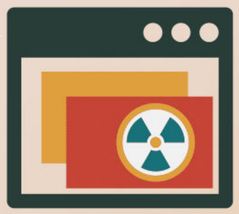
Ransomware | TIPS & ADVICE

ZŁOŚLIWE OPROGRAMOWANIE, KTÓRE TRZYMA TWOJE DANE JAKO ZAKŁADNIKA ZA ODPOWIEDNIĄ CENĘ

Ransomware uniemożliwia lub ogranicza dostęp użytkowników do ich systemów lub urządzeń, żądając zapłacenia okupu poprzez określone metody płatności online (i w nieprzekraczalnym terminie), w celu odzyskania kontroli nad danymi.

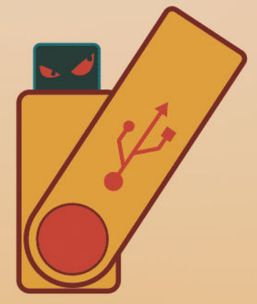
JAK SIĘ ROZPOWSZECHNIA?



Odwiedzanie skompromitowanych stron internetowych

Klikanie na złośliwe linki i załączniki

Ściąganie fałszywych aktualizacji aplikacji lub oprogramowania



Podłączanie do systemu komputerowego zainfekowanego urządzenia

#NoMoreRansom #DontPay

EUROPOL EC3 European Cybercrime Centre

Ransomware | TIPS & ADVICE

CHROŃ SIĘ!

Używaj silnych produktów bezpieczeństwa, aby chronić swój system przed wszelkimi zagrożeniami

Systematycznie wykonuj kopię zapasową danych trzymanych na komputerze. Trzymaj przynajmniej jedną wersję kopii offline.

Upewnij się, że Twoje oprogramowanie zabezpieczające i system operacyjny są aktualne.

Nie klikaj w linki w niespodziewanych lub podejrzanych mailach.

Bądź czujny podczas przeglądania internetu i nie klikaj w podejrzane linki, pop-upy czy okna dialogowe.

Przeglądaj i ściągaj tylko oficjalne wersje oprogramowania i zawsze z zaufanych stron.

Nie używaj kont z prawami administratora do codziennych spraw.

#NoMoreRansom #DontPay

EUROPOL EC3 European Cybercrime Centre

Ransomware | TIPS & ADVICE

ZAINFEKOWANY? CO ROBIĆ DALEJ?

Zgłoś sprawę na policję. Im więcej informacji przekażesz policji, tym bardziej efektywnie będzie można przerwać działalność przestępczą.

Odłącz urządzenie od internetu oraz innych sieci (takich jak domowe Wi-Fi) tak szybko, jak to możliwe, aby zapobiec rozpowszechnianiu się infekcji.

Nie płać okupu. W ten sposób finansujesz przestępców i zachęcasz ich do kontynuowania nielegalnej aktywności.

Sformatuj dysk twardy zainfekowanego urządzenia, przeinstaluj system operacyjny oraz aplikacje, skorzystaj ze wszystkich dostępnych aktualizacji i przywróć pliki ze swojego urządzenia zapasowego.

NO MORE RANSOM!

Zawsze skonsultuj się z www.nomoreransom.org, żeby sprawdzić, czy zostałeś zainfekowany jednym z wariantów ransomware, na który istnieje narzędzie deszyfrujące, dostępne bezpłatnie.

#NoMoreRansom #DontPay

EUROPOL EC3 | European Cybercrime Centre