

TrendCenter: Accelerating SANS GIAC



Todd Heberlin

todd@NetSQ.com

530-758-4338

Outline



- Introduction
- Sensor Grid
- Communication & Representation
- **Analysis**
- Interpretation
- **Examples**
- Conclusions

Introduction



- This presentation covers work performed under TrendCenter, an AFRL Phase I SBIR, and our tech-transition plans with SANS Global Incident Analysis Center (GIAC).
- TrendCenter was conceived as a disease surveillance system for the Internet.

Surveillance

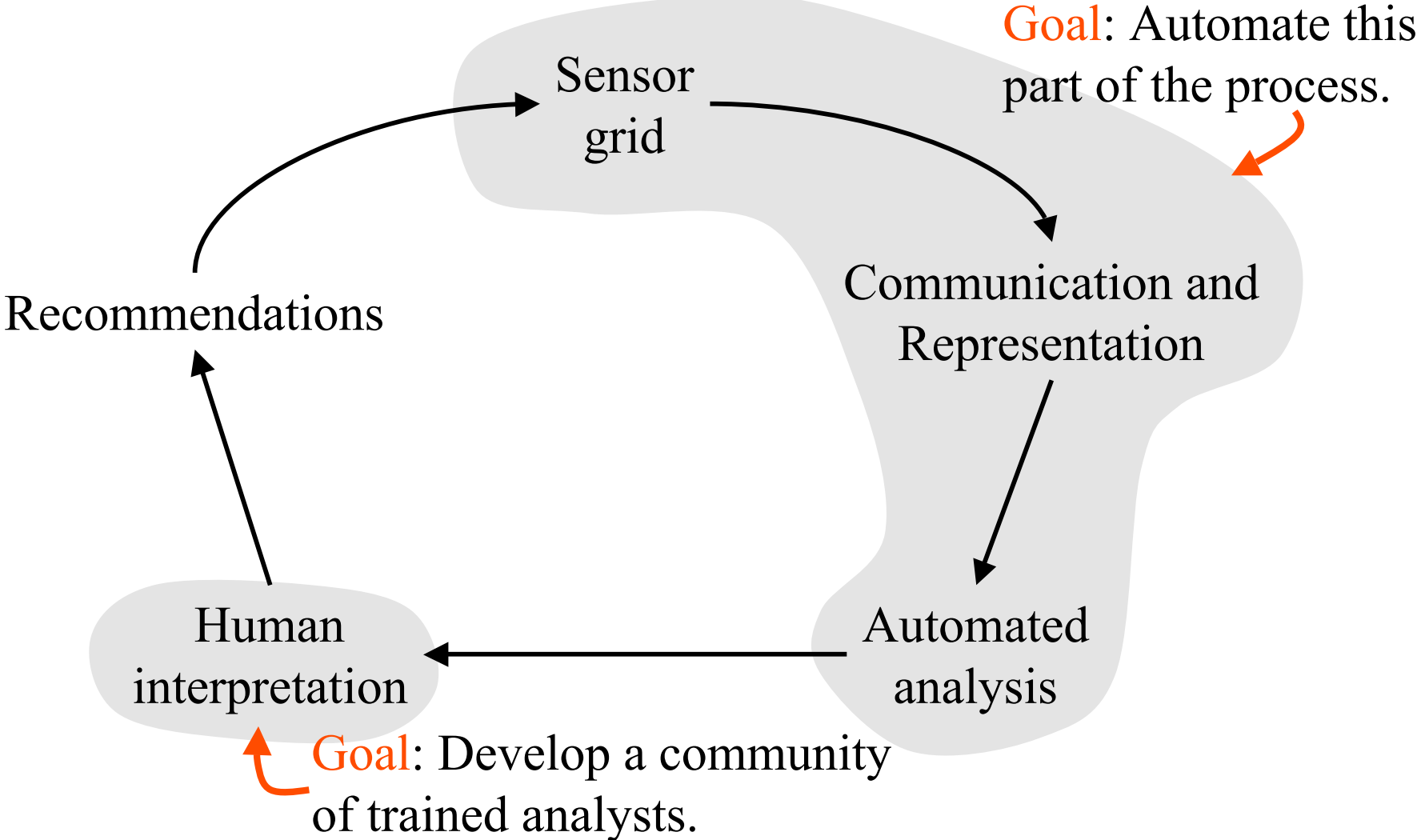


Surveillance is the *ongoing systematic* collection, collation, analysis and interpretation of data; and the dissemination of **information** to those who need to know in order that **action** may be taken.

Principles of Disease Surveillance
World Health Organization

<http://www.who.int/emc/slideshows/Survintro/sld001.htm>

The Process



Sensor Grid

- Initially focus on installed sensor base
- Early sensor targets include:
 - free IDSs (e.g., Snort)
 - market leading network IDSs
 - firewall logs
 - syslog, virus logs, host-based IDS logs later
- Our data/analysis improves existing sensors
- Opens door for more sophisticated sensors

Communication and Representation



- Moving data to site to be analyzed
 - HTTP used to upload data
 - IETF IDWG IAP under development
 - daily or continuous reporting?
- Aggregating and sanitizing of data
 - if a site has 64,000 addresses scanned, do we include a record for each incident?
- Database Representation
 - similar in difficulty to message representation by IDWG and CIDF before them

Outline

- Introduction
- Sensor Grid
- Communication & Representation
- **Analysis**
 - automated analysis
 - intrusion detection paradox
 - prediction
 - amazon model
- Interpretation
- **Examples**
- Conclusions

Automated Analysis



■ Simple

- top scanned ports
- trend analysis
- correlating attackers

■ Predictions

- what attacks are you most likely to see?

■ Data Mining

- structures in the data
- human interpretation required

Intrusion Detection

Paradox



- Most sensors today are only useful for detecting already known attacks with existing solutions.
 - Wouldn't it be better to simply apply the solution?
- Would the vast majority of administrators know what to do if a sensor reports a previously unknown attack against a previously unknown vulnerability?
 - It is hard enough to get people to use "Live Update"
 - Is there a commercial market for such sensors?

Detection to Prediction

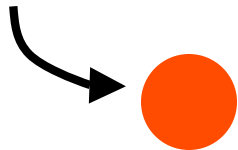


- Use sensors to predict the attacks before they occur
- Requires shared, correlated reporting
- Amazon model
 - Amazon has millions of books, but they have a very limited opportunity to present to you books they think you will buy.
 - There are hundreds or thousands of vulnerabilities at any site, but a system administrator has time to fix a small number.

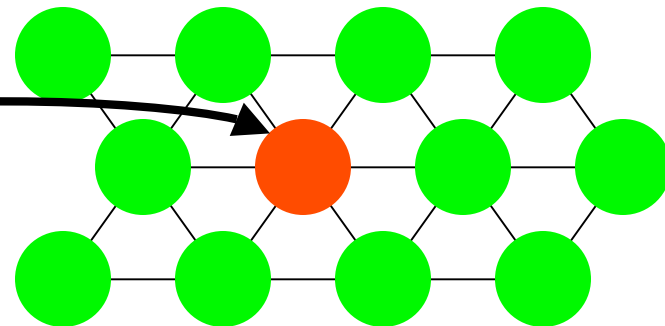
Prediction Requires a Community

- A single site by itself only knows what has already attacked it.
- It cannot have foresight.
- When part of a community sharing information, a site can **predict** what attacks it will probably see.

Site by itself



And part of a community



Amazon Techniques



- Top sellers
- Movers and Shakers
- Top sellers unique to your defined group
- Books purchased by those who look the most like you

Amazon Top Sellers



- Simple ranking of the biggest sellers
- Also broken down by topic area
- Our model: most detected attacks/probes
 - epidemic proportions
 - much of it launched by “script kiddies”
 - first rough cut as to what problems need to be fixed
 - could be broken down by OS or application
 - formalized “top threats”
 - eventually look for top anomalies


Amazon Movers & Shakers

- Biggest gainer in sales rank in the past 24 hours
- Possible future best sellers
- Our model: Rising threats
 - which vulnerabilities are most likely to be exploited
 - which exploits are most likely to become epidemics
 - time permitting, you might want to fix these problems

What Are Movers & Shakers?

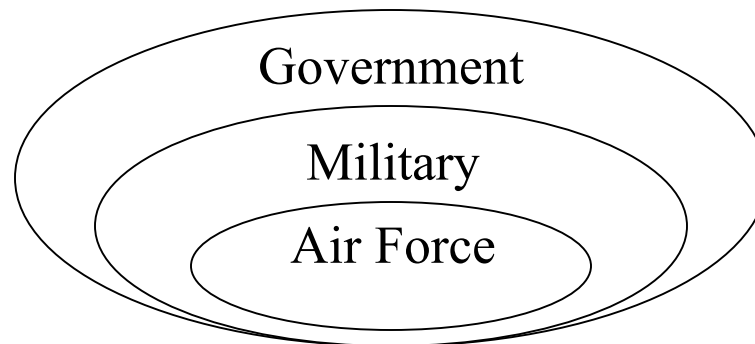
The biggest gainers in Amazon.com sales rank over the past 24 hours. [Learn more](#)

Movers & Shakers

- ▲ 718%
 [Boomer Babes](#)
by Linda Stasi,
Rosemary Rogers
 - ▲ 529%
 [Gold](#)
~ Abba
 - ▲ 562%
 [Gone in 60 Seconds](#)
DVD
~ Nicolas Cage
 - ▲ 1,036%
 [The Powerpuff Girls
Small Plush Doll \(Shiny
Dress\)](#)
by Trendmasters
- ▶ [See all the Movers & Shakers](#)

Amazon Purchase Circles

- Identifies top sellers unique to defined groups.
- Groups are defined a priori
- Our model:
 - may indicate an attack targeted at a specific group (e.g., Air Force or power grid)



Unique to U.S. Air Force



[Purchase Circles](#) > [Government](#) > [Military](#) > [U.S. Air Force](#)

Books: [Unique to U.S. Air Force](#)

More:

Pur
...

- 1 **Air Power: A Centennial Appraisal**
- 2 **They Also Flew: The Enlisted Pilot Legacy, 1912-1942**
- 3 **Victor Padrini: A Novel of the United States Air Force Academy**
- 4 **The Limits of Air Power: The American Bombing of North Vietnam**

These books are important to people in the Air Force. What attacks might be unique to the Air Force, and should we pay closer attention to them?

Unique to U.S. Navy



[Purchase Circles](#) > [Government](#) > [Military](#) > [U.S. Navy](#)

Books: Unique to U.S. Navy

More:

- 1 Jane's Fighting Ships 1999-2000**
- 2 Jane's Fighting Ships 2000-2001**
- 3 The Naval Institute Guide to Naval Writing**
- 4 Naval Operations Analysis**

Bestsellers for U.S. Air Force



[Purchase Circles](#) > [Government](#) > [Military](#) > [U.S. Air Force](#)

Books: [Bestsellers for U.S. Air Force](#)

More:

- 1 **Harry Potter and the Goblet of Fire**
- 2 **Harry Potter and the Chamber of Secrets**
- 3 **Harry Potter and the Sorcerer's Stone**
- 4 **Harry Potter and the Prisoner of Azkaban**

Activity unique to Air Force, and perhaps most important to the Air Force, is lost in the noise.

Amazon Recommendations



- 1 Web Navigation: Designing the User Experience**
- 2 Data Mining Solutions: Methods and Tools for Solving Real-World Problems**
- 3 Information Architects**
- 4 The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography**
- 5 Data Mining Your Website**

Based on similar buyers. Our model? Look for similar victims.

Human Interpretation



- Even today's sensors are capable of detecting new and subtle threats, but few can understand what is being detected.
- Structures found within large amounts of distributed data will need to be interpreted.
- Too many operating systems, applications, protocols, and programming languages.
 - No single organization can field the expertise to diagnose all potential new threats.

Outline

- Introduction
- Sensor Grid
- Communication & Representation
- **Analysis**
- Interpretation
- **Examples**
 - portal/community
 - data submission & instant value
 - top threats & subtle threats
 - need for community
- Conclusions

Net Squared's GIAC R&D Effort - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print

Address http://www.netsq.com/GIAC/proto.php3

Net²

Automated GIAC Prototype

Overview

- [Home](#)
- [GIAC](#)
- [SANS](#)
- [Net Squared, Inc.](#)
- [Submit Report](#)
- [Events](#)
- [Resources](#)

GIAC's Threat Level

THREAT LEVEL ▶

Welcome to SANS GIAC prototype for automated event reporting and analysis. If you have had an incident, please [Submit a Report](#)

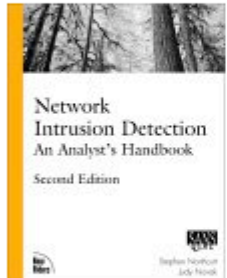
Top Threats

Top Ports

1. **515** Print Spool
2. **21** FTP
3. **109** POP-2
4. **510** Unknown
5. **21121** Unknown

[More ...](#)

Featured Book



Stephen Northcutt, SANS instructor extraordinaire, updates his classic book on

Security News From The Net

- [Any port is a hacker storm](#), NWFusion
- [Senate panel presses FBI on Carnivore](#), ZDNet
- ['Romeo and Juliet' Virus Strikes MS Outlook](#), TechTV
- [Nothing Romantic About New Romeo & Juliet Virus - GFI](#), NewsBytes
- [Romeo and Juliet virus could end in PC tragedy](#), Silicon.com
- [Denial of Service Attacks Planned For Christmas](#), ComputerUser

Low and Slow

1. **6699** Napster
2. **20** FTP Data
3. **6688** Napster
4. **8311** Unknown
5. **4922** Unknown

On The Rise

1. **6972** Unknown
2. **6973** Unknown
3. **6974** Unknown
4. **100** Unknown

Popular Readings in Computer Security

1. [Secrets and Lies : Digital Security in a Networked World](#), Bruce Schneier
2. [Building Internet Firewalls](#), Elizabeth D. Zwicky

Internet



Instant view of overall threat level.

Top threats (“fix these problems”), with drill down for details.

Security related news and entertainment. Helps to keep visitors abreast of the issues, and helps bring them back to the site regularly.

Tools and educational material to improve the communities skills.

Popular Readings in Computer Security

1. [Secrets and Lies : Digital Security in a Networked World](#), Bruce Schneier
2. [Building Internet Firewalls](#), Elizabeth D. Zwicky


GIAC Incident Information Entry - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print

Address <http://www.netsq.com/GIAC/DataEntry/index.php3> Go

Net² GIAC Incident Information Data Entry



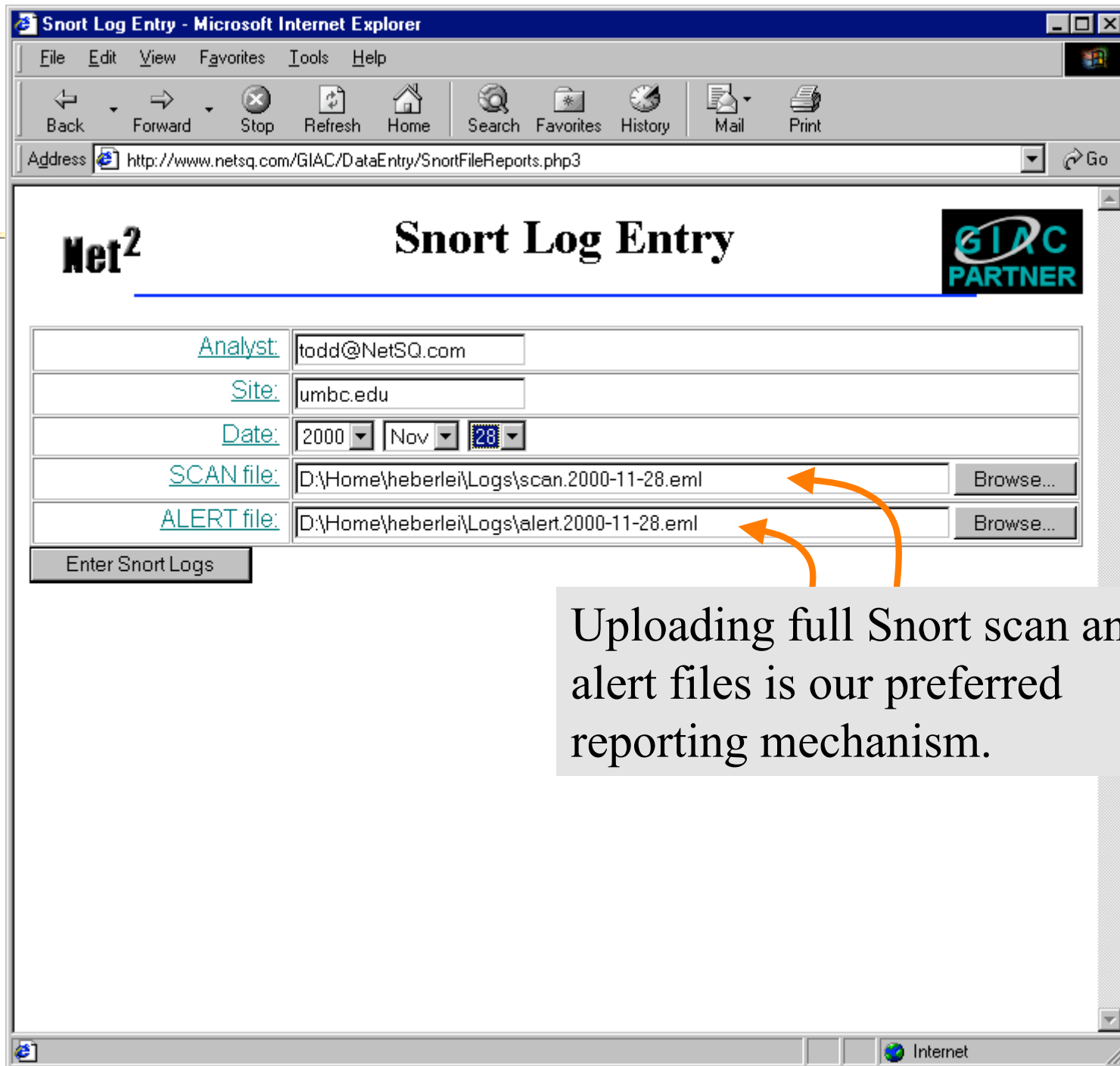
Welcome To SANS GIAC's incident information center. We accept attack reports from around the Internet, perform basic trend analysis and correlation to spot attack patterns that may be too subtle to detect from a single site. We also support an army of analysts to interpret new and interesting attack patterns.

Your data can go a long way to making the Internet as a whole a much safer place in which to work, shop, and play, so we encourage you to notify us whenever your system or site is probed. In return for your data, we will perform instant analysis on it and providing you with immediate feedback.

Currently we are only accepting reports of probes to specific port and if available, snort scan or alert report files. The information in the latter data is much richer, and so whenever possible, we encourage you to post this data.

- **Probe Report.** Has an attacker probed your system? If so, enter your information here.
- **Snort Reports.** Do you have Snort attack or scan logs? If so, upload the log files here.

<http://www.netsq.com/GIAC/DataEntry/SnortFileReports.php3> Internet



Uploading full Snort scan and alert files is our preferred reporting mechanism.

GIAC Snort File Submission - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address http://www.netsq.com/GIAC/DataEntry/SnortFileReportsSubmit.php3

Net² GIAC Analysis

Scan Summary

Rank	Port	Attackers	Targets
1	109	1	1912
2	27374	2	1462
3	4336	3	3
4	10	2	3
5	633	1	3

Alert Summary

Rank	Port	Description	Attackers	Targets
1	109	SYN-FIN scan!		
2	32771	Attempted Sun RPC high port a		
3	1080	WinGate 1080 Attempt		
4	-1	Tiny Fragments - Possible Hostile		
5	633	Queso fingerprint		

No Correlation on scanning hosts.

Done Internet

After submission of the Snort logs, we summarize information in the scan and alert log files.

If any of the hosts scanning your network also scanned another network in the last 30 days, we report the correlation

GIAC Entry - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print

Address http://www.netsq.com/GIAC/top_scans.php3 Go

Net²

Top Probed Ports


Recent Activity				Previous Month	
Rank	Port	Score	Targets	Rank	Score
1	515	100	59672	9	1.39304
2	21	43.4006	25898	1	100
3	109	3.6399	2172	new	new
4	27374	3.21759	1920	2	58.9977
5	510	0.517831	309	new	new
6	21121	0.286567	171	new	new
7	6970	0.189369	113	new	new
8	100	0.184341	110	new	new
9	6972	0.167583	100	new	new
10	6976	0.142445	85	new	new
11	6974	0.14077	84	new	new
12	23	0.110605	66	5	5.65481
13	6699	0.0754123	45	12	0.546986
14	6971	0.0553023	33	new	new
15	6977	0.0519507	31	new	new
16	31337	0.0502748	30	7	1.93806

Internet

GIAC Entry - Microsoft Internet Explorer

Address http://www.netsq.com/GIAC/top_scans.php3

Probed Ports



Rank	Port	Score	Targets	Previous Month	
				Rank	Score
1	515	100	59672	9	1.39304
2	21	43.7006	25898	1	100
3	109	3.6399	2172	new	new
		3.21759	1920		
		0.517831	309		
		0.286567	171		
		0.189369	113		
8	100	0.184341	110		
9	6972	0.167583	100		
10	6976	0.142445	85	new	new
11	6974	0.14077	84	new	new
12	23	0.110605	66	5	5.65481
13	6699	0.0754123	45	12	0.546986
14	6971	0.0553023	33	new	new
15	6977	0.0519507	31	new	new
16	31337	0.0502748	30	7	1.93806

515, the print spool server port, is the most heavily probed port. This reflects active use of attack scripts.


The most actively probed port receives a relative score of 100.

The previous month (days 11-40), it only ranked 9th with a relative score of 1.3. This indicates new scripts tools are being actively used

GIAC Entry - Microsoft Internet Explorer

Address http://www.netsq.com/GIAC/top_scans.php3

Net² Top Probed Ports



				Previous Month	
			Targets	Rank	Score
1	515	100	59672	9	1.39304
2	21	43.4006	25898	1	100
3	109	3.6399	2172	new	new
4	27374	3.1759	1920	2	58.9977
5	510	0.517831	309		
		0.286567	171		
		0.189369	113		
		0.184341	110		
		0.167583	100		
		0.142445	85	new	new
11	6974	0.14077	84	new	new
12	23	0.110605	66	5	5.65481
13	6699	0.0754123	45	12	0.546986
14	6971	0.0553023	33	new	new
15	6977	0.0519507	31	new	new
16	31337	0.0502748	30	7	1.93806

109, the port for the old version of POP, is ranked 3rd.

Its relative score is 3.6, so it is probed only 3.6% as much as port 515.

However, it was not even on the charts during the previous month, so we should keep an eye on this one.

There is currently a low and slow probing of ports 6688 and 6699.

Each probe consists of only one packet to one target.

Date	Source	Dst Port	Probe Type	Count
2000-09-30	24.113.198.51	6688	2*SF**A*	1
2000-09-30	24.22.255.16	6688	21SF****	1
2000-09-30	65.33.16.3	6688	***F****	1
2000-09-30	65.33.16.3	6688	21*FR*AU	1
2000-10-01	129.93.198.104	6688	*1S**P**	1
2000-10-01	195.132.25.237	6688	**S**P*U	1
2000-10-01	204.126.150.4	6688	21SF****	1
2000-10-01	24.201.107.159	6688	2*****U	1
2000-10-02	211.108.230.134	6688	*1**R*AU	1
2000-10-02	24.112.44.237	6688	21*FRPAU	1
2000-10-02	195.132.36.195	6688	***F*P**	1
2000-10-02	24.92.215.107	6688	****RP*U	1
2000-10-02	200.241.102.70	6688	2*SFRPA*	1
2000-10-02	205.143.221.235	6688		1
2000-10-02	205.143.223.65	6688		1
2000-10-02	157.182.33.208	6688		1
2000-10-06	200.52.51.139	6688		1
2000-10-07	129.2.150.96	6688		1
2000-10-08	129.93.209.218	6688	21***P*U	1
2000-10-08	195.132.148.29	6688	*1SF*PA*	1

There is a small but steady 1-3 probes per day from many different IP addresses.

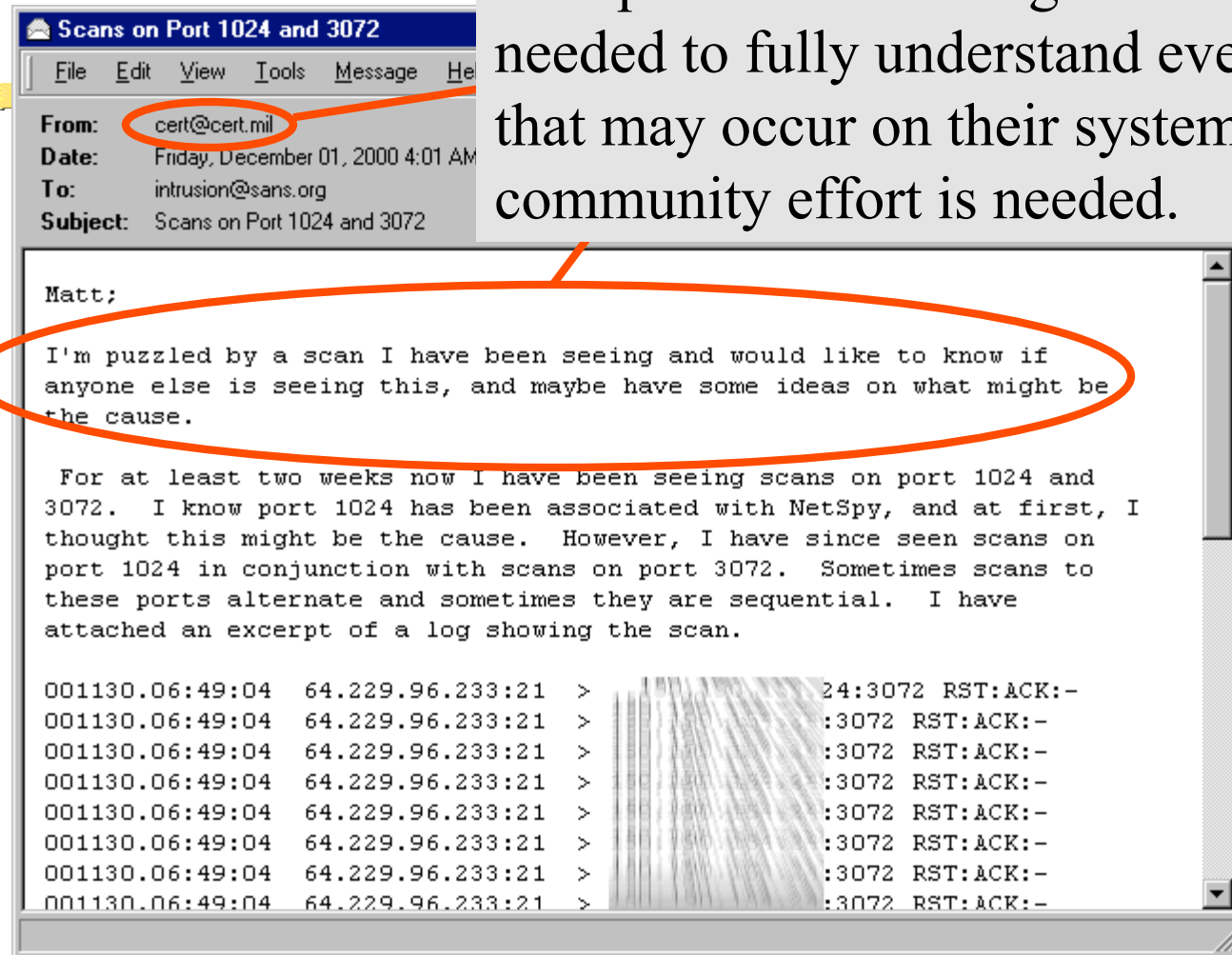
TCP flag settings are clear indications these are indeed probes.

Mystery of the 6688 Probe



- Why are people (or a single person?) probing 6688?
 - Is there an unknown vulnerability?
 - Is the music industry secretly determining who is using Napster?
- Why are they probing it at such a low level?
- Are these single probes from many sources part of a coordinated activity?

No one organization can field the depth of expertise or the range of sensors needed to fully understand everything that may occur on their systems. A community effort is needed.



Conclusions



- We have been building a disease surveillance system under a Phase I SBIR.
- Creating an integrated sensor grid greatly enhances the value of the sensors.
 - Detect subtle attacks
 - Moves us from detection & reaction to prediction & preparation
- Operational prototype has already demonstrated the plausibility and value of this approach.