



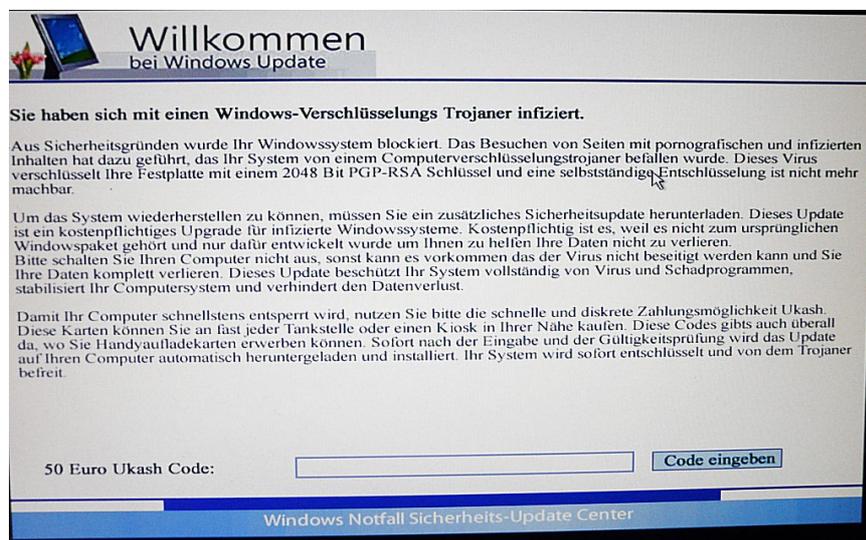
Essen, 14.05.2012

BITFOX Ltd. & Co. KG  
Postfach 102523  
45025 Essen

## Verschlüsselung-Trojaner 4/2012, Typ I

1) Hat es mich erwischt?

Wenn Sie diesen Bildschirm gesehen haben,  
sind sie aller Wahrscheinlichkeit nach betroffen:

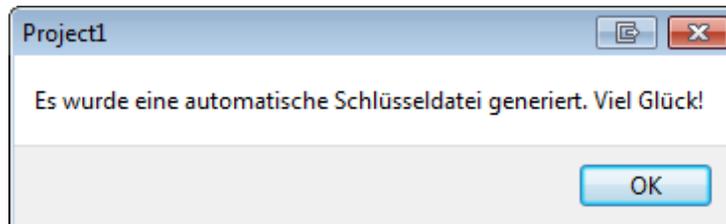


Alle ihre Dateien liegen nun im Format locked-dateiname.alt.1234 vor und sind nicht mehr lesbar.

2) Was kann ich nun tun?

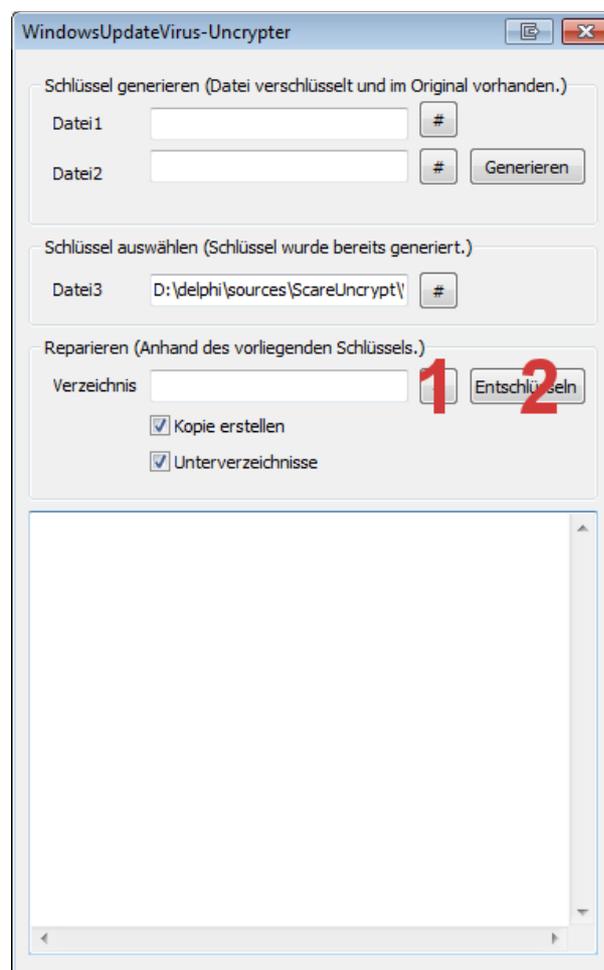
Laden Sie unser Tool herunter (ist anscheinend schon geschehen :-)

Nach dem Starten generiert das Programm nach Möglichkeit selbst einen Schlüssel und meldet sich mit der folgenden Meldung:



Sie brauchen dann nicht mehr viel durchführen:

Wählen Sie **1** das Verzeichnis, in dem sich ihre verschlüsselten Dateien befinden und schon kann es los mit dem **2** Entschlüsseln los gehen.



- 3) Es wurde kein Schlüssel erstellt bzw. scheint der Schlüssel nicht bei allen Dateien zu funktionieren.

Oft kann es passieren, dass leider kein automatischer Schlüssel gefunden wurde.

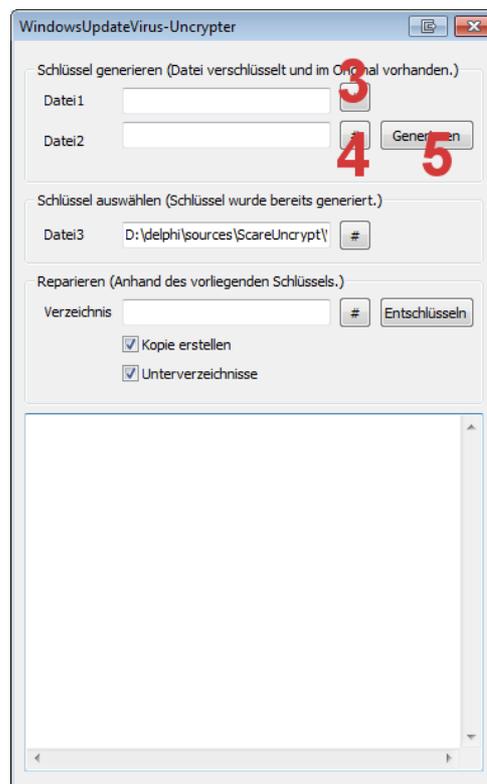
Auch kann es passieren, dass der Rechner beim Verschlüsseln gestört (abgeschaltet) wurde und so verschiedene Schlüssel für verschiedene Verzeichnisse benötigt werden.

### **Immer dann muss man selbst einen Schlüssel erzeugen.**

Dafür benötigt man dann zunächst **3** eine Datei die verschlüsselt wurde und nochmals die **4** Datei im „heilen“ Zustand – also so, wie sie eigentlich aussehen sollte.

Vielleicht haben Sie als Vorlage ein verschlüsseltes Bild auf der Festplatte, welches sie jemanden aus Ihrer Familie vorher per eMail gesendet haben?  
Vielleicht besitzen Sie eine Datei auch noch mal auf einem Medium wie einer CDROM als Sicherheitskopie?

Wählen Sie dann **3** die „heile“ Datei aus und unter **4** die defekte Datei aus um dann



den Schlüssel **5** zu generieren.

Entschlüsseln Sie dann wie gewohnt. (Siehe das vorherige Kapitel 2. )

4) Hat geklappt – Danke!

Wir freuen uns, wenn wir Ihnen in Erinnerung bleiben!

Sollten Sie finanziell etwas beitragen wollen, so spenden Sie doch bitte einen Betrag an den

Arbeitskreis für Jugendhilfe Ahlen e.V.  
Hellstr. 5  
59227 Ahlen

<http://www.akj-ahlen.de/start.htm#spende>

Konto 1004282      BLZ 40050150

Der Verein ist als gemeinnützig anerkannt und stellt Ihnen gern eine Spendenquittung aus, die sie ggf. von der Steuer absetzen können.

Wir selbst freuen uns über jeden Cent der dort ankommt -  
und natürlich auch über eine Postkarte mit einem bloßen „Danke“!

BITFOX Ltd. & Co. KG  
Postfach 102523  
45025 Essen

<http://startseite.bitfox24.de>

Sollen wir Sie über neue Dinge rund um die BITFOX Ltd. informieren,  
schreiben Sie bitte ihre eMail-Adresse mit auf die Postkarte.

5) Hat alles nicht funktioniert – und nun?

Sie haben leider den „großen Bruder“ des ursprünglichen Trojaners erwischt.  
Senden Sie uns bitte Ihre Erfahrungen an [spamdb@bitfox24.de](mailto:spamdb@bitfox24.de)

**Werfen Sie die verschlüsselten Dateien nicht weg!**  
**(DER HAKEN SICHERHEITSKOPIE IST NICHT OHNE GRUND VORHANDEN!)**

Besonders wichtig für uns sind:

- a) Der Trojaner ansich – bitte anhängen!
- b) Das Einschaltbild – was genau steht auf dem Bildschirm? (Photo!)
- b) Ein paar verschlüsselte Dateien, bitte um die
- c) Nach Möglichkeit die gleichen Dateien im „heilen“ Zustand
- d) Den Weg, wie Sie sich ihren PC angesteckt haben
- e) Ggf. ergänzende Informationen, wie z.B. von welcher eMail-Adresse kam die infizierte eMail etc. pp.

Schon jetzt DANKE! - denn nur so können wir weiter helfen.

Hinweis: Natürlich verlassen Ihre persönlichen Daten niemals unser Haus!

6) Anleitung nicht gelesen.

Leider mussten wir feststellen, dass einige Menschen die obigen Hinweise nicht beachtet haben. Das Resultat ist dann sehr ernüchternd:

Die Anwender besitzen nun Dateien die im Windows-Explorer wieder korrekt assoziiert werden, doch der Anfang der Datei ist noch immer verschlüsselt.

Die Dateien können noch nicht fehlerfrei geöffnet werden.

Die Dateien können also mit diesem Tool noch nicht entschlüsselt werden.

Sie müssen leider auf das nächste Entschlüsselungstool warten!

Wenn der Anwender nun den Haken „Kopie erstellen“ entfernt hat, hat der Anwender ein zusätzliches Problem geschaffen:  
Das neue Tool wird nun keine Dateien mehr finden, die es entschlüsseln kann...

Wir haben für solche Fälle ein Tool bei gelegt, welches die „nicht wirklich“ entschlüsselten Dateien wieder in verschlüsselte Daten verwandelt - nahezu so, wie der Trojaner sie schuf.  
Benennen Sie dafür die beiliegende Datei „ScareCrypt.Ex-“ in „ScareCrypt.EXE“ um.

**WIR BIETEN AUF DIESES TOOL KEINERLEI SUPPORT.**

**WIR KÖNNEN NICHT GARANTIEREN, DASS EIN FOLGETOOL MIT DIESEN ZURÜCK VERSCHLÜSSELTEN DATEN PROBLEMLOS WEITER ARBEITEN KÖNNEN WIRD.**

**LÖSCHEN SIE DAHER N-I-E-M-A-L-S DIE VERSCHLÜSSELTEN DATEN, BIS DIESE AUCH WIRKLICH ERFOLGREICH ENTSCHLÜSSELT UND GETESTET WURDEN!**