# ANALIZA PRZYPADKU Edukacja

## SEKTOR

Edukacja

## ŚRODOWISKO

- 7 500 studentów
- 1 500 punktów końcowych

## WYZWANIA

Zmniejszenie ilości złośliwego oprogramowania wprowadzanego do sieci przez zainfekowane punkty końcowe studentów.

Powstrzymanie wykorzystania zasobów uniwersytetu oraz ochrona danych studentów, które mogą być przypisane do konkretnych osób.

Ochrona komputerów studentów przy zachowaniu minimalnym spadku ich wydajności.

## ROZWIĄZANIE

Uruchomienie CylancePROTECT® na komputerach studentów, wykładowców oraz należących do Uniwersytetu.

## Klient

Tradycyjny amerykański uniwersytet, na który uczęszcza 7 500 studentów (studia dzienne i podyplomowe).

## Sytuacja

Biuro pomocy finansowej uniwersytetu padło wcześniej ofiarą odmiany CryptoLockera. CryptoLocker to Trojan typu ransomware, który atakuje komputery z systemem operacyjnym Microsoft Windows®. Rozprzestrzenia się przez zainfekowane załączniki wiadomości email oraz botnety, a po aktywacji szyfruje konkretne typy plików na dyskach lokalnych i sieciowych. Zaszyfrowane pliki mogą być otwierane tylko przy pomocy prywatnego klucza znajdujące się na serwerze atakującego.

Strona zaatakowana otrzymała wiadomość z ofertą odszyfrowania danych tylko w wypadku zapłaty w Bitcoinach lub w formie przedpłaconego vouchera do określonego terminu. W wiadomości poinformowano, że nieuiszczenie haraczu w terminie spowoduje skasowanie klucza lub podniesienie stawki okupu.

Władze uniwersytetu zdały sobie sprawę, że tradycyjne antywirusy bazujące na sygnaturach nie są w stanie chronić infrastruktury uczelni przed zaawansowanym złośliwym oprogramowaniem takim jak CryptoLocker. Uczelnia skontaktowała się z firmą Cylance i uruchomiono test w postaci POC (Proof of Concept) programu CylancePROTECT, produktu antywirusowego następnej generacji.

## Proces

Przez cztery tygodnie firma Cylance uruchomiła i monitorowała CylancePROTECT na 57 systemach Uniwersytetu. Z 57 monitorowanych hostów firma Cylance zidentyfikowała i zablokowała złośliwe oprogramowanie nieodkryte wcześniej przez tradycyjne antywirusy na 33 urządzeniach końcowych.

W sumie Cylance przeprowadziło natychmiastową kwarantannę 183 istniejących egzemplarzy złośliwego oprogramowania oraz 107 dodatkowych potencjalnie niepożądanych programów. Wśród tych próbek 35 zostało kompletnie pominięte przez wszystkie inne silniki antywirusowe.

Podczas testu POC znaleziono wiele wersji CryptoLockera. Zostały one zablokowane oraz powstrzymane od uruchomienia bez wpływu na standardowe działanie Uniwersytetu.

## Rezultaty

Po zakończonym teście POC uniwersytet zakupił pełną licencję na CylancePROTECT i uruchomił usługę na urządzeniach końcowych, zastępując program Microsoft Security Essentials w niespełna 8 godzin bez wpływu na użytkowników końcowych.

## Darmowe konsultacje

Chcecie sprawdzić sami, jak CylancePROTECT i firma VIDA dają przewagę w obronie przeciwko cyberatakom? Skontaktujcie się z nami w sprawie darmowych konsultacji!

**Zobowiązanie do prywatności**
Firma Cylance zobowiązuje się do ochrony organizacji przeciwko zaawansowanym zagrożeniom, między innymi przeciwko ujawnieniu prywatnych informacji. Z tego powodu nie publikujemy nazw organizacji ani nazwisk osób zaangażowanych w badania.

*„CylancePROTECT szybko zidentyfikował i zablokował prawie 200 zagrożeń, które zostały po prostu pominięte przez tradycyjne antywirusy. Jesteśmy pewni, że firma Cylance jest w stanie obronić nasze systemy, z których korzysta duża grupa wykładowców i studentów”*

- Kierownik IT Uniwersytetu

VIDA
Teatralna 8/13, 40-003 Katowice
+48 32 252 13 10
+48 32 350 00 50
cylance@vida.pl

CYLANCE