Sonda - oceń to sam

// Usuwanie blokady komputera przez policje - czyli trojana weelsof.

UWAGA: Nie należy wpłacać pieniędzy na wskazane konta - to próba wyłudzenia przez blokadę komputera niby przez policję.

Metoda I usuwania blokady komputera przez policję

1.Tak więc pobieramy kaspersky rescource disk 10 (tu do pobrania) z innego kompa,nagrywamy na płytę cd lub dvd JAKO OBRAZ!!!!(czyli nagraj obraz dysku).

2.Wchodzimy do biosu i odnajdujemy sekcję boot i zmieniamy na cd(tak samo jak byśmy instalowali windowsa)

3.Wkładamy płytę z nagranym OBRAZEM płyty.Uruchamiamy system ponownie i czekamy troszkę na uruchomienie kaspersky(pare minut zwykle) wybieramy język polski i tryb graficzny.

4.Naciskamy w lewym dolnym rogu(tak jak przycisk Start).Wybieramy Kaspersky Rescource

Disk i Scan zaznaczamy partycję do skanowania czyli C i jesli mamy D.....

5.Program działa zupełnie niezależnie od Windowsa więc żaden wirus nie jest w stanie się ukryć czy go zablokować.Po przeskanowaniu program zapyta co zrobić z wirusami(zapewne będzie nie jeden.....) i jeśli NIE WSKAZUJE do usunięcia plików ANTYWIRUSA którego mamy zainstalowanego w systemie np z lokalizacji Program FilesAvast czy podobne to każemy usunąć.

6.Po przeskanowaniu i usunięciu wybieramy menu lewego górnego rogu -tak jak w przycisku Start Wyłącz komputer.Wchodzimy do biosu (i podo.bnie jak po instalacji widny zmieniamy na uruchamianie z tego samego dysku jak przed zmianą na cd). Po ponownym uruchomieniu komputera blokada komputera przez policję już nie powinien się pojawić.

Metoda II usuwania blokady komputera przez policję

Polega na wpisaniu 13 cyfrowego numeru UKASH przy odłączonym komputerze od sieci internetowej.

Tu jest generator kodu "ukash"

Sprawdzeniu podlega jedynie prefiks – czyli wpisujemy kod zaczynający się od ciągu 633781 lub 718 – oraz ilość dowolnych cyfr po prefiksie – (musi być równa 13). Po uznaniu wpisanego numeru za poprawny uruchamiana jest procedura odblokowania komputera oraz wysłanie metodą POST pod adres http://adres-cnc/topic.php wpisanego kodu.

Procedura odblokowania jest odwróconym procesem instalacji. Na początku zamykane jest okno przesłaniające ekran.

Następnie uruchamiany jest proces explorer.exe oraz za pomocą funkcji EnumWindows(), WindowEnable() i WindowShow() przywracane są ukryte okna.

Na koniec malware usuwa zmienione wpisy w rejestrze oraz stworzone pliki. Blokada komputera przez policję już nie działa.

Metoda III (najbardziej skuteczna) usuwania blokady komputera przez policję

Uruchom komputer w trybie awaryjnym z wierszem poleceń i z pamięci przenośnej uruchom program antywirusowy Combofix .

1. Na innym komputerze pobieramy Combofixa , wgrywamy na pendrive ze zmienioną nazwą łatwą do zapamiętania np: 1234aa.exe

2.Wkładamy pendriv'a do naszego chorego komputera i uruchamiamy tzn: startujemy od początku Windowsa (nie z uśpienia)

3.Po włączeniu naciskamy kilkukrotnie F8 tak aby pojawiło się na czarnym tle białe napisy z wyborem opcji uruchomienia.

4.Wybieramy "Uruchom w trybie awaryjnym z paskiem poleceń"

5.Po uruchomieniu możemy w pasku wpisywać polecenia do wykonania - teraz należy poszukać literki pod którą zamontował się nasz pendrive.Dla Windows 7 najczęściej to bedzie F:/

dla Xp to litera następna po wszystkich naszych parytycjach plus CD-rom - jeśli 2 parytycje dysku c: d: plus CD-rom E: to nasz pendrive jest też F:

w pasek poleceń wpisujemy zatem: F:/1234aa.exe

i czekamy.

Jak skończy się skanowanie restart blokada komputera przez policję jest usunięta.

Po odwirusowaniu i ponownym rozruchu czasem trzeba usunąć ręcznie planszę z komunikatem.

Metoda IV nowej wersji wirusa policja (napis POLIZZIA)

dzięki postowi internauty Tomasza jest metoda na nową wersję wirusa weelsof

"Jest patent na wirusa Policja. Nowe wersje blokuja możliwość trybu awaryjnego, dlatego po załadowaniu systemu w "normalnym trybie" i pojawieniu się komunikatu , Policja' otwieramy wszyskie programy co się tylko da jak najszybciej (w tym celu klikamy flagę windowsa na klawiaturze i kliamy co się da na pasku zadań). Wirus się powinien zawiesić, a system zapyta o jego zamknięcie. Oczywiście go zamykamy i wtedy uruchamiamy dowolny sprawdzony, darmowy program do skanowania np. CCleaner i usuwamy nim wirusa. Powodzenia!"

{jcomments on}