:

https://www.openpr.de/news/913929/Cerber-Ransomware-bekommt-Cerber-2-Erweiterung.html