symantec.

Confidence in a connected world.

The Emerging Threat Landscape

Zulfikar Ramzan, Ph.D.
Technical Director and Architect
Security Technology and Response

Tuesday, June 03, 2008

Agenda

symantec.

1 Intro

2 Shifting Threat Landscape

3 Malware: Growing Dangerously

4 Web attacks: The New Epicenter

5 Global Intelligence Network

6 The Road Ahead

Most of the data I'll present comes from the Symantec Internet Security Report Edition XIII – covering Jul-Dec 2007

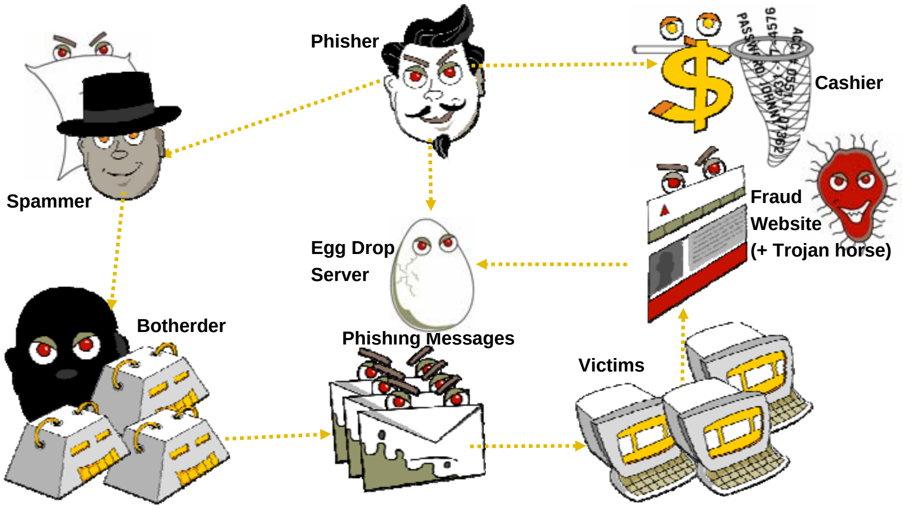
Some Key Trends

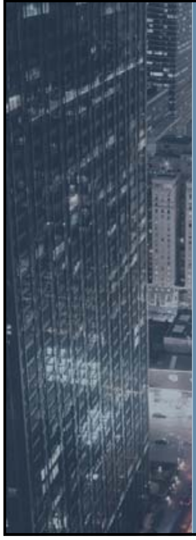
- Underground economy and supply chain lowers bar for who can participate in cybercrime
- Lack of trust among underground economy participants may force additional organization
- Malicious software levels consistently rising
  - More malicious software in ‘08 than all previous years combined
  - By all accounts, ’09 will be same
  - Good vs. bad software inflection point
- Web will continue as an attack vector because of its popularity and content richness
- Targeted attacks will likely be an issue and will necessitate defense-in-depth protection
- Attackers starting at the supply chain (infected digital picture frames)

Fraud Economy Menu & Ads

Rank	Previous	Goods and Services	Current %	Previous %	Prices
1	2	Bank Accounts	22%	21%	$10-$1000
2	1	Credit Cards	13%	22%	$0.40-$20
3	7	Full Identity	9%	6%	$1-$15
4	N/R	Online Auction Site Accounts	7%	N/A	$1-$8
5	8	Scams	7%	6%	$2.50/wk - $50/wk (hosting); $25 (design)
6	4	Mailers	6%	8%	$1-$10
7	5	Email Addresses	5%	6%	$0.83/MB-$10/MB
8	3	Email Passwords	5%	8%	$4-$30
9	N/R	Drop (request or offer)	5%	N/A	10-50% of drop amount
10	6	Proxies	5%	6%	$1.50-$30

The Fraud Food Chain

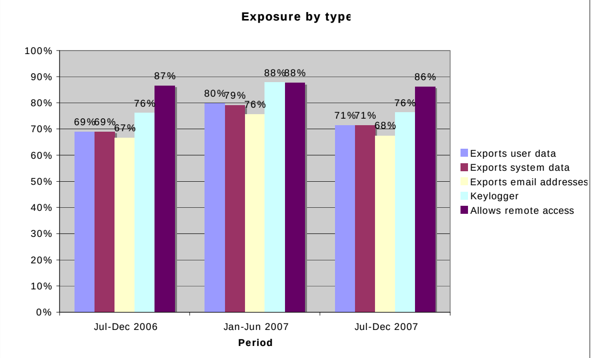




Confidence in a connected world.

Malware: Growing Dangerously & Dangerously Growing

Designed for data theft & unauthorized access

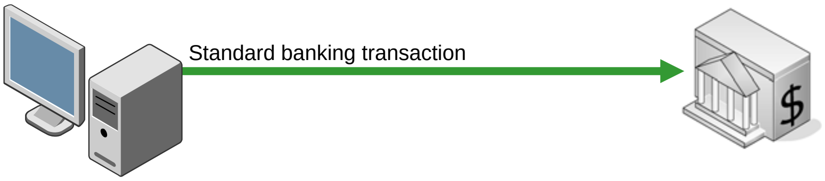


For the 2nd half of ’07,

- 68% of the top 50 malicious code posed threat to confidential info
  - 3% ↑ from H1 ’07;
  - 15% ↑ from H2 ’06;
- Keystroke loggers represent 76% of the reported threats to confidential information

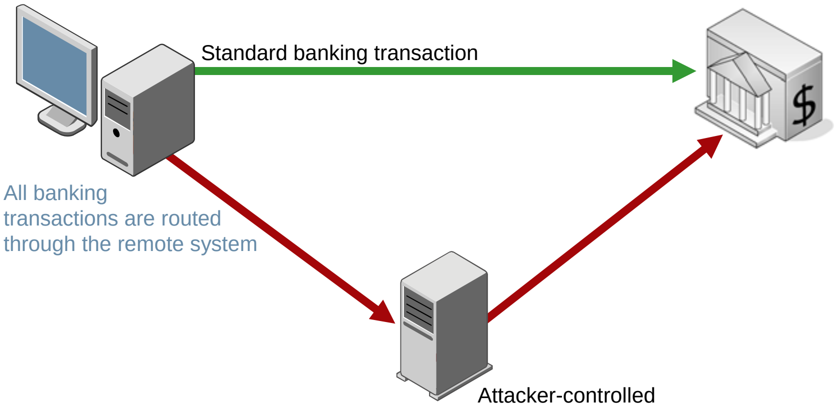
The decline in all five categories could be attributable to a specific piece of malware being more targeted and having fewer capabilities (e.g., versus having all five capabilities); malware authors may be employing such techniques to make detection more difficult.

Trojan.Silentbanker



Trojan.Silentbanker

Remote
Man in the Middle



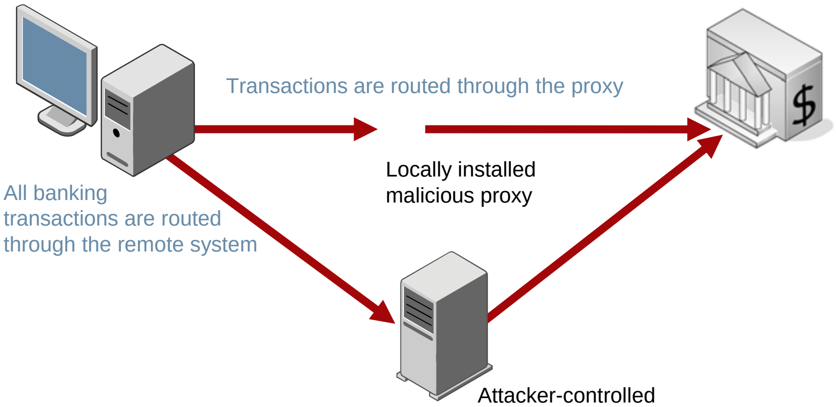
Standard banking transaction

All banking transactions are routed through the remote system

Attacker-controlled remote system

Trojan.Silentbanker

Local Remote
Man in the Middle

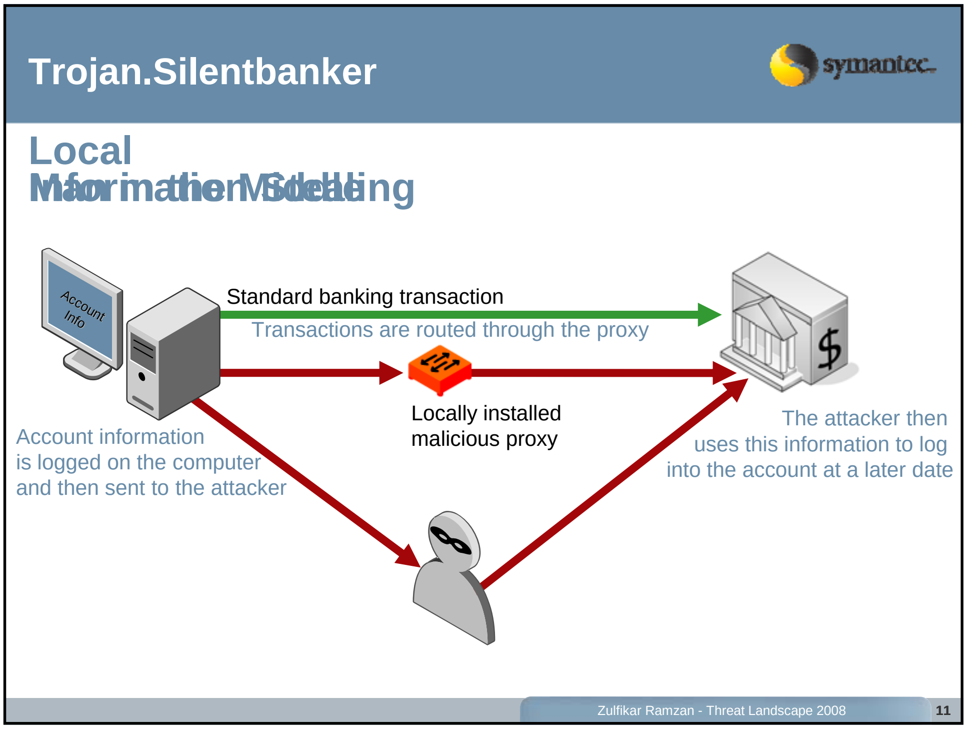


Transactions are routed through the proxy

Locally installed malicious proxy

All banking transactions are routed through the remote system

Attacker-controlled remote system



Trojan.Silentbanker

Local
Man in the Middle
Information Stealing

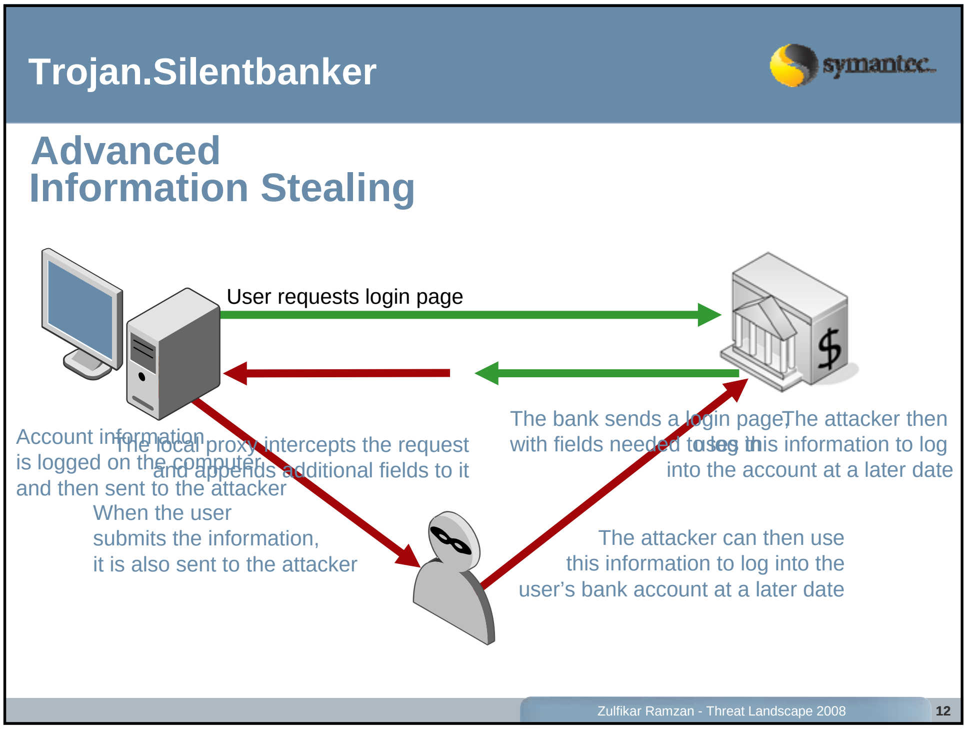
Standard banking transaction

Transactions are routed through the proxy

Locally installed
malicious proxy

Account information
is logged on the computer
and then sent to the attacker

The attacker then
uses this information to log
into the account at a later date



Trojan.Silentbanker

Advanced
Information Stealing

User requests login page

The bank sends a login page,
with fields needed to log in

Account information
is logged on the computer
and then sent to the attacker

The local proxy intercepts the request
and appends additional fields to it

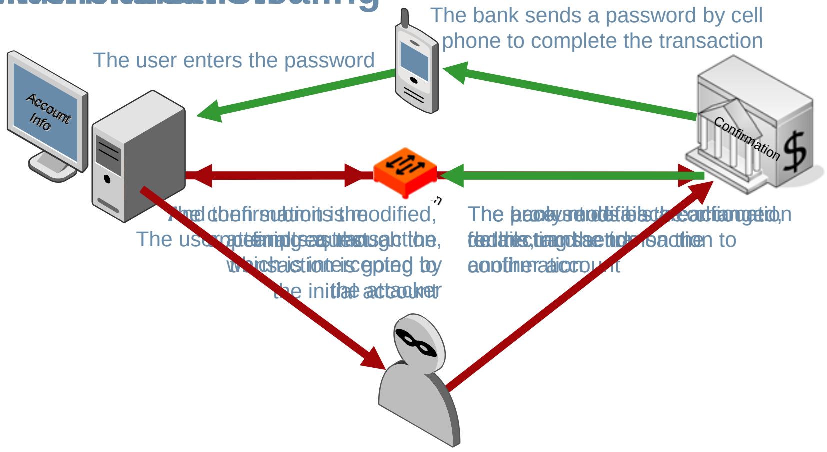
The attacker then
uses this information to log
into the account at a later date

When the user
submits the information,
it is also sent to the attacker

The attacker can then use
this information to log into the
user's bank account at a later date

Trojan.Silentbanker

Two-Factor Authentication / Advanced Information Stealing



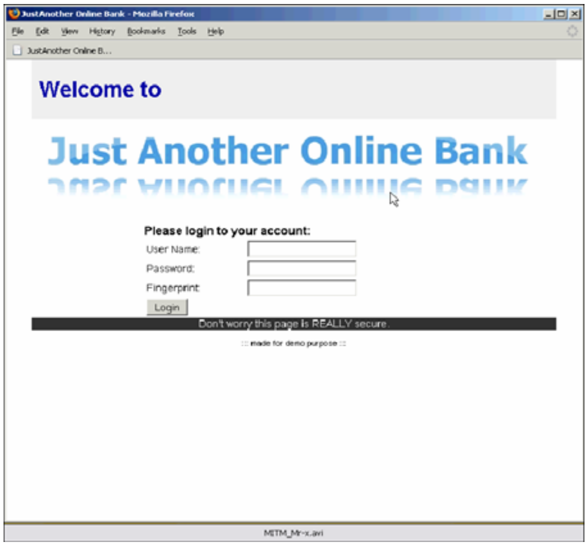
The bank sends a password by cell phone to complete the transaction

The user enters the password

The user attempts a transaction, which is intercepted by the attacker / The confirmation is modified, the initial account

The proxy modifies the transaction details, and sends them to another account / The bank sends back a confirmation

Man-in-the-Middle Trojans in Action



JustAnother Online Bank - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JustAnother Online B...

Welcome to

Just Another Online Bank

Please login to your account:

User Name:

Password:

Fingerprint:

Login

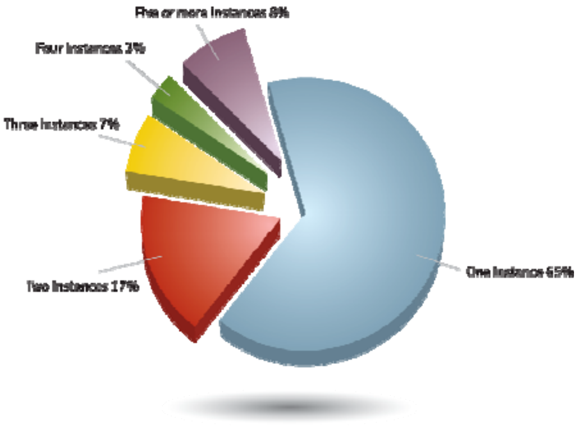
Don't worry this page is REALLY secure.

:: made for demo purpose ::

Staged Downloaders: When it rains, it pours

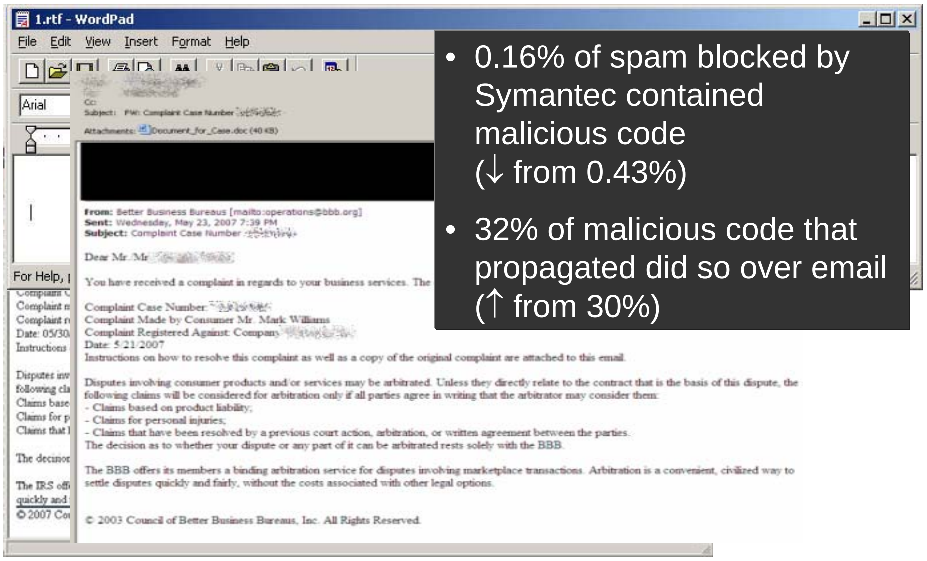
For the 1st half of '07:

- 35% of computers reporting potential malicious code infections reported more than once
- Many of these likely the result of staged downloaders



Only 10% of malware samples Symantec sees actually exploit a technical vulnerability; the rest either piggyback or rely on social engineering…

Using IRS Fears to Install Malware: Backdoor.Robofo



[redacted]
Cc:
Subject: FW: Complaint Case Number [redacted]
Attachments: Document_for_Case.doc (40 KB)

[redacted]

From: Better Business Bureaus [mailto:operations@bbb.org]
Sent: Wednesday, May 23, 2007 7:39 PM
Subject: Complaint Case Number [redacted]

Dear Mr./Mr [redacted]

You have received a complaint in regards to your business services. The

Complaint Case Number: [redacted]
Complaint Made by Consumer Mr. Mark Williams
Complaint Registered Against: Company [redacted]
Date: 5/21/2007
Instructions on how to resolve this complaint as well as a copy of the original complaint are attached to this email.

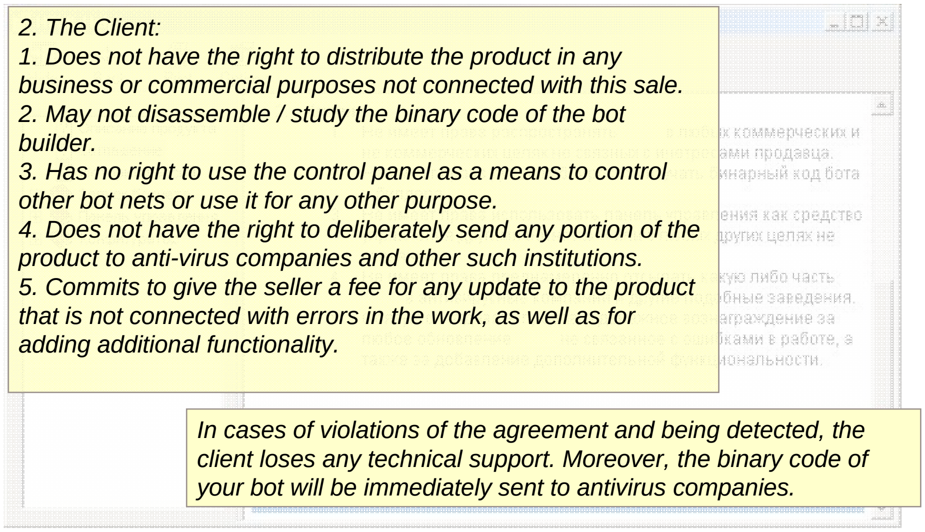
Disputes involving consumer products and/or services may be arbitrated. Unless they directly relate to the contract that is the basis of this dispute, the following claims will be considered for arbitration only if all parties agree in writing that the arbitrator may consider them:
- Claims based on product liability;
- Claims for personal injuries;
- Claims that have been resolved by a previous court action, arbitration, or written agreement between the parties.
The decision as to whether your dispute or any part of it can be arbitrated rests solely with the BBB.

The BBB offers its members a binding arbitration service for disputes involving marketplace transactions. Arbitration is a convenient, civilized way to settle disputes quickly and fairly, without the costs associated with other legal options.

© 2003 Council of Better Business Bureaus, Inc. All Rights Reserved.

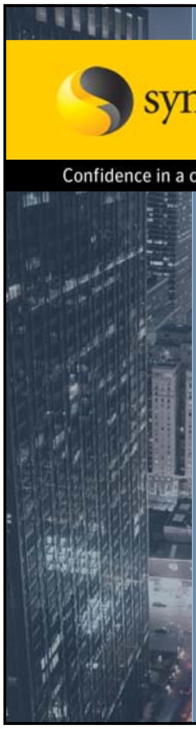
- 0.16% of spam blocked by Symantec contained malicious code (↓ from 0.43%)
- 32% of malicious code that propagated did so over email (↑ from 30%)

Using Fear to “Copy Protect” Malware



2. The Client:
1. Does not have the right to distribute the product in any business or commercial purposes not connected with this sale.
2. May not disassemble / study the binary code of the bot builder.
3. Has no right to use the control panel as a means to control other bot nets or use it for any other purpose.
4. Does not have the right to deliberately send any portion of the product to anti-virus companies and other such institutions.
5. Commits to give the seller a fee for any update to the product that is not connected with errors in the work, as well as for adding additional functionality.

In cases of violations of the agreement and being detected, the client loses any technical support. Moreover, the binary code of your bot will be immediately sent to antivirus companies.

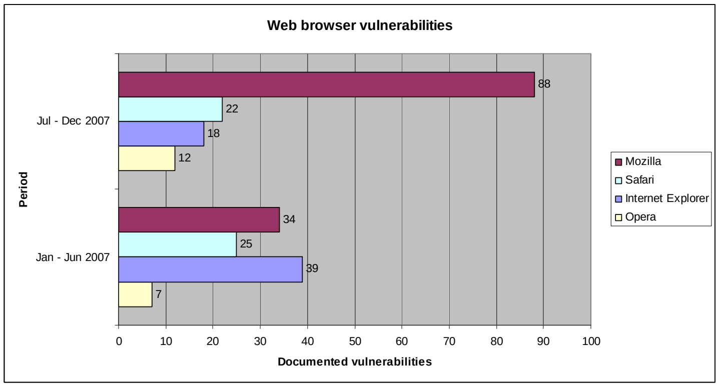


symantec.

Confidence in a connected world.

Web Attacks: The New Epicenter

Web browsers: many holes

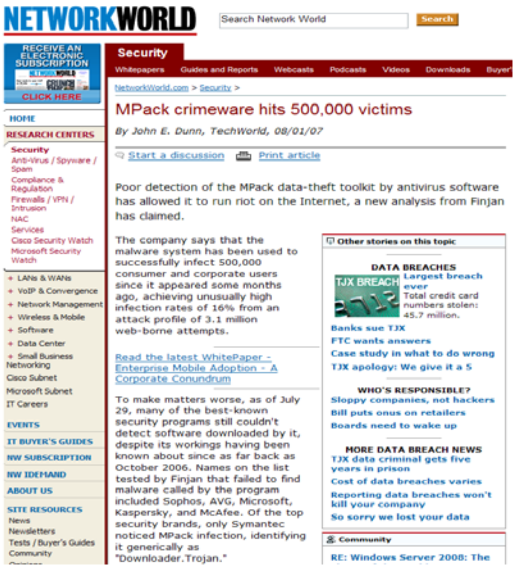


- In H2 2007, 88 vulnerabilities (19 medium, 69 low) affected Mozilla browsers (↑ from 34)
- Safari (1 high, 12 medium, 9 low); IE (13 medium, 5 low); Opera (8 medium, 4 low)
- 239 Browser plug-in vulns (190 affected ActiveX, 19 QuickTime, 13 Sun Java, 11 Adobe Flash, 4 Windows Media Player, 1 Adobe Acrobat, 1 Mozilla browser extension)

MPack: Malware Commoditized

- MPack: web attack toolkit that appeared late ’06;
- Toolkit is hosted on a web server and infects pages on that server
- Page visitors get infected

- Customized: Toolkit determines exploit method on the fly based on user’s configuration (operating system, browser, etc)
- Easy to use: management console provides stats on infection rates
- Customer care: toolkit can be purchased with one-year support contract!



MPack crimeware hits 500,000 victims

By John E. Dunn, TechWorld, 08/01/07

Poor detection of the MPack data-theft toolkit by antivirus software has allowed it to run riot on the Internet, a new analysis from Finjan has claimed.

The company says that the malware system has been used to successfully infect 500,000 consumer and corporate users since it appeared some months ago, achieving unusually high infection rates of 16% from an attack profile of 3.1 million web-borne attempts.

Read the latest WhitePaper - Enterprise Mobile Adoption - A Corporate Conundrum

To make matters worse, as of July 29, many of the best-known security programs still couldn't detect software downloaded by it, despite its workings having been known about since as far back as October 2006. Names on the list tested by Finjan that failed to find malware called by the program included Sophos, AVG, Microsoft, Kaspersky, and McAfee. Of the top security brands, only Symantec noticed MPack infection, identifying it generically as "Downloader.Trojan."

Other stories on this topic

DATA BREACHES

Largest breach ever

Total credit card numbers stolen: 45.7 million.

Banks sue TJX

FTC wants answers

Case study in what to do wrong

TJX apology: We give it a 5

WHO'S RESPONSIBLE?

Sloppy companies, not hackers

Bill puts onus on retailers

Boards need to wake up

MORE DATA BREACH NEWS

TJX data criminal gets five years in prison

Cost of data breaches varies

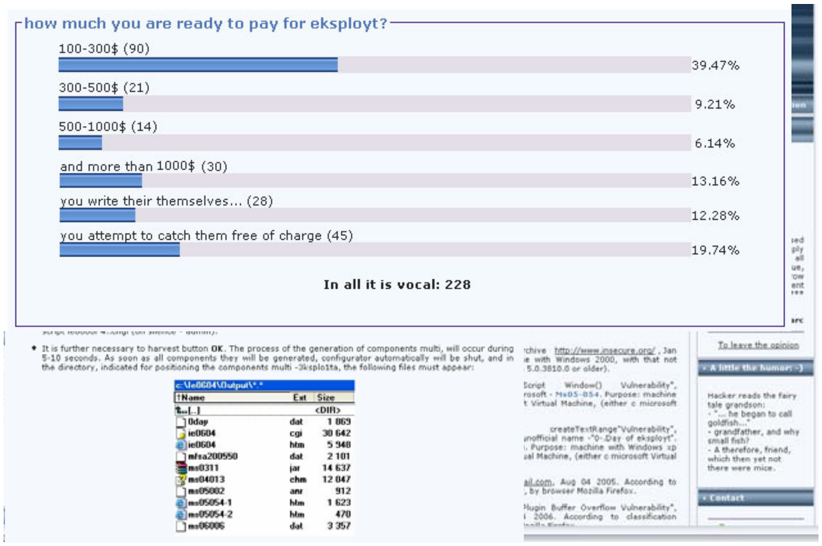
Reporting data breaches won't kill your company

So sorry we lost your data

Community

RE: Windows Server 2008: The

Web Attacker: Automated Tools Make it Easy



how much you are ready to pay for eksployt?

100-300$ (90)	39.47%
300-500$ (21)	9.21%
500-1000$ (14)	6.14%
and more than 1000$ (30)	13.16%
you write their themselves... (28)	12.28%
you attempt to catch them free of charge (45)	19.74%

In all it is vocal: 228

- It is further necessary to harvest button **OK**. The process of the generation of components multi, will occur during 5-10 seconds. As soon as all components they will be generated, configurator automatically will be shut, and in the directory, indicated for positioning the components multi -3ksplo1ta, the following files must appear:

```
c:\ie0604\Output\*.*
↑Name            Ext   Size
[..]                  <DIR>
0day             dat   1 069
ie0604           cgi  30 642
ie0604           htm   5 948
mfsa200550       dat   2 101
ms0311           jar  14 637
ms04013          chm  12 047
ms05002          anr     912
ms05054-1        htm   1 623
ms05054-2        htm     470
ms06006          dat   3 357
```

rchive http://www.insecure.org/ , Jan
e with Windows 2000, with that not
5.0.3810.0 or older).

Script Window() Vulnerability",
rosoft - Ms05-054. Purpose: machine
t Virtual Machine, (either c microsoft

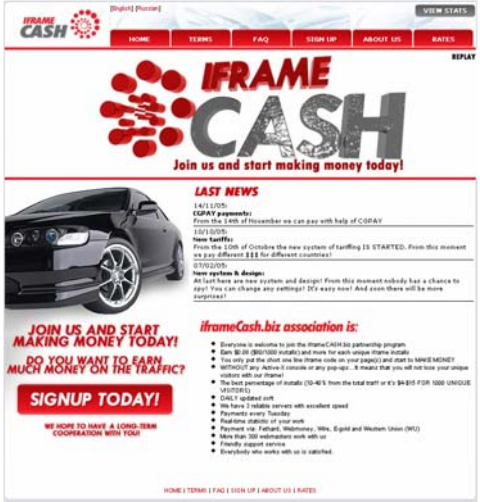
createTextRange"Vulnerability",
unofficial name -"0-.Day of eksployt".
. Purpose: machine with Windows xp
ual Machine, (either c microsoft Virtual

ail.com, Aug 04 2005. According to
, by browser Mozilla Firefox.

Plugin Buffer Overflow Vulnerability",
2006. According to classification

Hacker reads the fairy tale grandson:
- "... he began to call goldfish..."
- grandfather, and why small fish?
- A therefore, friend, which then yet not there were mice.

Making $$$ By Exploiting Browsers: Rogue Affiliate Programs



IFRAME CASH
[English] [Russian]
VIEW STATS
HOME
TERMS
FAQ
SIGN UP
ABOUT US
RATES
REPLAY
IFRAME CASH
Join us and start making money today!
JOIN US AND START MAKING MONEY TODAY!
DO YOU WANT TO EARN MUCH MONEY ON THE TRAFFIC?
SIGNUP TODAY!
WE HOPE TO HAVE A LONG-TERM COOPERATION WITH YOU!
HOME | TERMS | FAQ | SIGN UP | ABOUT US | RATES

LAST NEWS

14/11/05:
CGPAY payments:
From the 14th of November we can pay with help of CGPAY

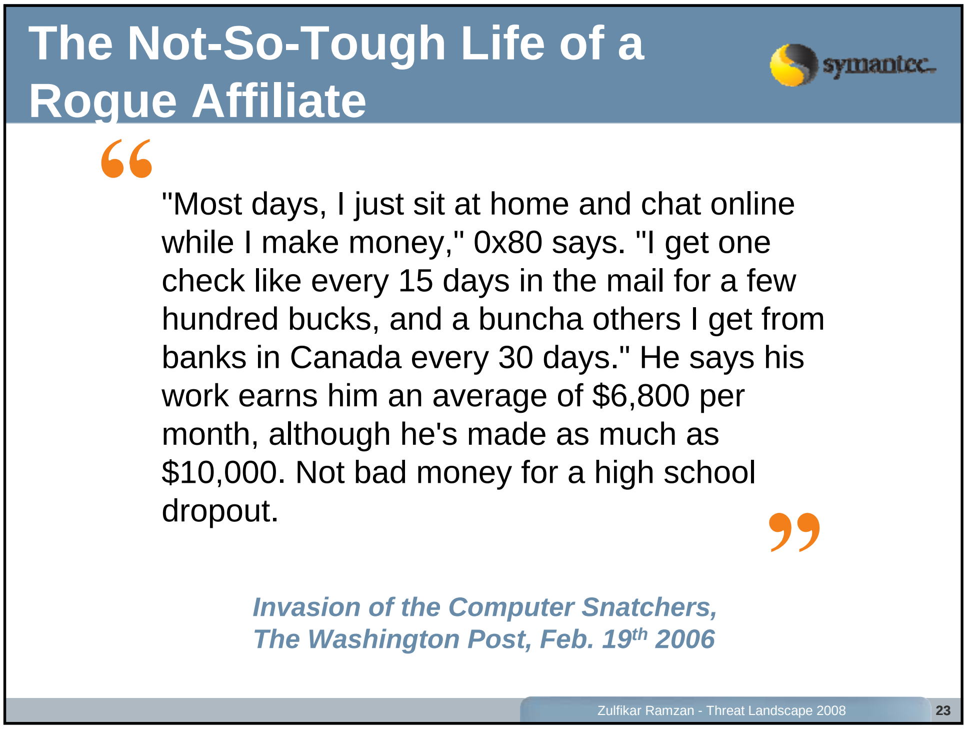
10/10/05:
New tariffs:
From the 10th of Octobre the new system of tariffing IS STARTED. From this moment we pay different $$$ for different countries!

07/02/05:
New system & design:
At last here are new system and design! From this moment nobody has a chance to spy! You can change any settings! It's easy now! And soon there will be more surprises!

iframeCash.biz association is:

- Everyone is welcome to join the iframeCASH.biz partnership program
- Earn $0.08 ($80/1000 installs) and more for each unique iframe installs
- You only put the short one line iframe code on your page(s) and start to MAKE MONEY
- WITHOUT any Active-X console or any pop-ups... it means that you will not lose your unique visitors with our iframe!
- The best percentage of installs (10-40% from the total traff or it's $4-$15 FOR 1000 UNIQUE VISITORS)
- DAILY updated soft
- We have 3 reliable servers with excellent speed
- Payments every Tuesday
- Real-time statistic of your work
- Payment via: Fethard, Webmoney, Wire, E-gold and Western Union (WU)
- More than 300 webmasters work with us
- Friendly support service
- Everybody who works with us is satisfied.

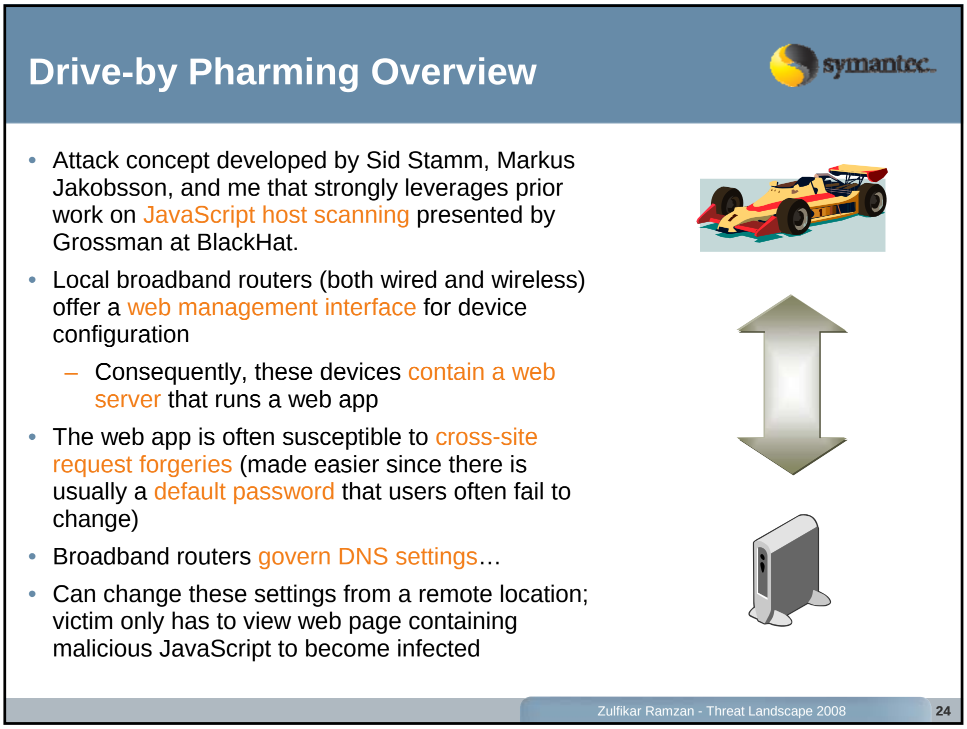
- Rogue distribution networks make money by using browser exploits to install downloader Trojan horse programs
- The downloaders are then used to install adware & spyware
- Reportedly pay for 0-day vulnerabilities such as WMF
- WMF vulnerability said to be purchased for ~$4K USD
- Discovered in active exploit via iframecash.biz & others



The Not-So-Tough Life of a Rogue Affiliate

> "Most days, I just sit at home and chat online while I make money," 0x80 says. "I get one check like every 15 days in the mail for a few hundred bucks, and a buncha others I get from banks in Canada every 30 days." He says his work earns him an average of $6,800 per month, although he's made as much as $10,000. Not bad money for a high school dropout.

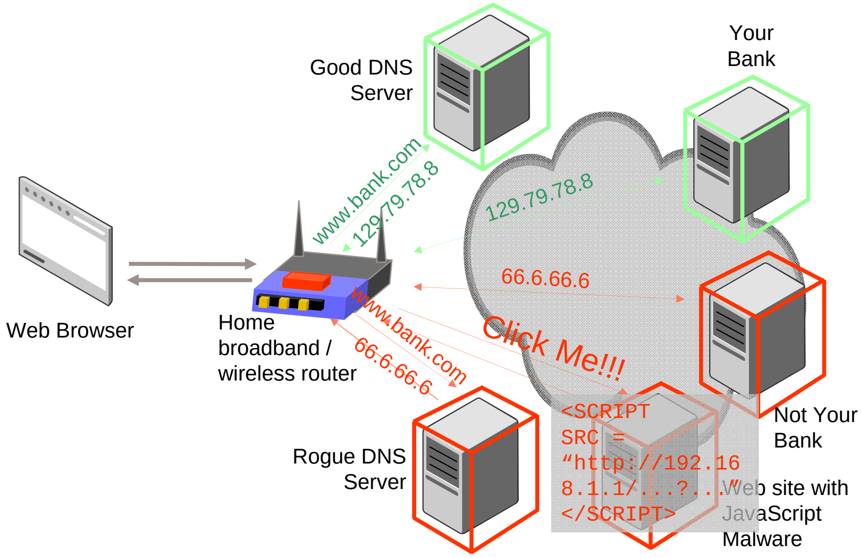
Invasion of the Computer Snatchers,
The Washington Post, Feb. 19th 2006



Drive-by Pharming Overview

- Attack concept developed by Sid Stamm, Markus Jakobsson, and me that strongly leverages prior work on JavaScript host scanning presented by Grossman at BlackHat.
- Local broadband routers (both wired and wireless) offer a web management interface for device configuration
  - Consequently, these devices contain a web server that runs a web app
- The web app is often susceptible to cross-site request forgeries (made easier since there is usually a default password that users often fail to change)
- Broadband routers govern DNS settings…
- Can change these settings from a remote location; victim only has to view web page containing malicious JavaScript to become infected

Drive-by Pharming Flow

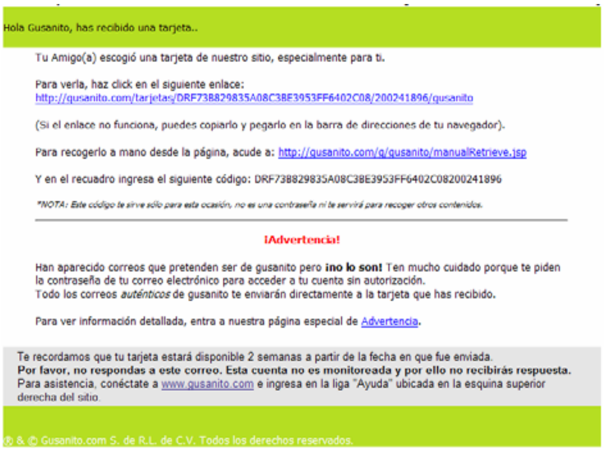


Drive-by Pharming In the Wild

- Used an HTML IMG Tag (No JavaScript!)
- Took advantage of virtual hostnames (no need to guess router's IP)
- Exploited router used by large Mexican ISP to pharm Mexican bank
- Added DNS entries directly (no separate DNS server needed!)
- Router was particularly susceptible to Drive-by Pharming since admin password not required to change router settings.

Attacks always get better; they never get worse

Old US National Security Agency Saying



Hola Gusanito, has recibido una tarjeta..

Tu Amigo(a) escogió una tarjeta de nuestro sitio, especialmente para ti.

Para verla, haz click en el siguiente enlace:
http://gusanito.com/tarjetas/DRF73B829835A08C3BE3953FF6402C08/200241896/gusanito

(Si el enlace no funciona, puedes copiarlo y pegarlo en la barra de direcciones de tu navegador).

Para recogerlo a mano desde la página, acude a: http://gusanito.com/g/gusanito/manualRetrieve.jsp

Y en el recuadro ingresa el siguiente código: DRF73B829835A08C3BE3953FF6402C08200241896

**NOTA: Este código te sirve sólo para esta ocasión, no es una contraseña ni te servirá para recoger otros contenidos.*

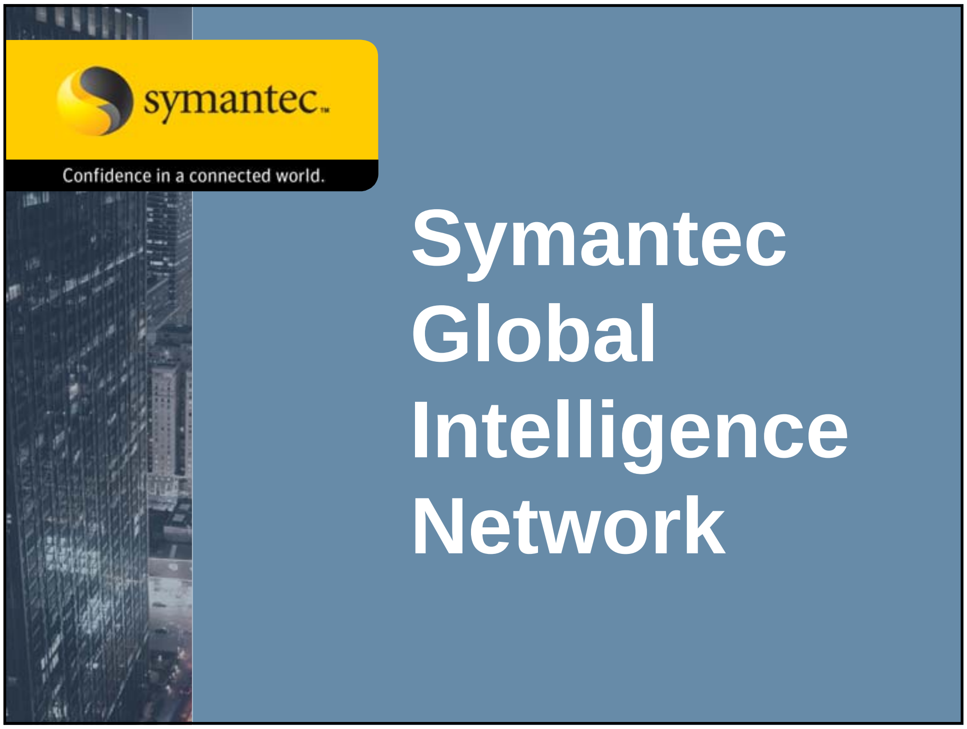
¡Advertencia!

Han aparecido correos que pretenden ser de gusanito pero **¡no lo son!** Ten mucho cuidado porque te piden la contraseña de tu correo electrónico para acceder a tu cuenta sin autorización.
Todo los correos *auténticos* de gusanito te enviarán directamente a la tarjeta que has recibido.

Para ver información detallada, entra a nuestra página especial de Advertencia.

Te recordamos que tu tarjeta estará disponible 2 semanas a partir de la fecha en que fue enviada.
Por favor, no respondas a este correo. Esta cuenta no es monitoreada y por ello no recibirás respuesta.
Para asistencia, conéctate a www.gusanito.com e ingresa en la liga "Ayuda" ubicada en la esquina superior derecha del sitio.

® & © Gusanito.com S. de R.L. de C.V. Todos los derechos reservados.



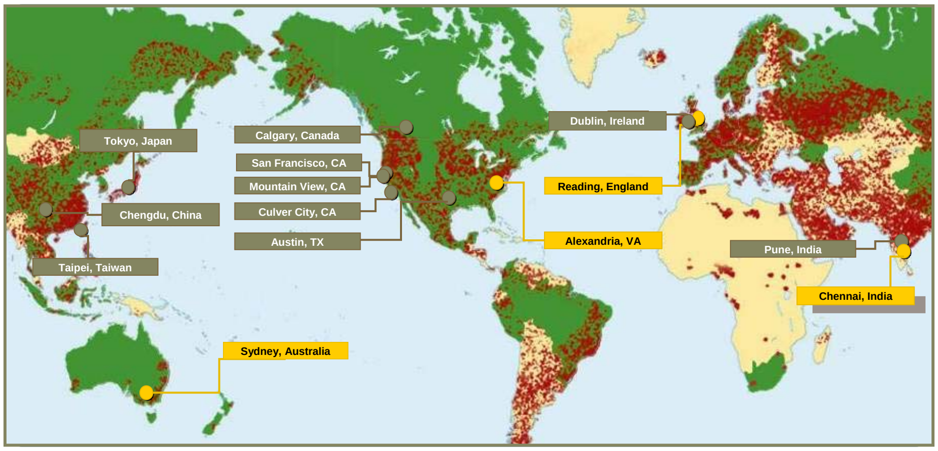
Confidence in a connected world.

Symantec Global Intelligence Network

Symantec™ Global Intelligence Network

4 Symantec SOCs	80 Symantec Monitored Countries	40,000+ Registered Sensors in 180+ Countries	11 Symantec Security Response Centers

> 7,000 Managed Security Devices + 120 Million Systems Worldwide + 2Million Probe Network + Advanced Honeypot Network



What Information does the GIN Contain?

The Global Intelligence Network contains several key types of information about Internet-based threats:

- Attack Intelligence
- Malicious Code and Security Risk Intelligence
- Fraud Intelligence
- Vulnerability Intelligence
- Exposure Intelligence

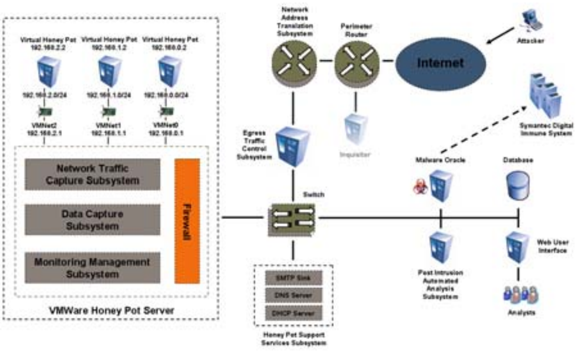
The various types of intelligence both come from and power many of Symantec’s products

GIN Production Information Sources

Where does the intelligence come from?

The Global Intelligence Network is comprised of information collected from a number of sources, both internal and external. The internal sources are a combination of customer-facing and Symantec-internal products and services:

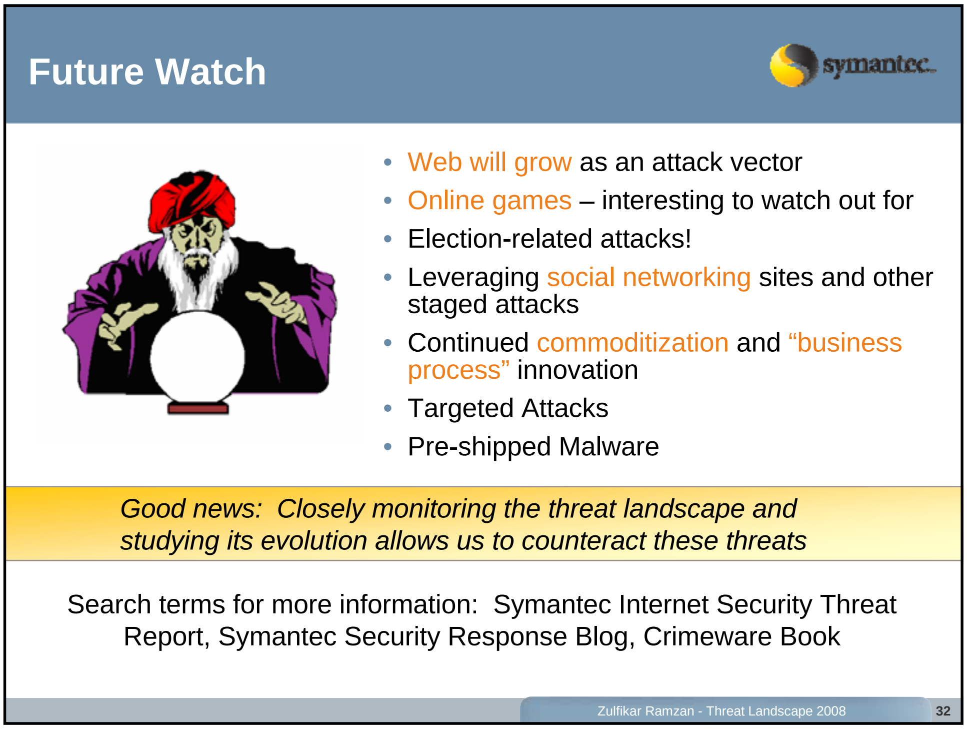
- Norton AntiVirus (NAV)
- Norton Internet Security (NIS)
- Norton 360 (N360)
- Norton Confidence Online (NCO)
- Symantec Endpoint Protection
- DeepSight
- Symantec Honeypots (AQS)
- Brightmail Anti-Spam
- Phish Report Network (PRN)
- Internal Research Projects
- Managed Threat Analysis (MTA)
- Managed Security Services.


Virtual Honey Pot 192.168.2.2
Virtual Honey Pot 192.168.1.2
Virtual Honey Pot 192.168.0.2
192.168.2.0/24
192.168.1.0/24
192.168.0.0/24
VMNet2 192.168.2.1
VMNet1 192.168.1.1
VMNet0 192.168.0.1
Network Traffic Capture Subsystem
Data Capture Subsystem
Monitoring Management Subsystem
Firewall
VMWare Honey Pot Server
Network Address Translation Subsystem
Perimeter Router
Internet
Attacker
Symantec Digital Immune System
Egress Traffic Control Subsystem
Inquisitor
Malware Oracle
Database
Switch
Web User Interface
Post Intrusion Automated Analysis Subsystem
Analysts
SMTP Sink
DNS Server
DHCP Server
Honey Pot Support Services Subsystem

symantec.

Confidence in a connected world.

The Road Ahead

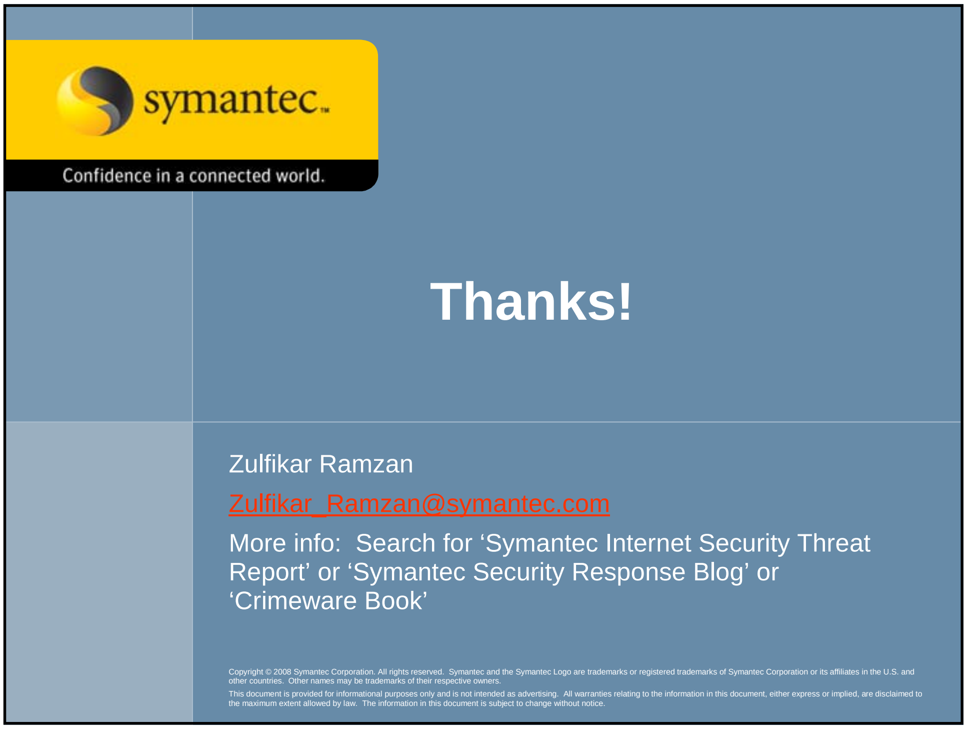


Future Watch

- Web will grow as an attack vector
- Online games – interesting to watch out for
- Election-related attacks!
- Leveraging social networking sites and other staged attacks
- Continued commoditization and “business process” innovation
- Targeted Attacks
- Pre-shipped Malware

Good news: Closely monitoring the threat landscape and studying its evolution allows us to counteract these threats

Search terms for more information: Symantec Internet Security Threat Report, Symantec Security Response Blog, Crimeware Book



Confidence in a connected world.

Thanks!

Zulfikar Ramzan

Zulfikar_Ramzan@symantec.com

More info: Search for 'Symantec Internet Security Threat Report' or 'Symantec Security Response Blog' or 'Crimeware Book'

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.