Word – twórca wirusów!?

Wśród konferencji poświęconych wirusom komputerowym na szczególną uwagę zasługuje organizowana przez brytyjski Virus Bulletin. Dlaczego? Otóż uczestniczy w niej – oprócz „stadka" specjalistów do spraw bezpieczeństwa komputerów w dużych firmach nie mniejsza „zgraja" autorów pakietów przeciwwirusowych.

Stylowe lobby hotelu (u góry), w którym debatowali zarówno szefowie firm, jak i autorzy aplikacji. Był tam również Mark Ellison „Stormbringer" (obok), były autor wirusów

Dwa dni trwała (2–3 X br.) VII międzynarodowa konferencja, zorganizowana w San Francisco przez Virus Bulletin, miesięcznik poświęcony wirusom komputerowym. Ten „spęd" to chyba jedyne miejsce, gdzie można było zobaczyć prawie wszystkich tych, którzy tworzą większość produktów antywirusowych, o których kiedykolwiek słyszeliście.

Impreza składała się z dwóch podstrumieni (jak zwali je organizatorzy): „technicznego" i „korporacyjnego". Na drugim z nich tematykę dobrano w ten sposób, by mogła zainteresować przedstawicieli dużych firm, zaś przedmiotem pierwszego były czysto techniczne aspekty prac związanych z tworzeniem „lekarstw" na powszechnie nie lubiane „stworzonka" (osoby nie będące na bieżąco z wirusologią mogły mieć trudności ze zrozumieniem).

Tegoroczne przeboje...

Oczywiście żaden z prelegentów nie pominął makrowirusów występujących dziś na różnorodnych platformach. Wzrost zainteresowania tymi „mikrobami" wiąże się z dynamiką ich rozwoju – wielokrotnie większą od tej, którą szczyciły się swego czasu wirusy plików czy dysków. Nawiasem mówiąc, wszechobecny Microsoft zapewnia godziwą rozrywkę twórcom antidotów, z każdą wersją zmieniając formaty plików (są tajne!), w których wirusy są przechowywane. Innym zjawiskiem, za które powinniśmy podziękować wspomnianemu gigantowi, jest to, że jego aplikacje posiadają zdolność modyfikacji wirusów i tworzenia ich odmian. Taki na przykład wirus Macro.Word.Npad, który występuje na świecie już w prawie stu odmianach, tylko w dwóch przypadkach (na wspomniane 100) zawdzięcza swe istnienie człowiekowi. Twórcą pozostałych 98 jest program Word (sic!).

W San Francisco m.in. wystąpiło dwóch naukowców, którzy przetestowali działanie kilku tysięcy wirusów. Okazało się, że częste zmiany platformy (z DOS-a na Windows 3.1 czy na Windows 95) przeżyło około 30% wirusów plików i tylko 8% bakcyli dyskowych. Infekcja pozostałymi kończy się z reguły trwałym zawieszeniem się komputera, wizytą fachowca oraz śmiertelnym i bezpotomnym zejściem wirusa. Gdyby nie Internet (a szczególnie Usenet), wielu z wirusów nie zobaczylibyśmy nigdy poza komputerem autora. W takiej sytuacji przestaje dziwić zainteresowanie zablokowaniem tego „kanału" rozprzestrzeniania się „zarazy". Takiego zadania dobrowolnie podjął się Dmitry Gryaznov, jeden z twórców programu antywirusowego Dr Solomon's Antivirus Toolkit, który opracował program działający 24 godziny na dobę na specjalnie w tym celu wydzielonym komputerze i poszukujący wirusów w Sieci – w grupach dyskusyjnych.

Stormbringer + Black Wolf = Mark Ellison

Sporą sensacją tegorocznej konferencji był występ człowieka znanego najpierw jako „Black Wolf", później jako „Stormbringer", a aktualnie jako Mark Ellison. Jak nie trudno się domyślić z przezwisk, ma on na swoim sumieniu napisanie kilku wirusów, z których część „osiągnęła sukces" (do pewnego stopnia), wydostając się na wolność. Tematem jego exposé było pytanie, czy firmy software'owe mogą mieć pożytek z niemałych umiejętności byłych autorów wirusów. Po krótkiej przemowie „Stormbringera" rozpętała się istna burza, której przesłanie było takie, iż pomimo wiedzy młodego geniusza szanse na ciekawą pracę są mizerne. Mówca przy okazji dowiedział się, że znajduje się na liście osób, które zostaną natychmiast aresztowane po przekroczeniu granicy Wielkiej Brytanii. Ten fragment dedykuję krajowym autorom wirusów.

Java i ActiveX – brak wirusów?

Od paru lat analizowana jest możliwość napisania wirusa w języku Java, jak również zagadnienie infekowania upiększających strony WWW modułów ActiveX. Także w tym roku poświęcono im trochę czasu. Oba te konkurujące środowiska są bardzo dokładnie testowane i co jakiś czas znajdują się w nich jakieś dziury w zakresie bezpieczeństwa. Raz odkrywają je testerzy, innym razem twórcy „koni trojańskich", ale jak dotąd nie udało się nikomu napisać działającego wirusa. Fakt ten nie przeszkodził jednej z amerykańskich firm w wyprodukowaniu i sprzedaniu ze sporym komercyjnym sukcesem programu wykrywającego i usuwającego wirusy ActiveX i Javy.

Poza opisanymi zagadnieniami omawiano też w nieco mniej odkrywczych (co nie znaczy kiepskich) wystąpieniach dziury w różnych popularnych systemach (czasem aż włos się jeżył).

W przyszłym roku spragnieni wirusowej wiedzy komputerowcy będą musieli udać się aż do Sydney.

Marek Sell