TorrentLocker fordert für Entschlüsselung Lösegeld

Experten warnen vor dem Trojaner „TorrentLocker“: Er verschlüsselt Daten und verlangt ein hohes „Lösegeld“ in der Online-Währung Bitcoin.

Der Trojaner „TorrentLocker“ verbreitet sich per E-Mail, verschlüsselt sämtliche Dateien und verlangt zur Freigabe ein hohes Lösegeld.

Seit Frühjahr 2014 treiben verschiedene Versionen des Verschlüsselungs-Trojaners ihr Unwesen und haben bereits Millionen von Dateien weltweit verschlüsselt. Eine aktuelle Variante der Malware hat es nun nach Angaben des Sicherheitsanbieters ESET auch auf europäische Nutzer abgesehen: In den vergangenen Monaten wurden durch das Schadprogramm über 40.000 Systeme infiziert. Italien hatte mit rund 4.500 Fällen und 53.761.689 betroffenen Dateien die meisten Attacken. In Österreich schlug TorrentLocker 1.504 Mal zu (28.178.401 Dateien), Deutschland rangiert mit 240 Vorfällen und 4.548.853 befallenen Dateien derzeit noch im unteren Mittelfeld.

TorrentLocker reist per Mail

Die Verbreitung erfolgt über Spam-E-Mails, denen eine Datei mit beispielsweise überfälligen Zahlungsaufforderungen, Transportverfolgungen von Paketen oder unbezahlten Strafzetteln wegen Geschwindigkeitsübertretungen, angehängt. Die Ransomware verschlüsselt sämtliche Dokumente, Bilder und andere Dateien auf den infizierten Geräten. Für die Entschlüsselung verlangen die Erpresser ein Lösegeld in der Online-Währung Bitcoin in einem Wert von bis zu 1.100 Euro. Insgesamt sollen 570 Opfer das Lösegeld bezahlt haben, durch den schwankenden Bitcoin-Kurs haben die Erpresser so eine Summe zwischen 220.000 und 468.000 Euro erbeutet.

Malware entwickelt sich weiter

Die Telemetrie des Sicherheitsanbieters erkennt TorrentLocker als Win32/Filecoder.Dl. Der Name ist aus dem Registrierungsschlüssel abgeleitet, den die Malware zur Speicherung der Konfigurationsinformationen mit dem falschen Namen „Bit Torrent Application“ zu Entwicklungsbeginn dieses Filecoders verwendet hat.

Die Code-Analyse brachte die Sicherheitsexperten auf eine Spur: „Wir gehen davon aus, dass die Akteure hinter TorrentLocker die gleichen sind, die hinter der Banking-Trojaner-Malware Hesperbot stecken“, erklärt Marc-Etienne M. Léveillé, ESET Forscher aus Kanada. „Die Angreifer haben darüber hinaus auf die Onlineberichterstattung reagiert und haben die Advanced Encryption Standards (AES) angepasst. Nachdem eine Methode zum Extrahieren des Schlüssel-Streams veröffentlicht wurde, verwenden sie anstelle des Counter Modes (CTR) nun den Cipher Block Chaining Mode (CBC)“, so Marc-Etienne M. Léveillé. Das bedeutet, dass die im Schadensfall bisher angewendete Wiederherstellung des Schlüssel-Streams durch die Kombination einer verschlüsselten Datei mit ihrem Klartext nicht mehr funktioniert. Durch diese Vorgehensweise konnten Opfer ihre Dokumente bislang wiederherstellen.

Der beste Schutz gegen eine digitale Erpressung sind regelmäßige Backups wichtiger Dateien und ein aktuelles Anti-Viren-Programm.
Bezahlen sollte man den geforderten Betrag jedenfalls nicht, denn der Zugriff auf die verschlüsselten Daten ist natürlich nicht gewährleistet.