Dlaczego z 80% przedsiębiorstw wyciekają poufne informacje i jak temu zaradzić - produkty Clearswift

Grzegorz Blinowski
G.Blinowski@cc.com.pl

CC Otwarte systemy Komputerowe Sp. z o.o.

Agenda

- Klasyfikacja zagrożeń:
  - Malware, Wirusy,
  - Worm-y, Trojan-y, RAT-y,
  - Spyware, Cyberwoozle, FUI, ...
  - Phishing,
  - Spam,
- Spam, Wirusy, Trojany, Spyware - Aktualne “trendy”
- Zagrożenia dla firm i instytucji – naruszenie bezpieczeństwa infrastruktury, szpiegostwo przemysłowe,
- Jak się bronić?
- O firmie Clearswift
- Przegląd produktów Clearswift

Źródła zagrożeń

- Główne źródła zagrożeń w IT:
  - **Fizyczne** (dostęp do pomieszczeń, serwerów i stacji roboczych oraz notebooków, nośników danych, kabli, itp.)
  - **Sieciowe** (warstwy 3,4) - kontrola i ograniczenie ruchu sieciowego na styku z internetem, a także wewnątrz organizacji
  - **Aplikacyjne** - WWW, E-mail, IM (Instant Messaging)
- Obecnie (2000 - ….) kwestie likwidacji zagrożeń na poziomie aplikacji są zarówno najbardziej palące jak i najtrudniejsze w realizacji

Klasyfikacja zagrożeń

- **Wirus** - *program komputerowy zdolny do samo-kopiowania, wymagający programu - nosiciela, dzięki któremu może funkcjonować i mnożyć się. Może, ale nie musi, posiadać wbudowanych funkcj złośliwych, nie jest zdolny do samodzielnego funkcjonowania*
- **Worm** - *program komputerowy zdolny do samo-kopiowania,* ***nie*** *wymagający programu-nosiciela, przenosi się przez sieć komputerową wykorzystując najczęściej systemowe mechanizmu transferu danych.*
- **Trojan** - *program komputerowy maskujący się jako nieszkodliwa aplikacja lub całkowicie ukrywający swoje istnienie, z założenia pełni funkcje destrukcyjne lub szpiegowskie*

Klasyfikacja zagrożeń

- Współczesne "wirusy" (w tym te najbardziej znane i najbardziej destrukcyjne) to twory hybrydowe będące kombinacją klasycznego wirusa i worma, a także coraz częściej trojan-a

- **RAT** - *Remote Access Trojan - Trojan posiadający funkcje zdalnego dostępu - atakujacy może przejąć kontrolę nad zarażoną maszyną*

- **FUI -** *Fake User Interface - oprogramowanie, którego interfejs użytkownika ukrywa rzeczywiste funkcje i przeznaczenie.*

- **Malware** ("złe oprogramowanie") - *dowolne oprogramowanie (wirus, worm, trojan) mające na celu zdestabilizowanie pracy systemu, zniszczenie lub kradzież danych*

Klasyfikacja zagrożeń

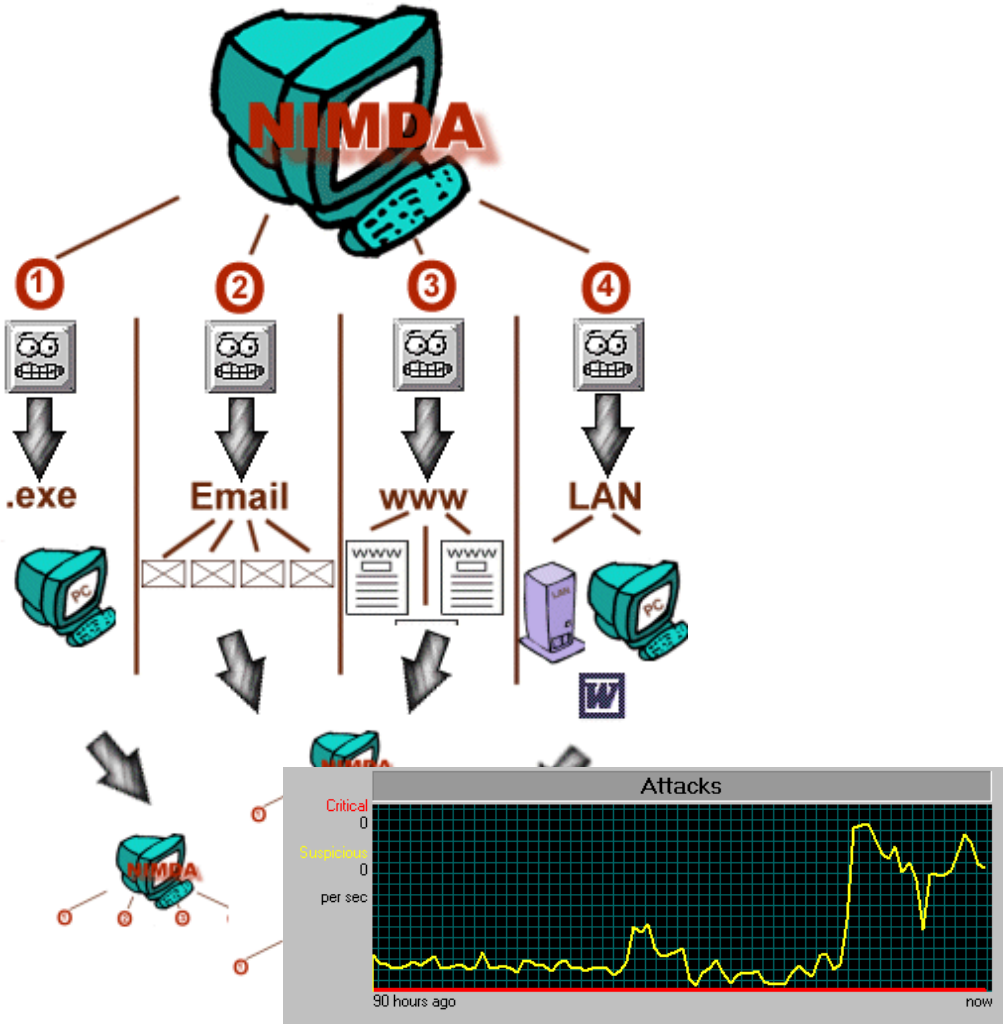
- **Spyware** - *dowolne oprogramowanie działające bez zgody (i wiedzy) użytkownika gromadzące i przesyłające siecią informacje o nim.*

- **Keylogger** - *oprogramowanie typu spyware (lub część składowa większego pakietu spyware) gromadzące informacje o znakach wpisanych z klawiatury*

- **Dialer** - *oprogramowanie przejmujące kontrolę nad połączeniem internetowym typu dial-up. Bez wiedzy użytkownika łączy komputer z internetem za pośrednictwem numerów typu 0-700 lub międzynarodowych.*

Przykład - Worm-y: Nimda

- **Klasyczny przykład robaka hubrydowego Nimda:**
- "4 wirusy w jednym"
- wektor - e-mail
- atakuje dostępne dyski sieciowe, udostepnia publicznie dysk C:
- atakuje serwer WWW Microsoft (IIS)
- Dokleja się do plików na lokalnym i zdalnych dyskach



Przykład - Wormy: Netsky, Bagle

- W32/Netsky-A […-AC] (wiele wariantów)
  - Rozprzestrzenia się przez e-mail
  - Zbiera adresy z wielu różnych plików znalezionych na dysku
  - Ma własny engine SMTP (sam wysyła maile, nie ko
    lokalnego API pocztowego
  - Usuwa niektóre programy AV
  - Nie rozsyła się do adresów "związanych" z firmami
  - Próbuje usuwać Blaster-a
  - Wariant -P - wystarczy przeczytać e-mail
  - Wariant Q - wbudowane mechanizmy DDoS
- W32/Bagle-A […-AA] (wiele wariantów)
  - Podobny do Netsky
  - niektóre warianty zatrzymują oprogramow
  - niektóre warianty instalują trojana
- Autorzy Netsky i Bagle "współzawodniczy
  wirusów

Sven Jaschan) 18 l - Autor Netsky i Sasser - odpowiada za 70% infekcji wirusowych w 2004 r.

Trojan-y - Sobig: Worm i Trojan:

- Infekcja poprzez e-mail, program zaszyfrowany (packer Telock 0.98)
- Po zainfekowaniu maszyny worm:
  - ładuje swój właściwy kod z internetu (stosowane są techniki mające na celu ukrycie faktycznego adresu
  - powiadamia (autora?) o fakcie infekcji poprzez URL: http://www.banking-concern.com/cgi-bin/index7.cgi
  - ładuje i instaluje:
    - keylogera
    - RAT "Lithium" (wchodzi też w skład W32.Blaster.C)
    - Proxy Wingate dla następujących serwisów (na nietypowych portach): www, telnet, smtp, ftp, pop3, …) - haker może wykorzystywać zainfekowane maszyny do zacierania swoich śladów
  - worm kasuje swój kod z maszyny (pozostawiając backdory)

Spyware

- Geneza - połowa lat 90-tych, początek bańki Internetowej -
  - producenci oprogramowania i dostawcy usług zdają sobie sprawę, że w dłuższej perspektywie nie mogą rozdawać produktów za darmo
  - ceną może być dostarczenie do użytkownika reklamy i/lub informacja o użytkowniku: im więcej, tym lepiej
- Wyewoluowały 2 rodzaje spyware-u:
  - **łagodny** - uciążliwy, czasami destrukcyjny (błędy oprogramowania), ale w istocie nieszkodliwy
  - **agresywny** - celem jest kradzież danych - od kradzieży tożsamości po szpiegostwo przemysłowe

Spyware

- Spyware jest w pewnym sensie wirusem -
  - Dołączany jest do wszelkiego rodzaju oprogramowania: freeware, shareware, komercyjnego (zwłaszcza wersji demo), e-mailach, itd.
  - Różnica - "infekcja" zazwyczaj nie jest "złośliwa"
  - Podobieństwo - użytkownik zazwyczaj nie zdaje sobie sprawy z obecności spyware, choć dość często informacja o nim jest zawarta w EULA (którego przed instalacją nikt z reguły nie czyta)
  - Podobieństwo - jest trudny do usunięcia, stosowane są klasyczne techniki znane twórcom wirusów - po usunięciu spyware-u program ponownie się instaluje, lub program macierzysty przestaje działać

CC Otwarte Systemy Komputerowe Sp. z o.o.

Adware -"łagodny" Spyware

- "Bezmyślne" pokazywanie reklam (banerów) jest mało skuteczne
- Skuteczniejsze jest dostarczanie takich banerów, które mają szansę zainteresować użytkownika
- Do tego potrzebne nam są dość szczegółowe dane o użytkowniku
- Klasyczne nośniki lagodnego spyware to programy / klienci sieci P2P (Kazaa, Grokser i inne)

Spyware - adware

Gator Advertising and Information Network,

Privacy Policy Statement

http://www.gator.com/help/app_privacy_latest.html

"Here's what we do know (about our users) . . .While we don't know the identity of GAINSupported Software users, the GAIN AdServer and TGC collect and use the following information:

- *Some of the Web pages viewed*
- *The amount of time spent at some Web sites*
- *Response to GAIN Ads*
- *Standard web log information (excluding IP Addresses)*
- *What software is on the personal computer*
- *First name, country, city, and five digit ZIP code*
- *Non-personally identifiable information on*
- *Web pages and forms Software usage characteristics and preferences"*

Spyware - adware

- Dlaczego "łagodny" spyware jest jednak groźny?
  - Automatyczne updaty spyware-u mogą prowadzić do otwarcia "dziur" w systemie, przez które nastąpić może infekcja innego typu
  - Spyware dość często obniża poziom bezpieczeństwa przeglądarki IE (pozwolenie wykonywania dowolnych skryptów, traktowanie wszystkich stron jak lokalnych) - podatność na ataki "drive-by"
  - Zapisywanie i przesyłanie adresów sieciowych odwiedzanych serwisów: URL-e mogą zawierać hasła i nazwę użytkownika
  - "Zatykanie sieci" - zwłaszcza w przypadku gdy spyware nie może skontaktować się z macierzystym serwerem

Agresywny spyware

- "Surveliance Spyware" - spyware szpiegowski
- Zakres monitorowania jest znacznie szerszy niż w Adware
- Stosowane są techniki "stealth" zabezpieczające spyware przed wykryciem i dezaktywacją
- Kategorie:
  - Nadzór rodzicielski, itp.
  - Zdalna kamera, mikrofon
  - Narzędzia hakerskie
  - Legalne oprogramowanie komercyjne
  - "Szary obszar" pomiędzy …
- … Wszystko zależy od faktycznego zastosowania, nie od przeznaczenia

Agresywny spyware

- Infekcja:
  - Email / IM (Worm)
  - Sekretna instalacja (np. poprzez e-mail)
  - FUI - fałszywy komunikat o błędzie skłania użytkowników do instalacji niepotrzebnego oprogramowania - (sprawa Bonzi Software)
- Funkcje:
  - keyloger, backdoor / trojan
  - przejęcie kontroli na kamerą/mikrofonem, faksmodemem
  - logowanie odwiedzanych url-i i ściąganych plików
  - logowanie sesji chat/IM
  - zrzuty ekranu
  - automatyczne łączenie z internetem
  - wysyłanie informacji poprzez e-mail
  - zmiany konfiguracji przeglądarki / klienta poczty
  - autoupdate

Agresywny spyware

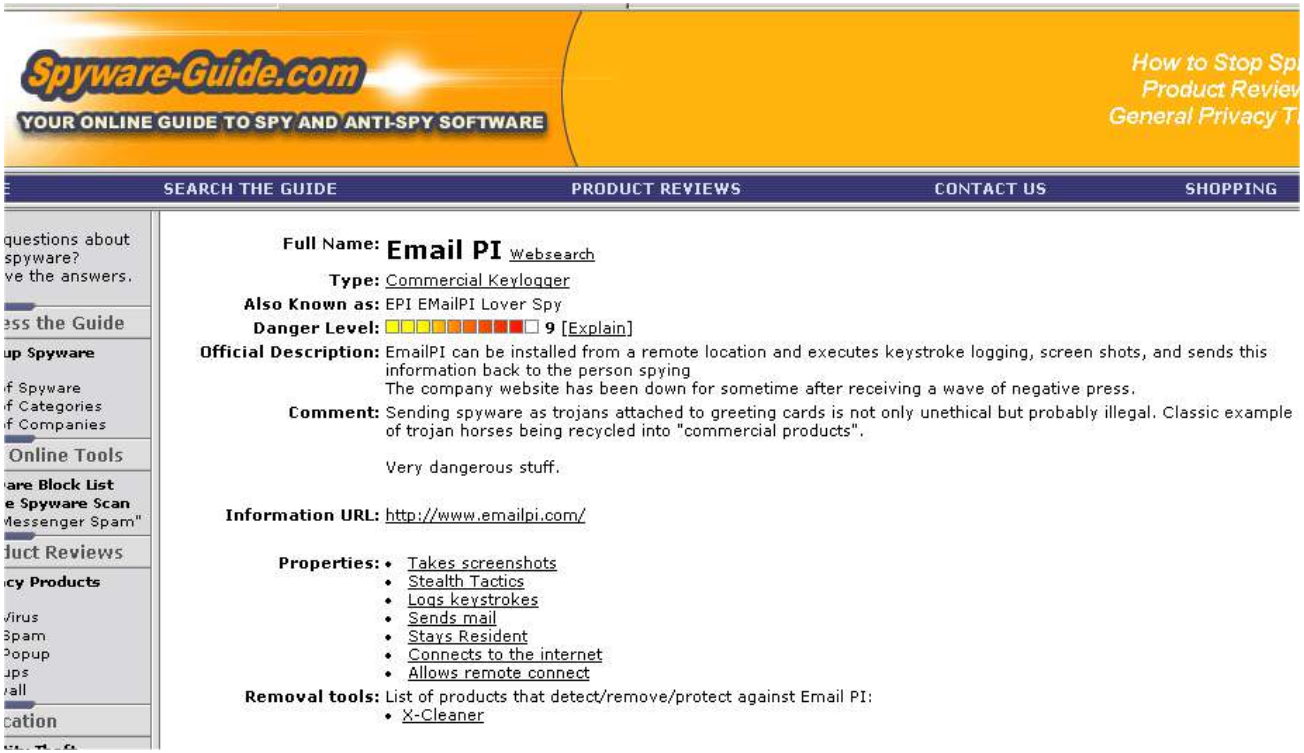
Agresywny spyware

- Najbardziej znane przykłady ataku poprzez spyware:
  - X / 2003 - Valve Software - producent gier - kradzież, a następnie publikacja w internecie kodu źródłowego gry "Half Life 2", technika: włamanie poprzez dziurę w Outlooku, instalacja keylogera, zdobycie haseł (firmy produkujące gry mają z reguły b. dobre zabezpieczenia)

    `http://www.wired.com/news/games/0,2101,60701,00.html`
  - "The Beast", VI 2003, program służący do analizy kursów akcji, rozpowszechniany poprzez fora dyskusyjne, zawiera trojana, autor oprogramowania przeprowadza transakcje na cudzych rachunkach inwestycyjnych
  - Kinko fraud, 2001 - 2003 - haker instaluje keylogera w 13 kawiarenkach internetowych na Manhatanie, przejmuje 450 różnego rodzaju kont w ciągu 2 lat(!), część uzyskanych danych sprzedaje, cześć wykorzystuje do przelania pieniędzy na własne konta

Spyware

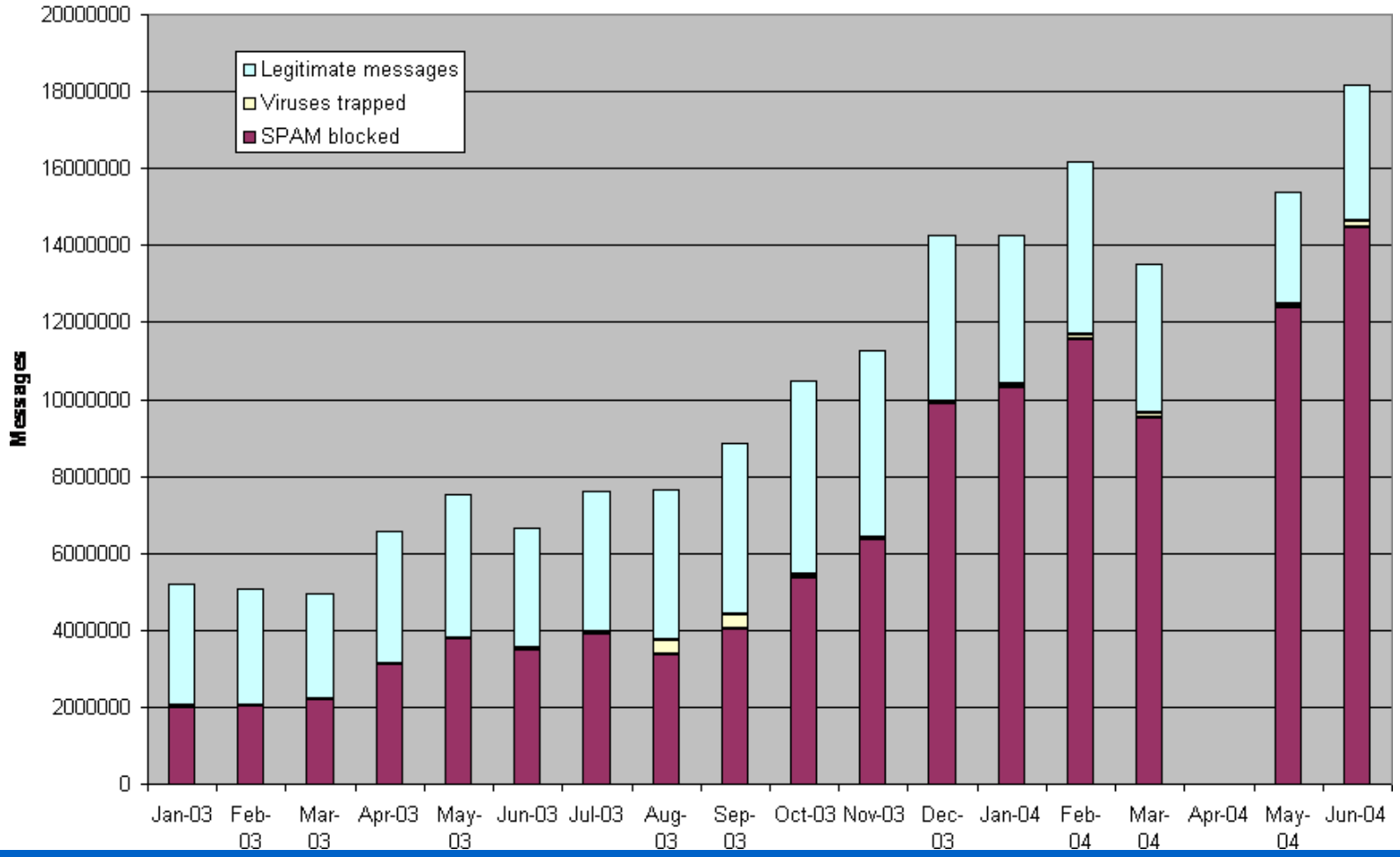
- Serwis Spyware-Guide.com podaje [20/08/2004]:
  - 444 programy typu spyware
  - 31 firm produkujących spyware (jednak wiele pakietów jest autorstwa indywidualnych osób)

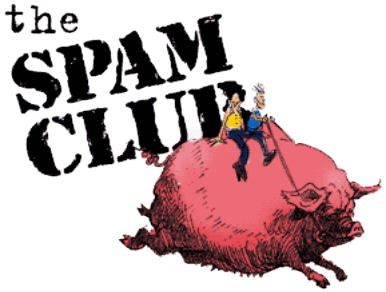


SPAM

- Badania podają, że obecnie ok. 80% całej korespondencji e-mailowej stanowi spam
- Zagrożenia związane z dystrybucją spam-u:
  - zagrożenia dla infrastruktury:
    - SPAM połączony z malwarem (wirusy, trojany, robaki, …)
    - zajmowanie pasma i zasobów
  - zagrożenia dla prowadzenia biznesu:
    - utrata produktywności
    - wyciek poufnych informacji
    - narażenie na odpowiedzialność prawną
- "Nowości" z dziedziny spamowania:
  - odejście od tradycyjnych “reklamowanych” treści – (serwisów pornograficznych, wirtualnych kasyn, łańcuszków szczęścia)
  - trendy: phishing i inne oszustwa finansowe (np. próby manipulowania kursami akcji)

SPAM - przykładowe statystyki





CC Otwarte Systemy Komputerowe Sp. z o.o.

Spam

- SPAM powiązany jest z innymi zagrożeniami:
  - Dystrybucja spamu coraz częściej odbywa się poprzez komputery zarażone trojanem (z zainstalowany proxy SMTP)
  - Inne zastosowanie zainfekowanych komputerów: duży rozproszony hakerski serwis DNS skutecznie ukrywa tożsamość nadawcy przesyłki
  - Ostatnie badania wskazują, że środowisko spamerów niebezpiecznie dąży w kierunku grup przestępczych

Anatomia SPAM-u

```
From - Mon Aug 9 13:34:39 2004
Return-Path: <allusiaa@virginia.edu>
From: <allusiov@virginia.edu>
To: <grzegorz.blinowski@cc.com.pl>
Subject: Buy V|agra through us, 70% OFF!          dys
Date: Mon, 9 Aug 2004 13:32:55 -0500
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Sender: allusiaa@virginia.edu

Best V|agra in the world at amazing prices!
We deliver express and discreet.
http://fxvy.hereviagra.com/ln/verycheap.php

No further announcements?
yxs.hereviagra.com/hot/out/

eklras
```

Anatomia SPAM-u

```
From: "Roslyn" <wlplc@cnnb.net>
To: "Cc" <cc@cc.com.pl>
Subject: Re: it on the chair
Date: Sun, 22 Aug 2004 15:21:51 -0600
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<HTML><BODY>
<P>cantqjt - qtwiod, pwapbpydc beguaqz, ikoqbdfd uwleildty, akohzc
   Pfqlmfo=
k=20gqhygv</P>
<P>llglvg, bafjzepk ywekf vazddnbua pphrf=20ajlrlaard</P>
<A
HREF=3D"http://www.jokmenao.info/">
<IMG SRC=3D"http://www.jokmenao.info/=
im/4.gif" BORDER=3D"0"></A>
<BR><BR><BR><P>qcvgyl yjvcpwbso Rofjilv tcglccnkn, wdqqroo jcqpbhfv,
   rjbsl=
jo=20rzkxol</P>
```

Anatomia SPAM-u

Hello,

We all want to wear SWISS WATCHS, they are expensive-we all know that, Now we have effordable Replica's--

Rolex

----------from $99 !!

also available :

==========

CARTIER, OMEGA, PATEK PHILIPE

==========

AND MORE: http://finestwatches.info/index.php?ref=hp

javelin cumulus glib sea bryan inverness reparation clockwork winemaster elegiac coypu eng anything bmw autocrat barefoot engage diopter seton diction crewman bloomington correct cuisine then greenfield despise hold ounce chopin kansas parisian traversable inhabit sup brainstorm adjudicate chemotherapy grata tau koppers dysplasia remembrance check penrose pontiff corey macdonald urine curran navajo

Phishing

- Połączenie klasycznych technik spamerskich i inżynierii społecznej
- Rozsyłane są e-maile mające skłonić użytkownika do podania numeru i PIN-u karty kredytowej lub informacji umożliwiającej dostęp do usług typu elektronicznej bankowości
- **Jak uzyskać 100 x (10 000%) "zysk z inwestycji" - Policzmy**:
  - wysyłamy 1 000 000 wiadomości: "drogi użytkowniku serwisu bankowego eBank S.A., w trosce o twoje bezpieczeństwo, ..."
  - koszt wysłania 1 000 000 wiadomości: 100 zł
  - 2% - 20 000 - trafi na faktycznych użytkowników serwisu
  - 0,5 % da się nabrać - uzyskaliśmy dostęp do kont 100 osób
  - z każdego konta pobieramy 100,- zł (większość właścicieli zapewne nie zauważy operacji)
  - zarabiamy: 10 000,- zł
- Klasyczny przykład: "***CitiBank scam***"

CitiBank Scam

Subject: Citibank regular verification of the accounts. [Tue, 29 Jun 2004 12:
From: Citibank <users-support23@citibank.com>
Date
To

citi

Dear client

As the T
We kindly
your acces

https://web

We are gra

Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit

<html> <A HREF="https://web.da-us.citi
<map name="FPMap0"><area coords="0, 0, 610, 275" shape
href="http://%31%34%38%2E%32%34%34%2E%39%33%2E
</map><img SRC="cid:part1.00000008.01050603@user-supp
</A> <font color="#FFFFF0">Will do it Tat

----------=_00080606020909020007 0002
Content-Type: image/gif;
name="substitutionary.GIF"
Content-Transfer-Encoding: base64
Content-ID: <part1.00000008.01050603@user-supports23@c
Content-Disposition: inline;

R0lGODlhaQIUAfTOAAECAAAAgMDAwMDcwKbK8AAAQOA
wOCgwKDAwP/78P8AAAAA/////wAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACH5BAQAAAAALAAA
AABiAhMBAAX/YCWOZGmeowQ1S2u0bSOhdG3feK7vfO//wKBwSCwaj8ikcslsHiULw2RKrU5eEKd2y+16
v+CweEwum2tQq1ptyJ7f8Lh8Tq/b73CVdC3drxczeIKDhIWGh4iJO2IWBg0QgSIqUY1uipeYmZqbnJ0oa

Citibank customers details confirmation - Microsoft Internet Explorer provide...

please confirm

ATM/Debit Card (CIN)

Checking account linked to your ATM/Debit Card (if you have)

PIN

Saving account linked to your ATM/Debit Card (if you have)

User ID* (if you have)

First and Last Name

Password (if you have)

Social Security Number (SSN)

http://148.244.93.9:4903

Business Code for CitiBusin
you have)

Expiration date for Credit Card

Date Of Birth (DOB)

CVV2 code for Credit Card (if you have)

E-mail address

sign on

Need help?
Forgot Your PIN?

* You must enter User ID if you use MyCiti, Citi Cards or Citi Business

Citigroup Privacy Promise Terms & Conditions Copyright © 2004 Citicorp

phishing scam report - smiles.co.uk

Metody Ochrony - "będzie gorzej"

Liczba znanych dziur

1995	171
1996	345
1997	311
1998	262
1999	417
2000	1090
2001	2437
2002	4129
2003	3784

Najbardziej dziurawe aplikacje

- Internet Information Services (IIS)
- Microsoft SQL Server (MSSQL)
- Windows Authentication
- Internet Explorer (IE)
- Windows Remote Access Services
- Microsoft Data Access Components (MDAC)
- Źle skonf. konta użytkowników (system haseł) (Unix)
- RPC (Unix)
- Microsoft Outlook i Outlook Express
- Windows Peer to Peer File Sharing (P2P)
- NIS/NFS - Unix
- Simple Network Management Protocol (SNMP - Win/Uuix)

Metody ochrony

- Najsłabsze ogniwo - My musimy pilnować 1000 wejść, naszemu wrogowi wystarczy tylko jedno!!!
- Sformułować, przestrzegać, uaktualniać **politykę bezpieczeństwa**
- Organizować okresowe (nie rzadziej niż raz na 6 mies), krótkie (godzinne) **szkolenia** dotyczące podstawowych zasad bezpieczeństwa IT
- Stosować restrykcyjną politykę dotyczącą instalacji oprogramowania przez użytkowników
- Stosować centralnie administrowany **system AV**
- Stosować centralny **system skanowania poczty/www**
  - wprowadzić silne restrykcje na typy załączników przesyłanych pocztą
  - zakazać przesyłania archiwów szyfrowanych hasłem
  - zakazać przesyłania plików wykonywalnych (exe, dll, ocx, scr, …)
  - stosować centralny skaner AV innego producenta niż skanery desktop
  - zakazać dostępu do zewnętrznych serwisów typu WebMail
- Stosować **centralny system antyspamowy** z sprzężeniem zwrotnym od użytkowników

CC
Otwarte Systemy
Komputerowe Sp. z o.o.

MAILsweeper™ Business Suite II

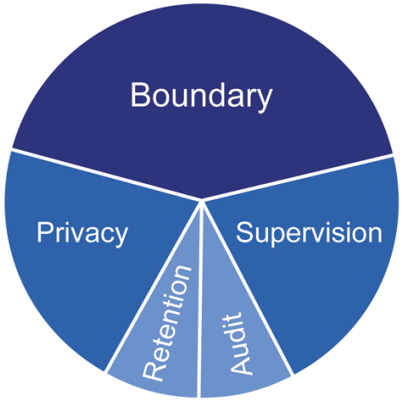
Clearswift: #1 w Content Security

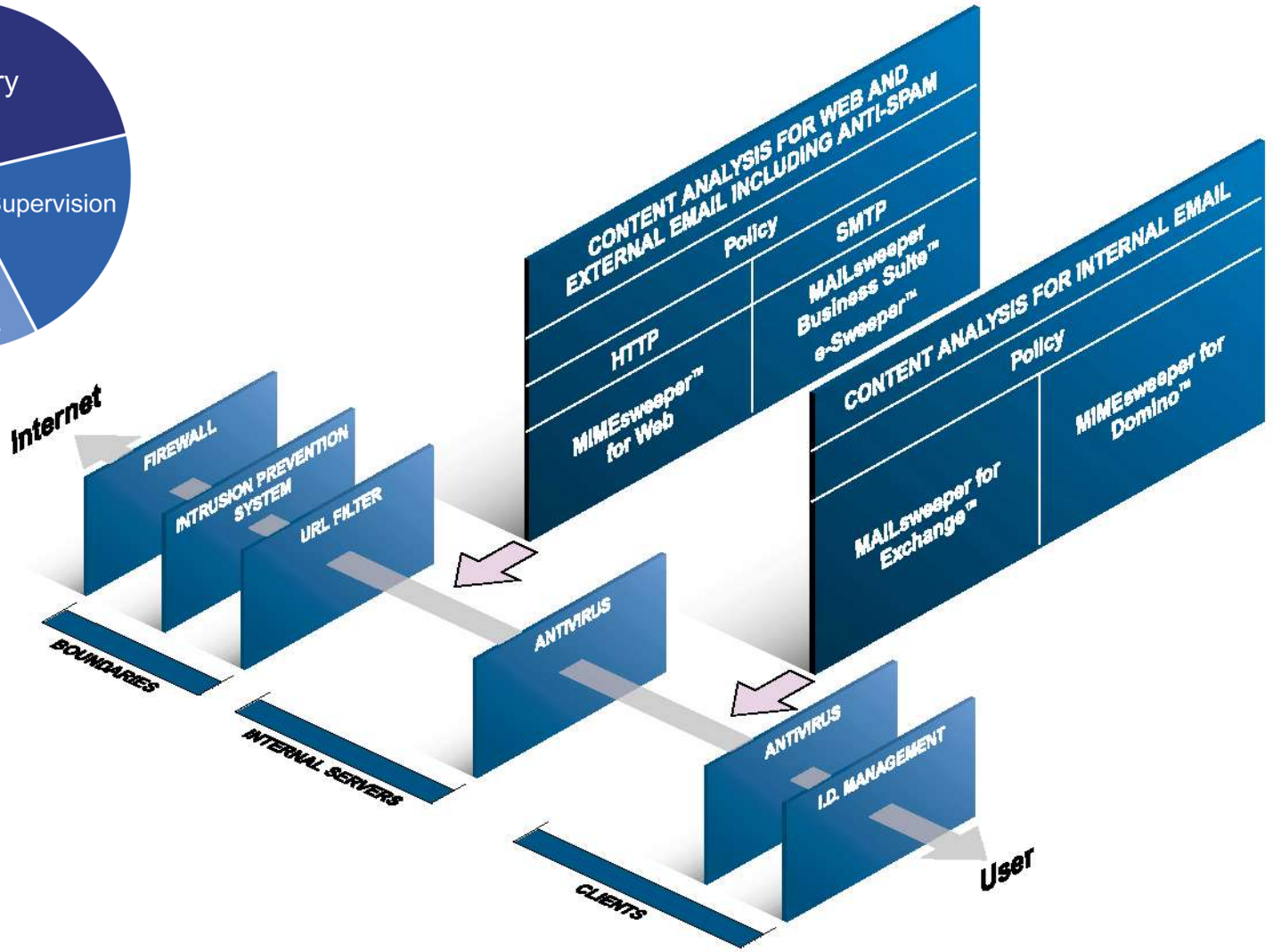
- Co to jest "Clearswift"?
  - Producent oprogramowania MIMEsweeper
  - #1 na światowym rynku produktów Content Security
- Obecny w: Wielkiej Brytanii (centrala), Francji, Niemczech, USA, Australii, Japonii
- 15,000+ klientów na całym świecie
  - 40 z 64 najwiekszych banków
  - Wszystkie z 10 nawiększych firm prawniczych
  - 70% firm z FTSE 200
  - 40% firm z grupy Global 500
  - Obecny w wielu dużych firmach i instytucjach w Polsce

Clearswift: #1 w Content Security

- Stabilny dostawca:
  - Dwadzieścia lat na rynku
  - Dobra sytuacja finansowa
- Technologia:
  - Firma, która stworzyła termin "content security"
  - Produkty wielokrotnie nagradzane
  - Produkty implementujace politykę bezpieczeństwa dla:
    - poczty wewnętrznej i zewnętrznej, WWW
- Obecność:
  - Ogólnoświatowy dostawca działający poprzez sieć partnerów
  - Brand #1 w Content Security
- Klienci:
  - 15,000 firm , 20 milionów użytkowników
  - SME, korporacje, organizacje rządowe i publiczne

Pełna ochrona





Pełna ochrona

- Przechwytywanie ruchu
  - bramka w każdym punkcie styku z sieciami zewnętrznymi
- Klasyfikacja wiadomości
  - Decyzja - jaka akcja dla danej wiadomości
- Content Security
  - kompleksowa analiza wiadomości
- Audyt i raportowanie
  - Informacje statystyczne i "materiał dowodowy"
- Archiwizacja
  - zachowanie wiadomości przechodzących przez system pocztowy

Produkty Clearswift

- MIMEsweeper Content Security
  - Oprogramowanie:
    - MAILsweeper Business Suite II
    - MIMEsweeper for Web
    - MIMEsweeper for Domino
    - MAILsweeper for Exchange
  - Usługa:
    - e-Sweeper

MAILsweeper Business Suite II

- Zawiera:
  - MIMEsweeper for SMTP
  - Personal Message Manager
  - Anti-spam filter
  - Raportowanie WEB
  - REMOTEmanager
- Zapewnia:
  - Zaawansowany "engine" content filtering (#1 leading wg. IDC, 2004)
  - "Osobisty" manager antyspamowy
  - 98% pewności w klasyfikacji spamu; << 1% false positives
  - Zaawansowane raportowanie
  - Rozproszone zarządzanie na poziomie "oddziałowym"

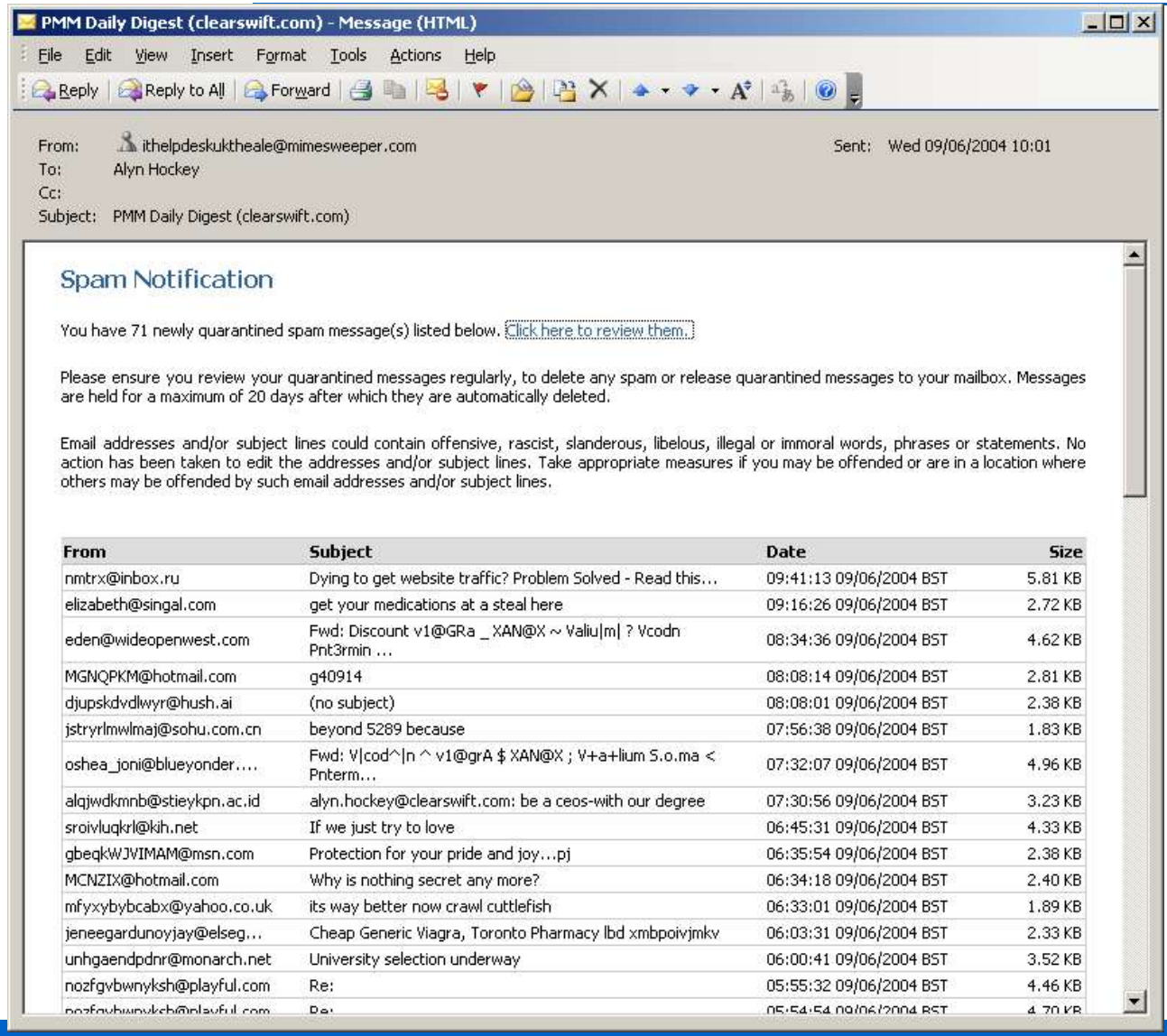
MAILsweeper for SMTP 4.3

- Najważniejsze funkcje:
  - Zapobiega infekcjom wirusowym (współpracuje z wiodącymi skanerami AV)
  - Elastyczne definiowanie polityk bezpieczeństwa
  - Wykrywa złośliwy kod i złośliwe skrypty
  - Wykrywa i usuwa załączniki wg. rzeczywistego typu pliku (np. MP3, gif/jpg, exe, itd.)
  - Rekursywna dekompozycja archiwów
  - Dodaje stopki
  - Kwarantanna dla "podejrzanych" wiadomości
  - Kreatory polityki bezpieczeństwa

Personal Message Manager (PMM)

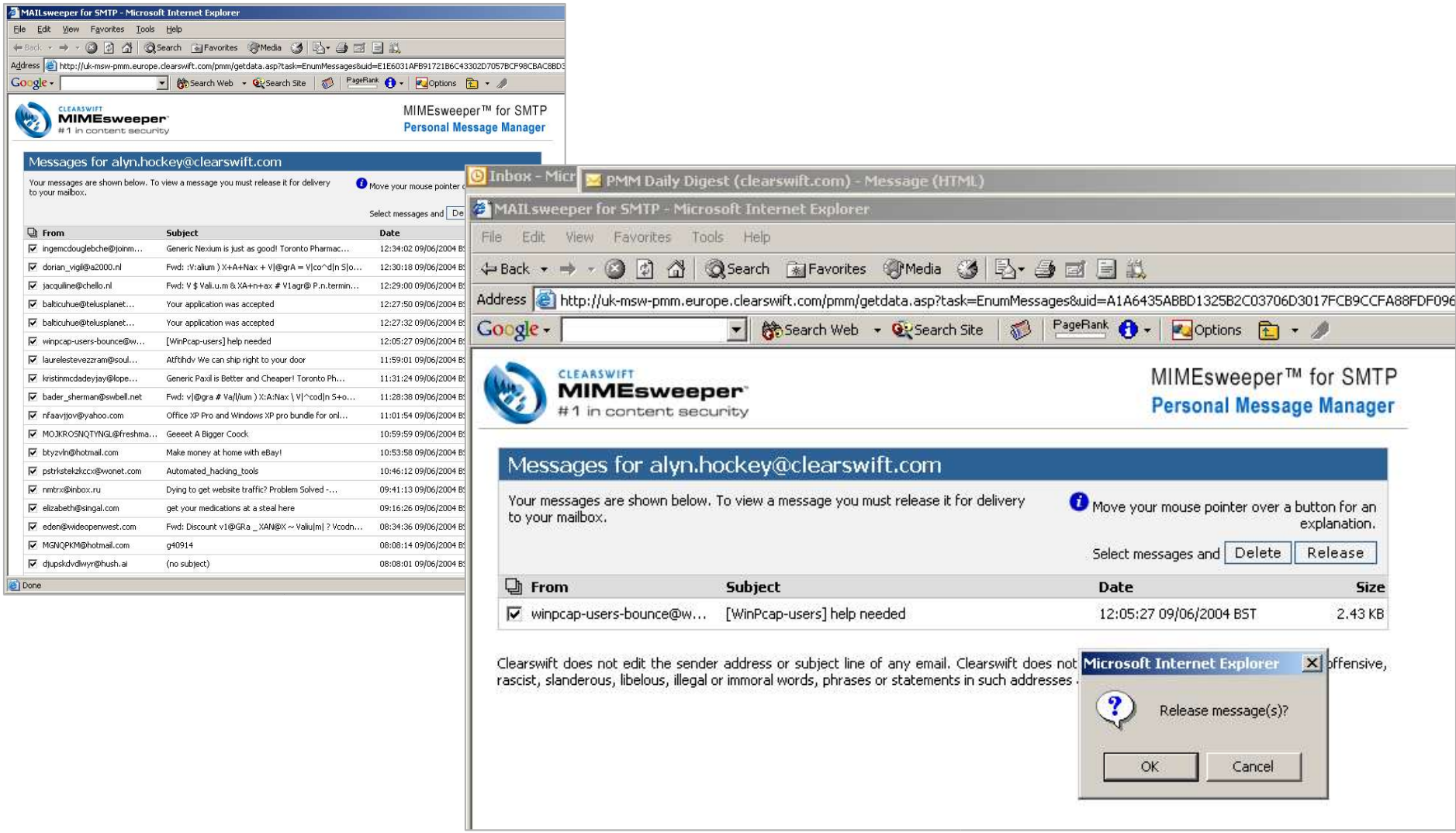
- Decyzje dotyczące spamu podejmowane są przez użytkowników:
  - Filtr usuwa wiadomości jednoznacznie sklasyfikowane jako spam, lecz w przypadku wątpliwości decyzja należy do odbiorcy - wiadomość podlega kwarantannie
  - Odbiorca otrzymuje listę wiadomości wstrzymanych
  - Odbiorca "zwalnia" wiadomości, które chce otrzymać i kasuje pozostałe
- Zalety:
  - Eliminacja klasyfikacji "false positive"
  - Sprawniejszy dopływ poczty do użytkownika
    - Użytkownik sam zarządza i defniuje spam
  - Odciążenie administratorów

PMM: użytkownik ogląda wiadomość ...



From	Subject	Date	Size
nmtrx@inbox.ru	Dying to get website traffic? Problem Solved - Read this...	09:41:13 09/06/2004 BST	5.81 KB
elizabeth@singal.com	get your medications at a steal here	09:16:26 09/06/2004 BST	2.72 KB
eden@wideopenwest.com	Fwd: Discount v1@GRa _ XAN@X ~ Valiu|m| ? Vcodn Pnt3rmin ...	08:34:36 09/06/2004 BST	4.62 KB
MGNQPKM@hotmail.com	g40914	08:08:14 09/06/2004 BST	2.81 KB
djupskdvdlwyr@hush.ai	(no subject)	08:08:01 09/06/2004 BST	2.38 KB
jstryrlmwlmaj@sohu.com.cn	beyond 5289 because	07:56:38 09/06/2004 BST	1.83 KB
oshea_joni@blueyonder....	Fwd: V|cod^|n ^ v1@grA $ XAN@X ; V+a+lium S.o.ma < Pnterm...	07:32:07 09/06/2004 BST	4.96 KB
alqjwdkmnb@stieykpn.ac.id	alyn.hockey@clearswift.com: be a ceos-with our degree	07:30:56 09/06/2004 BST	3.23 KB
sroivluqkrl@kih.net	If we just try to love	06:45:31 09/06/2004 BST	4.33 KB
gbeqkWJVIMAM@msn.com	Protection for your pride and joy...pj	06:35:54 09/06/2004 BST	2.38 KB
MCNZIX@hotmail.com	Why is nothing secret any more?	06:34:18 09/06/2004 BST	2.40 KB
mfyxybybcabx@yahoo.co.uk	its way better now crawl cuttlefish	06:33:01 09/06/2004 BST	1.89 KB
jeneegardunoyjay@elseg...	Cheap Generic Viagra, Toronto Pharmacy lbd xmbpoivjmkv	06:03:31 09/06/2004 BST	2.33 KB
unhgaendpdnr@monarch.net	University selection underway	06:00:41 09/06/2004 BST	3.52 KB
nozfgvbwnyksh@playful.com	Re:	05:55:32 09/06/2004 BST	4.46 KB
nozfgvbwnyksh@playful.com	Re:	05:54:54 09/06/2004 BST	4.70 KB

PMM: … i dokonuje wyboru

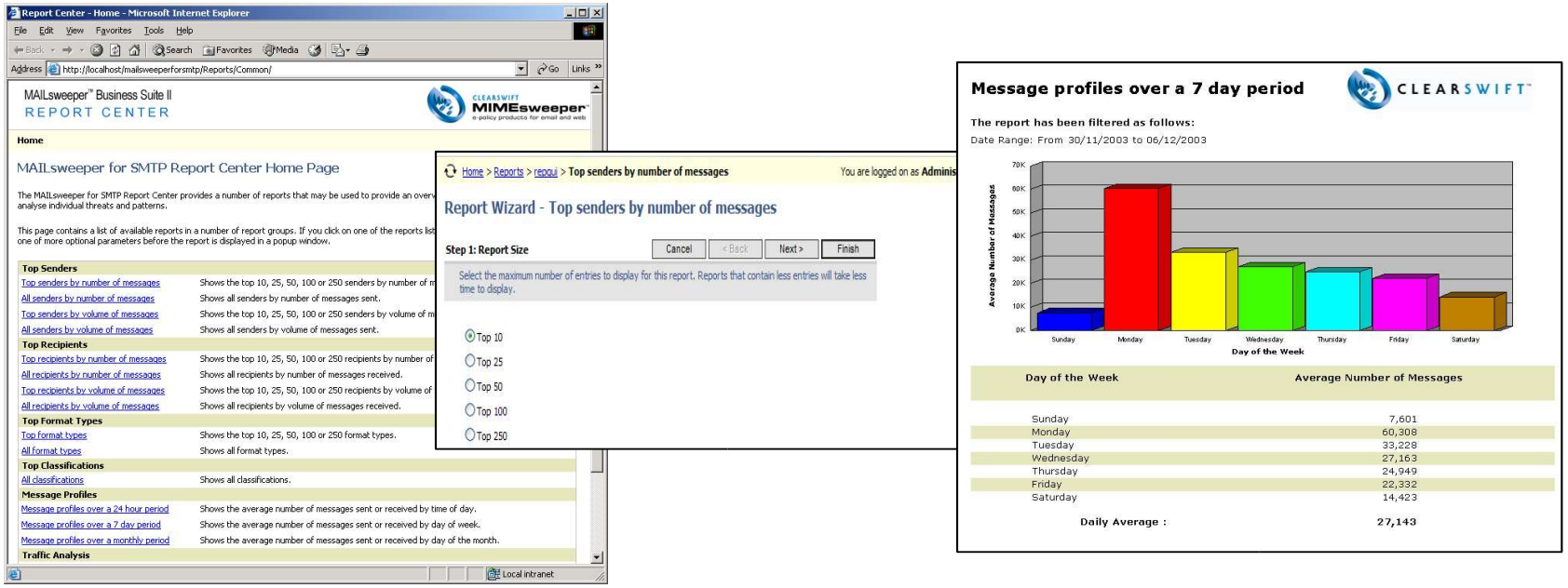


Podsumowanie funkcji anty-spam

- Pozwalają użytkownikowi końcowemu na eliminowanie płynących z niego zagrożeń wg. własnych preferencji
- Efektywność klasyfikacji wynosi 98% ("out-of-the-box")
- False positives << 1%
- Mechanizmy anty-spam:
  - Leksykalny, heurystyczny i Bayesowski
  - System samouczący
- Serwis on-line spamActive™:
  - stale aktualizowana lista adresów
  - stale aktualizowane słowniki
  - śledzenie i reagowanie na kampanie spamowe

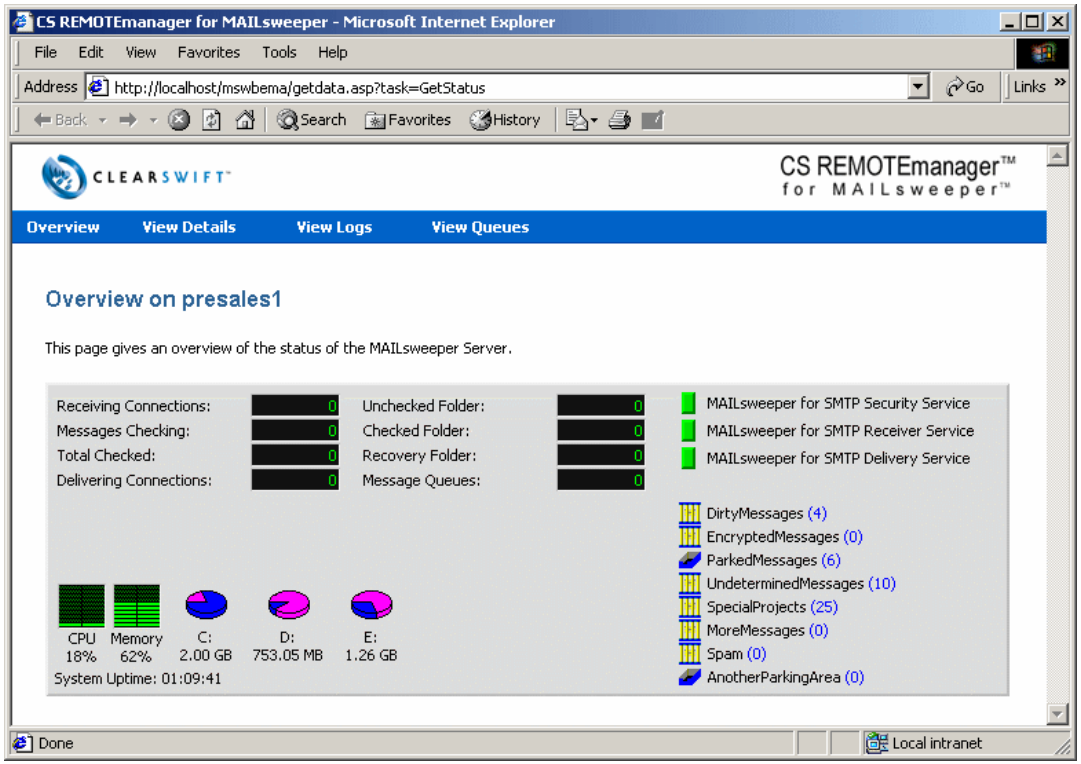
Raportowanie

- Pre-konfigurowane raporty
  - interfejs "tradycyjny" (Crystal Reports)
  - nowy interfejs WWW
- Szczegółowe raportowanie statystyk ruchu e-mail z wykresami
- Wbudowane raporty pozwalają szybko zlokalizować patologiczne zjawiska
- Raportowanie ułatwia też planowanie rozwoju i strojenie serwerów e-mail



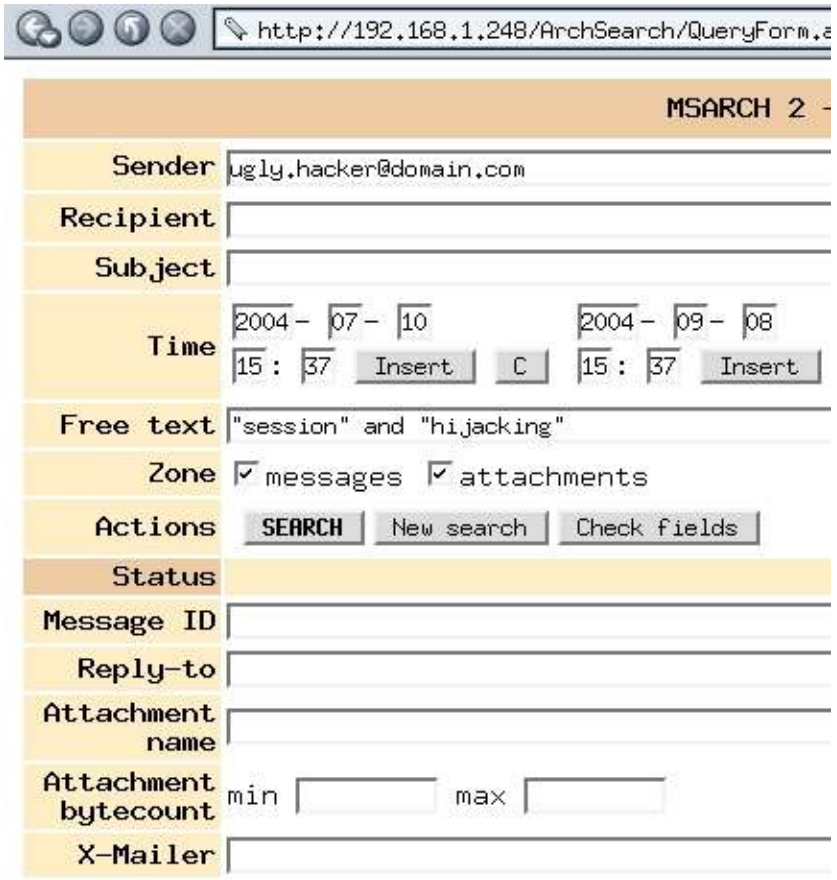
REMOTEmanager 1.4

- Konsola Web służąca do zdalnego zarządzania MAILsweeper-em SMTP
- Interfejs "Dashboard" do najważniejszych funkcji serwera
- Pozwala na zarządzanie wieloma serwerami
- Prosta "codzienna" administracja kolejkami wiadomości
- Konsola WWW - dostęp niezależny od lokalizacji



MSARCH

- Opracowany przez CC
- System archiwizujący współpracujący z:
  - MAILsweeperem
  - serwerami pocztowymi Unix: postfix, sendmail, qmail, …
  - innymi proxy SMTP
  - innymi serwerami SMTP
- Obsługa archiwów e-mail o b. dużym rozmiarze (rzędu setek GB)
- Wyszukiwanie wg.:
  - pól nagłówka -nadawca, odbiorca, temat
  - zawartości treści,
  - zawartości załączników
- Interfejs użytkownika: WWW
- Platforma: Windows 2000/2003
- Licencjonowanie: "per-mbox"



Nagrody i wyróżnienia

- Rodzina MIMEsweepr otrzymała szereg prostiżowych nagród i wyróżnień:
  - MAILsweeper
    - For SMTP
      - SC Award Winner 2003, Best Content Security
      - Frost & Sullivan Award Winner 2002
      - SC Award runner up 2002, Best Content Security
      - SC Award Winner 2000, Best Content Security
    - For Domino
    - For Exchange
      - SC Award Winner 2000, Best Email Security Solution
    - Anti-spam Edition
  - MIMEsweeper for Web
    - Highly Commended, SC Awards for Best Internet Security Product", 2002
  - IMAGEmanager
    - SC Award Winner 2000, Best Content Security (jako PORNsweeper)

SC MAGAZINE AWARDS 2003 WINNER

FROST & SULLIVAN
Market Engineering Award Recipient
Customer Brand Recognition 2002

FROST & SULLIVAN
Market Engineering Award Recipient
Customer Satisfaction 2002

CC Otwarte Systemy Komputerowe Sp. z o.o.

Referencje

Dziękuję za uwagę!

Pytania?