Anleitung zum Emsisoft-Decrypter für STOP Djvu

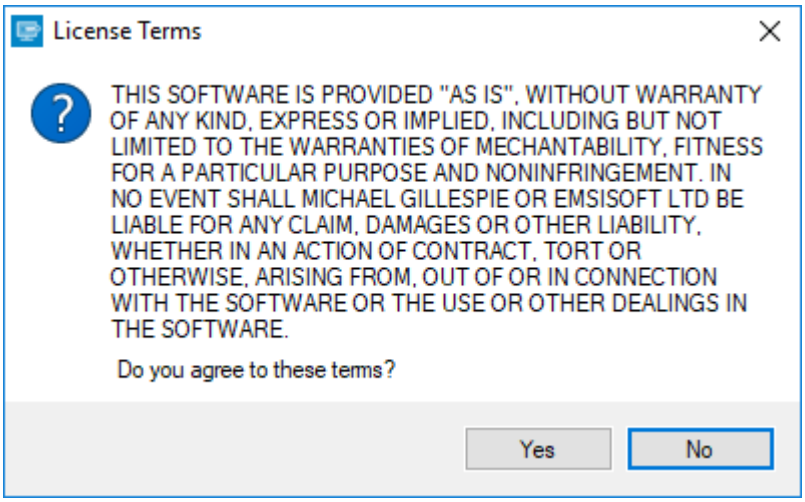
WICHTIG! Verschieben Sie die Malware zunächst auf Ihrem System in Quarantäne. Anderenfalls werden Ihre Dateien erneut verschlüsselt oder Ihr System wieder gesperrt. Falls Ihre aktuelle Antivirenlösung den Schädling nicht erkennen kann, verwenden Sie die kostenlose Testversion von Emsisoft Anti-Malware, um ihn in Quarantäne zu verschieben. Wenn Ihr System über die Remotedesktopfunktion von Windows infiziert wurde, raten wir Ihnen, die Kennwörter sämtlicher Benutzer zu ändern, die sich per Fernzugriff anmelden dürfen. Überprüfen Sie auch Ihre lokalen Benutzerkonten, ob die Angreifer eventuell eigene Konten hinzugefügt haben.

Hinweis: Während das Tool ausgeführt wird, muss es die gesamte Zeit mit dem Internet verbunden sein, um vom Server Anweisungen zur Entschlüsselung empfangen zu können.

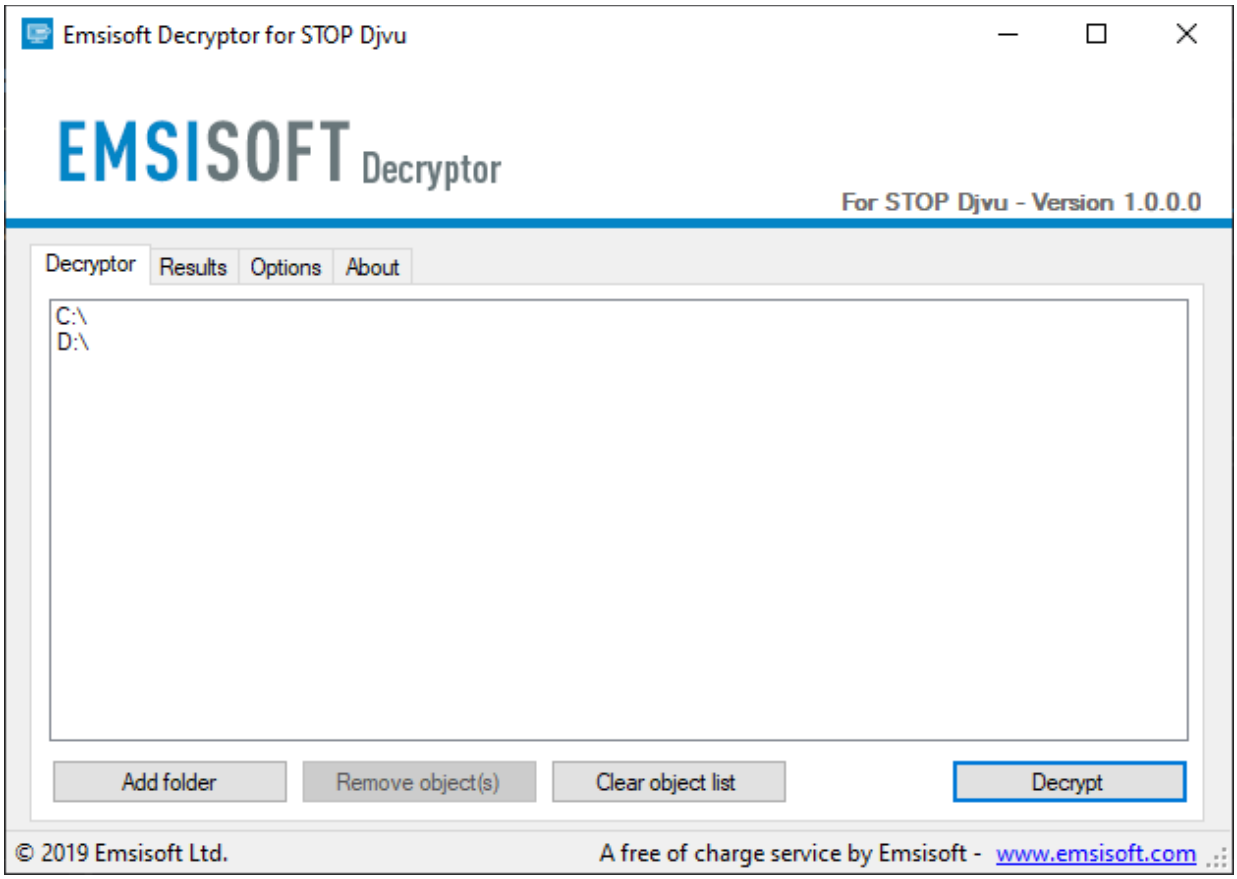
Es gibt einige Einschränkungen, welche Dateien entschlüsselt werden können. Für sämtliche Versionen von STOP Djvu gilt: Dateien können erfolgreich entschlüsselt werden, wenn sie mit einem uns vorliegenden Offline-Schlüssel verschlüsselt wurden. Im Falle von alten Djvu-Versionen (nur bis August 2019) lassen sich Dateien auch mithilfe eines Paars aus verschlüsselter und Originaldatei entschlüsseln, das Sie über das STOP-Djvu-Portal einreichen können. Weitere Informationen dazu finden Sie auf der Portalseite

So entschlüsseln Sie Ihre Dateien

1. Laden Sie sich den Decrypter von derselben Seite herunter, auf der Sie auch diese Anleitung gefunden haben.
2. Führen Sie den Decrypter als Administrator aus. Wenn Ihnen die Lizenzbedingungen angezeigt werden, klicken Sie auf „Yes“, um diesen zuzustimmen.



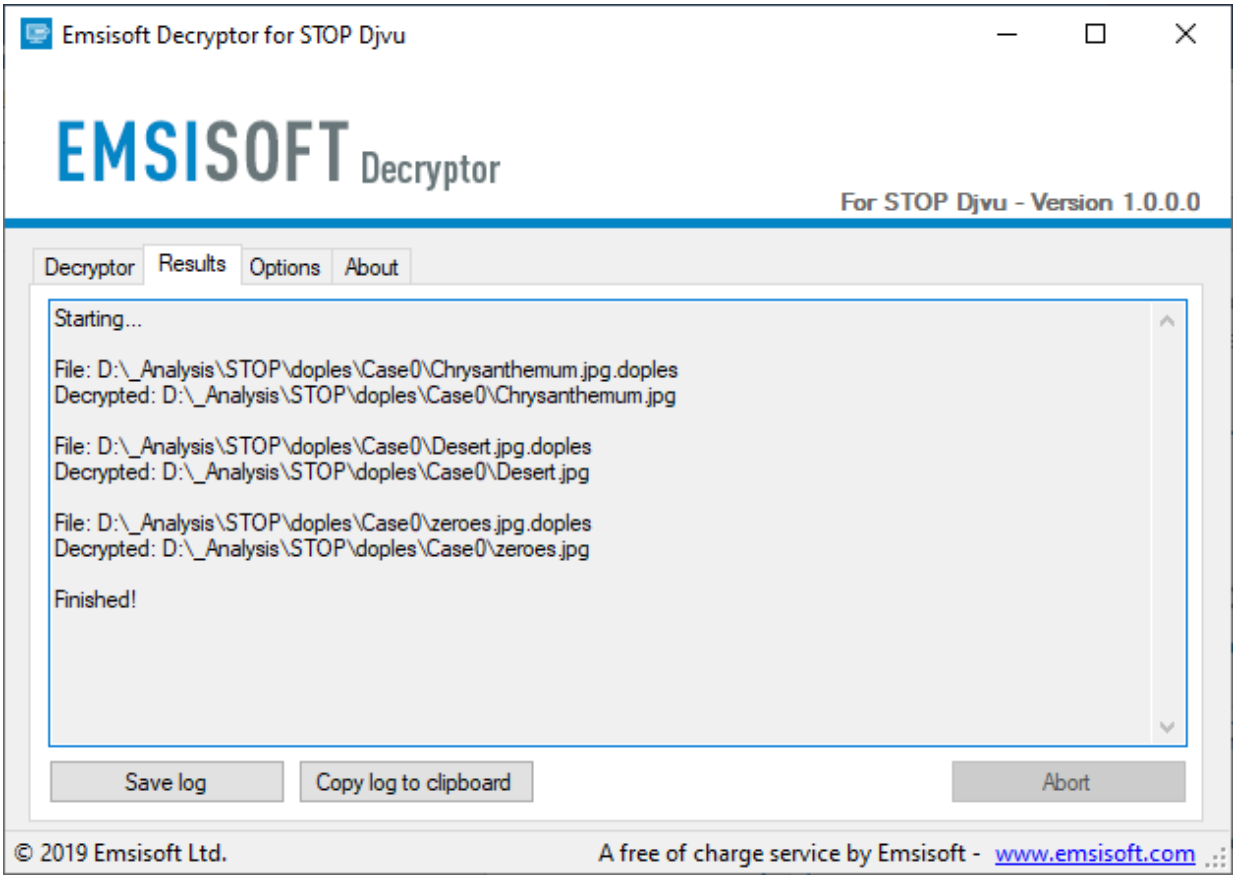
3. Nach Bestätigung der Lizenzbedingungen wird das Hauptfenster des Decrypters geöffnet:



4. Standardmäßig werden Ihnen die aktuell lokal oder über das Netzwerk verbundenen Laufwerke zum Entschlüsseln vorgeschlagen. Über die Schaltfläche „Add" können Sie weitere Speicherorte hinzufügen.

5. Abhängig von der jeweiligen Malware-Familie bieten Decrypter in der Regel unterschiedliche Optionen an. Die jeweils verfügbaren Optionen finden Sie im Register „Options“ (Optionen), wo Sie diese aktivieren oder deaktivieren können. Eine Liste der verfügbaren Optionen finden Sie im Folgenden.

6. Wenn Sie alle Speicherorte, die Sie entschlüsseln möchten, zu der Liste hinzugefügt haben, klicken Sie auf „Decrypt“, um mit dem Entschlüsseln zu beginnen. Ihnen wird nun der jeweils aktuelle Prozess und der Entschlüsselungsstatus Ihrer Dateien angezeigt:



7. Sie erhalten eine Meldung, wenn der Decrypter den Entschlüsselungsvorgang abgeschlossen hat. Klicken Sie auf „Save log“, um bei Bedarf einen Bericht für Ihre eigenen Unterlagen zu speichern. Sie können das Protokoll mit „Copy log to clipboard“ auch direkt in die Zwischenablage kopieren, um es in eine E-Mail oder einen Forumbeitrag einzufügen, wenn Sie darum gebeten werden.

Verfügbare Decrypter-Optionen

Dieser Decrypter bietet derzeit folgende Optionen:

- **Keep encrypted files** (Verschlüsselte Dateien behalten)
  Da die Ransomware keine Informationen über die unverschlüsselten Dateien speichert, lässt sich mit dem Decrypter leider nicht garantieren, dass die entschlüsselten Daten mit denen identisch sind, die zuvor verschlüsselt wurden. Daher ist der Decrypter vorsichtshalber standardmäßig so eingestellt, dass die verschlüsselten Dateien auch nach dem Entschlüsseln nicht gelöscht werden. Wenn Sie möchten, dass der Decrypter die verschlüsselten Dateien nach ihrer Verarbeitung löscht, können Sie diese Option deaktivieren. Das ist eventuell notwendig, wenn Sie nur über beschränkten Speicherplatz verfügen.

Entschlüsselung von STOP Djvu

Zur Entschlüsselung Ihrer Dateien benötigen wir einige verschlüsselte Dateien und deren Originalversionen.
Diese Dateipaare müssen folgende Bedingungen erfüllen:

• Die verschlüsselte Version und das Original müssen von derselben Datei stammen.[1]
• Für jedes zu entschlüsselnde Dateiformat benötigen wir ein anderes Dateipaar.[2]
• Die Dateien müssen mindestens 150 kB groß sein.

[1] Als Originale eignen sich etwa aus dem Internet heruntergeladene Dateien, per E-Mail verschickte Dokumente, standardmäßige Windows-Hintergrundbilder oder Kopien von Wechseldatenträgern.
[2] Zum Entschlüsseln von PNG-Dateien benötigen wir zum Beispiel eine verschlüsselte PNG-Datei und ihr Original. Je nach Dateiformat kann es sein, dass weitere Anforderungen erfüllt werden müssen.

Hinweis: Diese Dienstleistung gilt nicht für die neuen Versionen, bei denen eine RSA-Verschlüsselung eingesetzt wird.
Wenn Ihre Dateien nach August 2019 verschlüsselt wurden, handelt es sich höchstwahrscheinlich um eine dieser neuen Versionen.

Verschlüsselte Datei

Originaldatei

Einreichen

Häufig gestellte Fragen
F: Was mache ich, wenn meine Dateien zu groß zum Hochladen sind?
Wenden Sie sich bitte an unseren Support. Wir werden Ihnen dann mit einer Alternative helfen.

F: Was geschieht mit den Dateien, die ich hochlade?
Datenschutz und Privatsphäre stehen für uns an oberster Stelle. Wie werden die von Ihnen bereitgestellten Dateien lediglich nutzen, um Ihnen das Entschlüsseln einiger Ihrer Dateien zu ermöglichen. Anschließend werden die Dateien sofort wieder von unseren Servern gelöscht. Es werden keinerlei personenbezogenen Daten gespeichert.

F: Welche Dateiendungen werden unterstützt?
Derzeit unterstützt werden:
.shadow, .djvu, .djvur, .djvuu, .udjvu, .uudjvu, .djvuq, .djvus, .djvur, .djvut, .pdff, .tro, .tfude, .tfudet, .tfudeq, .rumba, .adobe, .adobee, .blower, .promos, .promoz, .promorad, .promock, .promok, .promorad2, .kroput, .kroput1, .pulsar1, .kropun1, .charck, .klope, .kropun, .charcl, .doples, .luces, .luceq, .chech, .proden, .drume, .tronas, .trosak, .grovas, .grovat, .roland, .refols, .raldug, .etols, .guvara, .browec, .norvas, .moresa, .vorasto, .hrosas, .kiratos, .todarius, .hofos, .roldat, .dutan, .sarut, .fedasot, .berost, .forasom, .fordan, .codnat, .codnat1, .bufas, .dotmap, .radman, .ferosas, .rectot, .skymap, .mogera, .rezuc, .stone, .redmat, .lanset, .davda, .poret, .pidom, .pidon, .heroset, .boston, .muslat, .gerosan, .vesad, .horon, .neras, .truke,

.dalle, .lotep, .nusar, .litar, .besub, .cezor, .lokas, .godes, .budak, .vusad, .herad, .berosuce, .gehad, .gusau, .madek, .darus, .tocue, .lapoi, .todar, .dodoc, .bopador, .novasof, .ntuseg, .ndarod, .access, .format, .nelasod, .mogranos, .cosakos, .nvetud, .lotej, .kovasoh, .prandel, .zatrov, .masok, .brusaf, .londec, .krusop, .mtogas, .nasoh, .nacro, .pedro, .nuksus, .vesrato, .masodas, .cetori, .stare, .carote

F: Was mache ich, wenn meine Dateiendung hier nicht aufgeführt ist?
Ihre Dateien wurden höchstwahrscheinlich mit einer neuen Version verschlüsselt, die das RSA-Kryptosystem einsetzt. Deren Entschlüsselung ist derzeit leider ohne Offline-Schlüssel noch nicht möglich.
Wir empfehlen Ihnen, den Decrypter dennoch auszuprobieren. Einige Dateien lassen sich möglicherweise wiederherstellen, falls sie doch mit einem der uns vorliegenden Offline-Schlüssel verschlüsselt wurden.