ERPRESSUNGSTROJANER

Locky und die Makro-Mafia

Locky haust in Deutschland und legt mächtige Firmen lahm. Meist hat ein Mitarbeiter eine unscheinbare Makro-Warnung in Word übersehen: Tappen Sie nicht in die Falle der Erpresser! ■ WOLF HOSBACH

Ein längst bezwungener Feind taucht plötzlich wieder auf, wie die Pest, die seit Langem als besiegt gilt und mit einem Mal wieder die Schlagzeilen beherrscht, weil sie irgendwo in der Welt ein Dorf ausgerottet hat. So feiern in diesen Wochen die Makroviren ein groteskes Comeback mit Hunderttausenden von Infektionen, die der aggressive wie schlaue Erpressungstrojaner Locky innerhalb von kurzer Zeit erzeugt hat. Und er verschonte dabei auch nicht namhafte Institutionen wie die Fraunhofer Gesellschaft oder eine Reihe nordrhein-westfälischer Krankenhäuser. Genauso wie die Öffentlichkeit bei der Pest haben bei Locky weder Anwender noch Sicherheits-Software mehr mit einem Ausbruch des Übels gerechnet.

Der Grund ist, dass Microsoft vor einigen Jahren die Schutzmechanismen bei Makros drastisch erhöht hat. Einerseits gibt es seit Word 2007 ein eigenständiges Wordmit-Makro-Format (*.docm* statt *.docx*). Und andererseits muss der Anwender die Ausführung eines Makros explizit bestätigen. Eine sichere Sache, so scheint es. Dennoch warnt Microsoft schon seit Anfang 2014 vor einem Wiederanstieg der Bedrohung. Denn die Virenautoren haben in anderer Hinsicht aufgerüstet. Die Mails, in denen sie Locky & Co. verteilen, sind in puncto Social Hacking stark perfektioniert.

In einwandfreiem Deutsch kommt eine Rechnung von einer namhaften Firma per Mail daher. Der Buchhalter sieht keinen Grund, die Mail nicht zu öffnen. Das anhängende Word-Dokument, das durch die auf Makros nicht scharf gestellte Virenerkennung der Firewall geschlüpft ist, ist nach dem Öffnen leer, enthält nur einen gelben Warnhinweis: *Inhalte aktivieren* – und klein daneben: *Makros wurden deaktiviert.* An dieser Stelle werden nur Anwender misstrauisch, die das Konzept Makrovirus aus der Vergangenheit noch kennen. Alle anderen tun das, was im Workflow naheliegend ist: Sie klicken auf *Inhalte aktivieren* im scheinbar leeren Dokument.

So schützen Sie sich vor Erpressern

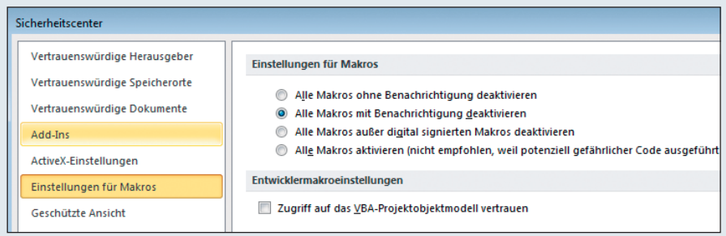
Online-Erpresser haben Konjunktur. Mit ein paar Maßnahmen schützen Sie sich.

☑ **Backup:** Sichern Sie regelmäßig Ihre Daten, dann geht eine Erpressung ins Leere. Wenn Sie ein System-Image anlegen, können Sie dieses einfach zurückspielen. Geeignete Programme sind Ocster oder DriveImage XML.

☑ **Sicherheitssuite:** Nutzen Sie eine Sicherheits-Suite mit Wächter, der im laufenden Betrieb vor Trojanern schützt, wie Kaspersky, Bitdefender, Avira oder Avast.

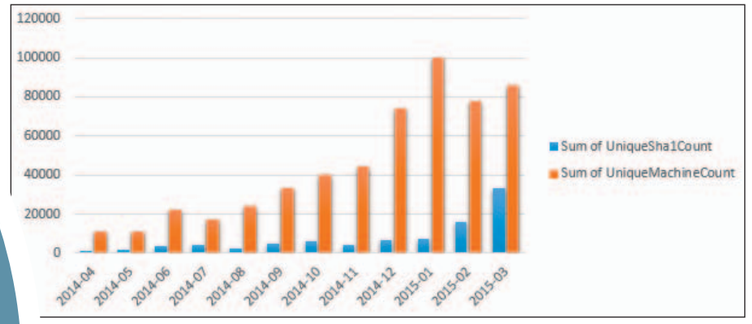
☑ **Vorsicht mit Mail-Anhängen:** Seien Sie prinzipiell misstrauisch bei Mail-Anhängen. Erkundigen Sie sich im Zweifelsfall beim Absender, ob die Mail in Ordnung ist.

☑ **Office-Makros einschränken:** Um sich vor der neuen Makro-Virenwelle zu schützen, achten Sie darauf, dass Office so eingestellt ist, dass Makros nicht automatisch starten (das ist die Grundeinstellung). Im *Sicherheitscenter* oder Trust Center in den Optionen wählen Sie *Alle Makros mit Benachrichtigung deaktivieren.*

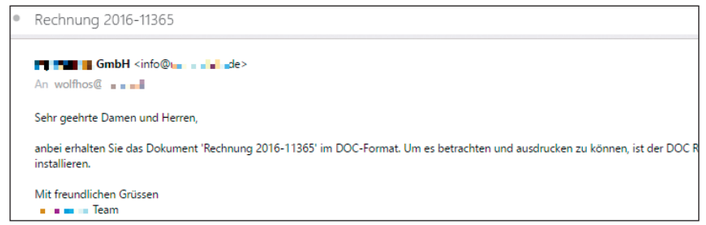


Um sich vor Makroviren zu schützen, stellen Sie Office so ein, dass es Makros nur nach Vorwarnung startet.

Locky blendet seine erpresserische Nachricht als Desktop-Hintergrund auf dem Rechner des Opfers ein.
Quelle: Kaspersky



Microsoft warnt offiziell vor einem steigenden Auftreten von Makroviren (orange nach betroffenen Maschinen, blau nach einzelnen Trojanern).



Locky kommt als Rechnung einer namhaften Firma mit verseuchtem Word-Dokument im Format .docm im Anhang.

Unternehmen im Visier

Andere Locky-Varianten tarnen sich als Fax oder als gescanntes Bild im Mail-Anhang, die Zielrichtung Büro und Unternehmen ist klar ersichtlich. Hat der Mitarbeiter das Makro erlaubt, lädt es die eigentliche Schadsoftware aus dem Netz und startet sie. Der Trojaner beginnt alle Dokumente, Bilder, Mediendateien oder Web-Dateien zu verschlüsseln, fatalerweise auch auf Netzlaufwerken, was gerade in Firmen großen Schaden anrichtet. Die Dateien bekommen die Endung .locky, und im geschredderten Verzeichnis liegt eine Textdatei *Locky_recover_instructions.txt*, die die Erpresser-Nachricht enthält: *Alle Dateien sind mit RSA 2048 und AES-128 Chiffre verschlüsselt … Entschlüsseln von Dateien ist nur mit dem privaten Schlüssel und einem Entschlüsselungsprogramm möglich, das auf unserem geheimen Server liegt.* Diesen Text blendet Locky nach getaner Arbeit zusätzlich auf dem Desktop-Hintergrund ein. Das Opfer soll einen anonymen Server im Tor-Netzwerk aufsuchen, wo die Erpresser ihn auffordern, 0,5 bis 1 Bitcoin zu zahlen, um den Locky-Encryptor zu erhalten. Der Kurs für einen Bitcoin schwankt zwischen 250 und 500 Euro. Haben Opfer kein Backup, wird ihnen nichts anderes übrig bleiben, als diesen Weg zu gehen (siehe Kasten *Infiziert – was tun?*), denn bisher ist die Verschlüsselung von Locky nicht geknackt. Sie macht es den Sicherheitsexperten besonders schwer, da der Trojaner den Schlüssel nicht lokal erzeugt, sodass man dessen Anfangspunkt beobachten und den Schlüssel reproduzieren könnte. Sondern Locky bezieht einen asymmetrischen RSA-Schlüssel aus dem Botnetz und nutzt eine eigene, solide Crypto-Infrastruktur.

Dark Business

Erpressungstrojaner – oder auch Ransomware genannt – sind nach wie vor das Big Business im Dark Web. Sowohl organisierte Banden als auch Einzeltäter tummeln sich hier, denn das erforderliche Know-how ist gering, das Risiko niedrig, die Ausbeute

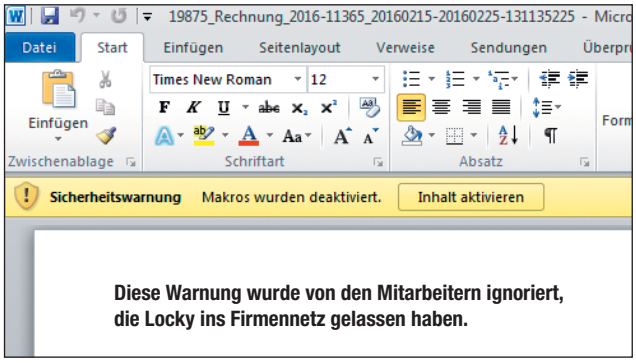
hingegen attraktiv. Locky wirkt aufgrund der Durchschlagskraft des Angriffs eher professionell. Außerdem sind die Komponenten von Locky den Sicherheitsexperten wohlbekannt und weisen in Richtung organisiertes Verbrechen. Forscher von Paloalto Networks (**bit.ly/1R3YVhW**) erkannten im Makro-Downloader *Bartallex* und im Hintergrund das *Dridex*-Botnetz, das in den letzten Jahren durch massive Angriffe mit Banking-Trojanern bekannt wurde. Das FBI hatte den amerikanischen Teil des Netzes samt Hintermännern im Oktober ausgeschaltet, aber der Rest floriert munter weiter. Die Sicherheitsfirma Bullguard nennt ohne weitere Quellen eine osteuropäische Gruppe *Evil Corp* als Betreiber.

Das Besondere an Dridex ist das Geschäftsmodell, das als Botnet-as-a-Service aufgebaut ist. Sprich, die Betreiber vermieten das Botnetz tagesweise. Über dieses kriminelle Netz läuft die gesamte Steuerung der Angriffe, die Verteilung der Schädlinge per Spam, die Steuerung der Trojaner, die Kommunikation mit den Opfern, der Verkauf der Entschlüsselung-Tools und die Abrechnung per Bitcoin. Die zugehörigen Webseiten liegen im Tor-Netz, also anonym und nicht zu lokalisieren.

Auch sämtliche weiteren Komponenten eines Angriffs, etwa Exploits, also Sicherheitslücken, oder Mail-Adressen für den Spam-Versand, lassen sich kaufen oder mieten – der Erpresser muss kein Hacker mehr sein, braucht von Netzwerken wenig Ahnung zu haben, sondern ist eher Geschäftsmann und Produktmanager. Für Erpressungs-Trojaner, wie sie der Makro-Downloader von Locky auf den Rechner holt, gibt es spezielle, komfortabel zu bedienende Baukästen. Der Täter klickt die Funktionen, die er benötigt, zusammen, und ein Packer-Tool erstellt den Trojaner. Die Sicherheitsexperten von Paloalto haben analysiert, dass der Locky-Packer dem der Banking-Trojaner von Dridex entspricht.

Einen weiteren Zusammenhang mit Dridex veröffentlichte Avira: gewisse Javascript-Mechanismen sind gleich (wobei im Fall von Locky JavaScript-Angriffe als Drive-by-Download im Browser derzeit eher selten im Vergleich zur Makro-Variante auftreten). Sicherheitsunternehmen und Strafverfolger versuchen gemeinsam und international gegen erpresserische Banden und Einzelverbrecher vorzugehen. Was oft nicht einfach ist. Die Verfolger arbeiten wie die Hacker und schleusen sich in die Kontrollstrukturen des Botnetzes ein, in der Hoffnung, etwas über die Betreiber herauszubekommen. Hin und wieder gelingt es, ein Botnetz zu knacken, auszuschalten und ein paar spooky Hintermänner zu verhaften, aber meist sind die Strukturen so verzweigt, dass ein neuer Ast irgendwo anders in der Welt die Arbeit wiederaufnimmt.

Fazit: Auffällig an Locky sind die psychologisch perfekt gemachten Social-Hacking-Mechanismen, die Firmenmitarbeiter geschickt beeinflussen, Sicherheitsbarrieren zu ignorieren. Das zeigt erheblichen Erfolg und verhilft einer totgesagten Angriffstechnik wieder zu neuem Leben: den Makroviren. Für Opfer gibt es keine Hilfe, sie müssen sich die Frage stellen, ob sie zähneknirschend bezahlen oder Daten verlieren. Der Schutz liegt wie meist bei digitalen Dingen in einer Mischung aus gutem Backup und gesundem Menschenverstand. **whs**



Diese Warnung wurde von den Mitarbeitern ignoriert, die Locky ins Firmennetz gelassen haben.

Microsoft markiert Dokumente im .docm-Format sogar mit einem Ausrufezeichen im Windows Explorer.

Legen Sie Backups auf einem externen Laufwerk an, das nicht dauerhaft verbunden ist.

Infiziert – was tun?

Wenn Locky bei Ihnen zugeschlagen hat, müssen Sie mit dem Verlust Ihrer Daten rechnen.

Bislang gibt es keinen Nachschlüssel für Locky, die Sicherheitshersteller knacken zwar immer wieder Erpressungstrojaner, jüngst z.B. Teslaycrpyt 2, aber Locky ist aufgrund seiner modernen Crypto-Infrastruktur eine harte Nuss.

Zahlen oder nicht?

Zahlen ist die schlechtere Wahl, denn es ist zwar wahrscheinlich, dass Sie den Schlüssel bekommen, aber nicht immer sicher. Außerdem gab es schon Fälle (allerdings nicht im Zusammenhang mit Locky), in denen der Erpresser nach der ersten Zahlung eine Nachforderung gestellt hat. Wenn Sie den Verlust der Daten verkraften können, weil Sie z.B. ein relativ frisches Backup haben, so zahlen Sie nicht!

Anti-Locky-Stick

Alle gängigen AV-Programme blockieren Locky effektiv. Die Entfernung gelingt mit der Rescue Disk auf der Heft-DVD. Ebenfalls auf DVD finden Sie das Tool *Rufus*, mit dem Sie aus dem Kaspersky-ISO einen bootfähigen Anti-Locky-Stick erzeugen. Keine schlechte Lösung ist auch, den Rechner nach einem Befall komplett zu formatieren und neu aufzusetzen. Damit gehen Sie sicher, alle Reste des Schädlings zu entfernen. Falls Sie ein Image eines sauberen Systems haben, können Sie auch das zurückspielen bzw. Windows ab Version 8 auf die Originaleinstellungen zurücksetzen.

Verschlüsselte Daten aufheben

Es besteht eine Chance, dass Sicherheitsspezialisten Locky doch irgendwann knacken oder dass die Polizei die Erpresserbande fasst und die Schlüssel veröffentlicht. Heben Sie also die verschlüsselten Daten auf.

Backup anlegen

Machen Sie künftig regelmäßig ein Backup, am besten auf einem externen Medium, das Sie nach jedem Backup vom Rechner wieder trennen.