Szanowni Państwo,
Prosimy o dystrybucję poniższej informacji, związanej z rozwijającym się zagrożeniem, jakim jest złośliwe oprogramowanie typu Ransomware.

W ciągu ostatnich miesięcy, do zespołu CSIRT NASK coraz częściej trafiają zgłoszenia incydentów związanych z zaszyfrowanymi danymi przez złośliwe oprogramowanie typu Ransomware. Zaczęły się również infekcje tym złośliwym oprogramowaniem szyfrującym w sektorze zdrowia. W związku z coraz większą aktywnością tego zagrożenia, zespół CSIRT NASK prognozuje, że może to być dopiero początek szerszej kampanii wymierzonej w sektor zdrowia.

Zespół CSIRT NASK zwraca uwagę na skutki jakie atak związany z tym zagrożeniem może spowodować. Między innymi prowadzi on do braku możliwości odczytu, edycji lub zapisu danych, które były umieszczone na zainfekowanej maszynie. W sektorze zdrowia może to spowodować niewydolność szpitala w związku ze znacząco utrudnionym dostępem do kluczowych informacji. Rzutuje to na bezpieczeństwo pacjentów placówek zdrowia. Nowe warianty tego zagrożenia również potrafią pobrać wszelkie dane, które znajdowały się na zainfekowanej maszynie. Stanowi to zagrożenie dla bezpieczeństwa danych pracowników oraz pacjentów. Ewentualny wyciek takich informacji może spowodować straty wizerunkowe placówki oraz wymierne skutki dla prywatności pacjentów, a także konsekwencje wynikające z naruszenia przepisów o ochronie danych osobowych.

W związku z powyższym, zespół CSIRT NASK przekazuje rekomendacje, które przedstawiają sposoby na minimalizację ryzyka wystąpienia oraz, w przypadku bycia ofiarą tego ataku, skuteczne działania naprawcze.

DZIAŁANIA PREWENCYJNE

- weryfikacja procedur wykonywania kopii zapasowych istotnych systemów - w szczególności mowa tutaj o wszystkich systemach zawierających informacje kluczowe dla funkcjonowania podmiotu, np. dane pacjentów, informacje o leczeniu, informacje o kontrahentach, dane kadrowo-płacowe. W związku z kopiami zapasowymi, należy zbadać następujące zagadnienia:
  - czy takie procedury są zaimplementowane?
  - czy treść kopii zapasowych jest aktualna?
  - czy cyklicznie wykonywane są kopie zapasowe?
  - czy kopie zapasowe są przechowywane w sposób trwały i odporny? (w szczególności należy zwrócić uwagę, by kopia zapasowa nie była podłączona jako zasób sieciowy w sieci roboczej)
  - czy kopia zapasowa faktycznie daje możliwość odtworzenia pracy?
  - czy przeprowadzane są cykliczne testy utworzonych kopii zapasowych?
- zwrócenie szczególnej uwagi na otrzymywane przez pracowników placówek maile. W szczególności należy:
  - upewnić się czy nie doszło do podszycia w celu zachęcenia odbiorcy do uruchomienia załączonego szkodliwego pliku
  - zwrócić uwagę na rozszerzenia załączonych plików
  - w przypadku gdy w treści wiadomości zostało umieszczone hiperłącze, należy sprawdzić czy prowadzi ono do znanej i zaufanej strony
- zastosowanie polityki bezpieczeństwa, odgórnie zapobiegającej uruchomieniu w potencjalnie złośliwych dokumentach aktywnej treści, tj. makra - dotyczy to w szczególności dokumentów z pakietu MS Office (rozszerzenia .doc, .docx, .xls, .xlsx)

ul. Kolska 12, 01-045 Warszawa
tel.: +48 22 380 82 74
fax: +48 22 380 83 99
Zgłaszanie incydentów: cert@cert.pl
e-mail: info@cert.pl
/CERT.Polska
@CERT_Polska
www.cert.pl
www.nask.pl

- zablokowanie kanałów zdalnego dostępu do infrastruktury oraz publicznych usług, które są dostępne w sieci (np. RDP, FTP, itp.), które nie są niezbędne do prawidłowego funkcjonowania placówki
- w przypadku koniecznego zdalnego dostępu do usług czy zasobów placówki, silnie sugerujemy wprowadzenie dodatkowych środków bezpieczeństwa (np. uruchomienie zdalnego pulpitu tylko przez firmowy VPN)
- cykliczna aktualizacja baz sygnatur programów antywirusowych używanych w organizacji
- należy na bieżąco wykonywać aktualizacje systemów operacyjnych oraz zainstalowanego oprogramowania
- upewnić się czy hasła domenowe pracowników placówki są odpowiednio mocne

DZIAŁANIA NAPRAWCZE

- jak najszybsze odpięcie zainfekowanej maszyny od sieci - ograniczy to skalę ataku
- w celu zmaksymalizowania szans odzyskania danych nie wyłączać zainfekowanego komputera. Należy go pozostawić włączonym lub w trybie hibernacji
- wykonanie kopii zapasowej zainfekowanych plików - w przypadku, gdy w danym momencie nie będzie możliwe odszyfrowanie plików, umożliwi to dostęp do utraconych danych w przypadku pojawienia się dekryptora
- warto odwiedzić zaufaną stronę nomoreransom.org, gdzie można znaleźć narzędzie pozwalające określić, do jakiej rodziny należy dane złośliwe oprogramowanie szyfrujące, oraz można dowiedzieć się, czy znane są metody odszyfrowania danych bez płacenia okupu
    - w przypadku znalezienia odpowiedniego dekryptora na wspomnianej stronie, w celu odszyfrowania danych należy postępować ściśle według załączonej instrukcji dla danego narzędzia
- w przypadku wykrycia infekcji oprogramowaniem szyfrującym, należy podjąć niezwłoczny kontakt z zespołem CSIRT NASK poprzez stronę incydent.cert.pl albo email cert@cert.pl. W przypadku kontaktu, rekomendowane jest załączenie następujących plików:
    - minimum 2 zaszyfrowane pliki
    - notatka z żądaniem okupu od przestępcy

  Rekomendowane jest również wysłanie następujących plików, w przypadku gdy jest to możliwe:
    - próbka złośliwy oprogramowania, która zainfekowała maszynę
    - logi z zainfekowanej maszyny oraz systemów bezpieczeństwa z czasu infekcji
    - oryginały plików, które zostały zaszyfrowane, jeżeli się zachowały

Zespół CSIRT NASK jednocześnie deklaruje możliwość bezpośredniej konsultacji, jeśli w trakcie realizacji technicznej części zaleceń pojawią się wątpliwości. W tym celu należy wysłać wiadomość email na adres cert@cert.pl.