Oprogramowanie ransomware: wszystko, co musisz wiedzieć

Masz mnóstwo pracy. Padasz z nóg. Marzysz o tym, żeby pograć w Pokémon Go albo przejrzeć firmowy intranet. Niezależnie od przyczyny, za każdym razem, gdy klikasz przycisk „Przypomnij mi później" w oknie aktualizacji oprogramowania, narażasz swoje urządzenie na atak ransomware.

To jedna z wielu dróg, którą oprogramowanie ransomware może dostać się do Twojego systemu. Złośliwe reklamy, fałszywe wiadomości e-mail, a nawet zaawansowane metody z użyciem pendrive'a to częste taktyki wykorzystywane przez cyberprzestępców, aby uzyskać dostęp do Twoich danych. Przyjrzyjmy się typowemu scenariuszowi.

Klikasz przycisk „Przypomnij mi później"

Żadne oprogramowanie nie jest doskonałe. Programiści często odkrywają błędy w programach i udostępniają poprawki, aby je usunąć. Jeśli odkładasz aktualizowanie dodatków lub aplikacji, cyberprzestępcy mogą łatwo wykorzystać znane luki w zabezpieczeniach. W przypadku jednego z popularnych pakietów wykorzystujących luki w zabezpieczeniach 80% skutecznych ataków przeprowadzono przez aplikację Flash. Niezależnie od tego, czy chodzi o aplikację Flash, Silverlight, czy nawet Google Chrome, pamiętaj, by regularnie je aktualizować i instalować poprawki.

Doszło do zarażenia

Teraz oprogramowanie ransomware przejmuje kontrolę nad zaatakowanymi systemami. Następnie przy użyciu asymetrycznej wymiany klucza szyfruje pliki. Mówiąc w skrócie, jest ono w stanie zaszyfrować dane bez Twojej zgody – i tylko autor oprogramowania ransomware ma klucz umożliwiający odszyfrowanie. Niektóre formy oprogramowania ransomware rozprzestrzeniają się także poprzez sieć. Specjaliści zajmujący się bezpieczeństwem przewidują, że z czasem tego rodzaju samopowielające się programy będą zyskiwać na popularności.

Pojawia się wiadomość o żądaniu okupu

Po zakończeniu procesu zarażenia na ekranie pojawia się wiadomość z żądaniem okupu w bitcoinach za dane. Z reguły okup wynosi 800–42 000 PLN, ale niektóre instytucje musiały zapłacić znacznie więcej. Jeden ze szpitali w Kalifornii przekazał za odzyskanie danych równowartość 71 000 PLN. Zdecydowano się na to, ponieważ każdy dzień blokady funkcjonowania kosztował placówkę 420 000 PLN.

Specjaliści zajmujący się bezpieczeństwem radzą, aby nie płacić okupu. Niektóre typy oprogramowania ransomware nie są w stanie odblokować plików albo automatycznie je niszczą. Specjaliści z firmy Talos zajmujący się zagrożeniami odkryli, że tego rodzaju złośliwe typy oprogramowania ransomware niszczące wszystkie pliki są coraz popularniejsze. Jak wynika ze Śródrocznego raportu na temat bezpieczeństwa w 2016 r., specjaliści ostrzegają, że nowym problemem dotyczącym oprogramowania ransomware jest integralność danych. Nie można ufać cyberprzestępcom, że zachowają integralność szyfrowanych danych, a modyfikacja rekordów medycznych lub projektów technicznych może mieć katastrofalne konsekwencje.

Ponadto, płacąc okup, wspiera się działalność przestępczą. Tak długo, jak cyberprzestępcy są w stanie czerpać zyski ze swojego procederu, będą tworzyć jeszcze skuteczniejsze mutacje oprogramowania ransomware.

Jak zatrzymać oprogramowanie ransomware

Najlepszym sposobem, aby przygotować się na atak oprogramowania ransomware, jest zastosowanie metody warstwowych zabezpieczeń.

Przed atakiem

Wystarczy kilka prostych kroków, aby wzmocnić linie obrony. Należy poważnie rozważyć współpracę z partnerem w zakresie przywracania po awarii – byłby to plan B zapewniający kontynuowanie działalności na wypadek, gdyby doszło do najgorszego. Ale są jeszcze prostsze środki zaradcze. Regularnie wykonuj kopie zapasowe plików, aby chronić ważne dane. Zainstaluj programy blokujące reklamy i zawsze aktualizuj oprogramowanie, gdy pojawi się monit.

Ale same programy blokujące reklamy nie są w stanie wykryć i zablokować całego złośliwego oprogramowania ani rozpoznać niebezpiecznych łączy. Zastanów się nad zastosowaniem rozwiązania Cisco® Umbrella, którego instalacja trwa zaledwie 5 minut. Wykrywa ono złośliwe witryny i blokuje żądania na poziomie hosta.

Podczas ataku

Dzięki rozwiązaniu Umbrella zdecydowana większość plików oprogramowania ransomware zostanie zatrzymana w warstwie DNS, zanim w ogóle będą w stanie dotrzeć do urządzenia użytkownika końcowego. Mimo podjęcia wszystkich działań zapobiegawczych żadna metoda nie zagwarantuje ochrony przed oprogramowaniem ransomware.

Musisz widzieć, co dzieje się w Twojej sieci, i umieć rozpoznawać ataki, gdy do nich dojdzie. Rozwiązanie do wykrywania zagrożeń Cisco Stealthwatch™ monitoruje ruch sieciowy i zauważa nietypowe zdarzenia – na przykład zarażenie oprogramowaniem ransomware. Wysyła ono ostrzeżenie, że system jest zagrożony.

Oprogramowanie ransomware: wszystko, co musisz wiedzieć

Podczas próby uruchomienia pliku Cisco ma skuteczne narzędzia, aby ją zatrzymać:

- Rozwiązanie Umbrella chroni system, blokując żądanie pliku wysyłane do infrastruktury klucza szyfrowania. Oznacza to, że oprogramowanie ransomware nie jest w stanie nawiązać komunikacji wstecznej i uzyskać informacji niezbędnych do zaszyfrowania danych.
- Gdy rozwiązanie Umbrella blokuje żądanie, zapora nowej generacji Cisco blokuje połączenie, zapewniając dodatkową ochronę.
- Jeśli plik zdoła przeniknąć przez warstwę DNS i zaporę, rozwiązanie Cisco Advanced Malware Protection (AMP) dla punktów końcowych blokuje jego uruchamianie, a następnie idzie o krok dalej. W sposób ciągły analizuje całą aktywność pliku w systemie, co umożliwia znalezienie i usunięcie wszystkich złośliwych plików.

Po ataku

Jeśli doszło do ataku oprogramowania ransomware, musisz ocenić zakres szkód i uniemożliwić jego rozprzestrzenianie się. Rozwiązanie AMP blokuje uruchamianie złośliwych plików i usuwa plik z punktu końcowego.

Aby zatrzymać rozprzestrzenianie się złośliwych plików w sieci, przy użyciu dynamicznej segmentacji dostępnej w technologii Cisco TrustSec® można określić, do których jej części dotarło oprogramowanie ransomware.

Chcesz dowiedzieć się więcej? Odwiedź stronę cisco.com/go/security.

C11-737870-00 09/16