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

Neue Spam-Welle mit Bewerbungsschreiben wird erwartet – ACHTUNG: dahinter verbirgt sich Ransomware

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

Wie aus nationalen und internationalen Ermittlerkreisen zu erfahren war, wird aktuell eine neue SPAM-Welle mit Bewerbungsschreiben erwartet; bei der angezeigten Absenderadresse soll es sich hauptsächlich um **julian.heyne@aon.at** handeln. Bei den in den Schreiben angeführten Bewerbungsunterlagen, welche über einen Link zum Download bereitgestellt werden, handelt es sich um Schadsoftware.

Der Download der Datei selbst soll zumeist von einer Dropbox erfolgen, die Datei könnte aber auch direkt an die Mail angehängt sein. Der Mail-Inhalt erscheint glaubwürdig, die Gründe dafür dass die Bewerbungsunterlagen nicht direkt beigelegt werden konnten, nachvollziehbar.

Bei der Schadsoftware selbst handelt es sich neuerlich um eine Variante der bekannten Ransomware „Cerber“. Beim Öffnen der als Office- oder Text-Dokument getarnten Datei wird diese ausgeführt und lädt zusätzlichen Schadcode aus dem Internet nach. In weiterer Folge werden die Daten auf sämtlichen im Netzwerk befindlichen Computern und Laufwerken verschlüsselt. Insbesondere **Betriebe und Firmen** sollten **daher besondere Vorsicht** beim Einlangen von **Bewerbungsschreiben** walten lassen.

Wie bereits in den vorherigen Versionen ist für den Erhalt des für die Entschlüsselung notwendigen „Key´s“ die Bezahlung eines „Lösegeldes“ (Ransom) mittels BitCoin erforderlich. Die Anweisungen für die Kontaktaufnahme erfolgen auf dem Bildschirm des Benutzers.

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 sind Sie, wenn Sie zeitgerecht die finanziellen Mittel in eine entsprechende BackUp-Lösung und Strategie investieren.

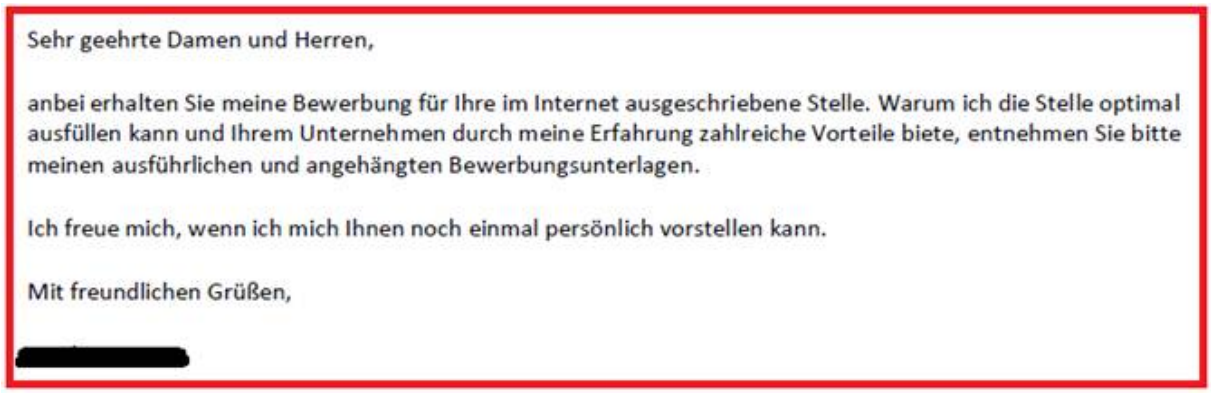
Eine Wiederherstellung oder Entschlüsselung der Daten ohne den erforderlichen „Key“ ist auf Grund der hohen Qualität der Verschlüsselung derzeit nahezu unmöglich.

Zudem können unter Umständen 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 werden. Bei den neueren Versionen der Schadsoftware erfolgt ebenfalls zu diesem Zeitpunkt die Löschung der sog. „Shadow Copy“, welche bei Vorversionen dieser Schadsoftware in manchen Fällen noch eine Teilwiederherstellung der Daten zuließ.

Empfohlene Vorgangsweisen:

- Seien Sie vorsichtig beim Erhalt von E-Mails, deren Absender Sie nicht kennen oder wenn Sie keine entsprechenden Mitteilungen erwarten.
- Kontrollieren Sie nach Möglichkeit die tatsächliche Absenderadresse, achten Sie auf Ungereimtheiten. Bei angeführten Weblinks legen Sie den Mauszeiger über den entsprechenden Link, ohne diesen zu aktivieren. Sollte die Web-Link-Adresse aufscheinen, kontrollieren Sie, ob diese tatsächlich zum Absender gehört.
- 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. Werden Ihnen Bewerbungsunterlagen zum Download „angeboten“, tun Sie dies bitte nicht! Wenn Sie dennoch der Ansicht sind, dass es sich um echte und notwendige Dokumente handelt, laden Sie die Datei nur in einer gesicherten Umgebung (Sandbox) und auf nicht produktiven Geräten herunter und öffnen diese dann auch dort.
- Wenn Sie sich unsicher sind, öffnen Sie derartige Dateien in einer gesicherten Umgebung (Sandbox, virtuelle Systeme mit Option auf Rücksetzung) oder bedienen Sie sich unterstützender 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 für Ihre 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.
- 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, jedoch liegt es im „Geschäftsmodell“ der Täter, einer solchen nachzukommen! 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.

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



Sehr geehrte Damen und Herren,

anbei erhalten Sie meine Bewerbung für Ihre im Internet ausgeschriebene Stelle. Warum ich die Stelle optimal ausfüllen kann und Ihrem Unternehmen durch meine Erfahrung zahlreiche Vorteile biete, entnehmen Sie bitte meinen ausführlichen und angehängten Bewerbungsunterlagen.

Ich freue mich, wenn ich mich Ihnen noch einmal persönlich vorstellen kann.

Mit freundlichen Grüßen,

[redacted]

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)

Watchlist-Internet –

- Bewerbungen verbreiten Schadsoftware (https://www.watchlist-internet.at/schadsoftware/bewerbungen-verbreiten-schadsoftware/)
- Bewerbungsschreiben verbreiten Ransomware (https://www.watchlist-internet.at/schadsoftware/bewerbungsschreiben-verbreiten-ransomware/)

No More Ransom Projekt: Initiative zur Wiederherstellung von Daten nach Angriffen mit Ransomware (https://www.nomoreransom.org/)

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

FEEDBACK

NEWSLETTER AN-/ABMELDUNG