aut. Artykuł Promocyjny 09.06.2020

RANSOMWARE CI NIE STRASZNY, JEŚLI MASZ BACKUP

Ataki ransomware paraliżują służbę zdrowia, doprowadzają do gigantycznych strat finansowych, unieruchamiają metro, czy nawet wpływają na prace uczelni wyższych. Są uważane za jedne z najgroźniejszych zagrożeń w cyberprzestrzeni. Stanowią wyzwanie nie tylko dla gigantów przemysłowych czy instytucji państwowych, ale również dla każdego użytkownika internetu i jego danych. Jak im przeciwdziałać?

„Okup za dane". Czym jest ransomware?

Szkodliwe oprogramowanie ransomware, znane też pod nazwą rogueware lub scareware, blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych danych. Cyberprzestępcy proponują ofiarom ściągnięcie blokady po opłaceniu okupu, który najczęściej przelewany jest na konta hakerów w kryptowalutach. Nasze dane i możliwość normalnej pracy stają się tym samym zakładnikiem w tej nieuczciwej walce. Złośliwe oprogramowanie jest podstępem przemycane do naszych komputerów choćby poprzez niewinnie wyglądający załącznik w e-mailu lub skłonienie nas do odwiedzenia przygotowanej przez cyberprzestępców strony WWW. Jednak uśpienie naszej czujności to nie jedyną droga do przejęcia naszego sprzętu. Ransomware może również przenikać do komputera poprzez sieć.

Ten rodzaj ataku staje się coraz popularniejszy, ze względu na fakt, że jest on stosunkowo prosty w przygotowaniu. Istnieje wiele bardzo dobrze udokumentowanych sposobów napisania takiego oprogramowania.

Ransomware – plaga dla firm i zwykłych użytkowników

Ataki ransomware nie należą wprawdzie do najpopularniejszego rodzaju zagrożeń, ale z pewnością są jednym z największych zagrożeń dla użytkowników sieci. Ponadto ich popularność stale rośnie, tylko w 2019 roku firma IBM zanotowała dwukrotny wzrost liczby ataków z użyciem ransomware.

Skutki ataków ransomware mogą być niezwykle kosztowne. W przypadku pojedynczego użytkownika uzyskanie klucza odszyfrującego to koszt średnio od 300 do 600 dolarów. Jednak straty dla firm sięgają milionów dolarów.

Atak z użyciem oprogramowania szyfrującego z kwietnia, który dotknął firmę Cognizant, świadczącą usługi moderacji treści m.in. dla Facebooka, mógł kosztować nawet 70 mln dolarów - poinformowała firma, która wciąż szacuje straty po incydencie. Jedna z największych firm transportowych na świecie, duński Maersk, poniosła straty sięgające 300 milionów dolarów. Jeszcze większe straty poniósł producent aparatów słuchowych Demant, który musiał zapłacić ponad 400 mln dolarów.

Liczne przykłady pokazują, że ransomware może być naprawdę dochodowym biznesem i nie powinno

dziwić, że coraz więcej cyberprzestępców angażuje się w tego typu działania. Straty wynikające z użycia przez cyberprzestępców ransomware będą stale rosły, w 2019 roku wyniosły one prawie 12 miliardów dolarów, a w 2021 mają przekroczyć 20 miliardów, jak wynika z szacunków CyberSecurity Ventures.

Przy ocenie ryzyka i potencjalnych strat nie pomagają apele ekspertów, by nie płacić okupu cyberprzestępcom. W niektórych przypadkach jest to jednak nieuniknione. Niejednokrotnie okazuje się, że tańsze będzie zapłacenie hakerom za klucz odszyfrujący niż odbudowa sieci, systemów, czy bezpowrotna strata cennych danych.

Ransomware jako broń

Jednak nie każdy atak ransomware ma na celu wyłudzenie okupu. Oprogramowanie to jest także stosowane przez państwa do niszczenia danych i paraliżowania działania firm i instytucji publicznych. Dwa największe ataki, WannaCry i NotPetya, nie były stworzone z myślą o wyłudzaniu okupu, a właśnie zniszczeniu danych.

Koszty uporania się z epidemią WannaCry wyniosły od 4 do 8 miliardów dolarów. Zainfekował on ponad 300 tys. komputerów w 99 krajach. Znacznie groźniejsza NotPetya spowodowała straty rzędu 10 miliardów dolarów, infekując ukraińskie ministerstwa, banki, system metra, a także przedsiębiorstwa na całym świecie.

To dowód na to, że okup nie jest jedynym czynnikiem motywującym atakujących. Celem może być np. sparaliżowanie państwa, określonego sektora gospodarki albo wpłynięcie na ceny ropy naftowej na świecie. Hakerzy osiągają te cele udając, że mamy do czynienia z oprogramowaniem, które wygląda i zachowuje się jak ransomware. Atak na bank na Tajwanie w 2017 roku był takim przykładem. Zaszyfrowano dane z użyciem ransomware w celu odwrócenia uwagi zespołu bezpieczeństwa. W tym samym czasie hakerzy manipulowali systemami bankowymi tak, aby wykraść jak największą ilość pieniędzy.

Backup przyjdzie Ci z pomocą

Najłatwiej jest zapobiegać ransomware poprzez upewnienie się, że wszystkie programy na komputerze są aktualne. Ważny jest również stale aktualizowany program antywirusowy i firewall. Czasami jednak zapory te są niewystarczające, wtedy niezbędne okazuje się sięgnięcie po niezawodny backup.

Warto pamiętać jednak, że nie może być on przechowywany w tym samym miejscu co nasze systemy. Opcją mogą być kopie zapasowe przechowywane w chmurze.

Takie rozwiązanie oferuje nazwa.pl w postaci usługi Cloud Backup. Jest ona wykorzystywana do wykonywania szyfrowanych kopii zapasowych danych z komputera działającego w systemie Microsoft Windows 7 lub 10 i pozwala na zabezpieczenie się przed atakami ransomware. Dane przed wysłaniem na serwer szyfrowane są lokalnie na komputerze i zabezpieczane hasłem znanym tylko użytkownikowi. Zapewnia to, że nikt nie będzie w stanie ich odczytać, nawet dostawca usługi. Narzędzie pozwala zmieniać hasło szyfrowania danych, dzięki czemu możliwe będzie zadbanie o jego bezpieczeństwo poprzez regularne zmiany oraz w przypadku, kiedy podejrzewamy, że ktoś wszedł w posiadanie naszego hasła.

Usługa Cloud Backup oferuje bardzo mocne szyfrowanie, które odbywa się za pomocą symetrycznego algorytmu AES-256. Nawet jeżeli hakerom uda się zainfekować dane i będą żądali okupu, to dzięki rozwiązaniu od nazwa.pl informacje są bezpieczne i mogą zostać przywrócone bez konieczności opłacenia okupu. Usługa Cloud Backup pozwala na dokonywanie kopii zapasowej w sposób prosty

i szybki, ale przede wszystkim bez zbędnego wysiłku ze strony użytkownika. Oprogramowanie instalowane jest na komputerze w przeciągu kilku sekund, a proces tworzenia kopii zapasowych danych jest na tyle prosty, że nie sprawi nikomu problemu i nie zniechęci do ich robienia.

W celu skutecznego zabezpieczenia się przed ransomware potrzebne jest tworzenie regularnych kopii zapasowych. Dlatego tak ważny jest funkcjonalny harmonogram backupu pozwalający na wykonywanie automatycznie kopii zapasowej o określonej godzinie, w wybrane dni tygodnia. Istnieje jednak również możliwość stworzenia jej w każdym momencie, niezależnie od zdefiniowanego kalendarza backupu. Nie ma skuteczniejszego środka na ochronę przed skutkami ransomware niż kopia zapasowa, dlatego usługa, która to umożliwia w prosty, intuicyjny sposób powinna stać się nieodłącznym narzędziem każdego internauty, firmy oraz instytucji.

Czytelnicy CyberDefence24.pl mogą teraz aktywować za darmo usługę Cloud Backup na okres 30 dni bez konieczności rejestracji w nazwa.pl. Aby pobrać aplikację bezpiecznie na swój komputer, wystarczy kliknąć poniżej: