LA-UR- 11-06782

Approved for public release;
distribution is unlimited.

Title: How Open IOC Saved My Life and Others

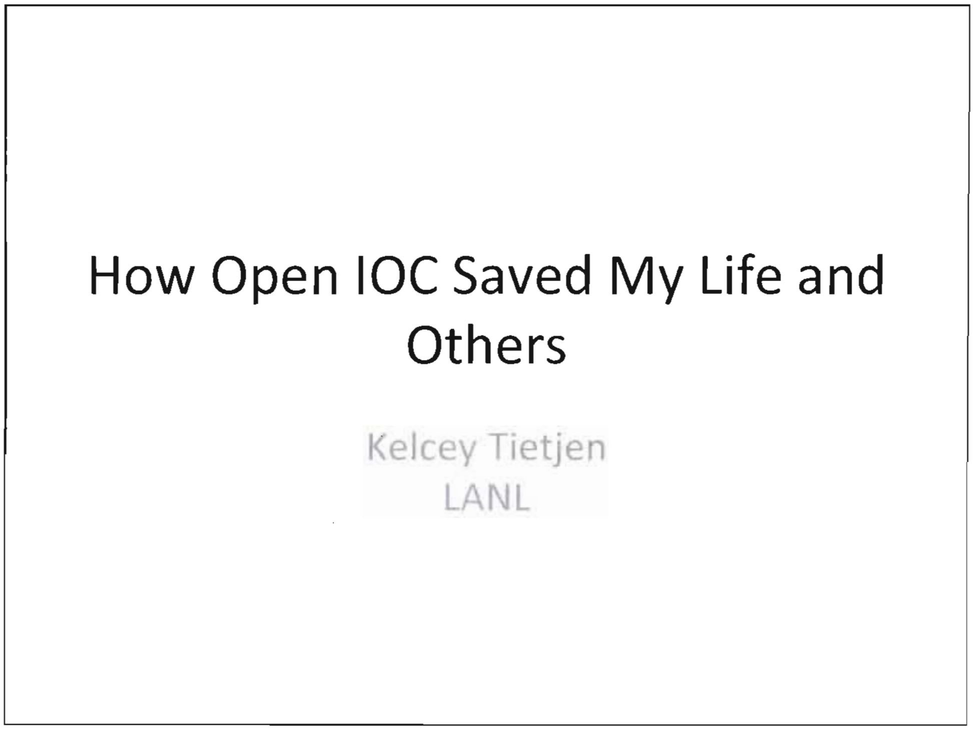
Author(s): Kelcey Tietjen

Intended for: MIRCon

Los Alamos
NATIONAL LABORATORY
EST. 1943

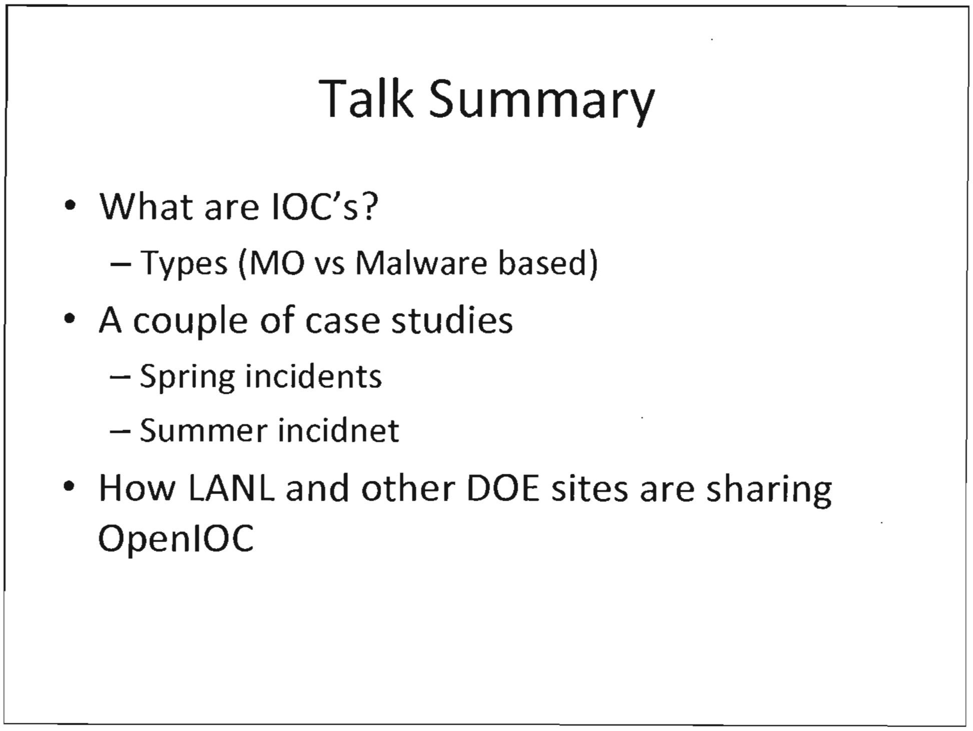
How OpenIOC Saved My Life and Others

This session will be about the active use of the OpenIOC format. OpenIOC can be used in a manner to keep the velocity of an incident from slowing down. Use cases will be discussed where the OpenIOC format has been used to quickly and near effortlessly help several separate entities with rapid incident response. The case studies discussed will show how the IOCs, and other incident data, are being shared across multiple entities as well. This distributed model of sharing information and resources are increasing each entities ability to detect, defend, respond, and remediate to advanced targeted attacks.



How Open IOC Saved My Life and Others

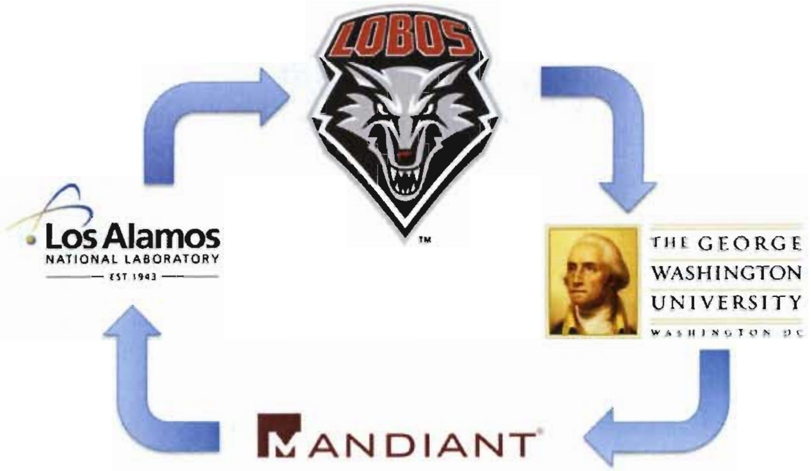
Kelcey Tietjen
LANL

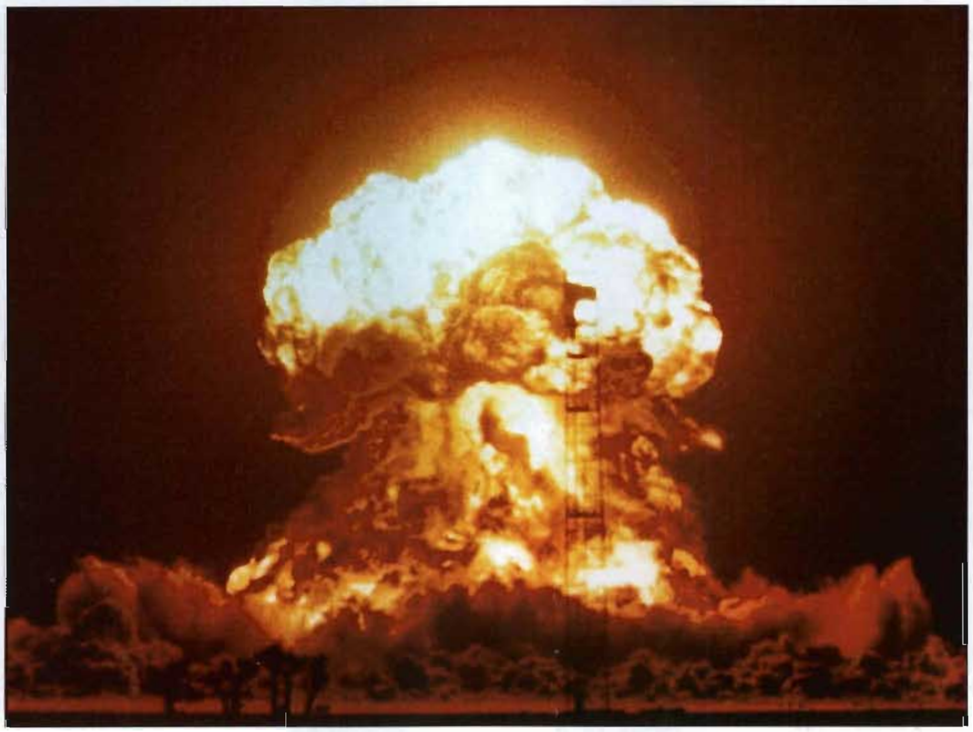


Talk Summary

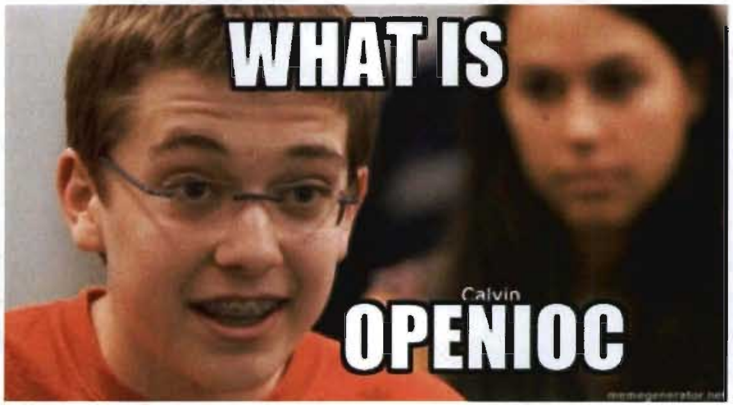
- What are IOC's?
  - Types (MO vs Malware based)
- A couple of case studies
  - Spring incidents
  - Summer incidnet
- How LANL and other DOE sites are sharing OpenIOC

Who Am I


LOBOS
Los Alamos
NATIONAL LABORATORY
EST 1943
THE GEORGE
WASHINGTON
UNIVERSITY
WASHINGTON DC
MANDIANT

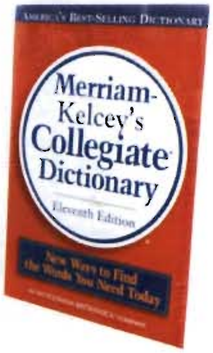


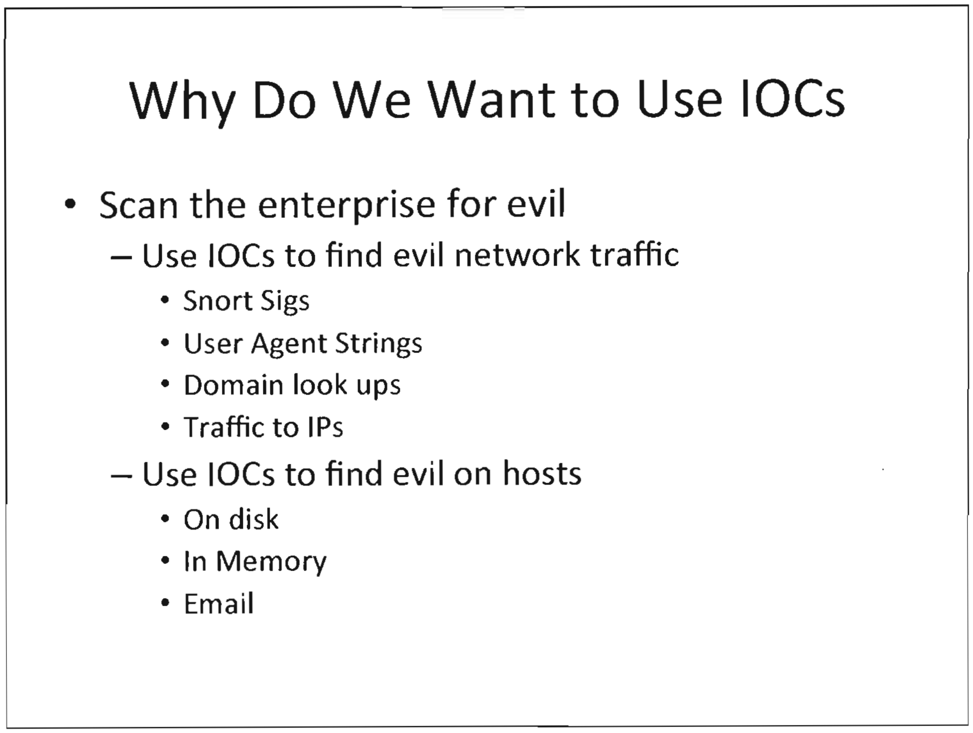
Indicators of Compromise (IOCS)



What is an IOC

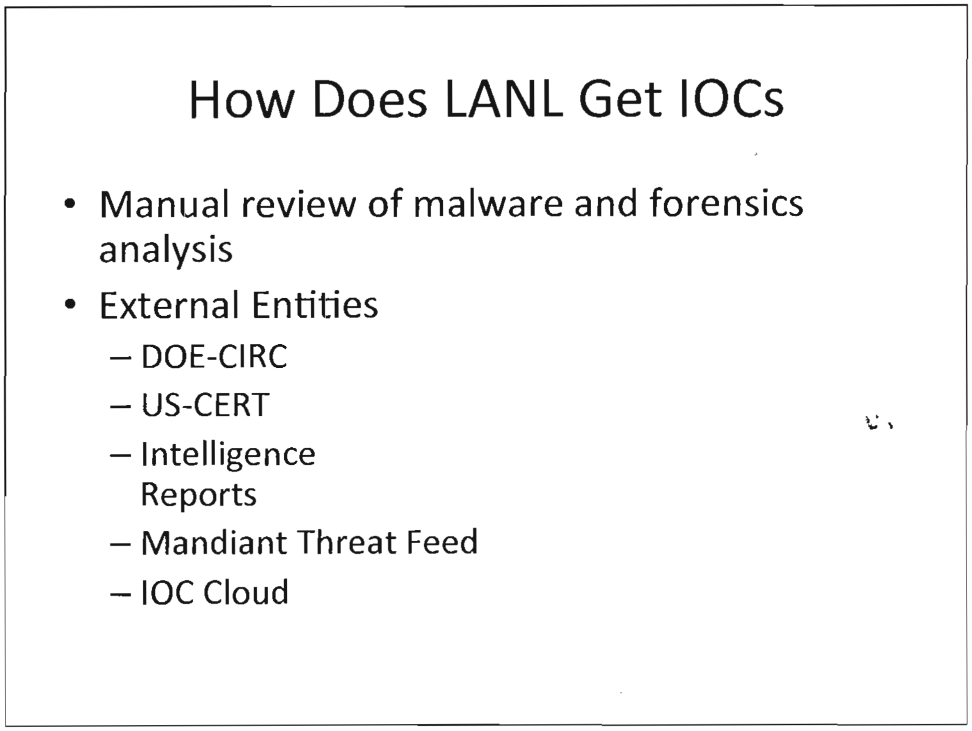
- Kelcey's dictionary definition
  - "The evidence on a system showing the host has been affected by an adversary"
- Urban dictionary definition
  - "Your system is pwned"


America's Best-Selling Dictionary
Merriam-Kelcey's
Collegiate
Dictionary
Eleventh Edition
New Ways to Find the Words You Need Today



Why Do We Want to Use IOCs

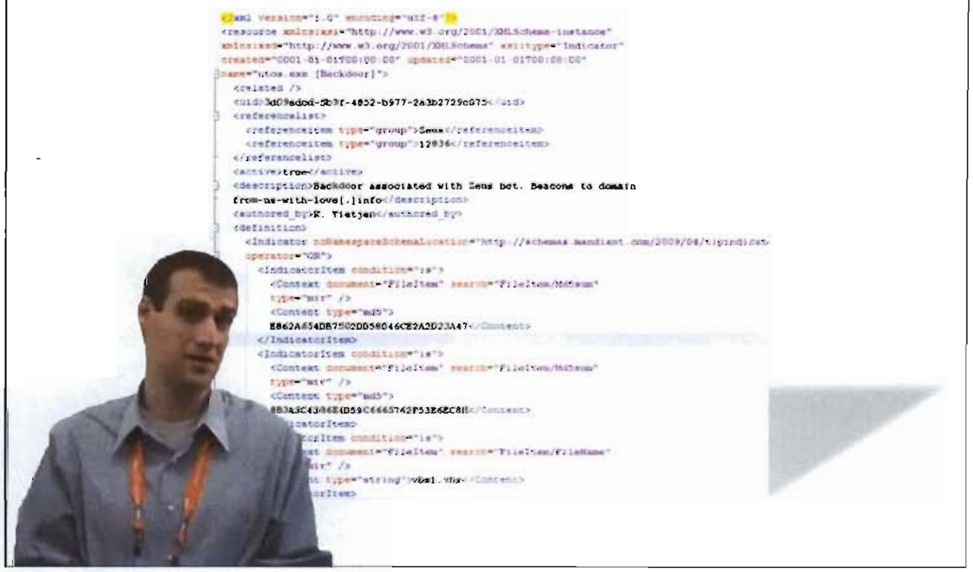
- Scan the enterprise for evil
  - Use IOCs to find evil network traffic
    - Snort Sigs
    - User Agent Strings
    - Domain look ups
    - Traffic to IPs
  - Use IOCs to find evil on hosts
    - On disk
    - In Memory
    - Email



How Does LANL Get IOCs

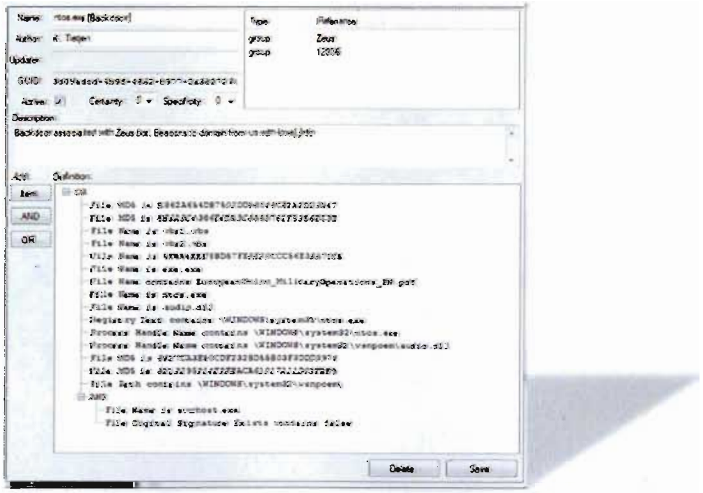
- Manual review of malware and forensics analysis
- External Entities
  - DOE-CIRC
  - US-CERT
  - Intelligence Reports
  - Mandiant Threat Feed
  - IOC Cloud

What Do They Look Like?



```
<?xml version="1.0" encoding="utf-8"?>
<resource xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xsi:type="Indicator"
created="0001-01-01T00:00:00" updated="0001-01-01T00:00:00"
name="ntos.exe [Backdoor]">
  <related />
  <uid>3d09adod-5b9f-4852-b977-2a3b2729c075</uid>
  <referencelist>
    <referenceitem type="group">Zeus</referenceitem>
    <referenceitem type="group">12036</referenceitem>
  </referencelist>
  <active>true</active>
  <description>Backdoor associated with Zeus bot. Beacons to domain
  from-us-with-love[.]info</description>
  <authored_by>K. Tietjen</authored_by>
  <definition>
    <Indicator xsiNamespaceSchemaLocation="http://schemas.mandiant.com/2009/08/tipindicat
    operator="OR">
      <IndicatorItem condition="is">
        <Content document="FileItem" search="FileItem/Md5sum"
        type="mir" />
        <Content type="md5">
        E862A654DB7502DD58046CE2A2D23A47</Content>
      </IndicatorItem>
      <IndicatorItem condition="is">
        <Content document="FileItem" search="FileItem/Md5sum"
        type="mir" />
        <Content type="md5">
        8B3A3C4386E4D59C6665742F53E6EC8B</Content>
       icatorItem>
        torItem condition="is">
          xt document="FileItem" search="FileItem/FileName"
          ir" />
          t type="string">vbs1.vbs</Content>
        orItem>
```

What Do They Look Like?



Name: ntos.exe [Backdoor]

Author: K. Tietjen

Updater:

GUID: 3d09adod-5b9f-4852-b977-2a3b2729c0

Active: ☑ Certainty: 0 Specificity: 0

Type	Reference
group	Zeus
group	12036

Description:

Backdoor associated with Zeus bot. Beacons to domain from-us-with-love[.]info

Definition:

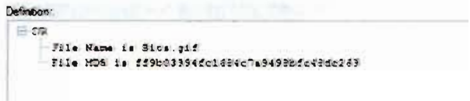
```
OR
  File MD5 is E862A654DB7502DD58046CE2A2D23A47
  File MD5 is 8B3A3C4386E4D59C6665742F53E6EC8B
  File Name is vbs1.vbs
  File Name is vbs2.vbs
  File Name is [illegible]
  File Name is exe.exe
  File Name contains EuropeanUnion_MilitaryOperations_EN.pdf
  File Name is ntos.exe
  File Name is audio.dll
  Registry Text contains \WINDOWS\system32\ntos.exe
  Process Handle Name contains \WINDOWS\system32\ntos.exe
  Process Handle Name contains \WINDOWS\system32\wsnpoem\audio.dll
  File MD5 is [illegible]
  File MD5 is [illegible]
  File Path contains \WINDOWS\system32\wsnpoem\
  AND
    File Name is svchost.exe
    File Digital Signature Exists contains false
```

What Format Are These IOCs Stored In?

- OpenIOC
  - It's Open
  - It's Extensible
  - Provides Context
  - More than just a list
    - Provides logic trees
  - You can add your own terms
  - You can easily share them in real time

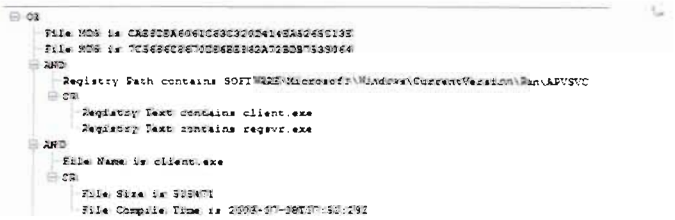
Simple vs. Complex IOCs

- Simple basic OR indicator

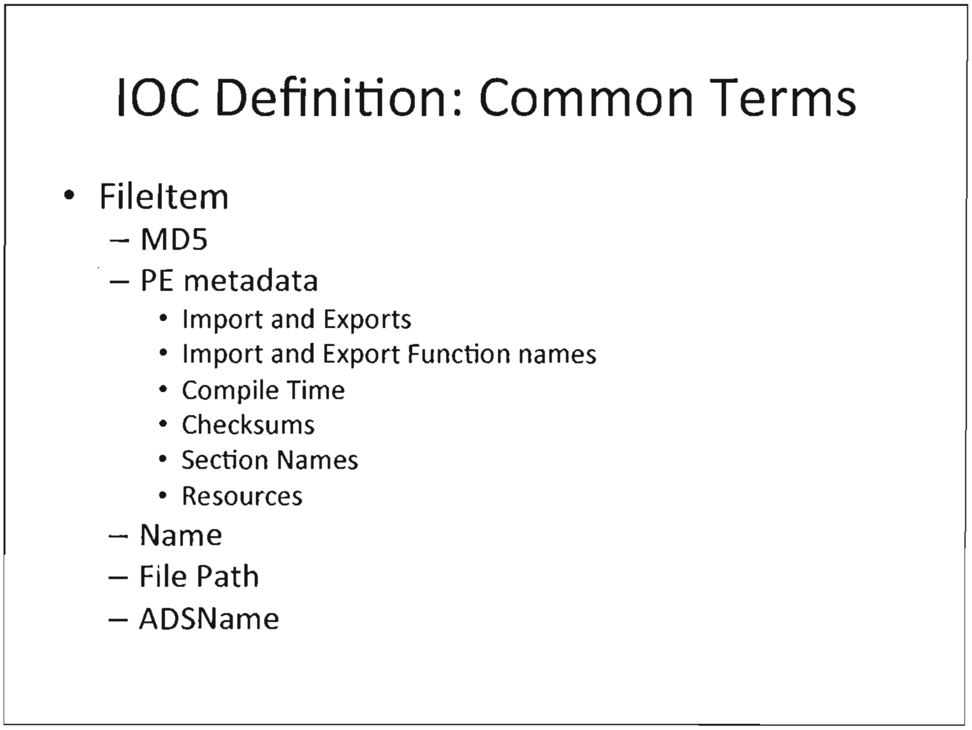


```
Definition:
⊟ OR
   File Name is Sics.gif
   File MD5 is f59b03394fc1684c7a9493bfc49dc263
```

- Complex multiple indicators

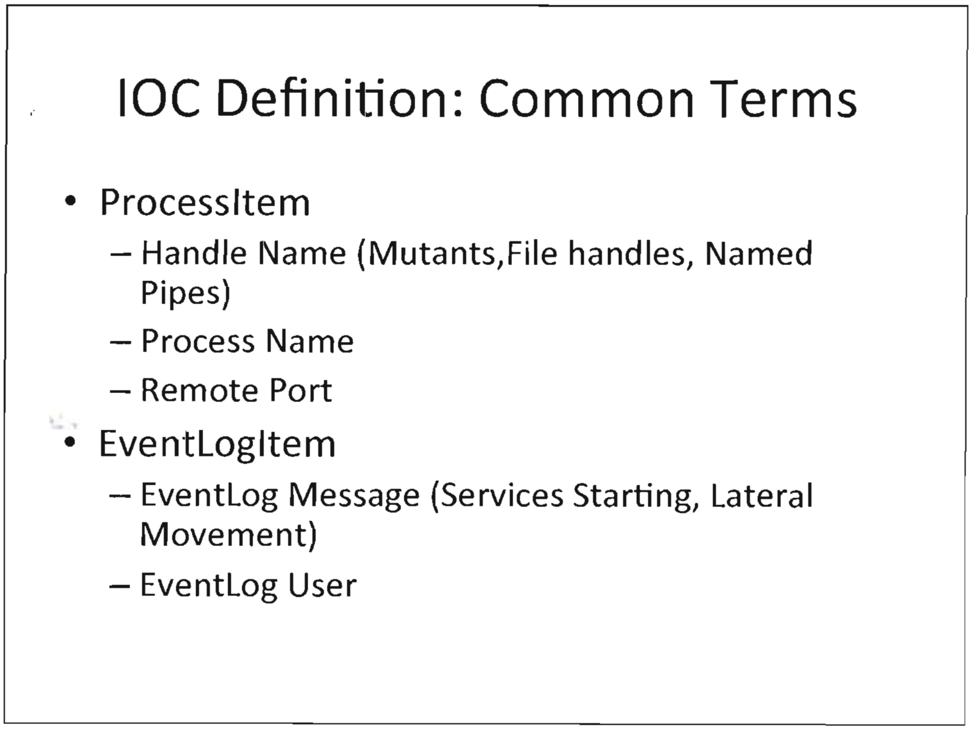


```
⊟ OR
   File MD5 is CA8FDEA6061C63C3202414EA5265C13E
   File MD5 is 7C5686C8670DB6BE842A72BDB7539064
  ⊟ AND
     Registry Path contains SOFTWARE\Microsoft\Windows\CurrentVersion\Run\APVSVC
    ⊟ OR
       Registry Text contains client.exe
       Registry Text contains regsvr.exe
  ⊟ AND
     File Name is client.exe
    ⊟ OR
       File Size is 525471
       File Compile Time is 2008-07-08T17:52:29Z
```



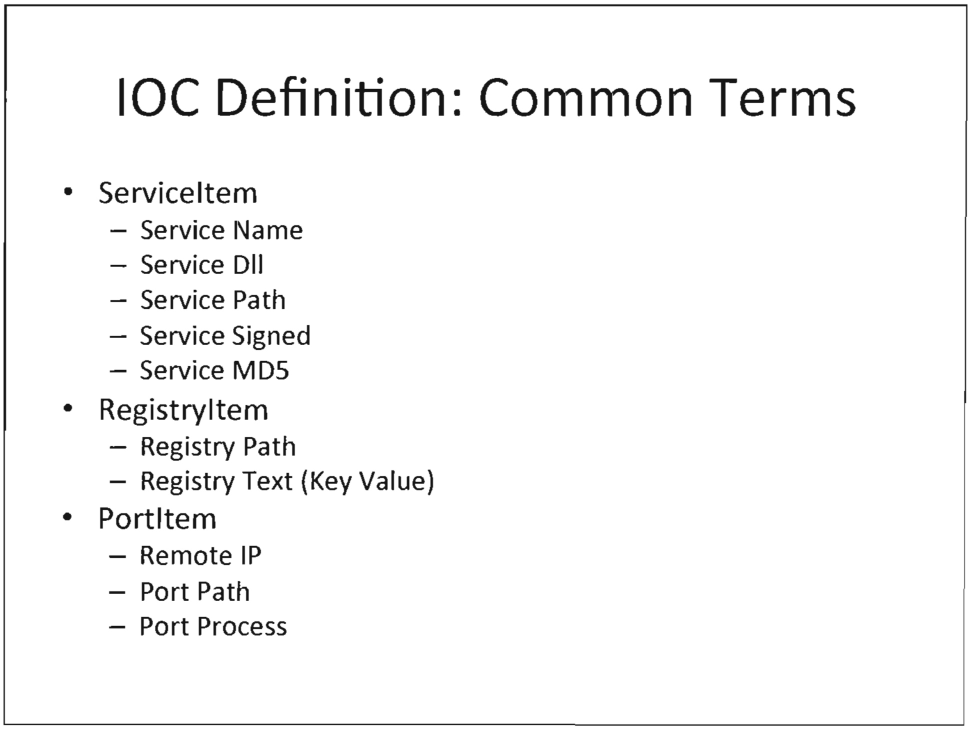
IOC Definition: Common Terms

- FileItem
  - MD5
  - PE metadata
    - Import and Exports
    - Import and Export Function names
    - Compile Time
    - Checksums
    - Section Names
    - Resources
  - Name
  - File Path
  - ADSName



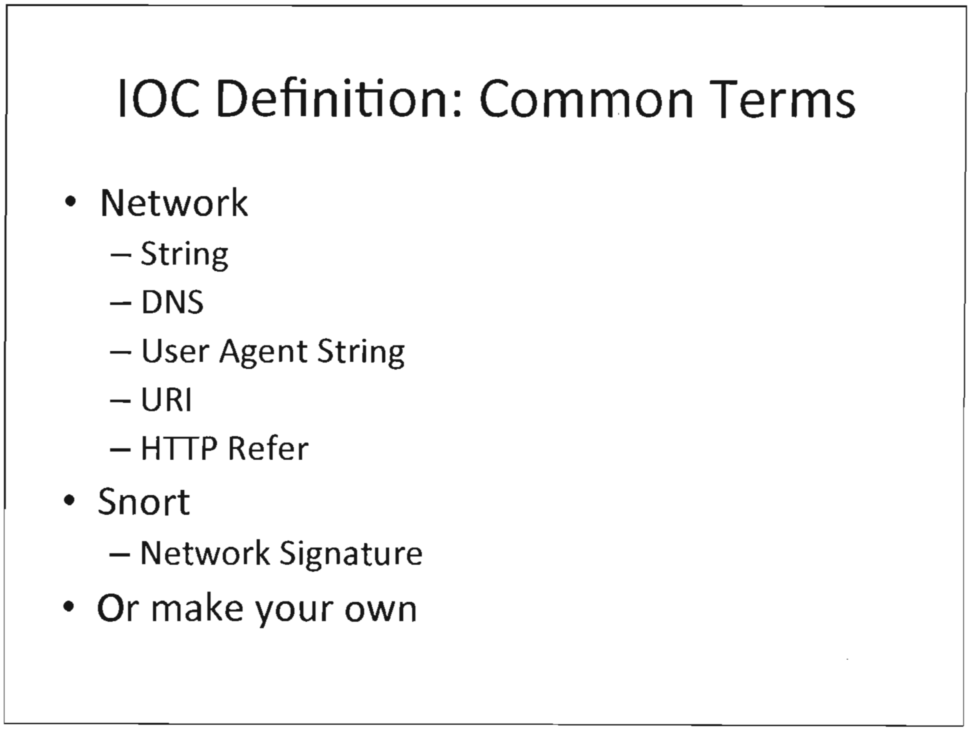
IOC Definition: Common Terms

- ProcessItem
  - Handle Name (Mutants,File handles, Named Pipes)
  - Process Name
  - Remote Port
- EventLogItem
  - EventLog Message (Services Starting, Lateral Movement)
  - EventLog User



IOC Definition: Common Terms

- ServiceItem
  - Service Name
  - Service Dll
  - Service Path
  - Service Signed
  - Service MD5
- RegistryItem
  - Registry Path
  - Registry Text (Key Value)
- PortItem
  - Remote IP
  - Port Path
  - Port Process



IOC Definition: Common Terms

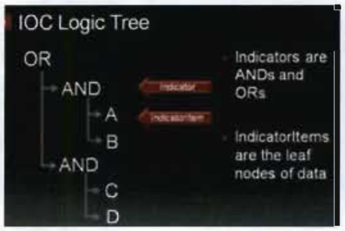
- Network
  - String
  - DNS
  - User Agent String
  - URI
  - HTTP Refer
- Snort
  - Network Signature
- Or make your own

Indicator Types

- Malware specific
  - Pertains specifically to the malware. (Files created, process hiding, import function, compile time)
- Modus Operandi
  - Pertains to the attackers actions while on the network. (Event Log messages, usernames, data storage locations)

Use of Logic Trees

- Svchost.exe (bad file name)
- Better
  - Filename = Svchost.exe
  - Path = C:\windows\
  - Filesize [0 to 20000]
  - File Import Name is “ws2_32.dll”

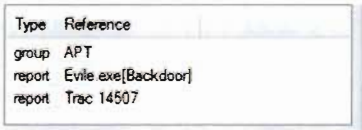


IOC Logic Tree

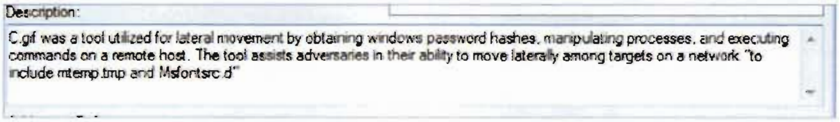
- Indicators are ANDs and ORs
- IndicatorItems are the leaf nodes of data

Context

- Groups
- Category
  - What does the malware do
- Report IDs (Ticket Numbers)
- Short Description
  - What does the malware or IOC Represent



Type	Reference
group	APT
report	Evile.exe[Backdoor]
report	Trac 14507

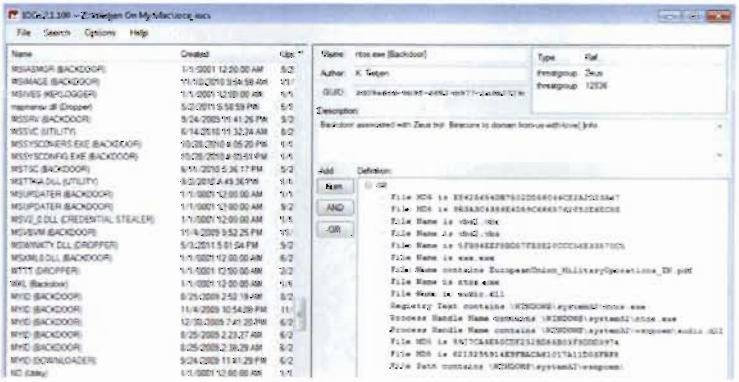


Description:

C.gif was a tool utilized for lateral movement by obtaining windows password hashes, manipulating processes, and executing commands on a remote host. The tool assists adversaries in their ability to move laterally among targets on a network "to include mtemp.tmp and Msfontsrc.d"

How to Edit and View OpenIOC

- OpenIOC editor
  - http://www.mandiant.com/products/free_software/ioce/



Name	Created	Upd
MSIASMGR (BACKDOOR)	1/1/0001 12:00:00 AM	5/2
MSIMAGE (BACKDOOR)	11/10/2010 9:54:58 AM	1/1
MSIVES (KEYLOGGER)	1/1/0001 12:00:00 AM	1/1
mspmsnsv.dll (Dropper)	5/2/2011 5:58:59 PM	5/1
MSSRV (BACKDOOR)	9/24/2009 11:41:26 PM	5/2
MSSVC (UTILITY)	6/14/2010 11:32:24 AM	6/2
MSSYSCONERS.EXE (BACKDOOR)	10/28/2010 4:05:20 PM	1/1
MSSYSCONFIG.EXE (BACKDOOR)	10/28/2010 4:03:51 PM	1/1
MSTSC (BACKDOOR)	6/11/2010 5:36:17 PM	5/2
MSTTHA.DLL (UTILITY)	9/3/2010 4:49:36 PM	1/1
MSUPDATER (BACKDOOR)	1/1/0001 12:00:00 AM	1/1
MSUPDATER (BACKDOOR)	1/1/0001 12:00:00 AM	5/2
MSV2_0.DLL (CREDENTIAL STEALER)	1/1/0001 12:00:00 AM	1/1
MSVBVM (BACKDOOR)	11/4/2009 9:52:25 PM	11/
MSWINKTY.DLL (DROPPER)	5/3/2011 5:01:04 PM	5/2
MSXML3.DLL (BACKDOOR)	1/1/0001 12:00:00 AM	6/2
MTTT (DROPPER)	1/1/0001 12:00:00 AM	2/2
MXL (Backdoor)	1/1/0001 12:00:00 AM	1/1
MYID (BACKDOOR)	8/25/2009 2:52:19 AM	8/2
MYID (BACKDOOR)	11/4/2009 10:54:09 PM	11/
MYID (BACKDOOR)	12/30/2009 7:41:20 PM	6/2
MYID (BACKDOOR)	8/25/2009 2:23:27 AM	6/2
MYID (BACKDOOR)	8/25/2009 2:39:29 AM	6/2
MYID (DOWNLOADER)	9/24/2009 11:41:29 PM	6/2
NC (Utility)	1/1/0001 12:00:00 AM	1/1

Name: ntos.exe [Backdoor]

Author: K. Tietjen

GUID: [illegible]

Type	Ref
threatgroup	Zeus
threatgroup	12036

Description:

Backdoor associated with Zeus bot. Beacons to domain from-us-with-love[.]info

Definition:

```
OR
    File MD5 is [illegible]
    File MD5 is [illegible]
    File Name is [illegible]
    File Name is [illegible]
    File Name is [illegible]
    File Name is exe.exe
    File Name contains EuropeanUnion_MilitaryOperations_EN.pdf
    File Name is ntos.exe
    File Name is audio.dll
    Registry Text contains \WINDOWS\system32\ntos.exe
    Process Handle Name contains \WINDOWS\system32\ntos.exe
    Process Handle Name contains \WINDOWS\system32\wsnpoem\audio.dll
    File MD5 is [illegible]
    File MD5 is [illegible]
    File Path contains \WINDOWS\system32\wsnpoem
```

More OpenIOC Resources

- IOC You and Raise You
  - http://www.mandiant.com/presentations/fresh_prints_of_mal-ware_ioc_you_and_raise_you/
- ABCs of IOC
  - http://www.mandiant.com/presentations/state_of_the_hack_abcs_of_ioc/
- 0x1,0x2,03s of IOC
  - http://www.mandiant.com/presentations/fresh_prints_of_mal-ware_0x10x20x3s_of_ioc/

Why Saving Lives?

SPRING INCIDENTS

Detection

- Detected by four avenues
  - User reported
    - Los Alamos does have the highest per capita PhD in the nation*
  - Host IDS
    - Detected registry key associated with previous attack and backdoor
  - Crash Dump Collection
    - Noticed evil JavaScript and attempt of exploit on Windows 7 machines IE that caused crashes
  - Snort Alerts
    - Previous network based indicators fired off when backdoors became active

Where was I?

- I was at home.
- Not getting any sleep.
- Daughter just born 5 days before.
- IOCs saving lives number one - mine

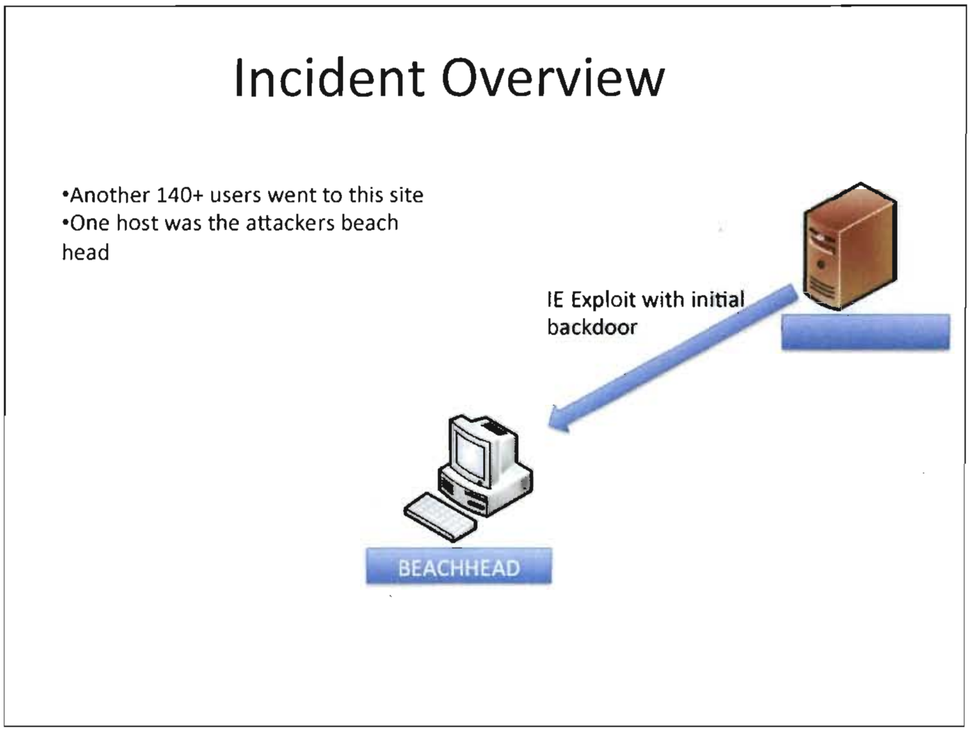
Opportunity

- Government shutdown was likely to happen the day we received the phish
- But I like to think it was because I was on leave

Who Where the Attackers

Characterization

- Over 1000+ people received the phish email
- How many infected machines
- Developed snort rules and flow alerts to detect further activity

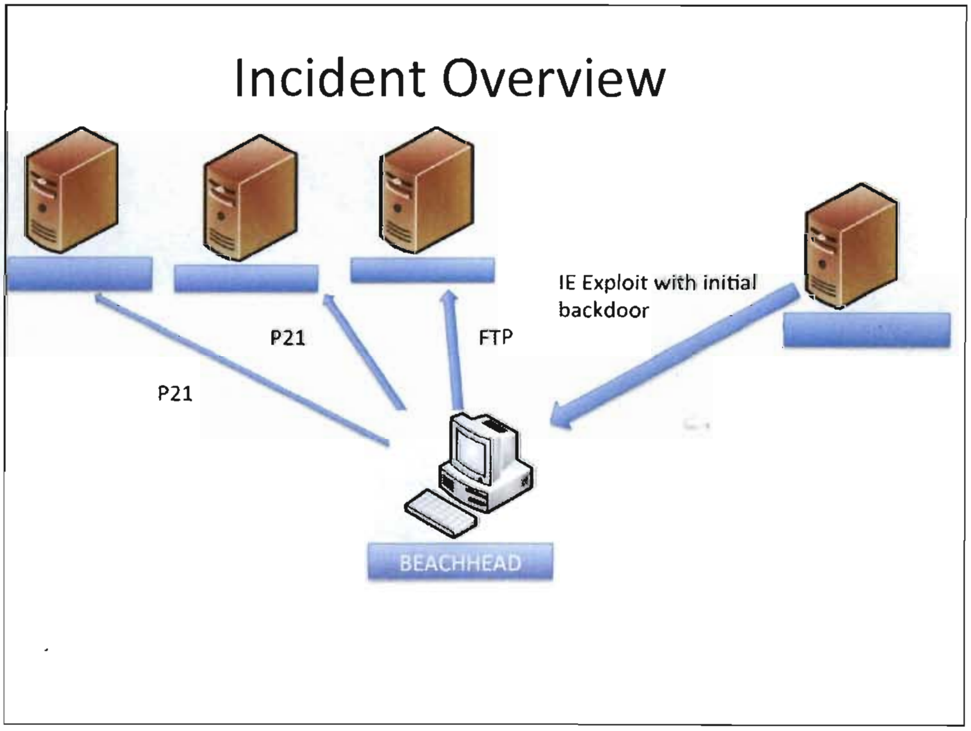


Incident Overview

- •Another 140+ users went to this site
- •One host was the attackers beach head

IE Exploit with initial backdoor

BEACHHEAD



Incident Overview

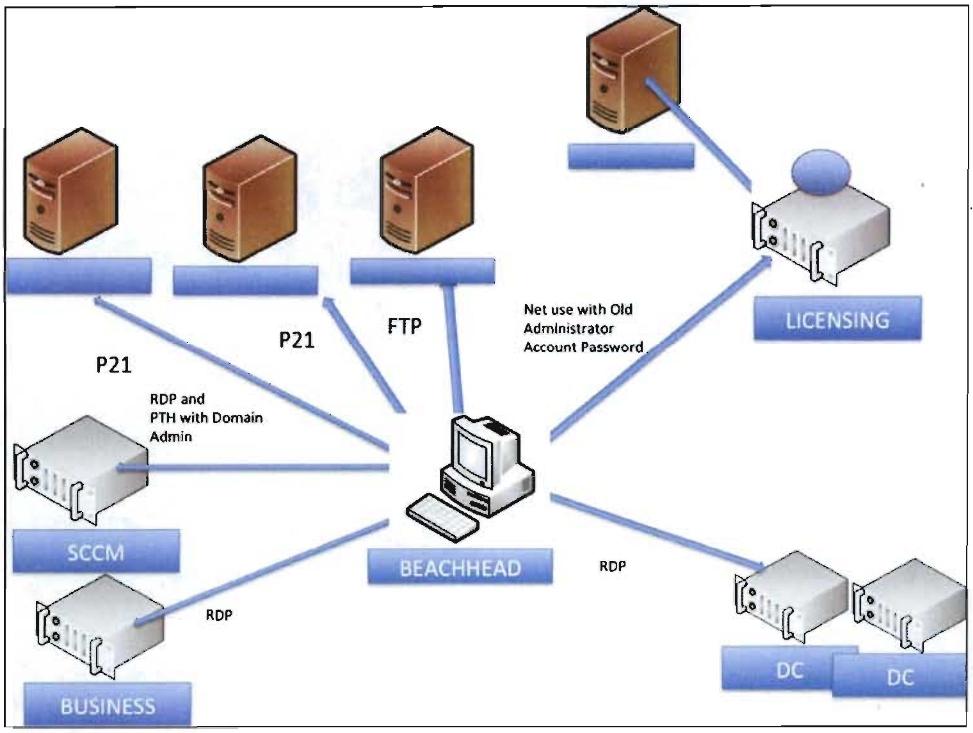
IE Exploit with initial backdoor

P21

FTP

P21

BEACHHEAD


LICENSING
Net use with Old Administrator Account Password
FTP
P21
P21
RDP and PTH with Domain Admin
SCCM
BEACHHEAD
RDP
RDP
BUSINESS
DC
DC

Response

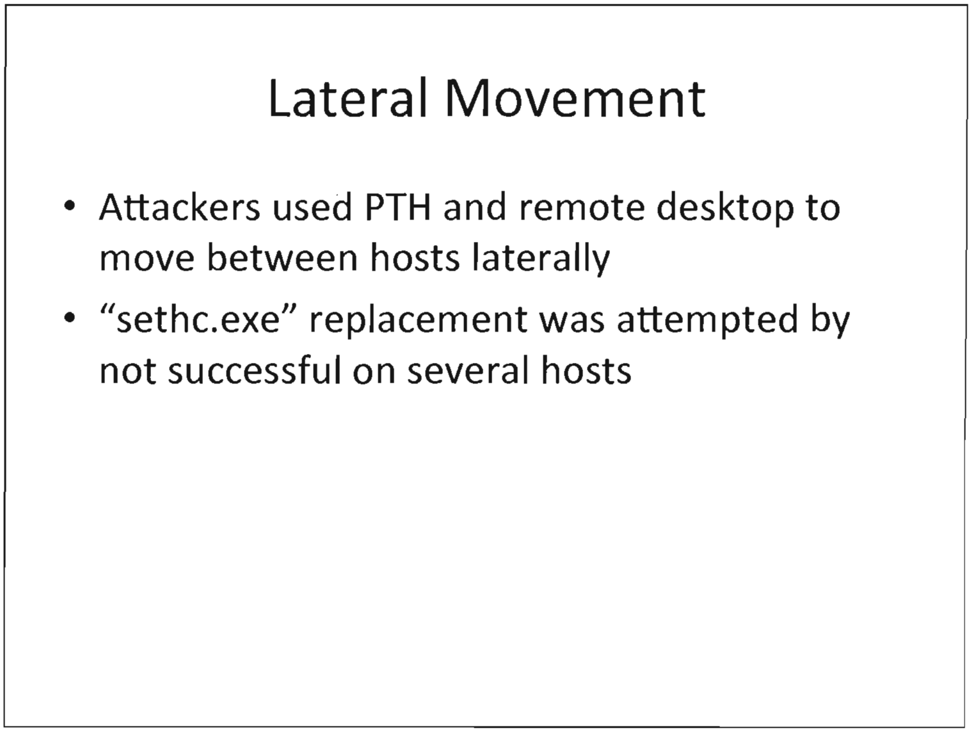
- Within an hour LANL IR team members were already responding to the incident
- Within 12 hours the incident had been characterized and actively being monitored
- Moved from characterization to Intelligence analysis

Intelligence Analysis

- All hosts were actively monitored with EnCase Enterprise (Our MIR Sniper) to watch active hosts

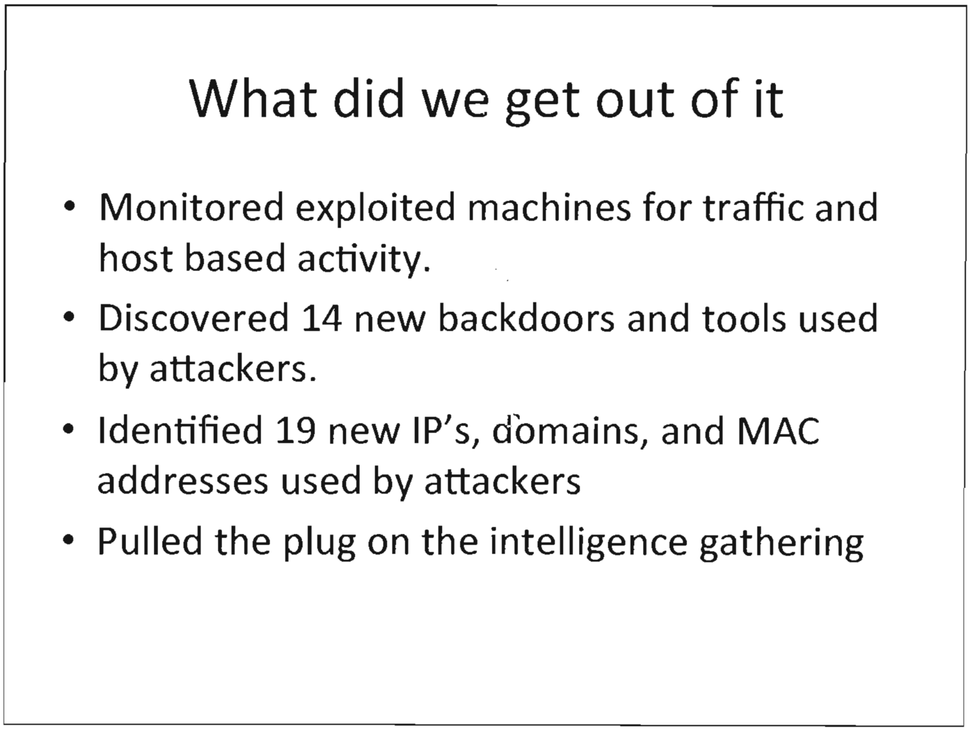
Attacker Playground

- Once characterized we decided to monitor the attackers to gain intelligence
- Made this decision because we wanted to make sure we had found everything (strike zone pic)
- Haven't seen the attackers in a couple of years so we wanted to see their new tool set



Lateral Movement

- Attackers used PTH and remote desktop to move between hosts laterally
- “sethc.exe” replacement was attempted by not successful on several hosts



What did we get out of it

- Monitored exploited machines for traffic and host based activity.
- Discovered 14 new backdoors and tools used by attackers.
- Identified 19 new IP’s, domains, and MAC addresses used by attackers
- Pulled the plug on the intelligence gathering

Remediation

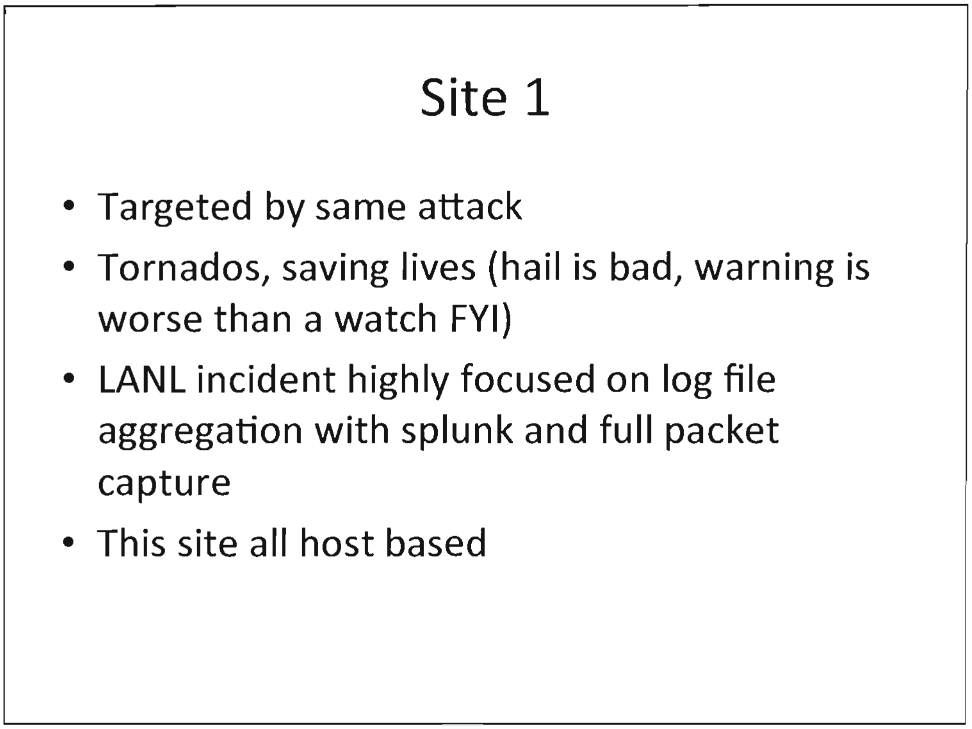
- Blocked all domains.
- Blocked all IP's.
- Blocked all hosts that clicked on "ansme.com" link.
  - CSIRT did not have time to repudiate
- Monitor for additional traffic with Snort Rules
- Monitoring for host based activity with SEP
- MIR scanning with IOCs from incident
- Initial blocking took 5 minutes (Rebuilding longer)

MIR scan Results

- One host from previous infection in 2009 showing "sethc.exe" changed to "cmd.exe"
  - Attackers tried to get to this machine in the network traffic but were unsuccessful

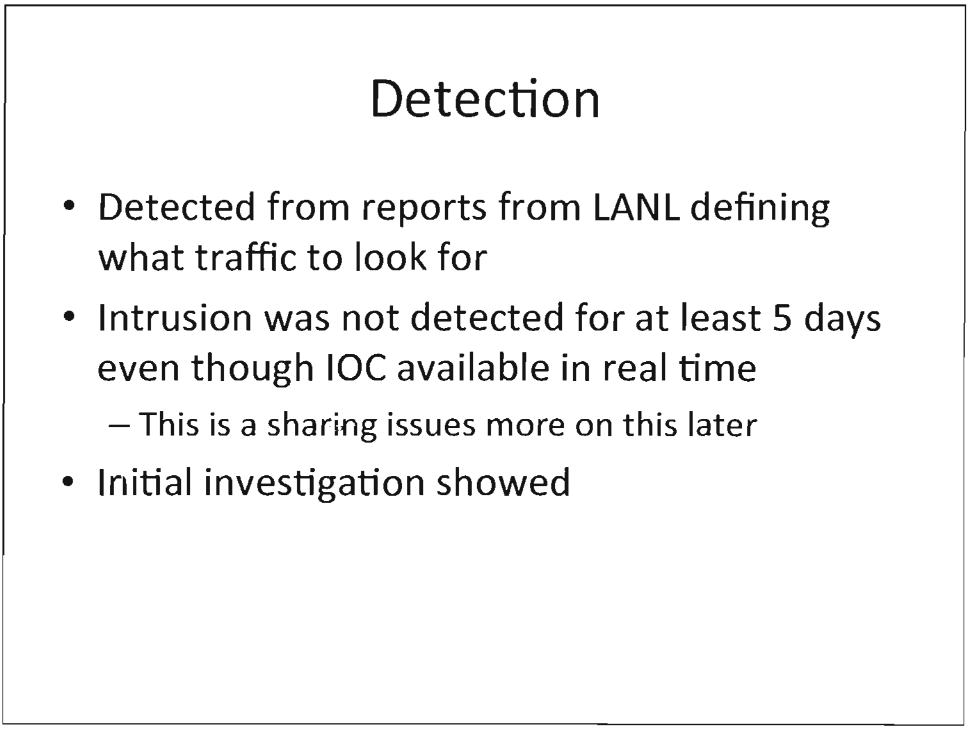
SPRING INCIDENT PART 2

Saving Lives



Site 1

- Targeted by same attack
- Tornados, saving lives (hail is bad, warning is worse than a watch FYI)
- LANL incident highly focused on log file aggregation with splunk and full packet capture
- This site all host based



Detection

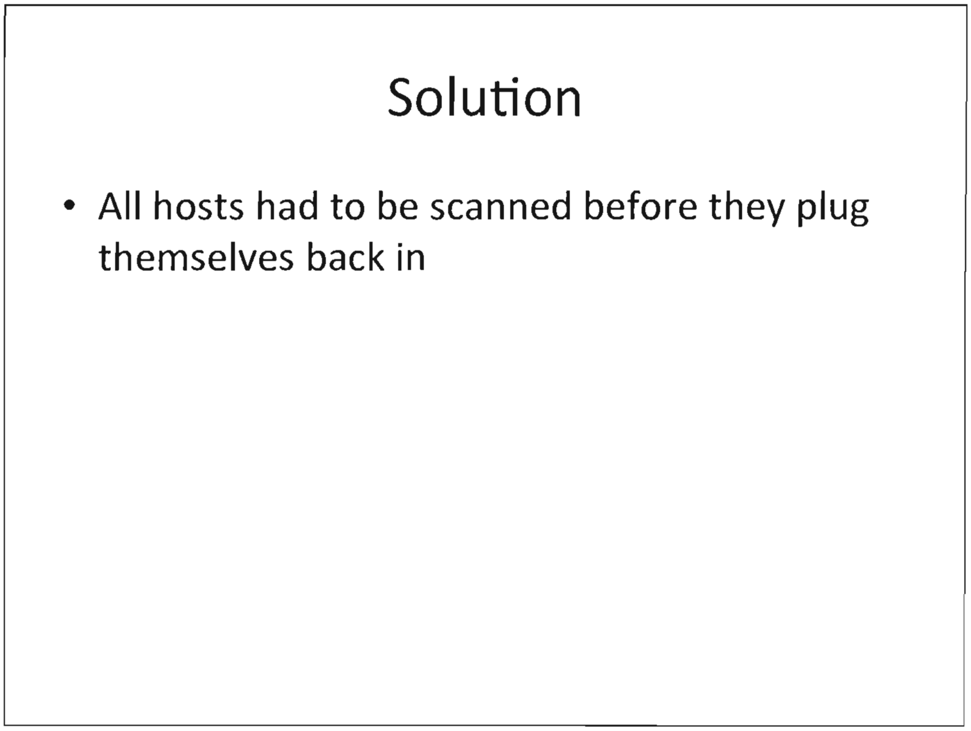
- Detected from reports from LANL defining what traffic to look for
- Intrusion was not detected for at least 5 days even though IOC available in real time
  - This is a sharing issues more on this later
- Initial investigation showed

Response

- Turn off the Internet
- Call everyone to help
  - Microsoft CERT
  - DHS
  - NSA
  - LANL
  - Several More

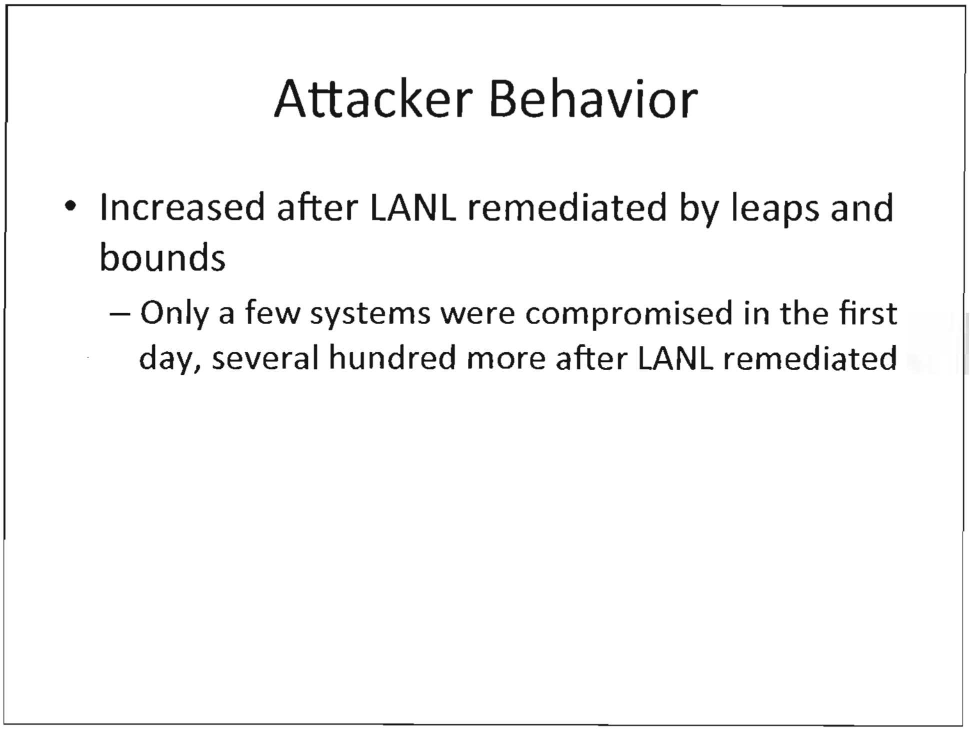
Problems

- No Host based detection capability
- Turned off the Internet
- Full packet capture of network traffic
  - Had this capability but they dropped all the traffic on the port the attackers were using
- Started remediating before they fully characterized the incident



Solution

- All hosts had to be scanned before they plug themselves back in



Attacker Behavior

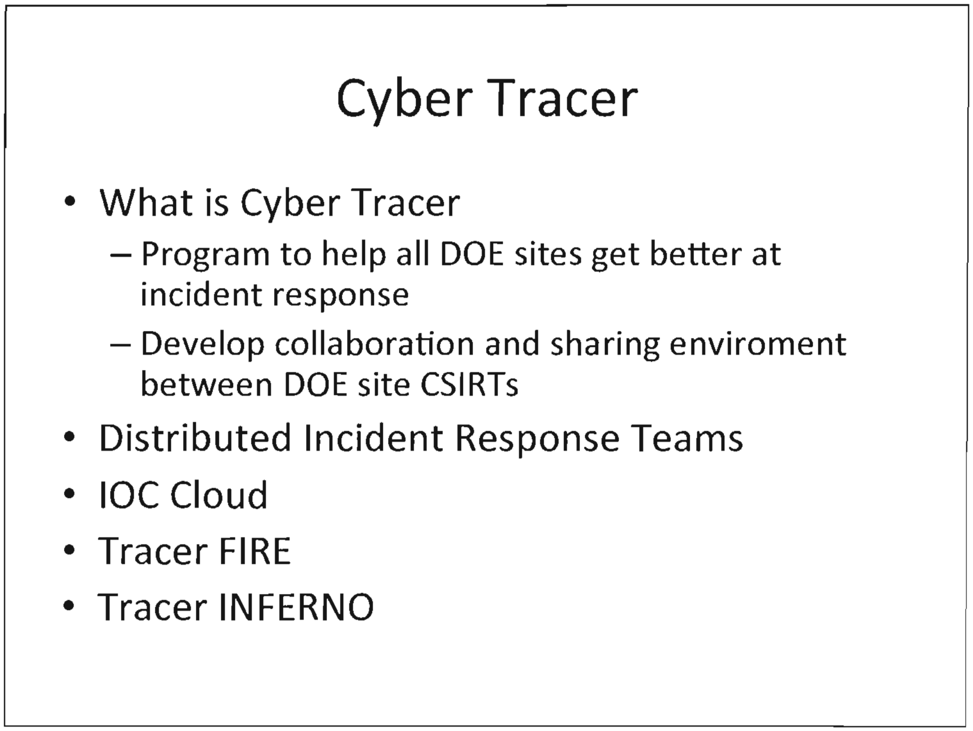
- Increased after LANL remediated by leaps and bounds
  - Only a few systems were compromised in the first day, several hundred more after LANL remediated

Results

- MIR scanned 8,000 systems
- Found 123 compromised hosts
  - Either attacker had access to this host or malware was found on it
- All compromised hosts the same IOCs created during the first incident
  - Attackers did not use the initial backdoor or configuration found originally at LANL

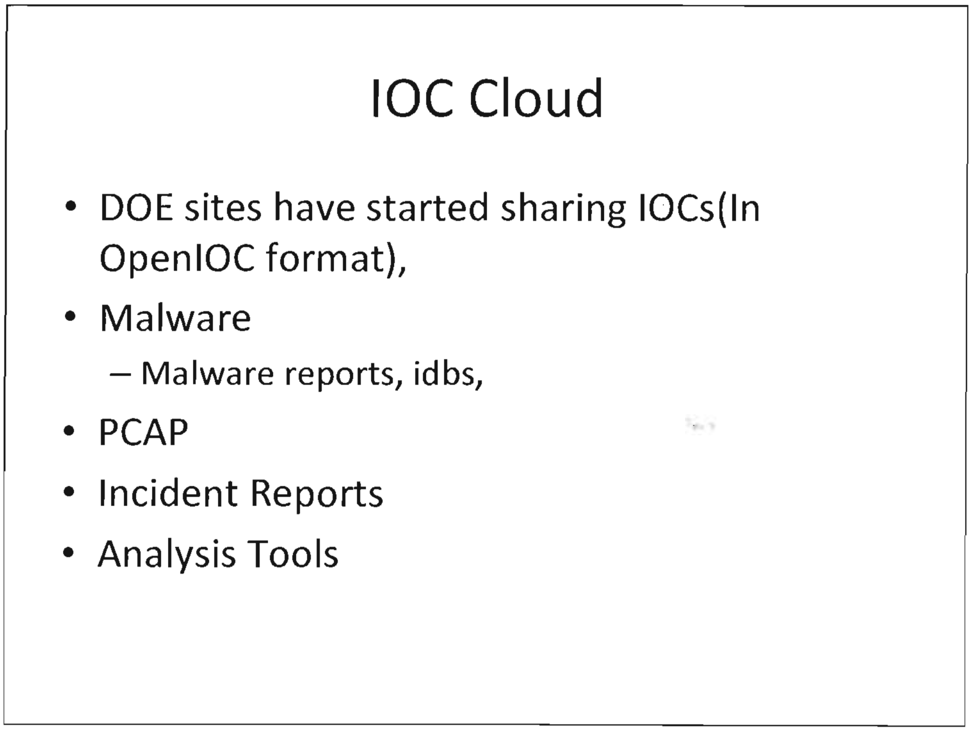
Findings

- Need to share better with other sites
  - Not just documents with indicators but IOCs you can execute on in real time



Cyber Tracer

- What is Cyber Tracer
  - Program to help all DOE sites get better at incident response
  - Develop collaboration and sharing enviroment between DOE site CSIRTs
- Distributed Incident Response Teams
- IOC Cloud
- Tracer FIRE
- Tracer INFERNO

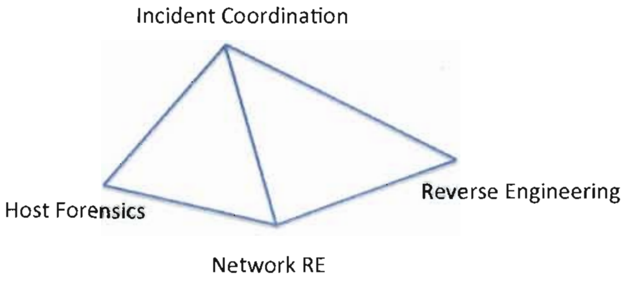


IOC Cloud

- DOE sites have started sharing IOCs(In OpenIOC format),
- Malware
  - Malware reports, idbs,
- PCAP
- Incident Reports
- Analysis Tools

Training within DOE

- Tracer FIRE
- Tracer Inferno


Incident Coordination

Host Forensics

Reverse Engineering

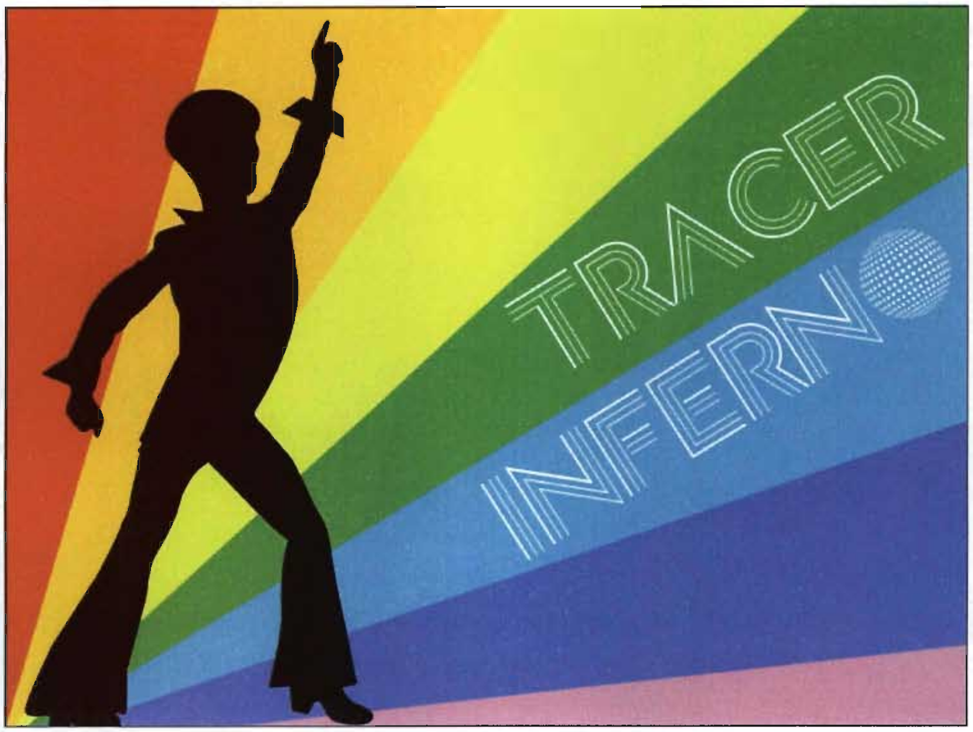
Network RE

TRACER FIRE 4

FEBRUARY 6-10, 2012

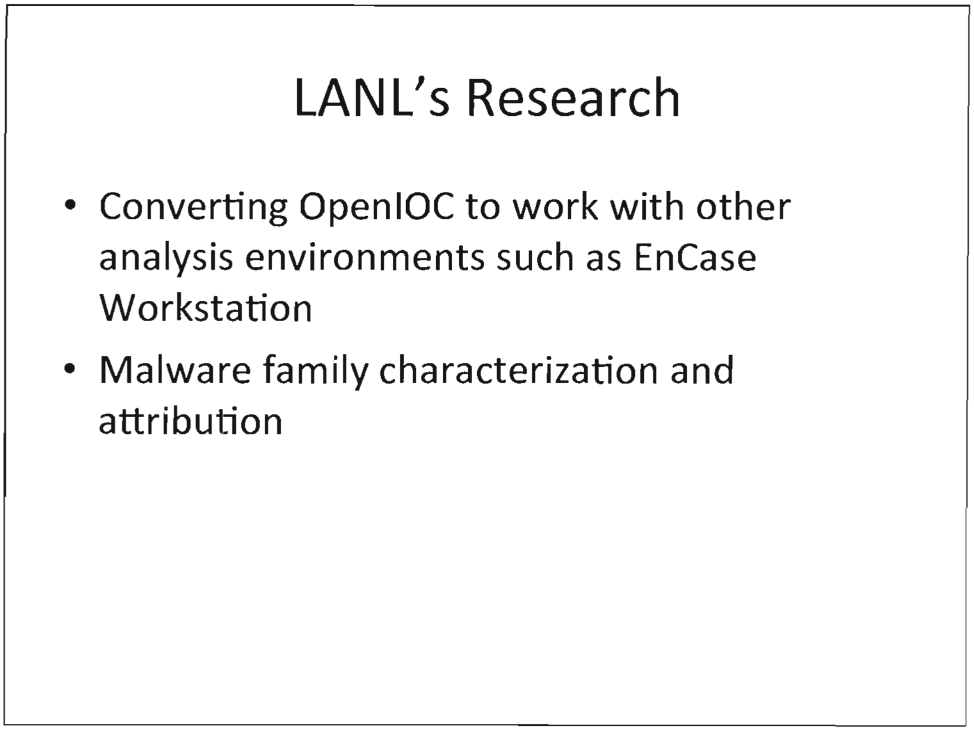
SANTA FE, NM

For details, visit
http://csr.lanl.gov/tf/



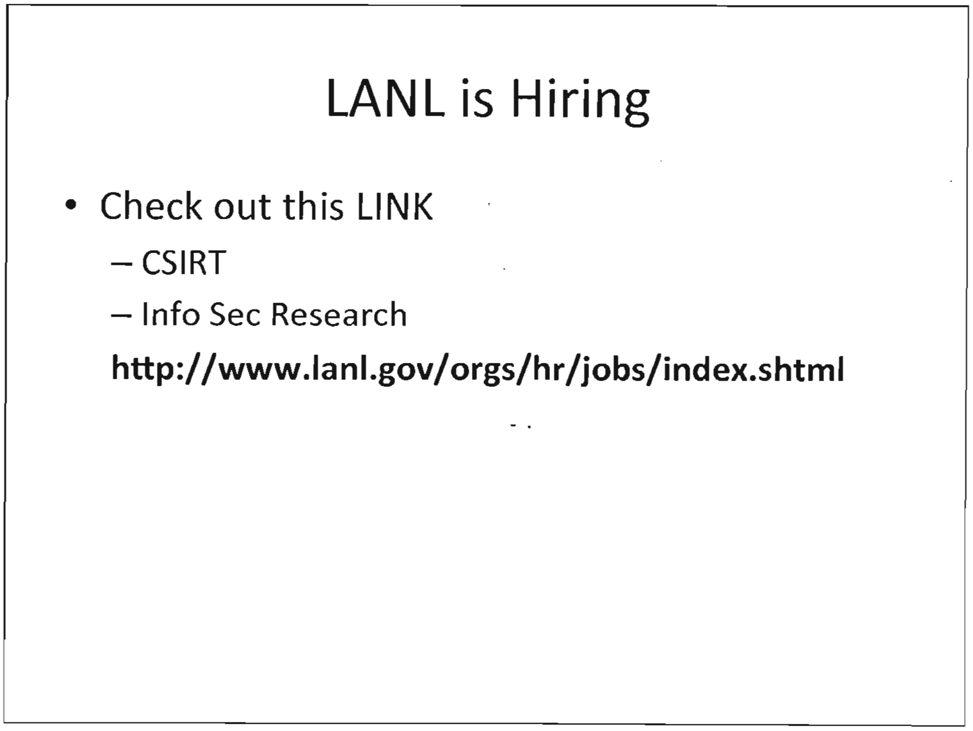
Distributed Incident Response Team-DIRT

- Experts in DOE dispersed through out labs and smaller sites with out these experts can relay on them to help respond
- Areas of Expertise
  - Digital Forensics
  - Incident coordination
  - Protocol Analysis
  - Reverse Engineering



LANL's Research

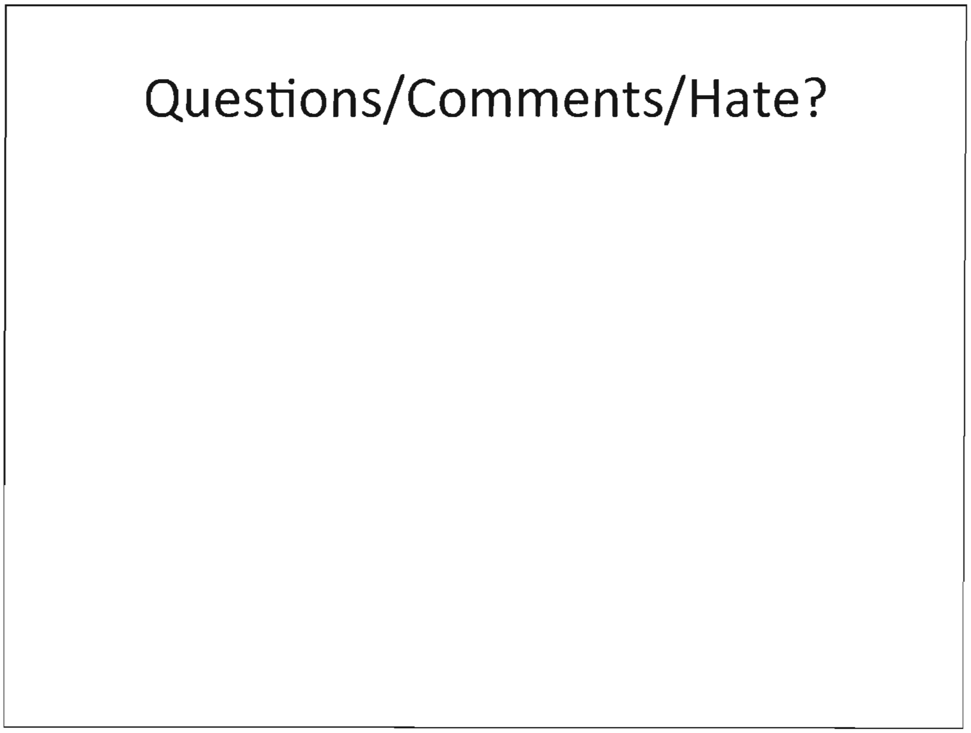
- Converting OpenIOC to work with other analysis environments such as EnCase Workstation
- Malware family characterization and attribution



LANL is Hiring

- Check out this LINK
  - CSIRT
  - Info Sec Research

  http://www.lanl.gov/orgs/hr/jobs/index.shtml



Questions/Comments/Hate?