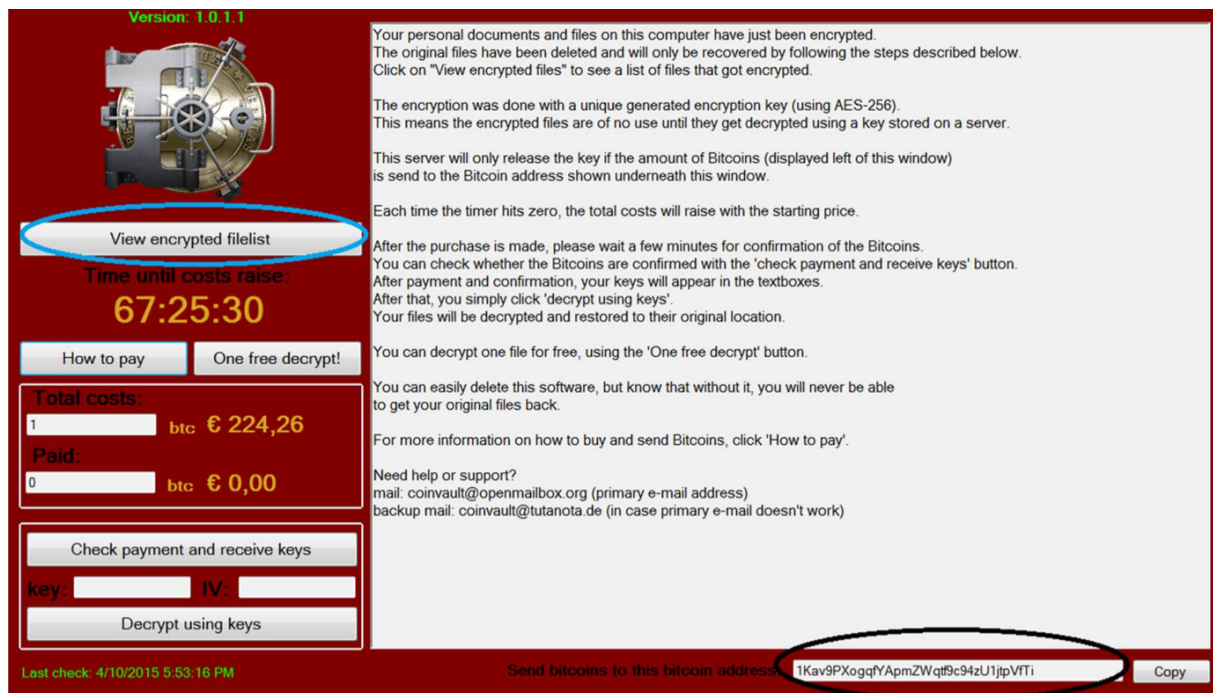


Poradnik: Jak usunąć szkodliwe oprogramowanie CoinVault z komputera i odzyskać zaszyfrowane pliki

Krok 1. Czy jesteś zainfekowany oprogramowaniem ransomware CoinVault?

Identyfikacja infekcji jest całkiem prosta - na zarażonym komputerze wyświetlany jest komunikat widoczny na poniższym rysunku.



Zrzut ekranu komputera zainfekowanego szkodliwym oprogramowaniem CoinVault

Krok 2. Zdobądź adres portfela Bitcoin.

W prawym dolnym rogu komunikatu wyświetlanego przez szkodliwe oprogramowanie CoinVault znajduje się adres portfela Bitcoin (zakreślony na czarno na powyższym zrzucie ekranu). Skopiuj ten adres.

Krok 3. Zdobądź listę zaszyfrowanych plików.

W lewej górnej sekcji komunikatu wyświetlanego przez szkodliwe oprogramowanie CoinVault znajduje się przycisk „View encrypted filelist” (zakreślony na niebiesko na powyższym zrzucie ekranu). Kliknij ten przycisk i zapisz listę zaszyfrowanych obiektów do pliku.

Krok 4. Usuń szkodliwe oprogramowanie CoinVault.

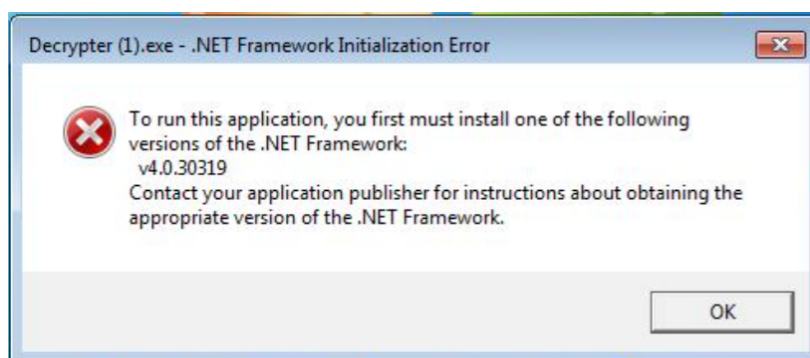
Pobierz wersję testową produktu Kaspersky Internet Security ze strony <https://kas.pr/kismd-cvault> i zainstaluj ją. Aplikacja usunie szkodliwe oprogramowanie CoinVault z Twojego komputera.

Krok 5. Wejdź na stronę <https://noransom.kaspersky.com>.

Wejdź na stronę <https://noransom.kaspersky.com> i podaj adres portfela Bitcoin z kroku 2 tego poradnika. Jeżeli adres zostanie rozpoznany, wyświetlone zostaną informacje o wektorze inicjującym (IV) oraz kluczu. W pewnych okolicznościach może pojawić się większa liczba wektorów inicjujących oraz kluczy. Jeżeli tak się stanie, zapisz wszystkie wyświetlone informacje na komputerze - będziesz ich potrzebował później.

Krok 6. Pobierz narzędzie deszyfrujące.

Pobierz narzędzie deszyfrujące ze strony <https://noransom.kaspersky.com> i uruchom je na swoim komputerze. Jeżeli na ekranie pojawi się komunikat o błędzie (widoczny poniżej), przejdź do kroku 7. Jeżeli komunikat taki nie pojawi się, przejdź do kroku 8.

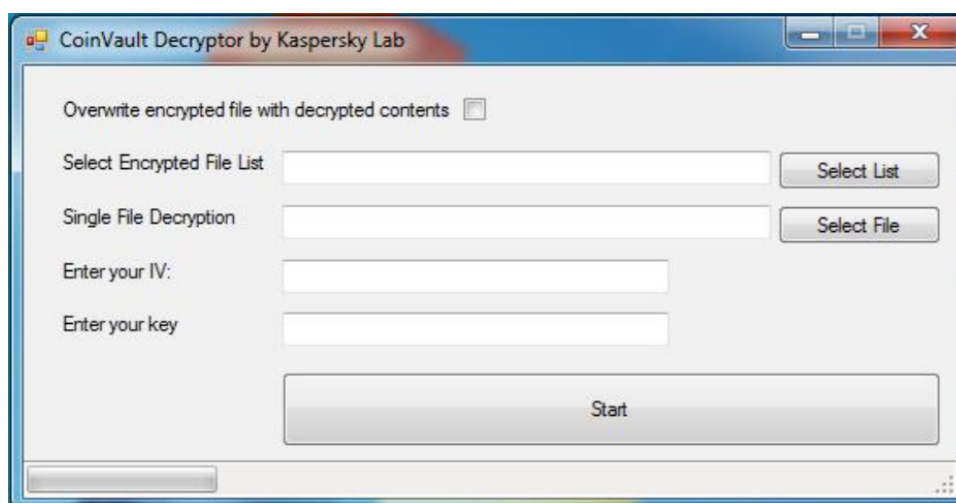


Krok 7. Pobierz i zainstaluj biblioteki dodatkowe.

Otwórz stronę <http://www.microsoft.com/pl-PL/download/details.aspx?id=40779>, pobierz i zainstaluj Microsoft .NET Framework zgodnie ze znajdującymi się tam informacjami.

Krok 8. Odszyfruj swoje pliki.

Uruchom pobrane wcześniej narzędzie deszyfrujące. Na ekranie pojawi się poniższe okno.



Podczas pierwszego uruchamiania narzędzia zalecamy wykonanie następujących działań:

- kliknij przycisk „Select File” w sekcji „Single File Decryption” i wskaż plik, który chcesz odszyfrować;
- wprowadź wektor inicjujący (IV) z kroku 5 tego poradnika w polu „Enter your IV”;
- wprowadź klucz z kroku 5 tego poradnika w polu „Enter your key”;
- kliknij przycisk „Start”.

Sprawdź, czy nowo utworzony plik został prawidłowo odszyfrowany. Jeżeli tak, zaznacz opcję „Overwrite encrypted file with decrypted contents”, kliknij przycisk „Select List” w polu „Select Encrypted File List”, wskaż plik zawierający listę zaszyfrowanych plików (utworzony w kroku 3 tego poradnika) i ponownie kliknij przycisk „Start”.

Jeżeli po podaniu adresu portfela Bitcoin na stronie <https://noransom.kaspersky.com> (w kroku 5 tego poradnika) wyświetlona została większa liczba wektorów inicjujących (IV) i kluczy, zachowaj szczególną ostrożność. Obecnie analitycy nie mają pewności, skąd pochodzą takie wielokrotne informacje dla jednego portfela Bitcoin. W takim przypadku pozostaw opcję „Overwrite encrypted file with decrypted contents” bez zaznaczenia i spróbuj odzyskać jeden plik (z listy wygenerowanej w kroku 3 tego poradnika). Jeżeli nowy plik nie zostanie poprawnie odszyfrowany, spróbuj ponownie podając inną parę IV/klucz. Powtarzaj ten proces aż do momentu, gdy uzyskasz poprawnie odszyfrowany plik. Wówczas możesz zastosować poprawną parę IV/klucz do wszystkich plików z listy.