Wirusy, robaki, boty – sposoby obrony

Marcin Jerzak

Zespół Bezpieczeństwa PCSS

O CZYM?

- Co jest robak, wirus, bot
- Ciekawe i sławne okazy
- Malware + rootkity
- Obrona
- Przegląd oprogramowania
- Zalecane środki ostrożności
- Podsumowanie

POZNAŃ SUPERCOMPUTING AND NETWORKING CENTER

Country	Price for 1k	
AU	300 $	Order now
GB	220 $	Order now
IT	$ 200	Order now
NZ	$ 200	Order now
ES	$ 200	Order now
DE	$ 200	Order now
NL	160 $	Order now
FR	150 $	Order now
BG	120 $	Order now
DK	110 $	Order now
PT	$ 100	Order now
US	$ 100	Order now
PL	80 $	Order now
CA	80 $	Order now
GR	80 $	Order now
SE	70 $	Order now
BR	70 $	Order now
TR	60 $	Order now
JP	$ 50	Order now
NO	$ 50	Order now
UA	40 $	Order now
RU	40 $	Order now
*	30 $	Order now

WIRUSY

- relikt przeszłości
- same się powielają
- wymagają nosiciela
- popularniejsze cechy:
  - *kasowanie i niszczenie danych*
  - *kasowanie MBR*
  - *niszczenie pamięci BIOS*
  - *pokazywanie napisów, odgrywanie dźwięków*
  - *utrudnianie pracy na komputerze*

Win95.CIH (Chernobyl)

- pierwotna wersja - atak: 26 kwietnia '99
- atakuje pliki .exe
- w systemach win 9x, ME
- kasuje MBR oraz próbuje nadpisać flashBIOS
- zajmuje ok. 1kb pamięci, ale pliki nie rosną po zarażeniu (Spacefiller)

ROBAKI

- rozsyłają się do wszystkich komputerów w sieci wykorzystując dziury w oprogramowaniu lub/i naiwność użytkowników
- nie wymagają nosiciela
- popularne cechy
  - *rozsyłanie spamu*
  - *kradzież danych*
  - *tylne furtki*
  - *kasowanie i niszczenie danych*

SASSER

- mini ftp (5554)
- reset (podobnie jak Blaster)
- luka: Remote Code Execution w LSASS (proces dot. polityki bezpieczeństwa, logowania)
- 128 nowych wątkow szukających systemów podatnych na atak
- atak DDOS na Islamic Republic News Agency (a następnie na BBC)
- twórca aresztowany (19-letni Sven Jaschan)
- luka w mini ftp: Dabber

MyDoom

- przełom – koniec ery
- infekuje przez otwieranie załącznika e-mail
- apogeum - co 3 e-mail w EU zarażony! (250mln USD strat)
- ataki DDOS na Microsoft i SCO
- twórca nieznany (pomimo wysokich nagród)
- koniec DDOS 12 lutego 2004
- DoomJuice

Nimda

- szczyt „popularności” osiągnął w 22min!
- przenoszony przez e-mail, www lub przez luki w systemach (MIME)
- autor nieznany
- infekuje pliki .exe
- powoduje DOS poprzez ciągłe skanowanie w poszukiwaniu luk w systemach

Rootkity

- ukrywanie procesów (Task Manager)
- ukrywanie wpisów w rejestrze
- Process Listers Crash
- dedykowany rootkit – w procesie systemowym
- Manipulacje Device/Physical Memory
- http://www.gmer.net
- http://www.sysinternals.com
- http://invisiblethings.org/tools.html

Elia Florio (Symantec) „When malware meets rootkits"

Name	Threat Category			Rootkit Characteristics				
	Worm /Virus	Backdoor /Trojan	Adware/ Spyware	DLL/IAT hooking	SDT/IDT hooking	DKOM	Use SYS driver	Use "Physical Memory"
Adware/Elitebar			X	X				
Adware/CommonName			X		X		X	
Spyware/Search			X		X		X	
Spyware/Elpowkeylogger			X		X		X	
Spyware/Apropos.C			X	X	X		X	
Backdoor/Graybird [a]		X			X		X	
Backdoor/Haxdoor [a]		X			X		X	
Backdoor/Darkmoon [a]		X			X		X	
Backdoor/Berbew [a]		X		X	X		X	
Backdoor/Ryejet [a]		X			X		X	
Trojan/Drivus		X			X		X	
PWSteal/Raidys		X			X		X	
W32/Spybot.NLX	X				X		X	
W32/Theals.A@mm	X			X				
W32/Tdiserv.A	X				X		X	
W32.Mytob.AR@mm					X		X	
W32.Loxbot.A@mm	X				X		X	
W32.Myfip.H@mm	X					X		X
W32.Fanbot.A@mm	X					X		X

Botnet

- Sieć komputerów ZOMBIE
- gigantyczna moc obliczeniowa (500 superkomputerów)
- zagrożenia:
  - **spam**
  - **pump-and-dump**
  - **phishing**
  - **klikanie**
  - **ataki DDOS**
  - **sniffing**

Virus Bulletin

- Avast (10/10)
- Cat QuickHeal (9/10)
- Nod32 (10/10)
- Sophos (10/10)
- Symantec (10/10)
- *Kaspersky (8/10)*

TopTenReviews

■■■■ Excellent
■■■□ Very Good
■■□□ Good
■□□□ Fair
□□□□ Poor

Rank	BitDefender	Kaspersky	ESET Nod32	PC-cillin	F-Secure Anti-Virus	McAfee VirusScan	Norton AntiVirus	AVG Anti-Virus Pro	CA Antivirus	Norman Virus Control
	GOLD	SILVER	BRONZE	4	5	6	7	8	9	10
Reviewer Comments	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW
Lowest Price	BUY $24.95	BUY $49.95	BUY $39.00	BUY $35.95	BUY $60.89	BUY $39.99	BUY $39.99	BUY $38.95	BUY $49.99	BUY $39.95
Overall Rating	■■■■	■■■■	■■■■□	■■■■□	■■■■□	■■■■□	■■■■□	■■■■□	■■■■□	■■■■□
Ratings										
Ease of Use	■■■■	■■■■	■■■□	■■■■	■■■■	■■■■	■■■■	■■■■□	■■■■	■■□□
Effectiveness	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■
Updates	■■■■	■■■■	■■■■□	■■■■□	■■■■□	■■■□	■■■□□	■■■■	■■■■	■■■■
Feature Set	■■■■	■■■■	■■■■	■■■■□	■■■■□	■■■■□	■■■■□	■■■■□	■■■□	■■■□
Ease of Installation	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■
Help/Support	■■■■	■■■■	■■■■	■■■□	■■■■	■■■□□	■■■■□	■■■■□	■■■■□	■■■■

Komputer Świat

1. Kaspersky Anti
2. Mks_vir
3. Norton AntiVirus
4. Panda Platinum Internet Security
5. AntiVirenKit
6. Panda Titanium Antivirus
7. BitDefender
8. NOD32

Clam AV

- dostępny na zasadzie Open Source
- intergracja z serwerami pocztowymi (skanowanie załączników)
- narzędzie do tworzenia sygnatur wirusów
- biblioteka do tworzenia własnych programów antywirusowych w oparciu o Clam AV
- narzędzie do aktualizacji bazy wirusów

Bezpieczny punkt wyjścia

- instalacja aktualizacji
- usunięcie zbędnych aplikacji i usług
- włączenie firewalla
- program antywirusowy
- minimalny poziom uprawnień
- konfiguracja programu pocztowego
- konfiguracja komunikatora
- testy programami do wykrywania luk

Zalecane dodatkowe ustawienia

- Plik HOSTS
  - /windows/system32/drivers/etc/
  - http://someonewhocares.org/hosts/
  - http://www.hosts-file.net
- Blocklist Manager
  - http://www.bluetack.co.uk
- HOSTS Manager
  - http://www.raymarron.com/hostess/

```
3 127.0.0.1 www.adtomi.com
4 127.0.0.1 www.baidu.com
5 127.0.0.1 localhost
```

e-mail

- filtr antyspamowy
- wyłączona aktywna zawartość HTML wiadomości
- przeglądanie poczty w formie tekstowej
- zablokowane niebezpieczne załączniki
- świadomość dotycząca ataków typu phishing (webmail)

Komunikatory

- instalacja aktualizacji
- wyłączone odbieranie plików (ew. pliki każdorazowo skanowane)
- blokowanie wiadomości od osób spoza listy kontaktów ew. nieotwieranie linków od nieznajomych
- ukrywanie swojego adresu IP
- szyfrowanie połączenia

Łańcuszki

- *„Skopiuj mnie do wszystkich znajomych!”*
- http://atrapa.net/chains/
- SPAM
- wirus albański:

„Drogi Odbiorco!

Jestem albańskim wirusem komputerowym, ale z uwagi na słabe zaawansowanie informatyczne mojego kraju nie mogę nic Ci zrobić.
Proszę skasuj sobie jakiś plik i prześlij mnie dalej”

Przeglądarki i P2P

- Przeglądarki:
  - Instalacja aktualizacji
  - instalacja *noscript* i *netcraft toolbar (FF)*
  - unikanie podejrzanych stron
  - http://bcheck.scanit.be/bcheck - skaner on-line
- Aplikacje P2P:
  - możliwie mocne ograniczenie albo zaprzestanie korzystania

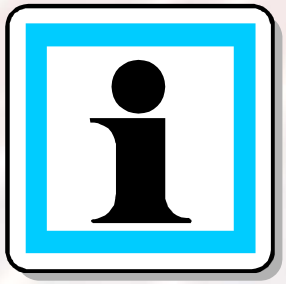
Gdy jest już za późno

- zapisać ważne dane
- wyłączyć komputer
- odłączyć od internetu
- uruchomić z CD/USB/FDD stworzonej podczas instalacji programu antywirusowego
- Spybot Search & Destroy
- HijackThis
  - http://www.forumpc.pl
  - http://www.bleepingcomputer.com/tutorials/tutorial42.html

Podsumowanie

- Świadomość zagrożenia
- Bezpieczny punkt wyjścia
- Aktualizacje
- Kopie zapasowe

Pytania



Dziękujemy za uwagę!