

Bezpieczeństwo w sieci

1. Rozwój Internetu



Internet stał się dzisiaj podstawowym narzędziem napędzającym rozwój cywilizacyjny, społeczny i gospodarczy świata. Jego zastosowania - począwszy od poczty elektronicznej, transmisji danych, zdalnej pracy, handlu i transakcji elektronicznych do usług multimedialnych włącznie - stają się coraz bardziej powszechne nie wspominając o użyteczności.

Usługi szerokopasmowe, telefonia poprzez Internet i interaktywna telewizja zmieniają podstawowe zasady komunikacji. Motorem coraz szybszych zmian jest postęp w rozwoju urządzeń IP (Internet Protocol) i sieci optycznych oraz technologii zapewniających bezpieczeństwo i jakość usług. Coraz doskonalsze sieciowe systemy operacyjne, przeglądarki, portale, wyszukiwarki, systemy pracy grupowej, rozproszone bazy danych, protokoły usług katalogowych i wymiany danych sprzyjają tworzeniu i wdrażaniu szerokiej gamy aplikacji. Występuje szeroko rozumiany proces budowy społeczeństwa informacyjnego. Proces przechodzenia do społeczeństwa informacyjnego będzie wymagał zasadniczych zmian w szeroko pojętej infrastrukturze (administracja państwowa i samorządowa, jednostki gospodarcze, każdego szczebla szkoły, ośrodki akademicko - naukowe i badawczo - rozwojowe itp.), kulturze biznesowej, otoczeniu prawnym i organizacyjnym. Dynamiczny rozwój technologii informatycznych w ostatnich kilkunastu latach, w tym Internetu, będzie miał olbrzymi wpływ na naukę i gospodarkę XXI wieku [1].

2. Początki hakerstwa

```
Last login: Mar 12 07:03:29 on console
Welcome to os4!
telnet -a -b ABSOLUT 192.168.100.1:8080
enter login: #####
enter passw: #####
invalid passw ERROR (retype)
retype passw #####
OK you are SUCCESSFULLY logged in
cd /usr/.ABSOLUT/SECRETS
ls -l -a BACKDOORVIRUSES
-rwxr-xr-- TROJANHORSE#BF1 - 306 Mar 7 20:55
-r-xr-xr-- TROJANHORSE#CA0 - 1026 Mar 11 00:13
-r-xr-xr-- TROJANHORSE#CB9 - 716 Mar 5 16:15
-rwxr-xr-- TROJANHORSE#CFE - 4865 Feb 9 22:06
-r-xr-xr-- TROJANHORSE#D2C - 48 Jan 28 17:24
-r-xr-xr-- TROJANHORSE#DBA - 512 Mar 2 02:22
-r-xr-xr-x TROJANHORSE#DA6 - 512 Mar 7 04:46
-r-xr-xr-- TROJANHORSE#DD7 - 642 Feb 13 01:58
-r-xr-xr-- TROJANHORSE#DE2 - 1784 Dec 31 11:33
-rwxr-xr-- TROJANHORSE#EA3 - 1256 Mar 4 14:56
-rwxr-xr-- TROJANHORSE#EB4 - 2873 Mar 5 08:17
-r-xr-xr-- TROJANHORSE#ED8 - 255 Feb 17 10:45
-r-xr-xr-- TROJANHORSE#FA3 - 207 Feb 17 10:57
> sudo -sp TROJANHORSE#D2C
System is about to reboot
Killing all processes .....
```

ABSOLUT HACKER.

ABSOLUT COUNTRY OF SWEDEN VODKA & LOGO, ABSOLUT, ABSOLUT BOTTLE DESIGN AND ABSOLUT CALLIGRAPHY ARE TRADEMARKS OWNED BY V&S SPIRIT AB. THOSE WHO APPROPRIATE QUALITY ENJOY IT RESPONSIBLY. THIS AD. WAS MADE BY FEB 2003.

Na początku istnieli tak zwani Prawdziwi Programiści. Nie nazywali siebie "hakerami", w ogóle nie nazywali siebie. Wyrażenie "Prawdziwy Programista" powstało dopiero po 1980 roku, zostało stworzone przez jednego z tych zdolnych ludzi. Od 1945 roku technologie komputerowe przyciągały największe i najbardziej kreatywne umysły świata. Od czasów ENIAC-a Eckerta i Mauchly'iego istnieje ciągle nieśmiała grupa entuzjastów programowania, ludzi, którzy tworzą i obsługują programy dla zabawy. Prawdziwi Programiści wywodzili się zazwyczaj z kręgów inżynierów, fizyków. Część z nich związana była z radiem amatorskim. Nosili koszule z

poliestru, krawaty i okulary z grubymi szklami, programowali w assemblerze, FORTRANIE i w kilku innych „starożytnych” językach, o których świat zapomniał. Kultura "Prawdziwych Programistów" była mocno związana z przetwarzaniem wsadowym (najczęściej w celach naukowych), które zostało wyparte przez pracę interaktywną, uniwersytety, sieci. Jednak dało to narodziny tradycji, która z czasem zmieniła się w projekt otwartych źródeł hakerskiej kultury [2].

3. Pierwsze szkodliwe programy Malware

Malware to ogólnie wszelkiego rodzaju oprogramowanie, które zostało stworzone w celu zaszkodzenia w dowolny sposób osobom, na których komputerach oprogramowanie to funkcjonuje. Programy takie są rozsyłane za pośrednictwem poczty elektronicznej, popularnych komunikatorów, umieszczane do pobrania w postaci linków na różnych stronach WWW. Bardzo często użytkownicy nie są świadomi posiadania na swoich komputerach takiego oprogramowania, dlatego zaleca się korzystanie (i bieżącą aktualizację) z oprogramowania antywirusowego. W skład malware, oprócz wirusów, wchodzi również:

- Robaki
- Konie trojańskie
- Bomby logiczne
- Króliki, bakterie
- Spyware
- Keyloggery
- Dialery

Robaki to bardzo podobne do wirusów samo - powielające programy, rozprzestrzeniające się jednak nie przy pomocy „żywiciela” jak to robią wirusy, lecz za pośrednictwem środków elektronicznego przekazu w sieci internetowej. Głównie za pomocą poczty elektronicznej i komunikatorów internetowych. Robaki powielają się i kopiują na nowe komputery w sposób automatyczny, przejmując funkcje odpowiedzialne za np. komunikację i przesyłanie plików. Rozprzestrzenianie się robaków przyczynia się do zwiększenia ruchu w Internecie i niekiedy „zapychania” całych sieci firmowych.

Konie trojańskie, zwane popularnie trojanami, to bardzo sprytne aplikacje, które pod pozorem ciekawych funkcjonalności przemycają na komputer użytkownika niezwykle groźną zawartość. Jak najbardziej na miejscu jest tu nawiązanie do mitologicznego konia trojańskiego, który podstępem, pod pozorem prezentu wprowadził do Troi greckich żołnierzy, którzy następnie zdobyli miasto. Taka jest właśnie rola komputerowych trojanów: podszywają się pod rozmaite aplikacje, a w rzeczywistości dokonują spustoszenia w systemie użytkownika.

Bomby logiczne to zagrożenie często przemycane wraz z trojanami. Jest to dosyć specyficzne oprogramowanie, aktywujące się dopiero w pewnych określonych sytuacjach, do tego czasu pozostając w stanie nieaktywnym, przez co zagrożenie to jest bardzo trudne do wykrycia.

Króliki i bakterie – bardzo sympatycznie nazwane, dosyć prymitywne aplikacje, których właściwie jedynym celem jest zawieszenie zaatakowanego systemu przez masowe powielanie się i zajęcie wszystkich dostępnych zasobów pamięci i czasu pracy procesora. Poza tym aplikacje te nie wykazują niszczycielskich skłonności.

Spyware to oprogramowanie szpiegujące działanie użytkownika, gromadzące rozmaite dane i przekazujące je bez wiedzy szpiegowanego do autora programu. Najczęściej spyware wykradają prywatne informacje takie jak loginy i hasła do serwisów internetowych, skrzynek email, kont bankowych, numery kart kredytowych, adresy email znajomych, z którymi użytkownik prowadzi korespondencję.

Keylogger to program przechwytyjący i zapisujący do pliku wszystkie wpisywane przez użytkownika na klawiaturze znaki, łącznie z nazwami aplikacji, w których użytkownik je wprowadził.

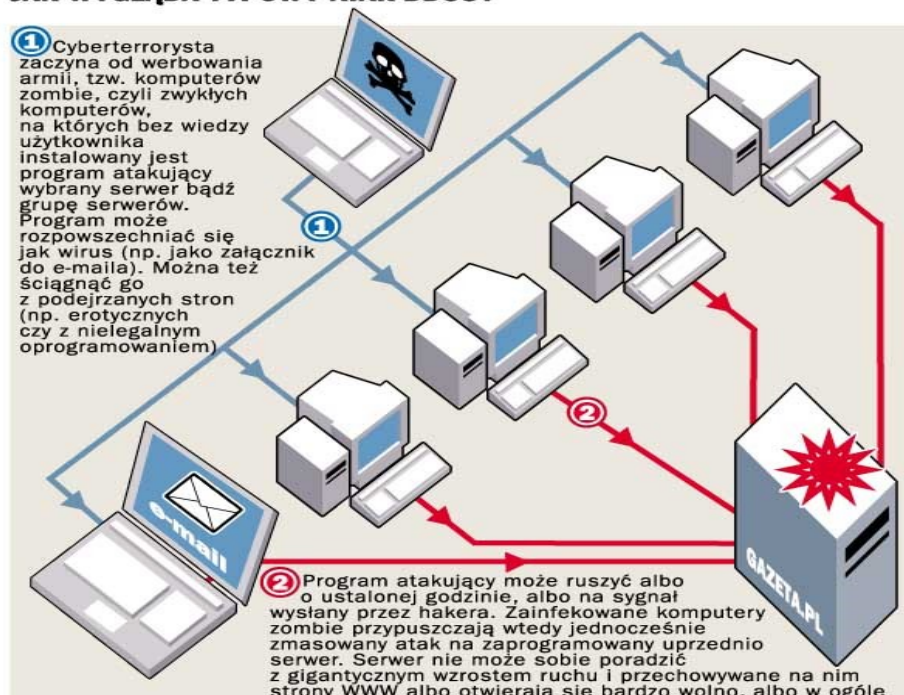
Dialery to programy wykonywalne, najczęściej w postaci niewielkich plików EXE, wykorzystujące modem i linię telefoniczną do zestawiania połączenia. Pierwotnie dialery nie były aplikacjami złośliwymi – miały ułatwić użytkownikom łączenie się z Internetem (dostęp DialUp) czy też z sieciami firmowymi [3].

4. Rozwój szkodliwego oprogramowania

Dzisiaj twórcy wirusów nie skupiają się już na zaawansowanych technologiach, ale przedkładają ilość na jakość. Autorzy szkodliwego kodu odchodzą od tworzenia wielu współdziałających ze sobą modułów, preferując stosowanie wielu funkcji w obrębie jednego programu. Wzrosła również liczba programów trojańskich stworzonych do kradzieży haseł do gier online. Jeżeli chodzi o mobilne szkodliwe oprogramowanie, twórcy wirusów wolą specjalizować się w programach trojańskich dla Javy niż atakować smartfony. Takie programy mogą działać na prawie wszystkich telefonach komórkowych i wysyłać SMS-y, które opróżniają konto użytkownika a napełniają kieszenie autorów trojanów. Obecnie branża antywirusowa musi skupić się na wczesnym wykrywaniu zagrożeń. Podczas gdy w przeszłości firmy antywirusowe mogły reagować na nowe zagrożenia w przeciągu kilku godzin (czasami nawet w ciągu kilku dni), obecnie jest to kwestia minut. To oznacza, że specjaliści ds. rozwiązań antywirusowych muszą zidentyfikować nowy szkodliwy kod w internecie, przeanalizować go, udostępnić ochronę i dostarczyć ją użytkownikowi końcowemu, a wszystko to w bardzo krótkim czasie [4].

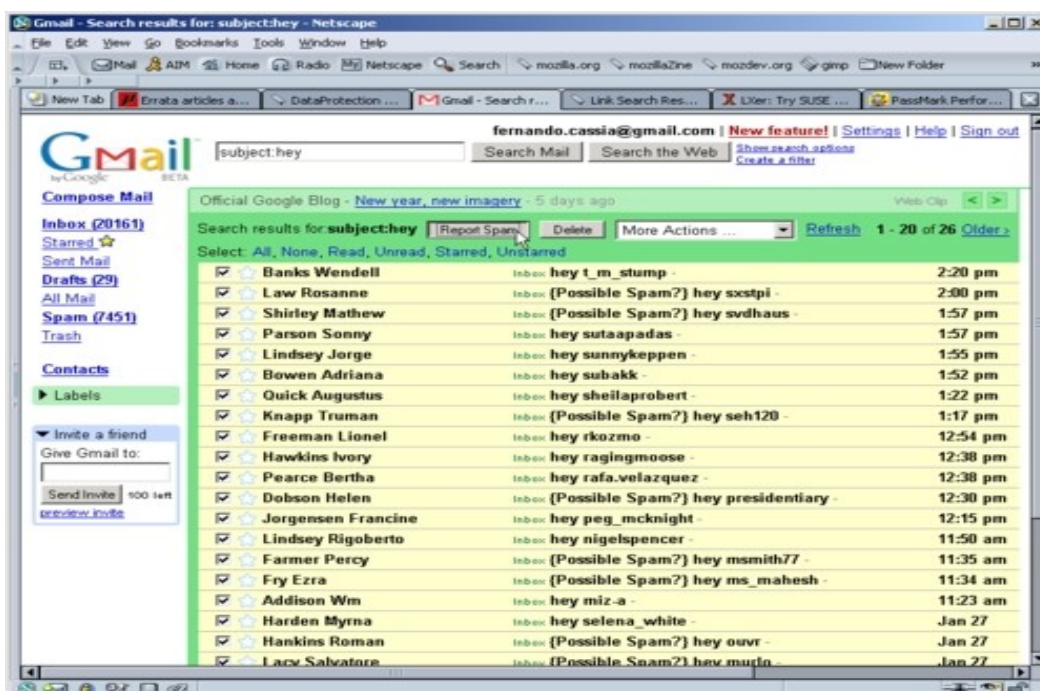
5. Ataki komputerowe

JAK WYGLĄDA TYPOWY ATAK DDOS?



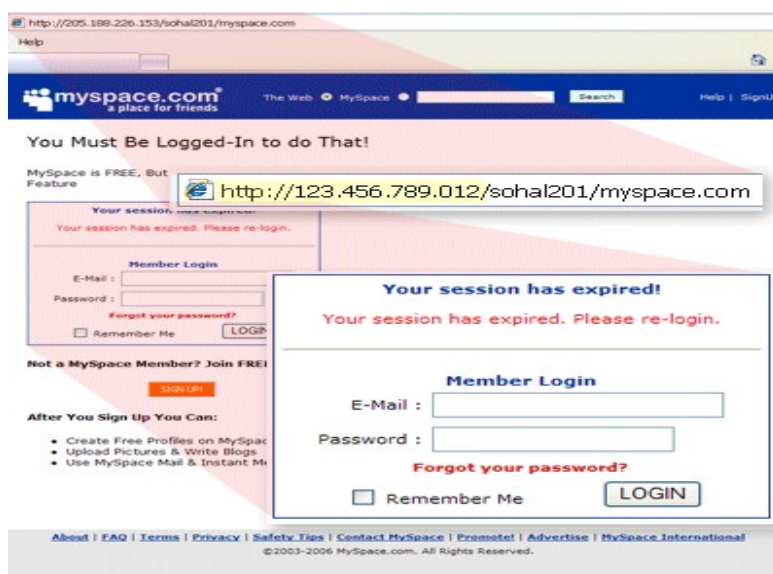
DoS - to atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów. Atak polega zwykle na przeciążeniu aplikacji serwującej określone dane czy obsługującej danych klientów (np. wyczerpanie limitu wolnych gniazd dla serwerów FTP czy WWW), wypełnienie całego systemu plików tak, by

dogrywanie kolejnych informacji nie było możliwe (w szczególności serwery FTP), czy po prostu wykorzystanie błędu powodującego załamanie się pracy aplikacji [5].



Spam – niechciane wiadomości elektroniczne. Najbardziej rozpowszechniony jest spam za pośrednictwem poczty elektronicznej. Część użytkowników doświadcza także spamu w komunikatorach (np. Gadu-Gadu). Zwykle (choć nie zawsze) jest wysyłany masowo. Aby określić wiadomość mianem spamu, musi ona spełnić trzy następujące warunki jednocześnie:

1. Treść wiadomości jest niezależna od tożsamości odbiorcy.
2. Odbiorca nie wyraził uprzedniej, zamierzonej zgody na otrzymanie tej wiadomości.
3. Treść wiadomości daje podstawę do przypuszczeń, iż nadawca wskutek jej wysłania może odnieść zyski nieproporcjonalne w stosunku do korzyści odbiorcy [6].



Phishing - wyludzanie poufnych informacji osobistych (np. haseł lub szczegółów karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne. Jest to rodzaj ataku opartego na inżynierii społecznej. Dzisiaj przestępcy sieciowi wykorzystują techniki *phishingu* w celach zarobkowych. Popularnym celem są banki czy aukcje internetowe. Phisher wysyła zazwyczaj spam do wielkiej liczby

potencjalnych ofiar, kierując je na stronę w Sieci, która udaje rzeczywisty bank internetowy, a w rzeczywistości przechwytyje wpisywane tam przez ofiary ataku informacje [7].

6. Rady bezpieczeństwa dla użytkowników Internetu

Wystarczy chwila nieuwagi, dosłownie jedno nieuważne kliknięcie w link, plik załącznika czy przycisk „OK” w okienku instalatora i już użytkownik „ma problem” w postaci nieproszonego gościa. A jego pozbycie się wcale nie jest takie proste.

Po pierwsze: należy unikać miejsc, w których możemy zostać narażeni na „atak” wszelkiej maści darmowych i pochodzących z niepewnego źródła wygaszaczy ekranu, zestawów ikon i tapet, gier, czy dodatków rzekomo mających usprawnić korzystanie z komputera, a w rzeczywistości niosących groźną zawartość w postaci spyware, dialera czy bomby logicznej. Programy i dodatki do systemu operacyjnego należy pobierać wyłącznie z zaufanych serwisów, w których ryzyko pojawienia się programu, mającego szkodliwe działanie, jest minimalne.

Po drugie: należy bezwzględnie mieć zainstalowany i regularnie uaktualniany program antywirusowy. Jeśli użytkownik jednak nie posiada takiego oprogramowania, powinien często sprawdzać stan bezpieczeństwa dostępnymi skanerami online [3].

Po trzecie: należy używać Windows Update w celu skanowania i aktualizacji twojego systemu operacyjnego Windows za pomocą najnowszych, darmowych poprawek oprogramowania, łącznie z przeznaczonymi dla programów Microsoft Internet Explorer i Microsoft Outlook Express.

Po czwarte: należy zainstalować zaporę ogniową w celu nie dopuszczenia do komputera szkodliwego oprogramowania lub intruzów.

Po piąte: nie należy otwierać załączników e-mail od nieznanego osoby, jak i również zachować ostrożność w przypadku osób znanych. Należy także uważać na nieznaną witryny Web, ponieważ mogą one bezpośrednio przenieść wirusa na komputer [8].

Przestrzegając powyższych zasad bezpieczeństwa użytkownik minimalizuje swoją ekspozycję na zagrożenia jakie niesie ze sobą poruszanie się w internecie. Podsumowując – ogólne zasady opierają się na zdrowym rozsądku i zabezpieczeniu programowym. Cała masa ciągle rozwijanych programów antywirusowych gwarantuje szeroki wybór rozwiązań zabezpieczających.

Bibliografia

[1]- <http://www.umk.pl/~zenkiewicz/kalendarium/>

[2]- http://pl.wikisource.org/wiki/Kr%C3%B3tka_Historia_Hakerstwa

[3]-

http://bezpieczenstwo.onet.pl/1416377,item,0,Konie_robaki_kroliki_i_bakterie_czyli_malware_je_st_grozny,artykuly.html

[4]- http://di.com.pl/di24/24416.0,Kaspersky_Rozwoj_szkodliwego.html

[5]- <http://pl.wikipedia.org/wiki/DoS>

[6]- <http://pl.wikipedia.org/wiki/Spam>

[7]- <http://pl.wikipedia.org/wiki/Phishing>

[8]-

http://www.alarmowesystemy.info/index.php?option=com_content&task=view&id=16&Itemid=97

Autor: Damian Raksimowicz