Weltweite Spamwelle verbreitet teuflische Variante des Locky

blog.botfrei.de/2017/08/weltweite-spamwelle-verbreitet-teufliche-variante-des-locky/

SoSafe August 10, 2017

Es ist wieder soweit, er ist zurück! Der Erpressungstrojaner Locky holt über eine weltweit groß angelegte Spam-Kampagne zum nächsten Streich aus. Wird die Ransomware Locky erneut zum Gobal-Player?

Derzeit sollten wir wieder mit Bedacht unsere E-Mail Postfächer lesen, denn scheinbar erlebt die Ransomware Locky ein absolutes Hoch und wird wieder weltweit kräftig über infizierte Spam-Mails verbreitet. Obwohl der Erpressungstrojaner Locky zu der wohl am meist verteilten Ransomware-Varianten weltweit gehört, taucht diese immer nur sporadisch auf. Andere Ransomware-Trojaner wie der Cerber, Spora, GlobeImposter u.a. machen uns zwischenzeitlich immer häufiger das Leben schwer.

> Schlägt der Erpressungstrojaner Locky zum großen Finale, oder nur ein weiterer Versuch die Welt in Atem zu halten? Experten sind sich derzeit noch nicht einig.

Die **Ransomware Locky mit neuer Variante „Diablo6“** wurde von dem Sicherheitsexperten Racco42 entdeckt und wird hauptsächlich als Zip-Archiv im Anhang einer Spam E-Mail verteilt. Der Inhalt der E-Mail ist in der Regel sehr schlicht gehalten, so heisst es ganz banal „**Dateien angehängt. Danke.**“ Die Betreffzeile beinhaltet z.B. den Namen der im Anhang befindlichen ZIP-Datei, zum Beispiel **E 2017.08.09 (698).docx**.

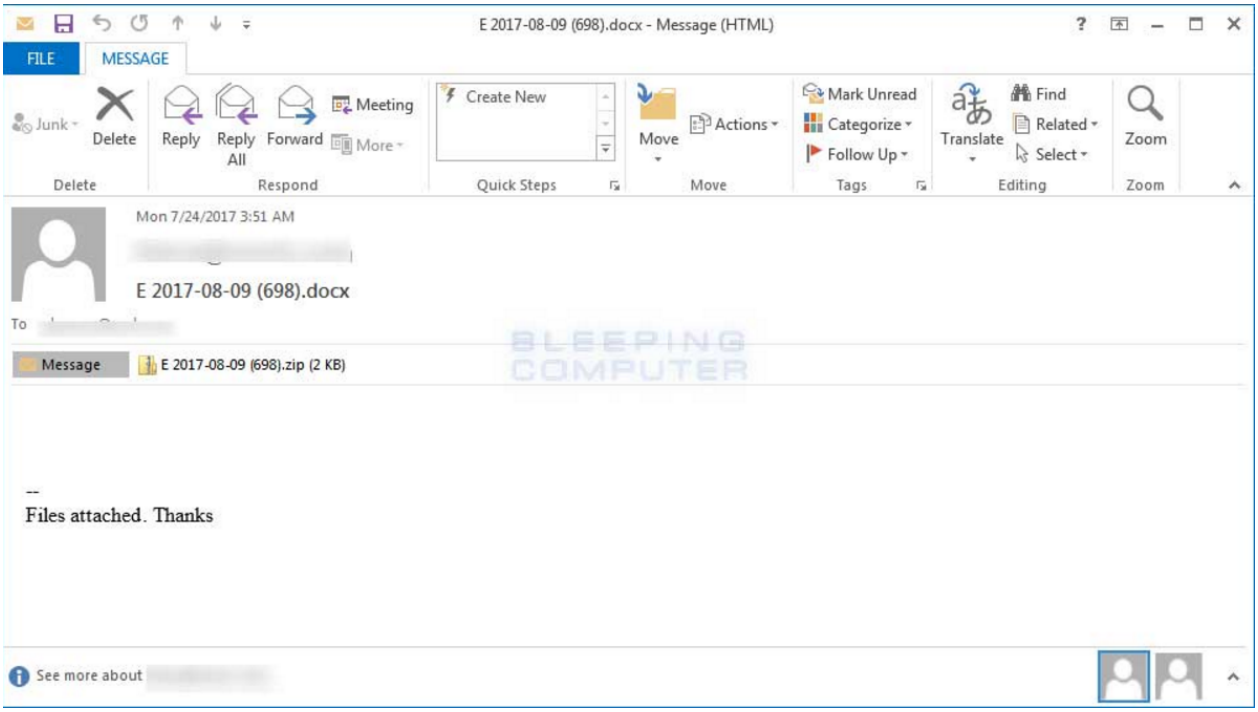

Bild: bleepingcomputer.com – Spam-Mail

Laut den Experten beinhaltet das **Ziparchiv einen VBS-Skript-Downloader**, der nach Ausführung über integrierte URL-Adressen den eigentlichen Locky-Trojaner auf das System herunter lädt und im %Temp%-Verzeichnis ablegt. Durch automatisches Ausführen beginnt der Erpressungs-Trojaner sein verheerendes Spiel!
Kommt die Locky Variante „Diablo6“ so richtig in Fahrt, ist kein Halten mehr. So wird das System nach Dateien durchsucht und diese verschlüsselt. Der Dateiname wird umbenannt und als Erweiterung bekommen die verschlüsselten Dateien „.diablo6“ angehängt. Die Dateinamen können folgende Formate aufweisen: „**[first_8_hexadecimal_chars_of_id] – [next_4_hexadecimal_chars_of_id] – [next_4_hexadecimal_chars_of_id] – [4_hexadecimal_chars] – [12_hexadecimal_chars] .zepto**“

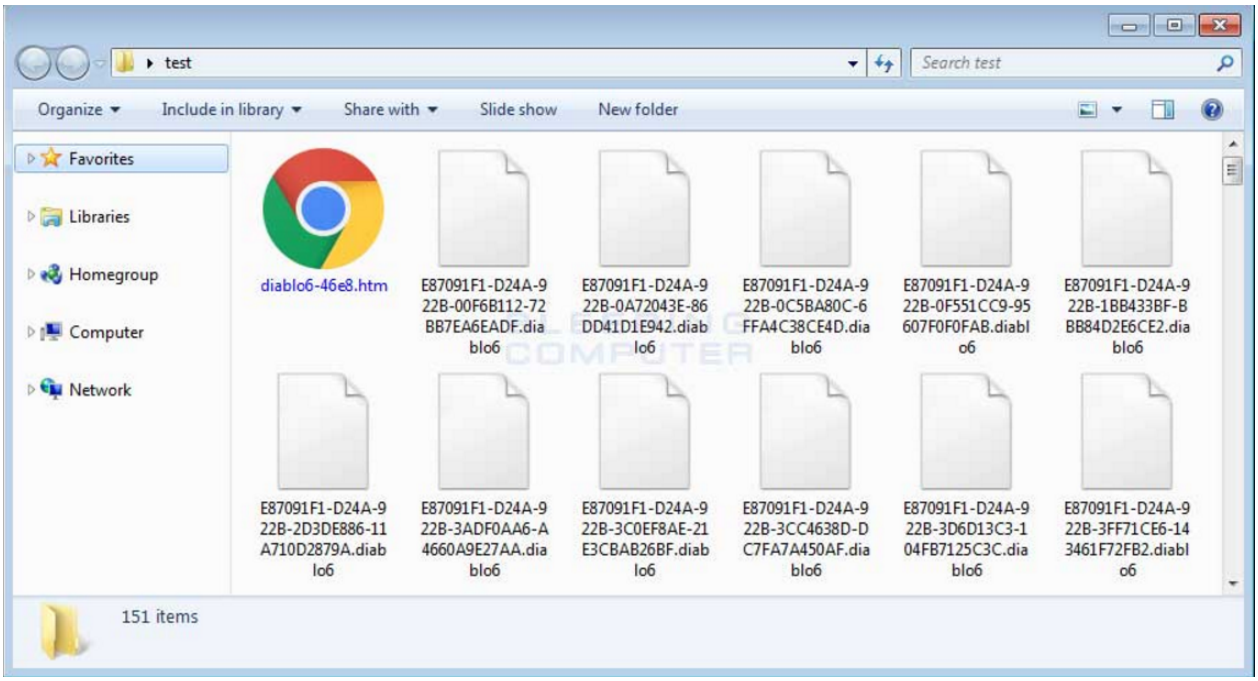

Bild: bleepingcomputer.com – verschlüsselte Dateien

Hat der Locky-Trojaner sein böses Spiel vollendet und damit alle Daten auf dem Rechner verschlüsselt, bereinigt die Malware hinter sich noch alle Spuren, löscht seine ausführbaren Dateien und zeigt großflächig die Lösegeldforderung der Kriminellen. Über diverse Angaben der Zahlungsmodalitäten sollen Opfer über das **Locky Decryptor TOR Bezahlsystem** eine Lösegeldsumme von **.49 BTC oder ungefähr $ 1.600 USD** für die Wiederherstellung der verschlüsselten Daten bezahlen.
[su_custom_gallery source="media: 290118,290119" link="image" target="blank" width="350" height="200" title="never"]

> **Achtung: Kommen Sie niemals der Lösegeldforderung nach** – Angst und Einschüchterung ist die Motivation der Kriminellen: Wir von Botfrei schließen uns der Meinung des BSI, dem BKA und Polizeibehörden an und raten dringend davon ab, hier das Lösegeld an die Cyberkriminellen zu bezahlen!

Leider gibt es derzeit noch keine Möglichkeiten, die über die **Locky Ransomware Variante „Diablo6"** verschlüsselten Daten wiederherzustellen! Die einzige Möglichkeit ist hier das Zurückspielen der letzten Backups. Eine weitere Möglichkeit kann das Herstellen der Daten aus Volumen-Schattenkopien bieten.

Wie können Sie den Rechner gegen Ransomware sicherer machen?

1. Wichtiger denn je, machen Sie **regelmäßig Backups von Ihren wichtigen Daten** und bewahren Sie diese getrennt vom Rechner auf. Schauen Sie sich dazu das kostenfreie EaseUS Todo Backup an. Oder lesen Sie hier, wie Dateien über Windows gesichert werden können>>

2. Deaktivieren Sie Macros in Office, laden Sie Dokumente nur aus vertrauenswürdigen Quellen! Gut zu Wissen: Macro-Infektionen sind in alternativen Office-Anwendungen wie Libre-Office nicht funktionsfähig.
3. **Überprüfen Sie Ihren Rechner** mit unseren kostenfreien EU-Cleanern>>
4. Schützen Sie Ihren Computer vor einer Infektion, indem Sie das System **immer** "**up-to-date**" halten! Spielen Sie zeitnah **Anti-Viren- und Sicherheits-Patches** ein.
5. Ändern Sie die Standardeinstellung von Windows, welche die Datei-Erweiterungen ausblendet>>
6. Seien Sie **kritisch beim Öffnen von unbekannten E-Mails.** Klicken Sie **nicht** auf **integrierte Links**, bzw. öffnen Sie **niemals unbekannte Anhänge.**
7. Arbeiten Sie immer noch am Computer mit **Admin-Rechten**? Ändern Sie die Berechtigungen beim täglichen Arbeiten auf ein Mindestmaß und richten Sie die Benutzerkontensteuerung (UAC) für ausführbare Programme ein.
8. Verwenden Sie unbedingt eine professionelle Anti-Viren-Software, auch auf einem Mac

Betroffene Unternehmen, Behörden und Institutionen sollten sich zudem an das BSI wenden bzw. bei „No More Ransom" über mögliche Hilfen zur Wiederherstellung informieren.

Brauchen Sie dazu Hilfe? Das Botfrei-Team bietet ein kostenfreies Forum an. Experten helfen „Schritt für Schritt" bei der Lösung, Entfernung und nachhaltigen Absicherung des Computers.

> **Darauf sollten Sie im Forum achten:** Damit die Experten auf Sie aufmerksam werden und helfend unterstützen können, sollten Sie sich im **Forum anmelden** und einen Beitrag erstellen, in dem Sie Ihr Problem schildern. Nur dann kann individuell geholfen und die Infektion entfernt werden!

Bilder: bleepingcomputer.com; pixabay.com