ZACHODNIOPOMORSKI UNIWERSYTET TECHNOLOGICZNY
W SZCZECINIE
WYDZIAŁ INFORMATYKI

mgr inż. Michał Glet

Uniwersalny zestaw wskaźników do wykrywania ataków ransomware

Streszczenie

Oprogramowanie ransomware stanowi poważne zagrożenie bezpieczeństwa. Opisane w pracy przykłady ataków pokazują, że zagrożenie to dotyczy państwa, organizacji/firmy jak również jednostek (pojedynczych użytkowników). Statystki związane zarówno z aktywnością samego oprogramowania ransomware jak również związane ze stratami jakie powodują pokazują, że zagrożenie jest duże oraz realne. Autorzy ransomware z jednej strony udoskonalają ciągle oprogramowanie, a z drugiej strony udoskonalają metody infiltracji np. stosując wyrafinowane socjotechniki albo nieustanie szukając nowych podatności w oprogramowaniu. Analizy oraz przewidywania badaczy bezpieczeństwa wskazują, że rynek ransomware będzie się w dalszym ciągu rozwijał. W przygotowanej dysertacji naukowej przeanalizowałem wybrane próbki oprogramowania ransomware i na tej podstawie wyodrębniłem ich cechy charakterystyczne związane m.in. z wykorzystywanymi funkcjami API systemu Windows. Dodatkowo zaproponowałem wykorzystanie metod badania losowości oraz kategoryzacji danych do wykrywania aktywnego ataku oprogramowania ransomware. W wyniku przeprowadzonych prac utworzona została koncepcja wskaźników detekcji aktywności oprogramowania ransomware. Istotną cechą zaproponowanych wskaźników jest fakt, iż powinny one wykrywać nowe, nieznane w momencie tworzenia, wersje oprogramowania ransomware. Dzięki temu, mechanizmy bezpieczeństwa korzystające z utworzonych wskaźników, powinny być w stanie skrócić znacząco średni czas życia nowych wersji tego typu oprogramowania. W pracy przedstawione zostały dodatkowo wyniki, jakie zostały osiągnięte podczas testów detekcji trwającego ataku oprogramowania ransomware z wykorzystaniem prototypowych implementacji zaproponowanych w pracy wskaźników.

Słowa kluczowe: ransomware, kryptologia, wirus, okup, wykrywanie, atak.

17.05.2024 Glet Michał