LEBER & PARTNER
Rechtsanwälte

Rechtsanwälte Leber& Partner, Falkenring 8 - 63454 Hanau

Martin Leber LL.M.
Rechtsanwalt

Maren Nitsche-Knapp
Rechtsanwältin

Westhafenplatz 1, 60327 Frankfurt a.M.
fon.: +49 69 710 45 63 63
fax.: +49 61 81 98 36 82

Falkenring 8, 63454 Hanau
fon.: +49 61 81 98 36 81
fax.: +49 61 81 98 36 82

email: info@leber-partner.com
Web : www.leber-partner.com

Aktenzeichen:

Datum:
22. September 2017

SICHERHEITSHINWEIS - Achtung neuer gefährlicher Virus im Umlauf!

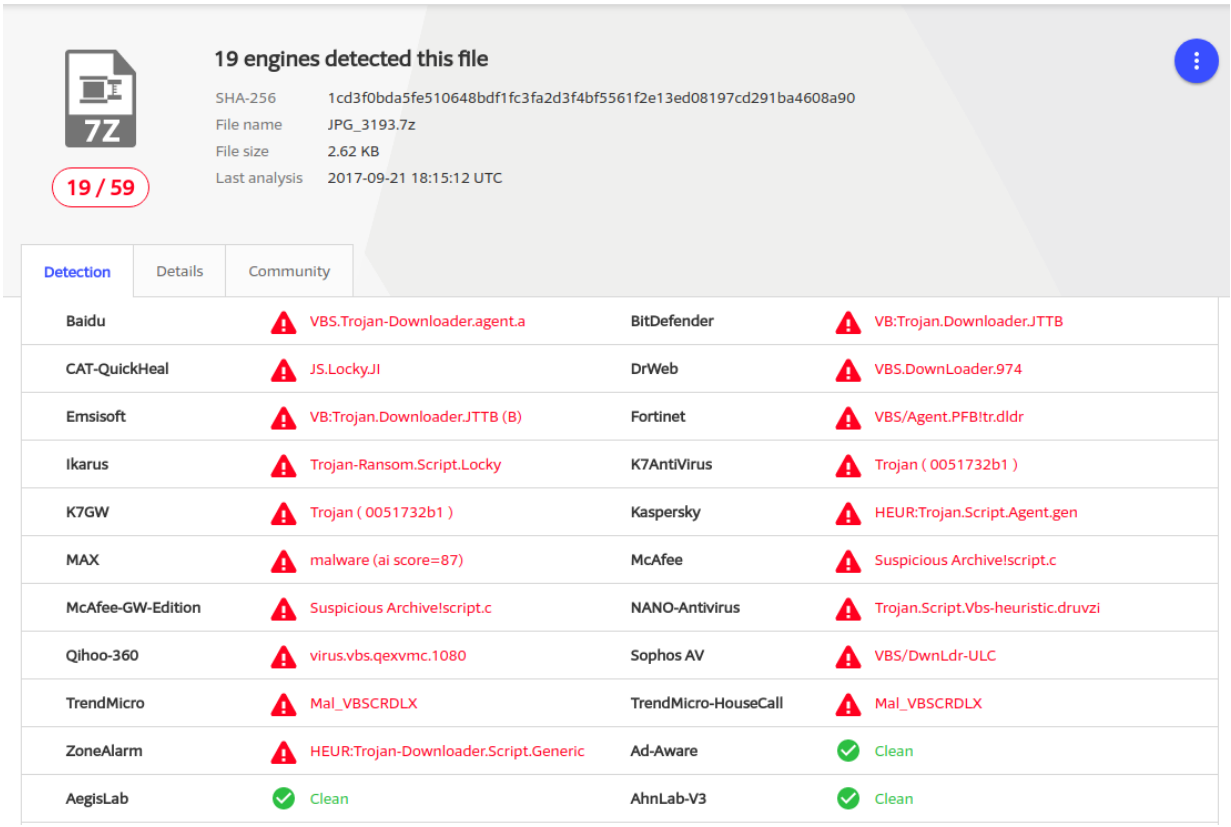
Liebe Mandanten, Kollegen, Verbandsmitglieder,

leider ist seit ein paar Tagen eine neue, aggressivere Variante, des „Locky-Virus“ im Umlauf und hat auch schon Kollegen von uns erwischt. Wir halten diese Bedrohung für so gefährlich, dass wir Sie darüber informieren wollen.

Haftungsausschluss: Die nachfolgenden Angaben sind nach bestem Wissen und Gewissen erstellt. Sie stellen lediglich einen Hinweis dar. Für Vollständigkeit und Richtigkeit können wir keine Gewähr übernehmen! Bei Umsetzung der Maßnahmen handeln Sie eigenverantwortlich und verzichten ausdrücklich auf die Geltendmachung von Schadensersatzansprüchen gegenüber der Kanzlei Leber&Partner, der Dr. Leber Datentechnik GmbH und Ihrer Erfüllungsgehilfen. Sprechen Sie bitte alle Schritte vorher mit dem IT-Fachmann/frau Ihres Vertrauens ab und holen sie sich bei Zweifeln Rat von entsprechenden Experten

Wie bekomme ich den Virus?

Variante 1 - Der Virus wird als Mailanlage mit der Endung **.7z** z.B. JPEG_3773.7z verschickt (diese Anlage auf keinen Fall öffnen!) und wird von vielen bekannten Antivirenprogrammen nicht erkannt.



Achtung! - Häufig wird man in der E-Mail gebeten, die „anliegende Rechnung oder einen Überweisungsbelegt zu überprüfen“, oder die Mail tarnt sich als „Bewerbung“ mit einem vermeintlichen Lebenslauf in Anlage. Der Absender, Betreff und Inhalt der E-Mail Inhalt variieren, achten Sie daher am besten auf E-Mails mit einer Anlage mit der Endung **.7z .**

Variante 2 - Link auf einen externen Server

Sie bekommen eine Mail, ggf. sogar von einem ganz bekannten Absender, die keine Anlage enthält, sondern einen Link oder ein Bild. Klicken Sie auf den Link oder das Bild laden Sie sich die Schadsoftware herunter und führen diese aus.

ACHTUNG! – Der Absender, der Ihnen z.B. in Outlook oder anderen E-Mail Programmen angezeigt wird, muss nicht der echte Absender sein. Es werden von Kriminellen gezielt Listen mit vertrauenswürdigen E-Mailadressen gekauft, um sie für diese Zwecke zu missbrauchen. Prüfen Sie bei verdächtigen Mails daher immer den „realen Absender“. Bei den meisten E-Mail Programmen können Sie durch Mouseover oder mit einem Rechtsklick auf die Adresse die echte Absender-Adresse anzeigen lassen. Informieren Sie bitte auch die Person, deren E-Mail Adresse missbraucht wurde, damit sie andere Personen davor warnen kann. Die Person oder das Unternehmen selbst kann nichts dafür, dass ihre Email-Adresse missbraucht wurde.

Was macht der Virus?

Wird die Anlage geöffnet, durchsucht der Virus auf dem infizierten Rechner alle Verzeichnisse auf Dokumentendateien und verschlüsselt diese. Parallel dazu durchsucht er die Verzeichnisse auf von diesem Rechner erreichbaren Netzwerklaufwerken, Servern und anderen Rechner und verschlüsselt auch die Dokumente auf diesen Systemen. Gefährdet sind also alle Rechner (auch die Server) im Netzwerk.

Wie bemerken Sie, dass Ihr Rechner infiziert ist?

Sie werden bald merken, dass Sie auf bestimmte Daten nicht mehr zugreifen können. Hat der Virus ein System vollständig verschlüsselt, erscheint zudem ein Dialog, der sie darüber informiert, dass Ihre Daten nun verschlüsselt sind und Sie Bitcoins überweisen sollen, um einen Key zu bekommen, der benötigt wird, um die Dateien wieder zu entschlüsseln. In den uns bekannten Fällen wurde nicht gezahlt, insofern wissen wir nicht, ob es etwas nützt, der Aufforderung nachzukommen und man dann einen Key erhält oder nicht und können diesbezüglich keine Aussage machen. Generell raten wir davon ab, dies zu tun.

Wie können Sie prüfen, ob Ihr System befallen ist?

➔ Suchen Sie auf Ihren Rechnern nach: ***.ykcol**

Was können Sie unternehmen, wenn Sie auf einem Rechner eine Datei mit der Endung „ykcol" finden?

Es werden zwar im Internet Lösungen angeboten, die den Virus entfernen sollen, von denen wir aber nicht wissen, ob sie funktionieren. Generell sind solche „einfachen Lösungen" aber mit extremer Vorsicht zu genießen und wenn dann nur auf einzelnen Rechnern zu testen, die vom Netzwerk getrennt sind, da sie häufig selbst Viren enthalten. Auch werden durch das Entfernen der Schadsoftware die bereits verschlüsselten Dateien nicht wieder entschlüsselt. Nach Aussage unsere IT-Fachleute gibt es – zumindest aktuell – keine Chance die Verschlüsselung zu knacken. Sprechen Sie in diesem Fall Ihr Vorgehen am besten mit einer Fachfirma, die sich auf forensische IT-Sicherheit spezialisiert hat, ab.

Unsere Empfehlung (keine Gewähr für Funktion o. Schäden s.O.):

1. Trennen Sie den Rechner vom Netz (Stecker raus, Switch/Rooter ausschalten)
2. Schalten Sie den/die Rechner und Server aus.
3. Suchen Sie im Log-Verzeichnis auf dem Mailserver nach einer E-Mail mit einem Angang mit der Endung **„.7z".** Durchsuchen Sie auch den Spamordner und vor allem den „gelöschte Objekte" Ordner. Viele Mitarbeiter löschen eine solche Mail, nachdem sie feststellen, dass sich der Anhang nicht öffnen lässt oder die E-Mail offensichtlich nicht wichtig ist. Wenn Sie mehrere Rechner finden, die eine solche E-Mail auf dem System haben, schauen Sie sich das Empfangsdatum der E-Mails an.
4. Tauschen/formatieren Sie die Platten aller infizierter Systeme und spielen Sie danach ein Backup auf, das älter ist als die erste Schadmail.

Westhafenplatz 1, 60327 Frankfurt a.M.
fon.: +49 69 710 45 63 63
fax.: +49 61 81 98 36 82
Web: www.raleber.de

Falkenring 8, 63454 Hanau
fon.: +49 61 81 98 36 81
fax.: +49 61 81 98 36 82
email: info@raleber.de

Bankverbindung:
Frankfurter Sparkasse 1822
BLZ 50050201
Kto: 200574922

Zul.Nr.: 146 703
USt-Id.: DE298047972
IBAN: DE31500502010200574922
BIC: HELADEF1822

5. Wenn Sie auf unverschlüsselte Inhalte auf infizierte Festplatten unbedingt zugreifen müssen, sollten Sie diese ausbauen und versuchen über einen externen Dongle mit einem autarken Linux oder IOS System darauf zu zugreifen. Platten mit den verschlüsselten Inhalten sollten Sie in einem sicheren Schrank verwahren. Möglicherweise wird in ein paar Wochen/Monaten der Key geknackt oder von den Kriminellen selbst veröffentlicht.

Was können Sie präventiv tun?

1. Informieren Sie Ihre Mitarbeiter, dass Sie aktuell auf keinen Fall E-Mail Anlagen mit der Endung **.7z** von unbekannten Absendern öffnen. Sofern Sie die Absenderaderesse einer solchen E-Mail kennen, rufen Sie den Absender an, und fragen ihn, ob er Ihnen tatsächlich einen solchen File geschickt hat – vielleicht ist sein System auch schon infiziert.

2. Durchsuchen Sie alle Mailingsystemen nach E-Mails mit Anlagen mit der Endung **.7z** und löschen Sie diese.

3. Erstellen Sie regelmäßig Vollbackups als „Snapshots“ auf getrennten Systemen und speichern Sie die Backups von mehreren Tagen (am besten abwechselnd auf zwei unterschiedlichen Systemen). Diese Sicherungen sollten zusätzlich zum permanenten sichern/spiegeln der Platten (Raid System) geschehen. Das permanente Spiegeln der Platten schützt Sie zwar beim Ausfall einer Platte, nicht aber bei einem Angriff durch einen Virus wie Locky, da dieser auf den weiteren Systemen dann automatisch mitverteilt wird und somit zeitgleich auch die Daten auf dem Sicherheitssystemen verschlüsselt werden.

Ohne Backups kann ein solcher Virus das Ende Ihres Geschäftsbetriebes bedeuten. Das Thema IT-Sicherheit ist leider aktuell eine der größten und zudem stetig wachsenden Gefahren, gerade auch für kleine und mittelständische Unternehmen. Die Fehler, die dazu führen, werden fast immer von Mitarbeitern versehentlich **aktiv** ausgelöst (z.B. durch Anklicken eines Bildes oder Öffnen einer Anlage einer E-Mail).

Nehmen Sie dieses Thema bitte ernst und sensibilisieren und unterweisen Sie Ihre Mitarbeiter regelmäßig im richtigen Umgang mit IT-Sicherheitsfragen!

Mit freundlichen Grüßen

RA Martin Leber LL.M
CEO – Dr. Leber Datentechnik GmbH