KASPERSKY lab

Zabezpieczanie danych użytkownika przed szkodliwym oprogramowaniem szyfrującym

Cyberprzestępcy szybko przyswajają techniki rozwijane przez przestępców w świecie fizycznym, łącznie z tymi służącymi do wyłudzania pieniędzy od ofiar. Według jednego z najpopularniejszych scenariuszy ataków ransomware (z ang. ransom - okup, software - oprogramowanie), dane użytkownika zostają zaszyfrowane przed dostarczeniem żądania okupu. Użytkownicy przykładają ogromną wagę do swoich danych i wielu z nich będzie skłonnych zapłacić, aby odzyskać swoje cenne pliki. Jednak zapłacenie okupu jest nierozsądne, głównie z powodu braku gwarancji, że zmodyfikowane dane zostaną odszyfrowane przez przestępcę. Jednocześnie, dzisiejsze szkodliwe oprogramowanie kryptograficzne wykorzystuje mechanizmy szyfrowania, które – jak na razie – wydają się nie do złamania, dlatego ofiary muszą wybrać: albo zapłacą okup, albo stracą te pliki. Naturalnie, zainstalowane na komputerze niezawodne oprogramowanie bezpieczeństwa internetowego zareaguje na szkodliwą aktywność, jednak nawet najlepsze rozwiązania antywirusowe mogą skutecznie wykryć nowo stworzone kryptograficzne szkodliwe oprogramowanie, dopiero gdy zacznie ono modyfikować dane. A zatem, od czasu do czasu nieznane wcześniej szkodliwe oprogramowanie, które nie znajduje się w żadnej bazie danych, zdoła zaszyfrować kilka plików, zanim zostanie zneutralizowane. Właśnie dlatego Kaspersky Lab opracował autorski podsystem do zwalczania szkodliwego oprogramowania kryptograficznego.

Zagrożenie ze strony szkodliwego oprogramowania kryptograficznego

Kryptograficzne szkodliwe oprogramowanie zwykle rozprzestrzeniane jest za pośrednictwem wiadomości spamowych z załączonymi plikami wykonywalnymi i podszywa się pod legalne dokumenty, ale może być również dostarczane na komputery przy pomocy innych sposobów. Odnotowano między innymi przypadki szkodliwego oprogramowania kryptograficznego instalowanego przez inny szkodliwy program – trojana z rodziny ZeuS/Zbot.

Zagrożenie ze strony kryptograficznego szkodliwego oprogramowania jest coraz większe – według danych z Kaspersky Security Network, w 2013 r. odnotowano około 2,8 mln ataków kryptograficznych – tj. dziewięciokrotnie więcej niż w 2012 r. – i wszystko wskazuje na to, że ich liczba nadal będzie wzrastać, ponieważ wiele osób wciąż jest gotowych zapłacić okup. Z badania przeprowadzonego w lutym 2014 r. przez Interdisciplinary Research Centre in Cyber Security na University of Kent wynika, że ponad 40% ofiar szkodliwego programu Cryptolocker zgodziło się zapłacić okup. Ponadto, raport Dell SecureWorks pokazuje, że to samo szkodliwe oprogramowanie „zgarnia” do 30 milionów dolarów co 100 dni.

Co więcej, brak możliwości odszyfrowania plików zaszyfrowanych przy użyciu dzisiejszego szkodliwego oprogramowania prowadzi do kolejnego zagrożenia – fałszywego rozwiązania. Zdesperowani użytkownicy, którzy utracili swoje pliki, przeczesują internet w poszukiwaniu jakiegokolwiek ratunku i czasem znajdują oprogramowanie, które twierdzi, że „odzyska” zaszyfrowane dane. W najlepszym wypadku, mamy tu do czynienia z oszustem sprzedającym bezużyteczne „rozwiązanie”; w najgorszym – takie narzędzie będzie rozprzestrzeniało kolejne szkodliwe oprogramowanie.

Ewolucja szkodliwego oprogramowania szyfrującego dane

Z każdym rokiem metody przestępcze stają się coraz bardziej wyrafinowane. Pierwsze kryptograficzne szkodliwe oprogramowanie wykorzystywało algorytm oparty na kluczu symetrycznym, gdzie ten sam klucz był wykorzystywany do szyfrowania i odszyfrowania danych. Zwykle, z pewną pomocą dostawców rozwiązań antywirusowych, zmodyfikowane informacje mogły zostać skutecznie odszyfrowane. Później jednak, cyberprzestępcy zaczęli implementować algorytmy kryptograficzne, które wykorzystywały dwa oddzielne klucze – publiczny do szyfrowania plików, oraz prywatny, niezbędny do odszyfrowania danych. Jeden z pierwszych możliwych do zaimplementowania przez cyberprzestępców systemów szyfrowania z kluczem publicznym nosił nazwę RSA (od pierwszych liter nazwisk osób, które opisały ten algorytm: Ron Rivest, Adi Shamir oraz Leonard Adleman). Jeszcze w 2008 r. eksperci z Kaspersky Lab zdołali złamać 660-bitowy klucz RSA stosowany przez trojana GPCode, jednak niedługo potem jego autorzy aktualizowali ten klucz do 1024 bitów, co utrudniło jego odszyfrowanie.

Algorytm oparty na kluczu publicznym jest również wykorzystywany przez jeden z najnowszych i najgroźniejszych szkodliwych programów kryptograficznych - wspomnianego wcześniej trojana Cryptolocker. Po tym, jak każdy komputer zostanie zainfekowany, szkodnik ten łączy się z serwerem kontroli w celu pobrania klucza publicznego, a zatem występuje tu inny, prywatny klucz, który jest dostępny tylko dla autorów Cryptolockera. Ofiara zwykle dostaje do 72 godziny na zapłacenie okupu, zanim klucz prywatny zostanie skasowany na zawsze, a odszyfrowanie jakichkolwiek plików bez niego jest niemożliwe. Produkty firmy Kaspersky Lab skutecznie wykrywają tego trojana, jeśli jednak system jest już zainfekowany, nie da się już nic zrobić ze zmodyfikowanymi plikami.

Żądanie okupu wyświetlane przez Cryptolockera

Podsystem Kaspersky Lab służący do zwalczania kryptograficznego szkodliwego oprogramowania

Odkodowanie plików zaszyfrowanych przez współczesne kryptograficzne szkodliwe oprogramowanie jest niemożliwe, dlatego jedynym środkiem bezpieczeństwa, który zapewni ochronę danym użytkownika, jest kopia zapasowa plików. Jednak ogólna kopia zapasowa, nawet wykonywana regularnie, nie wystarczy, ponieważ nie zabezpiecza plików, które zostały zmienione w ostatniej chwili. To dlatego Kaspersky Lab opracował alternatywne środki bezpieczeństwa w oparciu o moduł Kontrola systemu.

Moduł Kontrola systemu Lab analizuje najistotniejsze dane dotyczące zdarzeń systemowych, w tym informacje związane z modyfikacją plików. Gdy zidentyfikuje podejrzaną aplikację próbującą otworzyć osobiste pliki użytkownika, od razu wykona ich lokalną, chronioną kopię zapasową[1]. Jeśli następnie aplikacja zostanie uznana za szkodliwą, Kontrola systemu automatycznie cofnie niepożądane zmiany. Użytkownik nie musi zatem wykonywać żadnych czynności w związku z kryptograficznym szkodliwym oprogramowaniem – zostaną wyświetlone powiadomienia prezentujące najświeższe informacje dotyczące statusu procesu ochrony.

[1] *Pliki kopii zapasowej nie powinny mieć większego rozmiaru niż 10 MB każdy*

Dzięki tej technologii, nawet jeśli nowo powstałe kryptograficzne szkodliwe oprogramowanie wykorzysta lukę zero-day i zdoła obejść wszystkie systemy bezpieczeństwa, nie wyrządzi żadnej szkody, ponieważ wszystkie dokonane przez nie zmiany zostaną automatycznie cofnięte.

Dostępność

Podsystem zapewniający ochronę przed kryptograficznym szkodliwym oprogramowaniem jest zintegrowany z komponentem Kontrola systemu, który wchodzi w skład następujących produktów przeznaczonych dla domu i biznesu:

Rozwiązania dla domu

- Kaspersky Internet Security
- Kaspersky Internet Security – multi-device (tylko dla systemu Windows)
- Kaspersky Total Security – multi-device (tylko dla systemu Windows)
- Kaspersky Anti-Virus

Rozwiązania dla biznesu

- Kaspersky Endpoint Security for Business
- Kaspersky Small Office Security