GEFAHREN

Die Bedrohung durch Ransomware geht nicht nur von einer Tätergruppe aus. Somit kann die Vorgehensweise auch nicht genau definiert werden. Grundsätzlich muss aber ein initialer Einbruch in das System beim Opfer erfolgen. Populär dabei sind folgende Methoden:

Spam Mails

E-Mails mit Betreffs bezüglich:

- Nachricht von Paketdiensten
- Rechnungen
- (Job-)Bewerbungen
- Anwaltsbriefe
- Nachrichten von Social Media Plattformen (Facebook,...)
- und viele andere ...

Darin sind meist Dateien oder Hyperlinks angehängt/angeführt, die beim Öffnen die eigentliche Schadsoftware herunterladen.

IM ZWEIFELSFALL KEINE LINKS ODER DATEIEN ÖFFNEN!!!

GEFAHREN

Fernwartungs-Tools

Zusätzlich werden Fernwartungs-Tools wie derzeit insbesondere der Remotedesktop (über das Remote Desktop Protokoll) von der Täterschaft dazu verwendet, um in ein System einzudringen. Daher erkundigen Sie sich am besten, wie Sie Ihre Fernwartungs-Zugriffe, sofern vorhanden, (besser) absichern können.

Downloads / Werbung

Weitere Wege, sich mit Verschlüsselungstrojanern zu infizieren, sind Drive-by-Downloads bzw. auch Malvertising (Öffnen von Webseiten oder klicken auf infizierte Werbe-Banner, die zur Verbreitung von Schadsoftware verwendet werden).

NO MORE RANSOM!

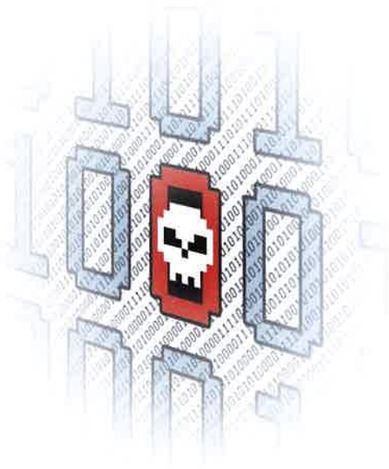
Auf der Webseite **www.NoMoreRansom.org** erhalten Sie weitere Informationen über Ransomware und bereits verfügbare Entschlüsselungstools!

.BK

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
BUNDESKRIMINALAMT

RANSOMWARE

Verschlüsselungstrojaner, Erpressungstrojaner, Cryplo-Trojaner, ...



Information und Prävention

SOKO CLAVIS

WAS IST RANSOMWARE?

Beispiel eines Erpresser-Screens

Ransomware ist eine Schadsoftware, die in einem System persönliche Daten des Nutzers verschlüsselt. Um die Dateien wiederherzustellen, wird ein Lösegeld (häufig in der Kryptowährung Bitcoin) gefordert.

Es gibt dabei zahllose Varianten, die jeweils unterschiedliche Verbreitungswege, Funktionsweisen und Verschlüsselungsalgorithmen nutzen (z.B. Cerber, CrypOL0cker, GoldenEye, Locky, CrySiS, u.v.m.)

PRÄVENTION

Vorsicht

- Finden Sie eine passende **Backup**-Strategie
- Vorsicht bei **Dateianhängen** und **Links in Emails** (auch bei bekanntem Absender!)
- **Makros** in Office Dokumenten nur wenn erforderlich aktivieren
- **Datei-Erweiterung anzeigen** (auch von bekannten Datei-Typen)

Regelmäßige Updates

Vergessen Sie nicht, Ihre Programme regelmäßig auf den aktuellsten Stand zu bringen (**Updates**) und nutzen Sie eine **aktuelle Anti-Viren- Software**.

Zugangsdaten

Verwenden Sie individuelle **Zugangsdaten für den Fernzugriff** auf Ihr Computersystem. Vermeiden Sie „Standarduser" wie Admin, Guest etc. Vergeben Sie dazu komplexe Passwörter.

WENN ES PASSIERT IST...

Sollten Sie in die Situation kommen, dass Ihr Computer, Netzwerk etc. infiziert wurde, schlagen wir u.a. folgende Maßnahmen vor:

Netzwerk und Daten schützen

- Infizierte(n) Computer und andere verbundene Geräte sofort **vom Netzwerk trennen** und, wenn möglich, abschalten
- Verschlüsselte **Datenträger aufbewahren**
- **Wiederherstellung** eines sicheren Betriebs
- **Schließen von Sicherheitslücken**
- **Passwörter/Zugangsdaten** nach dem Angriff **ändern**

Anzeigen

Anzeigenerstattung in der nächstgelegenen Polizeidienststelle. Die angezeigten Sachverhalte in Zusammenhang mit Ransomware werden zentral im Bundeskriminalamt von der SOKO Clavis weiterbearbeitet.

Cybercrime Competence Center
Meldestelle against Cybercrime
Tel (24h): +43-(0)1-24836 Dw. 986500
E-Mail: against-cybercrime@bmi.gv.at