Information in four dimensions

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

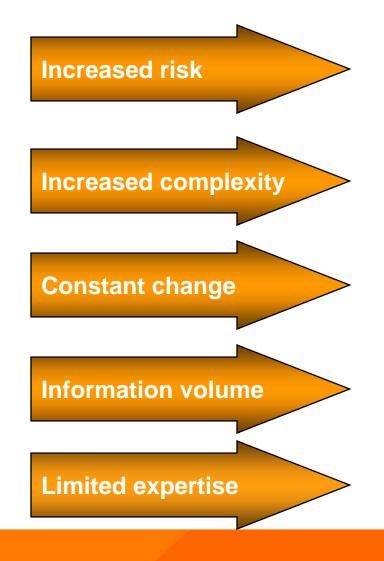


How Much Security?

- 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



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

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

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

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

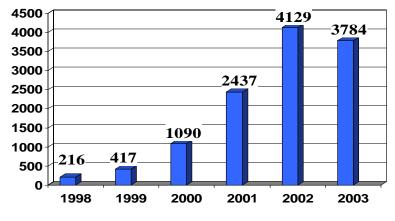
Few companies have the necessary in-house security expertise. The enemy has become more sophisticated, organized and better resourced.



Information in four dimensions

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

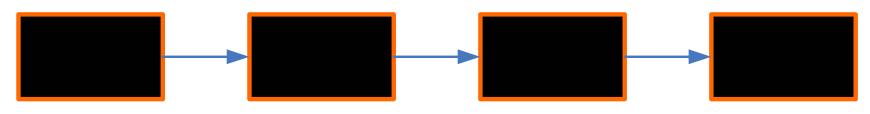
Intelligence Led Decision Making

- 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 &

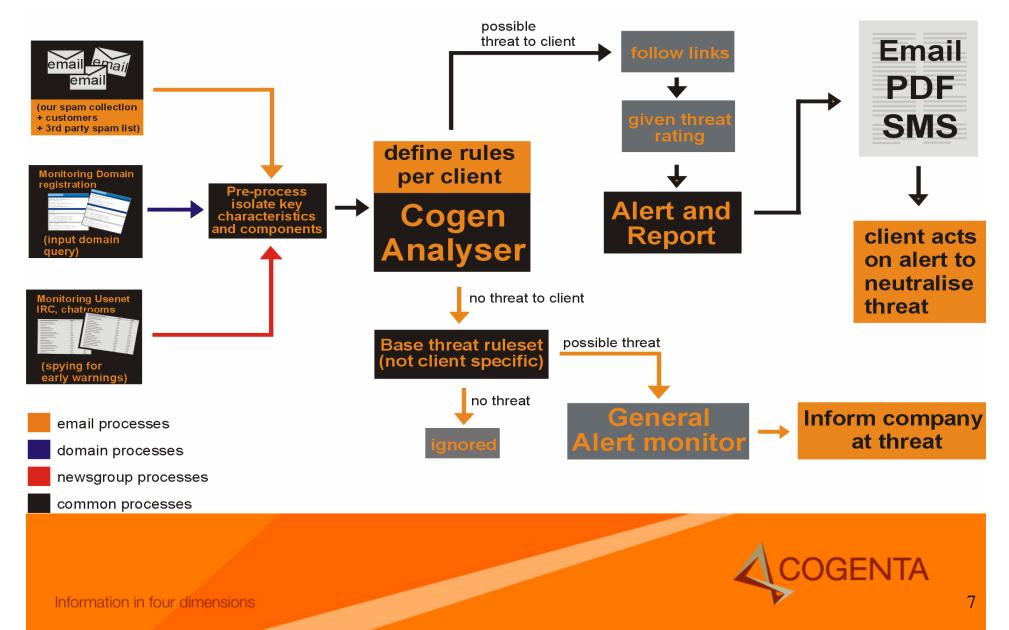
 Password
- Phishing emails containing Company name
- Seed fake sites with account details and monitor accounts

GENTA

Register Domain

Information in four dimensions

Anti Phishing Tool Workflow



Prototype Email Phishing Threat Analyzer

🗟 Domainwatch Configuration		Domainwatch Configuration
Configuration Results Start St	top	Configuration Results Start Stop
Rules MailBoxes Alerters	Rules	Open Logfile Display mail results_log_20040610-1500.bxt Mail files
Add Delete Add Term Barclays Ebay All Body Tu Halfax Doyds Purchase Purchase Paypal Prishing general download Verification Account fraud PIN ATM	-6 Remove	Score Item Id Client 134 20040510140953016 Cogenta Abt 57 20040510140953016 Cogenta Abt 54 2004051014095301 Cogenta Abt 54 2004051014095301 Cogenta Abt 36 2004051014095301 Cogenta Abt 36 2004051014095306 Cogenta Abt 36 2004051014095306 Cogenta Abt 36 2004051014095306 Cogenta Abt 36 2004051014095302 Cogenta Abt 36 2004051014095302 Cogenta Abt 36 2004051014095302 Cogenta Abt 37 2004051014095302 Cogenta Abt 38 2004051014095302 Cogenta Abt 30 2004051014095302 Cogenta Abt 30 2004051014095302 Cogenta Abt 30 2004051014095303 Cogenta Abt 30 2004051014095303 Cogenta Abt 30 2004051014095303 Cogenta Abt 30 2004051014095303 Cogenta Abt 30 2004051014095306 Cogenta Abt 2
Activale		



Information in four dimensions

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



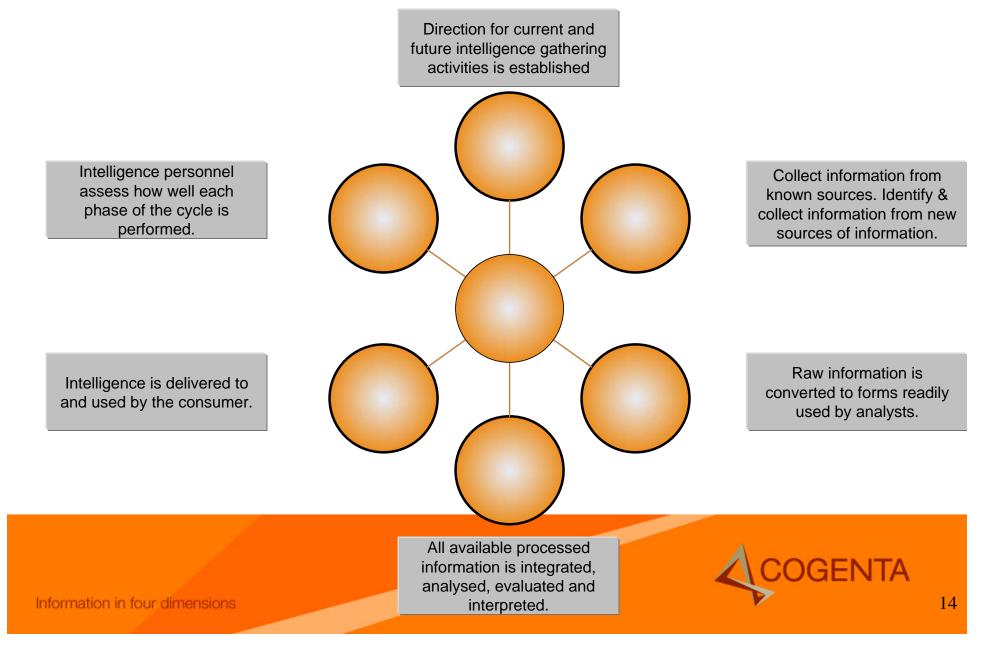
Understand Information Needs

- 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)





Information in four dimensions

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
- Yahoo http://www.yahoo.com
- HotBot http://www.hotbot.com

Address http://www.google.com/search/Sourceid=navclient&ie=UTF-8&q=bluetoothexploit Google bluetooth exploit BETT- New.url @Gmail-Inbox.url @DNS tools.url @IP Info. Web Images Groups News Froogle more a Bluetooth exploit Search Web Cost of Search Strees Forbes.com: Everyone's Betting On Bluetooth PCs. The anticipation of Bluetooth's success has spurred a good deal of jockeying among companies looking to exploit it. In April www.forbes.com/bould to fBluetooth's success has spurred a good deal of jockeying among companies looking to exploit it. In April Web The control of the exploit it. In April Www.forbes.com/bould/tm//D0/jun/D615/feat.htm - 89k - Cached - Similar pages The Credence Report - Lowering Cost-of-Test for Integrated Buetooth devices were among the first type of devices to exploit the availability of these integration capabilities, due to the relatively relaxed radio www.credence.com/e_news/issue0703/article05-0703.html - 21k - 10 Jun 2004 - Cached - Similar pages Bluetooth Resource Center This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www. palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - Cached - Similar pages Amazon.com: Books: Bluetooth Application Programming with the Java to JSR-82 Expert Group) Book Info Test explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of bot technologies www. amazon.com/exec/obidos/ tg/detail//1558609342?v=glance - 65k - Cached - Similar pages Introducing the latest hacker exploit. War Phoning [The Register Introducing the latest hacker exploit. War Phoning By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - Cached - Similar pages Philinks/index.php	Google -	bluetooth explo	oit 🔽 🕻	🏂 Search Web	• 📿 Se			_
Links Cassandrauri FTRST - New.uri Comail - Inbox.uri DNS tools.uri Tron.						earch Site	🍇 🚊	R 62
Web Images Groups News Frongle Modular Bluetooth exploit Search Advant Web Search Advant Images Search Advant Web Search Advant Images Search Advant Images Search Search Prefer Search Advant Images Search Search Prefer Search Search Images Search Search Prefer Search Search Images Search Search	Links 🗐	Cassandra.url	FIRST - New.	url 🕘Gmail:	Taba			
Advance Description Description Description Advance Web Search Search Prefer Web Search Search Search Prefer Www.forbes.com/tool/html/D0/jun/D615/feat.htm - 89k - Cached - Similar pages Similar pages Search Prefer Web Search Similar	Go	1			- Inpox.url	🙆 DNS	tools.url	🕘 I P Info
Advant Preter December 2019 The Preter Prete	Go	1	Web Imar	nes Groups	News	Eroogle	mores	
Web Eorbes.com: Everyone's Betting On Bluetooth PCs. The anticipation of Bluetooth's success has spurred a good deal of jockeying among companies looking to exploit it. In April www.forbes.com/tool/html/00/jun/0615/feat.htm - 89k - Cached - Similar pages The Credence Report - Lowering Cost-of-Test for Integrated Bluetooth devices were among the first type of devices to exploit the availability of these integration capabilities, due to the relatively relaxed radio www.credence.com/e_news/issue0703/article05-0703.html - 21k - 10 Jun 2004 - Cached - Similar pages Bluetooth Resource Center This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - Cached - Similar pages Amazon.com: Books: Bluetooth Application Programming with the Java to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.wava.on.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - Cached - Similar pages Introducing the latest hacker exploit: War Phoning [The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - Cached - Similar	GU	<u>o</u> <u>a</u> l <u>o</u>			140110	<u>i roogio</u>		arch Adva
 Forbes.com: Everyone's Betting On Bluetooth 		USIC		pion				Prefe
 Forbes.com: Everyone's Betting On Bluetooth 	Mah	-						
 PCs. The anticipation of Bluetooth's success has spurred a good deal of jockeying among companies looking to exploit it. In April www.forbes.com/tool/html/00/jun/0615/feat.htm - 89k - <u>Cached - Similar pages</u> <u>The Credence Report - Lowering Cost-of-Test for Integrated</u> Bluetooth devices were among the first type of devices to exploit the availability of these integration capabilities, due to the relatively relaxed radio www.credence.com/e_news/issue0703/article05-0703.html - 21k - 10 Jun 2004 - <u>Cached - Similar pages</u> Bluetooth Resource Center This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth - 31k - 9 Jun 2004 - <u>Cached - Similar pages</u> <u>Amazon.com: Books: Bluetooth Application Programming with the Java</u> <i></i> to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-1558609342?v=glance - 65k - <u>Cached - Similar pages</u> Introducing the latest hacker exploit: War Phoning [The Register	vveb							
 PCs. The anticipation of Bluetooth's success has spurred a good deal of jockeying among companies looking to exploit it. In April www.forbes.com/tool/html/00/jun/0615/feat.htm - 89k - <u>Cached - Similar pages</u> <u>The Credence Report - Lowering Cost-of-Test for Integrated</u> Bluetooth devices were among the first type of devices to exploit the availability of these integration capabilities, due to the relatively relaxed radio www.credence.com/e_news/issue0703/article05-0703.html - 21k - 10 Jun 2004 - <u>Cached - Similar pages</u> Bluetooth Resource Center This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth - 31k - 9 Jun 2004 - <u>Cached - Similar pages</u> <u>Amazon.com: Books: Bluetooth Application Programming with the Java</u> <i></i> to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-1558609342?v=glance - 65k - <u>Cached - Similar pages</u> Introducing the latest hacker exploit: War Phoning [The Register	Forbes.co	om: Evervon	ie's Bettina (on Bluetoo	th			
companies looking to exploit it. In April www.forbes.com/tool/html/00/jun/0615/feat.htm - 89k - <u>Cached</u> - <u>Similar pages</u> The Credence Report - Lowering Cost-of-Test for Integrated Bluetooth devices were among the first type of devices to exploit the availability of these integration capabilities, due to the relatively relaxed radio www.credence.com/e_news/issue0703/article05-0703.html - 21k - 10 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> Bluetooth Resource Center This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> <u>Amazon.com: Books: Bluetooth</u> Application Programming with the Java to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> <u>Introducing the latest hacker exploit: War Phoning The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u></u>						qood dea	l of jocker	ving amon
 www.forbes.com/tool/html/00/jun/0615/feat.htm - 89k - <u>Cached</u> - <u>Similar pages</u> <u>The Credence Report - Lowering Cost-of-Test for Integrated</u> Bluetooth devices were among the first type of devices to exploit the availability of these integration capabilities, due to the relatively relaxed radio www.credence.com/e_news/issue0703/article05-0703.html - 21k - 10 Jun 2004 - <u>Cached - Similar pages</u> <u>Bluetooth Resource Center</u> This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - <u>Cached - Similar pages</u> <u>Amazon.com: Books: Bluetooth Application Programming with the Java</u> to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached - Similar pages</u> <u>Introducing the latest hacker exploit: War Phoning The Register</u> Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached - Similar pages</u> 						J	.,	,
 Bluetooth devices were among the first type of devices to exploit the availability of these integration capabilities, due to the relatively relaxed radio www.credence.com/e_news/issue0703/article05-0703.html - 21k - 10 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> Bluetooth Resource Center This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> Amazon.com: Books: Bluetooth Application Programming with the Java to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> Introducing the latest hacker exploit: War Phoning The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u> 					- <u>Cached</u>	- <u>Similar p</u>	ages	
 Bluetooth devices were among the first type of devices to exploit the availability of these integration capabilities, due to the relatively relaxed radio www.credence.com/e_news/issue0703/article05-0703.html - 21k - 10 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> Bluetooth Resource Center This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> Amazon.com: Books: Bluetooth Application Programming with the Java to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> Introducing the latest hacker exploit: War Phoning <u>The Register</u> Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u> 								
 Bluetooth devices were among the first type of devices to exploit the availability of these integration capabilities, due to the relatively relaxed radio www.credence.com/e_news/issue0703/article05-0703.html - 21k - 10 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> Bluetooth Resource Center This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> Amazon.com: Books: Bluetooth Application Programming with the Java to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> Introducing the latest hacker exploit: War Phoning <u>The Register</u> Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u> 	The Cred	lence Report	t - Lowering	Cost-of-Tes	st for Inte	egrated.		
integration capabilities, due to the relatively relaxed radio www.credence.com/e_news/issue0703/article05-0703.html - 21k - 10 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> Bluetooth Resource Center This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> <u>Amazon.com: Books: Bluetooth</u> Application Programming with the Java to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> Introducing the latest hacker exploit: War Phoning The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u>	Bluetoo	th devices wer	re among the fi	rst type of dev	vices to e	xploit the	availabilit	tv of these
www.credence.com/e_news/issue0703/article05-0703.html - 21k - 10 Jun 2004 - <u>Cached - Similar pages</u> Bluetooth Resource Center This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - <u>Cached - Similar pages</u> Amazon.com: Books: Bluetooth Application Programming with the Java to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached - Similar pages</u> Introducing the latest hacker exploit: War Phoning The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached - Similar pages</u>						•		,
Similar pages Bluetooth Resource Center This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - Cached - Similar pages Amazon.com: Books: Bluetooth Application Programming with the Java to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - Cached - Similar pages Introducing the latest hacker exploit: War Phoning The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - Cached - Similar pages						k - 10 Jun	2004 - C	ached -
This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth , and show how to www.palowireless.com/ bluetooth / - 31k - 9 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> <u>Amazon.com: Books: Bluetooth Application Programming with the Java</u> to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> <u>Introducing the latest hacker exploit. War Phoning The Register Introducing the latest hacker exploit. War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u></u>								
This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth , and show how to www.palowireless.com/ bluetooth / - 31k - 9 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> <u>Amazon.com: Books: Bluetooth Application Programming with the Java</u> to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> <u>Introducing the latest hacker exploit. War Phoning The Register Introducing the latest hacker exploit. War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u></u>	Blueteet	b Docourco	Contor					
will help exploit the power of Java and Bluetooth, and show how to www.palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> <u>Amazon.com: Books: Bluetooth Application Programming with the Java</u> to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> Introducing the latest hacker exploit: War Phoning The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u>				this ADL size	deteile	a a suda su it		فمر المعربة
www.palowireless.com/bluetooth/ - 31k - 9 Jun 2004 - <u>Cached</u> - <u>Similar pages</u> <u>Amazon.com: Books: Bluetooth Application Programming with the Java</u> to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> <u>Introducing the latest hacker exploit: War Phoning The Register</u> Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u>	This boo	ik explains now	vio programio svotilovo opdi	triis API, give	es details al about b	UN WRY IL	was creat	itea, now it
Amazon.com: Books: Bluetooth Application Programming with the Java to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - Cached - Similar pages Introducing the latest hacker exploit: War Phoning The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - Cached - Similar pages							nagae	
to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> Introducing the latest hacker exploit . War Phoning The Register Introducing the latest hacker exploit . War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth -enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_ exploit / - 17k - <u>Cached</u> - <u>Similar pages</u>	www.paiow	ireless.com/bi	uetooul/ - STK	- 5 Jun 2004	- <u>Cached</u>	- <u>omiar</u>	pages	
to JSR-82 Expert Group) Book Info Text explains in detail how to write BlueTooth applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> Introducing the latest hacker exploit . War Phoning The Register Introducing the latest hacker exploit . War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth -enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_ exploit / - 17k - <u>Cached</u> - <u>Similar pages</u>	Amazon	com: Books:	Bluetooth	Application	Progra	mmina w	ith tha - I	lava
applications using the Java APIs to exploit the power of both technologies www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> Introducing the latest hacker exploit: War Phoning The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u>		DOM: DOOKS.	Didetootin	Application	n rograi	uto urito	PlueTee	<u></u>
www.amazon.com/exec/obidos/ tg/detail/-/1558609342?v=glance - 65k - <u>Cached</u> - <u>Similar pages</u> Introducing the latest hacker exploit: War Phoning The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u>)ui
Similar pages Introducing the latest hacker exploit: War Phoning The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - Cached - Similar pages								
Introducing the latest hacker exploit: War Phoning The Register Introducing the latest hacker exploit: War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth-enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u>			Didus/ tg/detai	1-710000004	z:v=grand	Se - ODK - 1	cacheu -	
Introducing the latest hacker exploit : War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth -enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_ exploit / - 17k - <u>Cached</u> - <u>Similar pages</u>	<u>Onniai pag</u>	<u></u>						
Introducing the latest hacker exploit : War Phoning. By John Leyden. Published Friday 11th October 2002 17:46 GMT. Bluetooth -enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_ exploit / - 17k - <u>Cached</u> - <u>Similar pages</u>	Introducin	a the latest h	hacker expl	bit : War Ph	onina I T	he Redi	ster	
11th October 2002 17:46 GMT. Bluetooth -enabled phones and PDAs with www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_exploit/ - 17k - <u>Cached</u> - <u>Similar pages</u>								d Eridav
www.theregister.co.uk/2002/10/ 11/introducing_the_latest_hacker_ exploit / - 17k - <u>Cached</u> - <u>Similar pages</u>								5 i nuay
Similar pages								Cached -
<u> </u>					reor_naer	collow bio		<u>o dono d</u>
n/links/index.php	www.thereg							
m/links/index.php	www.thereg							
	www.thereg <u>Similar pag</u>	<u>les</u>						

• List of Search Engines

http://www.hotbot.comhttp://searchenginewatch.com/links/index.php



Personalized Web Search Updates

G Browse Results

G Search Settings

G User Settings

Search Ideas

C Tell A Friend

G Questions...

G Feed Settings

G Feedback

G Logout

	Dartmouth College INSTITUTE FOR SEC TECHNOLOGY STU A National Center For Cybersecurity and Counter	DIES (Advanced Search)
IRIA IRIA Home IRIA Projects Who We Are Tools, FAQ's and Papers UPublished Papers		
a Contine Courses a Security in the News a Security in the News a Security CyberSleuth ISTS Information aISTS Home a Research a Research a Research a Courses a Security CyberSleuth	Security CyberSleuth Preferences - Make any changes you want below. Be sure to bottom to store your edits. If you make a mist button and your original queries will be preserv Example: Keywords: homeland security (Click here for more examples)	click on the Save changes button at the ake, click on the DON'T Save Changes
Dartmouth Home Questions?	Collections to search: 1) Keywords: exploit Found: [in the last week	Security in the News Linux Security Search type: Any Word
	Collections to search: 2 Keywords: hacking	✓ Security in the News ✓ Linux Security
~		FAQ - Send us

GOOQLC[™] Google News Alerts (BETA)

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

Create your News Alerts with the form on the right.

keeping tabs on your favorite sports teams

Create a Google News Alert						
Enter the topic you wish to monitor.						
blaue a carbo						
News search:						
How often: 🛛 once a day 💌						
Your email:						
Create News Alert						
croate riswo / lien						
Google will not sell or share your email address.						

GOOGLE ALERT!

Search Settings

Helpful Hints Enter up to 5 Google searches (see examples) for Google Alert to automatically perform: 1. All of: Merrill Lynch more. 30 - results Updated: in the past 3 months SafeSearch off 2. All of: @ml.com more... 30 🔽 results Updated: in the past 3 weeks SafeSearch off 3. All of: Hacking more 30 💌 results Updated: in the past 3

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 50 💌

You can track up to 150 results in total.

TRACERLOCK

Your monitor for changes on the web WatchThatPage.com

weeks SafeSearch off



Information in four dimensions

Meta Search Engines

File

∉ Baa Links A<u>d</u>dres

Goog Ful

🙆 Don

 Meta Search Engines return best results from leading search engines

> <u>www.vivisimo.com</u> <u>www.dogpile.com</u> <u>www.metacrawler.com</u>

Crawler - Search: Intelligence Cycle - Met	aCrawler - Microsoft Internet Explorer	_ 8 ×
<u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		1
: 🔻 🔿 🔻 🔕 🕼 🚮 🔞 Search 📾 Fi	avorites 🛞 Media 🎯 🖪 🕶 🎒 📷 👻 📄 🎆 🖸 🍪 💬	
🖹 ACID 🥘 advICE 🕘 AntiOnline 👸 Bl	EN @BulliT Portal @Cassandra. @CatchUp @Cerias @CERT @CSIRT @Customize Links @deVitry.com	»
ttp://www.metacrawler.com/info.metac	/search/web/Intelligence%252BCycle	j ∂Go
🕶 search engines 💿 👔 🍪 Search	Web 🔻 🎨 Search Site 🔹 🝺 🖓 🕪 👘 PagePank 🚯 🖉 🗗 🗗 blocked 📲 AutoFill 📴 Options 💼 👻 🔌	<u>د</u> عد 🔘
)INTELLIGENCE TO OLBARM ()	nternet Intelligence Index 🔻 🖞 CI Tools 📲 Intelligence Education Options 💌	
		_
Web Search Yellow Pages		
• Web Pages	C Images C Audio C Multimedia C News C Shopping	
Intelligence	Cycle Search	
	Advanced Search • Preferences • Tools & Tips	
	UP TO 1000 PLAYERS ONLINE	
	oogle About Yahoo Ask Jeeves Overture Find What Look Smart Alta Vista More	
	intelligence cycle" (1 - 20 of 70) 1 <u>2</u> <u>3</u> <u>4 Next>></u>	
- " <u>intelligence cycle</u> " (70) + <u>Business</u> (10) + <u>U.S. Military</u> (9) + <u>Raw information</u> (5) + <u>Competitive, Research</u>	Int cycle Int Notes Page The Intelligence Cycle Simply put, the "intelligence cycle" is the process used to make intelligence as focused, accurate and effective as possible http://www.intbranch.org/engl/intntbk/int03.html	
(6) <u>Focused, accurate</u> (2) <u>Security, Collect</u> (2) <u>Factbook, Cia</u> (3) <u>Detailing</u> (3) <u>Military Database</u> (2)	 <u>CSIS and the Security Intelligence Cycle</u>. CSIS and the Security <u>Intelligence Cycle</u>. The primary mandate of CSIS is to collect and analyze information and subsequently to provide http://www.csis-scrs.gc.ca/eng/backgnd/back3_e.html 	
More	 INTELLIGENCE CYCLE - USNI Military Database TITLE: INTELLIGENCE CYCLE The processes by whichusually five steps in the cycle: a. planning and directiondetermination of intelligence requirements, preparationacquisition of information or intelligence information and the provision Mth: (Maxeumentescope) user compares 40000152 Mtml. 	Ţ
	🔮 Internet	



Copernic Agent Professional

(meta-search engine)



- → Power-search the Web
- → <u>Advanced Management of Searches</u> <u>and Results</u>
- → 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
- → <u>Integration with Internet Explorer</u> and Office

🐹 Copernic Agent Profession	al						_	ъ×
<u>File E</u> dit <u>V</u> iew <u>S</u> earch <u>R</u> esults	; Tracking	Favorites <u>T</u> ools <u>W</u> indow <u>H</u>	<u>l</u> elp					
🔎 New 🎬 Modify 🔎 Update 👻 🔇	3 🛛 🗸 Verif	y Links 懂 Analyze 📕 Save Page	es 📔 Filter 📕 F	ind in Results 🥻	🖇 Browse 📗 Sumr	marize 🗙 🗸		
🕘 Result Layout 🔹 🋓 Sort Results 🔹	- 🔁 Group	Results 🔹 🖕 🛃 Track Search 🏾 🍯	Track Page	Tracking Manager	•			
Analyzing	\$	Sort by: Update Date 🔻				Oldest on top 🛛 🛆	Folders -	
Analyzing	10%	i exploits	All words	The Web	49 results	10/10/03 01	🛅 My Searches	
		🤰 exploit rpc examples	All words	Tech News	0 result	10/02/04 03		
	Stop	exploit rpc examples	All words	Tech News	20 results	10/02/04 03		
		exploit rpc examples	All words	The Web	2358 results	10/02/04 03		
Analyzed: 241 out of 2358		•				Þ		
Broken: 16 results		St <u>a</u> tus: Any - Reg	gion: Any	✓ Domain:		Show Broken Links A	dvanced Filters Clear	×
Skipped: 3 results		Look for:	In: Result	list 👻	Find Now Options	 Advanced Find 	ear	×
Errors: None		Sort by: Score -					Most relevant on	top ⊽
Analysis: Validating links		v Cover Pages: XML-RPC 93% □ ▲						
		<u>Cover Pages: XML-RPC</u> CGI Scripts Available via XML-RPC. Providing a Programmatic is of interest. Examples of data-oriented CGI interfaces and						
					is of interest. Exam	ples of data-oriented (CGI interfaces and	
		examples.'] "As you might e	expect from the nam			-		101
		examples.'] "As you might e	expect from the name html	ne, XML- <mark>RPC</mark> is	Ms	-	Lycos, HotBot, Yahoo!, Teoma, /	40L
		examples.'] "As you might e xml.coverpages.org/xml-rpc." Insecure.Org - Nmap Free Se	expect from the name html curity Scanner, Too	ne, XML- <mark>RPC</mark> is Is Hacking resourc	es.	5N Web Search, AltaVista,	Lycos, HotBot, Yahoo!, Teoma, / 93% 🛽	40L
		examples [*] .] "As you might e mil.coverpages.org/xml-rpc.l rpscure.Org - Nmap Free Se Network Security Tools/Softw exploit it using the SSH1 CR	expect from the name html curity Scanner, Too vare (Free Download	he, XML- <mark>RPC</mark> is I <u>s Hacking resourc</u> I) including Nmap (Ms <u>es</u> Dpen Source it to l	5N Web Search, AltaVista,	Lycos, HotBot, Yahoo!, Teoma, / 93% 🛽	40L
		examples.'] "As you might e xml.coverpages.org/xml-rpc.! Insecure.Org - Nmap Free Se Network Security Tools/Softw	expect from the name html curity Scanner, Too vare (Free Download	he, XML- <mark>RPC</mark> is I <u>s Hacking resourc</u> I) including Nmap (Ms <u>es</u> Dpen Source it to l	- 5N Web Search, AltaVista, find a vulnerable SSH se	Lycos, HotBot, Yahoo!, Teoma, / 93% 🛽	
		examples .] "As you might a xml.coverpages.org/xml-rpc.l insecure.org - Nmap Free Se Network Security Tools/Softw exploit it using the SSH1 CR www.insecure.org unititled	expect from the name html curity Scanner, Too vare (Free Download C32 <mark>exploit</mark> from 2	ne, XML- RPC is <u>Is Hacking resourc</u> J) including Nmap (001. Shame on	MS <u>es</u> Dpen Source it to l	SN Web Search, AltaVista, find a vulnerable SSH se Yahool, MSN Web Search	Lycos, HotBot, Yahool, Teoma, / 93% [erver, and then proceeds to n, AltaVista, Lycos, AOL Search, 93% [
		examples.] "As you might e xml.coverpages.org/xml-rpc.l insecure.Org - Nmap Free Se Network Security Tools/Softw exploit it using the SSH1 CR www.insecure.org untitled Here are a few example:	expect from the name html curity Scanner, Too are (Free Download C32 exploit from 2 s: - IRIX mountd lea	ie, XML- RPC is <u>Is Hacking resourc</u> 1) including Nmap (001. Shame on iks information abc	M: <u>es</u> Dpen Source it to l put the existence of f	SN Web Search, AltaVista, find a vulnerable SSH se Yahool, MSN Web Search	Lycos, HotBot, Yahool, Teoma, / 93% [erver, and then proceeds to n, AltaVista, Lycos, AOL Search, 93% [
		examples .] "As you might a xml.coverpages.org/xml-rpc.l insecure.org - Nmap Free Se Network Security Tools/Softw exploit it using the SSH1 CR www.insecure.org unititled	expect from the name html <u>curity Scanner, Too</u> are (Free Downloac C32 exploit from 2 5: - IRIX mountd lea ain RPC programs,	ie, XML- RPC is Is <u>Hacking resourc</u> I) including Nmap (001. Shame on ks information abo e.g. rpc .statd,	Ms Open Source it to I out the existence of f 	, SN Web Search, AltaVista, find a vulnerable SSH se Yahool, MSN Web Search iles vulnerable to at	Lycos, HotBot, Yahool, Teoma, / 93% [erver, and then proceeds to n, AltaVista, Lycos, AOL Search, 93% [HotBot
		examples ¹] "As you might e xml.coverpages.org/xml-rpc.l ✓ Insecure.Org - Nmap Free Se Network Security Tools/Softw exploit it using the SSH1 CR www.insecure.org ✓ unitiled Here are a few example forwarding mechanisms. Cert	expect from the name term of the second sec	le, XML- RPC is Is <u>Hacking resourc</u> I) including Nmap (001. Shame on ks information abc e.g. rpc .statd, txt	Ms Open Source it to I out the existence of f 	, SN Web Search, AltaVista, find a vulnerable SSH se Yahool, MSN Web Search iles vulnerable to at	Lycos, HotBot, Yahool, Teoma, 93% erver, and then proceeds to n, AltaVista, Lycos, AOL Search, 93% ttacks that exploit RPC -	HotBot
		examples.] "As you might a xml.coverpages.org/xml-rpc.l insecure.Org - Nmap Free Se Network Security Tools/Softw exploit it using the SSH1 CR www.insecure.org utitiled Here are a few example forwarding mechanisms. Cert www.antibozo.net/ogata/wel An Architectural Overview of & attempt to find at least one	expect from the name that curity Scanner, Too lare (Free Download C32 exploit from 2 s: - IRIX mountd les ain RPC programs, LUNIX Network Secu- UNIX Network Secu-	Is <u>Hacking</u> resource (i) including Nmap 0 001. Shame on ks information abcc e.g. rpc .statd, bxt rity amples of a tool	Ms Open Source it to l out the existence of f Te	SN Web Search, AltaVista, find a vulnerable SSH se Yahool, MSN Web Search iles vulnerable to at oma, WiseNut, HotBot, Loo	Lycos, HotBot, Yahool, Teoma, 93% erver, and then proceeds to h, AltaVista, Lycos, AOL Search, 93% ttacks that exploit RPC- ikSmart, AOL Search, AltaVista, 92%	HotBot
		examples.'] "As you might a xml.coverpages.org/xml-rpc.l insecure.Org - Nmap Free Se Network Security Tools/Softw exploit it using the SSH1 CR www.insecure.org utitiled Here are a few example: forwarding mechanisms. Cert www.antibozo.net/ogata/wei www.antibozo.net/ogata/wei www.antibozo.net/ogata/wei wamples of common metho examples of common metho	expect from the name that aurity Scanner, Too are (Free Downloac C32 exploit from 2 s: - IRIX mountd lea ain RPC programs, btools/nfs/README; UNIX Metwork Secu 1, maybe several ex	ls Hacking resource (i) including Nmap (001. Shame on ks information abce e.g. rpc .statd, txt txt inty implement &	Ms Open Source it to l out the existence of f Te	SN Web Search, AltaVista, find a vulnerable SSH se Yahool, MSN Web Search iles vulnerable to at oma, WiseNut, HotBot, Loo to address & next sectii	Lycos, HotBot, Yahool, Teoma, 93% erver, and then proceeds to 1, AltaVista, Lycos, AOL Search, 93% ttacks that exploit RPC- skSmart, AOL Search, AltaVista, 92% on of this paper will discuss	HotBot Yahoo!
		examples.'] "As you might a xml.coverpages.org/xml-rpc.l xml.coverpages.org/xml-rpc.l Insecure.Org - Nmap Free Se Network Security Tools/Softw exploit t using the SSH1 CR www.insecure.org utitled Here are a few examples forwarding mechanisms. Gert www.antibozo.net/ogata/wel An Architectural Overview of & attents to find at least one examples of common metho www.aw.nih.gov/Security/D	expect from the name that curity Scanner, Too are (Free Download C32 exploit from 2 s: - IRDX mountd lead ain RPC programs, btools/nfs/README. UNIX Network Secu UNIX Network Secu dds and tools used t cos/network-securit	ls Hacking resource (i) including Nmap (001. Shame on ks information abce e.g. rpc .statd, txt txt inty implement &	Ms Open Source it to l out the existence of f Te	SN Web Search, AltaVista, find a vulnerable SSH se Yahool, MSN Web Search iles vulnerable to at oma, WiseNut, HotBot, Loo to address & next sectii	Lycos, HotBot, Yahool, Teoma, 93% [erver, and then proceeds to , AltaVista, Lycos, AOL Search, 93% [ttacks that exploit RPC - skSmart, AOL Search, AltaVista, 92% [on of this paper will discuss t, LookSmart, MSN Web Search,	HotBot Yahoo!
		examples.'] "As you might a xml.coverpages.org/xml-rpc.l insecure.Org - Nmap Free Se Network Security Tools/Softw exploit it using the SSH1 CR www.insecure.org utitiled Here are a few example: forwarding mechanisms. Cert www.antibozo.net/ogata/wei www.antibozo.net/ogata/wei www.antibozo.net/ogata/wei wamples of common metho examples of common metho	expect from the name that curity Scanner, Too curity Scanner, Too are (Free Downloac C32 exploit from 2 s: - IRIX mountd lea ain RPC programs, btools/nfs/README, UNIX Network Secu UNIX Network Security ds and tools used t ccs/network-security U#387387	Is Hacking resource (i) Including Nmap (001. Shame on Is information abc e.g. rpc .statd, txt txt inplement & y.html	Ms Spen Source it to l out the existence of f Te or method designed	SN Web Search, AltaVista, find a vulnerable SSH se Yahool, MSN Web Search ilesvulnerable to at oma, WiseNut, HotBot, Loo to address & next sectii Lycos, AltaVista, WiseNut	Lycos, HotBot, Yahool, Teoma, 93% erver, and then proceeds to n, AltaVista, Lycos, AOL Search, 93% ttacks that exploit RPC- skSmart, AOL Search, AltaVista, 92% on of this paper will discuss t, LookSmart, MSN Web Search, 92%	HotBot Yahoo! HotBot
Common Tasks	*	examples. ¹] "As you might a xml.coverpages.org/xml-rpc.l insecure.org Nmap Free Se Network Security Tools/Softw exploit it using the SSH1 CR www.insecure.org utitied Here are a few example forwarding mechanisms. Cert www.antibazo.net/ogata/wel An Architectural Overview of & attempt to find at least one examples of common metho www.alw.nih.gov/Security/Dv CERT/CC Vulnerability Note V access to the ToolTaik RPC that the ToolTaik RPC	expect from the name that curity Scanner, Too are (Free Download C32 exploit from 2 s: - IRIX mounted les ain RPC programs, tools/nfs/README, UNIX Network Secu- ty maybe several ex dds and tools used t acs/network-securit: U#389387 c database service se server is running	ls Hacking resource) including Nmap (001. Shame on ks information abc e.g. rpc.statd, txt rity amples of a tool o implement & , html could exploit this	Ms Spen Source it to l out the existence of f Te or method designed	SN Web Search, AltaVista, find a vulnerable SSH se Yahool, MSN Web Search iles vulnerable to at oma, WiseNut, HotBot, Loo to address & next secti Lycos, AltaVista, WiseNut pecially 8 system, th	Lycos, HotBot, Yahool, Teoma, 93% [erver, and then proceeds to n, AltaVista, Lycos, AOL Search, 93% [ttacks that exploit RPC - skSmart, AOL Search, AltaVista, 92% [on of this paper will discuss t, LookSmart, MSN Web Search, 92% [ne following examples indic	HotBot Yahoo! HotBot
Common Tasks	*	examples.'] "As you might e xml.coverpages.org/xml-rpc.l xml.coverpages.org/xml-rpc.l Insecure.Org - Nmap Free Se Network Security Tools/Softw exploit it using the SSH1 CR www.insecure.org utitited Here are a few example forwarding mechanisms. Cert www.antibozo.net/ogata/wel An Architectural Overview of & attempt to find at least one examples of common methe www.alw.nih.gov/Security/DV CERT/CC Vulnerability Note V access to the ToolTalk RP	expect from the name that curity Scanner, Too are (Free Download C32 exploit from 2 s: - IRIX mounted les ain RPC programs, tools/nfs/README, UNIX Network Secu- ty maybe several ex dds and tools used t acs/network-securit: U#389387 c database service se server is running	ls Hacking resource) including Nmap (001. Shame on ks information abc e.g. rpc.statd, txt rity amples of a tool o implement & , html could exploit this	Ms Spen Source it to l out the existence of f Te or method designed	SN Web Search, AltaVista, find a vulnerable SSH se Yahool, MSN Web Search iles vulnerable to at oma, WiseNut, HotBot, Loo to address & next secti Lycos, AltaVista, WiseNut pecially 8 system, th	Lycos, HotBot, Yahool, Teoma, 93% erver, and then proceeds to n, AltaVista, Lycos, AOL Search, 93% ttacks that exploit RPC- skSmart, AOL Search, AltaVista, 92% on of this paper will discuss t, LookSmart, MSN Web Search, 92%	HotBot Yahoo! HotBot
	*	examples. ¹] "As you might a xml.coverpages.org/xml-rpc.l xml.coverpages.org/xml-rpc.l insecure.org - Nmap Free Se Network Security Tools/Softw exploit it using the SSH1 CR www.insecure.org untitled Here are a few example forwarding mechanisms. Cert www.antibaza.net/ogata/wel An Architectural Overview of & attempt to find at least one examples of common metho www.alw.nih.gov/Security/Do CERT/CC Vulnerability Note V access to the ToolTalk RPC that the ToolTalk RPC databe www.kb.cert.org/vuls/id/387 ✓ Eormat Strings - An Interview	expect from the name that curity Scanner, Too are (Free Download C32 exploit from 2 exploit from 2 exploit from 2 exploit from 2 exploit from 2 exploit from 2 exploit and PC programs, tools/nfs/README, UNIX Network Securit UNIX Network Securit UM387387 C database service se server is running 387 with Chris Evans	ls Hacking resource ls Hacking resource d) including Nmap 0 001. Shame on des information abo e.g. rpc.statd, bot rity could exploit this could exploit this	MS Spen Source it to l out the existence of f Te or method designed vulnerability with a s	SN Web Search, AlkaVista, find a vulnerable SSH se Yahool, MSN Web Search iles vulnerable to at oma, WiseNut, HotBot, Loo to address & next secti Lycos, AlkaVista, WiseNut pecially 8 system, th AlkaVista, MSN Web Sear	Lycos, HotBot, Yahool, Teoma, 93% [erver, and then proceeds to n, AltaVista, Lycos, AOL Search, 93% [ttacks that exploit RPC - skSmart, AOL Search, AltaVista, 92% [on of this paper will discuss t, LookSmart, MSN Web Search, 92% [ne following examples indic	HotBot Yahoo! HotBot

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



WebSite Watcher

Fold

 Monitors Web pages and notifies you when they change

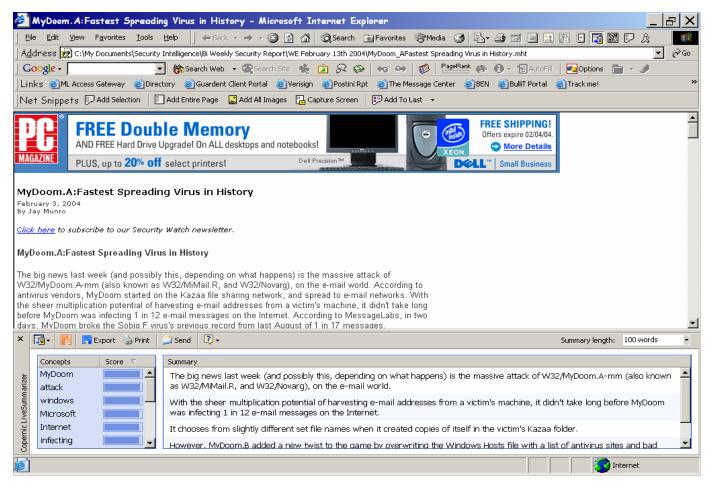
http://www.aignes.com/

WebSite-Wata				am files\website-watcher\bookr	nark.wsw]	Lice	ense: Ian Cook			P X
F <u>o</u> lder <u>B</u> ookmarks	<u>S</u> earch	<u>T</u> ools O <u>p</u> ti	ons <u>V</u> iew	Help						
1		* + 4	+	- 4 🗟 🗟 🔊						
er	Total	[🗉 Name			URL	Met	last change	last check	Status	
Bookmarks	0			ond-Security's SecuriTeam.com	http://www.s	С	15:25	15:25	OK	-
All Bookmarks	708			oits-World	http://www.a		15:26	15:26	OK, Warning:	
Changed Book	507		oits - Fux0		http://fux0r.p		15:25 15:25	15:25	OK OK	
HotSites [3]	3			gle Groups ernmentsecurity.org Exploits	http://groups http://www.g		15:25	15:25 15:25	OK	
AutoWatch	0			kerzhell.co.uk	http://www.h		15:25	15:25	OK	
Search Results	0			kerzhell.co.uk Page 1	http://www.h		15:25	15:25	OK	
Errors	39			kerzhell.co.uk Page 2	http://www.h		15:25	15:25	OK	
Trash	0		oits - Kotic		http://www.k		2004-06-02 1	2004-06-02 1	Page not availab	
Alerts [1]	2		oits - Oper		http://www.o		15:25	15:25	OK	
Blog [9]	11		oits - Paci oits - Phisl	ketstorm.linuxsecurity.com	http://packet http://search		15:26 15:25	15:26 15:25	OK OK	
Chat [1]	1	· · Expl			http://www.r		15:25	15:25	OK	
Crime [4]	5			urity Corporation	http://www.s		2004-06-02 1	15:25	OK	
Cymru (7)	10		oits - Tool		http://packet		15:26	15:26	OK	
Exploits [16]	34		oits - Web		http://www	C	15:25	15:25	OK	
Finance	9		ts - 0x557.c		http://0x557.org/	C	2004-06-02 13:3	15:25	OK	
Hacker Sites [1]	10		its - Antiserv its - Biowin d		http://www.antis http://www.biow	C	2004-01-27 19:0	15:26 15:25	OK, Warning: do	-
Intelligence [26]	32						2004-01-25 22:3			
IRC [1]	1	9 🔍	3 🕋 🔎	🔍 📰 🗸 📑 🖌 📊 file:///C:/Program%20Files/V	/ebSite-Watcher/bookn	nark_ws	w/UUU//Explo_1	🕂 📩 🚳 [) 🖹 🗎 🖬 🗐 🔶 🁌	ы -
News [180] News Feed [39]	215 65	/// File	Name:	roundUP.txt				/// Last 1	0 Files	
NewsGroup [2]	6	Descri		Roundup is susceptible to a directory to	aversal attack that w	ill nerm	nit an attacker	: roundUP		
Protest [3]	4			to view files outside of the web root.	aroroar allaon inar n	in poin	an and the	: sa11791		
Proxies [13]	14	Author:		Vickenty Fesunov				: 06.08.04		
Security Radar Site Watch [1	21 144	File Siz	:	1796				sbd-1.23).tar.gz prk-2.1.tar.gz	
Spam Alerts [4]	6	Last M	dified:	Jun 10 10:09:25 2004					-20040609-catos.txt	
USENET Grou	15	MD5 Cł	ecksum:	751d0c8016c146f80cc191a6fe075334				: aspdotne		
Vendor Alerts [3]	20							: 092004.t	×t	
Virus [9]	11	/// File	lame:	cpanellnject.txt					iceScan55.txt	
Vulnerabilities [72	Descri		Reseller accounts used with Cpanel a	ro oblo to chongo oll	nacew	orde without	: cpanelinj		
		Descri	uon.	verification.	e able to change all	passw	oras without	[Last 2	0 Last 50 Last 100	1
		Author:		verbOs						_
		File Siz	:	569				/// Last 1	0 Advisories	
		Last Me	dified:	Jun 10 09:08:06 2004				: sa11791		
			ecksum:	f1426a10b54aadf67391f001ffad1b4b				: 06.08.04		
			oonounh	1.1254.555444465.5516511641646					-20040609-catos.txt	
								L := aspdotor	et33.txt	

Bookmarks: 708 [507]



Copernic Summarizer



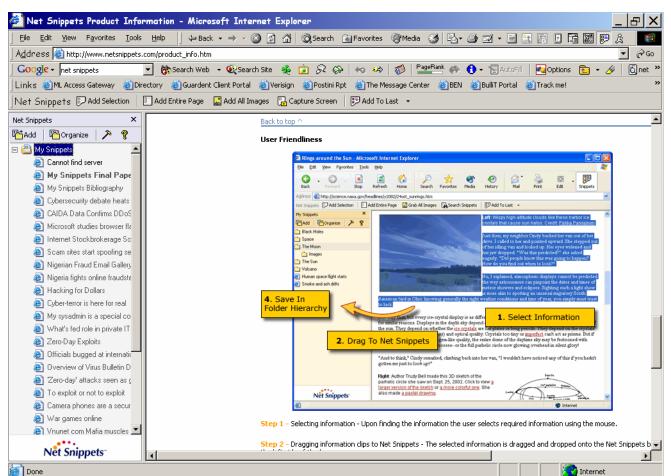
Using sophisticated statistical and linguistic algorithms, it pinpoints the key concepts and gives summary of any document

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)



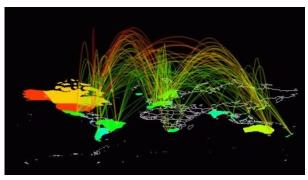
INFORMATION IS GUSHING

TOWARD YOUR BRAIN LIKE A FIREHOSE AIMED

AT A TEACUR

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



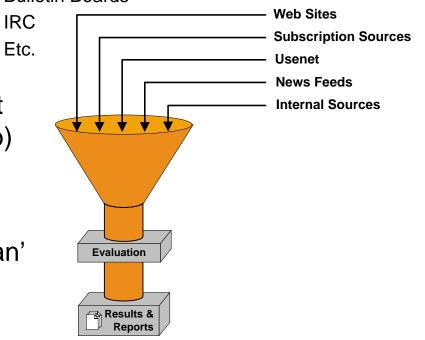
- The average enterprise wastes at least \$1.6 to \$2.3m per year searching for non existent information, failing to find existing information and recreating information that cant be found
- The Fortune 1000 stands to waste at least \$2.5 billion per year due to an inability to locate and retrieve information.



Intelligence Tool Requirements

- Single point of access to multiple sources:
 - Search engines
 - Subscription sites
 - Specialised portals •
- User defined web sites •
- Newsfeeds
 - s Newsgroups

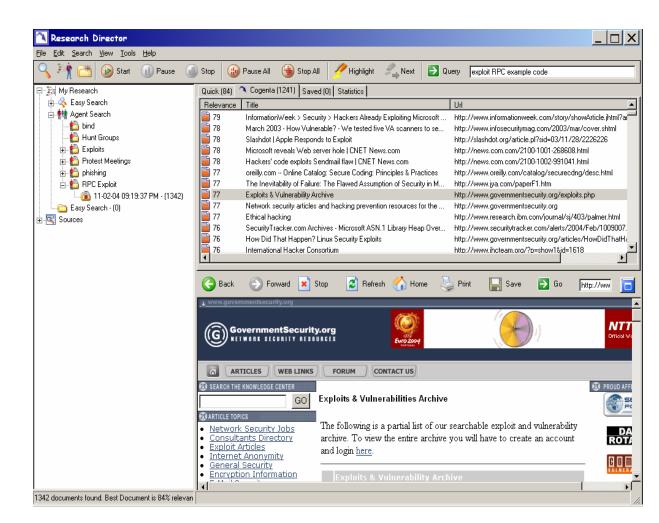
- Bulletin Boards
- Collect Information from parts of web not indexed by search engines (Hidden Web)
- Support multiple data formats
- Log-in search source capability
- Automate the search process with 'human' like abilities to translate, analyze and intelligently discover content
- Intelligently rank 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 coworkers – distributed analysis.
- Intelligent agents search hidden web
- Finds new sources
- Searches dynamically created web pages
- Documents ranked using computational linguistic algorithms
- Summarises documents





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
- lan.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

