

# ***Computer Intrusion Threat Assessment System***

*Presented by*



**CITAS**

# ***Task Force Mission***

Identify and investigate computer intrusion matters in accordance with the investigative priorities established by the Department of Defense (DOD) and Department of Justice (DOJ) of the United States of America.

# ***Task Force Goals***

- Provide a technical solution to assess cyber threats targeting unclassified computer networks affecting our national security & economic wellbeing.
  - Real-time data analysis
  - Static log analysis
  - Global event correlation

# Philadelphia Regional Computer Intrusion Task Force

*Law Enforcement*



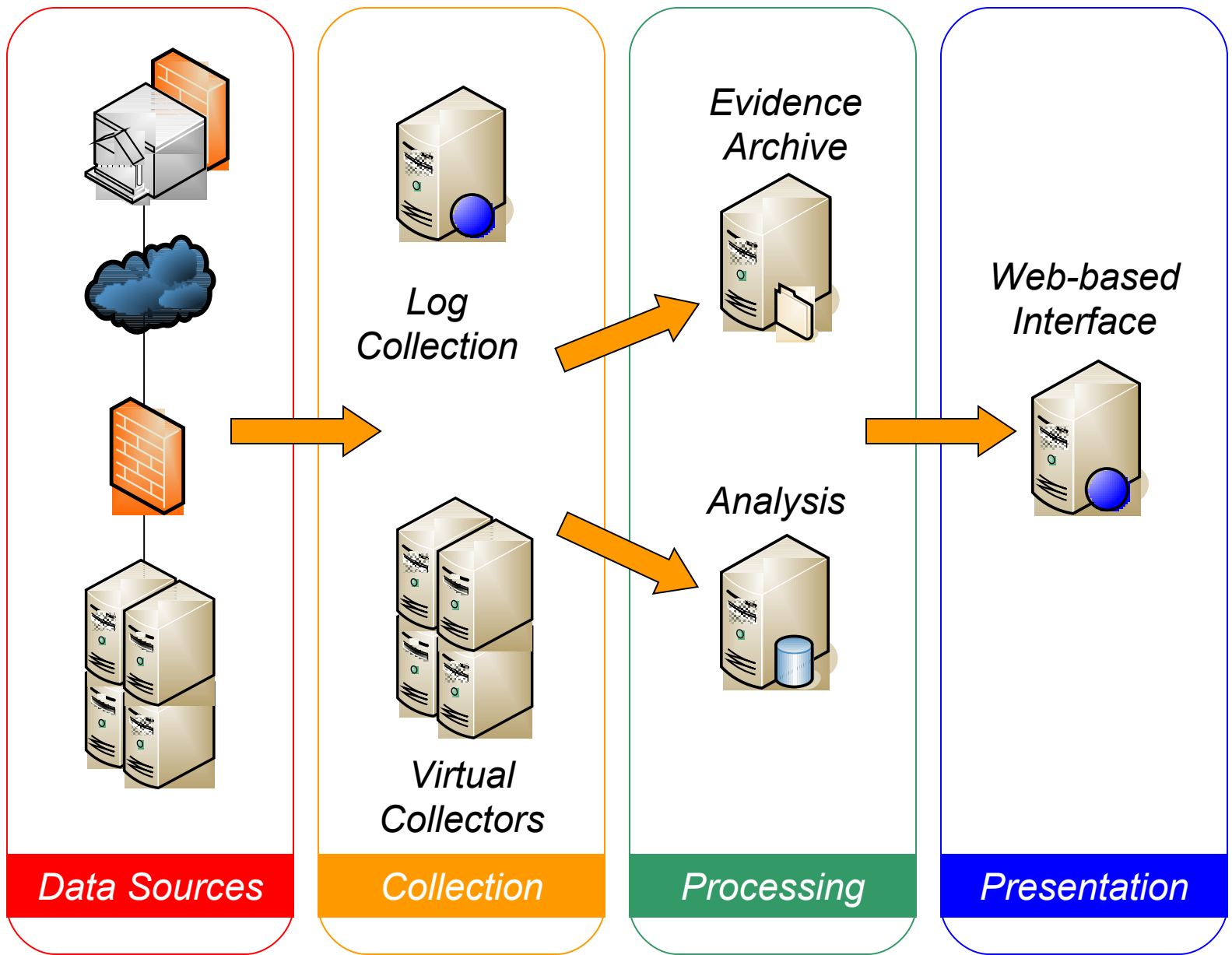
*Technical Support*



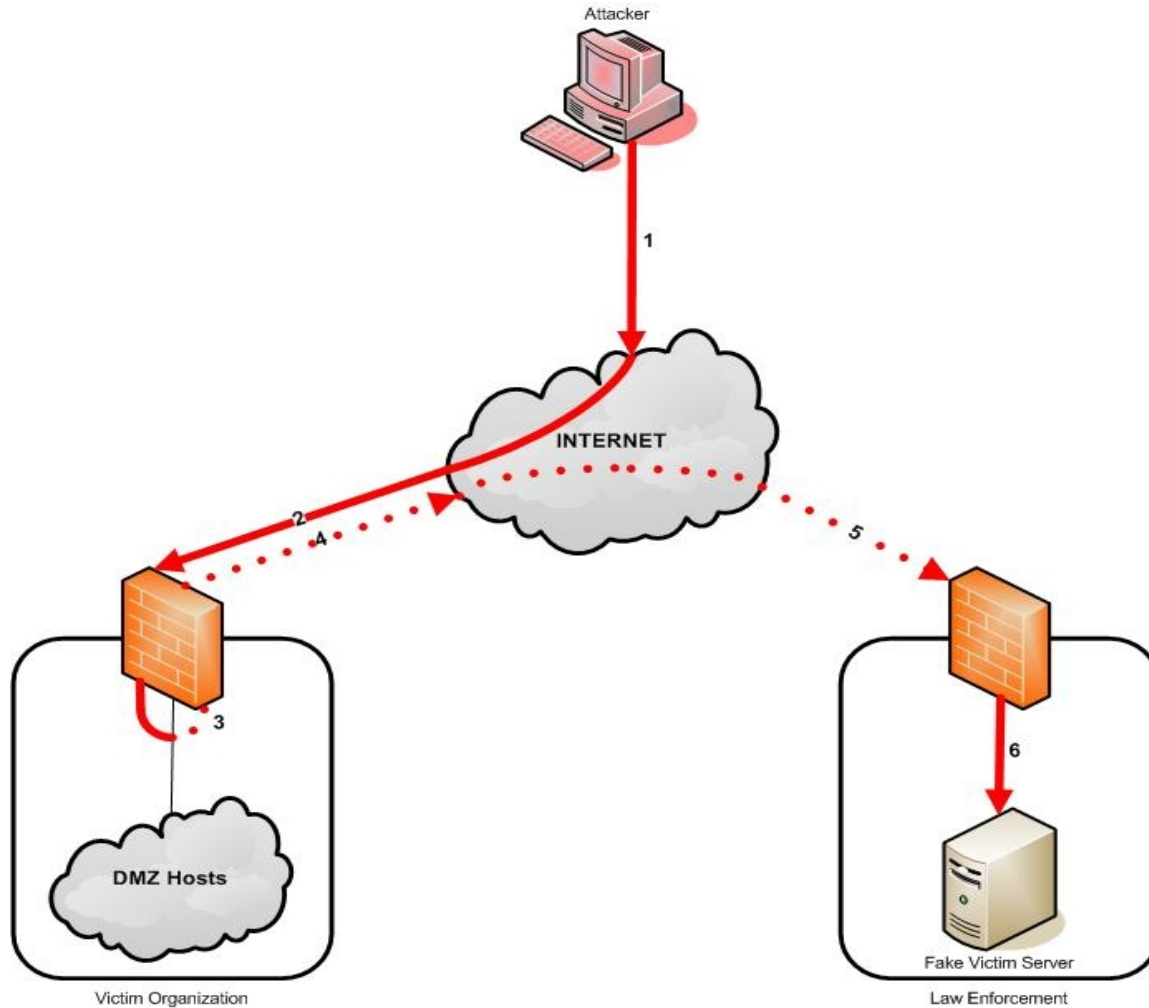
*Working together to protect the National Information Infrastructure*

**CITAS**

# ***How it Works***



# Threat Redirection



# ***Legal Authority***

LE network monitoring under this project is accomplished under an exception to the **Wiretap Act - 18 U.S.C. 2510**

**18 U.S.C. 2511(2)(c) – Consent Exception**  
lawful to intercept electronic communication where one party to the communication has given prior consent to the interception

# ***DOJ Requirements***

- Signed consent from participants
- Use of network banners on open ports, *where possible*
- Network-based and Host-based Intrusion Detection Systems
- Rate limiting of outbound connections
- 24/7 Alerting with a remote VPN disconnect capability

# ***General Participation Requirements***

- Point of contact (POC) for technical support & incident response
- InfraGard membership for POC
- Signed consent form
- Internet routable IP for VPN connections
- Permission to use public web page content for decoy machine

# ***Participation Benefits***

- No cost host threat monitoring
- Law Enforcement analysis of anomalous network activity and reporting
- Improved incident response to cyber threats for source identification and location
- Potentially enhance regulatory compliance requirements
- Enhancing our National Infrastructure Protection (NIP)

# ***Public Relations Risk Mitigation***

- System not intended for criminal prosecutions
- LE assumes liability for all deployed sensors (cost, build, maintenance)
- No public disclosure of company participation in the project
- No public disclosure of a sensor's identity

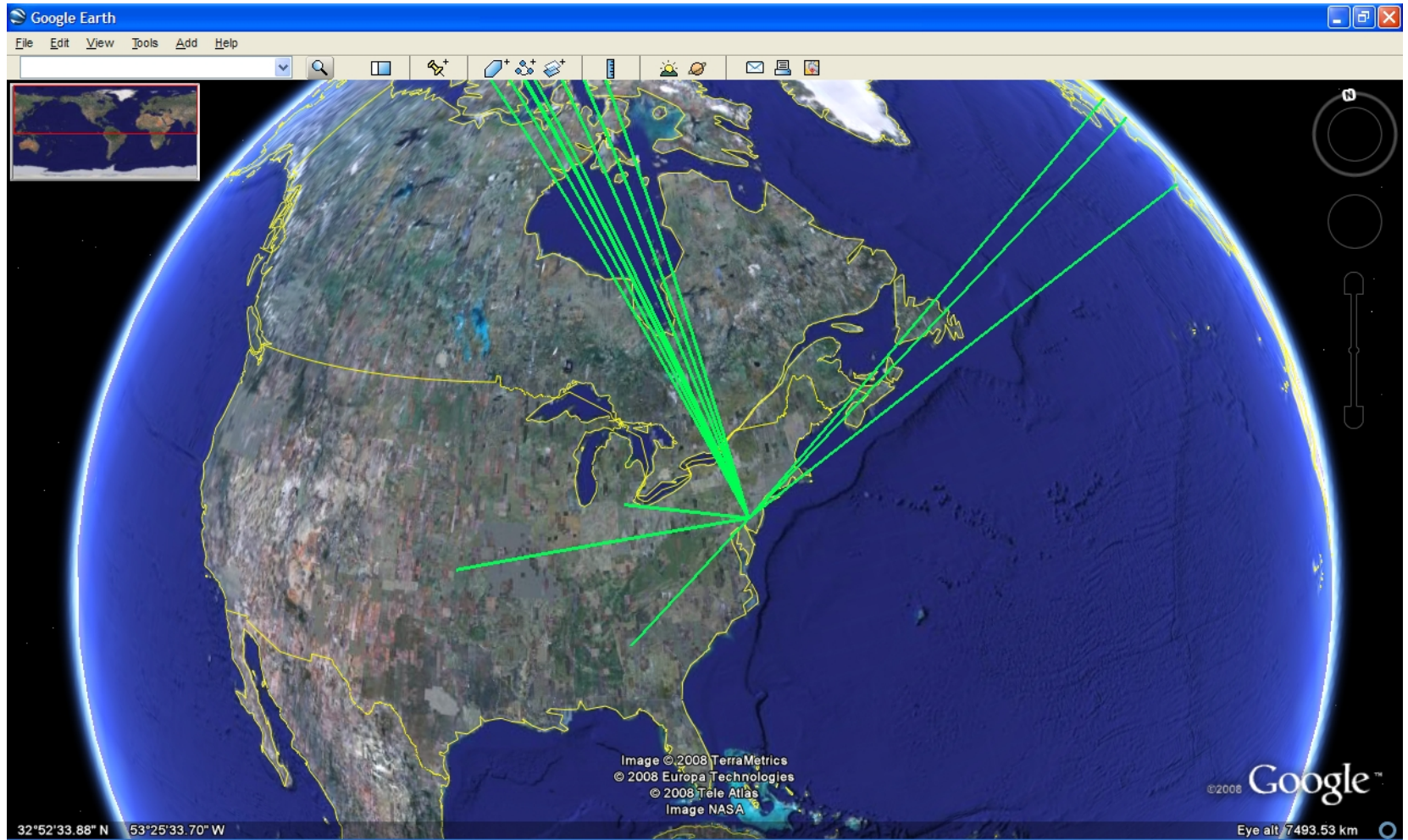
# ***Project Goals***

- Automate log sharing to improve cyber threat identification
- Anonymize logs to allow peer review and cross network correlation
- Establish compromised computer traffic redirection procedures for ongoing LE analysis
- Utilize NIST Common Criteria approved products

# ***Sample Analysis***

# Sample Analysis

## Google Earth


















CITAS



# Sample Analysis

## Attacking Countries List

Date	IP SRC	DNS	Occurances	Origin	Flag
2008-11-29 12:26:39	<a href="#">218.10.111.106</a>	218.10.111.106	14	China	
2008-11-29 14:22:32	<a href="#">221.192.199.36</a>	221.192.199.36	7	China	
2008-11-29 21:59:49	<a href="#">202.99.11.99</a>	202.99.11.99	6	China	
2008-11-29 15:53:54	<a href="#">218.75.199.50</a>	218.75.199.50	6	China	
2008-11-29 12:02:02	<a href="#">221.233.242.4</a>	221.233.242.4	6	China	
2008-11-29 14:41:16	<a href="#">218.71.136.106</a>	218.71.136.106	6	China	
2008-11-29 12:18:23	<a href="#">122.30.248.224</a>	p5224-ipbf801sapodori.hokkaido.ocn.ne.jp	6	Japan	
2008-11-29 14:48:42	<a href="#">219.133.37.42</a>	219.133.37.42	6	China	
2008-11-30 18:28:40	<a href="#">82.223.148.105</a>	mlwd696.servidoresdns.net	5	Spain	
2008-11-29 20:26:04	<a href="#">60.223.101.196</a>	60.223.101.196	3	China	
2008-11-29 18:17:40	<a href="#">222.82.249.235</a>	222.82.249.235	3	China	
2008-11-29 22:29:29	<a href="#">60.222.224.138</a>	60.222.224.138	3	China	
2008-11-30 19:04:52	<a href="#">201.6.244.26</a>	c906f41a.static.virtua.com.br	3	Brazil	
2008-11-30 01:44:41	<a href="#">125.64.17.179</a>	125.64.17.179	3	China	
2008-11-29 17:57:27	<a href="#">218.23.142.157</a>	157.142.23.218.broad.static.hf.ah.cndata.com	3	China	
2008-11-29 19:57:52	<a href="#">124.171.111.185</a>	124-171-111-185.dyn.iinet.net.au	3	Australia	
2008-11-30 11:11:44	<a href="#">60.190.202.170</a>	60.190.202.170	3	China	
2008-11-29 19:59:42	<a href="#">220.250.21.226</a>	220.250.21.226	3	China	

# Sample Analysis

## All Countries

### INBOUND DENIES

#### Top 30 Inbound Denies

##	IP Address	Count	Region
1	204.141.87.33	4621	
2	204.141.87.24	3822	
3	205.234.175.175	2369	
4	65.207.183.121	2306	
5	204.141.87.17	1898	
6	204.141.87.18	1850	
7	68.142.228.136	1358	
8	204.141.87.19	1020	
9	221.192.199.36	878	
10	204.141.87.35	723	
11	66.102.1.165	641	
12	66.235.139.62	634	
13	208.111.160.6	578	
14	64.154.84.74	549	
15	192.221.110.123	519	
16	66.235.139.54	484	
17	66.235.138.2	482	
18	76.13.6.132	476	
19	66.179.104.138	472	
20	216.74.37.170	460	
21	204.141.87.9	452	
22	74.125.242.89	442	
23	146.145.153.236	414	
24	64.235.139.103	400	

			Source				Destination			
Seq	Date	Prot	Origin	Location	Port	GIS	Origin	Location	Port	GIS
46802120	Oct 07 2008	tcp	outside	66.235.133.2	80		inside		9898	
46802119	Oct 07 2008	tcp	outside	66.235.133.2	80		inside	· · ·	9898	
46802118	Oct 07 2008	tcp	outside	66.235.133.2	80		inside	· · ·	9898	
46802117	Oct 07 2008	tcp	outside	66.235.133.2	80		inside	· · ·	9898	
46802094	Oct 07 2008	tcp	outside	66.235.133.2	80		inside	· · ·	9892	
46802093	Oct 07 2008	tcp	outside	66.235.133.2	80		inside	· · ·	9892	
46802092	Oct 07 2008	tcp	outside	66.235.133.2	80		inside	· · ·	9892	
46802088	Oct 07 2008	tcp	outside	66.235.133.2	80		inside	· · ·	9892	
46802087	Oct 07 2008	tcp	outside	66.235.133.2	80		inside	· · ·	9892	
46802003	Oct 07 2008	tcp	outside	198.99.107.37	80		inside	· · ·	9891	
46802002	Oct 07 2008	tcp	outside	198.99.107.37	80		inside	· · ·	9891	
46802001	Oct 07 2008	tcp	outside	198.99.107.37	80		inside	· · ·	9891	
46802000	Oct 07 2008	tcp	outside	198.99.107.37	80		inside	· · ·	9891	
46801999	Oct 07 2008	tcp	outside	198.99.107.37	80		inside	· · ·	9891	
46801998	Oct 07 2008	tcp	outside	198.99.107.37	80		inside	· · ·	9891	
46801997	Oct 07 2008	tcp	outside	198.99.107.37	80		inside	· · ·	9891	
46801925	Oct 07 2008	tcp	outside	204.141.87.17	80		inside	· · ·	9827	
46801917	Oct 07 2008	tcp	outside	204.141.87.18	80		inside	· · ·	9834	
46801916	Oct 07 2008	tcp	outside	204.141.87.24	80		inside	· · ·	9831	
46801915	Oct 07 2008	tcp	outside	204.141.87.33	80		inside	· · ·	9823	
46801914	Oct 07 2008	tcp	outside	66.235.139.62	80		inside	· · ·	9837	
46801913	Oct 07 2008	tcp	outside	66.235.139.62	80		inside	· · ·	9837	
46801912	Oct 07 2008	tcp	outside	204.141.87.17	80		inside	· · ·	9827	
46801911	Oct 07 2008	tcp	outside	204.141.87.18	80		inside	· · ·	9834	
46801910	Oct 07 2008	tcp	outside	204.141.87.24	80		inside	· · ·	9831	
46801909	Oct 07 2008	tcp	outside	204.141.87.33	80		inside	· · ·	9823	
46801908	Oct 07 2008	tcp	outside	66.235.139.62	80		inside	· · ·	9837	
46801907	Oct 07 2008	tcp	outside	204.141.87.17	80		inside	· · ·	9827	
46801906	Oct 07 2008	tcp	outside	204.141.87.18	80		inside	· · ·	9834	

# *Summary*

- Threat Redirection
- Analysis of anomalous network activity with Law Enforcement reporting
- Improved incident response for threat source identification and location
- Failsafe shutdown capabilities

# ***CITAS Development Team***

- Brian Schaeffer
- Russell Handorf
- Bill Toffel
- Mitch Parker
- Jose Ortiz

# ***Thank You***

Richard Marr, DCIS  
Richard.Marr@dodig.mil  
610-595-1904 ext 223

John Chesson, FBI  
John.Chesson@ic.fbi.gov  
215-418-4579