

- Sollte dieser Newsletter bei Ihnen nicht einwandfrei angezeigt werden, beachten Sie bitte die beigefügte Version als PDF.

Angebliche Paket-Verständigung von der „Post“ kann Ihre Daten durch Verschlüsselung unbrauchbar machen

Art der Bedrohung

Verschlüsselung von Privat- und Firmendaten und anschließende Erpressung zur Bezahlung eines Geldbetrages mittels BitCoin zur Erlangung des Entschlüsselungs-Codes / Programms

Modus Operandi

Kaum ist die Bedrohung durch angebliche E-Mails von DHL im Abklingen, erreicht uns eine neue Welle von E-Mails mit gefährlichem Inhalt. Nunmehr gibt die Mail vor von der „Post“ zu stammen und informiert über eine nicht erfolgreich durchgeführte Zustellung. Die weitere Vorgehensweise bleibt dabei gleich; der Empfänger wird aufgefordert den Versandschein über einen Link in der Mail herunter zu laden.

Der Download des „Versandscheines“ erfolgt nach Eingabe eines Ziffern-Codes (Captcha) in einer komprimierten ZIP-Datei, die darin befindliche ausführbare *.exe wird durch Vortäuschen eines falschen Icons als PDF angezeigt. Wird diese tatsächlich ausgeführt, werden Benutzerdaten auf dem lokalen System, verbundene Server-Shares sowie angeschlossene, beschreibbare USB-Laufwerke durch die Ransomware „CryptOLocker“ verschlüsselt. Für den Erhalt des für die Entschlüsselung notwendigen „Key´s“ ist die Bezahlung eines „Lösegeldes“ mittels BitCoin erforderlich. Die Transaktion selbst, sowie die Anweisungen für die Bezahlung, erfolgen dabei über einen angeführten Link in das Tor-Netzwerk.

Wir raten derart geforderte Zahlungen nicht zu leisten. Die Bezahlung sollte das allerletzte Mittel sein, wenn Sie auf die verschlüsselten Daten keinesfalls verzichten können. Besser beraten wäre man jedoch, zeitgerecht die finanziellen Mittel in eine entsprechende BackUp-Lösung und Strategie zu investieren.

Eine Wiederherstellung oder Entschlüsselung der Daten ohne dem erforderlichen „Key“ ist auf Grund der hohen Qualität der Verschlüsselung derzeit nahezu unmöglich.

Zudem werden von der Schadsoftware in der Windows (Registry) gespeicherte Zugangsdaten und Passwörter, unter anderem für FTP und E-Mail-Accounts ausgelesen und per Mail an eine vom Täter adressierte Stelle im Internet versandt. Ebenfalls erfolgt zu diesem Zeitpunkt die Löschung der sog.

„Shadow Copy“, welche bei Vorversionen dieser Schadsoftware in manchen Fällen noch eine Teilwiederherstellung der Daten zuließ.

Harvests credentials from local FTP client softwares (1 event)	
registry	HKEY_CURRENT_USER\Software\Martin Prikryl

Harvests credentials from local email clients (4 events)	
registry	HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts\00000001
registry	HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outloo
registry	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Account Manager\Outlook
registry	HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts

Removes the Shadow Copy to avoid recovery of the system (1 event)	
cmdline	vssadmin.exe Delete Shadows /All /Quiet

Empfohlene Vorgangsweisen:

- Seien Sie vorsichtig beim Erhalt von E-Mails, deren Absender Sie nicht kennen oder wenn Sie keine entsprechenden Mitteilungen erwarten.
- Achten Sie auf die Schreibweise und Rechtschreibung solcher Nachrichten, Täter verwenden hier gerne Übersetzungsprogramme, wodurch der Betrug leicht erkennbar ist.
- Öffnen Sie keinesfalls Ihnen unbekannte Dateianhänge, ohne sich vorher von deren „Echtheit“ zu überzeugen.
- Wenn Sie sich unsicher sind, öffnen Sie derartige Dateien in einer gesicherten Umgebung (Sandbox, virtuelle Systeme mit Option auf Rücksetzung) oder bedienen Sie sich unterstützenden Seiten im Internet (z.B. Virustotal.com).
- Ändern Sie regelmäßig Ihre Zugangsdaten, verwenden Sie unterschiedliche und komplexe Passwörter für verschiedene Accounts und Anwendungen.
- Legen Sie sich eine BackUp-Strategie Ihrer Daten zu. Trennen Sie das BackUp-Medium nach der Sicherung vom System und lösen Sie Share-Links zu BackUp Servern nach erfolgter Sicherung wieder auf, um ein Übergreifen durch die Schadsoftware zu verhindern.
- Beschränken Sie die Benutzerrechte der jeweiligen User so weit als möglich und arbeiten Sie nur unter dem Administrator-Account, wenn dies unbedingt notwendig ist.
- Die Investition in eine entsprechende Sicherheits- und BackUp-Lösung erspart Ihnen Sorgen und Ärger und finanziell höhere Verluste!
- Wir raten den geforderten Betrag nicht zu bezahlen, es sei denn, dass die Wiederherstellung der Daten für Sie unumgänglich ist. Eine Garantie auf eine solche, selbst nach Bezahlung, gibt es nicht! Eine letztendliche Entscheidung darüber müssen Sie für sich selbst treffen.
- Beachten Sie die Sicherheitshinweise und Tipps, für einen Sicheren Umgang mit dem Internet und Schutz vor IT-Kriminalität der Kriminalprävention: <http://www.bmi.gv.at>.

Text und Grafik der E-Mail, welche über die Sendung informiert:




die Sendung zur Bestellung AT81846979 wurde an das Logistikunternehmen "übergeben und wird voraussichtlich am 20.04.2016 zugestellt.

Hier erhalten Sie auch weitere Informationen zu Ihrer Sendung.

[herunterladen](#)

Newsletters sind ein kostenloser Service der "Österreichischen Post AG" für registrierte Nutzer und dienen zur Information über die von der "Österreichischen Post AG" angebotenen Produkte und Services und über Finanzdienstleistungen der P.S.K. Wenn Sie einen Newsletter nicht mehr erhalten wollen, dann klicken Sie auf den Abmeldelink im Newsletter.

Darstellung der Downloadseite für die Schadsoftware:



Privat

Geschäftlich

Über Uns

Shop

Meine Post

Hotline: 0810 010 100 (max. € 0.10 / Min) | Übersicht | English | Zum Kundenservice

Suchfeld

Sendungsverfolgung | Tarifrechner | Standorte

Versenden

Empfangen

- Brief
- Paket**
 - e-Benachrichtigung
 - Paketumleitung
 - Nachsenden
 - Abstellgenehmigung
 - Schadensmeldung
 - Wunsch-Abholstation & Wunsch-Postfiliale
- Post Empfangsbox

Filialen

Briefmarken & Philatelie

Kontakt

SENDUNGSVERFOLGUNG

SENDUNGSVERFOLGUNG

Eine Sendungsnummer erhalten Sie bei der Aufgabe einer Sendung oder vom Versender.

Um Versandschein downloaden, geben Sie bitte Zahl in das Bild unten:

33869

Versandinfos

- Track und Trace
- Postkarte, Porto
- Tarifrechner
- Maße & Gewicht
- Formatschablone
- Briefmarken & Philatelie

Standorte

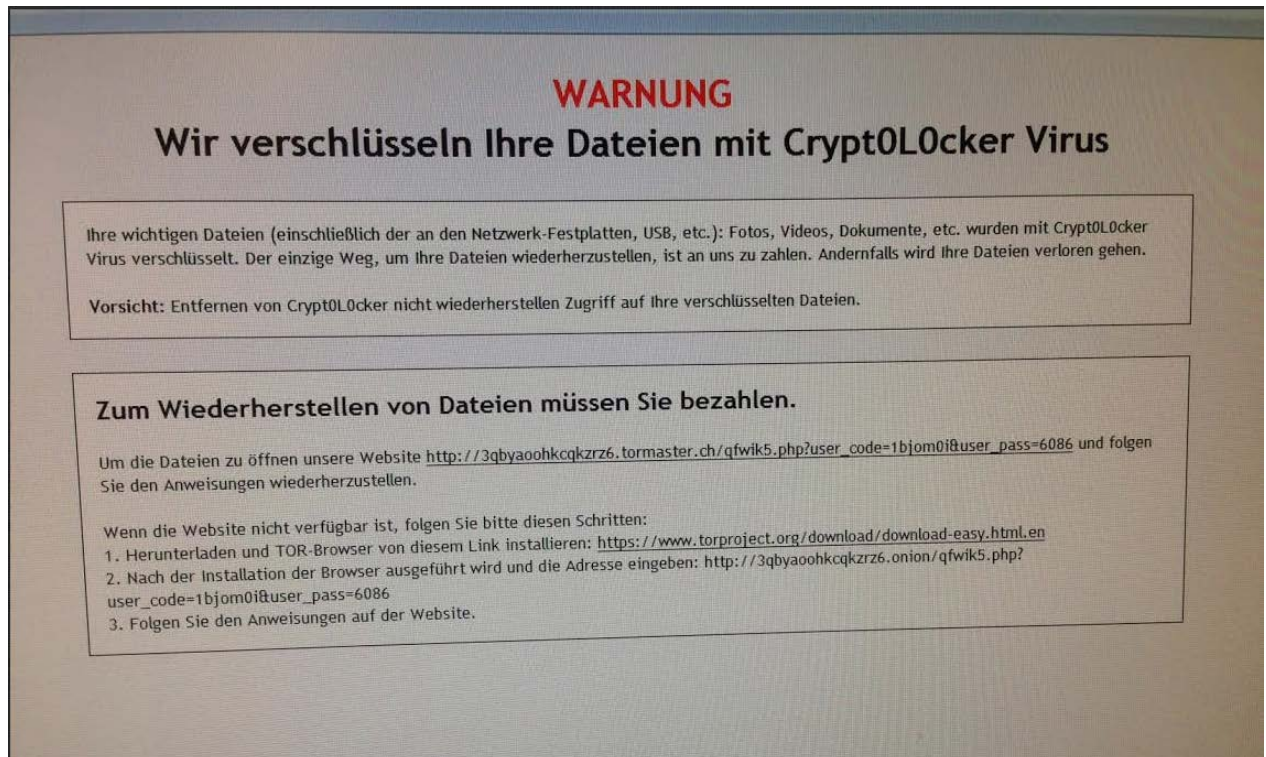
- A1 Shop
- Post Filiale suchen
- Postzeitfinder
- Briefkastenfinder
- Online Shop

Produkte

- Das Flugblatt
- Postkarte versenden
- Meine Sendung
- Produkte von A-Z
- Briefmarken
- Paketmarken
- Meine Marke
- Post Fotoservice

Services

Nach der Verschlüsselung erscheint die Aufforderung zur Bezahlung:



Weiterführende und erklärende Links:

Wikipedia – CryptoLocker (englisch): was ist CryptoLocker und dessen Geschichte
(<https://en.wikipedia.org/wiki/CryptoLocker>)

Wikipedia – BitCoin: die Entstehung und Entwicklung der „digitalen Münze“
(<https://de.wikipedia.org/wiki/Bitcoin>)

HERAUSGEBER: Bundesministerium für Inneres
Bundeskriminalamt
A-1090 Wien, Josef Halaubek Platz 1
Tel.: +43 1 24836 986500

FEEDBACK

NEWSLETTER
AN-/ABMELDUNG

Hinweis: Die vorliegende Information beruht auf einer Momentaufnahme aus dem Geschehen in der C4-Meldestelle ohne Berücksichtigung allen Falls vorhandener statistischer Daten aus dem Bundesgebiet und dient einem eingeschränkten Empfängerkreis zu Informations- und Präventionszwecken. Der beschriebene Tathergang sowie dazugehörige technische Details wurden im Rahmen der hier vorhandenen Möglichkeiten recherchiert und erheben keinen Anspruch auf Vollständigkeit. Angeführte Web-Links zu weiterführenden Artikeln und Informationen wurden zwar bei der Erstellung des Newsletters auf ihre sachliche und inhaltliche Richtigkeit überprüft, es besteht jedoch keine Haftung für das BK bei Änderung dieser Inhalte durch Dritte. Medienanfragen sind ausschließlich an die Pressestelle des Bundeskriminalamts zu stellen.