AKADEMIE FÜR LEHRERFORTBILDUNG UND PERSONALFÜHRUNG
DILLINGEN

SCHULNETZ

Qualifizierung von Systembetreuerinnen
und Systembetreuern

Verschlüsselungstrojaner
LOCKY

– Testbericht –

Dillingen, März 2016

Anlass für den Test des Verschlüsselungstrojaners waren Berichte auf Heise.de (vom Februar 2016), einige Fernseh- und Radioberichte über Kommunen, die Lösegeld bezahlten, um wieder an ihre Daten zu kommen, und auch persönliche Erfahrungen von IT-Administratoren im Landkreis Dillingen, die von Unternehmen, bei denen dieser Trojaner Schaden angerichtet hat, beauftragt wurden.

Download

Der Verschlüsselungstrojaner locky wurde im Internet nach einiger Suche unter dem Namen 7t6f65g.exe über einen Hinweis auf der Seite http://blog.dynamoo.com gefunden, wobei der Trojaner einige Tage später unter dieser Adresse schon nicht mehr auffindbar war.

Virenschutz

Im März 2016 wurde der Trojaner von einem aktuellen Virenscanner erkannt. Der nachfolgende Test wurde ohne Virenschutz durchgeführt.

Testszenario

Auf dem Testrechner wurden einige Dokumente (Office-Dokumente, Bilder, Multimedia-Dateien) in verschiedenen Verzeichnissen abgelegt. Zudem standen zwei Netzlaufwerke zur Verfügung, in denen ebenfalls solche Dokumente lagen. Eines dieser Netzlaufwerke war mit einem Laufwerksbuchstaben verbunden.

Auf dem Testrechner lief auch ein Owncloud-Client, der bestimmte Verzeichnisse automatisch mit einer Cloud im Internet synchronisierte. Weitere Verbindungen im lokalen Netz wurden durch eine Firewall blockiert, auf das Internet konnte der Trojaner ungehindert zugreifen, die Zugriffe wurden protokolliert.

Test

Der Trojaner wurde als normaler Benutzer gestartet. Es gab keine Rückmeldung, dass etwas passiert, im Taskmanager konnte man sehen, dass die exe-Datei ausgeführt wird.

Bei einer funktionierenden Internetverbindung war der Trojaner sofort aktiv, hat in einigen Verzeichnissen Dokumente verschlüsselt, seine eigene exe-Datei gelöscht und sich selbst beendet. Der gesamte Vorgang hat nur wenige Sekunden gedauert.

Bei einer getrennten Internetverbindung gab es keine Verschlüsselung von Dokumenten. Der Trojaner blieb jedoch im Taskmanager aktiv und startete die Verschlüsselung, sobald der Internetzugang funktionierte.

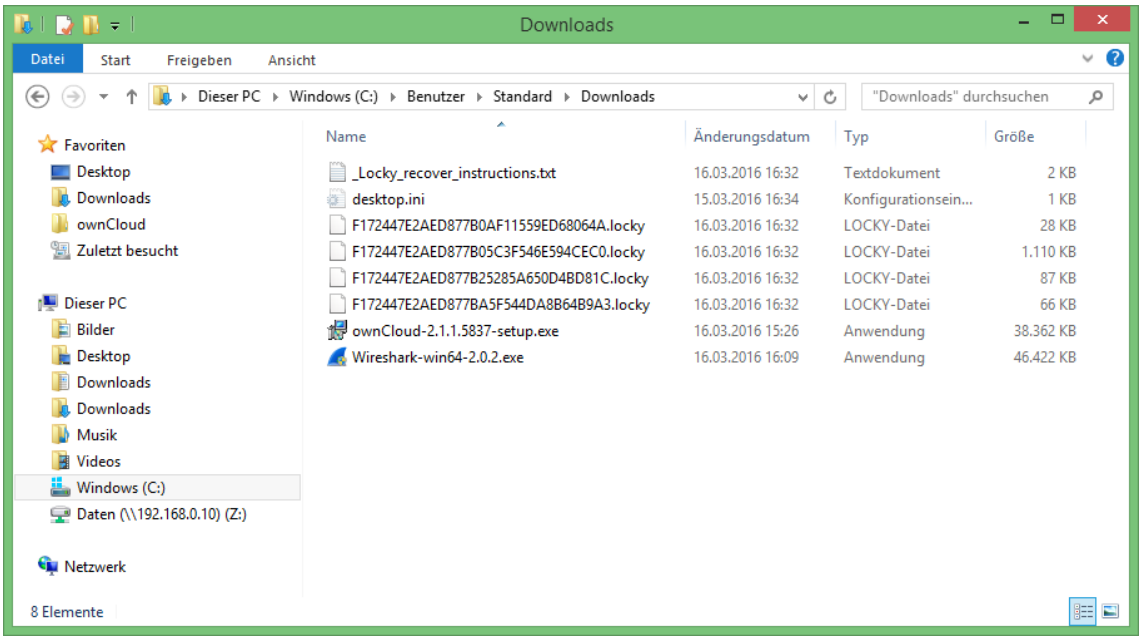
Verschlüsselte Dokumente

Der Trojaner verschlüsselte auf dem lokalen Rechner Dokumente in den üblichen Verzeichnissen (z. B. Dokumente, Downloads, Desktop). Dokumente in ungewöhnlichen Ordnern (z. B. c:\temp) wurden nicht gefunden.

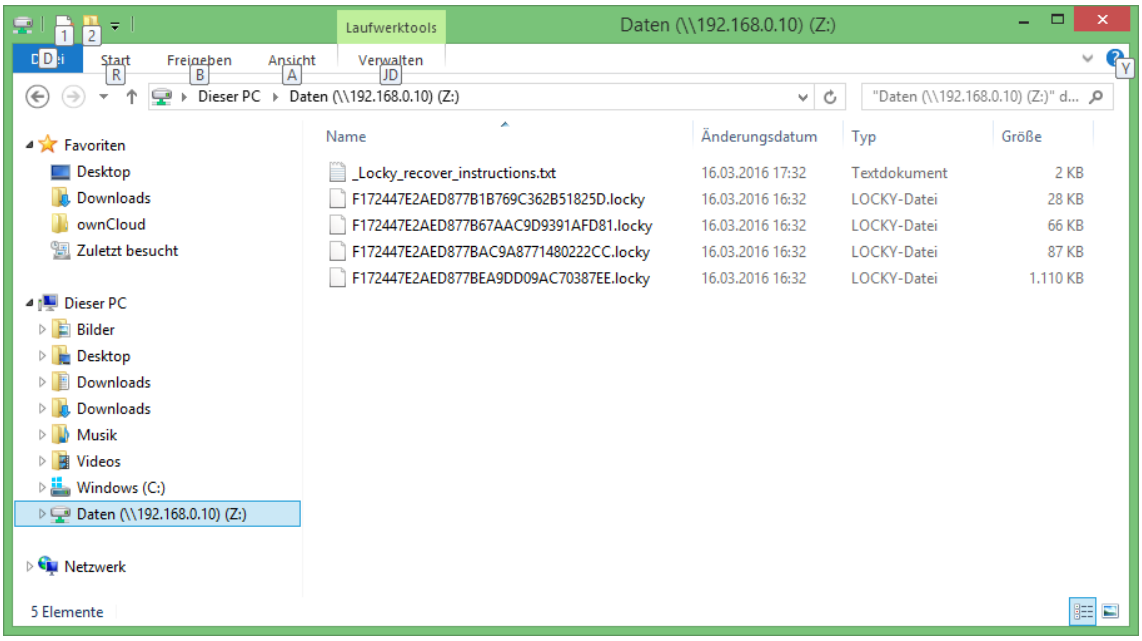
Das mit einem Laufwerksbuchstaben verbundene Netzlaufwerk wurde gefunden und die Dokumente darin verschlüsselt. Das zweite verbundene Netzlaufwerk ohne Laufwerksbuchstabe wurde nicht gefunden.

Auf dem Cloudspeicher im Internet und im synchronisierten lokalen Ordner waren die Dokumente verschlüsselt.

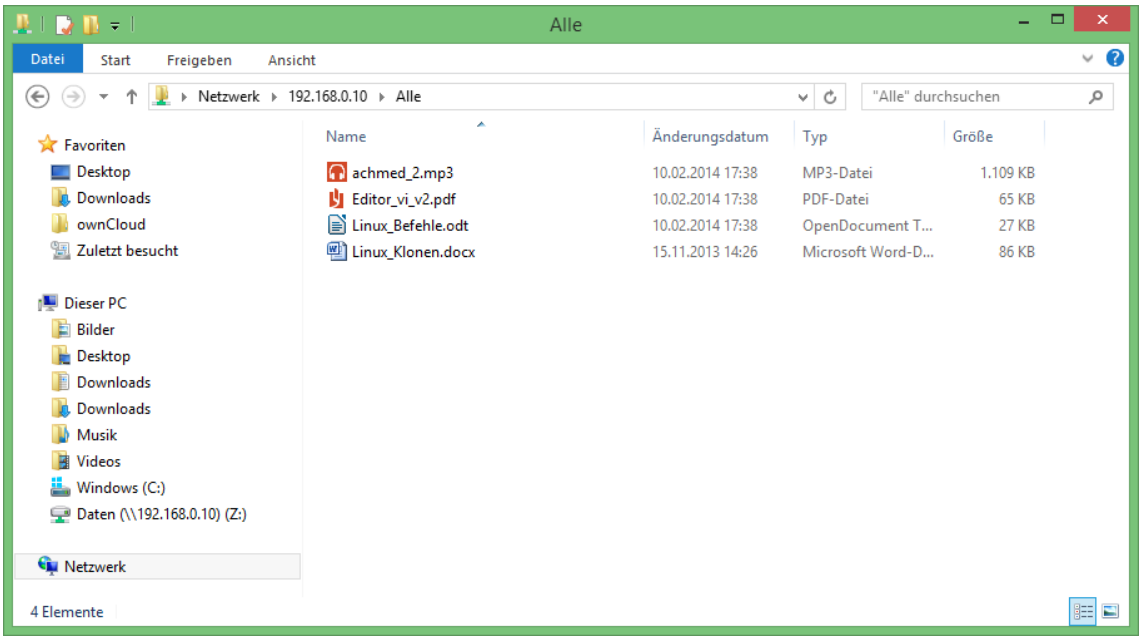
Verschlüsselte Dokumente in den üblichen Ordnern (z. B. Dokumente, Downloads und Desktop):



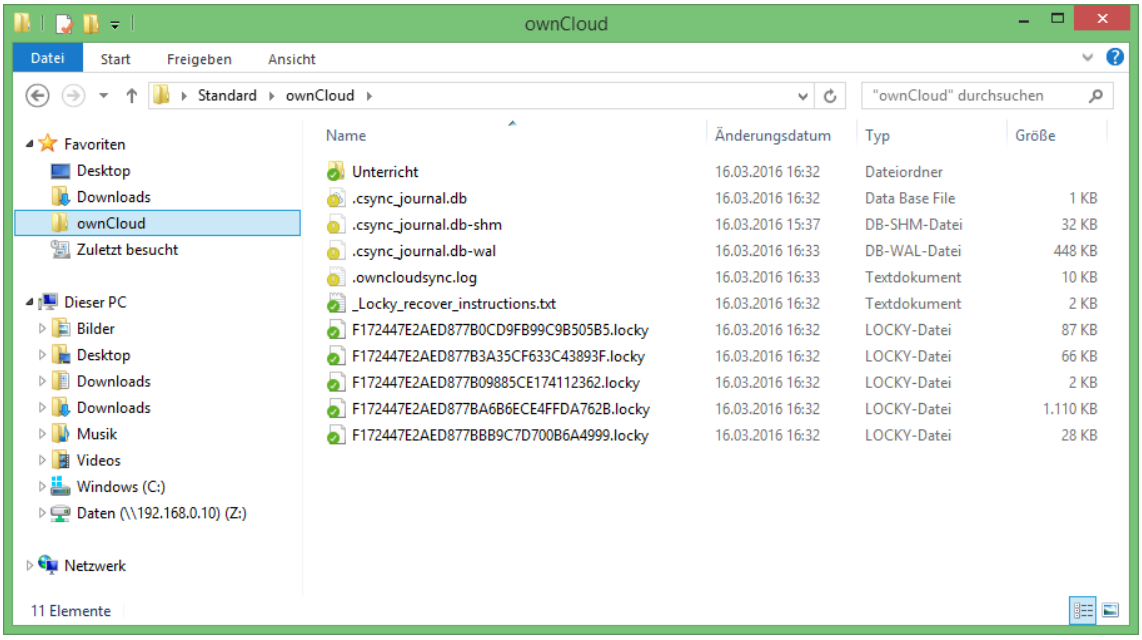
Verschlüsselte Dokumente im Netzlaufwerk, das mit einem Laufwerksbuchstaben verbunden war:



Nicht verschlüsselte Dokumente im Netzlaufwerk, das geöffnet, aber nicht mit einem Laufwerksbuchstaben verbunden war:

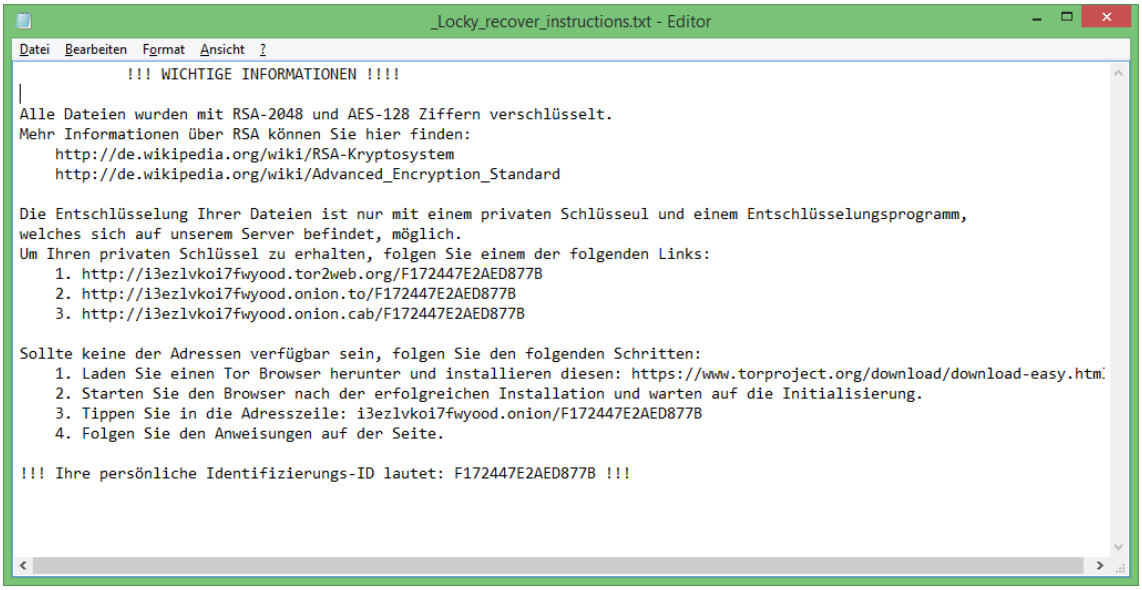


Verschlüsselte Dokumente in der Cloud und im synchronisierten lokalen Ordner:

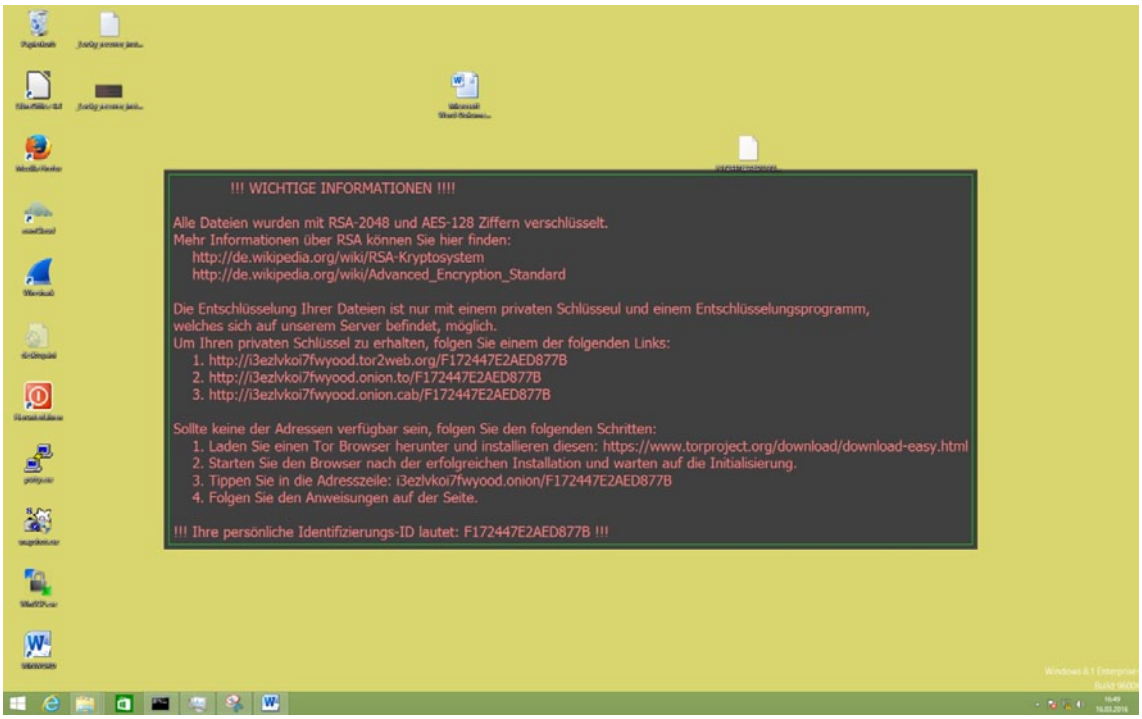


Hinweise zur Verschlüsselung

In allen Verzeichnissen, in denen die Dateien verschlüsselt wurden, war eine Textdatei mit Hinweisen zum weiteren Vorgehen zu finden



Ebenso war der auf dem Bildschirmhintergrund ein entsprechender Hinweis zu finden:

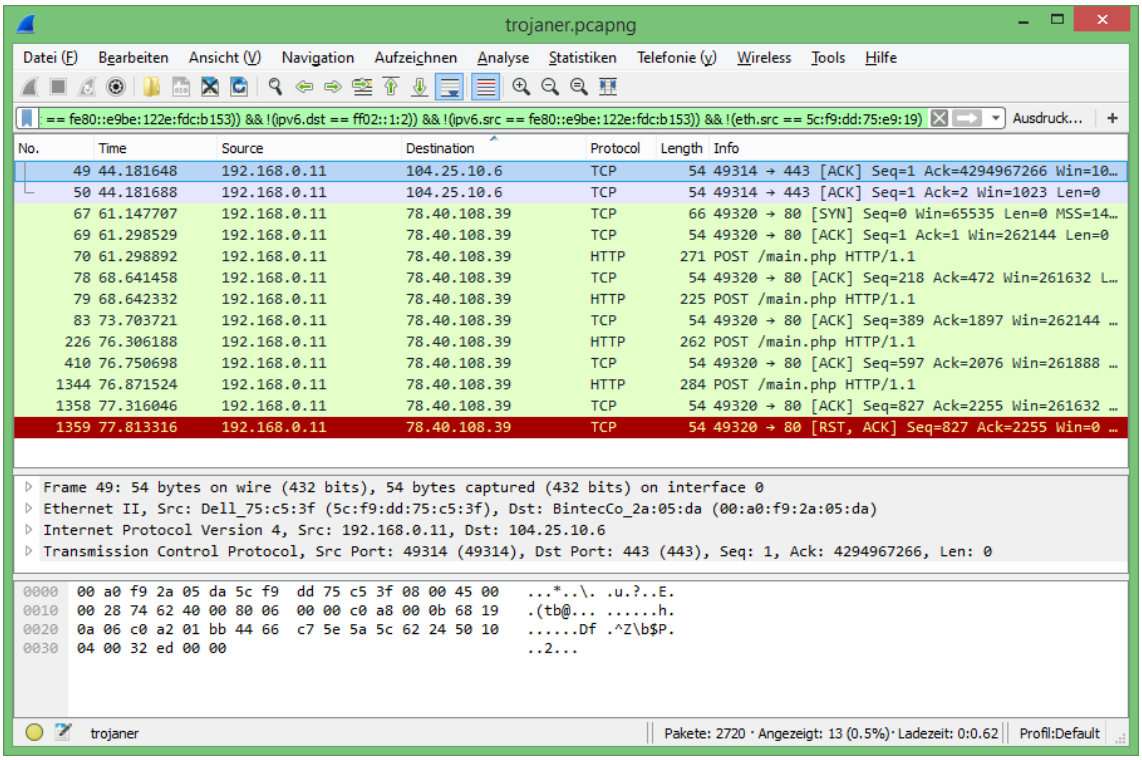


Zugriff auf die Entschlüsselungsprogramme

Die angegebenen Links funktionieren nur, wenn ein Tor-Browser installiert ist. Dieser anonymisiert die Netzwerkverbindungen (sowohl für die Client als auch für den Server) Er verlangsamt die Verbindung jedoch deutlich (bis hin zum gelegentlichen Timeout).

Netzzugriffe des Trojaners

Die Netzzugriffe des Trojaners wurden mit Wireshark protokolliert. Nachfolgend sind alle Netzzugriffe auf lokale Netze und in die Cloud herausgefiltert.



Einschlägige Programme lokalisieren die aufgerufene IP-Adresse in Russland oder Kasachstan.

Vorbeugung

Ein aktueller Virenscanner hat den Trojaner (der offensichtlich schon längere Zeit im Netz unterwegs war) erkannt. Bei neuen Trojanern kann dies nicht vorausgesetzt werden.

Der Trojaner arbeitet im Benutzermodus. Er fragt nicht nach einem Passwort und er verlangt auch keine Eingaben oder Bestätigungen des Benutzers. Er kann alle Daten löschen oder verschlüsseln, auf die der Benutzer schreibenden Zugriff hat. Als Konsequenz bedeutet dies, dass eine Datensicherung, auf die ein Benutzer schreibenden Zugriff hat, für dieses Szenario nicht viel Wert ist.