Informationen im Umgang mit Schadsoftware
03.2016

Aktueller Status und Erklärung

Alleine im Februar 2016 gab es mehr Schäden durch eine bestimmte Art von Viren, als in den vergangenen 5 Monaten. Seit dem 15. Februar treibt „locky", eine sogenannte „Ransomware" (Kofferwort aus ransom=Lösegeld und ware=Software) auch Verschlüsselungs-, Erpressungs-Trojaner oder Cryptolocker genannt, sein Unwesen. Der Spitzenwert lag bei 5000 Infektionen pro Stunde bzw. 5 Infektionen pro Sekunde weltweit.
Wird ein Computer von diesem Schädling befallen, versucht dieser so viele Daten als möglich zu verschlüsseln. Vom Opfer wird im Anschluss Lösegeld gefordert, bei locky zwischen 0,5-1 Bitcoin (1 Bitcoin = 380€).

Dabei arbeitet diese Schadsoftware extrem schnell. Innerhalb von 40 Minuten waren bei einem betroffenen Unternehmen 85000 Dateien unbrauchbar. Die Software hat es dabei auf die wichtigsten Dateiformate abgesehen. Rund 54 verschiedene Dateitypen werden verschlüsselt. (weitere Quellen sprechen von mehr als 150 Dateitypen)

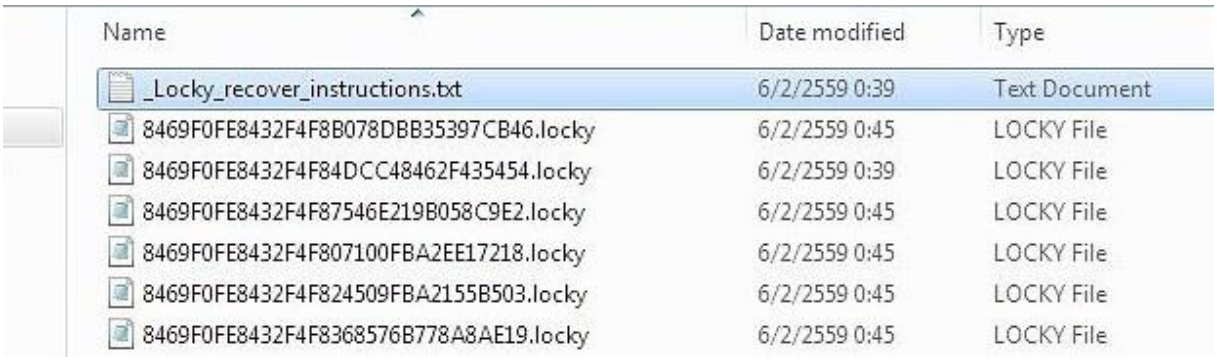


Bild: https://www.xgadget.de/

In der _recover_instructions.txt wie im Bild zu sehen, befindet sich der „Erpresserbrief", in dem die Anweisungen für die Lösegeldzahlung enthalten sind. Die weiteren Dateien wurden verschlüsselt, in einen kryptischen Namen umbenannt und die Dateiendung .locky angehängt.

Wie kommt der Schädling auf den Rechner?

a) Als E-Mail Anhang (Word oder Excel)
Sie erhalten eine E-Mail mit einer beigelegten Rechnung im Word- oder Excel-Format. Im E-Mail-Text werden Sie aufgefordert, die beigelegte Rechnung zu begleichen. Wird der Anhang geöffnet, werden Makros (Automatismen) aktiv. Diese durchsuchen den Rechner nach Schwachstellen und versuchen aus dem Internet den eigentlichen Virus herunterzuladen und diesen zu starten. In diesem Szenario kann es auch möglich sein, dass Sie aufgefordert werden, Makros zu aktivieren. Dabei wird der Text im Worddokument als wirre Zeichenfolge dargestellt.

b) Als E-Mail-Anhang (zip-Datei\JAVA-Script)
Genau wie unter Punkt a) wird eine Rechnung bzw. der Erhalt einer Fax-Nachricht vorgetäuscht. Der Anhang ist hier aber kein Office-Programm, sondern ein ZIP-Archiv, dass eine JAVA-Script-Datei enthält. Beim Öffnen versucht das Script ebenfalls Schadsoftware nachzuladen und die Verschlüsselung zu starten.

c) Drive by Download
Der Schädling lauert dabei auf gekaperten, harmlos wirkenden Webseiten. Er nutzt Sicherheitslücken im Betriebssystem Windows oder anderen installierten Programmen auf dem Rechner des Opfers aus, dass diese Webseite ansurft. Sobald der Schädling Zugriff auf den Rechner hat, beginnt er damit die Dateien zu verschlüsseln.

Bitte beachten Sie, dass sich das Angriffsszenario immer weiter verändern kann. Um es in den Worten von Marco Preuss, Leiter des europäischen Forschungs- und Entwicklungsteams von Kapersky auszudrücken: „Die Kriminellen hinter Locky versuchen derzeit aus der Erpressersoftware alles rauszuholen und größtmöglichen Profit zu erzielen. Locky ist kein ‚Kinderfasching', hier hat jemand viel kriminelle Energie investiert.
Dies zeigt sich auch an den E-Mails mit Schadsoftware. Diese sind in einwandfreien Deutsch verfasst und kommen oft auch noch mit persönlicher Ansprache in Ihren Posteingang.

Zudem hat sich gezeigt, dass Einrichtungen mit hochsensiblen Daten, wie Krankenhäuser, gezielt angegriffen wurden. Kriminelle nutzten hier noch eine weitere Komponente. Neben dem Verschlüsseln der Daten, drohen diese mit der Veröffentlichung im Internet. Somit stehen neben dem Schaden im IT-Netzwerk auch noch mögliche Image-Verluste und Strafzahlungen von Aufsichtsbehörden im Raum.

Diese Art der gezielten Angriffe bezeichnet man als Spear-Phishing Attacken. Damit lassen sich bei überschaubaren Mehraufwand höhere Lösegelder erpressen.

Wie kann ich mich schützen?

Zuerst einmal ist es wichtig, vor diesen Themen nicht zu kapitulieren. Nichtstun ist die schlechteste aller Optionen, auch wenn nur ein begrenztes Budget vorhanden ist. Schutzmaßnahmen setzen sich aus organisatorischen und technischen Bausteinen zusammen.

1. **Bleiben Sie auf dem Laufenden**

   Wir kennen die wichtigsten Einfallstore der Schadsoftware z.B. als Rechnungsanhang in einer E-Mail. Diese Varianten werden sich fortlaufend ändern und neue Angriffsmöglichkeiten werden hinzukommen.
   Lassen Sie sich informieren. Gerne können Sie unseren security-newsletter abonnieren. Dieser erscheint 1-2 Mal pro Monat und enthält die wichtigsten Sicherheitshinweise. Wenn Sie dies wünschen, senden Sie eine E-Mail mit der Empfänger-Adresse an security@ines-it.de. Ein weiterer Newsletter-Dienst den ich empfehlen kann, ist das BuergerCERT, eine Initiative des BSI. Anmeldung unter https://www.buerger-cert.de/subscription-new-request

2. **Nutzen Sie dieses Wissen (z.B. Makro-Funktionalität)**

   Wie wir wissen, kann der Virus über Office-Dokumente mit eingeschalteter Makro-Funktionalität auf den Rechner geladen werden. Diese Makro-Funktionalität lässt sich deaktivieren. Damit verringern Sie das Risiko einer Infektion über diese Methode.
   http://www.heise.de/security/bilderstrecke/bilderstrecke_3112082.html?back=3111774

   Informieren Sie auch Ihre direkten Kollegen, wenn Ihnen eine „gefährliche E-Mail" zugestellt wurde, damit diese gewarnt sind.

3. **Erst denken, dann klicken**

   Sollten Sie E-Mails mit Anhängen oder Links erhalten, bewerten Sie diese. Haben Sie diese digitale Post erwartet? Passt die Empfangs-Adresse zum Absender? (in der Regel sollten Sie keine private Telefonrechnung an Ihre Arbeitsplatz-E-Mail-Adresse bekommen). Warten Sie auf ein DHL-Paket? Öffnen Sie nur Anhänge, wenn Sie sich absolut sicher sind, dass die Nachricht von einem vertrauenswürdigen Absender kommt. Alles andere sollten Sie ungeöffnet löschen.
   Klicken Sie nicht ungeprüft Links in E-Mails. Tippen Sie die Linkadresse besser manuell in den Browser ein bzw. überprüfen Sie das Ziel. Linkadressen können leicht gefälscht werden z.B. www.tsv1860.de – wenn Sie den Mauszeiger über den Link setzen – ohne zu klicken – erscheint eine Anzeige mit dem wirklichen Ziel. Diese Variante verwenden Angreifer oft auch in E-Mails.

4. Funktionierende Datensicherung

Die Daten-Lebensversicherung, ist eine funktionierende Datensicherung. Im Zusammenhang mit Verschlüsselungs-Trojanern ist es wichtig, dass Sie dabei Ihre Sicherungsmedien nicht dauerhaft am Computer angeschlossen haben. Locky verschlüsselt alles, auf das er Zugriffsrechte besitzt. Haben Sie eine USB-Festplatte, einen USB-Stick angeschlossen, würde Locky auch hier zuschlagen.
Auch eine Synchronisation in einen Cloudspeicher ist vor Locky nicht sicher. Idealerweise sind Ihre Sicherungsmedien getrennt und in einem anderen Brandabschnitt. Das schützt die Daten auch bei einem möglichen Feuer.
Eine funktionierende Datensicherung bedeutet auch, dass Sie überprüfen, ob die Daten auf dem Medium in Ordnung sind. (Wiederherstellungstest)
Wenn wir von einem Einzelplatz-Rechner ausgehen, können Sie die windowseigene Sicherung „Dateiversionsverlauf" einsetzen. Nutzen Sie am besten 2 USB-HDDs die Sie im Intervall verwenden. Eine Anleitung finden Sie z.B. hier http://www.pc-magazin.de/ratgeber/dateiversionsverlauf-aktivieren-einrichten-windows-7-windows-10-backup-3195659.html

Möchten Sie eine Netzwerk-Infrastruktur sichern, sprechen Sie mit Ihrem IT-Dienstleister bzw. kommen Sie direkt auf mich zu.

5. Nie mit Admin-Rechten arbeiten

Arbeiten Sie nie im „Normalbetrieb" mit Administrationsrechten. Dies ist deshalb so wichtig, weil im Falle eines Virusbefalls, der Schädling die gleichen Rechte besitzt wie Sie selbst. Mit Administrationsrechten kann der Virus weit mehr Schaden anrichten, als unter eingeschränkten Benutzerrechten.

Möchten Sie Software nachinstallieren oder Konfigurationen durchführen, können Sie dies auch unter Benutzerrechten umsetzen, ohne sich An- und Abmelden zu müssen. Bei Bedarf fragt Sie das System nach den Zugangsdaten des Administrator-Accounts.
Weitere Informationen finden Sie in der Microsoft-Hilfe:
http://windows.microsoft.com/de-de/windows/what-is-user-account-control#1TC=windows-7

In einer Netzwerkumgebung sollten Sie Rechte immer nach dem Minimal-Prinzip vergeben. Jeder Anwender sollte nur auf die Daten Zugriff haben, die er für seine Arbeit unbedingt benötigt.

6. Halten Sie Ihren Rechner aktuell

Schadsoftware nutzt vorhandene Sicherheitslücken aus, um auf Ihren Rechner zu gelangen. Deshalb ist es wichtig:

a) dass Sie Ihr Betriebssystem auf dem aktuellen Stand halten. Verwenden Sie dazu die automatische Updatefunktion.
b) dass Sie jede weitere Software auf Ihrem Computer mit Updates versorgen. Dabei können Sie sich durch Tools wie z.B. http://www.chip.de/downloads/CHIP-Updater_70656452.html oder http://www.heise.de/download/personal-software-inspector-psi.html unterstützen lassen.
c) Deinstallieren Sie Software, die Sie nicht zwingend benötigen z.B. den Adobe FlashPlayer, der in der Vergangenheit oft als Einfallstor für Schadsoftware verwendet wurde.

7. Setzen Sie aktuelle Virenscanner für alle Endgeräte ein

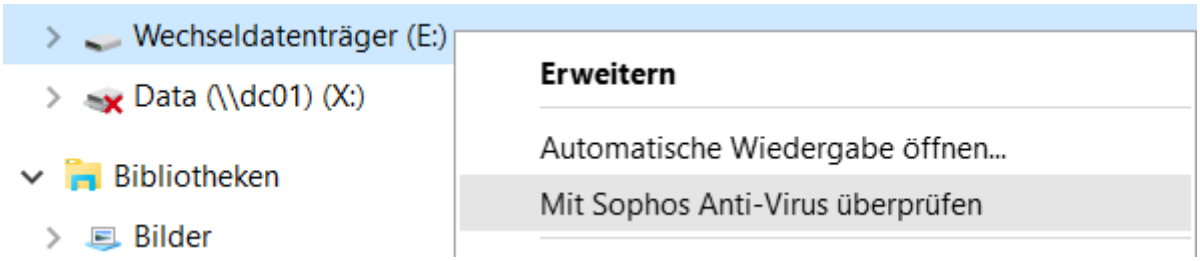
Alle Geräte müssen mit einer aktuellen Virenschutzsoftware ausgestattet sein. Ab Windows 8 ist das Schutzprogramm Defender vorinstalliert.

Bitte vergessen Sie den Virenschutz bei Smartphone und Tablet nicht. Nimmt man die drei großen Hersteller: iOS, WindowsPhone und Android, empfehlen wir den Einsatz zwingend bei Android-Geräten. Sie können sich bei der Auswahl von Schutzsoftware an Testberichten orientieren, z.B. https://www.av-test.org/de/antivirus/mobilgeraete//

8. Keine fremden\privaten USB-Sticks

Lassen Sie es nicht zu, dass unbekannte oder private USB-Sticks an Ihrem Arbeitsrechner angesteckt werden. Lässt es sich nicht vermeiden, überprüfen Sie den Stick mit einem aktuellen Virenscanner, bevor Sie Daten öffnen. Vorgehensweise:

- stecken Sie den USB-Stick an
- wechseln Sie in den Windows Datei-Explorer
- klicken Sie den Wechseldatenträger mit der rechten Maustaste an
- wählen Sie im erscheinenden Menu „mit Virenscanner XY überprüfen"
- sollte es einen Virusfund geben, stecken Sie den Stick umgehend ab



Windows beinhaltet die Möglichkeit, beim Anstecken eines USB-Sticks Dateien sofort auszuführen – „Autorun". Dies birgt die Gefahr, dass ein Virus auf dem USB-Stick automatisch beim Anstecken gestartet wird. Wenn Sie öfters fremde USB-Sticks anstecken müssen, sollten Sie diese Funktion deaktivieren. Eine Anleitung finden Sie hier: http://www.netzwelt.de/news/138721-windows-autorun-laufwerksbuchstaben-deaktivieren.html

Und es ist doch passiert!
Was tun, wenn locky meinen Rechner verschlüsselt?

- Bewahren Sie Ruhe
- Fahren Sie Ihren Rechner und alle angeschlossenen Systeme runter und schalten Sie diese aus
- Trennen Sie die Verbindung ins Internet

Ziehen Sie einen IT-Experten hinzu, wenn Sie unsicher sind.

- Starten Sie den Rechner über eine spezielle Boot-CD –USB-Stick z.B. http://www.heise.de/download/desinfect.html
- Sind die Systeme bereinigt, sichern Sie Ihre Daten aus der Datensicherung zurück
- Scannen Sie im Anschluss nochmals auf Viren, idealerweise noch einmal mit dem Boot-Virenscanner.

Wenn wir Anwender nach einem Trojaner-Angriff unterstützen, empfehlen wir die Neuinstallation des Rechners, da das System nicht mehr zu 100% vertrauenswürdig ist. Dies liegt aber in der Entscheidung des Anwenders.

Und es ist doch passiert!
Was tun, wenn keine Datensicherung vorhanden ist?

- Bewahren Sie Ruhe
- Zahlen Sie nicht den geforderten Betrag

Ziehen Sie einen IT-Experten hinzu, wenn Sie unsicher sind.

- Starten Sie den Rechner über eine spezielle Boot-CD –USB-Stick z.B. http://www.heise.de/download/desinfect.html
- Erstellen Sie eine Kopie der verschlüsselten Daten inklusive den Textfiles (z.B. _recover_instructions.txt). Somit kann mit einem zukünftig erstellten Entschlüsselungsprogramm, die Platte wieder entschlüsselt werden. (dies gilt für jeden einzelnen Rechner, da die Verschlüsselung nicht auf einem einheitlichen Prinzip beruht)

Grundsätzlich wird bei Erpressersoftware davon abgeraten, das Geld zu bezahlen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist darauf hin, dass Kriminelle in vielen Fällen auch nach einer Zahlung einfach darauf verzichten, die Daten freizuschalten. Betroffene sollten lieber den Bildschirm samt der Erpressungsnachricht fotografieren und Anzeige erstatten.

Die Vorgehensweise kann man aus meiner Sicht nicht immer pauschal entscheiden. Bewahren Sie Ruhe und sprechen Sie sich mit IT-Spezialisten ab, die Erfahrungen im Umgang mit Erpressersoftware haben.

Wir hoffen die Zusammenfassung hat für Sie einen Mehrwert und die Themen sind nachvollziehbar beschrieben. Sie wurden speziell an kleine Arbeitsumgebungen ausgerichtet. Wenn Sie für eine größere IT-Infrastruktur verantwortlich sind, kommen zusätzlich weitere oder andere Themen hinzu, die hier bewusst nicht aufgenommen wurden.

So kritisch der Umgang mit dem Internet in diesem Kontext erscheinen mag, so gut können Sie das gespeicherte Wissen im „world wide web" für Recherchen nutzen. Denken Sie daran, dass in der Regel jemand vor Ihnen betroffen war und Sie dieses Wissen im Internet abfragen können.

Bleiben Sie geschützt

Ihr Team der INES IT