Cryptowall 3.0 entfernen

Cryptowall 3.0 ist eine Form von Ransomware / Cryptolocker, welche **Daten verschlüsselt** und nur gegen Bezahlung eines Lösegeldes (=Ransom) wieder entschlüsselt.

Cryptowall **entfernt sich nach der Verschlüsselung sämtlicher Daten selbst** und hinterlässt praktisch keine Spuren. Eine direkte Entfernung ist damit nicht möglich/nötig. Nichtsdestotrotz kann folgender Ablauf zur Überprüfung durchgeführt werden.



1. Computer im abgesicherten Modus starten
2. Autostart bereinigen
3. %appdata% bereinigen
4. Analog zu Ransomware entfernen verfahren (Kaspersky Rescue Disc)

Der auf anderen Seiten empfohlene **„Cryptowall 3.0 Remover“** oder **„Spyhunter-Installer“** ist eine klassische Rogueware. Von der Installation dieser Software und einer somit auf den ersten Blick scheinbar einfacheren Lösung **wird dringend abgeraten!**

Cryptowall Daten entschlüsseln

Eine Entschlüsselung der Daten ohne den korrekten Entschlüsselungscode **ist zurzeit nicht möglich**. Einzige Hoffnung ist das **Wiederherstellen der Daten von einem sauberen Backup** oder aber der Versuch Daten aus Caches, Volume Shadow Copies, etc. wiederzubeschaffen.

Dementsprechend empfiehlt sich folgendes Vorgehen:

1. Netzwerkverbindungen trennen, Infizierter Computer ausschalten (evtl. wurden noch nicht alles Files verschlüsselt)
2. Versuchen unverschlüsselte Daten per LiveCD zu exportieren

Die übrigen verschlüsselten Daten können mit ListCWall als Liste exportiert werden. Diese Liste kann

anschliessen genutzt werden, um die Daten aus anderen Quelle wiederherzustellen, z.B.

- Volume Shadow Copy
- Backups
- Caches / Zwischenspeicher
- Externe Medien (z.B. USB-Sticks, Festplatten)
- E-Mails

Prävention

Zu **Vermeidung** einer Infektion oder aber wenn Sie **bereits** von Cryptowall 3.0 **betroffen** sind, sollten folgende Punkte beachtet werden:

- System **regelmässig** aktualisieren (insbesondere Java)
- **Zuverlässigen** Antivirus verwenden (z.B. Kaspersky)
- **Vorsicht** bei Mailanhängen (Artikel dazu: Ein Fax mit Folgen)
- Backups **korrekt** einrichten (Mind. 3-2-1 Regel beachten)

Bemerkungen

- Cryptowall 3.0 verschlüsselt **unbekannte Dateiformate nicht**, um das System funktionsfähig zu halten
- Aus demselben Grund werden **Systemdaten** nicht verschlüsselt
- Der Cryptolocker entfernt sich nach Beendigung der Arbeit selbständig vom System
- Cryptowall 3.0 kann nur Daten verschlüsseln, auf die der betroffene Benutzer **Schreibberechtigungen** hat
- Originaldaten werden von Cryptowall nach der Verschlüsselung **mehrfach überschrieben** - eine Wiederherstellung der Daten auf dem betroffenen Computer ist damit praktisch nicht möglich.
- Die Infizierung erfolgt zurzeit **nur auf Windowssystemen**. Hingegen kann **Cryptowall auch Daten auf NAS, Server, etc. verschlüsseln** sofern der infizierte Computer diese als **Netzlaufwerke** mit Schreibberechtigungen angehängt hat.
- Nachdem wir einige Fälle in der Schweiz festgestellt haben, scheinen nun v.a. Benutzer aus Deutschland und Österreich betroffen zu sein.

ListCWall

Mt dem Tool ListCWall kann eine Liste der mit Cryptowall verschlüsselten Daten angezeigt werden[1)].

Befehl	Beschreibung
listcwall -h	This command will list the help file for ListCwall.
listcwall -q	This command will suppress the output of the ListCwall program.
listcwall -m	This command will move the encrypted files to the %Desktop%\ListCWall_Backup folder.

Befehl	Beschreibung
listcwall -c	This command will copy the encrypted files to the %Desktop%\ListCWall_Backup folder.
listcwall -m -b c:\backup	This command will move the encrypted files to the C:\backup folder.
listcwall -c -b c:\backup	This command will copy the encrypted files to the C:\backup folder.

Direkthilfe

Sofern Sie Hilfe bei der Wiederherstellung von gesperrten Daten durch Cryptowall 3.0 benötigten, können wir Ihnen im Rahmen des technisch möglichen gerne weiterhelfen. Kontaktieren Sie uns.

1)

http://www.bleepingcomputer.com/download/listcwall/

Pedrett AG IT+Web

Dieses Dokument stammt aus dem Wiki der Pedrett IT+Web AG.
Unter Berücksichtigung der Nutzungsbedingungen ist eine Weiterverbreitung des Inhalts erlaubt, solange die Pedrett IT+Web AG als Autor genannt wird.

Zum Eintrag