Już na trzy dni po katastrofie samolotu z Prezydentem Lechem Kaczyńskim na pokładzie, aż siedem z dziesięciu pierwszych wyników wyszukiwania "Tupolev 154 crash" w Google opatrzonych było ostrzeżeniem „Ta witryna może wyrządzić szkody w Twoim komputerze". Żerujących na tragedii śmiałków trzeba było usuwać z serwisu aukcyjnego Allegro, nie zabrakło szemranych ofert wysyłanych przez sms, uaktywnili się spamerzy. Wszystko według tego samego co zawsze scenariusza.

Mówi Tomasz Zamarlik z **G Data Software**, firmy zajmującej się bezpieczeństwem sieciowym: "Istnieje szereg praktyk, które cyberprzestępcy stosują w sytuacji kryzysu. Więcej emocji to większa szansa na manipulację. W ruch idą naprędce przygotowywane strony internetowe i wiadomości e-mail, które rozchodzą się w sieci niesione falą tragedii. W tak wyjątkowej sytuacji przestępcy nie muszą tworzyć nowych trojanów, robaków itp. - wystarczy, że skorzystają ze zwiększonego popytu na informację. Tak trafiają do nowych użytkowników - tych bez oprogramowania antywirusowego."

VOD - Virus on demand
Jak wynika z informacji podawanych przez serwis infosecurity-us.com, w każdą rocznicę ataków na World Trade Center notuje się gwałtowny wzrost ilości stron rzekomo zawierających informacje o zamachach z 11 września 2001r. Witryny te, zainfekowane plikiem podszywającym się pod oprogramowanie antywirusowe, rozprzestrzeniają się za pomocą Black Hat SEO, czyli zestawu niedozwolonych technik pozycjonowania. Choć są one szybko usuwane z indeksów wyszukiwarek, w chwilach popularności danego tematu, trzeba zaledwie godzin, by dotarły do tysięcy użytkowników. Informacja o wykrytym wirusie, która wyświetlana jest przy okazji otwarcia takiej witryny, jest faktycznie zachętą do ściągnięcia konia trojańskiego.

Tragedia w Smoleńsku, a wcześniej trzęsienie ziemi w Haiti, wielkie pożary w Kalifornii, śmierć Patricka Swayze, czy wypadek samochodowy Tigera Woodsa - to idealne okoliczności do poszukiwania materiałów video z miejsca katastrofy. "Ściągnij kodek, by obejrzeć ten film" - głoszą zdradliwe strony, a zastosowanie się do tego polecenia w praktyce oznacza instalację na komputerze złośliwego oprogramowania.

Okazja czyni złodzieja
Kilka dni temu media podały informację o krążącej w sieci wiadomości e-mail: „Proszę zachować tę tajemnicę. Jestem adwokatem Marii Kaczyńskiej, żony prezydenta Kaczyńskiego, która wpłaciła w jednym z hiszpańskich banków EUR.4.500.000.00 na nazwisko o podobnym brzmieniu do Pańskiego. Chcę podzielić się z Państwem 50 proc. tej kwoty. Proszę skontaktować się ze mną w sprawie kolejnych szczegółów". Kuszenie nieoczekiwanym, szczęśliwym zbiegiem okoliczności, szczególnie dobrze sprawdza się w kryzysie. Jeśli wydarzyła się rzecz nieoczekiwana - wielu osobom wzrasta wiara w wystąpienie innych niemożliwych sytuacji.
Mechanizm ten wykorzystywany jest nie tylko przez internetowych oszustów - stosuje się go całkowicie legalnie przy okazji systemów gier losowych.

Gdy rozum śpi, budzą się demony
Aktywność kryzysowa cyberprzestępców nie jest niczym nowym. Wpisuje się ona w nurt praktykowanej od wieków socjotechniki. Już w starożytnym Egipcie, podczas krucjat krzyżowych, czy za czasów Adolfa Hitlera wykorzystywano lęk przed zagrożeniem - realnym lub tylko wyobrażonym - by skłonić nieświadomych ludzi do pożądanego działania. Złośliwe oprogramowanie zarażające komputery przy wykorzystaniu tego mechanizmu nosi nazwę „scareware" (ang. scare – straszyć).

Someday Interactive