Duża akcja NASK przeciw wirusowi Virut

19 stycznia 2013

Eksperci z instytutu badawczego NASK przejęli w czwartek wieczorem 23 polskie domeny internetowe służące do zarządzania siecią komputerów zainfekowanych groźnym wirusem Virut. W 2012 r. odnotowano w Polsce aż 890 tys. zgłoszeń adresów IP zainfekowanych Virutem.

Zainfekowane wirusem komputery stają się „komputerami-zombie" – bez wiedzy swoich właścicieli łączą się w sieci, tzw. botnety, które wykorzystywane są często do działań niezgodnych z prawem. Za sprawą botnetu m.in. przeprowadzane są zmasowane ataki sieciowe (tzw. DDoS), rozsyłany jest spam, czy kradzione są poufne dane. Komputery-zombie polecenia otrzymywać mogą za pośrednictwem domen internetowych.

Okazało się, że część domen obsługujących wirus Virut znajdowało się w Polsce. Ekspertom z NASK w czasie największej dotychczas w Polsce akcji tego typu udało się przejąć najważniejsze domeny, które kontrolowały zainfekowanymi Virutem komputerami. Przejęto więc polskie serce tego botnetu i uniemożliwiono sterowanie komputerami-zombie poprzez zarejestrowane w Polsce domeny internetowe.

NASK informuje, że głównymi źródłami wirusa były domeny zief.pl oraz ircgalaxy.pl, które pełniły funkcję centrów sterujących zainfekowanymi komputerami-zombie i wysyłały rozkazy ataku. W ostatnim roku pojawiły się kolejne domeny z końcówką .pl, które miały te same zadania, a także przyczyniały się do rozpowszechniania złośliwych programów – m.in. Palevo i Zeusa.

„To pierwszy przypadek, gdy podjęliśmy decyzję o zaprzestaniu utrzymywania nazw w domenie .pl. Zadecydowała skala zjawiska i zagrożenie dla wszystkich użytkowników internetu. W takiej

sytuacji odmówiliśmy świadczenia usług” – komentują przedstawiciele instytutu badawczego NASK.

Jak przyznają w rozmowie z PAP przedstawiciele NASK, część infrastruktury botnetu Virut odpowiedzialna za sterowanie siecią komputerów-zombie znajduje się na domenach z innych krajów. Polska akcja przeciw wirusowi może więc nie wyeliminuje całkowicie problemu z Virutem, ale z pewnością botnet osłabi.

Zainfekowane Virutem komputery-zombie dalej łączą się z przejętymi przez NASK polskimi domenami, czekając na polecenia, ale tym razem żadnych poleceń nie otrzymują. NASK zapowiada, że będzie się kontaktować z dostawcami internetu. Dopiero oni będą mogli dotrzeć do swoich użytkowników zainfekowanych komputerów i pomóc im w odzyskaniu kontroli nad swoimi urządzeniami.

Pierwsze infekcje Virutem odnotowano w 2006 roku, ale od tego czasu zagrożenie to znacznie przybrało na sile. Od 2010 roku NASK podjął intensywne prace nad wyeliminowaniem działalności Viruta w naszym kraju. W samym 2012 roku zespół CERT Polska, działający w ramach instytutu badawczego NASK, odnotował 890 tys. zgłoszeń zainfekowanych adresów IP z Polski. Według szacunków NASK, potwierdzanych przez dane firmy Symantec, sieć komputerów kontrolowanych przez Virut składa się obecnie na świecie z około 300 tys. urządzeń. Według danych kolejnego producenta oprogramowania antywirusowego – Kaspersky’ego – w III kwartale 2012 roku Virut zajął 5. miejsce wśród najpopularniejszych wykrytych wirusów.

Wirus rozpowszechnia się m.in. poprzez luki w przeglądarkach internetowych, a do zarażenia może dojść w wyniku odwiedzenia strony www, na której przestępcy umieścili Viruta. Aby nasz komputer nie stał się komputerem-zombie, należy dbać o to, by był chroniony przez program antywirusowy, regularnie instalować aktualizacje czy łaty do programów, a w nieznane linki klikać z rozsądkiem.

Czy nasz komputer już jest zombie? Nie jest to takie proste do ustalenia. Wirusy cały czas się zmieniają i występują w różnych wersjach. „Programy antywirusowe nie zapewniają więc w 100 proc. bezpieczeństwa” – wyjaśniają eksperci z NASK. Radzą, by korzystać ze stron, które umożliwiają przeskanowanie naszego urządzenia przez wiele różnych programów antywirusowych – wtedy szanse na wykrycie zagrożeń znacznie rosną.

NASK – Naukowa i Akademicka Sieć Komputerowa funkcjonuje jako instytut badawczy, podlega Ministerstwu Nauki i Szkolnictwa Wyższego. Instytucja pełni rolę krajowego rejestru nazw internetowych w domenie „.pl”.

Autor: Ludwika Tomala
Źródło: PAP – Nauka w Polsce