Zygmunt Ryznar

Wczesne i groźne wirusy komputerowe

(w opracowaniu - under development)

Z puntu widzenia użytkownika komputera wirusów jest "nieskończenie wiele" (wiele tysięcy). Wirusy tworzone są przez hackerów, hejterów, złośliwców wszelakiego pokroju, zapewne tez przez twórców oprogramowania użytkowego (aby zniechęcić do tzw. bezpłatnych programów) i antywirusowego (aby skompromitować konkurentów). Zdarzają się przypadki, że program niby usuwający wirusy zamiast tego instaluje nowe albo ponownie te same (w wersji "ulepszonej" czyli trudniejszej do usunięcia).

Kierunki ataków:

- na nośniki - dyskietki, cd-dvd (przy nagrywaniu), pendrive'y
- na hardware: bios, bootsektory
- na oprogramowanie: system operacyjny, programy, poczta-email
- ataki finansowe - na aplikacje bankowe, karty płatnicze

Data	Wyszczególnienie
Decade70 -XXc.	In the early 1970s Creeper was found an ARPANET. It was a worm that moved through modems to other systems where it displayed the message "I'M THE CREEPER : CATCH ME IF YOU CAN." A similar program called Reaper followed Creeper. It appeared to attempt to find and delete Creeper.
1974	Malware called Rabbit which multiplied so fast making copies of itself that systems crashed.
1975	A game called **Pervading Animal** written for the UNIVAC 1108 asked questions in an attempt to determine what animal the user had thought of. The game, however, attempted to write itself to every writable program file, changing the creation time to be able to determine if it had already written to that file or not. It was never determined if this Trojan-like behavior was intentional or just an unintended bug. >
1986	First PC-based Trojan was released in the form of the popular shareware program **PC-Write**.
Decade 80 XX c.	**Elk Cloner** on Apple II floppy disks (which contained the operating system)
1986 (beginning)	**Brain** Two brothers from Pakistan (Basit Farooq Alvi and Amjad Farooq Alvi) analyzed the boot sector of a floppy disk and developed a method of infecting it with a virus dubbed "Brain".
1986 (December)	**Virdem** Creator:Ralf Burger. Virdem overwrites the first part of the program and appends the original code to the end of the file. Variants of this virus were being created several years later. 1993, VirDem-1542 in 1998
1980	27 października 1980r wirus zawiesza całą sieć ARPANET (prekursor internetu), a 2 listopada 1988 r zaraża 6 tysięcy komputerów sieciowych. Aby uniknąć takich zagrożeń, agencja DARPA powołuje grupę CERT (Computer Emergency Response Team).
1991-	**Michał Anioł** - wirus zagnieżdżający się w bootsektorze
1998	Wirus **CIH** wymazujący pamięć BIOS

1999	the **Melissa** virus in March 1999 Melissa spread in Microsoft Word documents sent via e-mail,
2001	The **Code Red** worm replicated itself more than 250,000 times in approximately nine hours on July 19, 2001 Each copy of the worm scanned the Internet for Windows NT or Windows 2000 servers that did not have the Microsoft security patch installed. Each time it found an unsecured server, the worm copied itself to that server. The new copy then scanned for other servers to infect. Depending on the number of unsecured servers, a worm could conceivably create hundreds of thousands of copies. The Code Red worm had instructions to do three things: Replicate itself for the first 20 days of each month Replace Web pages on infected servers with a page featuring the message "Hacked by Chinese" Launch a concerted attack on the White House Web site in an attempt to overwhelm it. *Polish:*Wirus wykorzystany został w ataku DoS była w 2001 roku do zarażania wirusem Code Red 255 tysięcy serwerów i skierowania ich na adres białego domu Whitehouse.gov (przed całkowitym "zatopieniem" stronę prezydencką uratowała zmiana nr adresu na inny). Wirus wykorzystywał znaną lukę (metodę tzw.przepełnienia bufora) Microsoftowego oprogramowania serwerów internetowych IIS (Internet Information Server). Code Red II nie atakował już strony internetowej Białego Domu, lecz instalował na serwerach "tylne drzwi" umożliwiając wejście hakerom. Straty (koszty oczyszczania - cleanup) spowodowane przez tę odmianę oceniane były na ponad 2 mld dolarów.
2001	W Waszyngtonie w październiku 2001 roku hakerzy przejęli bazę fimy handlującej elektronicznie, zawierającą informacje zakupowe łącznie z numerami kart płatniczych Visa i dokonali szeregu transakcji na ich konto. W wyniku tego zastosowano radykalny środek ratunkowy polegający na wycofaniu dotychczasowych kart i zastąpieniu ich nowymi.
2001	W połowie 2001 roku wykryto błąd w oprogramowaniu IOS firmy CISCO, umożliwiający krakerom - poprzez żądanie okreslonego URL z serwera - ominięcie procedury autentyfikacji i działanie na najbardziej uprzywilejowanym poziomie 15, pozwalającym na przejęcie kontroli nad routerami i switchami używającymi IOS oraz protokołu HTTP.
2001	Przykładem wirusa "zalewającego" microsoftowy serwer IIS był wirus **Nimda**, który prezentowany był w postaci strony zawierającej skrypt javowy, który uruchamiał się w momencie otwarcia strony, powodując rozprzestrzenienie się kodu na wszystkie strony na serwerze oraz generowanie emaili (w niewidocznych oknach - zero-size windows) do innych komputerów wg przypadkowo wybieranych adresów IP oraz adresów znajdujących się w książce adresowej MS Outlook. Ponadto emaile zawierały wykonywalny kod **readme.exe**, który po otwarciu stawał się źródłem dalszej propagacji.
2001	Na początku lutego 2001 roku "włamano" się do serwerów obsługujących Światowe Forum Gospodarcze w Davos i ukradziono bazę danych osobowych, zawierającą m.i. adresy poczty elektronicznej i numery kart płatniczych, po czym dokonano szeregu nielegalnych operacji finansowych. W wyniku tego musiano zablokować wiele kart płatniczych. W parę tygodni potem policja szwajcarska poinformowała o aresztowaniu podejrzanego Szwajcara, wykonującego zawód konsultanta IT.
2000	The **ILOVEYOU** virus, which appeared on May 4, 2000, was even simpler. It contained a piece of code as an attachment. People who double-clicked on the attachment launched the code. It then sent copies of itself to everyone in the victim's address book and started corrupting files on the victim's machine. This is as simple as a virus can get. It is really more of a Trojan horse distributed by e-mail than it is a virus.
2002	Wirus **LFM-926** atakujący pliki flash
2003	Wirus **Sasser** atakuje usługi sieciowe
2003	A worm usually exploits some sort of security hole in a piece of software or the operating system. For example, the **Slammer** worm (376 bytes)(which caused mayhem in January 2003) exploited a hole in Microsoft's SQL server.

2007	A worm called **Storm**, which showed up in 2007, immediately started making a name for itself. Storm used social engineering techniques to trick users into loading the worm on their computers. And boy, was it effective -- experts believe between 1 million and 50 million computers have been infected [source: Schneier]. Anti-virus makers adapted to Storm and learned to detect the virus even as it went through many forms, but it was easily one of the most successful viruses in Internet history and could someday rear its head again. At one point, the Storm worm was believed to be responsible for 20 percent of the Internet's spam mail
2007	Wirus **ZeuS** używany do defraudacji bankowych
2011	**Dugu** szpiegowski szkodnik zaatakował komputery firmowe w całej Europie - podobno wywodził się z kręgów izraelskich służb specjalnych (zbierał informacje o zabezpieczeniach). W 2015 roku **odmiana Dugu-2** instalowała się wyłącznie w pamięci operacyjnej. Kaspersky twierdzi, ze również został zainfekowany. Konkurenci - ze to wymysł samej firmy antywirusowej Kaspersky.
-----	będzie kontynuowane - to be continued