Biuletyn Bezpieczeństwa Komputerowego

Ochrona przed złośliwym oprogramowaniem

Wstęp

Prawdopodobnie słyszałeś o wirusach, trojanach, oprogramowaniu szyfrującym, rootkitach oraz innych, podobnych zagrożeniach, z którymi można spotkać się w Internecie. Przestępcy korzystają z tego rodzaju narzędzi w celu infekowania i przejmowania kontroli nad urządzeniami swoich ofiar. Wymienione rodzaje zagrożeń możemy określić mianem złośliwego oprogramowania, lub z języka angielskiego - malware. W bieżącym wydaniu biuletynu wyjaśnimy, czym jest złośliwe oprogramowanie, jakie zagrożenia niesie za sobą infekcja, a także jak możemy się przed nim uchronić.

Czym jest złośliwe oprogramowanie?

Złośliwe oprogramowanie to w uproszczeniu program komputerowy napisany specjalnie w celu wykonywania szkodliwych działań. Termin malware pochodzi z j. angielskiego ze złożenia słów malicious (złośliwy) oraz software (oprogramowanie). Przestępcy starają się zainstalować złośliwe oprogramowanie na urządzeniu ofiary, by przejąć nad nim kontrolę lub uzyskać dostęp do zawartych na nim danych. Jeżeli infekcja powiedzie się, malware może umożliwić przestępcom szpiegowanie aktywności użytkownika, kradzież haseł, plików, a nawet atak na innych użytkowników Internetu, z wykorzystaniem urządzenia ofiary. Złośliwe oprogramowanie może pozbawić Cię dostępu do plików, prowadząc do sytuacji, w której będziesz musiał zapłacić okup w zamian za odszyfrowanie danych. Wiele osób błędnie zakłada, że problem złośliwego oprogramowania dotyczy jedynie komputerów z systemem Windows. Niestety, malware może zainfekować praktycznie każdy typ urządzenia, począwszy od komputerów z systemem Mac OS, przez smartfony, a kończąc np. na rejestratorach wideo oraz kamerach. Im więcej urządzeń uda się zainfekować przestępcom, tym większe korzyści prawdopodobnie odniosą.

Jak się chronić?

Jak można przypuszczać, instalacja oprogramowania antywirusowego nie wystarczy, aby uchronić się przed infekcją. Niestety antywirus nie zapewnia ochrony przed wszystkimi zagrożeniami. Przestępcy stale rozwijają swoje narzędzia w taki sposób, by minimalizować detekcję stosowanych przez siebie narzędzi. Z kolei twórcy programów antywirusowych starają się nadążyć za bieżącymi atakami i tak poszerzać funkcjonalność swoich rozwiązań, by ich skuteczność była jak największa. Prowadzi to do swego rodzaju wyścigu zbrojeń, w którym o krok dalej są zazwyczaj przestępcy. Ponieważ, jak wspomnieliśmy, poleganie wyłącznie na ochronie antywirusowej nie wystarczy, przedstawiamy poniżej kilka dodatkowych kroków, jakie warto podjąć w celu osiągnięcia skuteczniejszej ochrony:

Infekując komputery czy urządzenia mobilne, przestępcy zazwyczaj wykorzystują podatności w zainstalowanym na nich oprogramowaniu. Im bardziej aktualna wersja posiadanego oprogramowania, tym mniej możliwych do wykorzystania podatności, a tym samym mniejsza możliwość przejęcia urządzenia. Zadbaj, by Twój system operacyjny, aplikacje, oraz instalowane w przeglądarkach internetowych dodatki, były zawsze w najnowszej dostępnej wersji. Optymalnym rozwiązaniem będzie skorzystanie z aktualizacji automatycznych.

Powszechnie stosowaną metodą dystrybucji złośliwego oprogramowania jest tworzenie fałszywych aplikacji, publikacja w Internecie oraz zachęta do ich pobrania i instalacji. Pamiętaj, żeby zawsze pobierać aplikacje z zaufanych źródeł. Unikaj tych niedawno opublikowanych, posiadających niewielką liczbę pozytywnych opinii, jak również takich, które zostały pobrane przez małą grupę użytkowników i od dawna nie były aktualizowane. Jeżeli nie korzystasz już z aplikacji, odinstaluj ją ze swojego urządzenia.

Często wykorzystywaną metodą ataku jest próba przekonania użytkownika do samodzielnej instalacji złośliwego programu. W tym celu przestępcy mogą wysłać wiarygodnie wyglądającą wiadomość e-mail zawierającą załącznik lub link. Może to być próba podszycia się np. pod bank, urząd lub kogoś znajomego. Jeżeli przestępcy uda się sprowokować ofiarę i otworzy ona link lub załącznik, może to spowodować wykonanie złośliwego kodu infekującego urządzenie. Jeżeli wiadomość wywołuje poczucie presji, zmusza do natychmiastowego działania, lub nosi znamiona czegoś mało prawdopodobnego, zachowaj szczególną ostrożność - może to być próba ataku. Zdrowy rozsądek stanowi tu najlepszą formę obrony.

Zadbaj o regularne wykonywanie kopii zapasowych. Możesz skorzystać z serwisów opartych o rozwiązania działające w chmurze, lub wykorzystać do tego np. zewnętrzne dyski twarde. Umożliwi to dodatkową ochronę danych, np. w sytuacji infekcji złośliwym oprogramowaniem szyfrującym. Poprawnie wykonane kopie zapasowe to często ostateczna i jedyna metoda pozwalająca na odzyskanie utraconych plików.

Najlepsze metody ochrony przed złośliwym oprogramowaniem to: posiadanie aktualnego oprogramowania na urządzeniach, instalacja oprogramowania antywirusowego pochodzącego z zaufanego źródła, jak również racjonalne podejście do otrzymywanych wiadomości, mogących stanowić próbę infekcji. Jeżeli wszystkie metody zawiodą, warto mieć przygotowaną aktualną kopię zapasową danych.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redaktor Gościnny

Lenny Zelster *w walce ze złośliwym oprogramowaniem wykorzystuje współtworzone przez siebie w Minerva Labs narzędzia do ochrony użytkowników końcowych, prowadzi również wykłady w Instytucie SANS. Aktywny użytkownik Twittera (@lennyzeltser), prowadzi blog poświęcony bezpieczeństwu - zeltser.com.*

Przydatne linki

Ransomware:	https://www.sans.org/u/EdI
Kopie zapasowe:	https://www.sans.org/u/EdN
Phishing i oszustwa w mailach:	https://www.sans.org/u/EdS