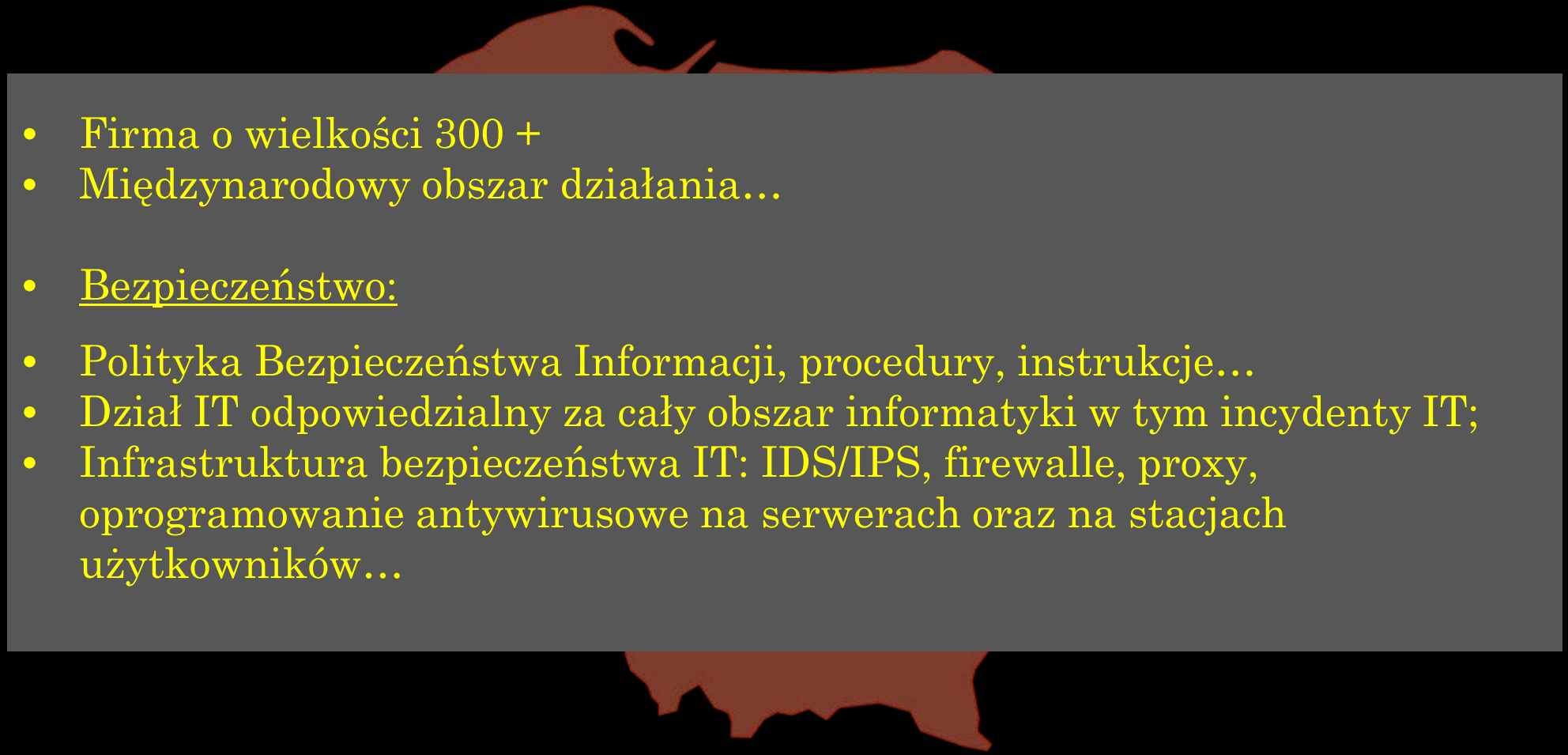
Ransomware - TeslaCrypt

Studium przypadku pojedynczego ataku

Gdzieś w Polsce… miejscowość, firma…



- Firma o wielkości 300 +
- Międzynarodowy obszar działania…

- <u>Bezpieczeństwo:</u>

- Polityka Bezpieczeństwa Informacji, procedury, instrukcje…
- Dział IT odpowiedzialny za cały obszar informatyki w tym incydenty IT;
- Infrastruktura bezpieczeństwa IT: IDS/IPS, firewalle, proxy, oprogramowanie antywirusowe na serwerach oraz na stacjach użytkowników…


BACK
TO
THE FUTURE

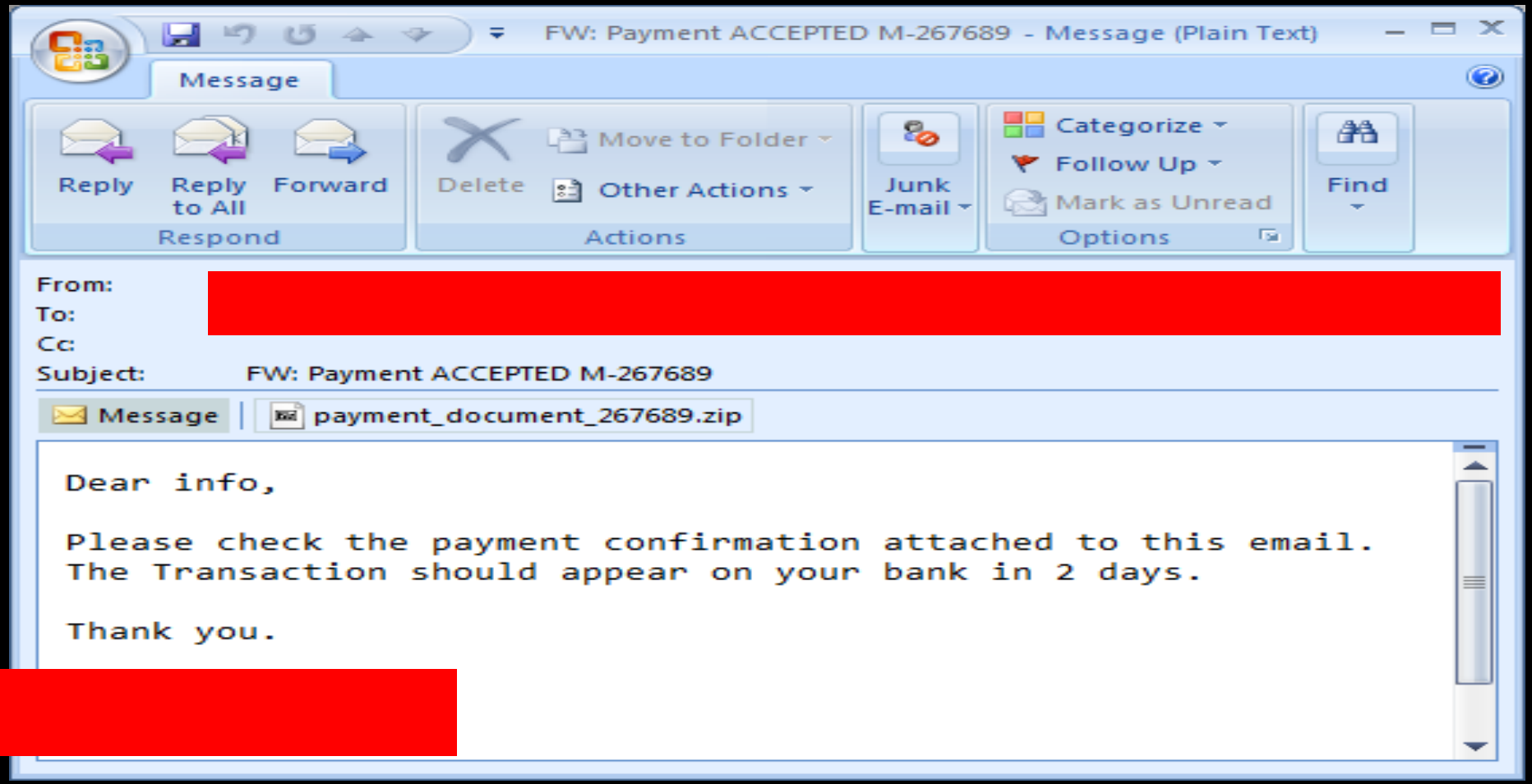
Pewnego dnia… marzec, 2016 r.

- Jeden z użytkowników (dział finansowy) dzwoni do działu IT z problemem…
- Na moim komputerze coś się stało z plikami… nie mogę ich otworzyć…
- Tym czasem u admina….

Co tak naprawdę się stało?

- Po analizie zgłoszenia, ustalono:
- W ramach jednego z prowadzonych projektów zgłoszono potrzebę zakupu nowego rozwiązania,
- Zakup został zrealizowany za granicą. Projekt realizowano…
- Tymczasem do działu finansowego wpłynęła informacja dot. projektu…

Faktura, płatność… ale co to jest?



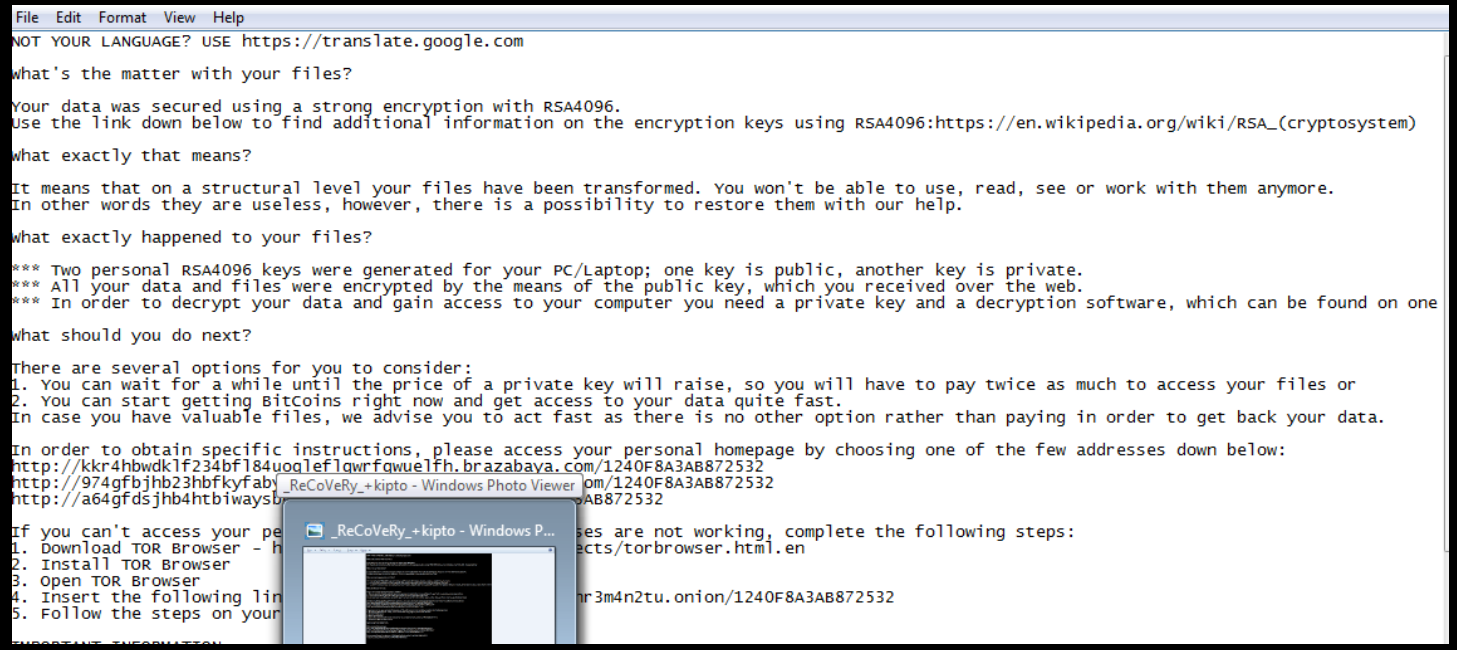
Po otwarciu… załącznika…

- Co było dalej…po otwarciu załącznika…za chwilę zobaczycie…

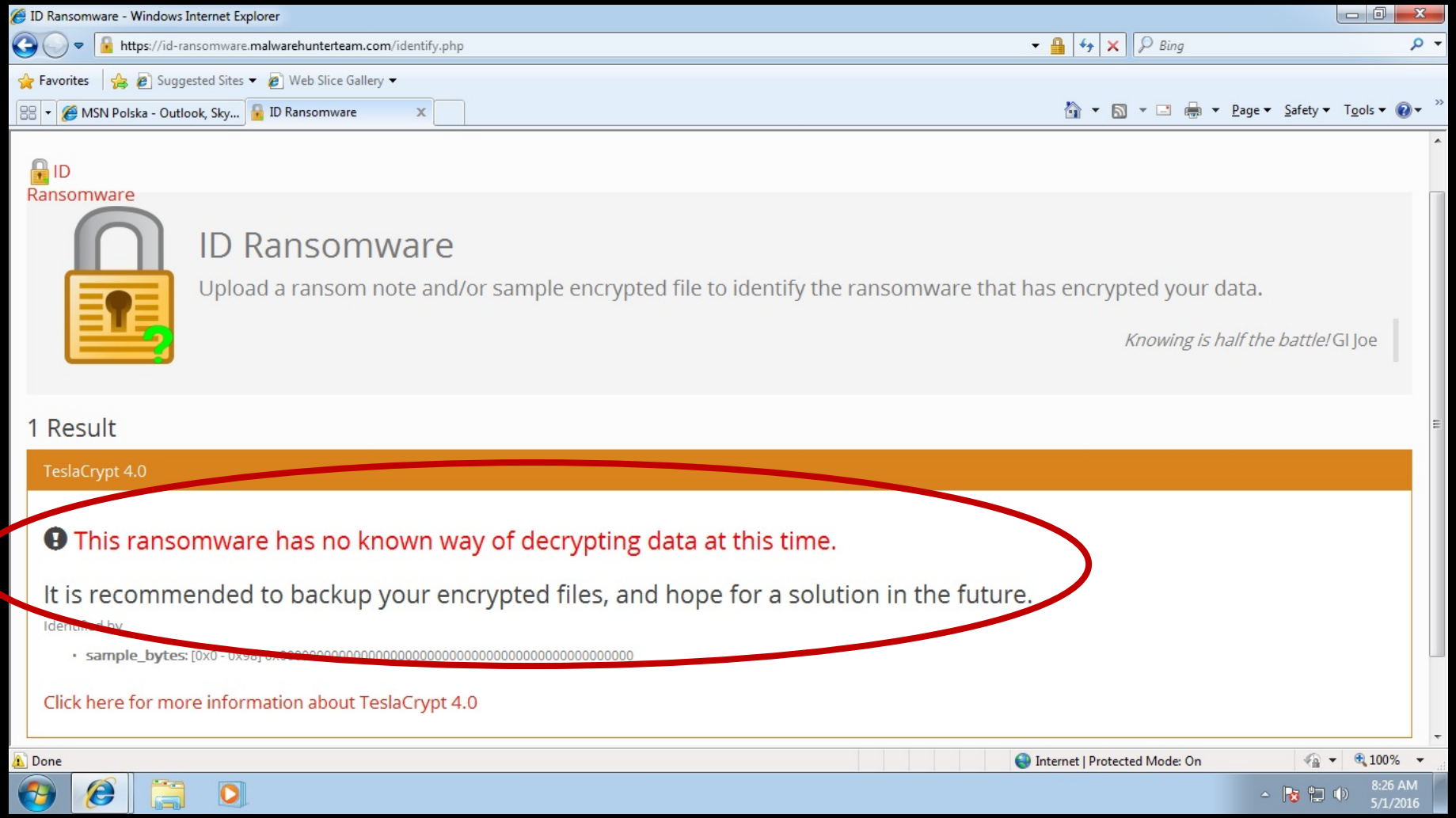
DEMO

Co to było?

- TeslaCrypt (określana m.in. przez Trend Micro jako TROJ_CRYPTESLA.A) jeden z wariantów oprogramowania typu ransomware. Szyfruje pliki, jednocześnie zamieniając rozszerzenia (w tym przypadku na multimedialne).
- Sposób dystrybucji, różny, uzależniony od grupy cyberprzestepczej, która stoi za konkretnym atakiem.



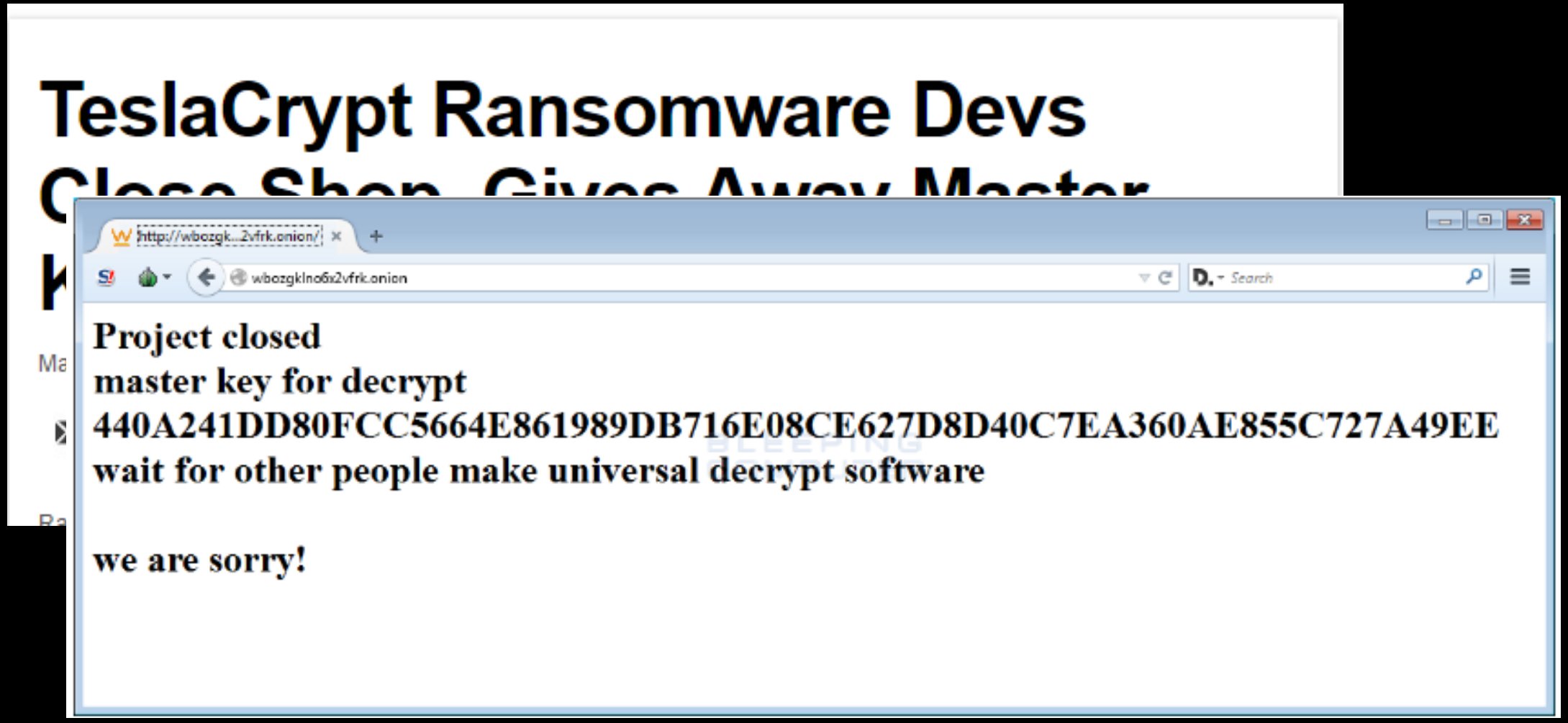
Po sprawdzeniu…



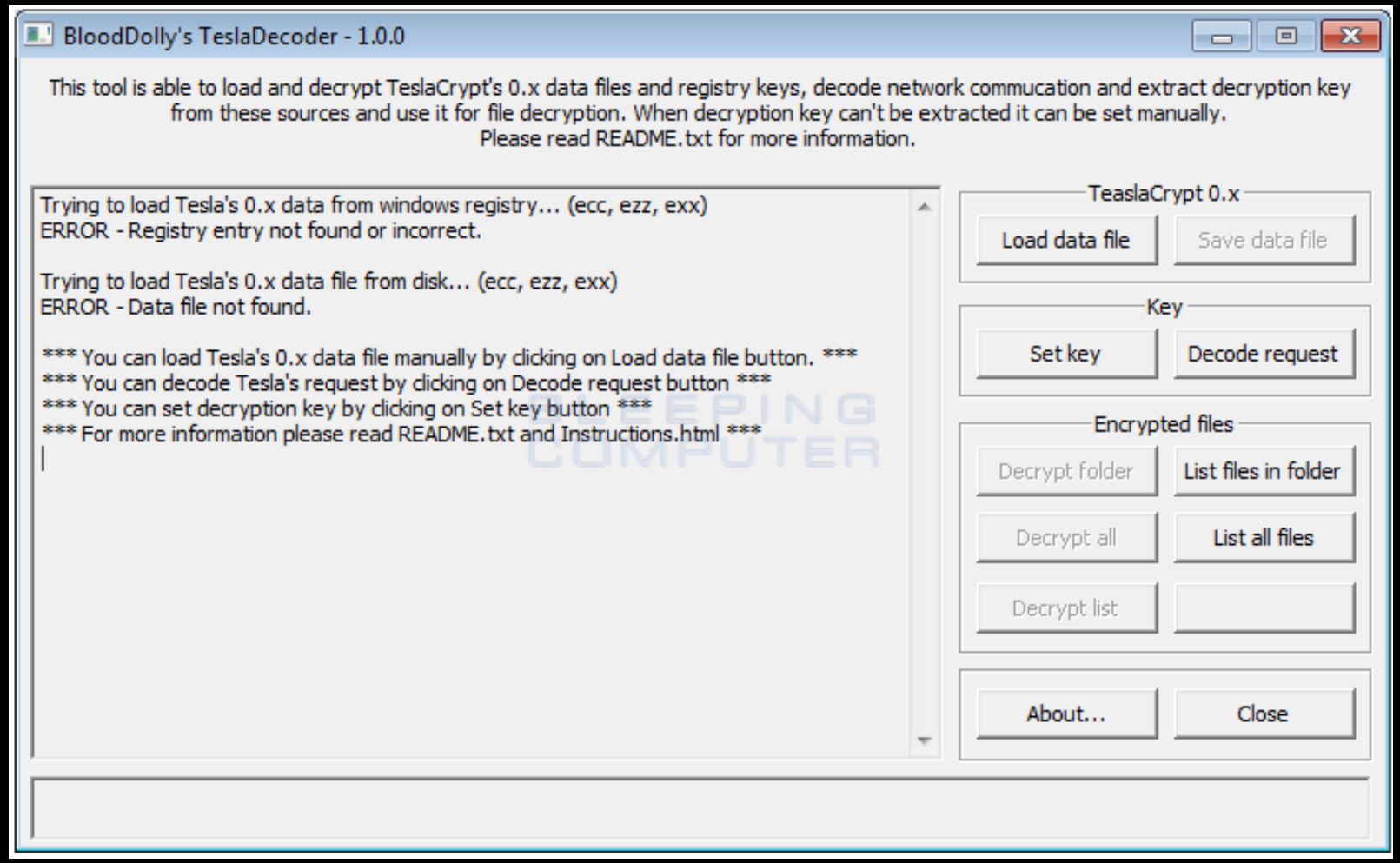
W tym konkretnym przypadku…

- W sumie zostało „zarażonych” jeszcze 5 innych stacji komputerowych…
- Na każdej z nich było oprogramowanie AV.
- Udało się odtworzyć tylko część plików z kopii zapasowej.
- Nie przeprowadzono zmian w procedurach.
- Nie przeprowadzono dogłębnej analizy zdarzenia oraz nie zgłoszono tego incydentu.
- **Najważniejsze… nie opłacono okupu!**

Obecnie TeslaCrypt…



Obecnie TeslaCrypt…dekoder



A gdyby tobie coś takiego się stało?

Jeżeli kiedykolwiek będziesz miał/a podobny kłopot…

Być może będziemy w stanie wam pomóc!

www.secons.com.pl

kontakt@secons.com.pl

Dziękuję za uwagę

Jarosław Sordyl

www.secons.com.pl

TT: @mr_news2

e-mail: kontakt@secons.com.pl