Nowa generacja wirusów: nikt nie jest bezpieczny?

wywiad z Mikko Hypponenem

Magazyn *hakin9*, Software-Wydawnictwo, ul. Piaskowa 3, 01-067 Warszawa, *pl@hakin9.org*

Wywiad

Nowa generacja wirusów: nikt nie jest bezpieczny?

wywiad z Mikko Hypponenem

Mikko Hypponen – człowiek, który poświęcił znaczną część swojego życia obronie tysięcy komputerów przed cyfrowymi mikrobami. W ubiegłym roku jako pierwszy ostrzegł świat przed atakiem siejącego ogromne spustoszenie Sassera. Prowadzony przez niego zespół doprowadził też do rozpracowania i zminimalizowania ataków sieciowych robaka Slapper w 2002 roku, a także zlokalizował i dezaktywował ogólnoświatową sieć używaną przez robaka Sobig.F w 2003 roku. Zobaczmy, co ma nam do powiedzenia tym razem.

h9: Lwią część swojego wystąpienia na konferencji F-Secure poświęciłeś kwestii wirusów, robaków i trojanów dla urządzeń mobilnych. Mówiłeś o obecnych realiach, powiedz jednak, jaka jest, Twoim zdaniem, przyszłość złośliwego kodu działającego w sieciach WLAN i Bluetooth?

MH: Potencjalne zagrożenia dla WLAN to jeden z najbardziej koszmarnych scenariuszy, jakie nękają członków naszego zespołu. Jak dotąd realnych zagrożeń nie spotkaliśmy, ale trzeba być czujnym.

Wyobraźmy sobie atak, którego siłę rażenia wyznacza automatyczna transmisja przez tysiące połączeń radiowych. Nieważne, czy będzie to Bluetooth, czy WLAN. Takie wirusy i trojany rozprzestrzenią się w mgnieniu oka – z jednego laptopa na następny, z niego na palmtop, z palmtopa na komórkę prezesa banku, natomiast z niej do wewnętrznej sieci bankowej.

h9: Zgroza. Co dalej?

MH: W ten sposób wirus uzyskuje łatwy dostęp do niechronionego przez firewalle i filtry obszaru wewnętrznego. Łatwy i bez konieczności obchodzenia zabezpieczeń, podkreślmy. Zupełnie tak, jak robaki sieciowe typu Zotob. Jego rozprzestrzenianie do strategicznych sfer wyglądało na przykład tak: pracownik nieświadomie zainfekował laptop u siebie w domu, następnie zabrał go do pracy, gdzie podpiął do niego kabel sieciowy. To wystarczyło, by Zotob dostał się do środowiska wewnętrznego firmy.

h9: Procedura infekcji będzie łatwiejsza, gdy pojawią się wirusy na WLAN i Bluetooth?

MH: Znacznie łatwiejsza! Wystarczy podróżować z zainfekowanym laptopem. Za chwilę wirus będzie nie tylko w twojej sieci, ale i u sąsiada piętro wyżej, piętro niżej. Na dodatek zainfekuje komórkę dostawcy pizzy, który właśnie opuszcza twoje biuro... Ale żeby taki atak miał szanse powodzenia, musiałyby istnieć jakieś zdalne eksploity działające na stosy Bluetooth i WLAN.

h9: Były pierwsze oznaki takiego zagrożenia?

MH: Niestety tak, na przykład dziury w zabezpieczeniach stosu Bluetooth Vidcomu. Większość stacji roboczych z zainstalowanym systemem operacyjnym Windows przez prawie dwa lata była podatna na zdalnego eksploita, który mógł zostać wykorzystany do uruchomienia przez Bluetooth dowolnego kodu na atakowanym komputerze. Nawiasem mówiąc, obawiamy się odkrycia luk w popularnych standardach WLAN, gdyż wiemy, że takie odkrycie jest nie tylko możliwe, ale wysoce prawdopodobne.

h9: W wystąpieniu mówiłeś o systemie Symbian OS. Z tego co wiem, jest to do tej pory jedyny system operacyjny działający na telefonach komórkowych, który udało się zainfekować. Co sprawia, że z taką łatwością można stworzyć wirusa właśnie Symbiana, a nie, przykładowo, na mobilnego Linuksa?
MH: Nie istnieje jedna określona luka. Każdy z wirusów, robaków, trojanów, które widzieliśmy nie tyle starał się wykorzystać konkretnej luki w zabezpieczeniach, ile bazował na omylności użytkownika. Wirusy tego typu działają dokładnie na tej samej zasadzie, co wirusy e–mailowe.
h9: Zupełnie jak LoveLetter?
MH: Dokładnie. Ludzie oszukani przez temat i treść wiadomości otwierają załącznik. Na tym samym bazują obecnie wirusy działające na telefonach komórkowych, rozprzestrzeniające się poprzez Bluetooth. Póki co największym zagrożeniem telefonów komórkowych są ich właściciele.

Gdyby porównać systemy Windows i Symbian, to można dojść do ciekawych wniosków. Symbian ostrzeże użytkownika przed próbą uruchomienia nieznanej aplikacji – Windows nie. Z tego punktu widzenia Symbian jest więc... bezpieczniejszy niż Windows.
h9: Z jakimi najniebezpieczniejszymi trojanami spotkaliście się w ciągu ostatnich miesięcy?
MH: Jeżeli chodzi o infekcje telefonów, to trzeba wymienić takie trojany, które w ogóle uniemożliwiają ich uruchomienie. Zdarzały się takie infekcje, że z zainfekowanymi telefonami nie można było nic zrobić – nawet zadzwonić pod numer alarmowy.

Naprawa takiego telefonu może się odbyć na kilka sposobów. Można zresetować telefon do ustawień fabrycznych, co spowoduje formatowanie całej pamięci i utratę wszystkich danych. Tego, jak wiadomo, nikt nie chce. Można też użyć innego telefonu do przygotowania karty pamięci z naszym oprogramowaniem – usuwającym złośliwy program z zainfekowanego telefonu.

Najciekawszym ostatnio trojanem był blank phone. Wziął on nazwę od metody działania – uniemożliwia odczytanie czegokolwiek. Są ikonki, obrazki, ale nie widać żadnych czcionek. Strasznie to podstępne, bo nawet jeśli zainstaluje się antywirusa, to przecież i tak nie widać żadnego tekstu. Trzeba wiedzieć jakie klawisze wcisnąć, żeby pozbyć się infekcji.
h9: Czy istnieje zagrożenie, że ściągając grę w Javie użytkownik zainfekuje swój telefon?
MH: Po pierwsze – nie widzieliśmy jeszcze żadnej gry w Javie, która zawierałaby wirusa. Zagrożenia wynikające ze stosowania jej w komórkach są na pewno możliwe, tym niemniej jeszcze się z nimi nie spotkaliśmy. Wszystkie złośliwe programy, z którymi mieliśmy do czynienia, były natywnym kodem Symbiana.
h9: Jaka jest ogólna recepta, którą można podać każdemu posiadaczowi telefonu z Symbianem i Bluetooth, aby mógł on zapewnić sobie maksimum bezpieczeństwa?
MH: Praktycznie wszystkie zagrożenia dotyczą Symbiana z serii 60. Jeżeli telefon pracuje na innym systemie, jak Symbian z serii 40 lub 80, Windows lub Linux – to ryzyko jest bardzo, bardzo małe. Jeżeli jednak mamy telefon z Symbianem serii 60, niebezpieczeństwo infekcji pojawia się w momencie instalowania nieznanych aplikacji. Podstawowe działania, jakie należy podjąć, to wyłączenie Bluetooth lub chociaż przejście do trybu ukrytego oraz nieakceptowanie nadchodzących aplikacji – chyba, że się ich spodziewamy. Pod żadnym pozorem nie należy instalować aplikacji nieznanego pochodzenia.
h9: Czy w przyszłości F-Secure ma zamiar wypuścić na rynek antywirusa na inne telefony komórkowe korzystające na przykład z Linuksa?
MH: Na ten temat niestety nie mogę się wypowiedzieć, co nie oznacza, że nie rozwijamy swojej linii antywirusowego oprogramowania linuksowego. Każdy wie, że Finlandia jest krajem bardzo przyjaznym dla Linuksa i jego użytkowników. Nawiasem mówiąc, Linus Torvalds mieszkał kiedyś tuż obok naszego biura. To jasne, że zawsze jesteśmy żywo zainteresowani wspieraniem każdej platformy linuksowej.
h9: Ciekawi mnie bardzo, w jaki sposób zabezpieczasz swój własny, prywatny system przed atakami i w jaki sposób zabezpieczasz swój telefon komórkowy...
MH: Po ponad 15 latach pracy w tym przemyśle mam trochę paranoidalne podejście do kwestii zabezpieczeń i wykorzystuję wielowarstwowe zabezpieczenia. Mój telefon ma zainstalowany program antywirusowy, zamykam też wszystkie otwarte porty, które mogą zostać wykorzystane do ataku. Na swoim komputerze używam dwóch sprzętowych firewalli – jeden bazujący na systemie BSD, drugi pochodzący z mojego rutera.

Co jeszcze? Na swoim laptopie używam programowego firewalla z oprogramowaniem antywirusowym skanującym system w czasie rzeczywistym. Jeśli chodzi o zabezpieczenia antyspamowe, to musisz wiedzieć, że od ponad 10 lat używam jednego adresu mailowego, który jest ogólnodostępny. Jak się domyślasz, oznacza to setki tysięcy sztuk spamu dziennie. Zabezpieczam się przed nim za pomocą procmaila na moim serwerze uniksowym, który wyrzuca i kasuje bardzo duży procent spamu. Po ściągnięciu pozostałych listów na moją stację roboczą używam dwóch innych filtrów wiadomości. W efekcie odbieram dziennie od 5 do 10 spamerskich listów elektronicznych.
h9: Znakomita skuteczność! Dziękuję bardzo za poświęcony czas, Mikko.
MH: Ja również dziękuję i pozdrawiam czytelników magazynu *hakin9*.

Mikko Hypponen
Mikko Hypponen ma 36 lat, pracuje jako Dyrektor Grupy Badawczej w F-Secure Corp. Z firmą związał się w 1991 roku. Od 1995 roku honorowy członek CARO (the Computer Anti-Virus Researchers Organization). Jest kolekcjonerem automatów do gier i pinballi z minionych dekad. Mieszka wraz z rodziną na małej wyspie niedaleko Helsinek.