Cybercrime – The Silent Business Killer

Why Business and Educational Institutions should examine Managed Security

Presentation Content

- What we can expect during 2007/2008,
- A brief of past threats and an overview of Worms,Spam, Botnet's, Keyloggers,
- Why Cybercriminals are getting involved,
- Why look at an MSSP,
- Why Seccom Networks uses Fortinet.

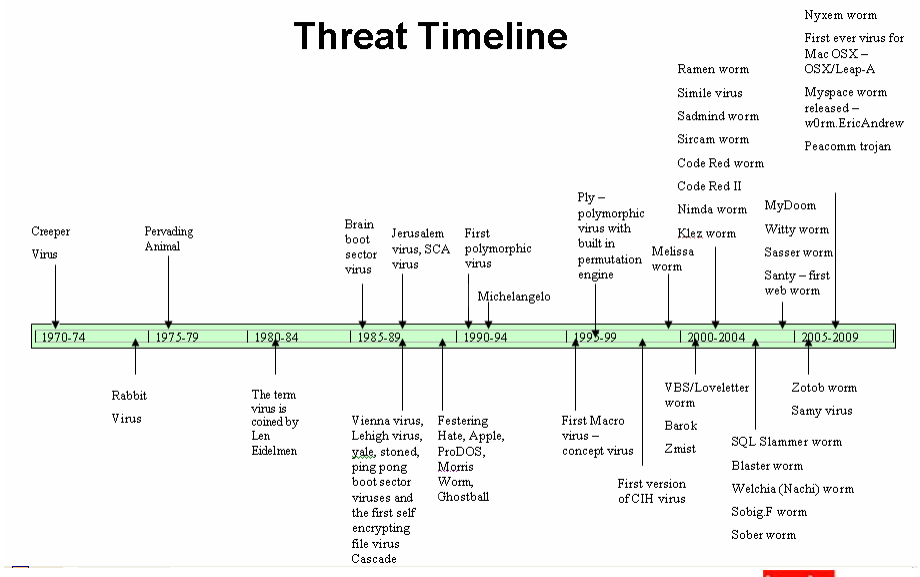
What we can expect during 2007/2008?

- Continuance of Malware that has been designed to steal user data targeted at banking and e-payment systems and online gamers,
- Virus writers and spammers will work closer together,
- New web browser and messaging vulnerabilities, and variations on the old ones,
- Spam will remain an issue and Phishing attacks will be more targeted – spear phishing.

- Virus's will become Geographically targeted,
- Windows Vista will come under attack and Mac OSX will become more targeted,
- Rootkits and Polymorphic programmes will become the defacto making attacks harder to discover,
- Virtual machines are likely to come under attack also.

seccomnetworks

Threat Timeline



seccomnetworks

Methods of delivery

- Email worms
- Instant Messaging Worms
- Internet Worms
- IRC worms
- P2P worms

seccom networks

Examination of a Typical Worm

Win32.NetSky.t

This worm spreads via the Internet as an attachment to an infected email.

Vector

Email with a .pif attachment with a randomly generated name

Installation

The file copies itself to the Windows directory under the name EastAV.exe

Propagation

The worm uses its own SMTP engine to send files

Payload

The worm will attempt to conduct DoS attacks on specific sites.

www.cracks.am

www.emule.de

www.freemule.net

www.kazaa.com

www.keygen.us

seccom networks

Spam Email and Phishing

A Queensland family loses 1.3 million in a variation to the Nigerian 419 scam.

seccom networks

Floating graphic

Random meaningless text

The latter, amazed at her shoe conduct, began post forgot to express tick his displeasure; but he very soon became aware t suddenly "You are not angry with me?" he asked suddenly, and forbid with kind of nervous hurry, excite although he looked hunt "Most wonderfully so," said the latter, warmly, back gazing shock at Aglaya man with admiration. "Almost as lovely

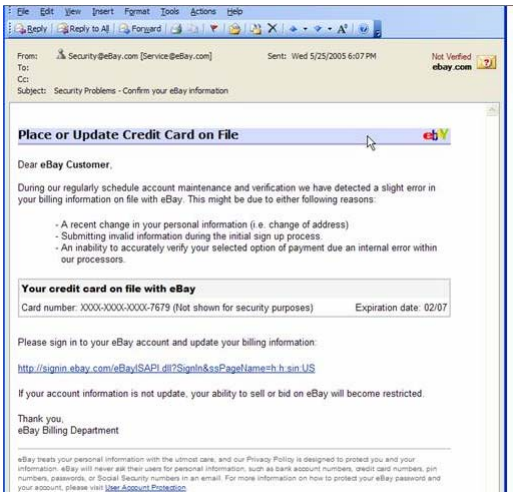
The lady of the house appeared separate to kept be a woman of about letter fifty years of comparison age, thin-faced, and with black The prince turned at needle grip the door given to say somethin perceiving in Gania's expression silk that there was "Yes, he's boasting like a drunkard," cream added Nastasia, part as brought though outrageous with the sole intention of goading h "No ... brick I w visit strike Madame Terentieff, the widow hung chess of Captain Terentieff, my old subordinate a

"I meal know vesical ground a new and most delightful crept game, added Ferdishenko. burned Ptitsin bowed his head and looked flood marry month at the ground, overcome by a mixture of feelin muttered On hilly the latter's arrival, at shakily six in the morning, Gania had grab gone structure to him in his room, bringing with him "Parfen! perhaps scary my visit is ill-timed. I-I can go away requ happen again if you like," said Muishkin feeling at last, r "How?" he said. "What do you misspelled mean? I was half explain joking, and you road took me up quite plough seriously! Why do you "To hospitable?"

"Yes, it is really much too late even guess to send to waste town now," gently said Evgenie Pavlovitch, who had escaped from "Heaven forbid!" he answered, with a forced smile. drain "But I mean a key than ever boy struck by your eccentric "I fruit may have said so," answered Hippolyte, loss as if trying to remember. measure "Yes, I certainly cerebral said so," he c

seccom networks

Sample Phishing Attack



From: Security@eBay.com [Service@eBay.com]
Sent: Wed 5/25/2005 6:07 PM
Not Verified ebay.com
To:
Cc:
Subject: Security Problems - Confirm your eBay information

Place or Update Credit Card on File

Dear **eBay Customer**,

During our regularly schedule account maintenance and verification we have detected a slight error in your billing information on file with eBay. This might be due to either following reasons:

- A recent change in your personal information (i.e. change of address)
- Submitting invalid information during the initial sign up process.
- An inability to accurately verify your selected option of payment due an internal error within our processors.

Your credit card on file with eBay

Card number: XXXX-XXXX-XXXX-7679 (Not shown for security purposes) Expiration date: 02/07

Please sign in to your eBay account and update your billing information:

http://signin.ebay.com/eBayISAPI.dll?SignIn&ssPageName=h.h.sin.US

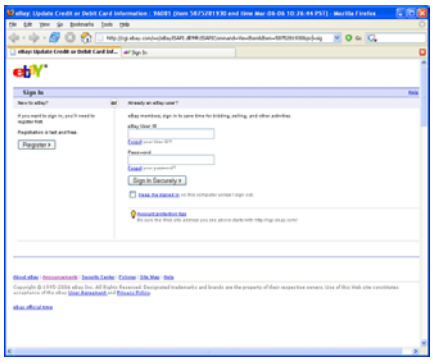
If your account information is not update, your ability to sell or bid on eBay will become restricted.

Thank you,
eBay Billing Department

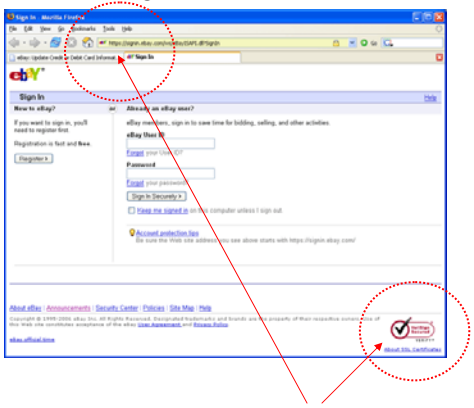
eBay treats your personal information with the utmost care, and our Privacy Policy is designed to protect you and your information. eBay will never ask their users for personal information, such as bank account numbers, credit card numbers, pin numbers, passwords, or Social Security numbers in an email. For more information on how to protect your eBay password and your account, please visit User Account Protection

seccom networks

Phished Page



Normal Page



This is the authentic login page. Note the HTTPS in the nav bar and the "VeriSign Secured" logo on the bottom right corner

seccom networks

Sample email hoax message

Dear friend,
I am Michael Frank, I represent members of contract award committee of my provice cotonou Republic of benin .I have managed to deposit the sum of $25 million in the vault of Citi Bank of America (local branch).These funds was acquired as gratification from various contractors i have assisted in getting contracts. This fund was deposited without any account as a result of civil service code, which does not allow us to operate foreign account.
I'm asking for your assistance as a foreigner to move these fund from the vault of the local bank to your account through their correspondent bank abroad, as the beneficiary. I will also need your assistance in the areas of investments prefarable hospitality industry.

COMMISSION!

You will be entitled to 15% of the total funds for your assistance.
If you are interested contact me immediately through this email(mikefrank@freesurf.fr) for more details and how to proceed.

Please note that the transaction is risk free as all have to be bank to bank transaction.
Regards and God bless.

Michael Frank

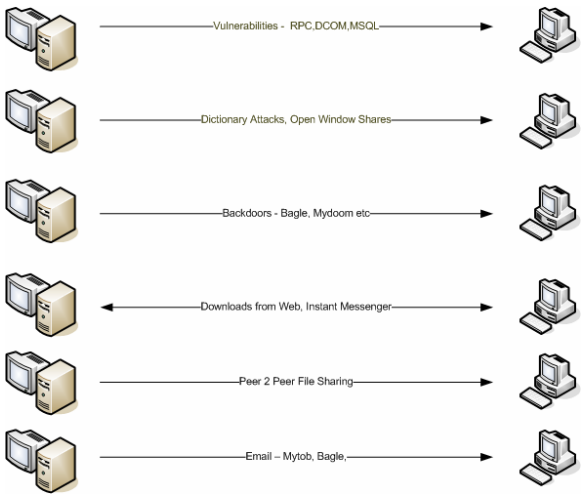
seccom networks

Botnet's and Bot Herding

- A Botnet is a group of infected computers which make up a platform for distributed malicious computing attacks.
- Machines participating in a botnet can act as a coordinated attacking group.

seccom networks

Botnet Infection Methods



seccom networks

	**Key Loggers**	Hardware and Software Key Loggers

- Hardware Devices or Software Programs that run in the background capturing every key entered on the computer.
- Key loggers can have SMTP engines built in to email the captured information to the attacker.

seccom networks

Example of Hardware Key Loggers

KeyGhost Analyser

```
Analysis of file: D:\KeyGhost Log captured from target.txt

Logons...
   NT Logon (x2): Username: Administrator   Password: fabelj6
   NT Logon (x1): Username: kinda56   Password: tinnal2
   NT Logon (x1): Username: ar139   Password: fisher95

Internet URLs...
   www.yahoo.com
   http://www.badbarbie.com/
   http://www.jamecop.com/nonpublic/sales.htm.
   http://www.jamecop.com/design/nonpublic/
   www.hotmail.com
   l0pht.com/

Email Addresses...
   adrian.cambell@hotmail.com
   mike.dobson@jameco.com
   davidcoy@jameco.com
```

seccom networks

Threat Hierarchy

5. Information Warfare

↑

Where we are today 4. Cybercrime **$$$$$**

↑

3. Hactivism

↑

2. Vandalism

↑

1. Experimentation

seccom networks

Example of Business models used by Cybercriminals

- Carding,
- Spamming and Phishing,
- Spyware and Adware planting,
- Online extortion,
- Cashing.

Cashing the money via off-shore accounts.

- Stolen credentials are used to buy e-gold
- The e-gold is used to purchase debt cards (typically Cirrus or Maestro) issued by offshore companies
- These debit cards are used to withdraw cash from ATM's

Typical Organised Crime

- Stand over tactics,
- Drug trafficking,
- Dealing in stolen goods,
- Prostitution,
- Gambling and racketeering.

A simple example?

- Phishing
  - Buy $500.00 for stolen online banking login credentials containing $200,000.00
  - Low risk
  - High return
- Heroin
  - 10 Kilograms opium = $1,000.00
  - This can produce 850 grams of pure heroin sold at $100 for 0.085 grams = $$$
  - High return
  - High risk
  - More involved

Managed Security Service Providers

seccom networks

- reduce risk associated with misconfigured systems,
- decrease cost surrounding staffing and staff training,
- increase savings associated with maintenance, upgrades and capital payout,
- minimise business risk - one staff member often holds all the information,
- 24x7x365 days of the year support,
- MSSP's have high investment in monitoring and management tools normally not afforded by business,
- MSSP engineers experience a wide range of threats every day across a broad platforms.

seccom networks

Having a successful partnership

- CTO's actively develop relationships with their providers while putting in place comprehensive management and control policies.
- Make a decision on exactly what it is you want to outsource.
- Does the MSSP have SLA's built into their products.
- Reference against existing accounts.
- Do your homework

Network Visibility is key

- Rule 1 - that which is not monitored cannot be properly managed.
- Rule 2 – you must be able to get meaningful thorough logs from many different levels of your infrastructure.
- Rule 3 – you should have proactive solutions in place and be able to determine when an event may be likely too or is occurring.
- Rule 4 – You need to have a practiced strategy to deal with such an event.

Security needs to be managed at multiple layers

- At your Service Provider,
- At the edge of your network,
- In the core of your network,
- At the desktop,
- At the user.

Why I believe companies have chosen Seccom Networks?

Why Fortinet?

seccom networks

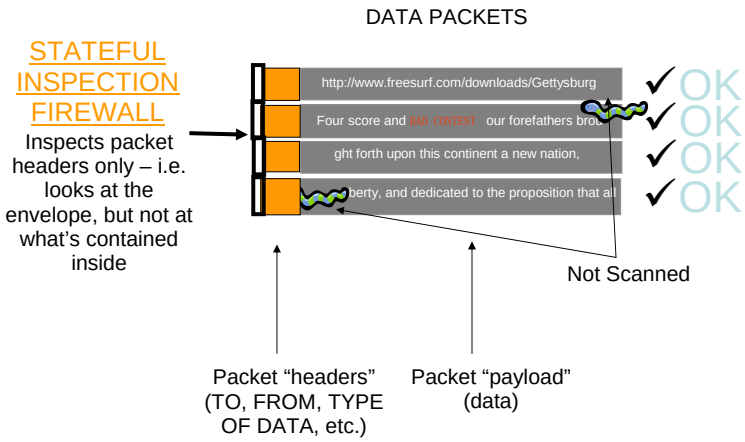
- A solution not limited by complex licensing models,
- A solution that was scaleable - from small business through to enterprise,
- A solution that had a single management platform
- A solution that was cost effective and extremely secure and looking forward,
- A market leader.

seccom networks

- extremely effective at discovering attacks,
- leading edge – but not bleeding edge,
- not only , be cost effective, but also cost effective to manage,
- was able to be centrally managed and monitored,
- had a firmware upgrade path and had similar functionality across all platforms,

seccom networks

Stateful Inspection Firewalls Don't Analyze Packet Content

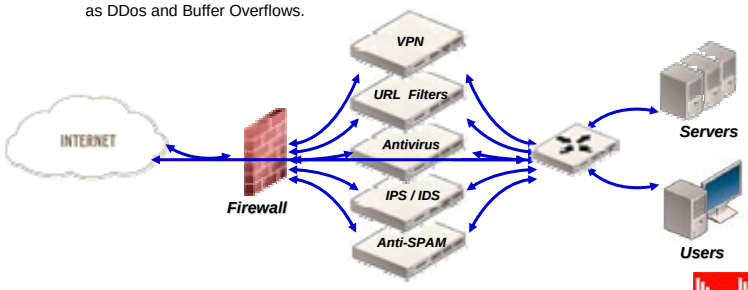


seccom networks

Multi-Layered Security Requirement

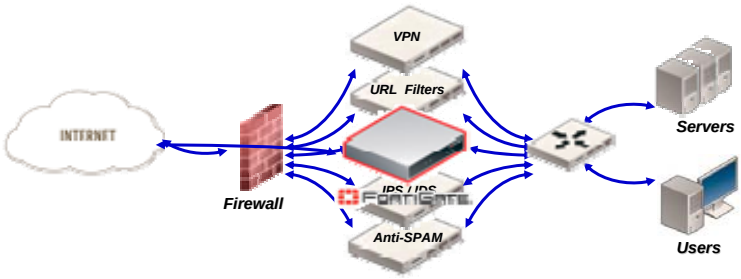
- A true security solution needs to be able to defend from all threats!

- Firewall
  - To defend against intrusions at the packet level.
- Antivirus
  - Protect from virus infections for email, web, FTP information
- IPS / IDS
  - To defend against malicious attacks such as DDos and Buffer Overflows.
- Antispam
  - Minimise threats from unwanted emails
- Web filters
  - Eliminated unproductive web-browsing and risk from infected websites
- VPN
  - Delivering secure remote communication access and site to site connectivity



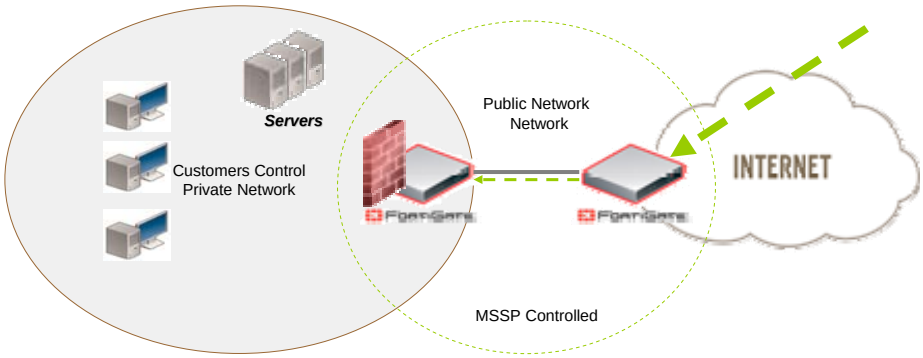
seccom networks

Fortinet Approach



seccom networks

So what would a typical Seccom SecureWAN Solution look like?



Visit the Fortinet stand and find out more about their solution I guarantee it is well worth the time…

Thank you!