PORADNIK – PRCyber-04
Cyberbezpieczeństwo - Jak sobie radzić ze skutkami ataków typu ransomware?

(Wydanie 1 – sierpień 2020 r.)

Departament Cyberbezpieczeństwa
Ministerstwo Cyfryzacji

Ransomware to szkodliwy program, który szyfruje pliki na komputerach, blokując nam do nich dostęp. Bardzo często jedyną osobą, która potrafi złamać szyfr, jest sam atakujący.

Rysunek 1 Zdjęcie informacyjne o infekcji ransomware.

Przede wszystkim, należy podejmować kroki zapobiegające infekcjom szkodliwym lub szantażującym oprogramowaniem. Zostały one opisane przez nas w innym artykule. **Jeżeli jednak doszło do ataku, podejmij niezwłocznie opisane niżej kroki.**

> ***Pamiętaj!*** *Jeżeli nie masz fachowców na miejscu, warto wezwać specjalistów w zakresie reagowania na incydenty lub informatyki śledczej. Pomogą oni poprawnie zabezpieczyć zebrać materiał dowodowy.*

Jeśli Twoja organizacja została już zainfekowana szkodliwym lub szyfrującym oprogramowaniem, te kroki mogą pomóc w ograniczeniu wpływu infekcji.

Komputery i inne urządzenia

1. Natychmiast odłącz zainfekowane komputery, laptopy lub tablety od wszystkich połączeń sieciowych, zarówno przewodowych jak też bezprzewodowych.
2. W celu zmaksymalizowania szans odzyskania danych nie wyłączaj komputera. Hibernacja systemu to też dobra (i ekologiczna) opcja.Zastanów się, czy w bardzo poważnym przypadku konieczne może być wyłączenie Wi-Fi i wyłączenie połączeń sieci bazowej (w tym przełączników sieciowych).
3. Zresetuj poświadczenia, w tym hasła (szczególnie dla administratorów) - ale sprawdź, czy nie blokujesz systemów niezbędnych do odzyskiwania danych.

Zgłoszenie incydentu

4. Zrób zdjęcie ekranu z komunikatem wyświetlanym przez ransomware. Upewnij się, że wszystkie informacje są na zdjęciu czytelne. Przegraj plik z notatką okupu (ransom note) i przykładowe zaszyfrowane pliki na czysty przenośny nośnik danych (np. pendrive) – będą jeszcze potrzebne. Jeśli jesteś biegły w obsłudze komputera, spróbuj też znaleźć próbkę złośliwego oprogramowania na dysku (wskazówka: ransomware bardzo często dopisuje się do autostartu).
5. Odwiedź stronę nomoreransom.org, gdzie znajdziesz narzędzie pozwalające określić, do jakiej rodziny należy dany ransomware, a także dowiesz się, czy są znane metody odszyfrowania danych bez płacenia okupu. Prawdopodobnie przyda się tutaj ransom note albo zaszyfrowany plik.
6. Jeżeli NoMoreRansom ma odpowiedni dekryptor, postępuj ściśle według instrukcji dla danego narzędzia. Jeśli się uda, gratulacje: trafiłeś na ten ułamek ransomware, który dało się zdeszyfrować. Jeśli nie, czytaj dalej.
7. Rozważ zgłoszenie incydentu do CERT Polska – najlepiej zaraz po wykryciu zdarzenia. W tym celu skorzystaj z https://incydent.cert.pl/**.** W zgłoszeniu przekaż informacje o podjętych do tej pory krokach oraz inne informacje, o które zostaniesz poproszony w formularzu, według najlepszej wiedzy na moment zgłoszenia.

Przywracanie danych z kopii zapasowej

8. Jeśli dysponujesz kopią zapasową, sformatuj dysk, zainstaluj system od nowa i przywróć dane z backupu.
9. Przed przywróceniem danych z kopii zapasowej sprawdź, czy kopia jest wolna od oprogramowania malware i ransomware. Dane należy przywrócić tylko z kopii zapasowej, jeżeli jesteśmy pewni, że kopia zapasowa nie jest zainfekowana.
10. Jeśli nie dysponujesz kopią zapasową i zgłosiłeś incydent do CERT Polska albo innego zespołu bezpieczeństwa, poczekaj na wynik analizy. Niestety, nie ma co robić sobie za dużych nadziei, w >95% przypadków ofierze nie da się pomóc – może się udać tylko jeśli przestępca popełnił błąd.

Uwaga! Istnieją „firmy od odzyskiwania danych", które są oszustami. *Danych zazwyczaj nie da się odzyskać bez płacenia, więc takie firmy działają tylko jako pośrednicy między przestępcami a ofiarami (negocjują zniżkę, a później biorą swoją prowizję). Nie warto się na to nabierać – jak już dawać się okraść, to tylko raz na infekcję. Pamiętaj, że tacy „pośrednicy" też popełniają przestępstwo.*

Po odzyskaniu danych z kopii zapasowej

11. Podłącz urządzenia do niezainfekowanej sieci, aby pobrać, zainstalować i zaktualizować system operacyjny i całe inne oprogramowanie.
12. Zainstaluj, zaktualizuj i uruchom oprogramowanie antywirusowe.
13. Połącz się ponownie z siecią.
14. Monitoruj ruch w sieci i uruchamiaj skanowanie antywirusowe, aby stwierdzić, czy nadal występuje infekcja.
15. Po usunięciu skutków ataku spróbuj ustalić, w jaki sposób do niego doszło oraz **podejmij działania zapobiegawcze**, by uniemożliwić powtórzenie się sytuacji (edukacja użytkowników, zabezpieczenia fizyczne, aktualizacja oprogramowania).

O tym jak się zabezpieczyć przed atakiem ransomware, możesz przeczytać w naszym innym artykule.

Uwaga! Pliki zaszyfrowane przez większość rodzajów ransomware nie mogą zostać odszyfrowane przez nikogo innego niż atakującego. Nie trać czasu ani pieniędzy na usługi, które rzekomo mogą to zrobić. W niektórych przypadkach specjaliści ds. bezpieczeństwa stworzyli narzędzia, które mogą odszyfrować pliki z powodu słabości szkodliwego oprogramowania (które mogą być w stanie odzyskać niektóre dane), ale należy zachować ostrożność przed uruchomieniem nieznanych narzędzi na urządzeniach.

Materiały

1. Opracowano na podstawie materiałów informacyjnych NCSC - National Cyber Security Centre, Narodowego Centrum Cyberbezpieczeństwa Zjednoczonego Królestwa.
2. Materiały NASK