Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Czym jest antywirus?

Wstęp

Antywirus jest programem, który instalujesz na komputerze lub urządzeniu mobilnym w celu zabezpieczenia go przed infekcją złośliwym oprogramowaniem (z ang. “malware” to termin powstały z kombinacji słów malicious - złośliwe, oraz software - oprogramowanie). Malware to ogólny termin używany do określenia różnego rodzaju złośliwego oprogramowania, np. wirusów, robaków internetowych, trojanów oraz oprogramowania szpiegującego. W przypadku, gdy komputer zostaje zainfekowany, przestępca może wykraść z niego dane, np. poprzez przechwytywanie wpisywanego tekstu z klawiatury, kradzież dokumentów, czy wykorzystanie go do ataków na innych użytkowników. W przeciwieństwie do ogólnie panującego poglądu, żaden z systemów operacyjnych nie jest odporny na malware, wliczając w to systemy takie jak Mac OS X oraz Linuksa.

Redaktor gościnny

Jake Williams jest założycielem firmy Rendition Infosec (**www.renditioninfosec.com**) oraz autorem kursów i certyfikowanym instruktorem Instytutu SANS. Prowadzi bloga **malwarejake.blogspot.com**, a także jest aktywnym użytkownikiem Twittera (**@MalwareJake**).

Oprogramowanie antywirusowe jest często dołączane jako część większego pakietu służącego do zabezpieczenia komputera, ale można je także kupić oddzielnie. Niestety głównym problemem antywirusów jest to, że coraz trudniej jest im nadążyć za ciągle pojawiającymi się nowymi typami złośliwego oprogramowania. Codziennie powstają dziesiątki jeśli nie setki tysięcy nowych wersji wirusów i absolutnie żaden antywirus nie jest w stanie wykryć i unieszkodliwić ich wszystkich. Nadal jednak antywirusy pozostają jednym z podstawowych narzędzi do zabezpieczania systemu. Aby nauczyć się jak je lepiej wykorzystywać, przyjrzyjmy się jak działają.

Jak działa oprogramowanie antywirusowe

Zwykle antywirusy identyfikują złośliwe oprogramowanie na dwa sposoby: używając tzw. sygnatur lub na podstawie zachowania podejrzanego programu w systemie operacyjnym. Wykrywanie za pomocą sygnatur działa podobnie do systemu odpornościowego człowieka. Antywirus skanuje system w poszukiwaniu charakterystycznych elementów, które zawiera złośliwe oprogramowanie. W celu ich odnalezienia, korzysta z bazy danych złośliwych próbek. Jeżeli na dysku komputera zostanie odnalezione coś, co pasuje do którejkolwiek z nich, antywirus stara się to zneutralizować. Podobnie do systemu odpornościowego człowieka, baza danych złośliwych próbek musi być aktualizowana - podobnie jak system odpornościowy musi być uczony o nowych chorobach za pomocą szczepionek. Antywirusy mogą chronić jedynie przed złośliwym oprogramowaniem, które mogą już rozpoznać. Niestety mnogość rodzajów złośliwego oprogramowania oraz szybkość pojawiania się nowych wersji jest tak duża, że programy antywirusowe nie są w stanie nadążyć. Dlatego właśnie, nie ważne jak bardzo aktualne jest oprogramowanie antywirusowe, zawsze znajdzie się jakaś próbka, która umknie uwadze Twojego antywirusa.

Czym jest antywirus?

Inny sposób wykrywania złośliwego oprogramowania polega na analizie zachowania programów w systemie operacyjnym, a nie wykrywaniu próbek znanego złośliwego oprogramowania. Gdy program zachowuje się podejrzanie, np. gdy stara się uzyskać dostęp do chronionego pliku lub gdy chce zmodyfikować inny program, antywirusy śledzące takie zmiany zaalarmują użytkownika. Takie podejście do wykrywania pozwala na zauważenie nowych odmian malware'u zanim jeszcze pojawią się one w bazach danych znanego złośliwego oprogramowania. Niestety, tego rodzaju metoda ma wady i może powodować fałszywe alarmy. Typowy użytkownik komputera może nie być pewny, jakie zachowanie jest dozwolone w systemie, a jakie nie, a po jakimś czasie może przestać zwracać na nie uwagę i klikać "Akceptuj" w każdym oknie dialogowym jakie się mu pokaże. Naraża to komputer użytkownika na dodatkowe ryzyko. Ponadto, gdy złośliwe zachowanie zostanie wykryte na komputerze, oznacza to, że malware jest już na nim uruchomiony i nie możemy być pewni co do akcji jakie wykonał, zanim został zablokowany przez antywirusa.

Antywirus jest bardzo ważnym elementem systemu zabezpieczeń Twojego komputera, ale nie potrafi wykryć i zatrzymać wszystkich ataków. Ostatecznie, to Ty jesteś najlepszą ochroną swojego komputera, a nie wyłącznie rozwiązania technologiczne.

Antywirus to ważny element wspomagający zabezpieczanie stacji roboczych i urządzeń przenośnych, dlatego zalecamy jego używanie. Należy jednak pamiętać, że antywirus nie jest w stanie całkowicie zabezpieczyć nas przed złośliwym oprogramowaniem. Ostatecznie tylko Ty stanowisz najlepszą ochronę przed atakami przestępców internetowych.

Porady

1. Instaluj oprogramowanie antywirusowe tylko z zaufanych źródeł. Przestępcy często starają się zainfekować Twój komputer poprzez dystrybuowanie darmowych kopii fałszywych programów antywirusowych.
2. Upewnij się, że masz zainstalowaną najnowszą wersję antywirusa oraz, że baza wirusów i sam program antywirusowy aktualizują się automatycznie. Jeśli Twój komputer przez pewien czas był wyłączony i baza wirusów się zdezaktualizowała, pozwól oprogramowaniu ściągnąć jej najnowszą wersję i nie odkładaj takiej aktualizacji na później.
3. Upewnij się, że Twój antywirus automatycznie skanuje każdy pendrive i dysk przenośny podłączany do komputera oraz, że masz włączoną ochronę komputera w czasie rzeczywistym.
4. Zwracaj uwagę na powiadomienia, jakie antywirus wyświetla Ci na ekranie. Większość z nich ma opcję pozwalającą uzyskać dodatkowe informacje o wykrytym problemie albo porady jak postąpić w danym przypadku. Jeśli tego typu powiadomienie pojawi się na komputerze w pracy, natychmiast skontaktuj się z działem pomocy technicznej lub ze swoim przełożonym.
5. Pod żadnym pozorem nie wyłączaj ani nie usuwaj oprogramowania antywirusowego, nawet jeśli uważasz, że spowalnia Twój komputer, blokuje instalację jakiejś aplikacji lub dostęp do strony internetowej. Wyłączenie oprogramowania antywirusowego może narazić Cię na niepotrzebne ryzyko i doprowadzić do poważnego naruszenia bezpieczeństwa.

Czym jest antywirus?

Skontaktuj się z działem pomocy technicznej w przypadku, gdy podejrzewasz, że na Twoim komputerze w pracy nie ma oprogramowania antywirusowego lub jest ono wyłączone. Jeśli antywirus nie chce z jakiegoś powodu działać na Twoim domowym komputerze, spróbuj zainstalować produkt innej firmy lub skontaktuj się z producentem oprogramowania.

6. W żadnym przypadku nie instaluj wielu antywirusów na jednym komputerze w tym samym czasie. Doprowadzi to do konfliktów pomiędzy nimi i w rezultacie obniży poziom zabezpieczeń Twojego komputera.
7. Naucz się odróżniać komunikaty zgłaszane przez Twój program antywirusowy od innych, jakie mogą pojawić się w systemie. Przestępcy często tworzą fałszywe strony WWW, które symulują komunikaty zgłaszane przez oprogramowanie antywirusowe i starają się nakłonić Cię do pobrania ich wersji w celu "naprawy" Twojego komputera. Klikanie w linki na takich stronach może w rzeczywistości zainfekować go złośliwym oprogramowaniem.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.
Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

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

Źródła

Porównanie oprogramowania antywirusowego:	http://ow.ly/Fdi2P
Socjotechnika:	http://www.securingthehuman.org/ouch/2014#november2014
Email i ataki phishingowe:	http://www.securingthehuman.org/ouch/2013#february2013
Co zrobić po włamaniu?:	http://www.securingthehuman.org/ouch/2014#may2014

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski

