JANUS Associates



Cyber Warfare
The Reality Is We Are
All Under Attack

Presented to: 2013 NYS Cyber Security Conference

Presented by: Matthew J. Lane, CIO



About JANUS Associates

Focused on Information Security and Business Continuity consulting since 1988

- Founded 1988, the oldest IT Security consultancy in the nation
- Privately held, woman-owned small business
- 25 Years serving government and business
- Locations in Stamford, Boston, Baltimore, Hartford











JANUS Areas Of Expertise

- Risk Management
- Information Security & Privacy
- Risk/Vulnerability Assessments
- Cloud Assessment and Security Services
- Smart Grid Assessment and Security Services
- Information Assurance
- Business Continuity and Disaster Recovery Planning
- Regulatory Compliance
- Security Awareness & Training
- 3rd Party Vendor Assessments
- Policy and Procedures
- Computer Forensics





JANUS Clients (partial)

ABC Television

Aetna Life & Casualty

Altura Energy (Occidental Petroleum)

Amnesty International

Asea Brown Boveri

Amoco

AT&T

Bath Iron Works

BlackRock Financial

Bausch & Lomb

Blue Cross/Blue Shield (multi -state)

Centers for Medicare/Medicaid

Services

Canadian Department of Defence

Charles Schwab & Co

Citibank

City of New York

Comm. of Massachusetts

ESPN

AXA/Equitable

Federal Aviation Admin (FAA)

Exxon Mobil

Federal Deposit Ins. Corp. (FDIC)

Federal Reserve Board of Gov

Gov't Accountability Office (GAO)

IBM

ITT Hartford

Incyte Genomics

Lockheed Martin

Metropolitan Life

Merrill Lynch

Microsoft

New York Power Authority

Oppenheimer Funds

Oregon State Lottery

Pacific Gas & Electric

Phoenix Life Insurance

Port Authority of NY & NJ

Santee Cooper

Social Security Administration

State of Florida

State of Maryland

State of New York

State of North Carolina

State of Texas

State of Wisconsin

State of Virginia

State of Wyoming

UCAL - Sacramento

Univ. of Massachusetts

University of Wisconsin

Texas A&M

US Customs

US Dept. of Interior

US EPA

Valley National Bank

VISA International

VW Credit Corp.

Wal-Mart



Food For Thought

"An integral part of warfare, the Peoples Liberation Army identifies Electronic Warfare as a way to reduce or eliminate U.S. technological advances."

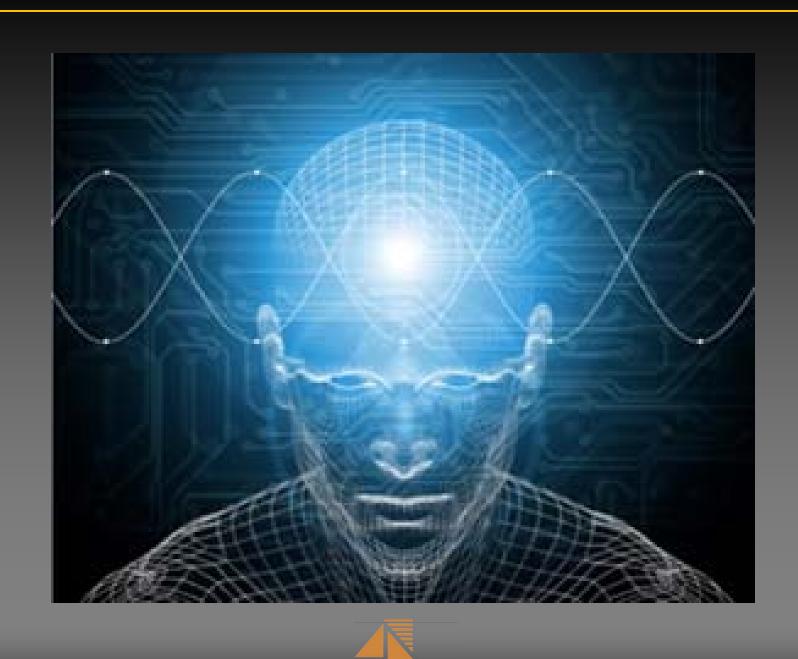
Annual report to congress, May 2013, Office of the Secretary of Defense

"I stand back in awe of the breadth, depth, sophistication, and persistence of the Chinese espionage effort against the United States of America." Former CIA and National Security Agency director Michael Hayden

"Well, there's no question that if a cyber-attack, you know, crippled our power grid in this country, took down our financial systems, took down our government systems, that that would constitute an act of war."

Secretary of Defense Leon Panetta





JANUS Associates

Hacker

- Made innovative modifications to electronics
- Modified Software
- Broke into Phone Systems
- Circumvents Computer Security



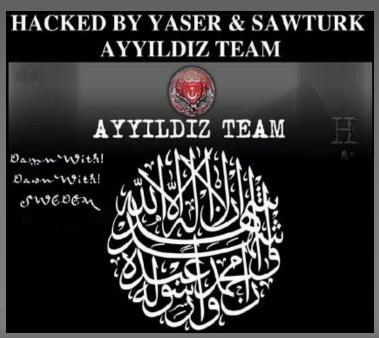


- Hacker
- Hacktivist
 - Political Motivation
 - Social Motivation
 - Non-violent
 - Independent





- Hacker
- Hacktivist
- Cyber Terrorist
 - Political Motivation
 - May be Violent
 - May be state sponsored





- Hacker
- Hacktivist
- Cyber Terrorist
- Cyber Criminal
 - Financially Motivated
 - Ties to Organized Crime
 - Majority in Eastern Europe





- Hacker
- Hacktivist
- Cyber Terrorist
- Cyber Criminal
- Cyber Warrior
 - State Sponsored
 - Traditional war activities





What is a Cyber War?

 A political mechanism to force another group of people to change and act differently





What is a Cyber War?

- A political mechanism to force another group of people to change and act differently
- An organized, prolonged, military conflict between sovereign entities



What is a Cyber War?

- A political mechanism to force another group of people to change and act differently
- an organized, prolonged, military conflict between sovereign entities
- It effects violence, aggression, and mortality



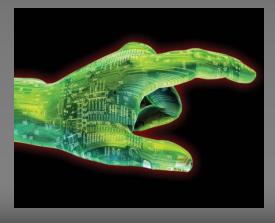


What Are Cyber Warriors After?

In the past the bad guys were after financial gain.

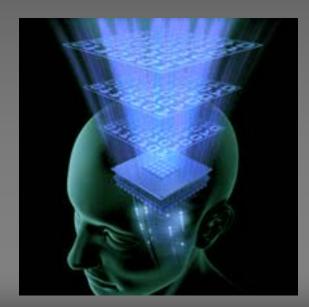
Today they are after everything

- Log On Information (User ID's & Passwords)
- Credit Card Information
- Intellectual Property
- Corporate Confidential Information
- Documents, Spreadsheets, Email, Images
- Access to Manufacturing Process Control



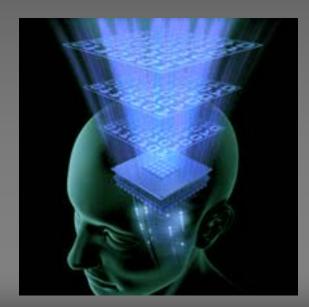


Reconnaissance



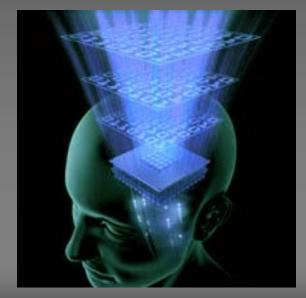


- Reconnaissance
- Espionage



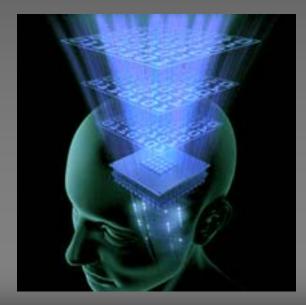


- Reconnaissance
- Espionage
- Arms Proliferation



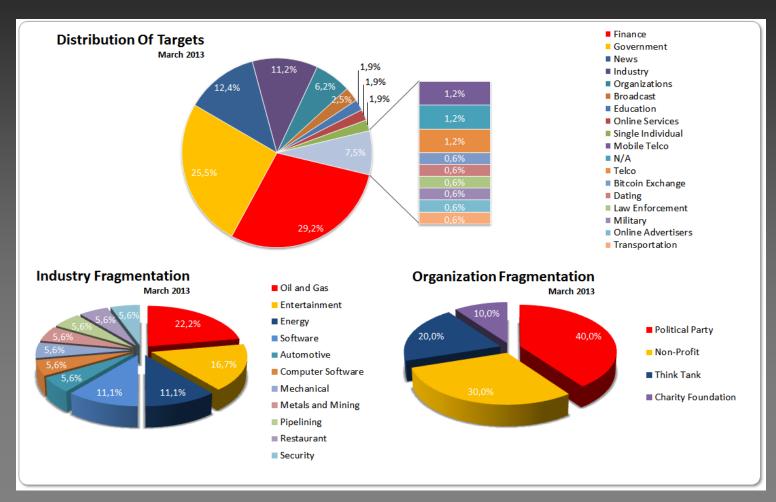


- Reconnaissance
- Espionage
- Arms Proliferation
- Aggression





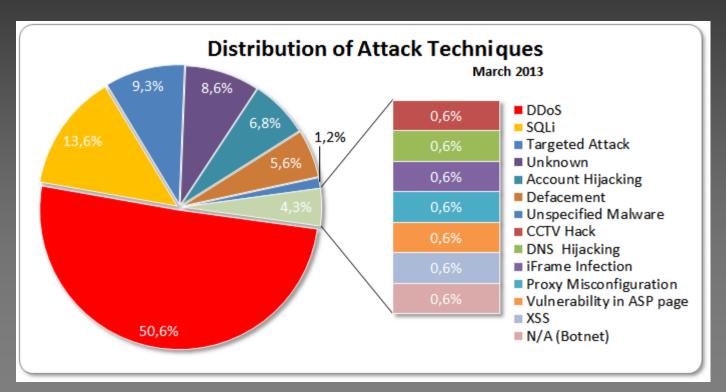
Cyber Warfare Distribution of Targets



^{*} Source: hackmageddon.com



Cyber Warfare Distribution of Attack Techniques



^{*} Source: hackmageddon.com



So Easy: A Six Year Old Can Do It!





Properly Responding To A Cyber Attack

- First Step Plan in Advance
 - Update Your Plan on a Regular Basis
 - Do a Table Exercise and Test Your Plan
- Notify the Proper Authorities
- Isolate and Protect Compromised System
- Document Everything
- Discuss on a Need to Know Basis





Hack-Back-Attack



Israeli Elite

@IsraeliElite

We are the Israeli Elite Force. BOW DOWN! Wanna join? #iEF @ efnet (for email browse the tweets)





Hack-Back-Attack

Escalate to traditional warfare





- Hack-Back-Attack
- Escalate to traditional warfare
- Buy more bandwidth





- Hack-Back-Attack
- Escalate to traditional warfare
- Buy more bandwidth
- Move to the Cloud





Internal Testing





- Internal Testing
- 3rd Party Testing





- Internal Testing
- 3rd Party Testing
- Cost Benefits





- Internal Testing
- 3rd Party Testing
- Cost Benefits
- What Should be Tested?





Purchase a similar looking domain

じ Log	In - M	lozilla I	Firefox						_OX
<u>F</u> ile	<u>E</u> dit	dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp							
-	•	🔷 🔻 🍪 👔 🔝 http://paypal-account-protection.com/eg/webscr.php?cmc 😂 🔻 🕟 💽 🔻 intitle:paypal							
	Pē		Pall'	8				Sign Up Log In Help	_
		Welc	ome	Send M	loney	Request Money	Merchant Tools	Auction Tools	
	Member Log In Secure Log In								
	Registered users log in here. Be sure to <u>protect your password</u> .								
	Email Address: Forget your email address?								
	Password: Forget your password?								
	New users <u>sign up here!</u> It only takes a minute.								
	Log In								
Done									11.



- Purchase a similar looking domain
- Set up an email for the domain





- Purchase a similar looking domain
- Set up an email for the domain
- Identify suspect classes of users



- Purchase a similar looking domain
- Set up an email for the domain
- Identify suspect classes of users
- Craft e-mail messages to each class of user





- Purchase a similar looking domain
- Set up an email for the domain
- Identify suspect classes of users
- Craft e-mail messages to each class of user
- Create Click Based attacks





- Purchase a similar looking domain
- Set up an email for the domain
- Identify suspect classes of users
- Craft e-mail messages to each class of user
- Create Click Based attacks
- Create attachment based attacks





- Purchase a similar looking domain
- Set up e-mail for the domain
- Identify suspect classes of users
- Craft e-mail messages to each class of user
- Create Click Based attacks
- Create attachment based attacks
- Generate statistics to improve process





Questions and Answers

JANUS Associates 1055 Washington Blvd. Stamford, CT 06901 www.janusassociates.com

Matthew J. Lane, CIO Office: 203-251-0229

matthewl@janusassociates.com

Lyle A. Liberman, COO Office: 203-251-0236

lylel@janusassociates.com



