Złapałem ransomware! Co teraz?

Jeśli dotarłeś do tego poradnika, to zapewne wiesz, czym jest ransomware, ale na wszelki wypadek przypomnijmy, że chodzi o złośliwe oprogramowanie, które szyfruje pliki na zarażonym komputerze (czasami również w lokalnej sieci), wymagając zapłaty okupu (od kilkuset do kilku tysięcy złotych w kryptowalucie) za ich odszyfrowanie. Ponieważ przestępcy używają silnej kryptografii, to w zasadzie, gdy klikniemy tam, gdzie nie trzeba, a na komputerze zainstaluje się ransomware, jest po wszystkim. Faktycznie w większości przypadków tak, jednak dzięki pracy ekspertów bezpieczeństwa sytuacja nie zawsze okazuje się beznadziejna.

Najlepszą metodą walki z ransomware jest ostrożność, zdrowy rozsądek i regularne backupy kluczowych danych. W ten sposób, nawet jeśli stanie nam się krzywda, potencjalne szkody zminimalizujemy jak tylko się da. Nie zapominajmy również o ustawieniu jako strony startowej witryny CyberTarczy Orange (https://cert.orange.pl/cybertarcza/) bądź przynajmniej regularnego odwiedzania tej witryny. Znacząca część tego typu ataków jest zatrzymywana dzięki CyberTarczy i do momentu, gdy ofiara jest w sieci Orange Polska, mimo iż pozostaje zarażone, pliki nie zostaną zaszyfrowane. W takiej sytuacji wystarczy po prostu usunąć złośliwe oprogramowanie.

Co jednak zrobić, jeśli zamiast być gotowi, okazaliśmy się lekkomyślni?

Zakładamy, że nie masz żadnych wątpliwości co do tego, że jesteś ofiarą ataku, np. dlatego, że pojawił się ekran z odpowiednią informacją. Przy założeniu, że sytuację uda się odwrócić, a malware który nas zaraził, został rozpracowany przez researcherów, co w ogóle musimy zrobić?

- Przedostać się przez ekran, informujący o ataku
- Odzyskać/odszyfrować pliki
- Usunąć złośliwie oprogramowanie (o tym tutaj nie będzie, ale ostatecznie usunięcie wirusa to najmniejszy z problemów)

W kwestii ostatniego punktu rekomendujemy, by po odzyskaniu plików zgrać je na zewnętrzny nośnik, a zarażone urządzenie - jeśli nie mamy stuprocentowej pewności usunięcia zagrożenia - po prostu sformatować i zainstalować od nowa system operacyjny.

Jeśli mamy przed oczami ekran ransomware'u, spróbujmy zrestartować komputer w trybie bezpiecznym z obsługą sieci. A w kolejnym kroku...

Sposób 1

...musimy rozpoznać, z jakim wrogiem mamy do czynienia. W tym celu zaglądamy na witrynę MalwareHunterTeam (https:/id-ransomware.malwarehunterteam.com/index.php). Możemy na niej wrzucić któryś z zaszyfrowanych plików z dysku, lub dokument, opisujący sposób wpłaty okupu. Ten drugi przypadek przydaje się, gdy zaszyfrowane pliki nie mają konkretnego rozszerzenia, które ułatwiłoby pracę narzędziu.

Tutaj w najlepszym przypadku dowiemy się, czym się zaraziliśmy i jak się wyleczyć. Szansa wbrew pozorom nie jest bardzo mała, bowiem eksperci od ransomware nie lubią poddawać się przestępcom, konsekwentnie wyszukują błędy w algorytmach, w efekcie czego lista "rodzin"

oprogramowania możliwego do odszyfrowania systematycznie rośnie. W części przypadków dostaniemy też link do oprogramowania, które pomoże nam odszyfrować pliki, ale jeśli tak się nie stanie, to też nie ma powodów do załamywania rąk. Wiedząc, czym się zaraziliśmy, możemy sami poszukać w Google odpowiedniego lekarstwa.

Sposób 2

...poszukajmy punktów odzyskiwania systemu. Jeśli sami nie wyłączyliśmy tej możliwości, system Windows raz na jakiś czas tworzy kopie plików na naszych dyskach, byśmy w razie problemu z instalacją nowej aplikacji, bądź kolejnej wersji systemu operacyjnego mogli wrócić do sytuacji, gdy wszystko było dobrze. Darmowa aplikacja ShadowExplorer (http://www.shadowexplorer.com/downloads.html) dzięki interfejsowi graficznemu ułatwi nam korzystanie z wbudowanego mechanizmu. Uruchamiamy ją, wybieramy dysk, a następnie datę kopii, którą chcemy odzyskać.

Sposób 3

...spróbujmy odzyskać to, co teoretycznie zostało skasowane, używając np. któregoś z narzędzi opisanych tutaj (http://lifehacker.com/5237503/five-best-free-data-recovery-tools). Narzędzie na wszelki uruchamiamy z pendrive'a, wybierając jak najdokładniejsze, najgłębsze i najbardziej czasochłonne metody skanowania.

Czy to pomoże?

Nadziei nie warto tracić do samego końca, tym niemniej sytuacji, gdy nasze pliki zostały już zaszyfrowane, nigdy nie będzie można określić jako optymistycznej. Autorzy materiału, z którego korzystałem, pisząc niniejszy tekst, wykonali serię testów na 10 próbkach ransomware, w każdym przypadku pozwalając oprogramowaniu zaszyfrować 1000 plików (pdf, jpg, ppt, txt, doc, xls) umieszczonych w trzech różnych lokalizacjach. **Najskuteczniejsza okazała się metoda 1**, gdzie w 5 przypadkach udało się odzyskać wszystkie pliki (w trzech jednak ani jednego). Metoda 2 była skuteczna w stu procentach trzykrotnie, w pozostałych wszystkie pliki pozostały zaszyfrowane. Ostatnia z metod była częściowo skuteczna w każdym przypadku - w 9 odszyfrowała od 26 do 33% plików, zaś w jednym (gdzie konkurencja nie dała rady) niemal 9 na 10.

Jeśli mimo wszystkich powyższych rad danych nie udało się odszyfrować, zachowaj zaszyfrowany nośnik i za jakiś czas ponownie podejmij próby.

Tekst oryginalny: securityaffairs.co; tłumaczenie i redakcja: CERT Orange Polska