KOMENDA POWIATOWA POLICJI W PODDĘBICACH

http://poddebice.policja.gov.pl/?serwis=epd&dzial=informacje&id=27665&drukuj=html
2018-07-21, 17:36

NO MORE RANSOM! POWIEDZ NIE INTERNETOWYM SZANTAŻYSTOM!

Biuro do Walki z Cyberprzestępczością Komendy Głównej Policji uczestniczy w projekcie nomoreransom.org. To międzynarodowa inicjatywa działająca pod auspicjami Europolu. Kilkadziesiąt organów ścigania z całego świata połączyło siły, by przeciwdziałać wymuszeniom w internecie. Przypominamy o najważniejszych zasadach bezpieczeństwa.

Dynamiczny rozwój technologii informatycznych coraz częściej wymusza wręcz od użytkownika aby był on-line. Dzieje się tak dlatego, iż Internet daje nam dostęp do nieograniczonych wręcz pokładów wiedzy, informacji i możliwości komunikacji. Tak naprawdę to jest on już nieodzownym elementem determinującym sprawne funkcjonowanie firm, instytucji, urzędów oraz „zwykłego" człowieka. Niewątpliwie taka symbioza nowoczesnego świata z technologiami informatycznymi to pole do popisu dla przestępców czyhających na naszą chwilę nieuwagi. I tak też coraz częściej padamy ofiarą oprogramowania które „zmusza" nas do zapłacenia okupu za odszyfrowanie i ponowny dostęp do tak naprawdę naszych własnych danych. Niestety problem staje się coraz większy gdyż dotyczy on wręcz każdej działalności użytkownika w Internecie. Za taką sytuację odpowiadają programy „szantażujące" (ang. ransomware; ransom – „okup" oraz software – „oprogramowanie") które wcześniej zostają uruchomione na dysku ofiary i po kilku sekundach opanowują cały system komputerowy.

Jak dajemy się złapać

Nie uaktualniamy systemów operacyjnych – często bywa tak, iż nie zwracamy uwagi na aktualizację oprogramowania jest to błąd gdyż producenci systemów operacyjnych starają się zabezpieczać swoje produkty przed podatnością na różnego rodzaju ataki i złośliwe oprogramowanie.
Używamy wtyczek do przeglądarek internetowych, które nie są już wspierane lub posiadają luki w zabezpieczeniach. W przypadku gdy korzystamy z dodatkowych podprogramów które współdziałają z naszymi przeglądarkami należy sprawdzić, czy są one odpowiednio zabezpieczone i czy na bieżąco aktualizowane przez twórców.
Wchodzimy na podejrzane strony internetowe. Trudno zakwalifikować stronę jako podejrzaną, lecz miejmy na uwadze, iż strony zawierające m.in. pornografię oraz „nielegalne" oprogramowanie są częstą przyczyną zainfekowania naszego systemu.
Nie uruchamiaj niezaufanych odnośników/linków zarówno wtedy, gdy znajdują się one w treści wiadomości e-mail, jak i na stronie internetowej. Użytkownicy wręcz bezwiednie klikają na linki które prowadzą do podstron które są zainfekowane lub bezpośrednio do instalatora złośliwego oprogramowania.
Wykorzystujemy niezweryfikowane makra w popularnych programach tekstowych i obliczeniowych. Należy wyłączyć domyślne zezwolenie na używanie makr.

Jak przeciwdziałać

Twórz kopie zapasowe najważniejszych danych. Bez wątpienia jednym z najbardziej skutecznym sposobem, niestety uciążliwym, jest tworzenie kopii bezpieczeństwa najcenniejszych danych. Należy podkreślić, iż taki sposób uchroni nas również przed utratą naszych zasobów w wyniku fizycznego uszkodzenia urządzenia magazynującego lub jego kradzieży.
Używaj oprogramowania które w czasie rzeczywistym jest wstanie zablokować działanie złośliwego oprogramowania.
Aktualizuj na bieżąco system operacyjny oraz oprogramowanie.
Uważnie czytaj treści które są w wiadomościach e-mail i stronach internetowych a wymagają od ciebie interakcji np. wejścia na podstronę lub otwarcie załącznika.

Po fakcie …

W pierwszej kolejności należy spróbować ustalić jakim programem zostały zaszyfrowane nasze dane. Jak to zrobić? W większości przypadków na monitorze/pulpicie pojawia się informacja, iż użytkownik dopuścił się „nielegalnych" działań w postaci np. dystrybuowania pirackich materiałów w postaci: muzyki, filmów lub pornografii. Oczywiście należy podkreślić, iż Polska Policja nie blokuje w ten sposób komputerów, jest to taktyka autorów oprogramowania ransomware. Chcą oni bowiem przekonać swoje ofiary, że zrobiły coś niezgodnie z prawem i teraz są w zainteresowaniu organów ścigania, a karą za popełnione „przestępstwo" jest narzucona grzywna.

Wyżej opisany model stanowi tylko jeden z wielu sposobów wywołania presji na użytkowniku i zmuszenia go do zapłacenia okupu.

Z pomocą mogą przyjść nam najpopularniejsze wyszukiwarki gdzie należy opisać komunikat z pulpitu a być może rozwiązanie już zostało zaimplementowane w jednym z programów anty-ransomware'owych. Dobrym rozwiązaniem jest również odwiedzenie strony https://www.nomoreransom.org/crypto-sheriff.php gdzie wgrywamy próbki zaszyfrowanych danych. Są duże szanse, iż w wyniku analizy otrzymanych danych strona „podeśle" nam rozwiązanie problemu.

Niestety w chwili obecnej nie daje się odszyfrować wszystkich danych. Co zatem zrobić? Wydaje się, że najrozsądniejszym sposobem jest poczekanie aż specjaliści od zabezpieczeń złamią algorytm szyfrujący i udostępnią program deszyfrujący.

Zdecydowanie nie należy poddawać się presji i nie płacić okupu. Takie postępowanie tylko zachęci przestępców do podejmowania kolejnych prób ataku i tworzenia kolejnych wersji złośliwego oprogramowania.

żródło: KWP Łódź