

Intelligence Led Corporate Security Programs

Why a Business Needs to Setup a Cyber Threat
Analysis Unit

Ian Cook

16th Annual Computer
Security
Incident Handling
Conference
Budapest, Hungary
June 13-18, 2004



How Much Security?

- The most critical question that security managers ask is how should they allocate the limited resources.
 - Where are the threats?
 - How much security is needed?
 - How much residual risk?
 - Where is the balance?
- A Cyber Intelligence Program based on proven Government Intelligence processes can help answer these questions

The Game Has Changed

Increased risk

Cyberspace is rapidly growing and has become part of the way we conduct our lives. Accelerating number of new threats and vulnerabilities that appear faster than vendors can fix and patches can be deployed. There is no Perimeter

Increased complexity

Technologies have grown increasing complex so that all the ways systems could be compromised by an attacker cannot be predicted.

Constant change

Networks, business requirements and risks continuously change and degrade security. Behavior banned today is promoted tomorrow

Information volume

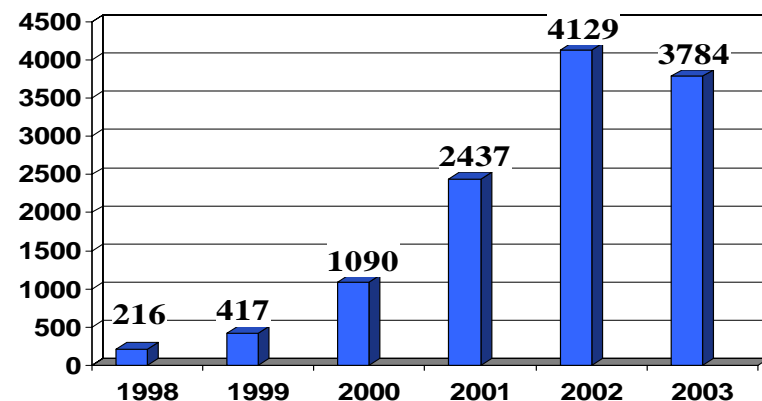
Daily volume of security information and intelligence is greater than most organizations can effectively process and analyze

Limited expertise

Few companies have the necessary in-house security expertise. The enemy has become more sophisticated, organized and better resourced.

Time in Which to Make Decisions Decreasing

- Vulnerabilities Increasing
- Patches proliferating
- Days between Alert and exploit decreasing
 - Nimda 331 Days
 - Blaster 21 Days
 - Witty 36 Hours
- Time to Propagate decreasing
 - Code Red 5+ Days
 - Slammer 87 Minutes
 - Witty 45 Minutes
- Exploits are more sophisticated
- Speed of attacks results in widespread damage in little time



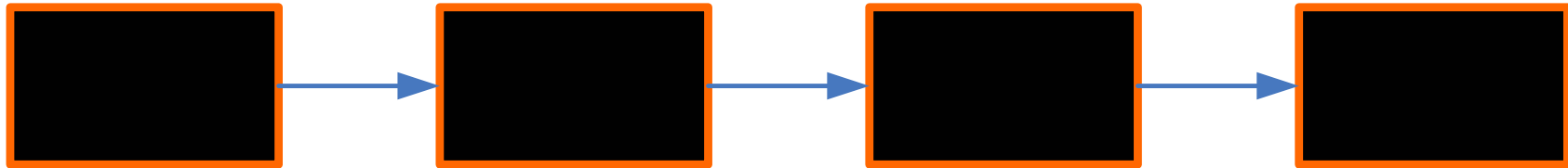
Source: CERT

Intelligence Led Decision Making

- Those making security related decisions have often been taking an uncoordinated, uninformed, and unplanned approach to security
- It's difficult to manage what you don't know about or understand *(Most Organizations spend less than \$250 for every \$1 million revenue on security.)*
- Security Decisions should be based on facts, not intuition
- An Intelligence Program will:
 - Identify the need for action
 - Provide the insight and context for deciding among courses of action (value added analysis)
 - Provide information/assessment on the effectiveness of pursuing the selected course of action

Intelligence Led Decision Making: Phishing

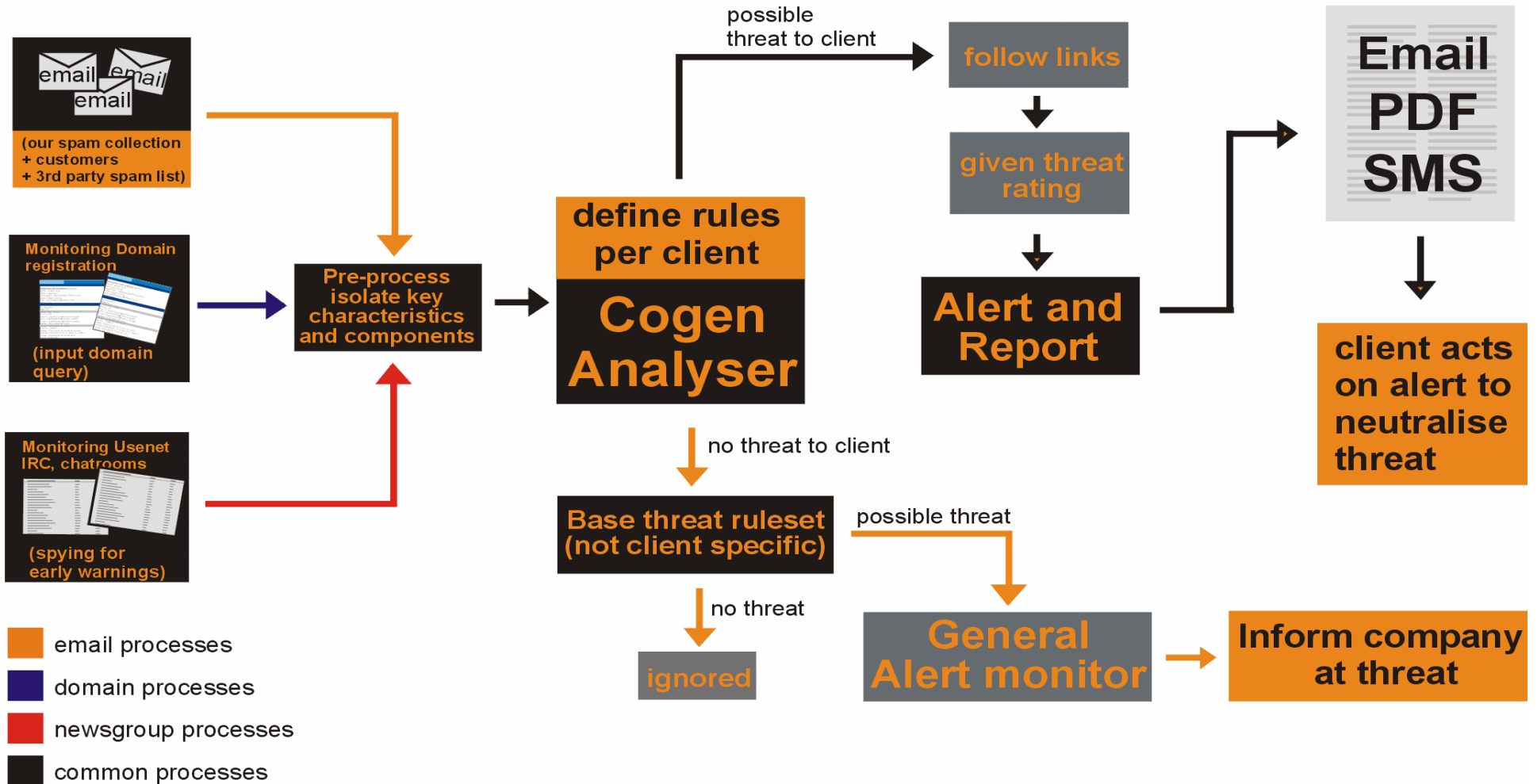
- Phishing Attack Stages



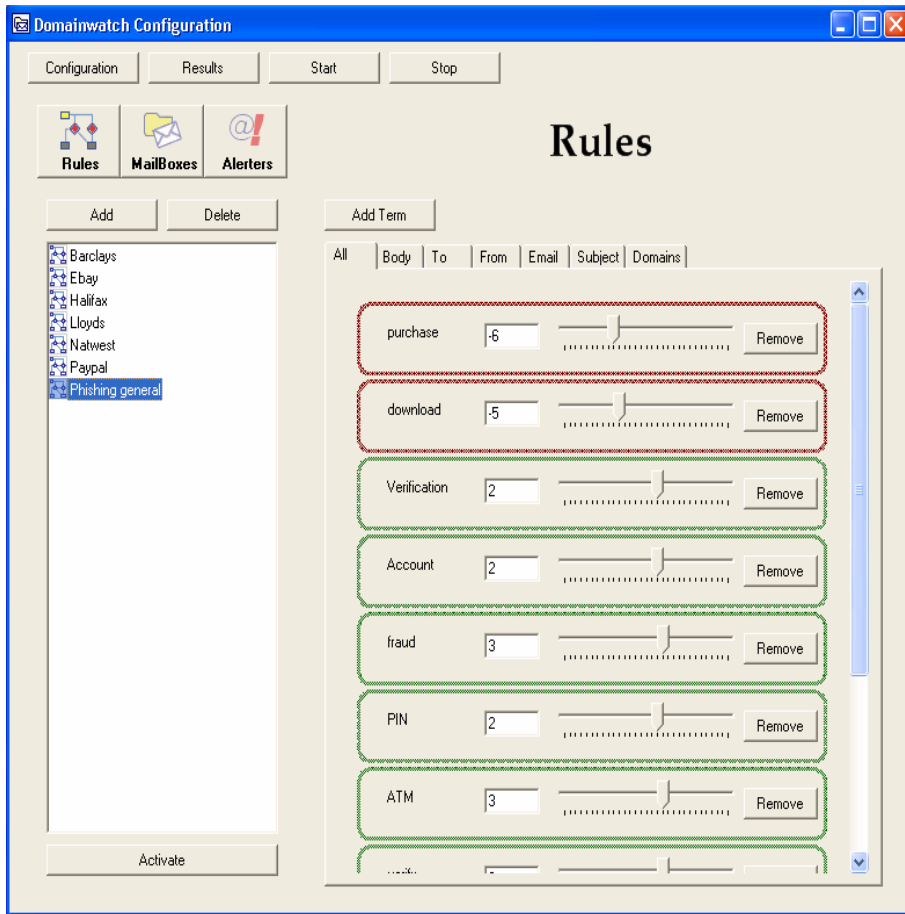
Monitor

- New Domains including Company name
- Sites containing Company name and requesting ID & Password
- Phishing emails containing Company name
- Seed fake sites with account details and monitor accounts

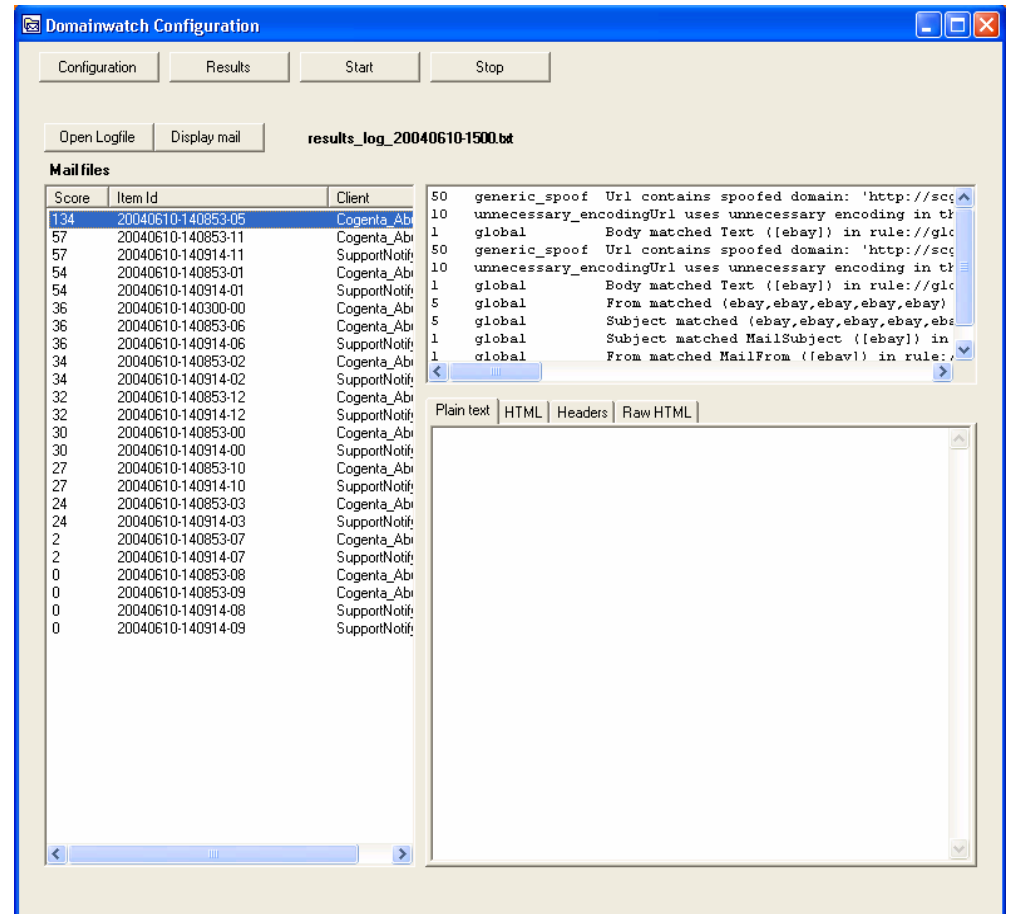
Anti Phishing Tool Workflow



Prototype Email Phishing Threat Analyzer



The screenshot shows the 'Rules' configuration window in Domainwatch. It features a sidebar with a tree view of domains including Barclays, Ebay, Halifax, Lloyds, Natwest, and Paypal. The main area is titled 'Rules' and contains a list of terms with their respective scores and 'Remove' buttons. The terms are: purchase (score 6), download (score 5), Verification (score 2), Account (score 2), fraud (score 3), PIN (score 2), and ATM (score 3). Each term has a slider control and a 'Remove' button. The window also has tabs for Configuration, Results, Start, and Stop, and buttons for Rules, Mailboxes, and Alerters.



The screenshot shows the 'Results' window in Domainwatch, displaying a log of email files. The window has tabs for Configuration, Results, Start, and Stop, and buttons for Open Logfile and Display mail. The log is titled 'results_log_20040610-1500.bt' and contains a table of mail files with columns for Score, Item Id, and Client. The table lists various items with scores ranging from 0 to 57. Below the table, there is a section for 'Mail files' with a list of log entries and a preview area for the selected item, showing 'Plain text', 'HTML', 'Headers', and 'Raw HTML' views.

Score	Item Id	Client
134	20040610-140853-05	Cogenta_Abi
57	20040610-140853-11	Cogenta_Abi
57	20040610-140914-11	SupportNotif
54	20040610-140853-01	Cogenta_Abi
54	20040610-140914-01	SupportNotif
36	20040610-140300-00	Cogenta_Abi
36	20040610-140853-06	Cogenta_Abi
36	20040610-140914-06	SupportNotif
34	20040610-140853-02	Cogenta_Abi
34	20040610-140914-02	SupportNotif
32	20040610-140853-12	Cogenta_Abi
32	20040610-140914-12	SupportNotif
30	20040610-140853-00	Cogenta_Abi
30	20040610-140914-00	SupportNotif
27	20040610-140853-10	Cogenta_Abi
27	20040610-140914-10	SupportNotif
24	20040610-140853-03	Cogenta_Abi
24	20040610-140914-03	SupportNotif
2	20040610-140853-07	Cogenta_Abi
2	20040610-140914-07	SupportNotif
0	20040610-140853-08	Cogenta_Abi
0	20040610-140853-09	Cogenta_Abi
0	20040610-140914-08	SupportNotif
0	20040610-140914-09	SupportNotif

Intelligence Defined

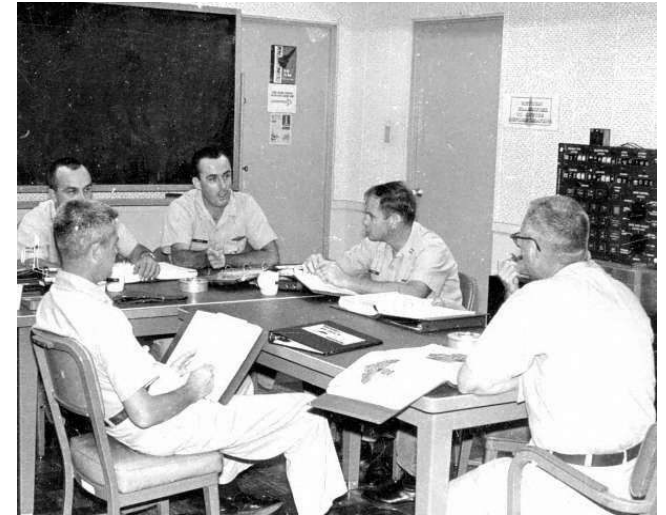
- Intelligence is the product that results or the knowledge that is derived from cyclical processing of information
United States Intelligence – An Encyclopaedia
- Cyber Intelligence is the systematic and broad-scale examination of Internet activity to assess, predict and understand current and prospective behaviors on the Internet.



Tenets of Intelligence

Intelligence must be:

- **Timely** - Late intelligence is as useless as no intelligence.
- **Accurate** – Must be unbiased and based on fact
- **Usable** – Understandable and specific to current need.
- **Complete** - Must identify all the adversary's capabilities, identify all available courses of action and forecast future adversary actions and intentions.
- **Relevant** - Must focus on current need.



Questions Decision Makers Ask

- Where are our weaknesses and vulnerabilities
- What threats/adversaries exist
- What tools/capabilities attackers have
- Who's targeting us and does it matter
- Which potential threats may be imminent
 - Are we vulnerable?
 - Are we an attractive Target
 - What impact might an attack have
- How do our Threats compare to those of our competitors
- What are our competitors doing
- What's being said about us and by whom
- What safeguards / countermeasures can we deploy
- What actions we should take

A Cyber Intelligence Program based on proven Government Intelligence processes can help answer these questions

Situational Awareness

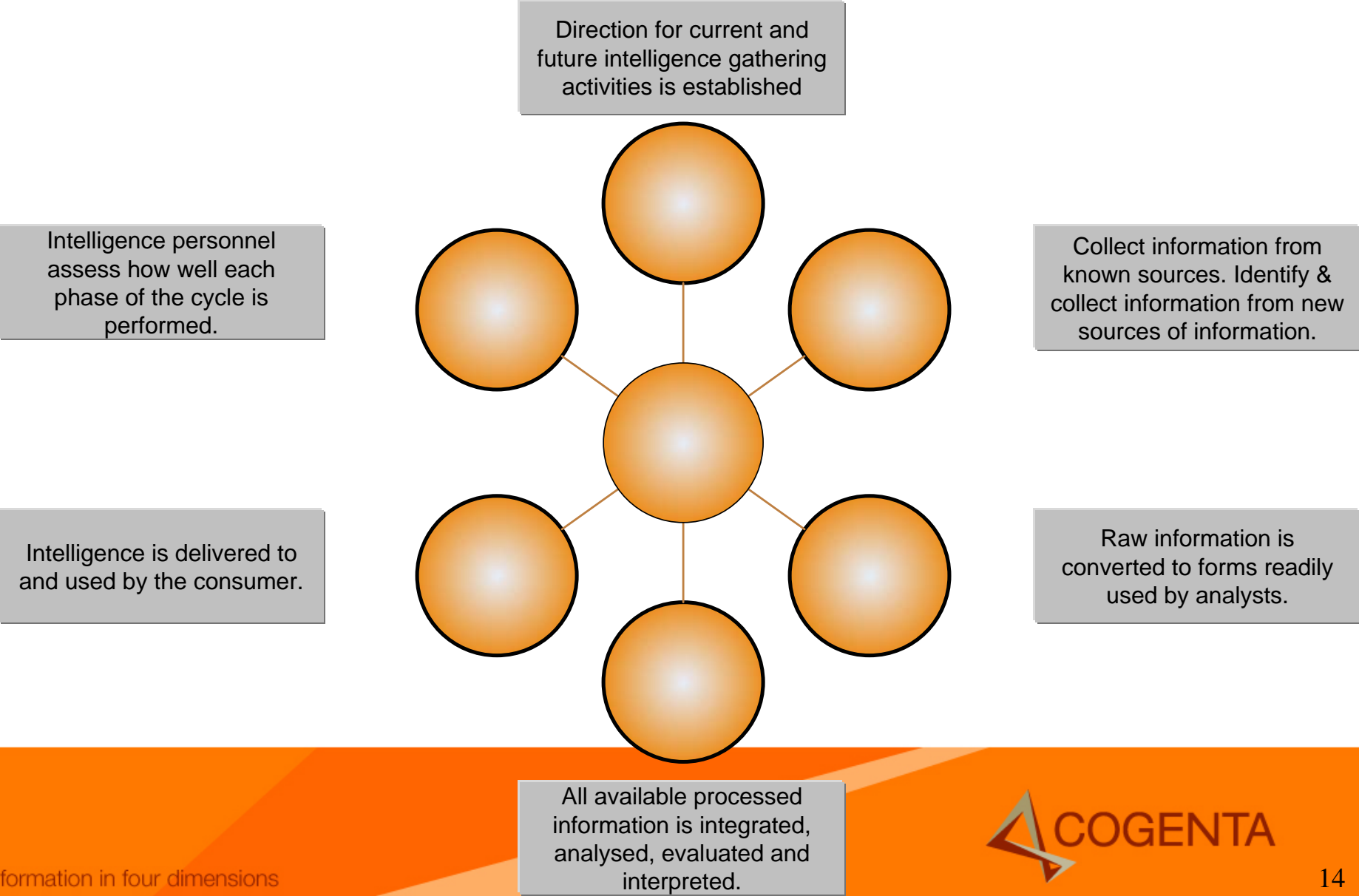
- Decision Makers need to understand the “big picture” of their Security posture
- Having the right information helps Decision Makers take actions that balance security and cost.
- Situational Awareness Requires:
 - Perception – What’s Happening Now
 - Comprehension – Is it Important
 - Projection – What could happen Next
- Intelligence Output Requires:
 - Right Content
 - Right Time
 - Right Place and People
 - Right Form

Understand Information Needs

- Get a clear understanding of Decision Makers information needs/timescales.
- **What** decisions need to be made?
- **Why** do the decisions need to be made?
- **When** do the decisions need to be made?
- **Who** will be using the intelligence to make the decisions?
- Is the intelligence **nice to know or need to know?**



The Six Stage Intelligence Cycle



Analysis

- Analysis is really the application of common sense and experience to raw information

Leonard Fault, The New Competitor Intelligence, p. 359.

- Turns information into actionable intelligence that leads to informed decisions and actions.



Basic Analysis Steps

- Read all previously processed information.
- Concentrate on the reliable data.
- Recognize gaps in information
- Read between the lines
- Look for patterns
- Organize the information
- Develop a number of possible scenarios.
- Develop long-term and short-term responses for each scenario.
- Know when to quit! (*Know Your Business Drivers*)

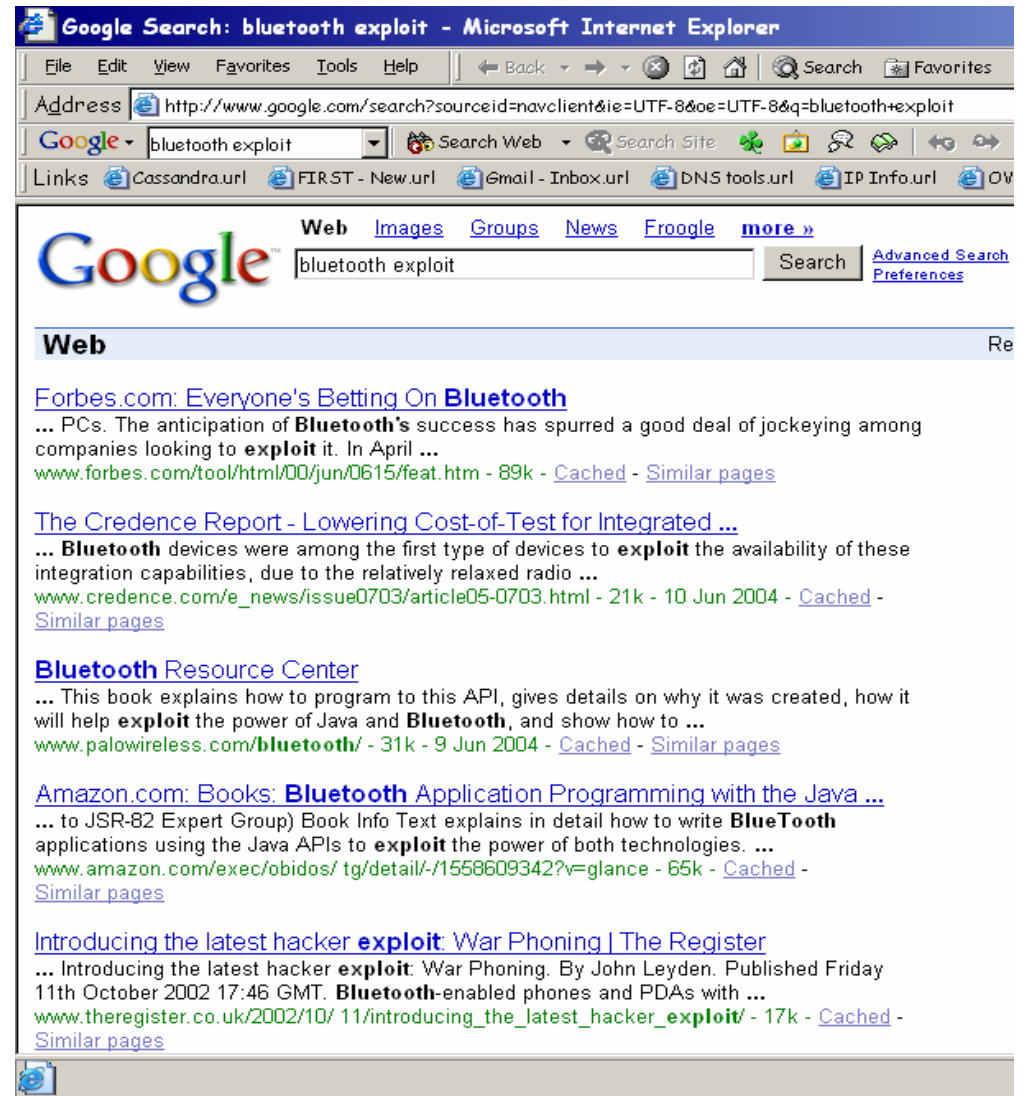


Potential Sources of Intelligence Information

- Web Sites
- Search Engines and Tools
- News Feeds
- FTP Sites
- Printed Material
- Vulnerability Alerts
- Professional Associations
- Government Sources
- Vendors
- Industry Organizations
- Media Organizations
- Hacker Organizations
- In House Technical experts
- Periodicals
- Subscription Services
- Newsgroups
- Chat (IRC)
- Information Exchange Partners
- Human Sources
 - Industry experts
 - Underground
 - Law Enforcement
 - Govt. Intelligence Agencies
- Public Record Databases
- Bulletin Boards
- Proprietary Sources
- Etc.

Search Engines

- Google
<http://www.google.com>
- AllTheWeb.com
<http://www.alltheweb.com>
- Yahoo
<http://www.yahoo.com>
- HotBot
<http://www.hotbot.com>
- List of Search Engines
<http://www.hotbot.comhttp://searchenginewatch.com/links/index.php>



Personalized Web Search Updates

Security CyberSleuth Preferences - Keywords

Make any changes you want below. Be sure to click on the **Save changes** button at the bottom to store your edits. If you make a mistake, click on the **DON'T Save Changes** button and your original queries will be preserved.

Example: Keywords:
(Click [here](#) for more examples)

Collections to search: Security in the News
 Linux Security

1) Keywords:
Found: Search type:

Collections to search: Security in the News
 Linux Security

2) Keywords:

GOOGLE ALERT!

Search Settings

- Browse Results
- Search Settings
- User Settings
- Search Ideas
- Tell A Friend
- Questions...
- Feedback
- Feed Settings
- Logout

Enter up to 5 Google searches (see [examples](#)) for Google Alert to automatically perform:

- All of: Merrill Lynch
Updated: in the past 3 months
SafeSearch off
[more...](#) results
- All of: @ml.com
Updated: in the past 3 weeks
SafeSearch off
[more...](#) results
- All of: Hacking
Updated: in the past 3 weeks
SafeSearch off
[more...](#) results

Helpful Hints

For advanced search options, click [more...](#)

Google Alert tracks the top Google results for each search.

To change the number of results tracked, click on .

You can track up to 150 results in total.

Google News Alerts (BETA) [FAQ - Send us your feedback](#)

Welcome to Google News Alerts

Google News Alerts are sent by email when news articles appear online that match the topics you specify.

Some handy uses of Google News Alerts include:

- monitoring a developing news story
- keeping current on a competitor or industry
- getting the latest on a celebrity or event
- keeping tabs on your favorite sports teams

Create your News Alerts with the form on the right.

Create a Google News Alert

Enter the topic you wish to monitor.

News search:

How often:

Your email:

Google will not sell or share your email address.

TRACERLOCK

Your monitor for changes on the web

WatchThatPage.com

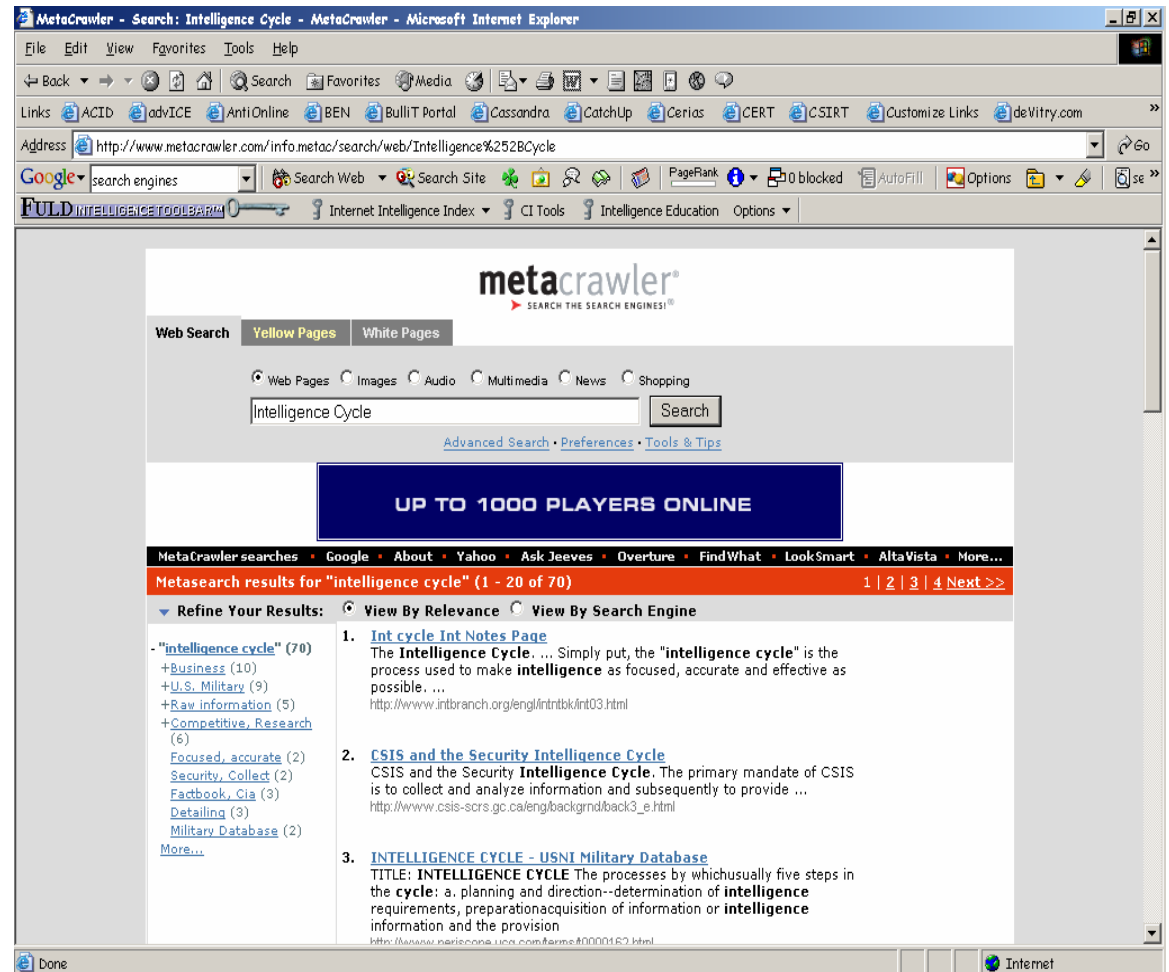
Meta Search Engines

- Meta Search Engines return best results from leading search engines

www.vivisimo.com

www.dogpile.com

www.metacrawler.com



Copernic Agent Professional (meta-search engine)



- [Power-search the Web](#)
- [Advanced Management of Searches and Results](#)
- [Analyze Search Results](#)
- [Summarize Search Results](#)
- [Track Changes in Web Pages Contents](#)

- [Track New Search Results](#)
- [Access Hidden Information](#)
- [Create Custom Search Categories](#)
- [Automate Result Analysis](#)
- [Integration with Internet Explorer and Office](#)

The screenshot shows the Copernic Agent Professional interface. The main window displays search results for the query 'exploit rpc examples'. The results are sorted by 'Update Date' and show several entries with their respective scores and sources. The top result is 'Cover Pages: XML-RPC' with a score of 93%. Other results include 'Insecure.Org - Nmap Free Security Scanner, Tools Hacking resources' (93%), 'untitled' (93%), 'An Architectural Overview of UNIX Network Security' (92%), 'CERT/CC Vulnerability Note VU#387387' (92%), and 'Format Strings - An Interview with Chris Evans' (92%).

Result	Score	Source
Cover Pages: XML-RPC	93%	MSN Web Search, AltaVista, Lycos, HotBot, Yahoo!, Teoma, AOL...
Insecure.Org - Nmap Free Security Scanner, Tools Hacking resources	93%	Yahoo!, MSN Web Search, AltaVista, Lycos, AOL Search, HotBot
untitled	93%	Teoma, WiseNut, HotBot, LookSmart, AOL Search, AltaVista, Yahoo!
An Architectural Overview of UNIX Network Security	92%	Lycos, AltaVista, WiseNut, LookSmart, MSN Web Search, HotBot
CERT/CC Vulnerability Note VU#387387	92%	AltaVista, MSN Web Search, AOL Search, Yahoo!, HotBot, Lycos
Format Strings - An Interview with Chris Evans	92%	

<http://www.copernic.com/en/products/agent/professional.html>

WebSite Watcher

- Monitors Web pages and notifies you when they change

<http://www.aignes.com/>

The screenshot shows the WebSite-Watcher 3.60c application window. The title bar indicates the file path [c:\program files\website-watcher\bookmark.wsw] and the license holder as Ian Cook. The interface includes a menu bar (File, Folder, Bookmarks, Search, Tools, Options, View, Help) and a toolbar with various icons. On the left, a folder tree lists categories like Bookmarks, AutoWatch, Search Results, Errors, Alerts, Blog, Chat, Crime, Cymru, Exploits, Finance, Hacker Sites, Intelligence, IRC, News, News Feed, NewsGroup, Protest, Proxies, Security Radar, Site Watch, Spam Alerts, USENET Groups, Vendor Alerts, Virus, and Vulnerabilities. The main pane displays a table of monitored items:

Folder	Total	Name	URL	Met...	last change	last check	Status
	0	Exploits - Beyond-Security's SecuriTeam.com	http://www.s...	C	15:25	15:25	OK
	708	Exploits - Exploits-World	http://www.a...	C	15:26	15:26	OK, Warning:...
	507	Exploits - Fux0r	http://fux0r.p...	C	15:25	15:25	OK
	3	Exploits - Google Groups	http://groups...	C	15:25	15:25	OK
	0	Exploits - Governmentsecurity.org Exploits	http://www.g...	C	15:25	15:25	OK
	0	Exploits - Hackerzhell.co.uk	http://www.h...	C	15:25	15:25	OK
	0	Exploits - Hackerzhell.co.uk Page 1	http://www.h...	C	15:25	15:25	OK
	39	Exploits - Hackerzhell.co.uk Page 2	http://www.h...	C	15:25	15:25	OK
	0	Exploits - Kotic	http://www.k...	C	2004-06-02 1...	2004-06-02 1...	Page not availab...
	2	Exploits - Opennet.ru	http://www.o...	C	15:25	15:25	OK
	11	Exploits - Packetstorm.linuxsecurity.com	http://packet...	C	15:26	15:26	OK
	1	Exploits - Phishing	http://search...	C	15:25	15:25	OK
	5	Exploits - Rootkit.com	http://www.r...	C	15:25	15:25	OK
	10	Exploits - Security Corporation	http://www.s...	C	2004-06-02 1...	15:25	OK
	9	Exploits - Tools	http://packet...	C	15:26	15:26	OK
	34	Exploits - Web-Hack	http://www....	C	15:25	15:25	OK
	10	Exploits - 0x557.org/	http://0x557.org/	C	2004-06-02 13:3...	15:25	OK
	9	Exploits - Antiserver.it	http://www.antis...	C	2004-01-27 19:0...	15:26	OK, Warning: do...
	1	Exploits - Binwin.org	http://www.binwin...	C	2004-01-25 22:3...	15:25	OK

The bottom pane shows details for two selected files:

- File Name:** roundUP.txt
Description: Roundup is susceptible to a directory traversal attack that will permit an attacker to view files outside of the web root.
Author: Vickenty Fesunov
File Size: 1796
Last Modified: Jun 10 10:09:25 2004
MD5 Checksum: 751d0c8016c146f80cc191a8fe075334
- File Name:** cpanelInject.txt
Description: Reseller accounts used with Cpanel are able to change all passwords without verification.
Author: verb0s
File Size: 569
Last Modified: Jun 10 09:08:06 2004
MD5 Checksum: f1426a10b54aadf67391f001ffad1b4b

Additional panes on the right show 'Last 10 Files' and 'Last 10 Advisories' lists.



Copernic Summarizer

MyDoom.A: Fastest Spreading Virus in History
February 3, 2004
By Jay Munro

[Click here](#) to subscribe to our Security Watch newsletter.

MyDoom.A: Fastest Spreading Virus in History

The big news last week (and possibly this, depending on what happens) is the massive attack of W32/MyDoom.A-mm (also known as W32/MIMail.R, and W32/Novarg), on the e-mail world. According to antivirus vendors, MyDoom started on the Kazaa file sharing network, and spread to e-mail networks. With the sheer multiplication potential of harvesting e-mail addresses from a victim's machine, it didn't take long before MyDoom was infecting 1 in 12 e-mail messages on the Internet. According to MessageLabs, in two days, MyDoom broke the Sobig.F virus's previous record from last August of 1 in 17 messages.

Concepts	Score
MyDoom	100
attack	80
windows	60
Microsoft	40
Internet	20
infecting	10

Summary length: 100 words

Summary

The big news last week (and possibly this, depending on what happens) is the massive attack of W32/MyDoom.A-mm (also known as W32/MIMail.R, and W32/Novarg), on the e-mail world.

With the sheer multiplication potential of harvesting e-mail addresses from a victim's machine, it didn't take long before MyDoom was infecting 1 in 12 e-mail messages on the Internet.

It chooses from slightly different set file names when it created copies of itself in the victim's Kazaa folder.

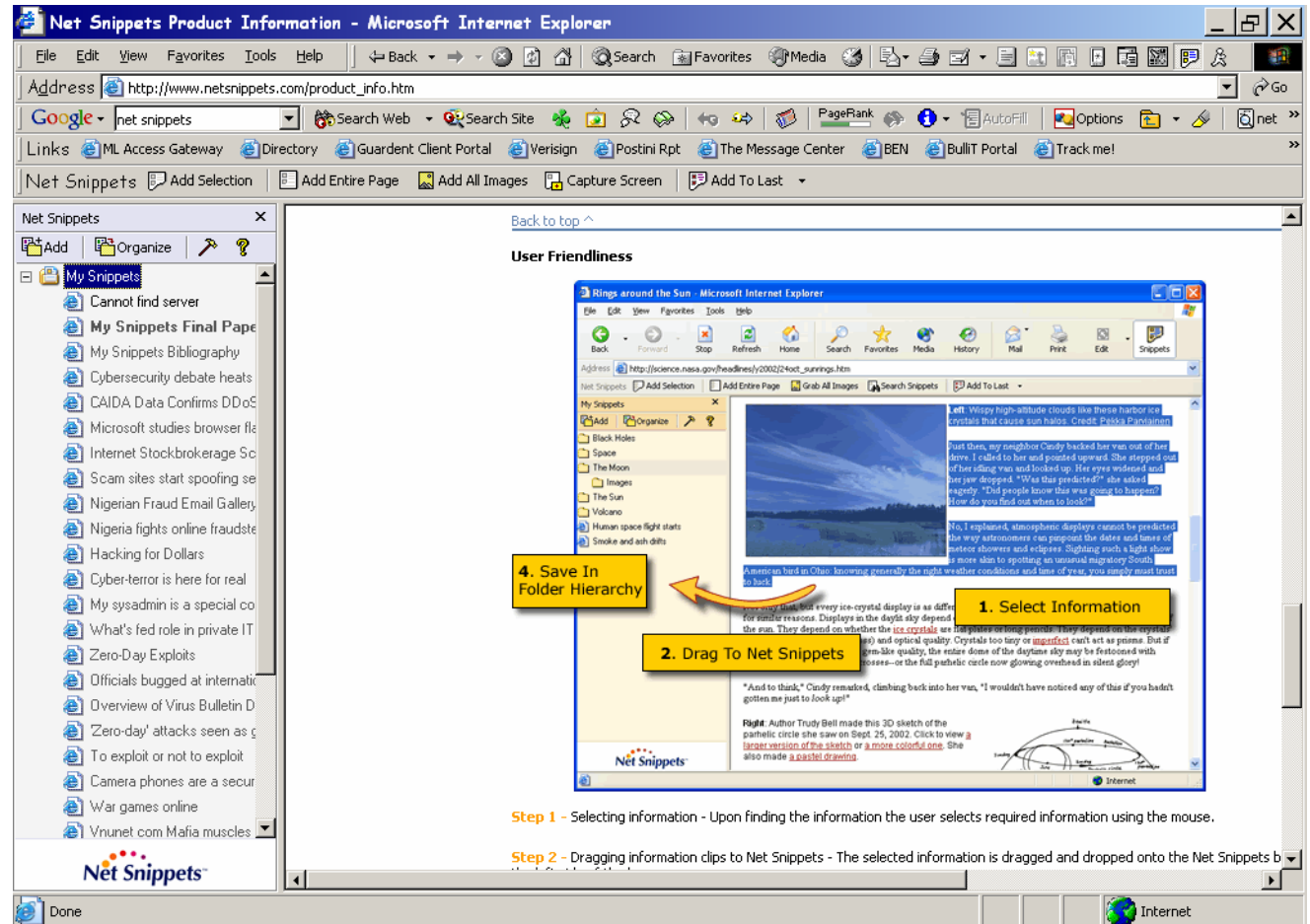
However, MyDoom.B added a new twist to the game by overwriting the Windows Hosts file with a list of antivirus sites and bad

Using sophisticated statistical and linguistic algorithms, it pinpoints the key concepts and gives summary of any document

<http://www.copernic.com/en/products/summarizer>

Net Snippets

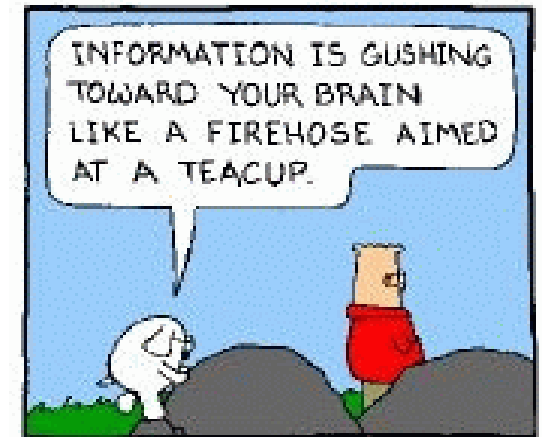
- Allows saving selected information on web page
- Information can be edited
- Add comments
- Automatically captures and saves bibliography information
- Automated bibliography reports
- Snippets stored in HTML format so you can later use them in MS Word etc



www.netsnippets.com

The Information Explosion

- The Potential Sources of Intelligence Information are increasing:
 - The size of the world-wide web is doubling every 12-months and this rate is increasing
 - Annual publication rates > 800mb person/annum for every person on the planet
 - Disk space usage in organisations increasing 50-70% per annum
 - The ‘Deep’ or ‘Hidden’ web includes databases of information from businesses, universities, government agencies which search engines can’t spider
 - The Hidden’ web is up to 50 times larger than the visible web (Sherman – Search Engine Watch Newsletter)



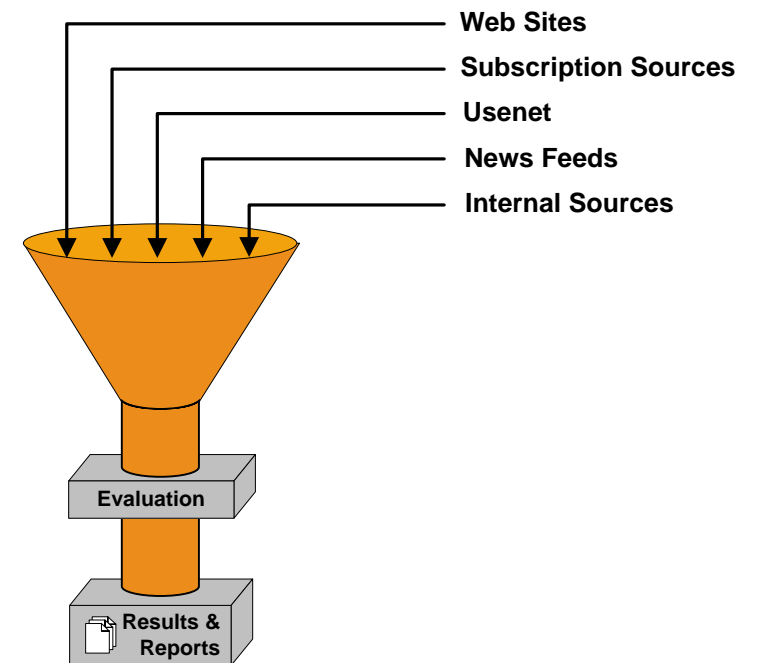
The High Cost of Not Finding Information

- Susan Feldman, in KMWorld-Volume 13, Issue 3, March 2004, estimates.
 - Knowledge workers spend from 15 to 30% of their time searching for information
 - Searchers find what they look for only 50% of the time or less
 - 40% of corporate users report they can't find the information they need to do their jobs on their intranets
 - The average enterprise wastes at least \$1.6 to \$2.3m per year searching for non existent information, failing to find existing information and recreating information that cant be found
 - The Fortune 1000 stands to waste at least \$2.5 billion per year due to an inability to locate and retrieve information.



Intelligence Tool Requirements

- Single point of access to multiple sources:
 - Search engines
 - Subscription sites
 - Specialised portals
 - User defined web sites
 - Newsfeeds
 - Newsgroups
 - Bulletin Boards
 - IRC
 - Etc.
- Collect Information from parts of web not indexed by search engines (Hidden Web)
- Support multiple data formats
- Log-in search source capability
- Automate the search process with 'human' like abilities to translate, analyze and intelligently discover content
- Intelligently rank results and summarise content using statistical and linguistic algorithms
- Link analysis for visualizing associations and interactions



Cogenta Research Director

- Single point of access to multiple data sources
- Central Data Repository
- Share results with co-workers – distributed analysis.
- Intelligent agents search hidden web
- Finds new sources
- Searches dynamically created web pages
- Documents ranked using computational linguistic algorithms
- Summarises documents

The screenshot displays the Cogenta Research Director application window. The interface includes a menu bar (File, Edit, Search, View, Tools, Help), a toolbar with icons for search, start, pause, stop, and highlight, and a search input field containing the query 'exploit RPC example code'. The main window is divided into several sections:

- Left Panel:** A tree view showing a hierarchy of search categories: My Research, Easy Search, Agent Search, bind, Hunt Groups, Exploits, Protest Meetings, phishing, RPC Exploit, and Sources.
- Search Results Table:** A table with columns for Relevance, Title, and Url. It lists 14 results, with the top one being 'Exploits & Vulnerability Archive' from the Government Security website.
- Browser View:** A preview of the selected document, showing the Government Security website's 'Exploits & Vulnerabilities Archive' page. The page includes a search bar, navigation links, and a list of article topics.

At the bottom of the application window, a status bar indicates '1342 documents found. Best Document is 84% relevant'.

Behavioral Profiling Techniques

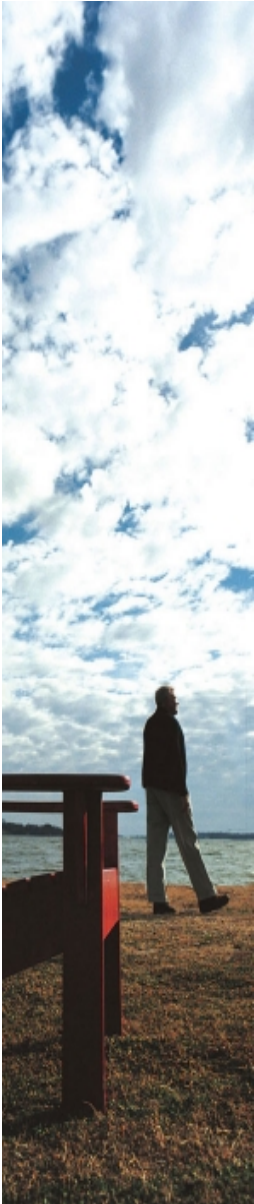
The same data mining technologies used by marketers can be used by Cyber Intelligence Analysts:

- **Data warehousing** for accessing multiple and diverse sources of information and demographics
- **Link analysis** for visualizing criminal associations and interactions
- **Intelligent Software agents** for retrieving, monitoring, organizing, analyzing and acting on information
- **Text mining** for sorting through gigabytes of documents, web pages, public records and e-mails in search of concepts and key words
- **Data mining** for predicting the probability of crimes and extracting profiles of perpetrators



Cyber Intelligence Program Enables You to:

- Facilitate more informed security related business decisions by providing situational awareness
- Predict, understand and give advance warning of imminent or emerging threats, and cyber attacks
- Prevent and effectively respond to potential or actual threats
- Understand how your threats compare to those of your competitors
- Identify whether any actions taken by you or news regarding the company may make you a target, and
- In a world of unlimited threats focus limited resources effectively



Questions ?

- www.cogenta.com
- Ian.cook@cogenta.com
- Tel: +44 (0)1252 725478

“Someone else may decide if you will be a target - but you decide whether or not you will be a victim.”

~ Gavin De Becker