**ATAK RANSOMWARE NA NORSK HYDRO KOSZTOWAŁ JUŻ FIRMĘ 40 MILIONÓW DOLARÓW**

**Odnotowany w zeszłym tygodniu atak ransomware na Norsk Hydro kosztował do tej pory 300-350 milionów NOK, czyli około 40 milionów dolarów (36 milionów euro). Firma weszła w tryb odzyskiwania danych już we wtorek, a mimo tego niektóre jej procesy nadal sterowane są ręcznie.**

Norweska firma produkująca aluminium i energię odnawialną ujawniła w zeszłym tygodniu, że zmaga się z „rozległym atakiem cybernetycznym”, który uderzył w jej systemy IT 18 marca i nasilał się z dnia na dzień. Incydent został wkrótce zidentyfikowany jako infekcja ransomware. Zmusiła ona Hydro, działającą w około 50 krajach, do zamknięcia całej swojej globalnej sieci. Wykorzystując wyciek wewnętrznej notatki, napastnicy użyli podobno wirusa LockerGoga do zainfekowania systemów norweskiego giganta.

*- W szeroko rozumianym pojęciu ransomware jest kategorią złośliwego oprogramowania, zaprojektowanego aby blokować dostęp do komputera, dopóki odpowiednia suma okupu nie zostanie uiszczona na konto przestępcy. Przeważnie ransomware rozprzestrzenia się podszywając się pod fakturę, informacje o dostawie zamówienia lub załączone CV. Często też znajdują się w załącznikach mailingu ze spamem. Kiedy użytkownik otworzy załącznik, rozpoczyna się proces szyfrowania. Kiedy proces szyfrowania dobiegnie końca, ofiara widzi na ekranie powiadomienie z instrukcjami, jak zapłacić okup i otrzymać klucz do deszyfracji -* ***wyjaśnia Wszebor Kowalski, inżynier techniczny Bitdefender z firmy Marken.***

W tym tygodniu Hydro opublikowała aktualizację, zgodnie z którą większość operacji przebiega teraz z normalną wydajnością, a tylko jeden proces biznesowy pozostaje prawie wstrzymany.

„Tydzień po tym, jak Hydro stała się celem ataku cybernetycznego, większość operacji przebiega z normalną wydajnością” – podała firma. „W najbardziej dotkniętym obszarze biznesowym, ‘Extruded Solutions’, produkcja realizowana jest obecnie w 70-80 procentach”, z wyjątkiem jednostki biznesowej ‘Buiding Systems’, w której procesy produkcyjne niemal stanęły”.

Extruded Solutions to należące do firmy zakłady produkujące aluminium, które znajdują się w Europie i Ameryce Północnej.

Hydro szacuje, że dotąd poniosła straty w wysokości 300-350 milionów koron, co przekłada się na 40 milionów dolarów, czyli 36 milionów euro. Firma twierdzi, że większość kosztów wynika z utraty marż i wolumenów w obszarze działalności Extruded Solutions. Zaznacza również, że posiada solidną polisę ubezpieczeniową od ryzyka cybernetycznego u uznanych ubezpieczycieli. Nie twierdzi jednak, że ubezpieczenie faktycznie pokryje wszystkie koszty.

Hydro zgłosiła atak do norweskiego Narodowego Biura Śledczego i współpracuje z norweskim Urzędem Bezpieczeństwa Narodowego, w zakresie prowadzonego śledztwa.

Przypuszcza się, że ci sami operatorzy oprogramowania LockerGoga zwrócili w tym tygodniu uwagę na dwie firmy chemiczne w USA, Hexion i Momentive. W przeciwieństwie do innych rodzin oprogramowania szantażującego, LockerGoga zawiera notę okupową, która zaprasza ofiary do negocjowania – za pośrednictwem poczty elektronicznej – ceny klucza deszyfrującego.