# Wrześniowy cyberatak na Polskę

Tomasz Pietryga 11-10-2009, ostatnia aktualizacja 11-10-2009 00:29

źródło: Fotorzepa
autor:

**W połowie września doszło do zorganizowanego ataku na serwery polskich instytucji państwowych. Szczegóły są tajne**

Atak nastąpił w gorącym okresie. Skończyła się właśnie wizyta premiera Władimira Putina na Westerplatte i nie ustawały spory polityczne wokół sejmowej uchwały dotyczącej rocznicy 17 września i zbrodni katyńskiej.

Wiadomo też, że atak pochodził ze strony rosyjskiej i był zorganizowany. Równocześnie usiłowano uderzyć w serwery kilku instytucji rządowych. Próby te jednak nie powiodły się, dzięki tzw. cyberpatrolom ABW, które na czas wychwyciły podejrzany ruch w sieci. Patrole ABW chronią obecne cyberprzestrzeń ponad 50 instytucji rządowych i samorządowych.

O sprawie poinformował wiceszef Agencji Bezpieczeństwa Wewnętrznego płk. Paweł Białek.

Agencja nie chce jednak rozmawiać o incydencie, zasłaniając się bezpieczeństwem państwa. Zadane przez „Rz" pytania o szczegóły ataku (m.in. kto był celem i czy wykryto sprawców) na razie pozostały bez odpowiedzi.

## Z czyjej inspiracji

Jak powiedzieli „Rz" eksperci ABW, nieustannie dochodzi do ataków sieciowych na serwery i witryny internetowe, również te państwowe. Przeprowadzają je zarówno indywidualni hakerzy, zorganizowane grupy przestępcze, jak i tzw. robaki sieciowe, które rozprzestrzeniają się samodzielnie. Część z tych ataków inspirują poszczególne państwa. Zdecydowana większość ataków jest wykrywana i blokowana na urządzeniach zaporowych i innych systemach zabezpieczeń. Te udane, połączone z przełamaniem zabezpieczeń i penetracją zasobów sieci wewnętrznych, to rzadkość – twierdzi ABW.

## Patrol w sieci

Sprawa jest jednak na tyle poważna, że w Departamencie Bezpieczeństwa Teleinformatycznego ABW powołano Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Na bieżąco zbiera on i analizuje informacje o atakach i zagrożeniach. Jednym z zadań CERT.GOV.PL jest nadzór nad systemem wczesnego ostrzegania o incydentach sieciowych ARAKIS-GOV. Dodatkowo CERT prowadzi rutynową akcję monitorowania bezpieczeństwa rządowych witryn internetowych.

– Sposób ochrony jest dość skomplikowany i wielopoziomowy. Ciągle są wdrażane poprawki do poszczególnych systemów i aplikacji i zabezpieczenia całej infrastruktury (np. routerów brzegowych), pracuje też odpowiednio przeszkolony zespół szybko reagujący na niestandardowe zdarzenia – mówi Piotr Błaszczeć, ekspert ds. systemów IT, biegły sądowy.

I dodaje, że to właśnie szybkość wykrycia anomalii sieciowej i odpowiednia reakcja administratorów jeszcze przed incydentem jest najbardziej istotna i stanowi najlepszą obronę przed takimi atakami. Dopiero na końcu analiza zebranych danych i ich jakość służy ustaleniu miejsca cyberprzestępstwa, a w konsekwencji późniejszemu ściganiu sprawców. To niestety jest trudne, dlatego wielu cyberprzestępców pozostaje bezkarnych.

## Pół milion alarmów

Tymczasem tylko w 2008 r. system ARAKIS-GOV zarejestrował ponad milion alarmów dotyczących sieci rządowych w Polsce. W tym roku zaobserwowano około 450 tys. zdarzeń. Zdecydowana większość to fałszywe alarmy, nieudane lub udaremnione próby.



– Ataki na systemy komputerowe stały się powszechne. Dawniej przeprowadzenie takiego ataku wymagało specjalistycznej wiedzy, a dziś wystarczy użycie jednego z exploitów

Tymczasem tylko w 2008 r. system ARAKIS-GOV zarejestrował ponad milion alarmów dotyczących sieci rządowych w Polsce. W tym roku zaobserwowano około 450 tys. zdarzeń. Zdecydowana większość to fałszywe alarmy, nieudane lub udaremnione próby.

– Ataki na systemy komputerowe stały się powszechne. Dawniej przeprowadzenie takiego ataku wymagało specjalistycznej wiedzy, a dziś wystarczy użycie jednego z exploitów (programy mające na celu wykorzystanie błędów w oprogramowaniu lub systemach), które publikowane są na wielu portalach. Wtedy wszystko odbywa się praktycznie automatycznie. Ataki jednak ciągle ewoluują i z poziomu „prywatnych", ukierunkowanych na daną osobę lub firmę, zmieniają się w zmasowane ataki wymierzone w daną sieć czy serwer – mówi Piotr Błaszczeć.

Najczęstsze źródło ataków wykrywanych przez system ARAKIS-GOV to komputery zlokalizowane w Chinach i USA. Jednakże sposób działania sieci Internet powoduje, iż nie można bezpośrednio łączyć źródła ataku z faktyczną lokalizacją sprawcy czy zleceniodawcy ataku – wskazują eksperci.

## Zombie

W zorganizowanej cyberprzestępczości najczęściej do ataku wykorzystywane są rozproszone systemy, które obejmują miliony komputerów i charakteryzują się scentralizowaną kontrolą. Są to tzw. botnety lub sieci zombie. Pozwalają cyberprzestępcom zdalnie kontrolować zarażone komputery bez wiedzy ich użytkowników. Zdalna kontrola natomiast może zostać wykorzystana np. do wywołania pewnej zdefiniowanej akcji w dany punkt sieci , by zmaksymalizować jego obciążenie i zablokować go (zawiesić usługi) czy też przejąć kontrolę, a co za tym idzie skraść dane.

Sieci zombie stały się źródłem dochodów. Najgroźniejsze ataki DDoS (Distributed Denial of Service) pochodzą z botnetów pieczołowicie utrzymywanych i powiększanych jako cenne narzędzie pracy całych grup cyberprzestępców. Złośliwe programy są już produkowane seryjnie przez profesjonalistów. Czarny rynek aplikacji do wykradania poufnych danych prężnie się rozwija, a gangi kontrolują wynajmowanie za określone sumy pieniędzy botnetów do ataku na dowolnie wskazaną infrastrukturę.

– Najgroźniejszy jest jednak fakt, że nie ma takiego łącza, którego nie da się zapchać. Na jak długo? To zależność matematyczna pomiędzy przepustowością łącza (z zachowaniem akceptowalnych parametrów) a liczbą użytych komputerów Zombi.
Rzeczpospolita