podkom. Tomasz Kłys
Zakład Kryminalny Szkoły Policji w Pile

Oprogramowanie ransomware – analiza zagrożenia i metody jego zapobiegania

Rozwój technologiczny przyczynił się do zwiększenia przetwarzanych danych i informacji. Niestety, wraz z tym wzrostem, zwiększyła się również liczba potencjalnych zagrożeń. Środowisko przetwarzania danych musi być nieustannie analizowane, a najistotniejsze obszary właściwie zabezpieczane. Jednym z najpoważniejszych zagrożeń z obszaru cyberbezpieczeństwa jest ransomware. Na czym polega, czym może skutkować i czy istnieją sposoby na zabezpieczenie się przed takim rodzajem ataku?

Czym jest ransomware?

Słowo ransomware wywodzi się z połączenia dwóch angielskich słów *ransom* oraz *software*. W wolnym tłumaczeniu *ransom* oznacza *okup*, zaś *software* - *oprogramowanie*. Zatem najprostsze tłumaczenie tego sformułowania to złośliwe oprogramowanie wymuszające okup czy też oprogramowanie szantażujące[1]. W przeciwieństwie do wirusów używanych podczas ataków związanych z kradzieżą danych – ransomware nie jest przeznaczony do uzyskiwania dostępu do komputera lub systemu informatycznego w celu pozyskania danych, ale służy do zablokowania części lub całości funkcjonalności systemu operacyjnego użytkownika albo zaszyfrowania części lub całości danych znajdujących się na urządzeniu ofiary. Sprawcy następnie wysyłają właścicielowi żądanie okupu, oczekując pieniędzy w zamian za cofnięcie dokonanych zmian, czyli przywrócenie kontroli nad systemem czy uzyskanie dostępu do zaszyfrowanych danych[2].

Choć zagrożenie pojawiło się już w 1989 roku, to znaczne rozpowszechnienie tego rodzaju ataków miało miejsce w latach 2005-2006, co wiąże się głównie z rozwojem kryptografii oraz Internetu. W późniejszych latach problem nasilił się z uwagi na pojawienie się bitcoina. Kryptowaluta pozwoliła uzyskiwać cyberprzestępcom zapłatę za zaszyfrowane pliki i zachowanie anonimowości. Cyberprzestępcy coraz częściej wybierają oprogramowanie szyfrujące jako metodę ataku. Główną przyczyną jest dużo większy zysk niż w przypadku innego rodzaju cyberprzestępstw, np. kradzieży danych osobowych klientów banku.

---

1 R. Skóra, *Ransomware jako zagrożenie dla cyberbezpieczeństwa. Analiza przypadku ataku Wannacry,* Cyberbezpieczeństwo XXI wieku, s. 40.

2 Tamże.

Przebieg ataku ransomware

Złośliwe oprogramowanie rozprzestrzeniane jest zwykle poprzez wiadomości e-mail, które wyłudzają informacje lub wykorzystują luki w zabezpieczeniach systemowych. Podczas ataku phishingowego atakujący wysyła wiadomość, która ma łudząco przypominać pochodzącą z wiarygodnego źródła. Wiadomość zawiera łącze lub załącznik, który po kliknięciu instaluje oprogramowanie ransomware na komputerze ofiary. Wykorzystanie luk w zabezpieczeniach systemu działa podobnie, z tą różnicą, że atakujący wykorzystuje błąd zabezpieczeń systemu do zainstalowania oprogramowania ransomware bez wiedzy ofiary. W obu przypadkach po zainstalowaniu oprogramowania ransomware może szybko rozprzestrzenić się na inne komputery w tej samej sieci.

Sprawca działa według schematu:

- uzyskanie dostępu do komputera,
- zainstalowanie na komputerze ofiary oprogramowania ransomware,
- oprogramowanie szyfruje pliki ofiary, przez co stają się one niedostępne dla użytkownika,
- atakujący żąda okupu, który często przybiera formę waluty cyfrowej,
- po opłaceniu okupu, sprawca dostarcza klucz deszyfrujący.

Nie ma jednak gwarancji na to, że osoba przeprowadzająca atak przekaże klucz do odszyfrowania danych. Ponadto dane mogą zostać uszkodzone lub ulec degradacji w wyniku procesu szyfrowania.

Innym sposobem zainfekowania systemu oprogramowaniem ransomware będzie odwiedzenie zaatakowanej witryny, na której mogą znajdować się kody, które dokonują automatycznej instalacji w momencie jej otwarcia przez użytkownika. Zagrożenie stanowią również dostępne do pobrania w Internecie pliki, szczególnie te udostępniane przez nieznaną osobę lub pochodzące z podejrzanych witryn.

Jak wygląda infekcja – przykładowe ataki

Jak już wspomniano, do pierwszych ataków ransomware doszło już w latach 80. ubiegłego wieku. Kilka z nich odbiło się szerokim echem w międzynarodowych mediach. Pierwszy znany ransomware na świecie nosił nazwę AIDS/PC Cyborg. Infekował komputery wyświetlając komunikat o blokadzie dostępu do plików, a następnie prosił o przesłanie 189$ na konto „PC Cyborg Corporation" w celu uruchomienia odblokowania komputera.

Rys. 1. Atak za pomocą oprogramowania CryptoLocker.
Źródło: https://www.varonis.com/blog/cryptolocker [dostęp: 26.02.2025 r.]

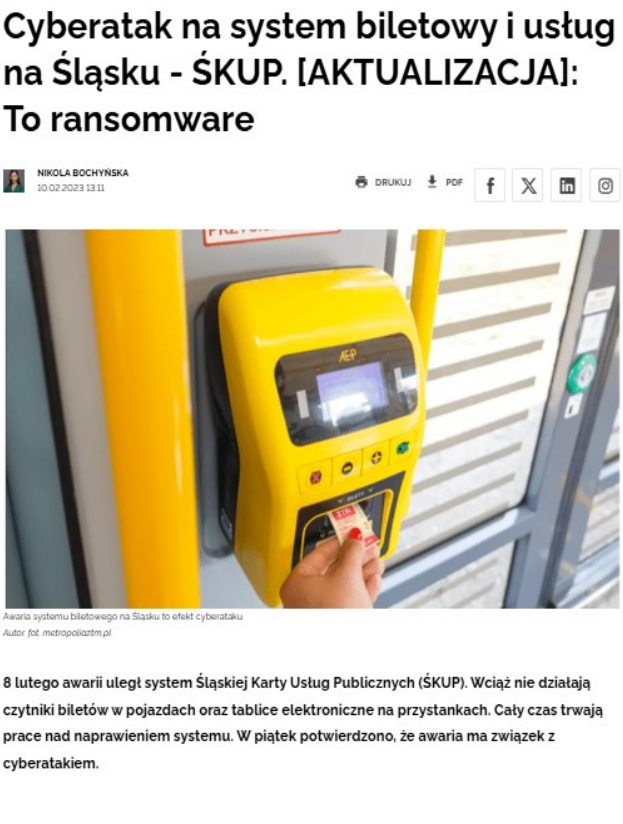
CryptoLocker to oprogramowanie, które w 2013 roku zaczęło atakować konta posiadaczy kryptowalut. System infekował dostęp do platform z cyfrową walutą i żądał okupu za odblokowanie dostępu. Twórcy wirusa mieli zarobić nieoficjalnie 27 milionów dolarów.

Atak ransomware WannaCry swoim zasięgiem objął ponad 150 krajów, infekując przy tym ponad 250 tysięcy użytkowników w ciągu tylko 2 dni. Zainfekowane komputery otrzymały nową tapetę oraz okno z informacją o ataku. Co ciekawe ransomware komunikował się z zainfekowanymi osobami w 28 różnych językach. Ofiara otrzymała informację o tym, że jej pliki zostały zaszyfrowane, a żeby odzyskać te dane musi zapłacić 300 dolarów (w bitcoinach). Jeżeli tego nie zrobi w ciągu 3 dni, kwota haraczu wzrośnie do 600 dolarów. Jeśli przestępcy nie otrzymają okupu w ciągu 7 dni, ofiara straci na zawsze możliwość odzyskania swoich danych (choć w przedstawionym komunikacie jest pewna sprzeczność, gdyż przestępcy zastrzegają, że jeśli ktoś nie będzie w stanie zapłacić, to po 6 miesiącach przewidują uruchomienie możliwości darmowego odzyskania danych). Ofiarami ataku WannaCry zostały podmioty prywatne i publiczne[3].

Rys. 2. Atak za pomocą oprogramowania WannaCry.
Źródło: https://cert.pl/posts/2017/05/wannacry-ransomware/ [dostęp: 26.02.2025 r.]

Ponadto na przestrzeni ostatnich lat, w naszym kraju doszło do wielu ataków ransomware, które ukierunkowane były zarówno na przedsiębiorstwa, instytucje edukacyjne, jak również związane z ratowaniem życia.

[3] Tamże, s. 44.



Cyberatak na system biletowy i usług na Śląsku - ŚKUP. [AKTUALIZACJA]: To ransomware

NIKOLA BOCHYŃSKA
10.02.2023 13:11

DRUKUJ PDF

Awaria systemu biletowego na Śląsku to efekt cyberataku
Autor fot. metropoliaztm.pl

8 lutego awarii uległ system Śląskiej Karty Usług Publicznych (ŚKUP). Wciąż nie działają czytniki biletów w pojazdach oraz tablice elektroniczne na przystankach. Cały czas trwają prace nad naprawieniem systemu. W piątek potwierdzono, że awaria ma związek z cyberatakiem.

Rys. 3. Atak ransomware na system ŚKUP.
Źródło:
https://cyberdefence24.pl/cyberbezpieczenstwo/cyberatak-na-system-biletowy-na-slasku [dostęp: 27.01.2025 r.]

Atak na uczelnię w Poznaniu to ransomware [ZNAMY SZCZEGÓŁY]

SZYMON PALCZEWSKI
31.01.2023 14:20

DRUKUJ PDF

Autor CyberDefence24.pl

Podczas cyberataku na Uniwersytet Artystyczny im. Magdaleny Abakanowicz w Poznaniu wykorzystano ransomware – ustaliła redakcja CyberDefence24.pl. Ryzyko dotyczy pracowników i współpracowników uczelni – łącznie kilkuset osób. Ich dane mogły wpaść w ręce sprawców.

Rys. 4. Atak ransomware na Uniwersytet w Poznaniu
Źródło:
https://cyberdefence24.pl/cyberbezpieczenstwo/atak-na-uczelnie-w-poznaniu-to-ransomware-znamy-szczegoly [dostęp: 27.01.2025 r.]

Czy można zabezpieczyć się przed atakiem?

Organy ścigania doskonale zdają sobie sprawę z tego, że przeciwdziałanie atakom ransomware stało się koniecznością. Pomimo tego liczba ataków staje się coraz większa. Wynika to z prostego faktu, generowane zyski są bardzo wysokie, natomiast ryzyko pozostaje stosunkowo niskie. Pierwsze technologie ataku ransomware, jak również późniejsze, udoskonalone, były znane w sieci już od lat. To jednak kilka ostatnich lat doprowadziło do powstania jednego z najważniejszych i najszybciej rosnących zagrożeń. Stało się tak głównie z powodu epidemii koronawirusa i niezwykłego wprost rozpowszechnienia w 2020 roku pracy zdalnej. Rozproszenie pracowników poza dobrze chronione sieci komputerowe firm spowodowało wzrost liczby i szybkości ataków ransomware. Ataki te są zwykle dziełem indywidualnym, rozpowszechnianym powoli, ale wyrządzają wielkie szkody wielu dużym firmom i organizacjom. Jest to poważny i globalny problem bezpieczeństwa[4].

W jaki sposób można się zabezpieczyć? Wszystkie wykonywane czynności podzielić można na działania prewencyjne oraz naprawcze. Celem ataku jest uzyskanie zapłaty za możliwość odszyfrowania danych, które znajdują się na serwerach lub stacjach roboczych. Kluczem działań prewencyjnych będzie więc określenie jasnych procedur związanych z wykonywaniem kopii zapasowych. Szczególnie ważne będzie zabezpieczenie danych niezbędnych dla funkcjonowania określonego

4 W. Nowakowski, *Człowiek i dokumenty*, nr 63, s. 84.

podmiotu. Istotne żeby wykonywane kopie były:

- wykonywane cyklicznie,
- przechowywane w sposób trwały i odporny,
- testowane.

Należy pamiętać o częstej aktualizacji systemów, przeglądarek, programów pocztowych oraz aplikacji użytkowników. Ważne jest zapewnienie separacji logicznej lub fizycznej pomiędzy różnymi działami lub komórkami firmy, co, przy odpowiedniej konfiguracji, pozwoli na ograniczenie skutków infekcji w sieci.

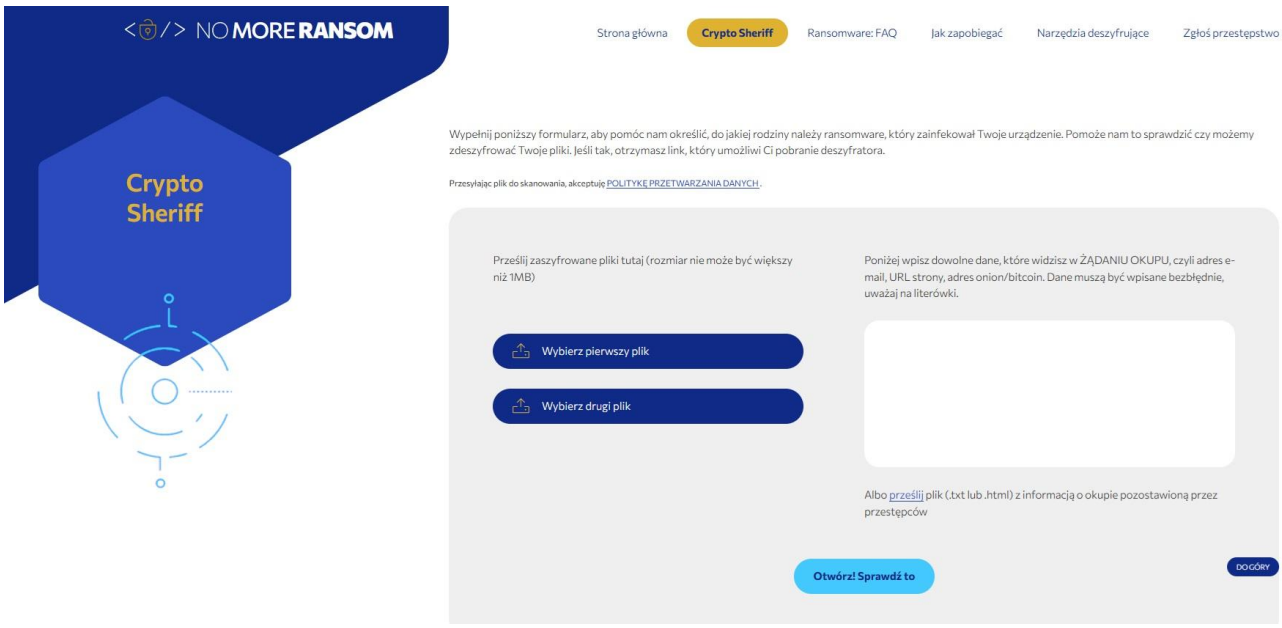
Uwagę trzeba zwrócić również na konkretne wektory ataku. Ryzyko należy ograniczać na warstwie technicznej oraz ludzkiej. Najistotniejszą kwestią od strony użytkownika jest zweryfikowanie czy nie doszło do podszycia się pod inną osobę lub podmiot, w celu zachęcenia do otwarcia załączonego, szkodliwego pliku. Przydatne będzie wprowadzenie filtrowania poczty elektronicznej z wykorzystaniem filtrów antyspamowych oraz zastosowanie polityki bezpieczeństwa odgórnie zapobiegającej uruchomieniu kodu w potencjalnie złośliwych dokumentach.

Wykorzystać należy zabezpieczenia techniczne, które sprawdzą się w przypadku próby uruchomienia złośliwego kodu. Do tego celu stosuje się regularnie aktualizowane oprogramowanie antywirusowe. Odpowiednia konfiguracja Access Control List, pozwoli na zapewnienie minimalnych uprawnień dla użytkowników. Może to ograniczyć potencjalne straty. Bieżące monitorowanie oraz bezpieczne przechowywanie logów z urządzeń w sieci, jest podstawą do sprawnej detekcji oraz skutecznego zablokowania ataku. Usprawni to również analizę powłamaniową w przypadku ewentualnego incydentu.

Reagowanie na incydent

Jeśli dojdzie do ataku należy z kolei rozpocząć wdrażanie działań naprawczych. Pierwszym krokiem powinno być odizolowanie zainfekowanej maszyny i odłączenie jej od sieci. Wyłączenie komputera może nastąpić wyłącznie w przypadku, gdy nie ma możliwości odłączenia go od sieci. W pamięci ulotnej mogą bowiem znajdować się informacje, które okażą się przydatne na etapie analizy incydentu oraz późniejszego odzyskiwania danych. Jeśli w danym momencie nie ma możliwości odszyfrowania plików, warto wówczas wykonać ich kopię zapasową. Pomoże ona uzyskać dostęp do danych po pojawieniu się dekryptora. W identyfikacji źródła infekcji pomaga analiza logów pod kątem nietypowych działań i połączeń sieciowych.

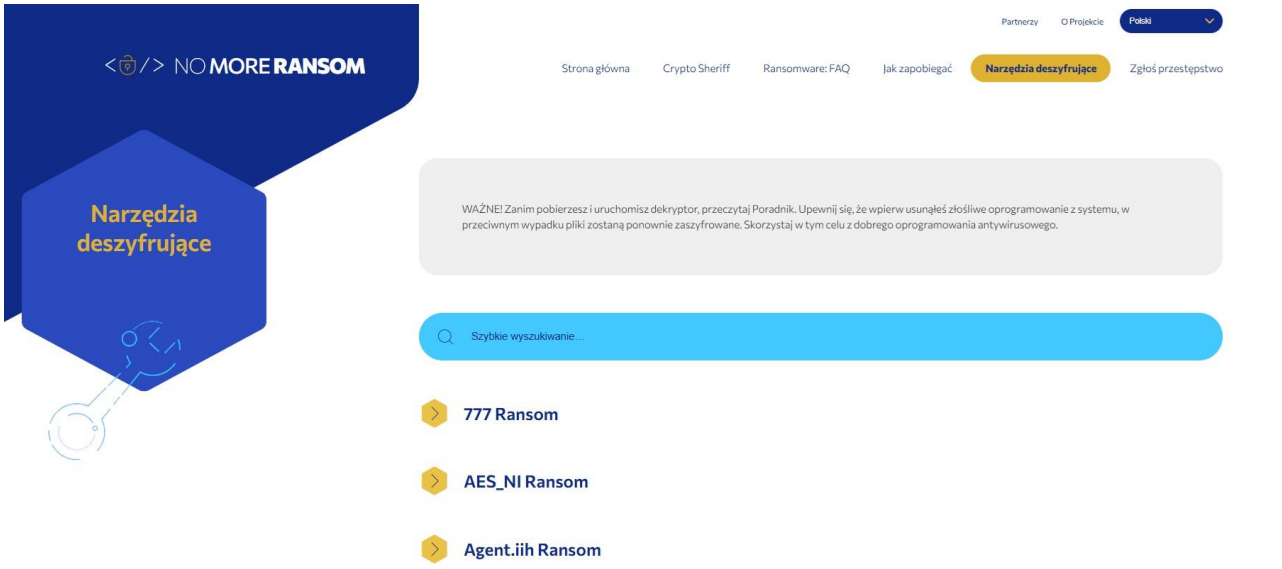
Jednym z najważniejszych działań będzie określenie rodziny oprogramowania szyfrującego. Można to zrobić poprzez przeprowadzenie analizy notatki z okupem lub zaszyfrowanych plików. Z pomocą w tym przypadku przychodzi narzędzie dostępne na stronie nomoreransom.org. Witryna pozwala na skorzystanie z narzędzia Crypto Sheriff, za pomocą którego można określić typ złośliwego oprogramowania, które zainfekowało urządzenie.



Rys. 5. Narzędzie Crypto Sheriff.
Źródło: https://www.nomoreransom.org/crypto-sheriff.php?lang=pl [dostęp: 10.03.2025 r.]

Jeśli do znalezionej rodziny zostanie dopasowany dekryptor, wówczas pojawi się instrukcja postępowania pozwalająca na próbę odzyskania plików. W przypadku znalezienia odpowiedniego dekryptora na wspomnianej stronie, w celu odszyfrowania danych należy postępować ściśle według załączonej instrukcji dla danego narzędzia.

Liczba narzędzi deszyfrujących jest bardzo rozbudowana. Użytkownik może również skorzystać z dostępnej wyszukiwarki.



Rys. 6. Narzędzia deszyfrujące.
Źródło: https://www.nomoreransom.org/pl/decryption-tools.html [dostęp: 10.03.2025 r.]

W przypadku wykrycia infekcji oprogramowaniem szyfrującym, należy podjąć niezwłocznie kontakt z zespołem CSIRT NASK poprzez stronę incydent.cert.pl albo e-mail cert@cert.pl. W przypadku kontaktu, rekomendowane jest dołączenie następujących plików:

- minimum dwa zaszyfrowane pliki,
- notatka z żądaniem okupu od przestępcy.

Rekomendowane jest również wysłanie następujących plików, w przypadku gdy jest to możliwe:

- próbka złośliwego oprogramowania, która zainfekowała maszynę,
- logi z zainfekowanej maszyny oraz systemów bezpieczeństwa z czasu infekcji,
- oryginały plików, które zostały zaszyfrowane, jeżeli się zachowały.

Ransomware stanowi niezwykle poważny problem i dotyczyć może każdego użytkownika Internetu. Najlepszym sposobem zapobiegania atakom ransomware jest zachowanie czujności i podjęcie kroków w celu ochrony komputera i danych. Może to pomóc zmniejszyć ryzyko ataku i ułatwić złagodzenie jego skutków, jeśli już nastąpi.