

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

## Neuerliche Datenverschlüsselungs-Welle durch Ransomware

### *Art der Bedrohung*

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

### *Modus Operandi*

Derzeit werden zahlreiche Fälle gemeldet, bei welchen Computerbenutzer von der Verschlüsselung ihrer privaten oder Firmen-Daten durch [Ransomware](#), vorwiegend durch Chimera, betroffen sind. Für die Entschlüsselung der mittels Endung „.crypt“ versehenen Dateien ist der von der Ransomware generierte Originalschlüssel“ erforderlich, für dessen Bekanntgabe eine Zahlung von 1,5 bis 4 [BitCoins](#) verlangt wird, was bei dem derzeitigen Wert der virtuellen Währung von ~ € 350,- einem Betrag in der Höhe von € 525,- bis 1.400,- entspricht. Eine Entschlüsselung und Wiedererlangung der Daten auf anderem Wege erscheint derzeit nicht möglich.

Die Ransomware wird den Betroffenen zumeist durch in Massen-Mails angehängten und als \*.PDF, \*.DOC oder \*.TXT getarnten Dateien zugestellt. Erst bei genauerer Betrachtung ist erkennbar, dass es sich dabei um ausführbare Dateien mit der Endung \*.exe, \*.bat und weiteren handelt.

**Betriebe und Firmen** sollten **derzeit besondere Vorsicht** beim Einlangen von **Bewerbungsschreiben** walten lassen. Um eine Überprüfung der tatsächlichen Dateiendung von im Anhang befindlichen Schreiben erst gar nicht zuzulassen, ergehen derzeit spezifische Job-Anfragen an Firmen, in welchen vorgegeben wird, dass die Übermittlung der Bewerbungsmappe nicht möglich war. Diese sollte nunmehr von einer [Dropbox](#) des Bewerbers heruntergeladen werden. Der dafür in der Bewerbungs-E-Mail übermittelte Link lässt vorerst keinen Hinweis auf die Dateiendung zu.

Nach dem Download der Datei ist es schwer zu erkennen, dass es sich um eine ausführbare Datei handelt, da zum Einen das Icon auf den entsprechenden vorgegaukelten Dateityp geändert wurde, zum Andren vom Betriebssystem die tatsächliche Endung (je nach Systemeinstellung) erst gar nicht angezeigt wird.

### Empfohlene Vorgangsweisen:

- 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).
- Legen Sie sich eine BackUp-Strategie Ihrer Daten zu. Trennen Sie das BackUp-Medium nach der Sicherung und lösen Sie Share-Links zu BackUp Servern danach auf, um ein Übergreifen durch die Schadsoftware zu verhindern.
- Die Investition in eine entsprechende Sicherheits- und BackUp-Lösung erspart Ihnen Sorgen und Ärger und finanziell höhere Verluste!
- Wir raten keinesfalls den geforderten Betrag zu bezahlen, es sei denn, dass die Wiederherstellung der Daten für Sie unumgänglich erscheint. Eine Garantie auf eine solche, selbst nach Bezahlung, gibt es nicht!
- 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>.

### Beispiel-E-Mail:

Betreff: Bewerbung als XXXXXXXXXXXX

|

Sehr geehrte Damen und Herren,

Durch meine mehr als 5-jährige Berufserfahrung als Tischler und die kontinuierliche, selbständige Weiterbildung bin ich davon überzeugt, ....

Durch meine mehr als 5-jährige Berufserfahrung als Koch und die kontinuierliche, selbständige Weiterbildung bin ich davon überzeugt, ....

Durch meine mehr als 5-jährige Berufserfahrung als Programmierer und die kontinuierliche, selbständige Weiterbildung bin ich davon überzeugt, die mit der herausfordernden Stelle als Programmierer verbundenen Anforderungen zu Ihrer Zufriedenheit erfüllen zu können. Daher bewerbe ich mich hiermit gerne bei Ihrem Unternehmen.

.....

Mit freundlichen Grüßen

Nxxxxx Hxxxxxxxxxxxxxxxxx

Anhang

Bewerbungsunterlagen und Zertifikate

<https://www.dropbox.com/sh/3wxxxxxxxxxxxxaf/AAxxxxxxxxxxxxxxxxxa?dl=0>

Ich konnte die Unterlagen nicht anhängen, dennoch müssen Sie sich nicht extra anmelden um die Bewerbung anzusehen, Entschuldigen Sie bitte die Unannehmlichkeiten!

### (mögliche) Datei in der DropBox:

#### Bewerbung

Name	Größe	Geändert
 BewerbungsMappe.PDF..exe	2,74 MB	vor 3 Tagen

**Hinweis der Ransomware auf die geforderte Bezahlung:**

**Chimera® Ransomware**

Sie wurden Opfer der Chimera® Malware. Ihre privaten Dateien wurden verschlüsselt und sind ohne eine spezielle Schlüsseldatei nicht wiederherstellbar. Möglicherweise funktionieren einige Programme nicht mehr ordnungsgemäß!

Hiermit werden Sie aufgefordert Bitcoins an die unten stehende Adresse zu transferieren, um Ihre persönliche Schlüsseldatei zu erhalten.

**Adresse: 1GaVKrVT17DN4dnWbTqGB9qG3rQrk1JBe9**  
**Forderung: 2,45267544 Bitcoins**

Das Entschlüsselungsprogramm und weitere Informationen, die Sie zur Wiederherstellung Ihrer Dateien benötigen, werden auf der folgenden Webseite zur Verfügung gestellt:

<https://mega.nz/ChimeraDecrypter>

Wenn Sie der Forderung nicht nachgehen, werden wir Ihre persönlichen Daten, Fotos und Videos in Verbindung mit Ihrem Namen im Internet veröffentlichen.

Sollten Sie über keine technische Innung verfügen kontaktieren Sie bitte einen Techniker, der Ihnen bestätigen kann, dass diese Forderung echt ist.

Profitieren Sie von unserem Affiliate-Programm!  
Weitere Informationen im Quelltext dieser Datei.

**Weitere Quellen:**

- Artikel der Polizei Niedersachsen zu „Chimera Ransomware“: <http://www.polizei-praevention.de/aktuelles/chimera-ransomware.html>
- Artikel des Blog von botfrei.de: <http://blog.botfrei.de/2015/10/chimera-ransomware-mit-fokus-auf-firmenrechner/>

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.