ESET Crysis Decryptor

Інструкція з видалення загрози Crysis
за допомогою дешифратора ESET

НАСОЛОДЖУЙСЯ БЕЗПЕКОЮ

Ознаки інфікування:

- Продукт ESET виявив загрозу Win32/Filecoder.Crysis.
- Особисті файли зашифровані, а інформація про здійснення шифрування відображається у вигляді фону робочого столу комп'ютера (рис. 1-1) або в .txt, .html, .png файлі.
- Файлам присвоєно одне з розширень: .xtbl, .crysis, .crypt.
- На робочому столі відображається одне з повідомлень:

  «Увага! Ваш комп'ютер був атакований вірусом шифрування.. bitcoin143@india.com»

  «Ваші дані зашифровані... Не намагайтеся розшифрувати їх – дані будуть втрачені... checksupport@163.com»

  Відновити інформацію через технічну підтримку по електронній пошті»

  «Всі ваші дані були зашифровані, щоб повернути їх пишіть на helphomeless@india.com»

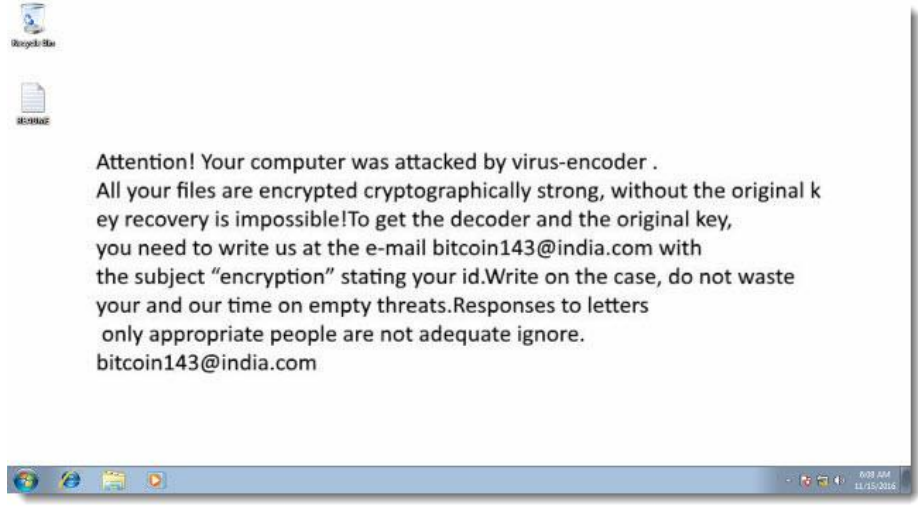


Рис. 1-1
Зразок повідомлення про здійснення шифрування, яке відображається на робочому столі

Детальніше:

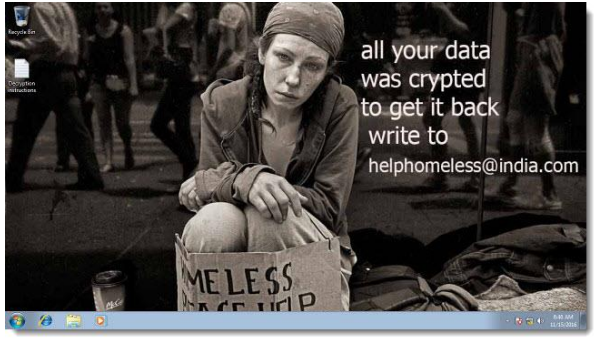
Win32/Filecoder.Crysis – це троян, який шифрує файли на локальних дисках та вимагає сплатити викуп через платіжну систему Bitcoin.

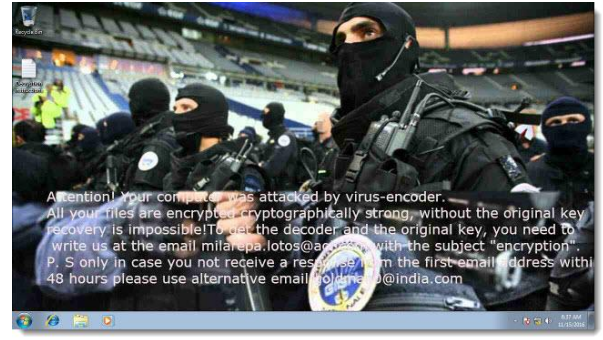
- Опис загрози Win32/Filecoder.Crysis на virusradar.com
- Реліз: Світ після TeslaCrypt: сімейство Crysis претендує на першість серед програм-вимагачів

Показники інфікування:

.{%EmailAddress%}.CrySiS
.{%EmailAddress%--%EmailAddress%}.xtbl
.ID%hexnum%.%EmailAddress%.xtbl
.id-%hexnum%.{%EmailAddress%}.crypt

Приклади робочих столів інфікованих комп’ютерів:





Як видалити загрозу:

1. Завантажте інструмент та збережіть файл на робочому столі.
   ESETCRYSISDECRYPTOR.EXE
2. Натисніть кнопку **Пуск** → **Усі програми** → **Стандартні**, клацніть правою кнопкою миші на **Командний рядок**, а потім виберіть **Запуск від імені адміністратора** в контекстному меню.
3. **Користувачі Windows 8 / 8.1 / 10:** натисніть клавішу Windows + **Q** для пошуку додатків, введіть **Командний рядок** в полі **Пошук**, клацніть правою кнопкою миші на Командний рядок, а потім виберіть **Запуск від імені адміністратора** в контекстному меню.
4. Введіть команду cd %userprofile%\Desktop (не замінюйте «userprofile» своїм іменем користувача), а потім натисніть **Enter**.
5. Введіть команду ESETCrysisDecryptor.exe та натисніть **Enter**.
6. Прочитайте та підвердьте згоду з умовами ліцензійної угоди з кінцевим користувачем.
7. Введіть ESETCrysisDecryptor.exe C: та натисніть **Enter**, щоб сканувати диск C в автоматичному режимі. Для сканування іншого диску замініть C: на назву відповідного диска.

Ключі дешифратора Crysis

У більшості випадків, запуск дешифратора відповідно до попереднього пункту, є найкращим способом. Крім цього, Ви також можете використовувати наявні ключі для інструменту Crysis:

- /s — запустити інструмент в автоматичному режимі
- /d — запустити інструмент в режимі виправлення помилок
- /h або /? — показати використання

8. Інструмент розшифрування буде запущений, а на екрані відобразиться повідомлення «Looking for infected files...» («Пошук інфікованих файлів»). У разі виявлення загрози виконайте підказки дешифратора Crysis для очищення системи.

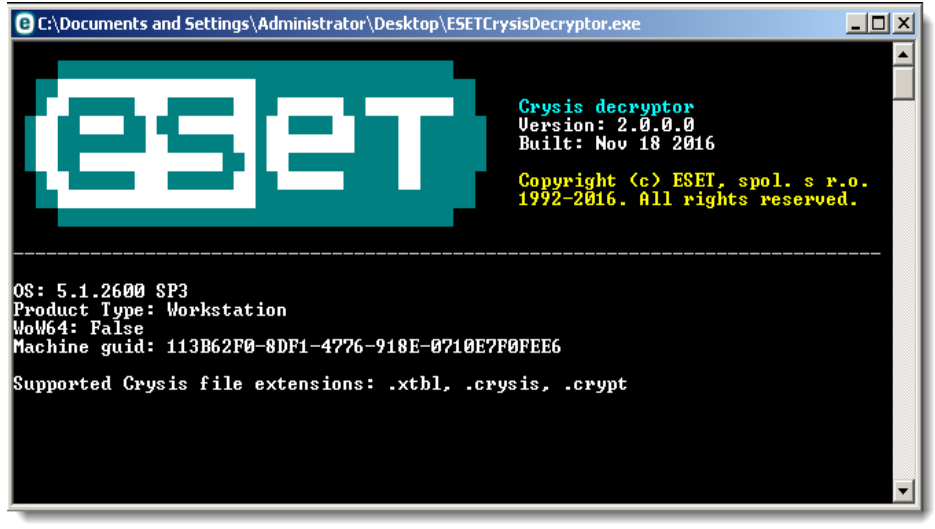


Рис. 1-2

Виникли запитання?

Зверніться до безкоштовної цілодобової служби технічної підтримки в Україні:

+38044 545 77 26

support@eset.ua