NEWS
INFORMATIONEN · TIPPS · RECHERCHEN · BERICHTE

Neue in Österreich auftretende Verschlüsselungs-Trojaner (Ransomware) machen Ihre Daten unwiederbringlich unbrauchbar!

Art der Bedrohung
Verschlüsselung von Privat- und Firmendaten mit anschließender Erpressung zur Bezahlung eines Geldbetrages in Form von BitCoin zur Erlangung des Entschlüsselungs-Codes / Programms

Modus Operandi
Derzeit vergeht kaum eine Woche, in welcher nicht neue Arten von Schadsoftware in Österreich auftauchen. Während viele noch die Nachwirkungen von CryptoLocker und Cerber im Kopf haben, schlägt bereits eine in Österreich neue Schadsoftware zu.

Die derzeit auftretenden Varianten der Ransomware benennen sich Vegclass@aol.com, Salazar-Slytherin10@yahoo.com, usw., der eigentliche Schadcode dürfte dabei jedoch auf die aus Russland stammende Ransomware „Troldesh“ zurück zu führen sein. „Troldesh“ verschlüsselt, ebenso wie die jetzt aktuellen Versionen der Ransomware, sämtliche Benutzerdaten mit einer „.xtbl-Extension“, wobei die heutige Verschlüsselung sämtliche angeschlossene und beschreibbare Peripherie-Geräte sowie das gesamte Netzwerk betrifft.

Die nunmehrigen Versionen ergänzen dabei den Namen mit ihrer eigenen „Signatur“, wie z.B. vegclass@aol.com.xtbl oder ecovector3@aol.com.xtbl. Obwohl verschiedene Varianten der Ransomware mit unterschiedlichen Mailadressen gemeldet wurden, wird von Experten angenommen, dass es sich aufgrund der Verwendung gleicher Hintergrundbilder und Vorgangsweise sowie dem sehr ähnlichen Schadcode, um die gleiche Tätergruppe(n) handelt.

Eine Infektion mit der angeführten Schadsoftware findet auf unterschiedlichste Art und Weise statt, zumeist aber durch aktives Zutun des Benutzers. Das Öffnen von unbekannten Anhängen in nicht vertrauenswürdigen E-Mails oder das Herunterladen von Dateien aus unbekannten Quellen wie z.B. einer fremden DropBox kann ebenso als Auslöser gelten, wie der Aufruf zu einem nicht verifizierten Web-Link, wie er zahlreich in SPAM-Mails oder den berichteten DHL- und Post-Verständigungs-Mails vorhanden ist.

Im Falle des vegclass@aol.com.xtbl wird der Geschädigte aufgefordert, eine E-Mail mit drei verschlüsselten Dateien im Anhang zu senden. Dies benutzen die Täter offensichtlich, um beweisen zu können, dass eine Entschlüsselung der Daten (nach Bezahlung der Erpressungssumme) möglich ist.

Wir raten derart geforderte Zahlungen, die letzten Forderungen lagen nach unserem Wissen im Bereich von 4 BitCoin (bei stark wechselndem Kurs dzt. rund 2.500 Euro), nicht zu leisten. Eine Bezahlung sollte das allerletzte Mittel sein, wenn Sie auf die verschlüsselten Daten keinesfalls verzichten können. Eine Wiederherstellung oder Entschlüsselung der Daten ohne dem erforderlichen „Key“ ist auf Grund der hohen Qualität der Verschlüsselung derzeit nahezu unmöglich.

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.
- **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! 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.
- Verwenden Sie bei der Kontaktaufnahme mit dem Täter **keinesfalls Mail-Adressen von Firmen**; dies könnte eine höhere Forderung des „erpressten Lösegeldes" mit sich ziehen.
- 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**. **Beachten Sie unbedingt**, dass sonst in den meisten Fällen auch **sämtliche BackUp-Files von der Verschlüsselung betroffen und somit nicht wiederherstellbar sind**!

Vorgehen im Schadensfall:

- Trennen Sie die betroffenen Geräte vom Netz und schalten Sie diese aus
- Erstatten Sie umgehend Anzeige auf der nächsten Polizeidienststelle
- Für weitere Informationen kontaktieren Sie die Cybercrime-Meldestelle im Bundeskriminalamt: Tel (24h): +43-1-24836-986500; Email: against-cybercrime@bmi.gv.at

Weiterführende und erklärende Links:

Sensors TechForum (englisch): Beschreibung der Schadsoftware „Vegclass" (http://sensorstechforum.com/remove-ecovector-vegclass-ransomware-xtbl-files/)

Check Point Software Technologies Ltd. (englisch): Beschreibung Ransomware „Troldesh" (http://blog.checkpoint.com/2015/06/01/troldesh-new-ransomware-from-russia/)

NoMoreRansom.org (englisch): Initiative zur Verhinderung von Schadenszahlungen (https://www.nomoreransom.org/decryption-tools.html)

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

Grafischer Desktop nach einer Infektion durch vegclass@aol.com.xtbl: