

# Dlaczego i po co walczymy ze spamem ?

Ireneusz Parafjańczuk

CERT Polska  
NASK

- **Co to jest spam...?**
  - **Historia spamu**
  - **Szkodliwość**
  - **O co jeszcze w tym chodzi...?**
  - **Zombie i botnet**
  - **odpowiedź na pytanie**
- 
- ***Definicje z nospam-pl***

**Co to jest spam...?**

**SPAM to:**



- 66 lat historii – inaczej... 4.752 puszki z całego świata
- SPAM to nazwa mielonki ("SPiced HAm luncheon meat") produkowanej przez firmę Hormel Foods
- nazwa SPAM jest zarejestrowanym znakiem towarowym !!!



**spam to:**

- mielonka wieprzowa, racja C - podstawa wyżywienia polowego wojsk USA w czasie II wojny światowej
- zniechęcona !
- w latach 60-tych w Wlk. Brytanii a potem w USA młodzieżowe określenie na niechcianą, rozsyłaną automatycznie pocztą tradycyjną
- punkt zwrotny – skecz Flying Circus Monty Pythona ;)



## Spam to:

- Elektroniczne wiadomości rozsyłane do osób, które ich nie oczekują.
- Najbardziej rozpowszechniony za pośrednictwem poczty elektronicznej oraz w Usenecie.
- Zwykle – choć nie zawsze – wysyłany masowo.

Junk E-mail			
Od	Temat	Otrzymano	Rozmiar
Stanley Small wood	Peerless prestige	N 2006-03-12 23:37	8 KB
Augustus Madrid	Best Pharmacy Today m2s	N 2006-03-12 22:53	5 KB
Stella Shields	Your doc thinks you`re millionaire? morristown	N 2006-03-12 22:48	6 KB
Gilbert	Our store is your cureall!	N 2006-03-12 22:16	15 KB
Alexander Goldberg	Wd cure any disease? Cheap Meds !	N 2006-03-12 21:58	24 KB
Alexander Goldberg	Cheap Meds !	N 2006-03-12 21:50	6 KB
Adam Hughes	What IS OEM Software And Why DO You Care?	N 2006-03-12 21:48	16 KB
trino_mikijump11@yahoo.c...	[CERT.PL #26856] 【緊急】ご確認ください。	N 2006-03-12 21:13	11 KB
Alexander	Men Health	N 2006-03-12 21:09	24 KB
John	Need medicine? All here!	N 2006-03-12 20:36	15 KB
Open Finance	Co z tanim kredytem mieszkaniowym w CHF?	N 2006-03-12 20:04	21 KB
Open Finance	Co z tanim kredytem mieszkaniowym w CHF?	N 2006-03-12 20:04	21 KB
Open Finance	Co z tanim kredytem mieszkaniowym w CHF?	N 2006-03-12 20:04	21 KB
William	All love enhancers on one portal!	N 2006-03-12 19:53	15 KB
Simon	Why seek? Choose any love pi 1 you want!	N 2006-03-12 19:47	15 KB
Reginald	Our store is your cureall!	N 2006-03-12 19:45	15 KB
Geoffrey	Need medicine? All here!	N 2006-03-12 19:32	15 KB
Gelbman	Advantages of online pharmacies!	N 2006-03-12 19:17	6 KB
Fernando Landis via RT	[CERT.PL #26850] Fuller & Harder Erections	N 2006-03-12 18:29	6 KB
John	* Generic Viagra bestseller *	N 2006-03-12 18:19	24 KB
Thomas	Our store is your cureall!	N 2006-03-12 18:18	15 KB
Philip	Any med for your girl to be happy!	N 2006-03-12 18:18	15 KB
urbeno	Become happy with ur thing	N 2006-03-12 18:15	8 KB
Hollis Flores	You Gonna Love This Zgu	N 2006-03-12 17:26	4 KB
Timothy	Hey my new {watch:replica} site	N 2006-03-12 16:48	5 KB
Geoffrey	Men Health	N 2006-03-12 16:39	24 KB
William	Medicines for real men !!!	N 2006-03-12 16:31	24 KB
Gilbert	* Propecia Maxaman Flomax *	N 2006-03-12 16:21	24 KB
June Jeffries	Fuller & Harder Erections	N 2006-03-12 16:10	6 KB
Bryce Flores via RT	[CERT.PL #26848] Last offer- Discount special for PE patch almost over!	N 2006-03-12 16:08	10 KB

**By wiadomość określić mianem spamu musi ona spełnić trzy następujące warunki jednocześnie:**

- treść wiadomości jest niezależna od tożsamości odbiorcy;
- odbiorca nie wyraził uprzedniej, zamierzonej zgody na otrzymanie tej wiadomości;
- treść wiadomości daje podstawę do przypuszczeń, iż nadawca wskutek jej wysłania może odnieść zyski nieproporcjonalne w stosunku do korzyści odbiorcy.

## spam dzieli się na dwie kategorie:

- tzw. Unsolicited Commercial Email (UCE), czyli spam komercyjny o charakterze reklamowym, zakazany przez prawo tak polskie jak i dyrektywę UE.
- tzw. Unsolicited Bulk Email (UBE), czyli maile o charakterze często niekomercyjnym, takie jak apele organizacji społecznych i charytatywnych, czy partii politycznych prośby o pomoc czy masowe rozsyłanie ostrzeżeń np. o wirusach komputerowych.
  - Próby wprowadzenia zakazu w dyrektywie UE rozsyłania e maili o charakterze społeczno-politycznym zostały w 2002 r. odrzucone przez Parlament Europejski wobec protestów europejskich partii politycznych i organizacji społecznych.

# Historia spamu...

---

### Pierwsze spamy:

- "Prekursor" spamu jest starszy od Internetu ~ 1971rok – ARPANET – 23 hosty !!!
- Za pomocą programu CTSS MAIL Peter Bos przesłał w sieci akademickiej MIT długą, antywojenną wiadomość do wszystkich użytkowników systemu CTSS.
- Pierwszy „internetowy” powstał też w ARPANET – 1 V 1978
- Einar Stefferud, moderator listy MsgGroup - pierwszej listy mailowej w ARPAnecie. Rozesłał on do około 1000 subskrybentów listy żartobliwe zaproszenie na swoje urodziny.
- odpowiedzi zablokowały dyski twarde jego serwera...

### Pierwsze spamy cd:

- Inne źródła – pierwszy spam komercyjny - napisany 1.V.1978 r. przez Gary Thuerk,
- wysłany 3 maja 1978.
- reklama producenta mini-komputerów, firmy Digital Equipment Corp., zapraszająca wszystkich użytkowników ARPAnetu z Zachodniego Wybrzeża USA na "dzień otwarty" - prezentację najnowszych produktów firmy.
- ostre kontrowersje – znaczne spowolnienie sieci

### Pierwszy spamer... ?

- Pierwszy spamer - Richard Depew
- W 1993 roku próbował napisać skrypt, który automatycznie usuwał z grup newsowych posty niezgodne z netykietą danej grupy.
- Skrypt wymknął się spod kontroli i zamiast kasować wysłał ciąg 200 postów na grupę news.admin.policy.
- Wiele z osób czytających tę grupę było też zapalonymi graczami w MUD-y i zastosowali oni znane z mudów pojęcie spamer do Richarda.

### **MUD (Multi-User Dungeon):**

- Akronim oznaczający gry komputerowe RPG, rozgrywane przez Internet przy użyciu interfejsu tekstowego.
- Tzw. świat, czyli scenariusz gry i definicje postaci użytkowników, jest umieszczony na serwerze, do którego może być podłączonych wiele osób w tym samym czasie.
- Po połączeniu gracz steruje swoją postacią przy pomocy zestawu komend i opcji umożliwiających m.in. decydowanie, w którą stronę postać ma "pójść" lub jaką akcję podjąć.
- Od początku teren wzajemnej walki i współzawodnictwa – pierwsze „wiadomości” zawierające cytaty z Monty’ego – „SPAM, SPAM, lovely SPAM, wonderful SPAM”

# Szkodliwość ...

---

- Powoduje zatykanie się łącz i blokuje miejsce na twardej dyskach.
  - Przetworzenie spamu zabiera czas serwerom spowalniając ich działanie.
  - Powoduje stratę czasu poszczególnych użytkowników Internetu - muszą oni czytać i kasować niepotrzebne wiadomości. Utrudnia czytanie "normalnej" poczty i stwarza ryzyko jej utraty np. przepełnienie skrzynki) lub niezauważenia (z powodu "przysypania" przychodzącym spamem). Zwiększa koszty pracy osób zawodowo korzystających z poczty elektronicznej.
- Przykład...

### Przykład:

medyczo-farmaceutyczne	80
finansowe	31
nie znane - krzaczk... :)	9
oprogramowanie - piractwo	15
pornografia dziecięca	1
<u>w tym - malware</u>	<u>54</u>

- w ostatnią sobotę i niedzielę otrzymałem 136 maili ze spamem

SUMA		sr. Dziennie	sr. Mies.	sr.roczenie	
136	szt.	68	2040	24820	szt.
1878016	bajtów	939008	2817024	342737920	Bajtow
1,79	MB	0,90	26,87	326,86	Mega Bajtow
<hr/>					
			300 pracownikow =	95,76	Giga Bajtów rocznie
				7 446 000	szt.
<hr/>					
każdy pracownik	6,5	minut dziennie na spam		4,06	dni w roku firma pracuje nad spamem

**4 dni w roku firma pracuje nad spamem**

**!!!**

### **Koszty (według Radicati Group):**

- W roku 2003 szacowano, że koszty gospodarki światowej związane ze spamem wyniosły 20 mld USD
- W roku 2004 – już 41 mld USD
- Rok 2005 ... na razie brak danych...
- do roku 2007 mają wynieść... 198 mld USD

- Naraża operatorów internetowych i użytkowników na dodatkowe koszty ponoszone na przeciwdziałanie pladze. Spam jest również metodą przerzucenia kosztów promocji na operatorów internetowych i odbiorców korespondencji - a zatem jest formą wyłudzenia.
- Narusza prywatność i bezpieczeństwo odbiorców, ponieważ często zawiera treści, których nie życzyliby sobie oglądać - np. obraźliwe, pornograficzne, nieodpowiednie dla dzieci. Spam wiąże się często z różnego rodzaju wirusami i innymi złośliwymi programami.
- Bezpośrednie niebezpieczeństwo – kradzież tożsamości i/lub pieniędzy
- Powoduje utratę zaufania do komunikacji elektronicznej jako takiej.

**O co jeszcze w tym chodzi ...**

## O technikę:

- Początkowo spam rozsyłany był za pośrednictwem tzw. proxy – serwerów pocztowych umożliwiających wysyłanie poczty e-mail od każdego do każdego – bez autoryzacji...
- walka ze zjawiskiem polegała na „zamykaniu” albo tworzeniu tzw. „czarnych list” do użycia przy blokowaniu jako nadawców
- Kłopoty serwisów tworzących takie listy – OpenRBL, SpamCop, PolSpam...
- Nowe „technologie” i sposoby rozsyłania - Botnety...

**Co to jest botnet ... ?**

## Botnet to:

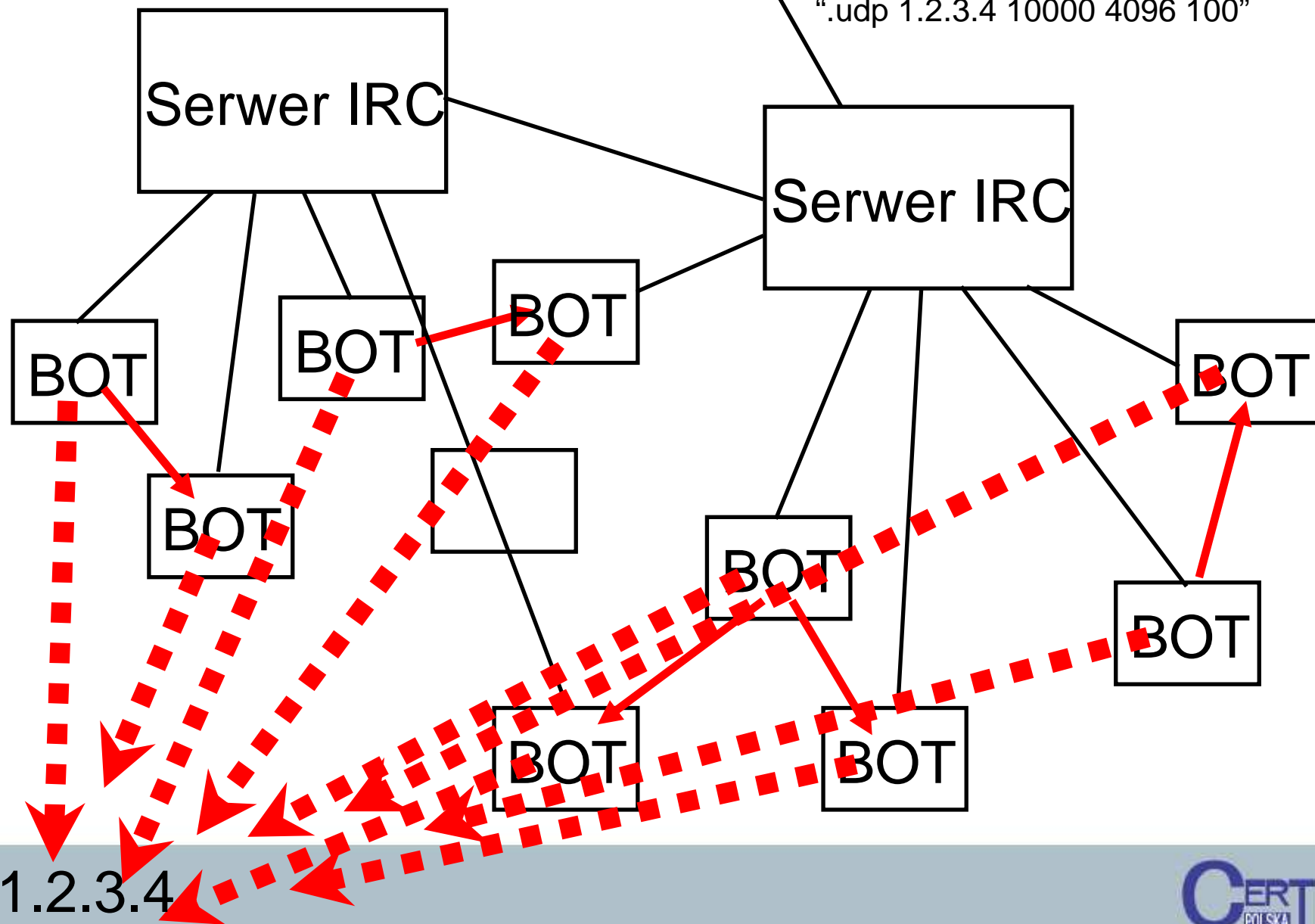
- Sieć zawirusowanych komputerów raportujących/posłusznych twórcy wirusa (konia trojańskiego) i zarządzanych w czasie rzeczywistym za pośrednictwem Serwera Kontrolującego
- Przejęte/zawirusowane komputery nazywamy Zombie – gdyż tak się zachowują
- Istnieją od kilku lat – niebezpieczne i opłacalne dla twórców
- A jest ich kilka/kilkaset milionów

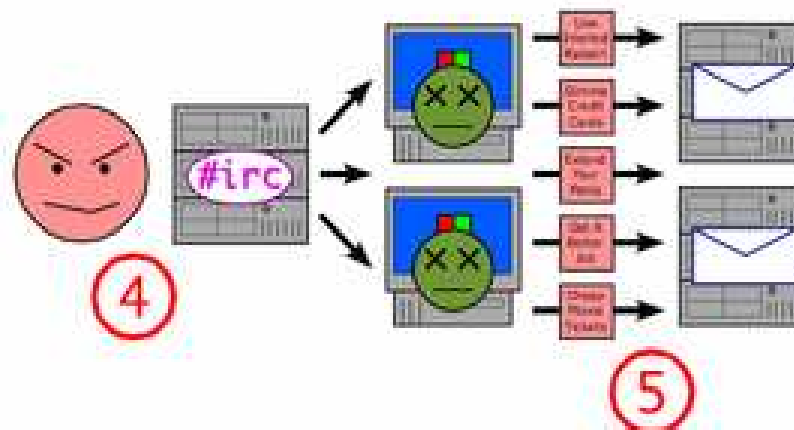
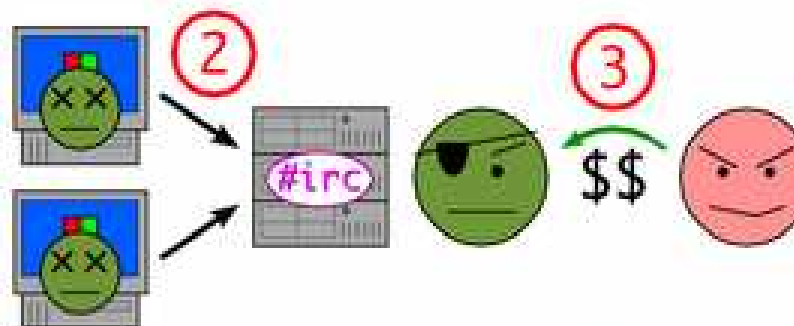
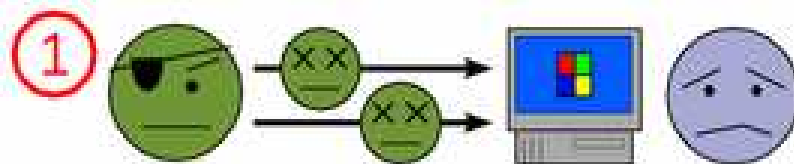
# **Jak działa botnet ... ?**

---

przestępca

“.udp 1.2.3.4 10000 4096 100”





1. Twórca wirusa rozsyła go zarażając „zwykłych” użytkowników komputerów – przeważnie SO Windows.
2. Zarażone komputery łączą się z serwerem IRC (lub innym kanałem komunikacyjnym) tworząc sieć zarażonych i przejętych komputerów zwanych botnet.
3. Spamer kupuje dostęp do takiego botnetu albo bezpośrednio od jego twórcy albo przez pośrednika.
4. Spamer wysyła instrukcje do botnetu nakazujące zarażonym komputerom rozsyłanie spamu.
5. Zarażone komputery wysyłają wiadomości ze spamem do użytkowników internetowych serwerów mailowych.

## Jak wykorzystywany jest botnet:

- podsłuch właściciela, kradzież numerów kart kredytowych, wykorzystywanie dysków twardych do przechowywania danych – piractwo, kradzież tożsamości
- atakowanie innych – DDoS, phishing, pharming
- spam
- główny cel – zarabianie pieniędzy !!!

- Dochody cyber - kryminalistów wg szacunków Departamentu Skarbu US wyniosły ok. 150 mld USD przekraczając dochody z handlu narkotykami

# Po co walczymy ze spamem ... ?

- niezgodny z prawem w coraz większej ilości krajów
- wysoce szkodliwy
- po nitce do kłębka
  - namierzenie spamerów
  - namierzenie botnetów
  - namierzenie twórców botnetów
  - namierzenie twórców wirusów
  - likwidacja patologii niszczącej internet
- konieczna ścisła i szybka współpraca międzynarodowa !!!
- więcej o projekcie – za chwilę

## **CERT POLSKA**

zgłaszanie incydentów: [cert@cert.pl](mailto:cert@cert.pl)

strona internetowa: [www.cert.pl](http://www.cert.pl)

tel. +48 22 380 82 74

fax +48 22 380 83 99

adres pocztowy:

NASK - CERT Polska

ul. Wąwozowa 18

02-786 Warszawa

Polska

# DZIĘKUJEMY ZA UWAGĘ