

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.

Dear Ransom Note to your files!
All of your files are encrypted with RSA-2048 using Cryptowall 3.0.
The information about the decryption key using RSA-2048 can be found here: www.verschlusself.de/verschlusself.com
What does RSA mean?
This means that the attack and RSA offers your files have been irreversibly encrypted, you will not be able to work with them, read them or edit them. It is the same thing as losing them forever, but with our help, this can't happen.
How did it happen?
All your files are encrypted with the public key which has been transferred to your computer via the internet. Decryption of your files is only possible with the help of the private key and the program, which is on our server.
What are keys?
Again, if you do not have the decryption key, then it is not possible to obtain the private key with the program. If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.
For more specific instructions, please visit our personal forum page, there are a few different addresses pointing to your page below:
1. tiny.cc/meyarw
2. tiny.cc/meyarw
3. tiny.cc/meyarw
4. tiny.cc/meyarw
If the above links to the address are not available, follow this one instead:
1. Download and install the browser: tiny.cc/meyarw
2. After a successful installation, open this address and wait for initialization.
3. Type in the Address bar:
4. If you see the situation is the site
IMPORTANT INFORMATION:
• tiny.cc/meyarw • tiny.cc/meyarw • tiny.cc/meyarw
• tiny.cc/meyarw • tiny.cc/meyarw • tiny.cc/meyarw

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 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 alle 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)

Obwohl die Priorität bei einer Infizierung durch Cryptowall in erster Linie auf dem Wiederherstellen der Daten liegt, darf die **Absicherung des System keinesfalls vernachlässigt werden**. „Einfach schnell einen Antivirus“ zu installieren reicht in den meisten Fällen nicht aus und wird auch zukünftigem Befall nicht zuverlässig vorbeugen!

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 selbstständig 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.
- Zurzeit scheinen vermehrt Nutzer aus der DACH-Region (Deutschland, Österreich, Schweiz) betroffen zu sein
- Die Dateien HELP_DECRYPT.HTML, HELP_DECRYPT.PNG, HELP_DECRYPT.URL, HELP_DECRYPT.TXT sind nicht schädlich, sondern dienen nur dazu infizierte Ordner zu markieren.

ListCWall

Mit dem Tool [ListCWall](#) kann eine Liste der mit Cryptowall verschlüsselten Daten angezeigt werden¹⁾.

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.
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 und der **Vermeidung** eines solchen Szenarios benötigten, können wir Ihnen gerne **weiterhelfen**.

[Kontaktieren](#) Sie uns unverbindlich.

¹⁾

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



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](#)