



*IronPort - systemy
antyvirusowe i antyspamowe
klasy Enterprise*



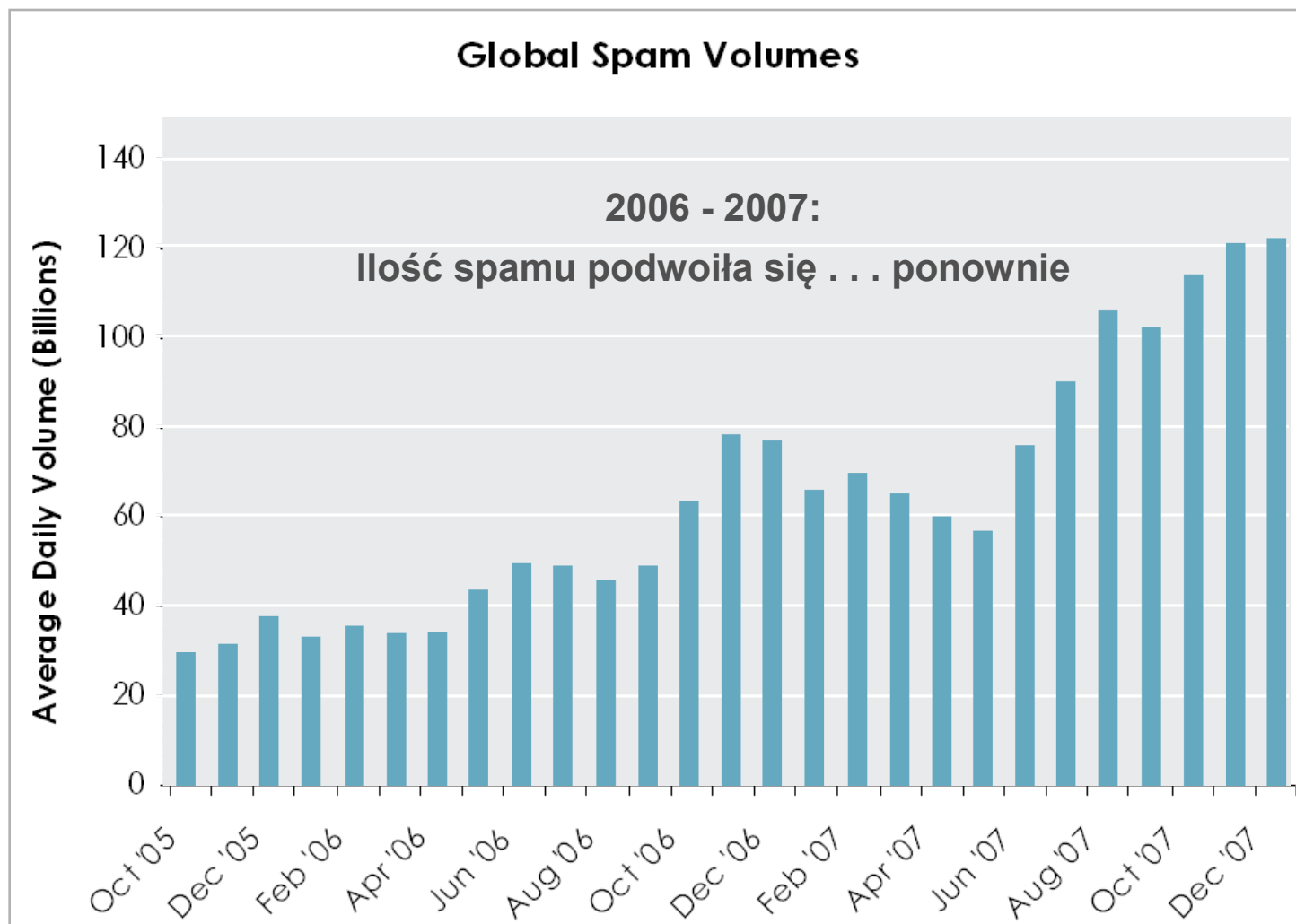
Grzegorz Wróbel

IronPort is now
part of Cisco.



Obecny trend

Więcej Spam



Source: IronPort's Threat Operations Center

Ewolucja spamu trwa

Spam “ASCII Art”

- Symbole akcji wyrażone za pomocą znaków ASCII
- Używane znaki losowo zmieniane

```
> ----- Original Message -----
> From: "Evan Platt" <evan <at> espphotography.com>
> To: <users <at> spamassassin.apache.org>
> Sent: Friday, November 17, 2006 10:48 AM
> Subject: Re: I've got TORA.08 spelled with numbers?
>
>
> > At 07:44 AM 11/17/2006, you wrote:
> >>I'm getting a bunch of spams this morning that have
> >>TORA.08 spelled out with numbers like this.
> >>
> >>4216775 0611576 215556 7 3308011 3258576
> >> 6 7 5 1 5 3 8 5 2 7 3
> >> 8 3 6 5 0 4 1 2 7 0 5
> >> 7 2 2 257873 5 7 4 1 3387715
> >> 6 2 5 7 1 111500075 8 6 2 2
> >> 8 2 2 7 7 3 2 656 0 3 0 8
> >> 0 6430533 4 4 8 6 207 5412501 7637213
> >>
```

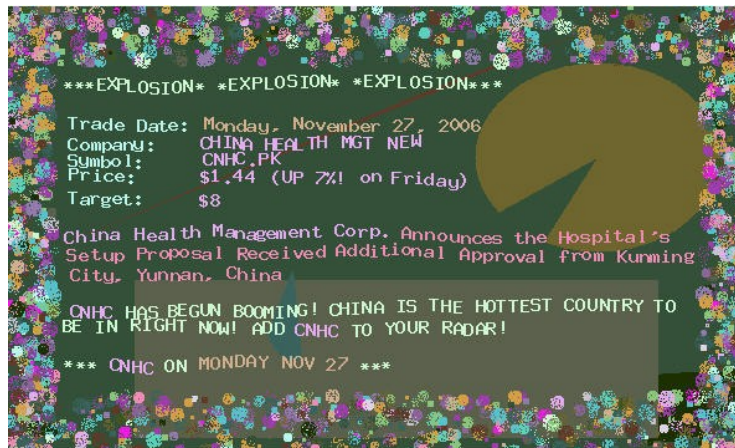


Image Spam 2.0

- Tworzenie obrazków w taki sposób, żeby przypominały „zwykłą” grafikę np. kartki z pozdrowieniami
- Używane obiekty z powerpointa i excela
- Fałujący tekst – utrudnienia dla technologii OCR

Spam obrazkowy

1. "Polka dots"

ATTENTION ALL DAY TRADERS AND INVESTORS

INVESTOR ALERT!

IT LOOKS LIKE ANOTHER RUN FOR SWNM!

WATCH SWNM LIKE A HAWK ON Tuesday July 1, 2006

Company Name: SOUTHWESTERN MEDICAL, INC.

Stock Symbol: SWNM

Monday Close: 0.11

Volume:

5,761,702

Change:

UP 0.025 (27.78%)

Market Cap: \$33,000,000.00 (Approx)

Goldmark Industries, Inc (GDKI.PK)

THIS STOCK IS EXTREMELY UNDERVALUED

Huge Advertising Campaign this week!

Breakout Forecast for July, 2006

Current Price: \$5.60

Short Term Price Target: \$12.00

Recommendation: Strong Buy

*300+% profit potential short term

RECENT HOT NEWS released MUST READ ACT NOW

LOS ANGELES_VANCOUVER, British Columbia -- Goldmark Industries, Inc. (GDKI.PK), the Company has recently signed a multi-movie distribution agreement with Mr. Rodriguez's production and distribution company, Polychrome Pictures, for the automatic theatrical and home video distribution of feature length films scheduled for release by Goldmark. Goldmark is making its ascent into the multi-billion

2. "Slice & Dice"

*** BREAKING NEWS ALERT ISSUED ***

Most stock brokers give out their new issues only to their largest commission paying clients. We assume many of you like to "trade the promotion" and may have made some big, fast money doing so.

Trade Date : Monday, July 31, 2006

Company : EVER GLORY INTL INC

Ticker: EGLY

Rises Over 5% on Friday.

Volume: 270,947

Price at Close Friday: \$1.15

3-6 Day Trading: \$3 - \$4

Expectations : STRONG BUY

Looking for a company with some good news? Here's one!

Breaking News:

Ever-Glow Signs \$500,000 Deal with Debenhams (Read Yahoo Finance) There is a massive promotion underway this weekend apprising potential eager investors of this emerging situation. Breaking news alert issue - big news coming. We feel this is a "Stock Alert" and you should have this on your Radar. Big news expected. This should invoke LARGE gains. Do this often enough, and your portfolio can double, even TRIPLE in value.

BREAKING NEWS ALERT ISSUED

Most stock brokers give out their new issues only to their largest commission paying clients. We assume many of you like to "trade the promotion" and may have made some big, fast money doing so.

Trade Date : Friday, July 28, 2006

Company : EVER GLORY INTL INC

Ticker : EGLY

Price : \$1.09

3-6 Day Trading : \$3 - \$6

Expectations : BUY

Looking for a company with some good news? Here's one!

Breaking News:

Ever-Glory Signs \$500,000 Deal with Debenhams (Read Yahoo Finance)

There is a massive promotion underway this weekend apprising potential eager investors of this emerging situation. Breaking news alert issue - big news coming. We feel this is a "Stock Alert" and you should have this on your Radar.

Spam w 2007 roku

Testowanie nowych technik



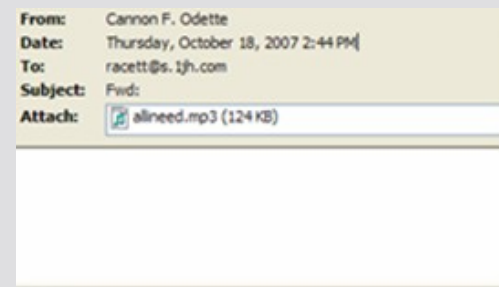
Text Spam

2005



PDF Spam

2007 2nd Qtr



MP3 Spam

4th Qtr

3rd Qtr



Image Spam



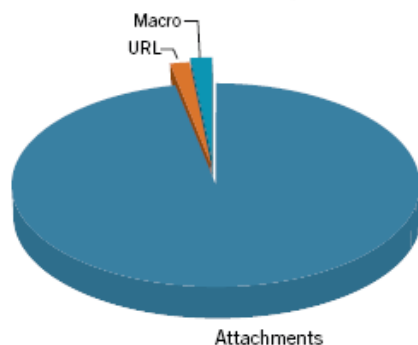
Excel Spam

“2007 has seen a proliferation of different attachment types...Spammers are using these different attachments in order to try and get past email security gateways that are unable to look into complicated file types”

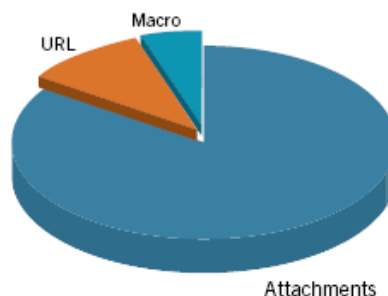
Poczta a wirusy

Więcej epidemii, więcej wariantów, więcej URLi

2006 Outbreak Composition



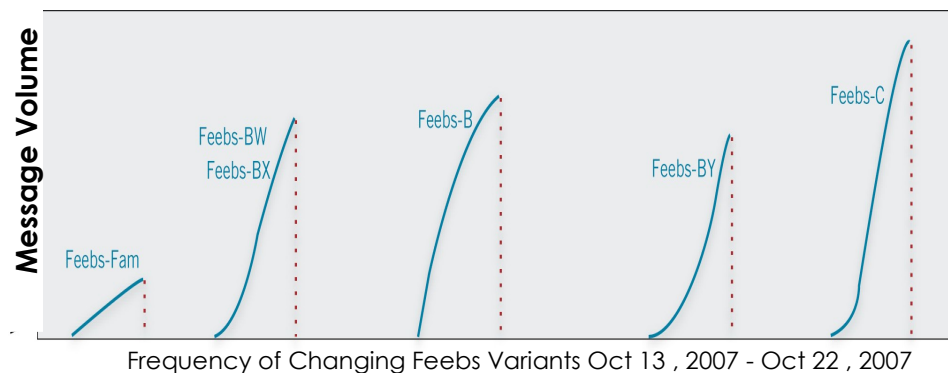
2007 Outbreak Composition



- Wirusy zawierające URLe - przyrost 256%
- Częściej klikamy w URLe niż w załączniki
- Wyzwanie dla systemów AV

- Feefs: 7 dni, 6 wariantów

Feefs Outbreak October 2007



Baza reputacyjna IronPort SenderBase®

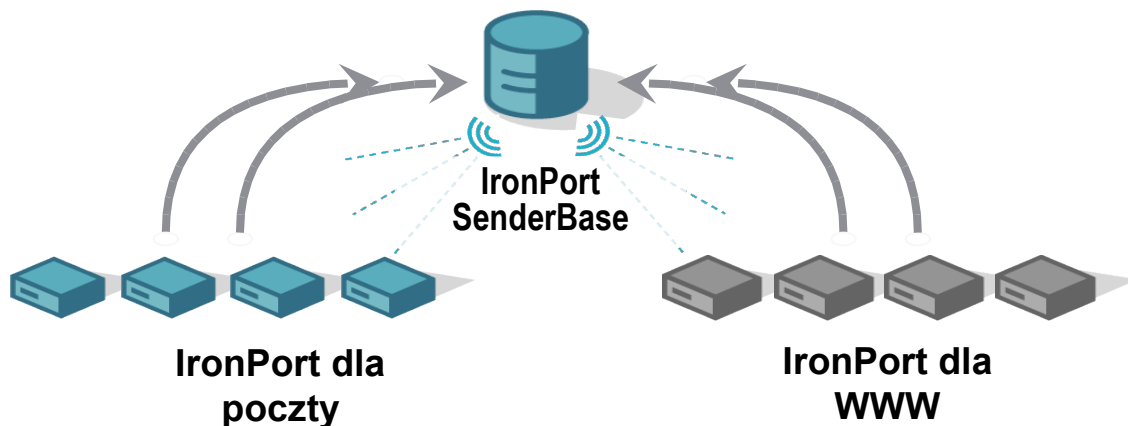
Globalny zbiór informacji o ruchu sieciowym



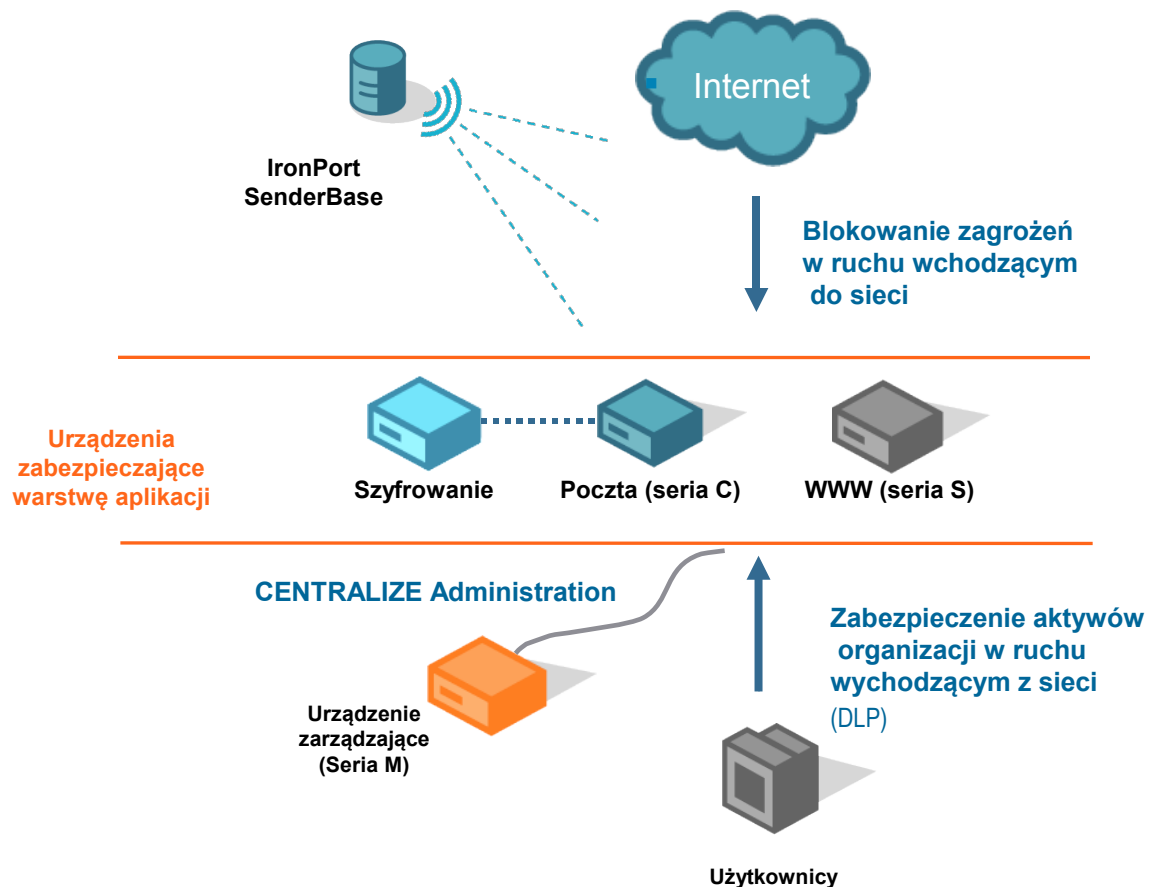
- **30Mil.+** ilość zapytań dziennie
- **150+** ilość analizowanych parametrów ruchu smtp i http
- **25%** procentowe pokrycie całego ruchu w sieci Internet
- **a wkrótce .. także informacje z urządzeń Cisco**

- Wgląd w dane dotyczące obydwu protokołów (poczta i www) znacząco podnosi efektywność rozwiązań IronPort
- 80% spamu zawiera URLe
- Email jest głównym medium dystrybucyjnym dla malwaru wystawionego na WWW
- Malware jest głównym narzędziem do instalacji silników smtp służących do spamowania

Połączona analiza ruchu Email & WWW

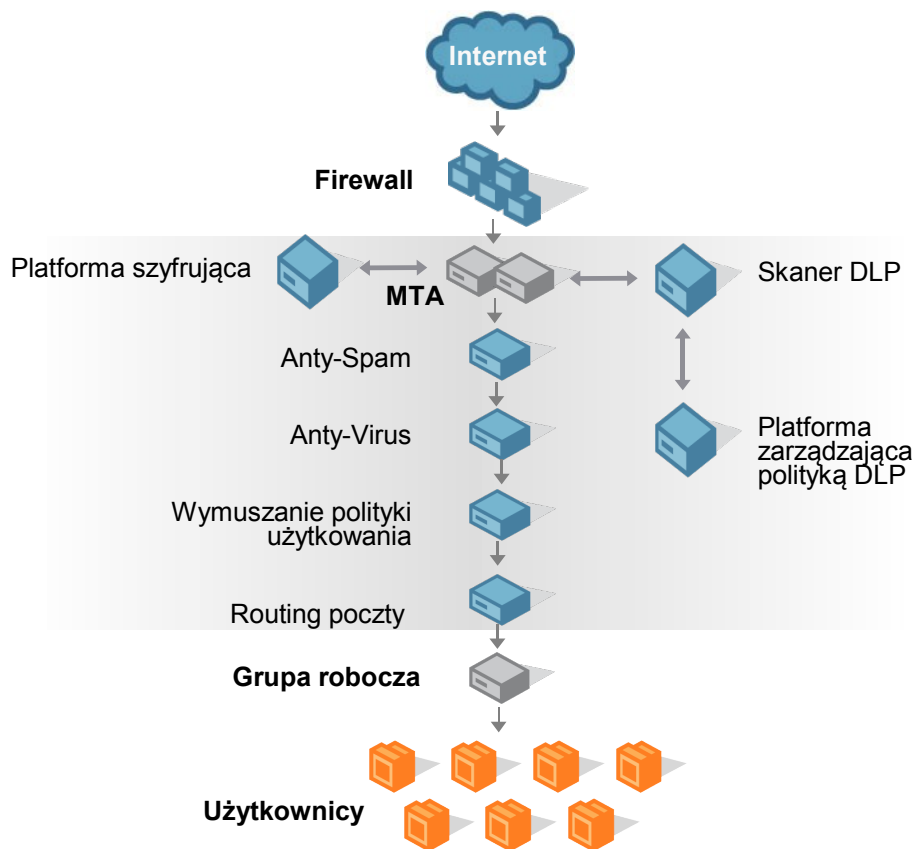


Rodzina produktów IronPort®

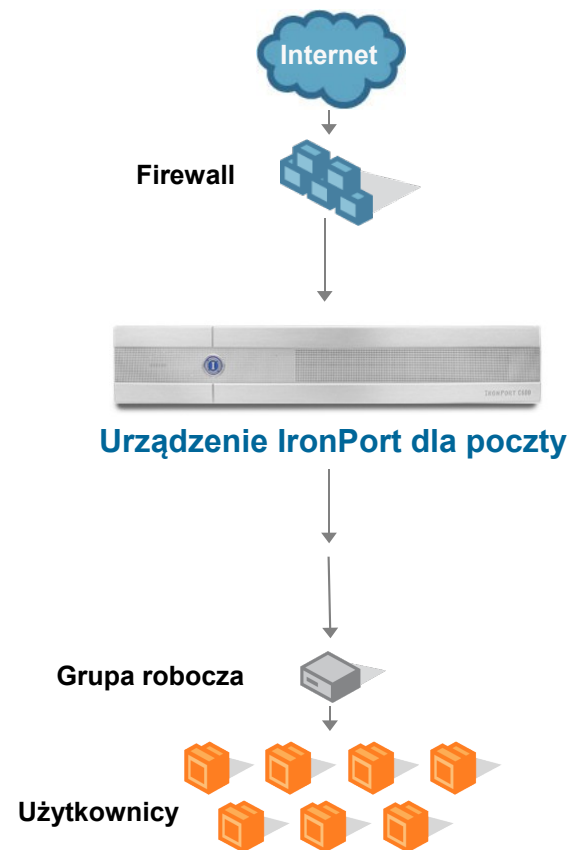


IronPort, a konsolidacja mechanizmów bezpieczeństwa na brzegu sieci

Bez IronPort



Z IronPort



Wielowarstwowa ochrona przed spamem

Zabezpieczenie typu „Gateway”



- **IronPort Reputation Filters™ / Filtry reputacyjne:** Pierwsza warstwa ochrony
- **IronPort Anti-Spam™:** Druga warstwa ochrony zatrzymująca spam, phishing, próby oszustw i wiele innych zagrożeń

IronPort's Anty Spam – metody ochrony

- Wielowarstwowa ochrona antyspamowa zaprojektowana w celu:

Powstrzymywania spamu w sposób niezwykle wydajny

Powstrzymywania spamu w sposób najdokładniejszy



Silnik IronPort Anti-Spam

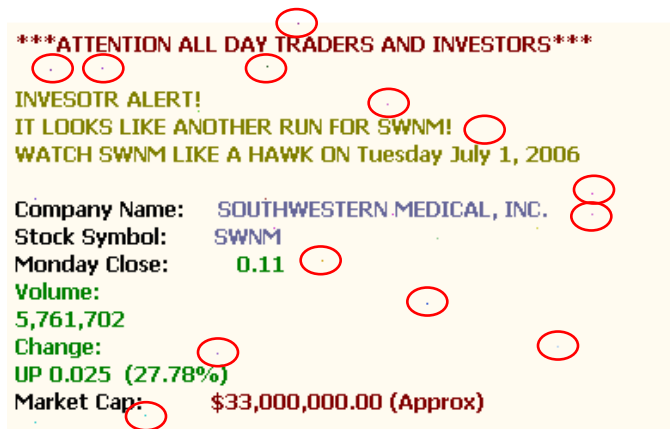
Dokładność dzięki Context Adaptive Scanning Engine (CASE)

JAK?

- Wiadomość zawiera ślad generatora spamu

CO?

- Obrazek zawiera tylko tekst
- Przypadkowe kropki wewnątrz obrazka
- Prawie identyczny schemat kolorów jak w ponad 100,000 wiadomościach przechwyconych przez pułapki spamowe



KTO?

- IP adres od niedawna wysyła maile
- Adres jest z puli dial-up
- Adres jest z puli przydzielonej w Rosji

DOKĄD?

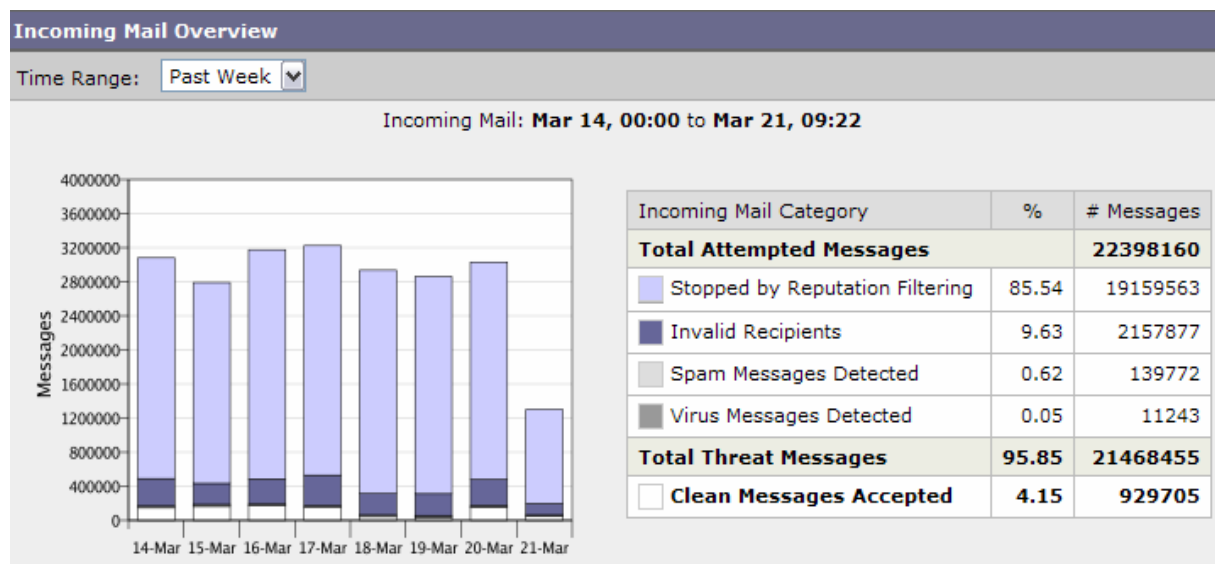
Werdykt

Blokuj

Network Owner	DataNet
Domain	dnet.pl
Date of first message seen from this address	2006-06-18
CIDR range	unknown
# of domains controlled by this network owner	500
Geography data	
Country	RU
State	MS
City	Moscow

Filtry reputacyjne IronPort

Dell - Studium przypadku



Wzrost dokładności wykrywania spamu - **10x**
Konsolidacja serwerów - **70%**
Redukcja kosztów operacyjnych - **75%**



***“Ironport zwiększył
jakość i stabilność
naszej sieci
jednocześnie
zmniejszając koszty
operacyjne.”***

— Tim Helmstetter
Manager, Global Collaborative
Systems Engineering and
Service Management,

DELL CORPORATION

Ilość skrzynek

100,000+

Wielowarstwowa ochrona przed spamem

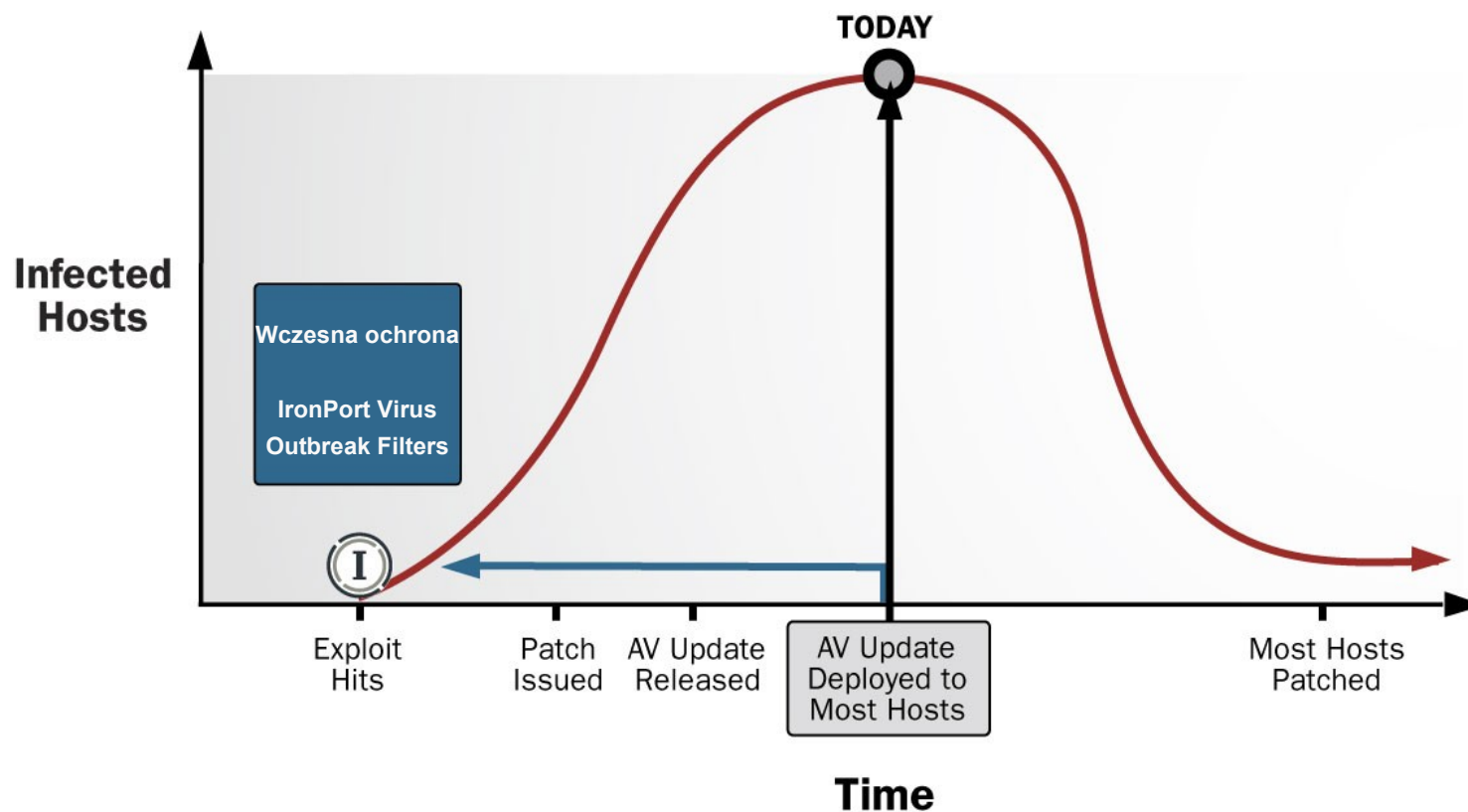
Zabezpieczenie typu „Gateway”



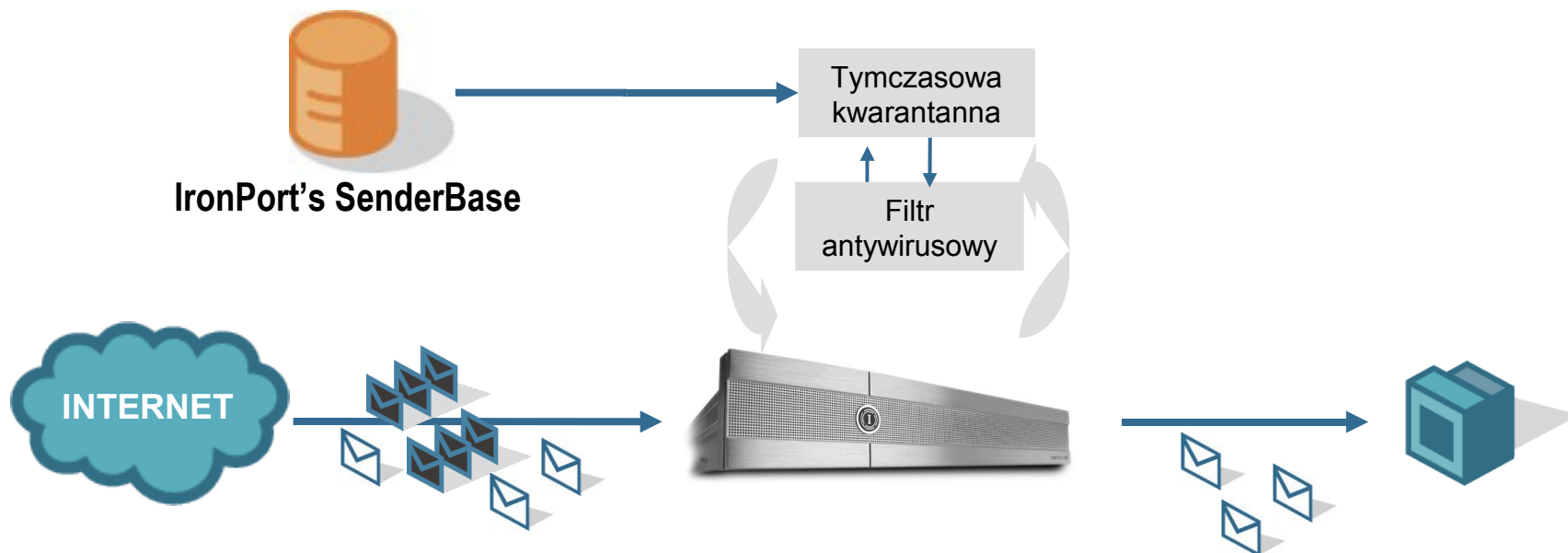
- **IronPort Virus Outbreak Filters™**: Zatrzymuje najnowsze wirusy nawet 13h przed silnikami antywirusowymi
- **McAfee i Sophos Anty-Virus**: Rozwiązanie bazujące na sygnaturach więcej niż jednego producenta AV

IronPort Virus Outbreak Filters(VOF)

Pierwsza linia obrony



IronPort Virus Outbreak Filters w akcji



- Porównanie poczty przychodzącej z regułami
- Automatyczna kwarantanna dla podejrzanych załączników
- Wypuszczenie wiadomości z kwarantanny i ponowne przeskanowanie przez silnik AV

Sygnatury antywirusowe McAfee Sophos

Kolejna warstwa ochronna

- Zintegrowane silniki McAfee i Sophos

Skanowanie szeregowo

Możliwy wybór jednego z dwóch silników

- Łatwa implementacja i zarządzanie

Intuicyjny interfejs zarządzania

Pojedyncze miejsce monitorowania pracy silników za pomocą IronPort Mail Flow Monitor™

Automatyczne uaktualnienia

Niższy koszt całkowity posiadania poprzez zintegrowanie różnych silników na jednej platformie

The screenshot displays the 'Mail Policies: Anti-Virus' configuration page. It is divided into two main sections: 'Anti-Virus Settings' and 'Message Scanning'. Under 'Anti-Virus Settings', the 'Policy' is set to 'DEFAULT', and 'Enable Anti-Virus Scanning for This Policy' is set to 'Yes'. The 'Message Scanning' section includes a dropdown menu set to 'Scan and Repair viruses', a checkbox for 'Drop infected attachments if a virus is found and it could not be repaired', and a checked checkbox for '(recommended) Include an X-header with the Anti-Virus scanning results in messages'. Below this is the 'Repaired Messages' section, which includes 'Action Applied to Message' (set to 'Deliver As Is'), 'Archive Original Message' (set to 'No'), 'Modify Message Subject' (set to 'Prepend' with a custom subject line '[WARNING: VIRUS REMOVED]'), and 'Send Notification Message' (with checkboxes for 'to sender', 'to recipient', and 'to others'). An 'Advanced' link is provided for optional settings. The bottom section, 'Encrypted Messages', follows a similar layout with 'Action Applied to Message' set to 'Deliver As Is', 'Archive Original Message' set to 'No', 'Modify Message Subject' set to 'Prepend' with a custom subject line '[WARNING: MESSAGE ENCRYPT]', and 'Send Notification Message' options.

IronPort DLP

Sankcjonowanie polityki bezpieczeństwa dla poczty przychodzącej i wychodzącej

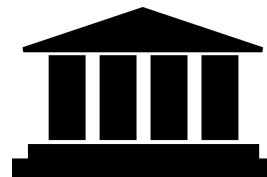


- **Elastyczne Tworzenie polityk** akceptowalnego użytkowania oraz ochrony własności intelektualnej
- **Rozwiązanie gwarantujące komplementarność** z wymogami regulacji
- **Zintegrowana architektura szyfrująca wiadomości**

DLP

Problem o różnych wymiarach

- Zgodność z regulacjami
np. Ustawa o ochronie danych osobowych, Ochrona danych objętych klauzulą poufne i wyższymi
- Polityka akceptowalnego użytkowania
Blokowanie treści obraźliwych
Wymuszanie polityki komunikacji (np. dozwolona wielkość maksymalnego załącznika)
Dodawanie stopki z załącznikiem
- Ochrona własności intelektualnej
Blokowanie komunikacji z konkurencją bądź podejrzanymi adresatami



Wielowarstwowa ochrona

Przyspieszenie komunikacji biznesowej – poufność zamiast kwarantanny

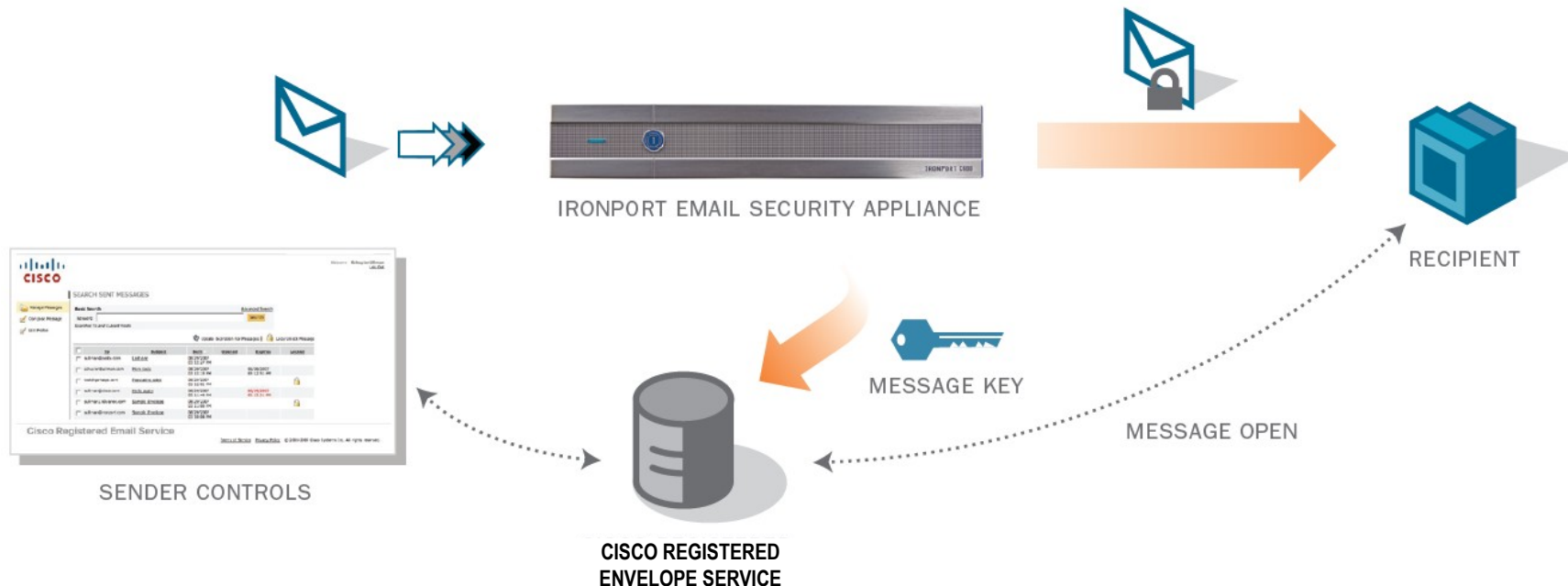


Hot news: PostX i Ironport razem



IronPort PXE: Wysyłanie zaszyfrowanej wiadomości

Zerowe koszty zarządzania i natychmiastowe wdrożenie

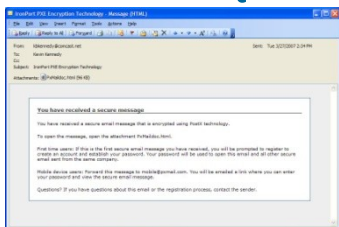


- **Automatyczne zakładanie konta dla użytkowników**
- Uwierzytelnienie odbiorcy i bezpieczne doręczenie klucza
- Śledzenie wiadomości
- Bezpieczna odpowiedź
- **Wiadomość NIGDZIE nie jest przechowywana**

Bezpieczniejsza poczta

Szyfrowanie łatwe do obsługi dla odbiorcy

1. Otwórz załącznik

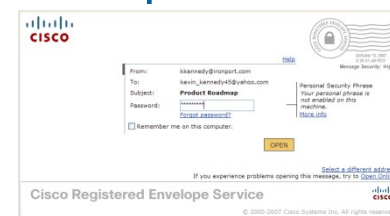


Bez ograniczeń
w adresach odbiorców

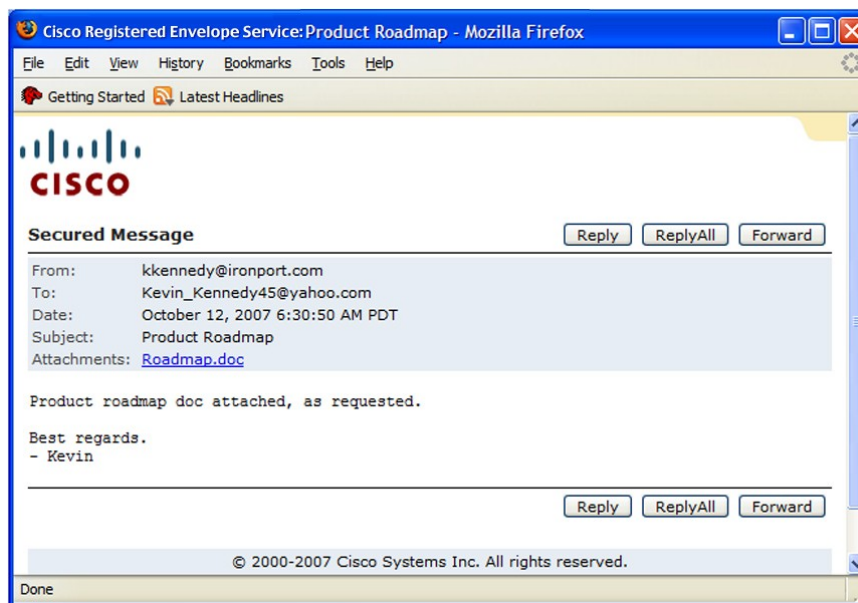
Bez certyfikatów

Bez pluginów

2. Wpisz hasło



3. Zobacz wiadomość





Pytania...



IronPort is now
part of Cisco.

