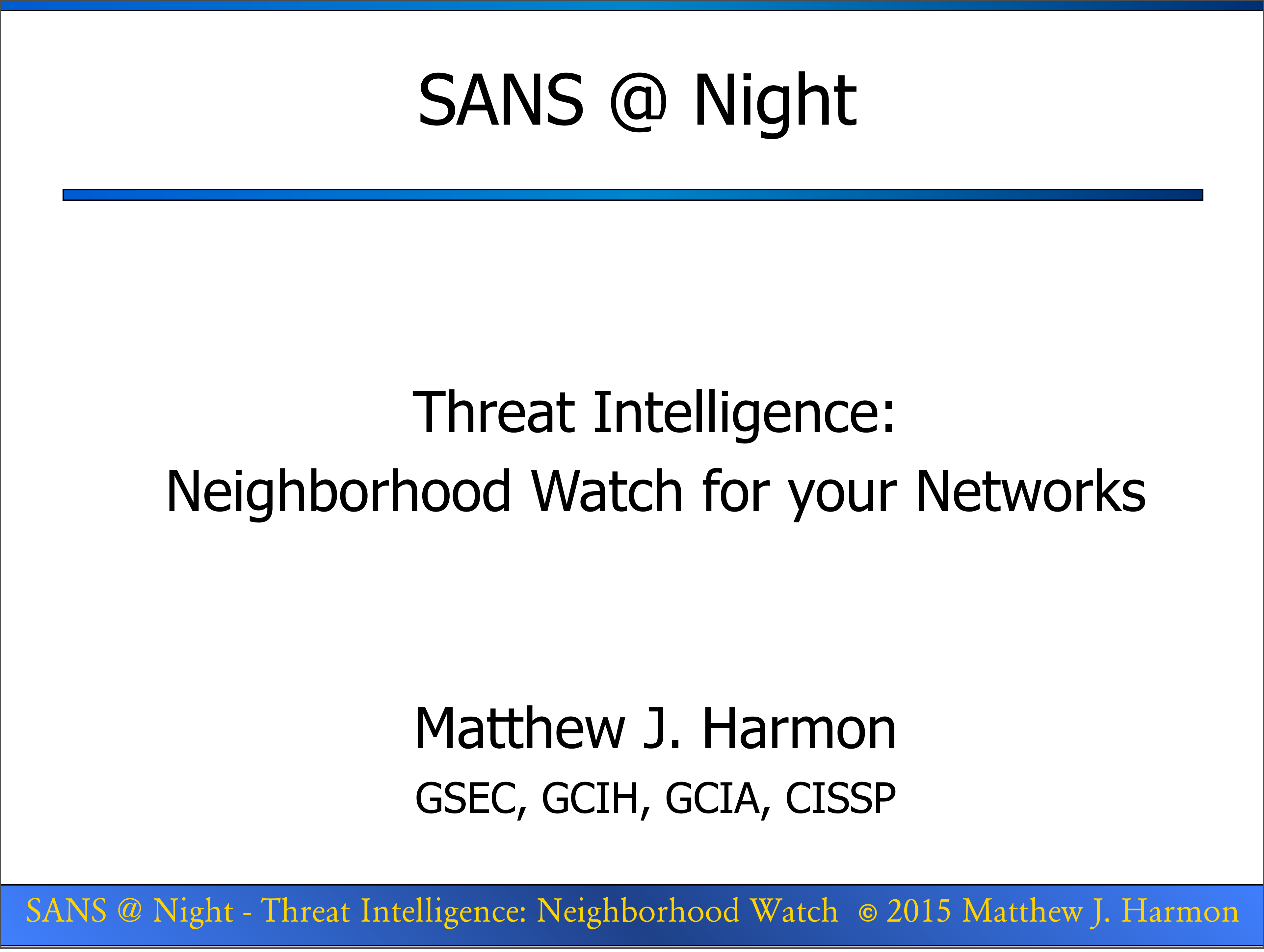


SANS @ Night

Threat Intelligence: Neighborhood Watch for your Networks

Matthew J. Harmon

GSEC, GCIH, GCIA, CISSP

Thursday, July 23, 15

Hello everyone! Welcome to SANS @ Night, Threat Intelligence: Neighborhood Watch for your Networks

Matthew J. Harmon

- SANS Community & Mentor Instructor
  - Security 401 (Security Essentials), 504 (Hacker Tools, Techniques, Exploits & Incident Handling), 464 (Hacker Guard, IT Operations Baselining), since 2009.
- NorSec ISAO, CTO & Executive Chairman
  - Information Sharing Analysis Organization
- IT Risk Limited, Principal Consultant
  - DFIR, Pen Testing, Risk Management

I'm told I should have a bio slide! So here's some stuff I do that's relevant to tonight's session.

What are we going to cover tonight?

- State of Cyber Security
  - Short overview of where we are today
- Discuss “What is Threat Intelligence?”
  - Explain CybOX, STIX & TAXII
  - Real world example structuring CybOX & STIX
- Show two examples of Threat Intelligence
  - Threat Connect and Critical Stack
- Show you how to Do It Yourself
  - Homework Lab with Bro and Critical Stack

State of Cyber Security

So the State of Cyber Security

State of Cyber Security

It could be worse... BUT

Source: PBS Sesame Street, Oscar the Grouch

The state of Cyber Security today, it could be worse!

---- BUT ---

Breaches are inevitable - against a motivated attacker

Breaches are inevitable - against a motivated attacker

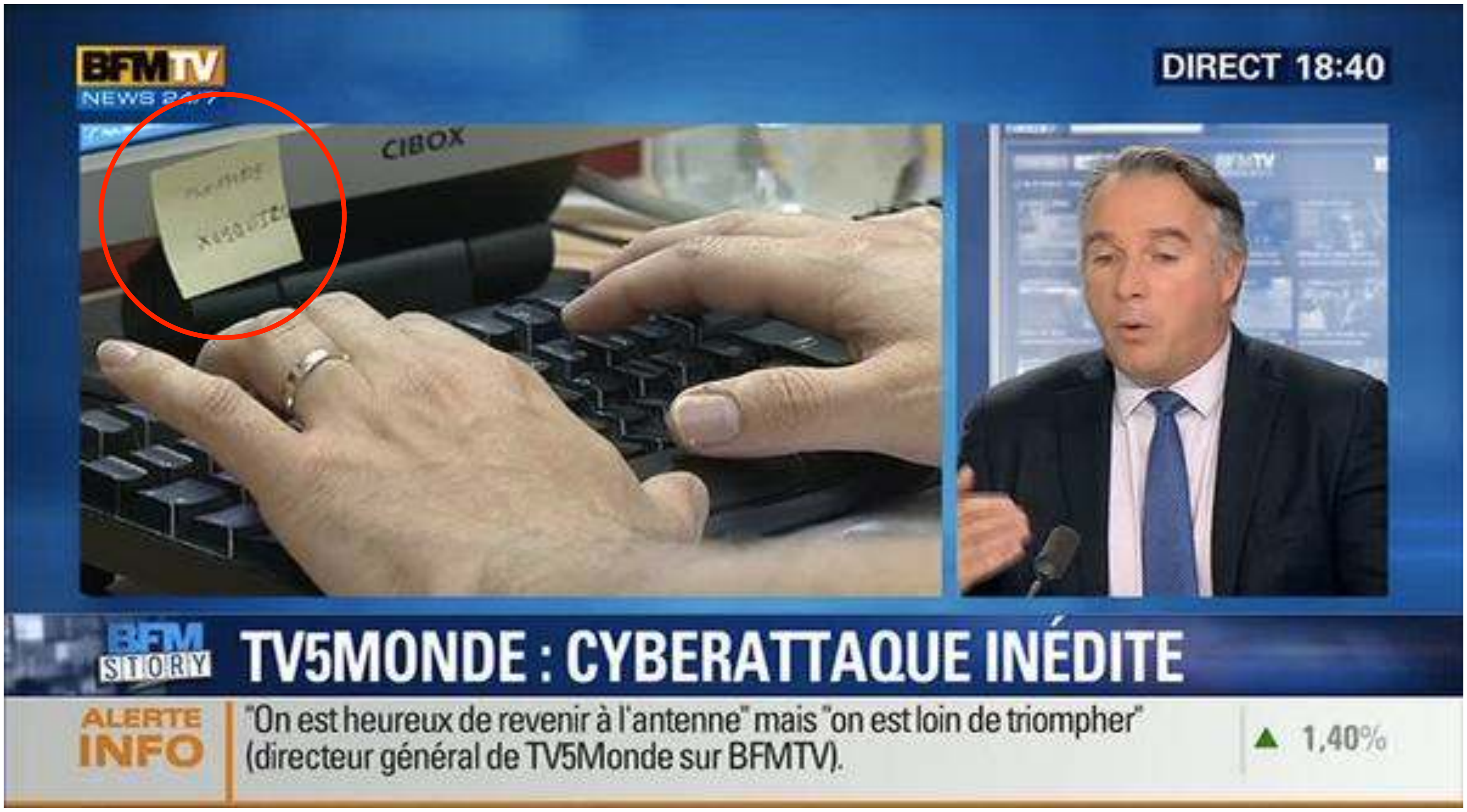
...with time and resources

Source: BBC Sherlock Holmes - "The Reichenbach Fall" Moriarty stealing the crown jewels

Breaches are inevitable against a motivated attacker with time and resources

but it doesn’t take a super genius

but it doesn't take a super genius

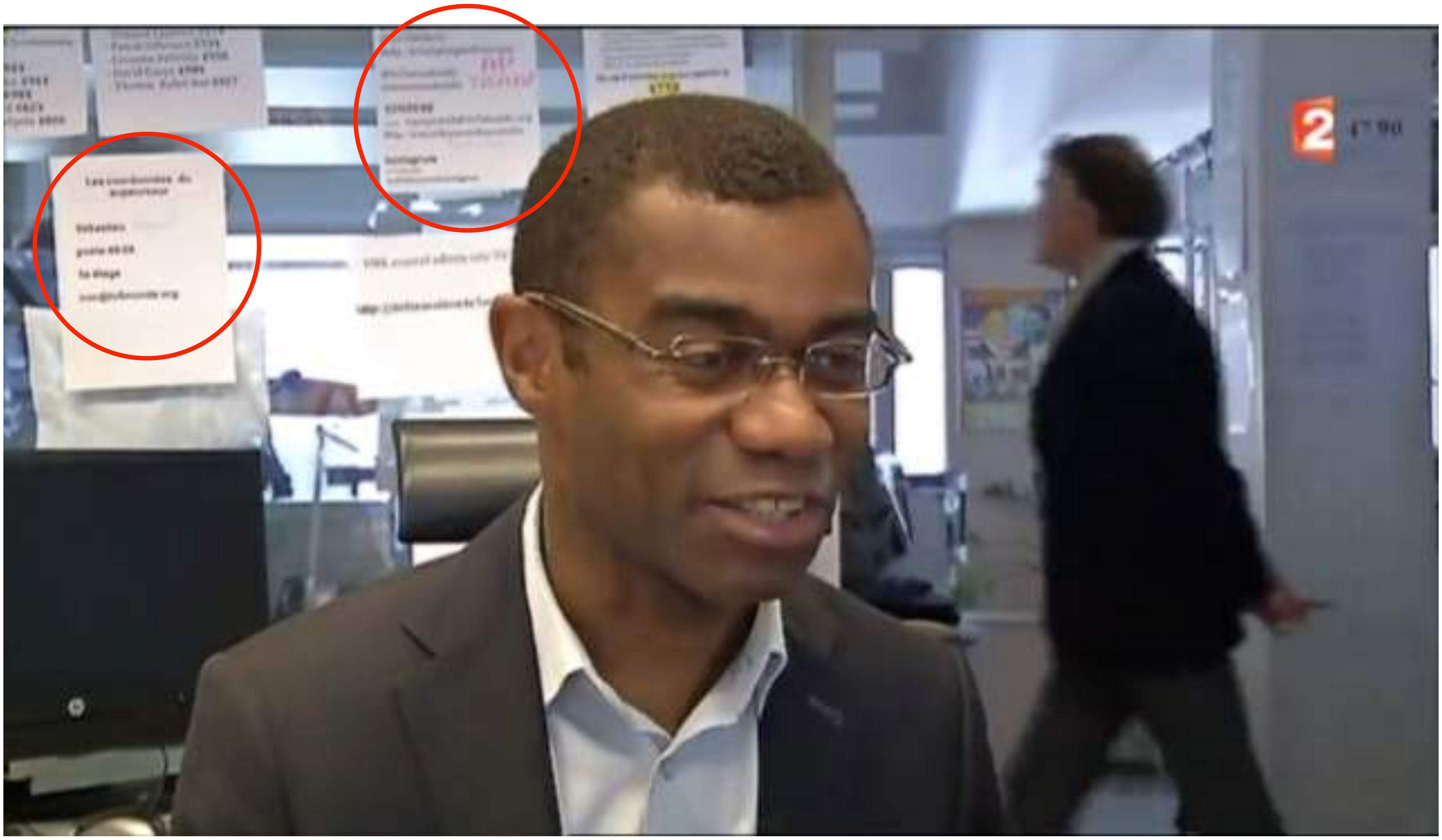


TV5MONDE : CYBERATTAQUE INÉDITE

"On est heureux de revenir à l'antenne" mais "on est loin de triompher" (directeur général de TV5Monde sur BFMTV).

It doesn't take a super genius if you show live video of someone with a post-it note containing their user and password on live TV

but it doesn’t take a super genius

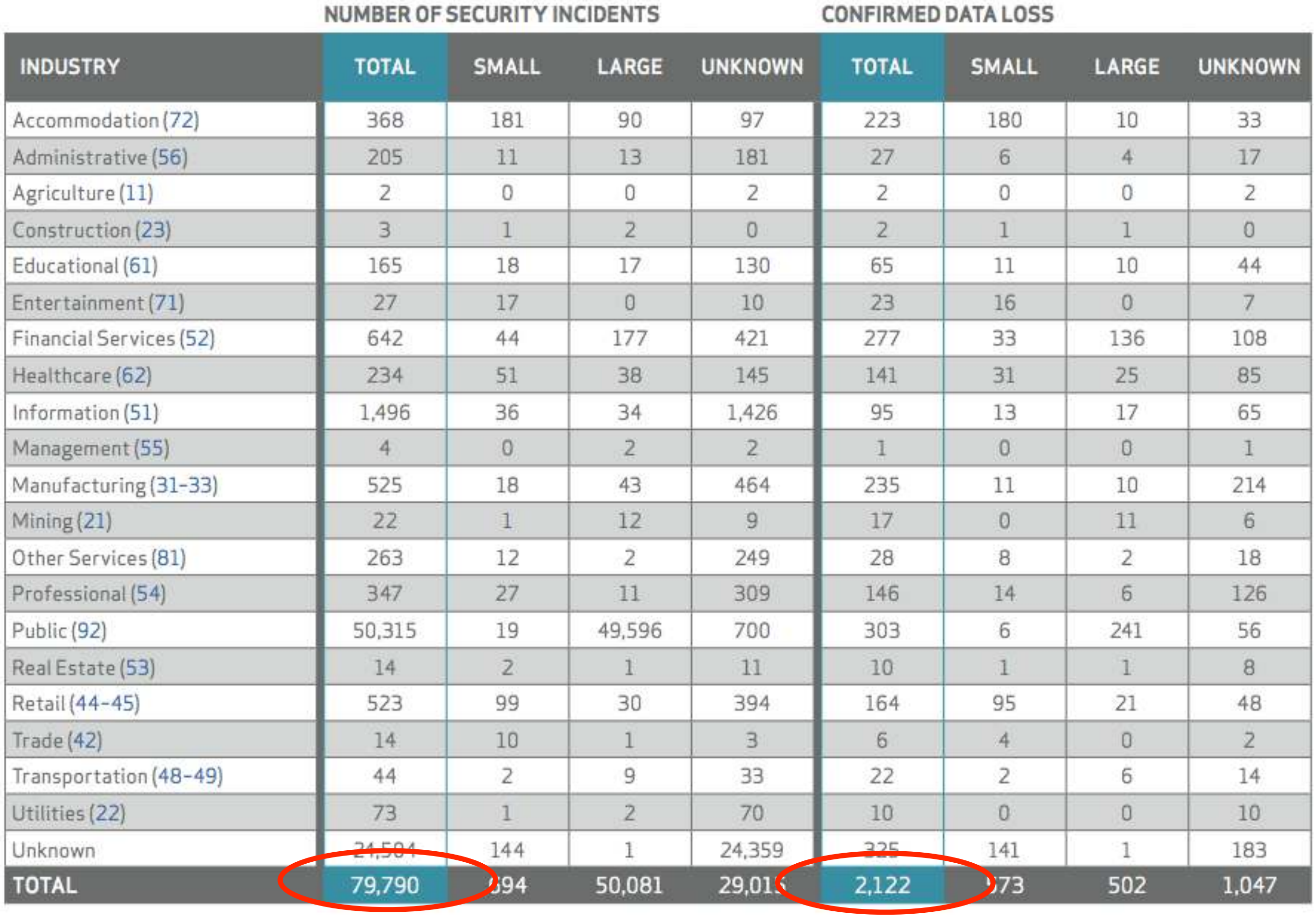


Thursday, July 23, 15

Or big sheets of paper in the background of an interview, talking about having a post-it note with user and pass on live TV

Incidents and Data Loss: 2014

Incidents and Data Loss: 2014



	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31-33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44-45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48-49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

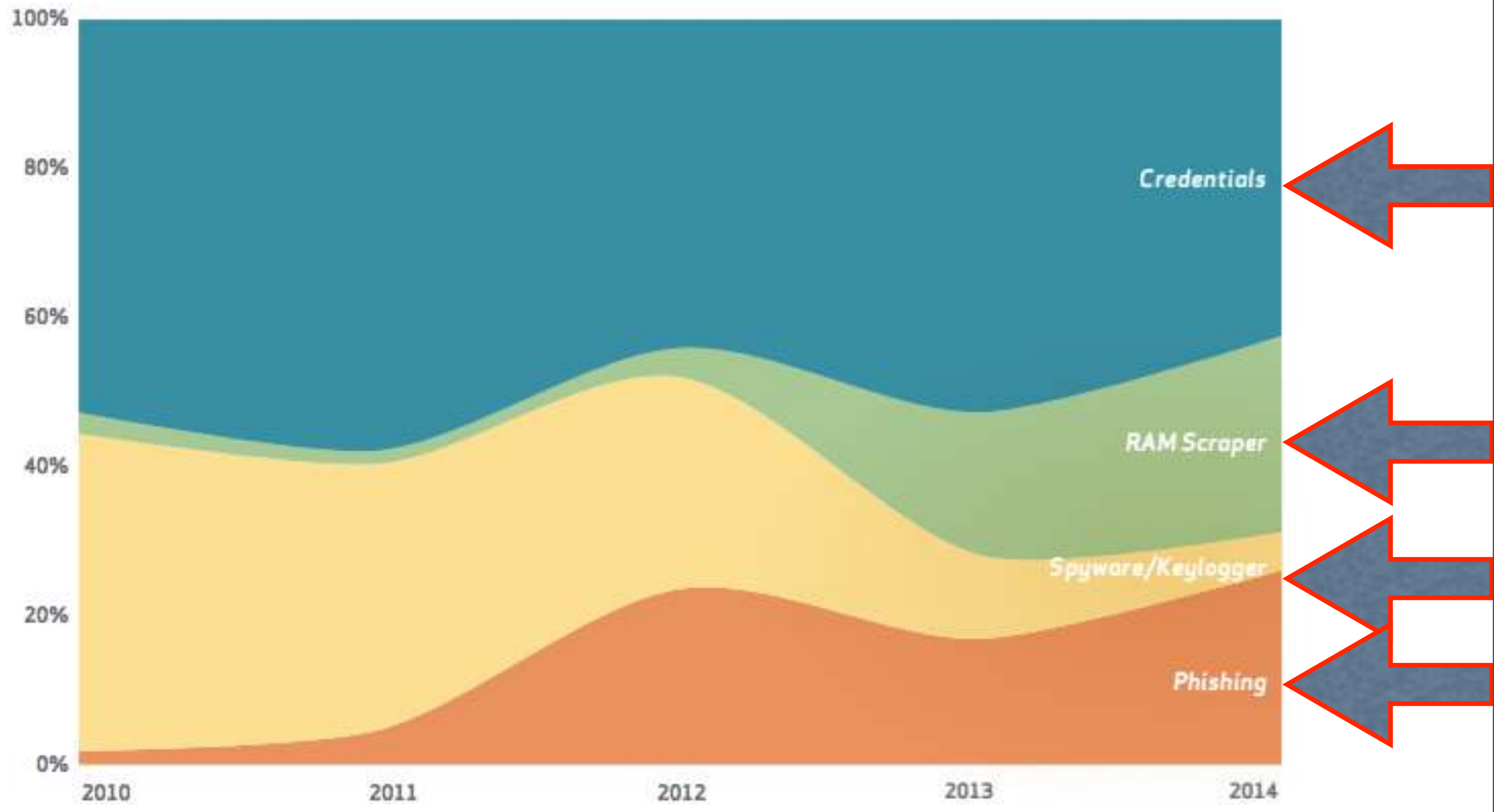
Source: Verizon 2015 Data Breach Investigations Report

Thursday, July 23, 15

In 2014 there were 79,790 reported security incidents (to Verizon or known to the general public) of those, 2,122 had confirmed data loss

Attack Vectors: 2014

Attack Vectors: 2014



Source: Verizon 2015 Data Breach Investigations Report

Compromised credentials are still leading the pack

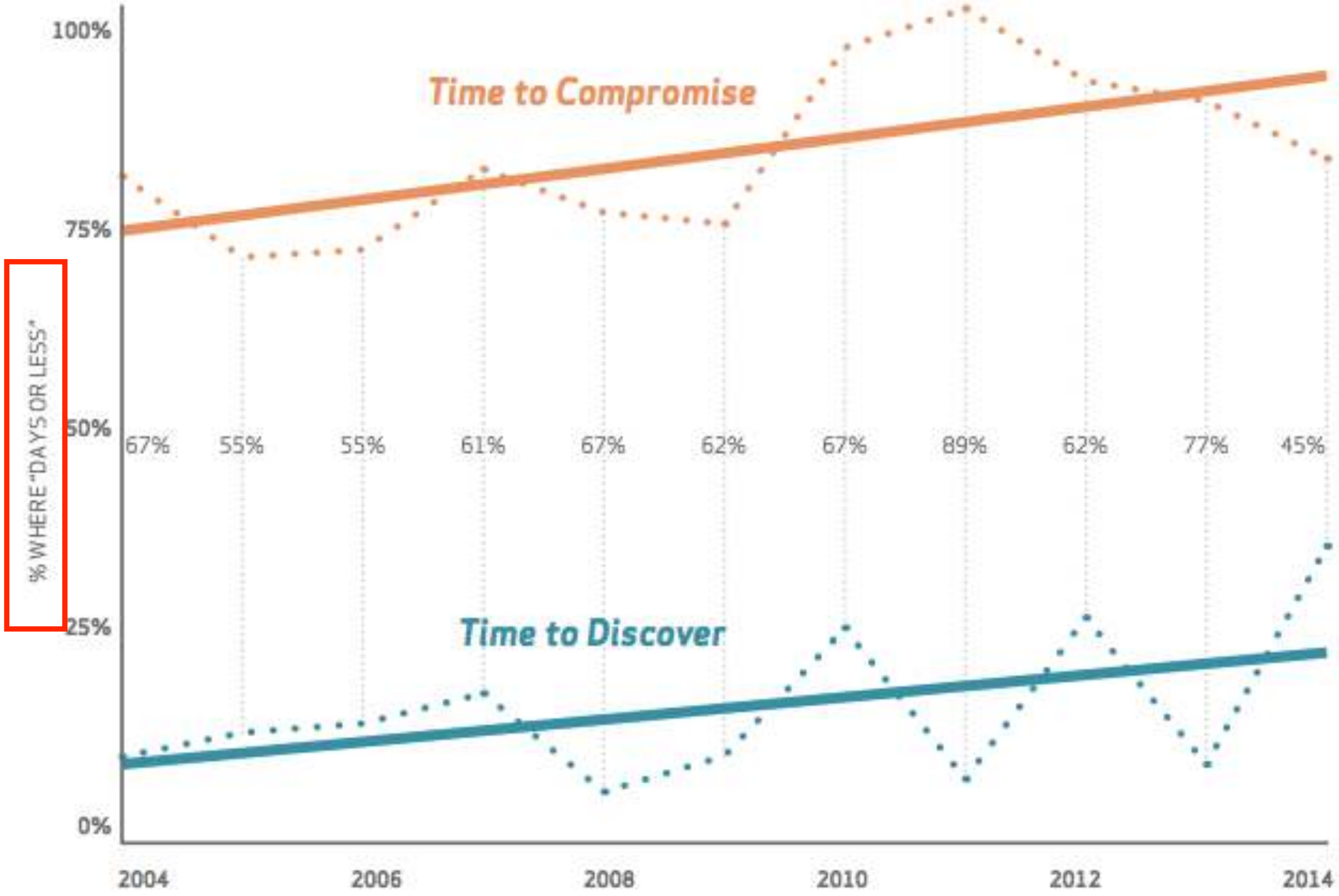
RAM scrapers are growing

Spyware and Keyloggers are going out of vogue due to easier ways to detect

Phishing is continuing to grow

Time to Discover: 2014

Time to Discover: 2014



Source: Verizon 2015 Data Breach Investigations Report

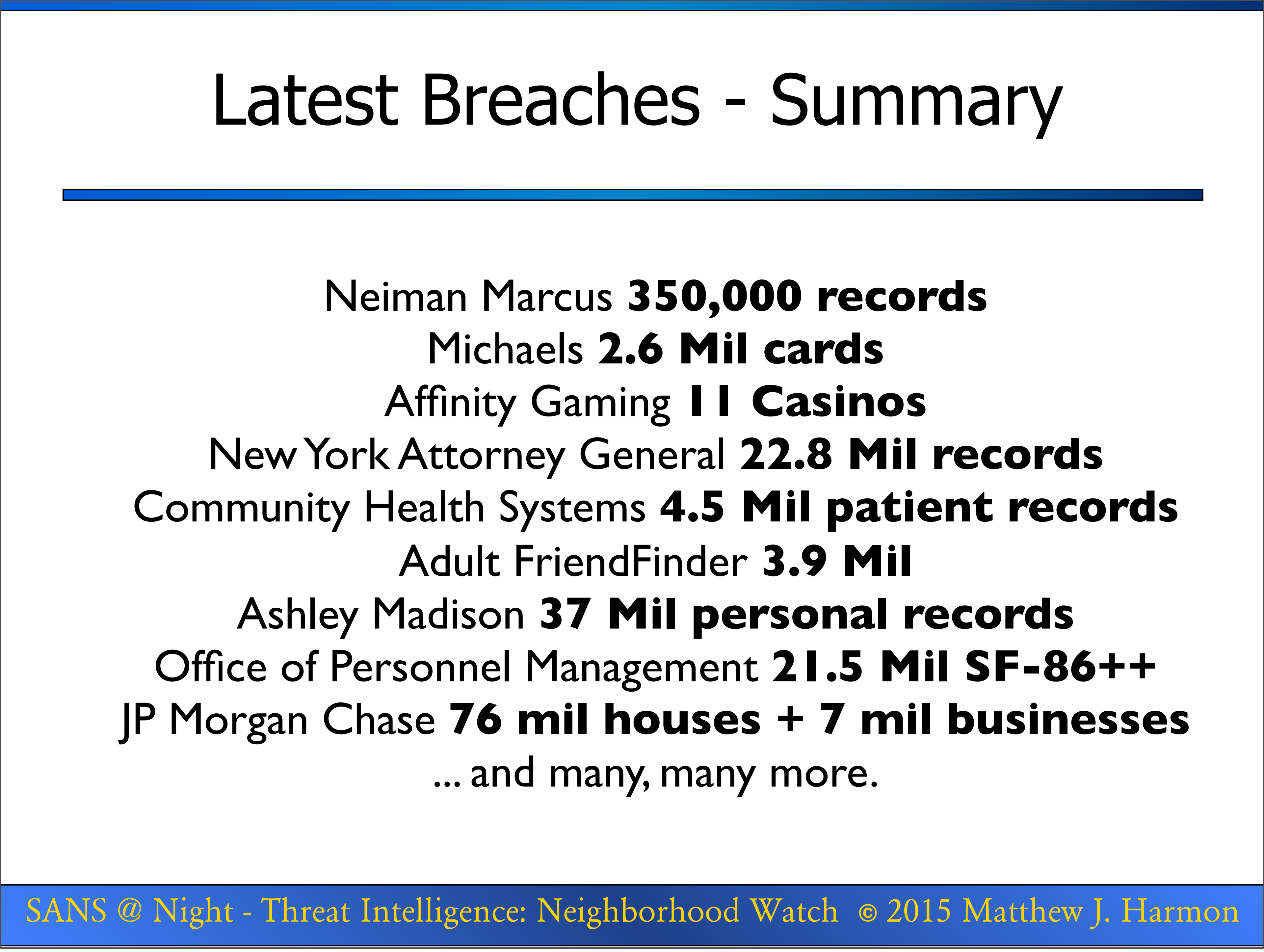
Thursday, July 23, 15

Where "DAYS OR LESS"

Time to compromise and time to discover, in less than 24 hours.

Compromise is approaching 90% in less than 24 hours

Time to discover is still less than 25% in less than 24 hours



Latest Breaches - Summary

Neiman Marcus **350,000 records**
Michaels **2.6 Mil cards**
Affinity Gaming **11 Casinos**
New York Attorney General **22.8 Mil records**
Community Health Systems **4.5 Mil patient records**
Adult FriendFinder **3.9 Mil**
Ashley Madison **37 Mil personal records**
Office of Personnel Management **21.5 Mil SF-86++**
JP Morgan Chase **76 mil houses + 7 mil businesses**
... and many, many more.

Now... what happens if we correlated the Adult FriendFinder, Ashley Madison and OPM breaches?

We really need to get better at this

As you can see... we really need to get better at this

We really need to get better at this

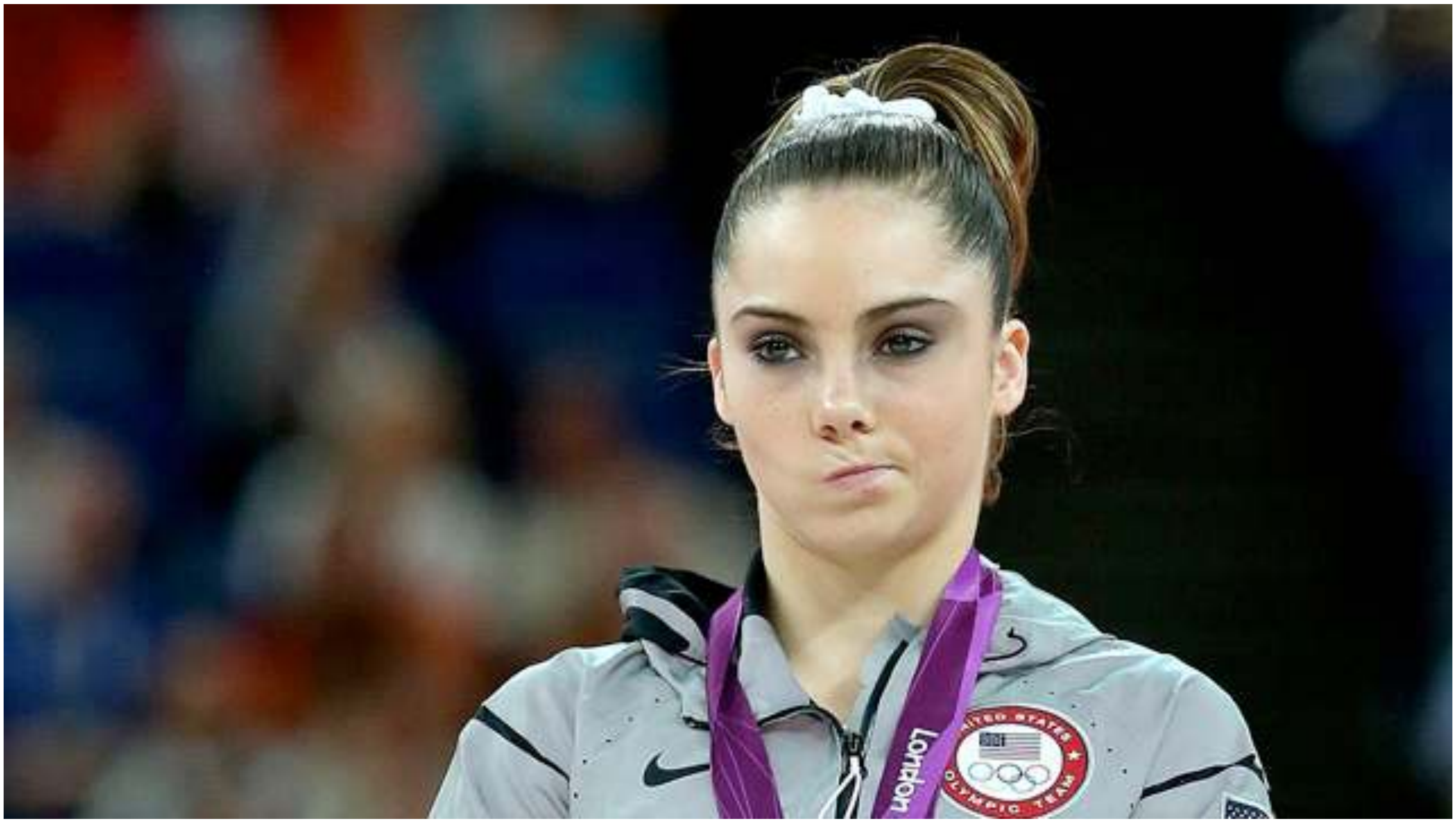


Photo: McKayla Maroney, 2012 London Olympics “McKayla Not Impressed”

Thursday, July 23, 15

The expression I expect the expression is when shareholders, a board of directors or customer finds out about a massive breach after a similar attack has just been used?

Or a 10 year old exploit?

or...

Change is good, Sharing is good

We all learned in school... or at least I hope so... that sharing is good.

Change is good, Sharing is good

CHANGE IS INVIGORATING! IF YOU DON'T ACCEPT NEW CHALLENGES, YOU BECOME COMPLACENT AND LAZY! YOUR ~~LIFE~~ Network ATROPHIES!

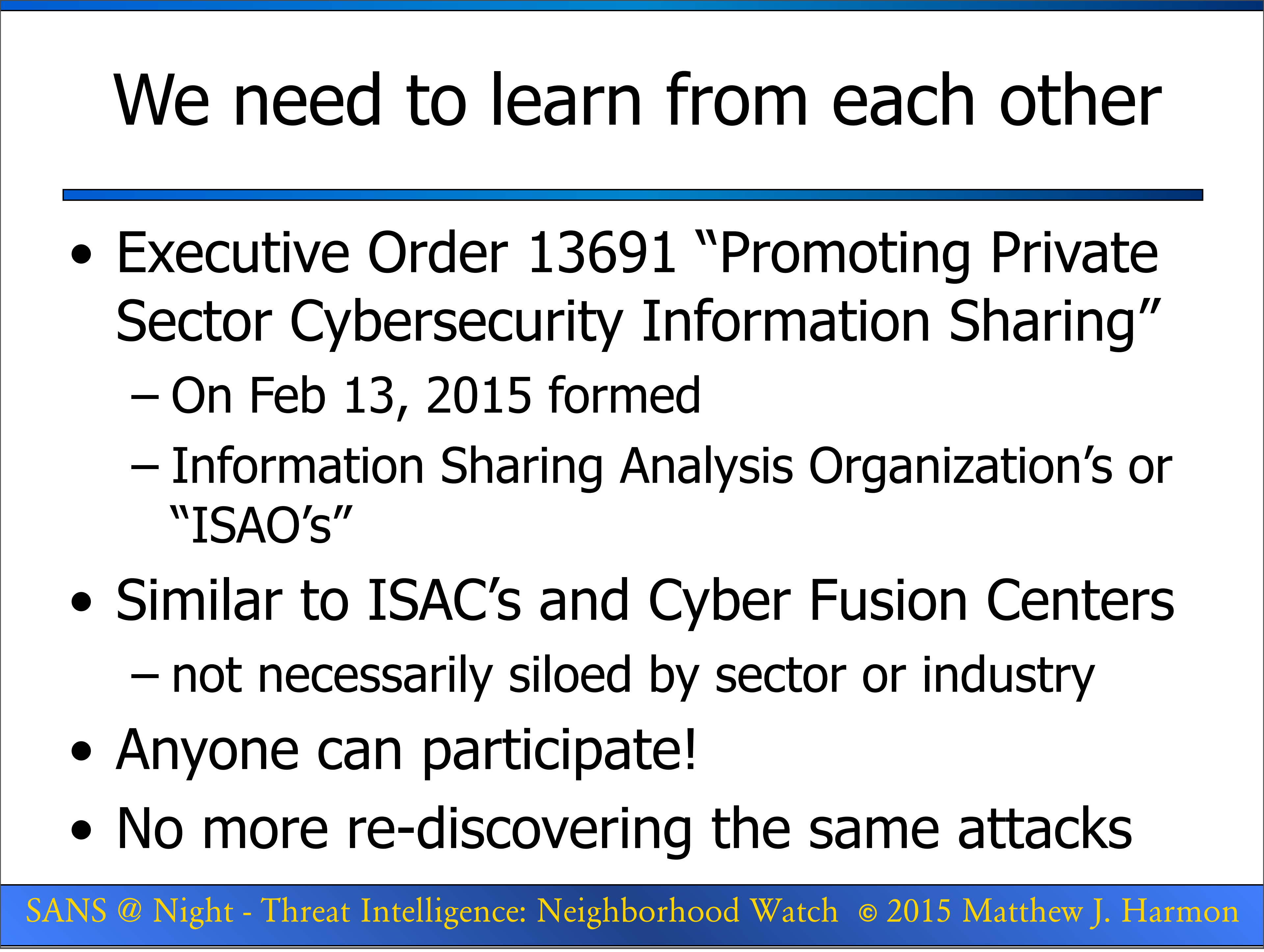
Source: Calvin and Hobbes by Bill Watterson (1995)

Thursday, July 23, 15

What I think we need to get better at is information sharing

Some people say change is scary, I agree that Change is Invigorating!
If you don't accept new challenges, you become complacent and lazy
Your network atrophies!

Anyone remember the next comic frame? No... Well they go off the side of a hill... everyone survives of course because kids and stuffed tigers are resilient



We need to learn from each other

- Executive Order 13691 “Promoting Private Sector Cybersecurity Information Sharing”
  - On Feb 13, 2015 formed
  - Information Sharing Analysis Organization’s or “ISAO’s”
- Similar to ISAC’s and Cyber Fusion Centers
  - not necessarily siloed by sector or industry
- Anyone can participate!
- No more re-discovering the same attacks

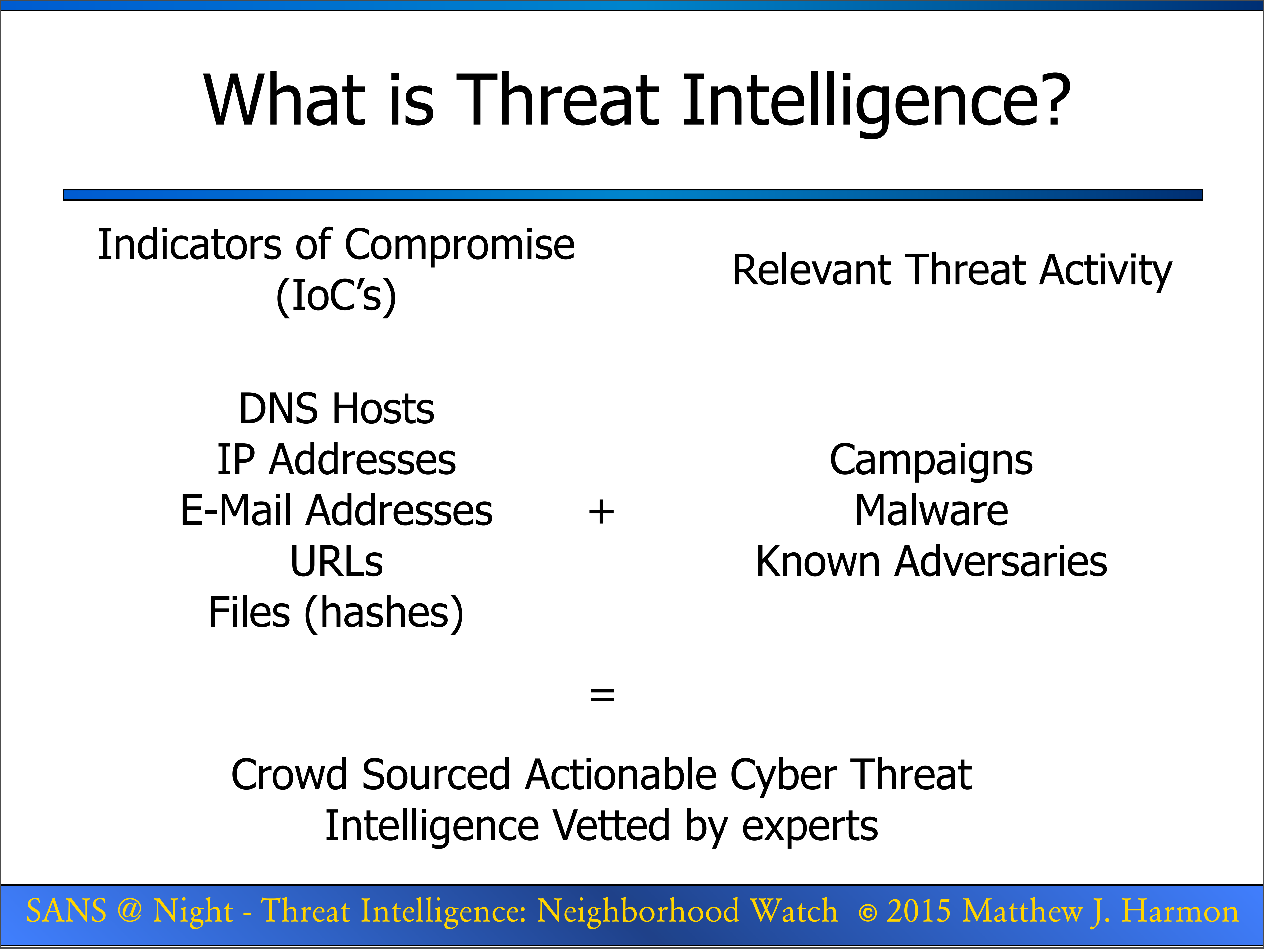
Thursday, July 23, 15

We need to learn from each other, this has become so apparent that on February 13th the POTUS signed Executive Order 13691 “Promoting Private Sector Cybersecurity Information Sharing”

without getting into too many details, this formed ISAO’s or “Information Sharing Analysis Organizations” as well as a Standards Body to oversee them and make deploying ISAO’s easy

Within two years, it is expected that there will be over 300 ISAO’s in various forms across the US, with international liaison relationships (nothing to do with the Ashley Madison breach)

The great thing is that anyone can participate!



What is Threat Intelligence?

Indicators of Compromise
(IoC's)

Relevant Threat Activity

DNS Hosts
IP Addresses
E-Mail Addresses
URLs
Files (hashes)

+

Campaigns
Malware
Known Adversaries

=

Crowd Sourced Actionable Cyber Threat
Intelligence Vetted by experts

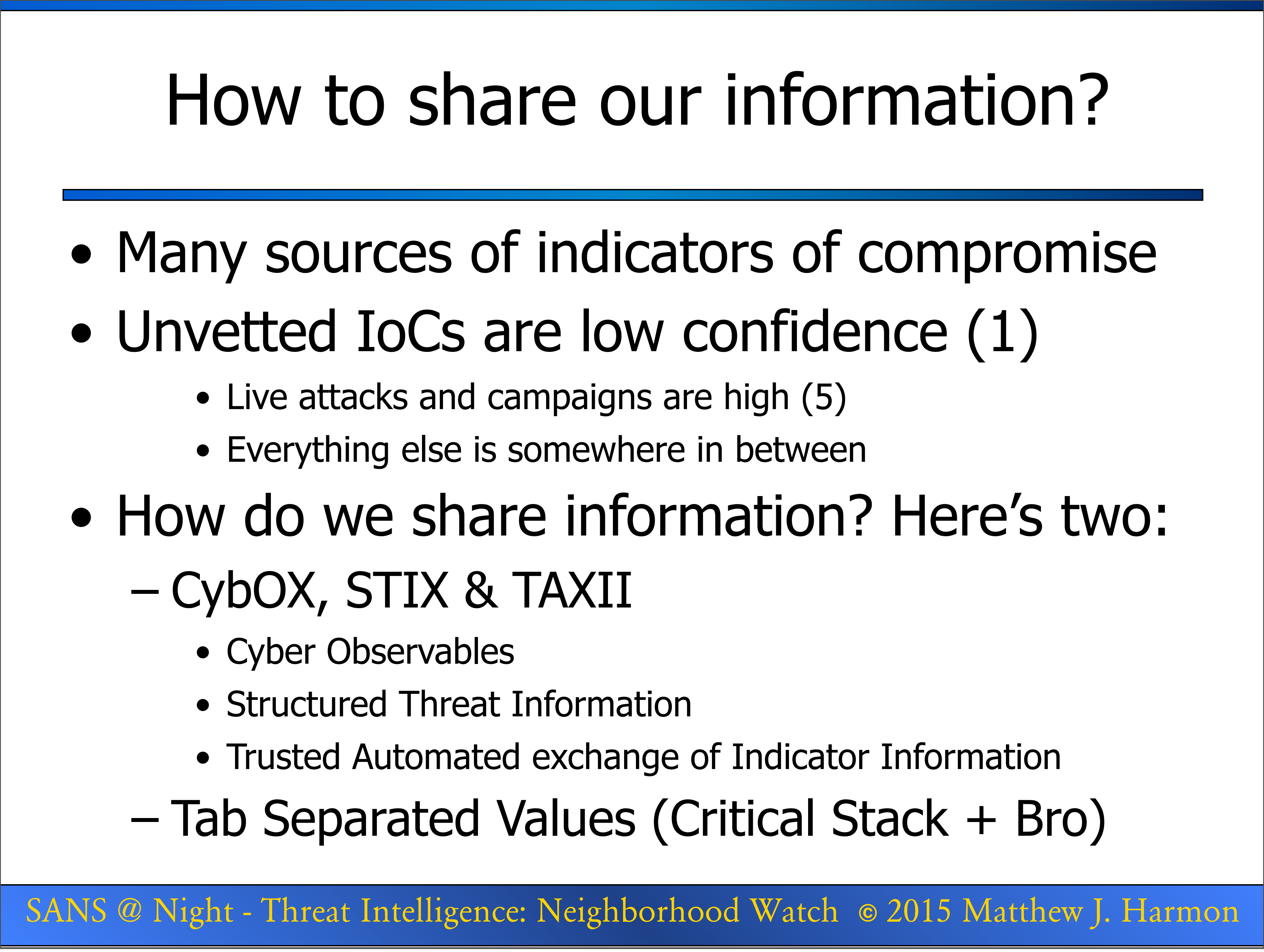
Threat Intelligence isn't easy, it's not ridiculously hard but as anyone with an formal .mil intel background can explain - the question is a matter of confidence in your sources

As we'll see, there are many sources out there which give you a combination of
DNS Hosts, IP Addresses, Email Addresses, URLs and File's with their associated names and hashes

The next step however, it to make that information relevant with campaigns and known adversaries

and finally, to link various crowd sourced IoCs and Threat Activity with vetting by experts

whew



How to share our information?

- Many sources of indicators of compromise
- Unvetted IoCs are low confidence (1)
  - Live attacks and campaigns are high (5)
  - Everything else is somewhere in between
- How do we share information? Here’s two:
  - CybOX, STIX & TAXII
    - Cyber Observables
    - Structured Threat Information
    - Trusted Automated exchange of Indicator Information
  - Tab Separated Values (Critical Stack + Bro)

So, how do we share this various intelligence information?

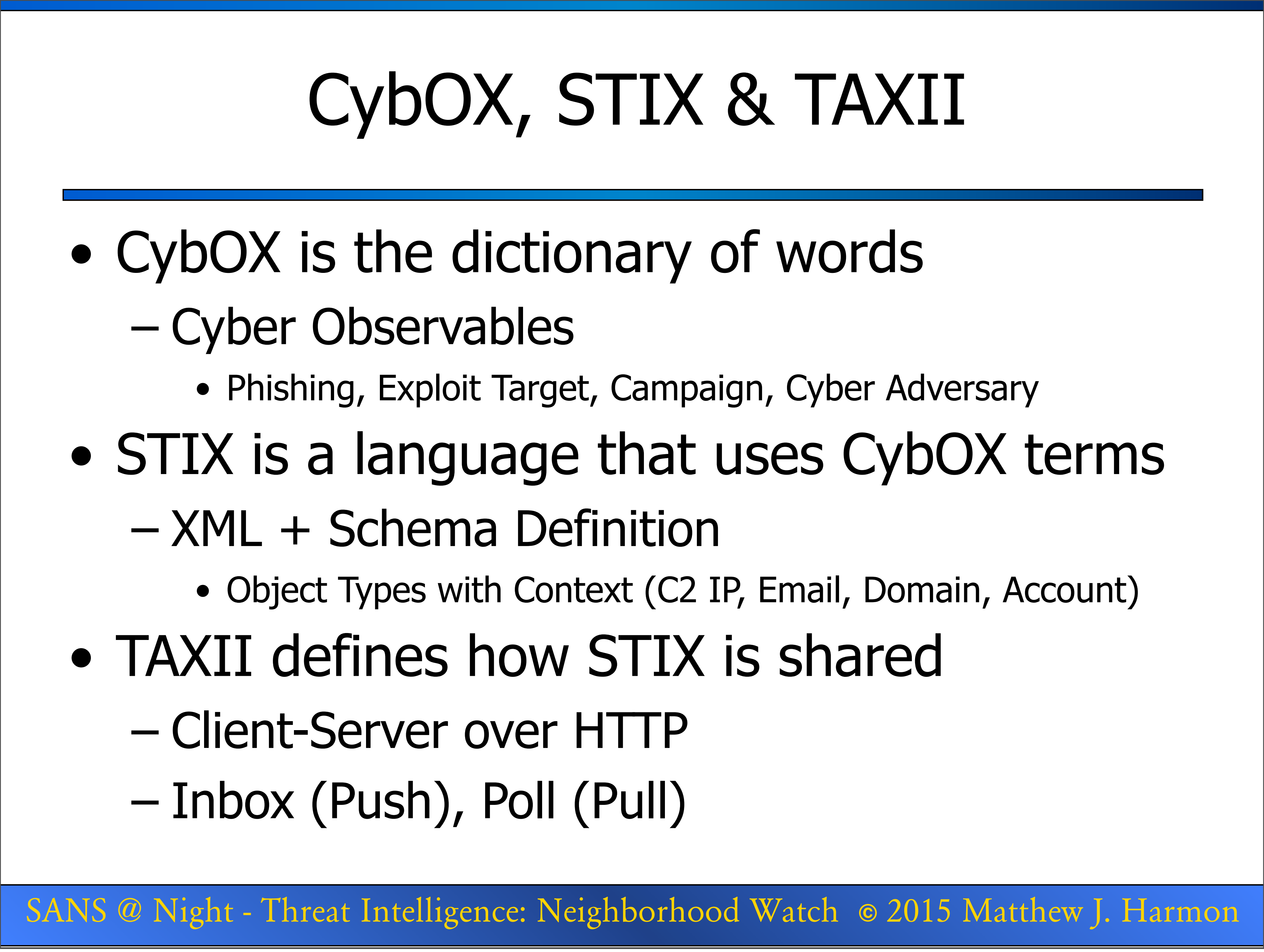
The up and coming methodologies are CybOX (Cyber Observables) STIX (Structured Threat Information) and TAXII the “Trusted Automated Exchange of Indicator Information”

spearheaded by the MITRE corporation (maintainers of CVE - the Common Vulnerability Enumeration glossary)

Recently transferred to OASIS

Bro however uses a much simpler combination of Tab Separated Values

Let’s take a look at both of these!



CybOX, STIX & TAXII

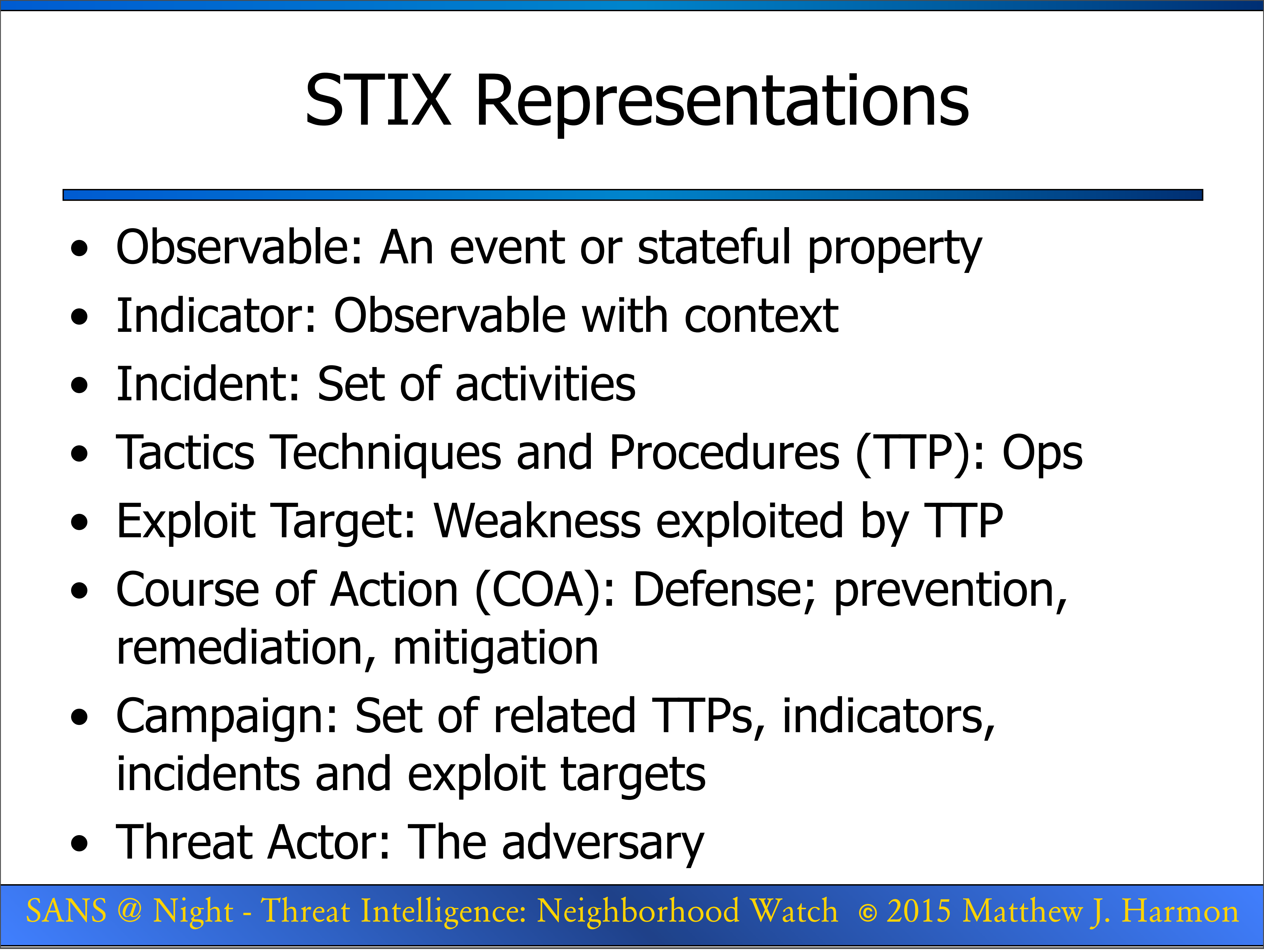
- CybOX is the dictionary of words
  - Cyber Observables
    - Phishing, Exploit Target, Campaign, Cyber Adversary
- STIX is a language that uses CybOX terms
  - XML + Schema Definition
    - Object Types with Context (C2 IP, Email, Domain, Account)
- TAXII defines how STIX is shared
  - Client-Server over HTTP
  - Inbox (Push), Poll (Pull)

CybOX, STIX and TAXII are very closely intertwined and take a bit to pull apart, there's also a malware analysis system but it's outside of the scope of what we're talking about today

CybOX is the dictionary of words - the cyber observables, things such as a Phishing Campaign, a Target, Tactics or an actual adversary

STIX is the language that uses the CybOX terms and includes objects with context, such as a Command and Control server, an email address a domain or an account

Finally, TAXII is the protocol for how STIX information is shared, it defines the client-server system over HTML and the concept of an Inbox (Pushing data) or pulling data through a poll request



STIX Representations

- Observable: An event or stateful property
- Indicator: Observable with context
- Incident: Set of activities
- Tactics Techniques and Procedures (TTP): Ops
- Exploit Target: Weakness exploited by TTP
- Course of Action (COA): Defense; prevention, remediation, mitigation
- Campaign: Set of related TTPs, indicators, incidents and exploit targets
- Threat Actor: The adversary

Thursday, July 23, 15

As mentioned, STIX are the representations, things such as an Observable (an email or file) or an indicator such as an IP , domain or file hash - which is an observable with a specific context

An incident is a set of specific activities

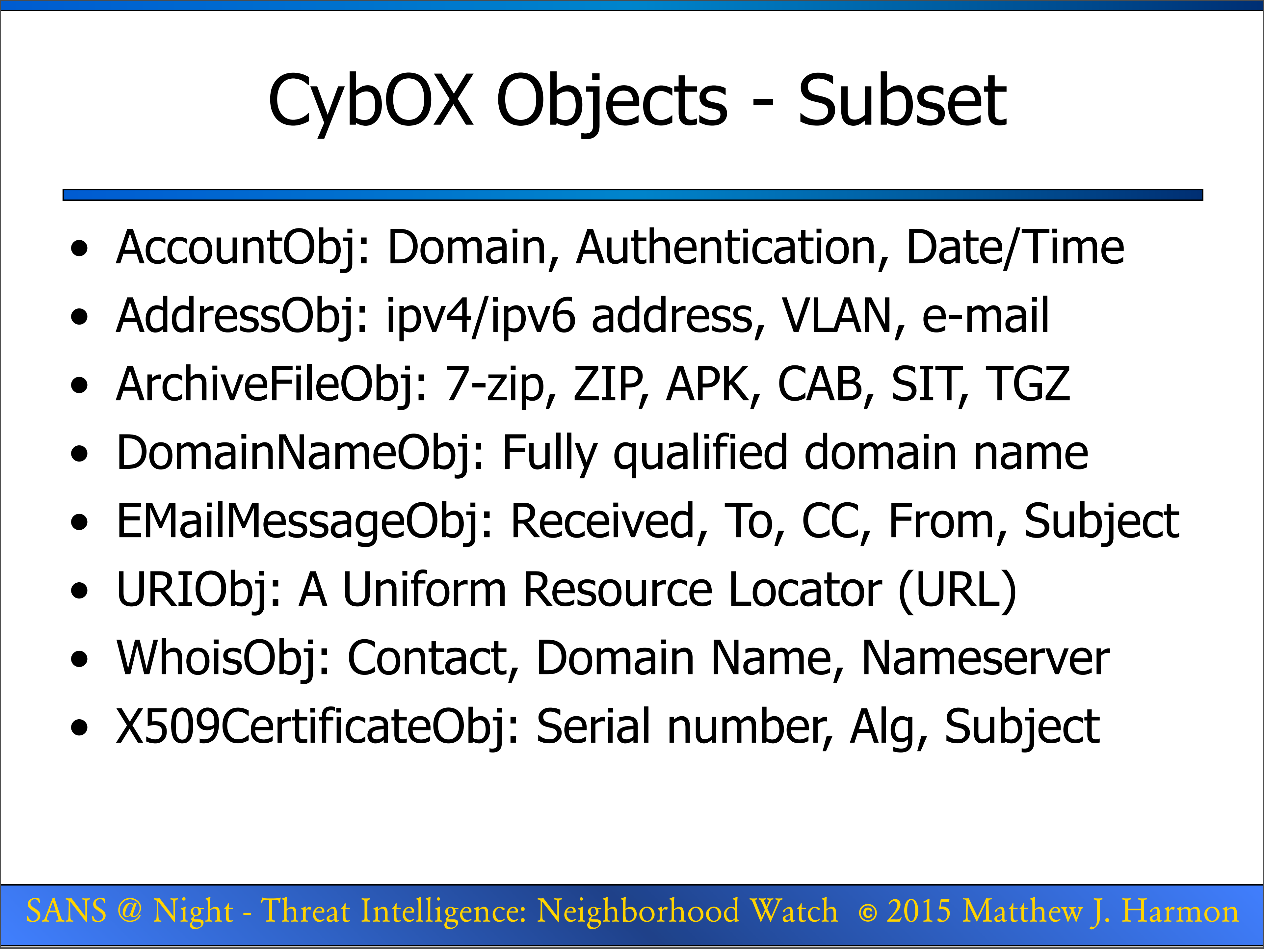
Your Tactics, Techniques and Procedures are the specific modus operandi or operations by a threat actor

An exploit target is a weakness exploited by a TTP

A COA or Course of Action is a defensive measure, prevention (blocking), remediation (patching) or mitigation to limit an impact

A campaign is a set of related Tactics, Techniques and Procedures, indicators, incidents and exploit targets

Finally a Threat Actor is the cyber adversary doing these actions.



CybOX Objects - Subset

- AccountObj: Domain, Authentication, Date/Time
- AddressObj: ipv4/ipv6 address, VLAN, e-mail
- ArchiveFileObj: 7-zip, ZIP, APK, CAB, SIT, TGZ
- DomainNameObj: Fully qualified domain name
- EMailMessageObj: Received, To, CC, From, Subject
- URIObj: A Uniform Resource Locator (URL)
- WhoisObj: Contact, Domain Name, Nameserver
- X509CertificateObj: Serial number, Alg, Subject

Thursday, July 23, 15

Cyber Obervables are things such as an Account (domain, authentication token or type, date and time of access and lock out state)

an address such as an ipv4 or v6 including things such as vlan, subnet or an email address

an Archive File Objects, such as 7-Zip, standard Zip, Android Package, CAB file, StuffIt or a unix Tar-GZip

As it sounds, a DomainName Objects is a fully qualified domain name such as SANS.org

The EmailMessage Objects include various headers such as received, to, cc, from, subject, body contents, any header, date or time

A Uniform Resource Identifier Object is in most cases a URL such as https://sans.org

Whois Objects are details from a domain whois record such as a contact, the domain name, a set of name servers

and an X509Certificate object includes items such as a serial number, algorithm or subject name

Real world CybOX, STIX & TAXII

- Excessive traffic is noticed on a server from a single workstation - investigation begins
- Tracing the workstation back to a user, an email from jane.smith@adp.com with a .zip attachment (Indicator)
- The email had a Return-Path: of <AmericanExpress@welcome.aexp.com>
- Received from: bba592142.alshamil.net.ae
- IP 86.98.54.68 (Indicator)

So, let's walk through a real world scenario using CybOX, STIX & TAXII

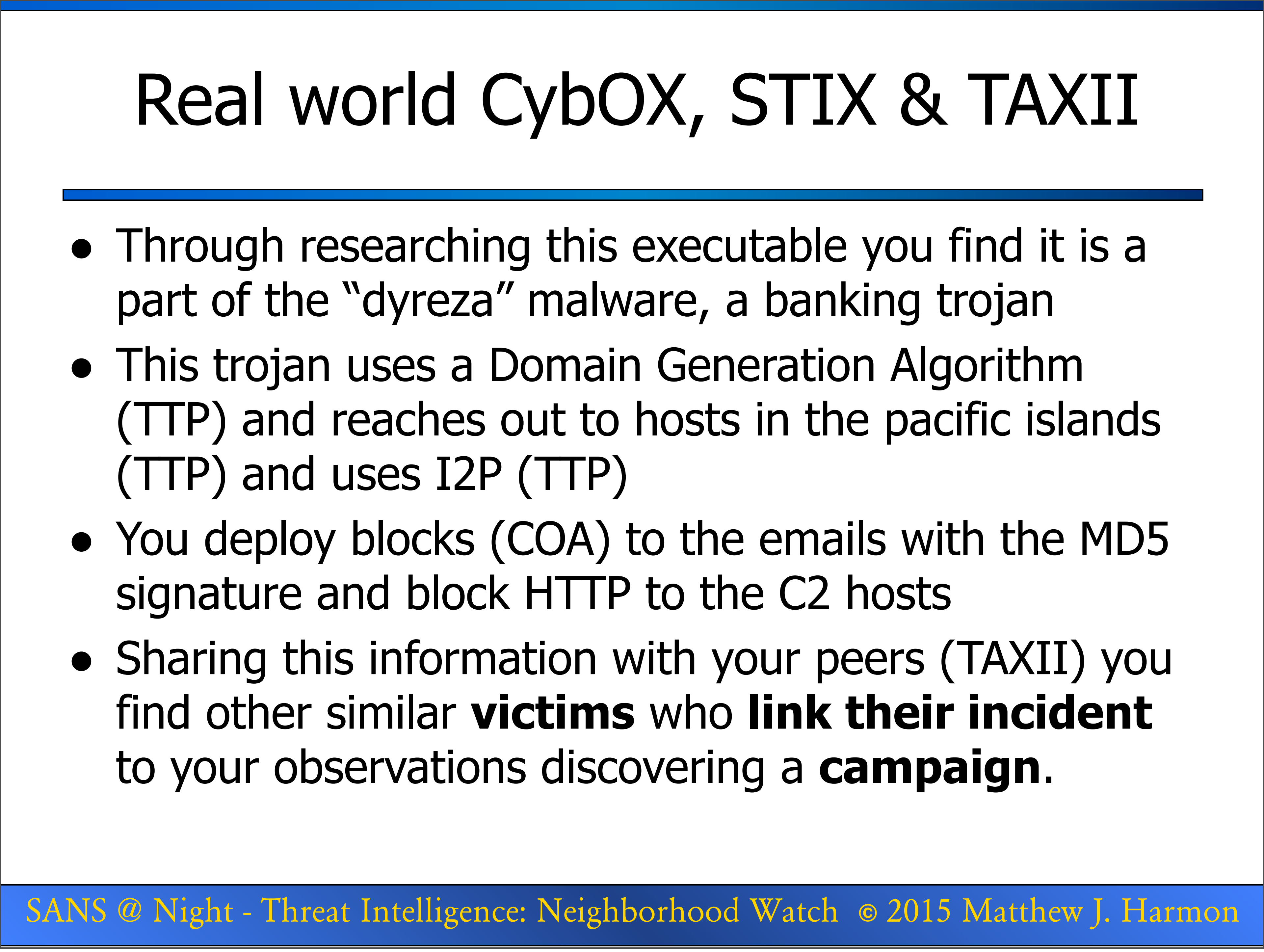
...

Real world CybOX, STIX & TAXII

- .zip attachment is named
  - Invoice_11082014.zip (indicator)
    - md5 5d6cbd0a557bb10603bb63b8fe0c4160
- .zip contains an executable
  - Invoice_11082014.exe
    - md5 911b7604e84096ee5bbb6741cf02542c (observable)
- Executable reaches out over HTTP to
  - 94.23.247.202 (indicator) redirects downloads to
    - porfintengoweb.com/css/11s1.zip
    - jc-charge-it.nl/pages/11s1.zip
    - flightss.d-webs.com/images/airlines-logo/h76id30.zip

When analyzing the zip attachment, we identified the md5, unzip'ed it and made an md5 of the executable as well

When researching this, we found the IPs that it reaches out to and the subsequent downloads that load additional material



Real world CybOX, STIX & TAXII

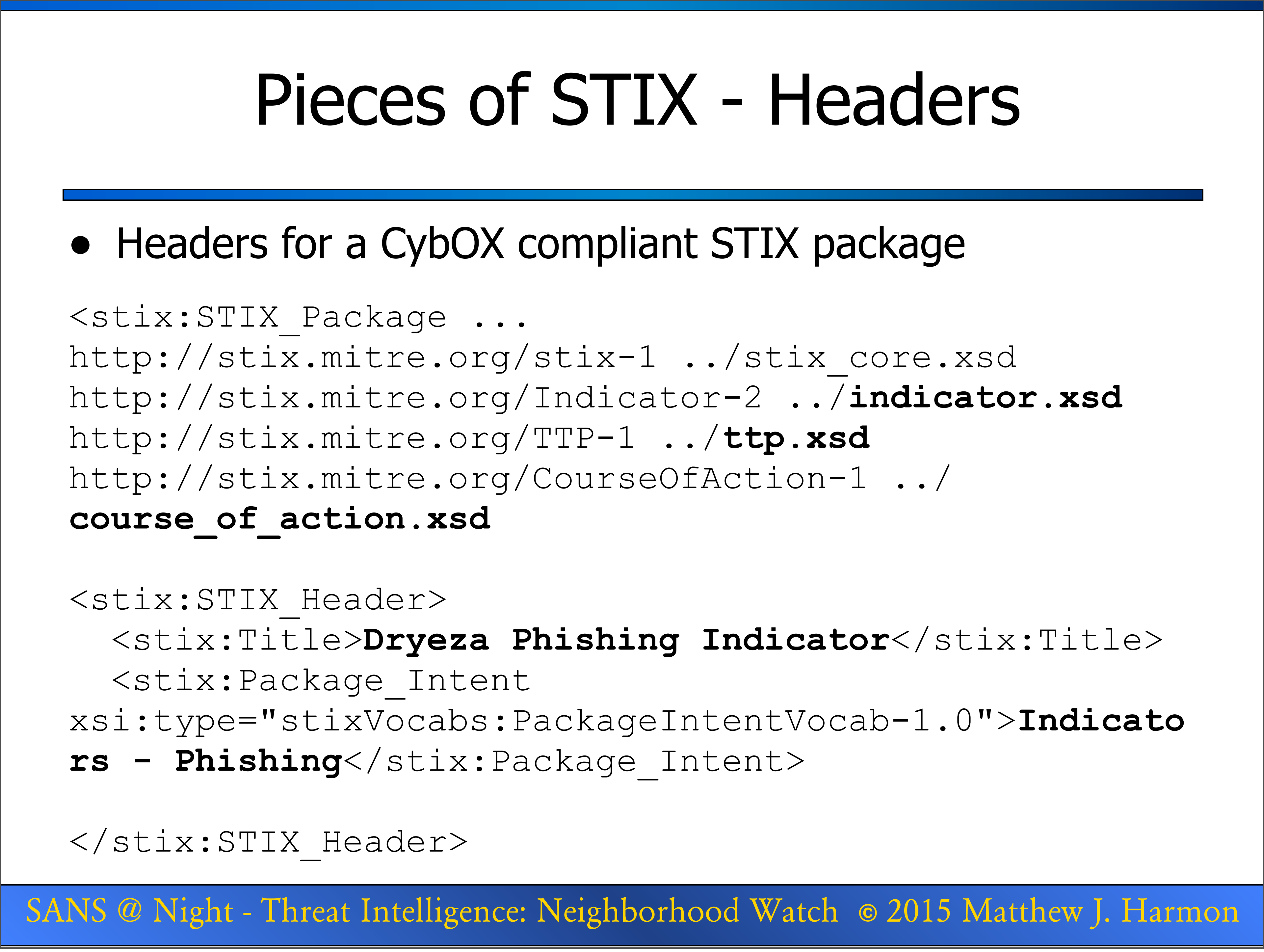
- Through researching this executable you find it is a part of the “dyreza” malware, a banking trojan
- This trojan uses a Domain Generation Algorithm (TTP) and reaches out to hosts in the pacific islands (TTP) and uses I2P (TTP)
- You deploy blocks (COA) to the emails with the MD5 signature and block HTTP to the C2 hosts
- Sharing this information with your peers (TAXII) you find other similar **victims** who **link their incident** to your observations discovering a **campaign**.

We discovered that this is the dyreza malware, which is a banking trojan

We found various TTP (Tactics, Techniques and Procedures), it uses a DGA, or Domain Generation Algorithm, uses I2P and frequently uses hosts in the pacific islands

In response, our Course of Action is to deploy various blocks to emails with a matching MD5 signature, and block HTTP traffic to the Command and Control Hosts

Afterwards, we share this information with our peers using TAXII and we find similar victims who link their incident observations to ours and we are able to map the campaign



Pieces of STIX - Headers

- Headers for a CybOX compliant STIX package

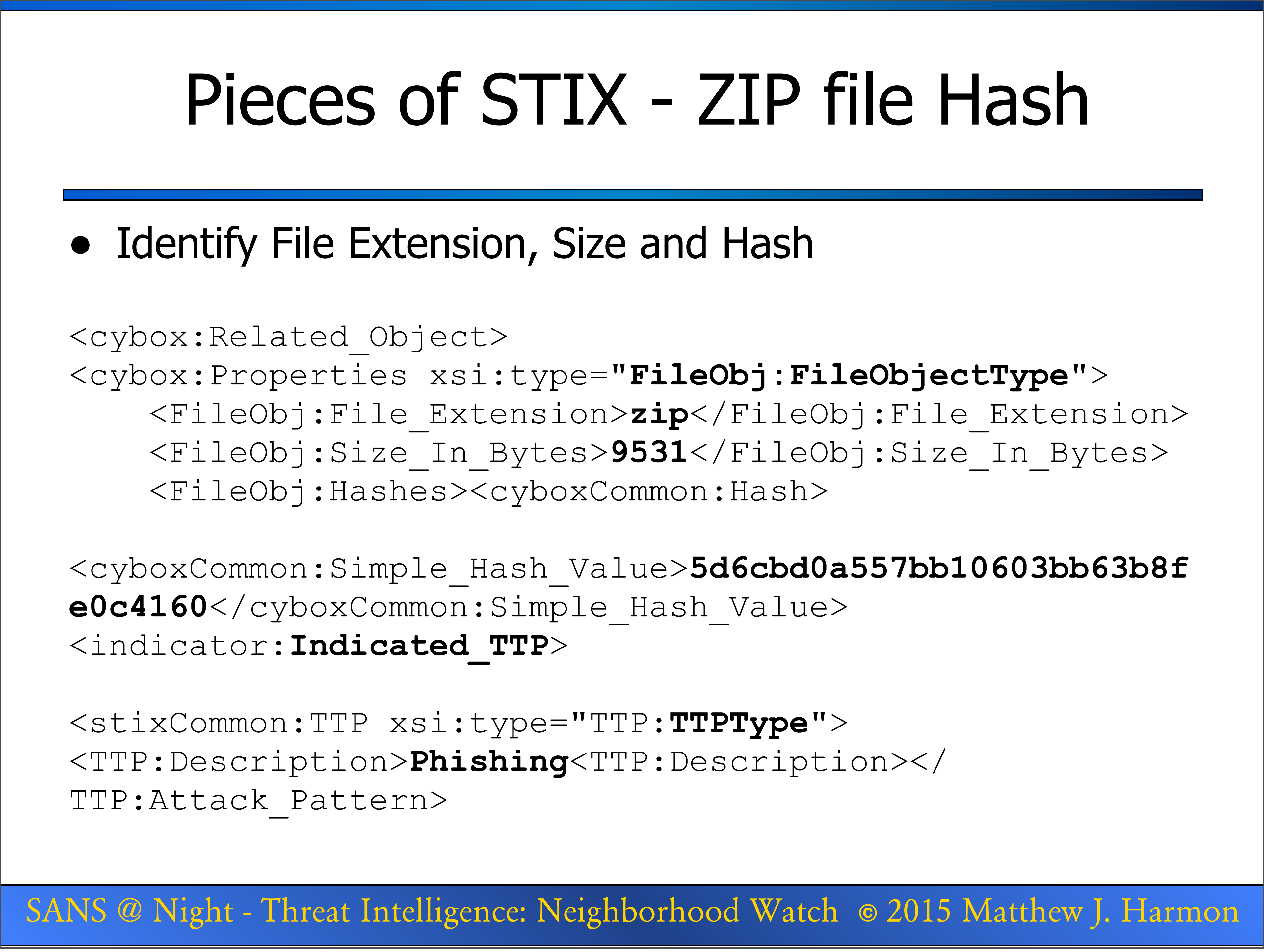
```
<stix:STIX_Package ...
http://stix.mitre.org/stix-1 ../stix_core.xsd
http://stix.mitre.org/Indicator-2 ../indicator.xsd
http://stix.mitre.org/TTP-1 ../ttp.xsd
http://stix.mitre.org/CourseOfAction-1 ../
course_of_action.xsd

<stix:STIX_Header>
  <stix:Title>Dryeza Phishing Indicator</stix:Title>
  <stix:Package_Intent
xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicato
rs - Phishing</stix:Package_Intent>

</stix:STIX_Header>
```

Thursday, July 23, 15

Using our scenario as an example, here are some pieces of our STIX header

We have the opening XML of the STIX Package and load the indicator, TTP and course of action xml schema definitions

We open with a STIX Header and Title it “Dryeza Phishing Indicator” and note that the Indicator is “Phishing”



Pieces of STIX - ZIP file Hash

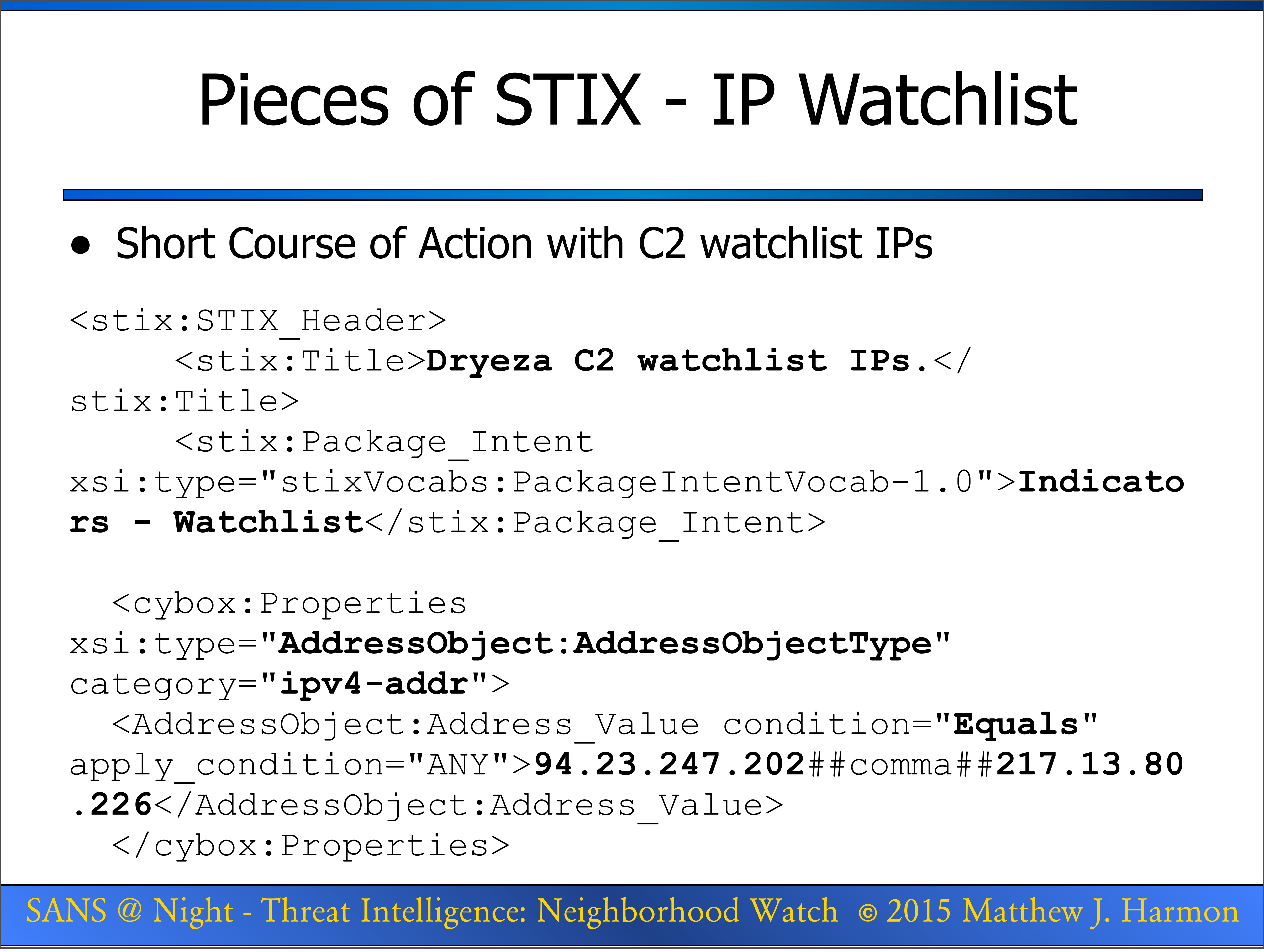
- Identify File Extension, Size and Hash

```
<cybox:Related_Object>
<cybox:Properties xsi:type="FileObj:FileObjectType">
    <FileObj:File_Extension>zip</FileObj:File_Extension>
    <FileObj:Size_In_Bytes>9531</FileObj:Size_In_Bytes>
    <FileObj:Hashes><cyboxCommon:Hash>

<cyboxCommon:Simple_Hash_Value>5d6cbd0a557bb10603bb63b8f
e0c4160</cyboxCommon:Simple_Hash_Value>
<indicator:Indicated_TTP>

<stixCommon:TTP xsi:type="TTP:TTPType">
<TTP:Description>Phishing<TTP:Description></
TTP:Attack_Pattern>
```

Thursday, July 23, 15

After our header, we want to identify that we received a ZIP file, it’s size, and our simple MD5 hash

Additionally, we want to mention that the TTP type and attack pattern is “Phishing”



Pieces of STIX - IP Watchlist

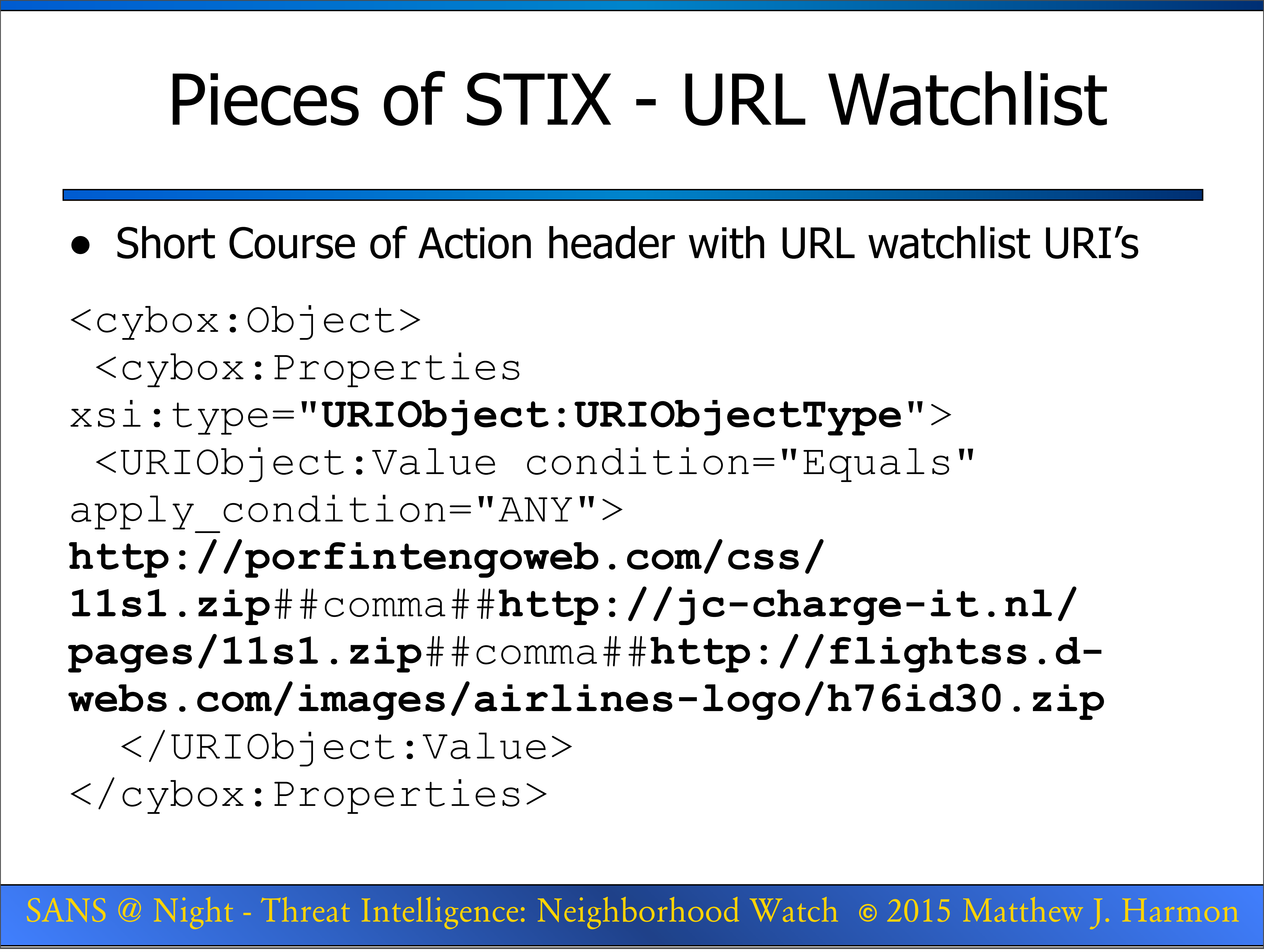
- Short Course of Action with C2 watchlist IPs

```
<stix:STIX_Header>
     <stix:Title>Dryeza C2 watchlist IPs.</
stix:Title>
     <stix:Package_Intent
xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicato
rs - Watchlist</stix:Package_Intent>

  <cybox:Properties
xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">
  <AddressObject:Address_Value condition="Equals"
apply_condition="ANY">94.23.247.202##comma##217.13.80
.226</AddressObject:Address_Value>
  </cybox:Properties>
```

Then we identify our C2 watchlist IPs with a clear title “Dryeza C2 watchlist IPs” and use our AddressObjectType of category ipv4-addr to match anything

that equals the values

94.23.247.202 or 217.13.80.226



Pieces of STIX - URL Watchlist

- Short Course of Action header with URL watchlist URI’s

```
<cybox:Object>
 <cybox:Properties
xsi:type="URIObject:URIObjectType">
 <URIObject:Value condition="Equals"
apply_condition="ANY">
http://porfintengoweb.com/css/
11s1.zip##comma##http://jc-charge-it.nl/
pages/11s1.zip##comma##http://flightss.d-
webs.com/images/airlines-logo/h76id30.zip
  </URIObject:Value>
</cybox:Properties>
```

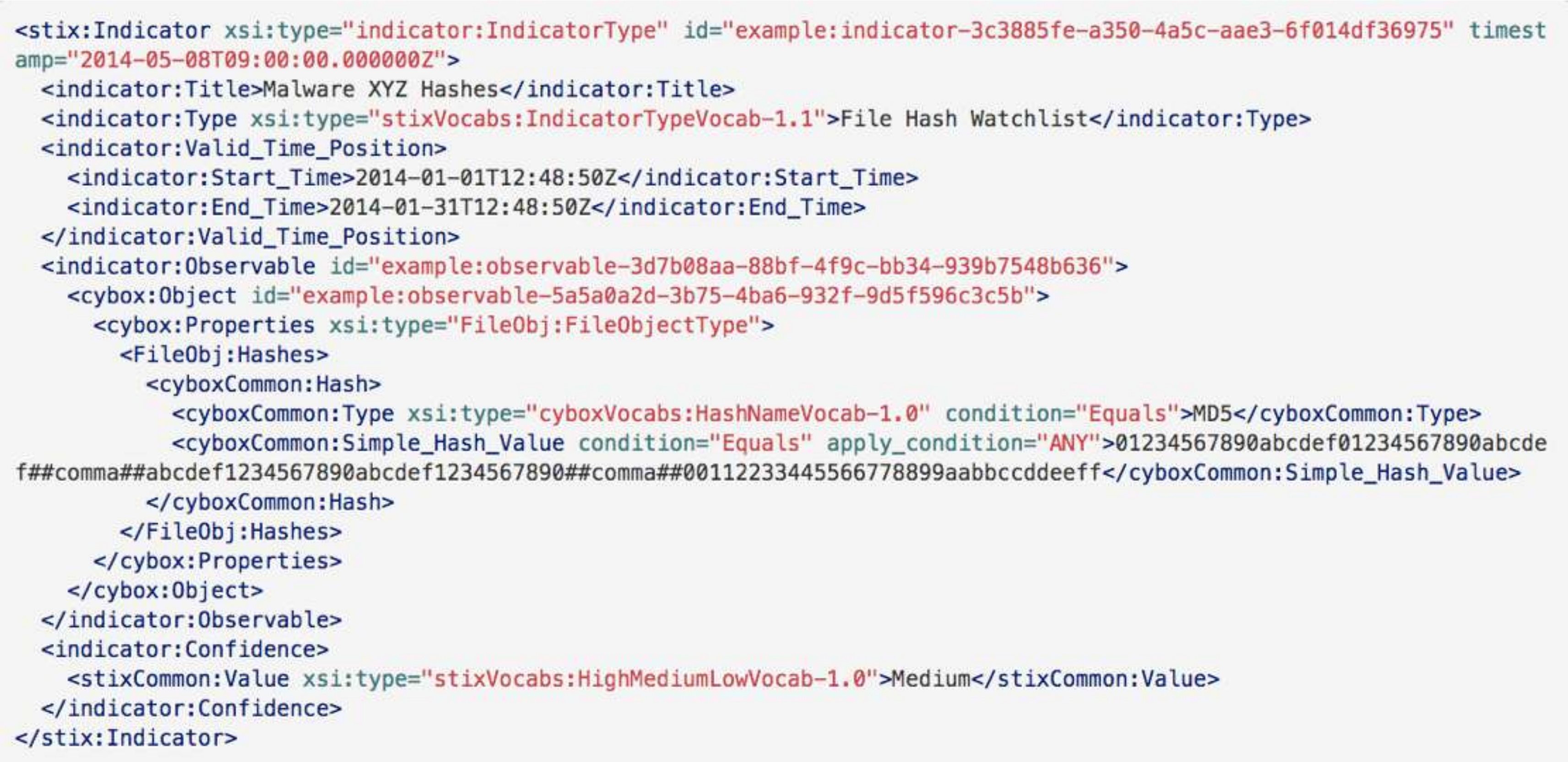
Thursday, July 23, 15

Finally, we write a URL Watchlist record to block the URIObjectType’s that match the domains with additional downloaders that we discovered

Example IOC via CybOX + STIX

What does a full IoC with CybOX and STIX look like?

Example IOC via CybOX + STIX



```
<stix:Indicator xsi:type="indicator:IndicatorType" id="example:indicator-3c3885fe-a350-4a5c-aae3-6f014df36975" timest
amp="2014-05-08T09:00:00.000000Z">
  <indicator:Title>Malware XYZ Hashes</indicator:Title>
  <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">File Hash Watchlist</indicator:Type>
  <indicator:Valid_Time_Position>
    <indicator:Start_Time>2014-01-01T12:48:50Z</indicator:Start_Time>
    <indicator:End_Time>2014-01-31T12:48:50Z</indicator:End_Time>
  </indicator:Valid_Time_Position>
  <indicator:Observable id="example:observable-3d7b08aa-88bf-4f9c-bb34-939b7548b636">
    <cybox:Object id="example:observable-5a5a0a2d-3b75-4ba6-932f-9d5f596c3c5b">
      <cybox:Properties xsi:type="FileObj:FileObjectType">
        <FileObj:Hashes>
          <cyboxCommon:Hash>
            <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0" condition="Equals">MD5</cyboxCommon:Type>
            <cyboxCommon:Simple_Hash_Value condition="Equals" apply_condition="ANY">01234567890abcdef01234567890abcde
f##comma##abcdef1234567890abcdef1234567890##comma##00112233445566778899aabbccddeeff</cyboxCommon:Simple_Hash_Value>
          </cyboxCommon:Hash>
        </FileObj:Hashes>
      </cybox:Properties>
    </cybox:Object>
  </indicator:Observable>
  <indicator:Confidence>
    <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">Medium</stixCommon:Value>
  </indicator:Confidence>
</stix:Indicator>
```

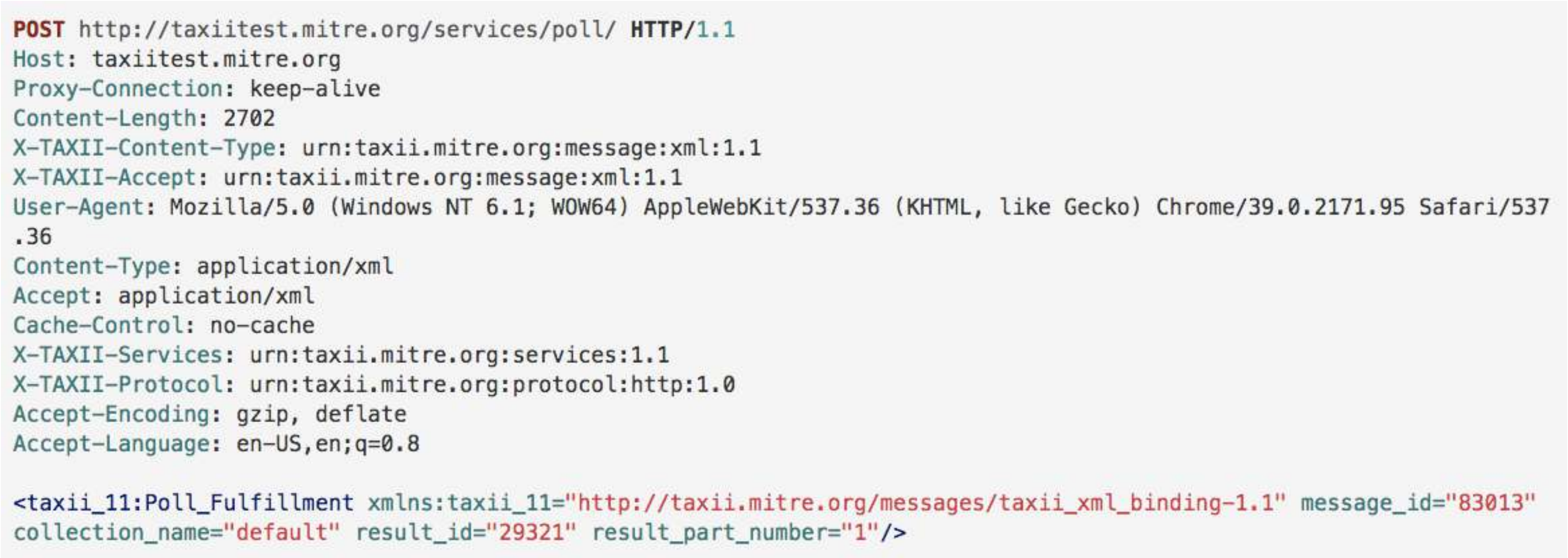
Something like this...

We have a File Hash Watchlist is the indicator
The valid time
The FileObjectType
Hash type is an MD5
Hash value is...
and the confidence level is Medium

Example TAXII Poll (Pull) Request

So once we’ve pushed out our TAXII record for our peers through the Inbox, they can pull it with a Poll Request

Example TAXII Poll (Pull) Request



```
POST http://taxiitest.mitre.org/services/poll/ HTTP/1.1
Host: taxiitest.mitre.org
Proxy-Connection: keep-alive
Content-Length: 2702
X-TAXII-Content-Type: urn:taxii.mitre.org:message:xml:1.1
X-TAXII-Accept: urn:taxii.mitre.org:message:xml:1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537
.36
Content-Type: application/xml
Accept: application/xml
Cache-Control: no-cache
X-TAXII-Services: urn:taxii.mitre.org:services:1.1
X-TAXII-Protocol: urn:taxii.mitre.org:protocol:http:1.0
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8

<taxii_11:Poll_Fulfillment xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1" message_id="83013"
collection_name="default" result_id="29321" result_part_number="1"/>
```

Thursday, July 23, 15

Here we see a TAXII Poll request, which runs over HTTP

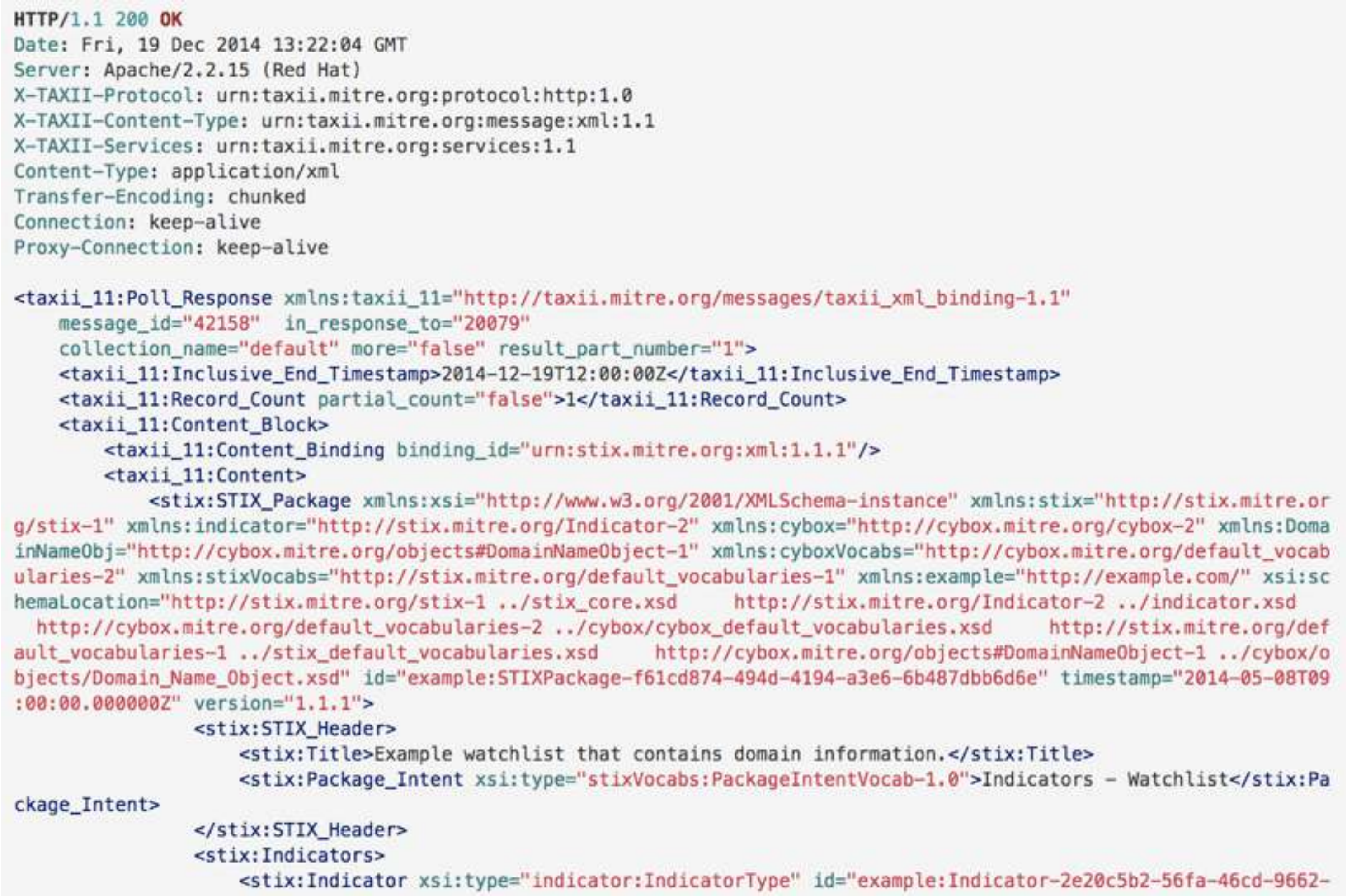
We see the headers: Host, Content-Type and User-Agent as well as Services and Protocol version numbers

Followed by a Poll_Fullfillment request

Example TAXII Poll (Pull) Response

The response will look similar to this

Example TAXII Poll (Pull) Response



```
HTTP/1.1 200 OK
Date: Fri, 19 Dec 2014 13:22:04 GMT
Server: Apache/2.2.15 (Red Hat)
X-TAXII-Protocol: urn:taxii.mitre.org:protocol:http:1.0
X-TAXII-Content-Type: urn:taxii.mitre.org:message:xml:1.1
X-TAXII-Services: urn:taxii.mitre.org:services:1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Connection: keep-alive
Proxy-Connection: keep-alive

<taxii_11:Poll_Response xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
    message_id="42158"  in_response_to="20079"
    collection_name="default" more="false" result_part_number="1">
    <taxii_11:Inclusive_End_Timestamp>2014-12-19T12:00:00Z</taxii_11:Inclusive_End_Timestamp>
    <taxii_11:Record_Count partial_count="false">1</taxii_11:Record_Count>
    <taxii_11:Content_Block>
        <taxii_11:Content_Binding binding_id="urn:stix.mitre.org:xml:1.1.1"/>
        <taxii_11:Content>
            <stix:STIX_Package xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:stix="http://stix.mitre.or
g/stix-1" xmlns:indicator="http://stix.mitre.org/Indicator-2" xmlns:cybox="http://cybox.mitre.org/cybox-2" xmlns:Doma
inNameObj="http://cybox.mitre.org/objects#DomainNameObject-1" xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocab
ularies-2" xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1" xmlns:example="http://example.com/" xsi:sc
hemaLocation="http://stix.mitre.org/stix-1 ../stix_core.xsd     http://stix.mitre.org/Indicator-2 ../indicator.xsd
  http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd     http://stix.mitre.org/def
ault_vocabularies-1 ../stix_default_vocabularies.xsd     http://cybox.mitre.org/objects#DomainNameObject-1 ../cybox/o
bjects/Domain_Name_Object.xsd" id="example:STIXPackage-f61cd874-494d-4194-a3e6-6b487dbb6d6e" timestamp="2014-05-08T09
:00:00.000000Z" version="1.1.1">
                <stix:STIX_Header>
                    <stix:Title>Example watchlist that contains domain information.</stix:Title>
                    <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Pa
ckage_Intent>
                </stix:STIX_Header>
                <stix:Indicators>
                    <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-2e20c5b2-56fa-46cd-9662-
```

Thursday, July 23, 15

In response to the Poll Fullfillment request, we see an HTTP response

Server version

Protocol, Content Type and Services versions

Followed by the Poll Response

Let’s look at two different exchanges

- ThreatConnect is a collaborative Threat Intelligence Platform
  - Threat data collection, analysis, collaboration
  - Incident response experts on staff to vet info
  - Free for NorSec and other ISAO Members
- CriticalStack // Intel is an aggregation of open source indicators of compromise
  - 100+ Feeds, easy to read Tab Separated Values, client integration with Bro!

So, how do we put all of this together? Let’s look at two different data exchange formats, first

we have systems that use CybOX, STIX and TAXII for inter-compatibility

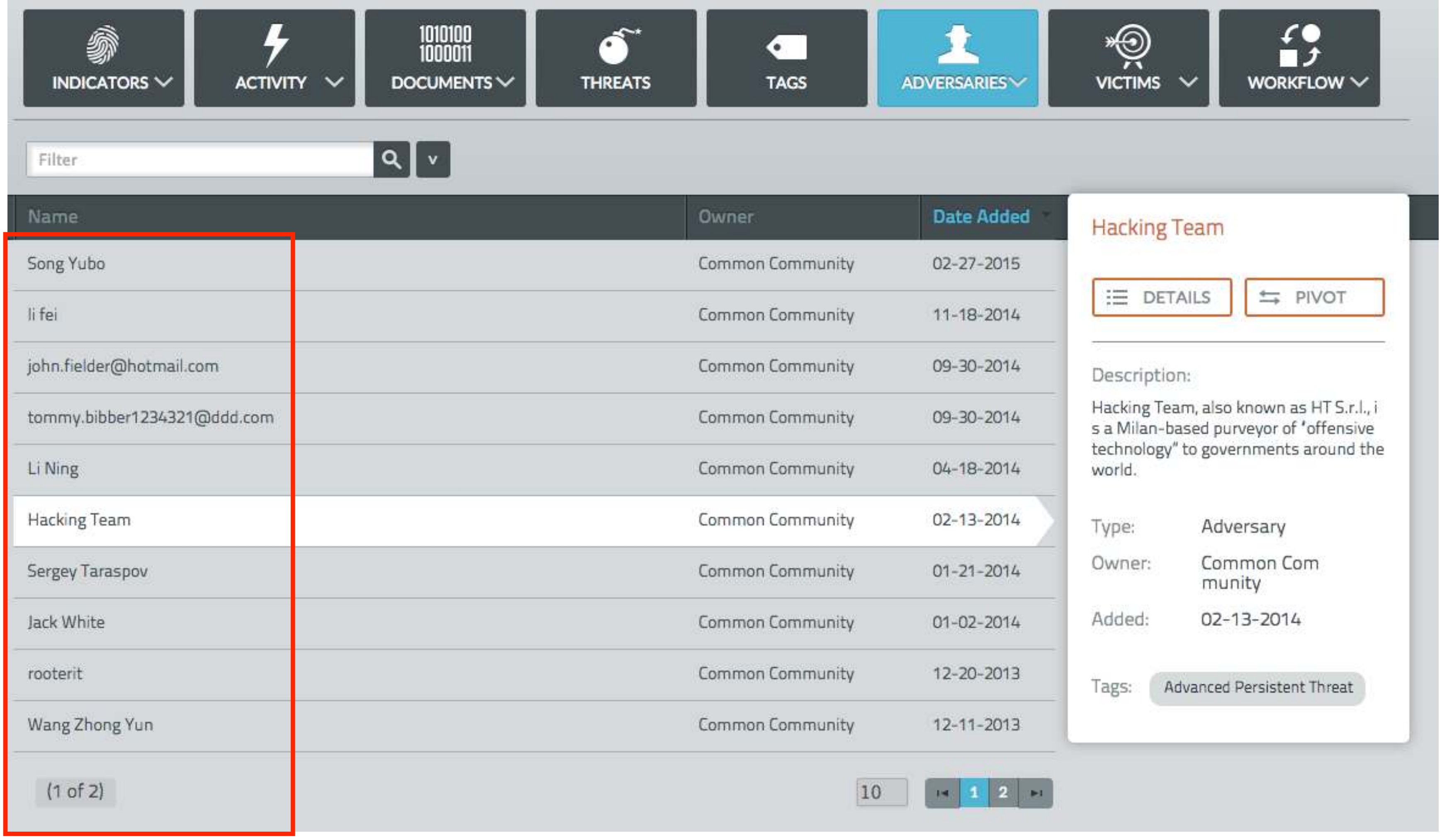
We also have systems such as CriticalStack // Intel that aggregate open source indicators of compromise using Tab Separated Values that load easily into BRO

Your open source IoCs should be considered low to medium confidence level as they are not vetted by experts as the ThreatConnect sources are, however they are still VERY valuable!

Known Adversaries (ThreatConnect)

Let’s take a look at some known adversaries in ThreatConnect

Known Adversaries (ThreatConnect)



Name	Owner	Date Added
Song Yubo	Common Community	02-27-2015
li fei	Common Community	11-18-2014
john.fielder@hotmail.com	Common Community	09-30-2014
tommy.bibber1234321@ddd.com	Common Community	09-30-2014
Li Ning	Common Community	04-18-2014
Hacking Team	Common Community	02-13-2014
Sergey Taraspov	Common Community	01-21-2014
Jack White	Common Community	01-02-2014
rooterit	Common Community	12-20-2013
Wang Zhong Yun	Common Community	12-11-2013

(1 of 2)

Hacking Team

Description:

Hacking Team, also known as HT S.r.l., is a Milan-based purveyor of 'offensive technology" to governments around the world.

Type: Adversary

Owner: Common Community

Added: 02-13-2014

Tags: Advanced Persistent Threat

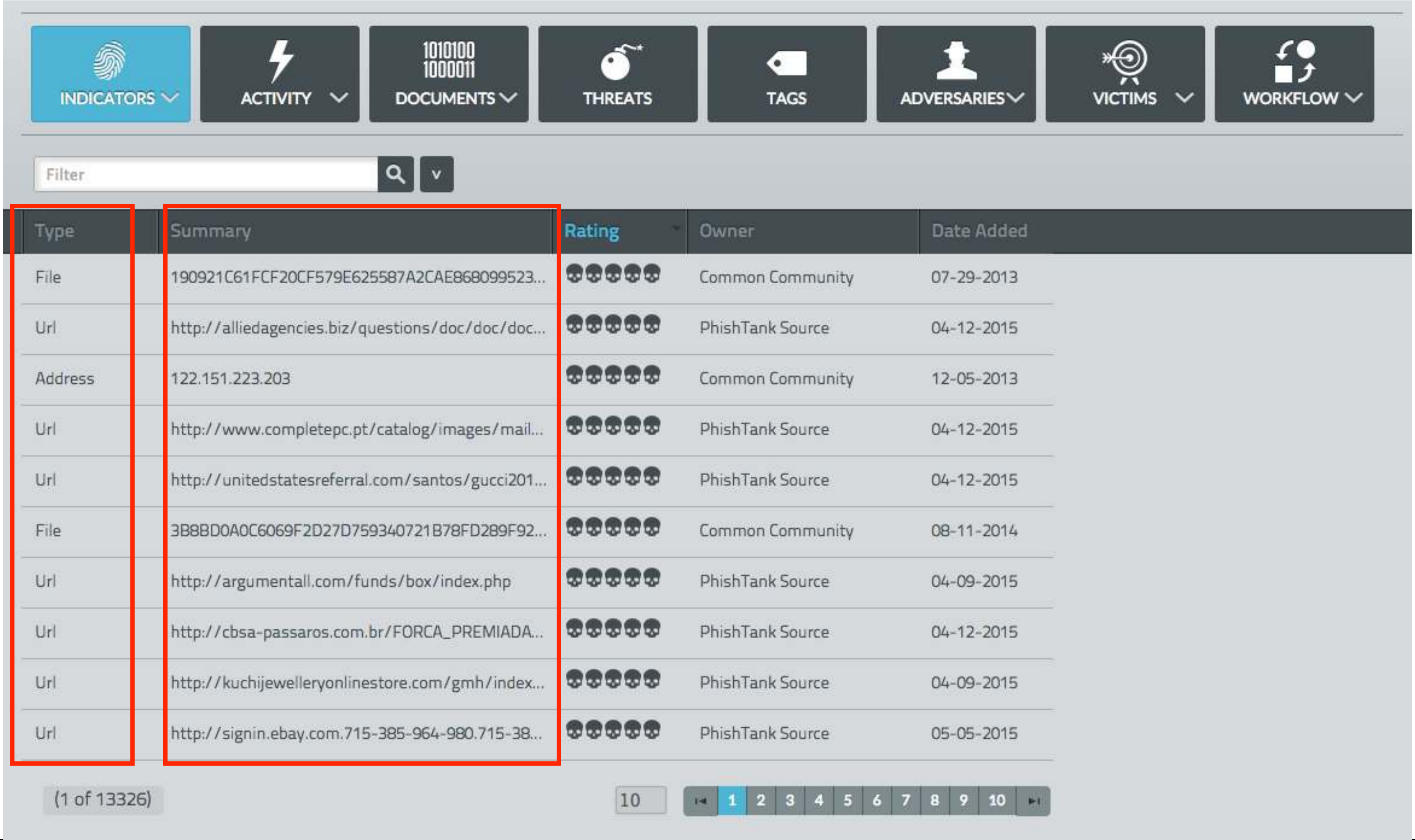
Thursday, July 23, 15

You may have heard of this group called "Hacking Team" based out of Milan, there are several other known adversaries out there

Indicators of Compromise (ThreatConnect)

Each adversary has specific IoCs associated with them as they frequently sell the same tools to multiple parties with very few modifications, not exactly polymorphic malware

Indicators of Compromise (ThreatConnect)



Type	Summary	Rating	Owner	Date Added
File	190921C61FCF20CF579E625587A2CAE868099523...	☠☠☠☠☠	Common Community	07-29-2013
Url	http://alliedagencies.biz/questions/doc/doc/doc...	☠☠☠☠☠	PhishTank Source	04-12-2015
Address	122.151.223.203	☠☠☠☠☠	Common Community	12-05-2013
Url	http://www.completepc.pt/catalog/images/mail...	☠☠☠☠☠	PhishTank Source	04-12-2015
Url	http://unitedstatesreferral.com/santos/gucci201...	☠☠☠☠☠	PhishTank Source	04-12-2015
File	3B8BD0A0C6069F2D27D759340721B78FD289F92...	☠☠☠☠☠	Common Community	08-11-2014
Url	http://argumentall.com/funds/box/index.php	☠☠☠☠☠	PhishTank Source	04-09-2015
Url	http://cbsa-passaros.com.br/FORCA_PREMIADA...	☠☠☠☠☠	PhishTank Source	04-12-2015
Url	http://kuchijewelleryonlinestore.com/gmh/index...	☠☠☠☠☠	PhishTank Source	04-09-2015
Url	http://signin.ebay.com.715-385-964-980.715-38...	☠☠☠☠☠	PhishTank Source	05-05-2015

(1 of 13326)   10   1 2 3 4 5 6 7 8 9 10

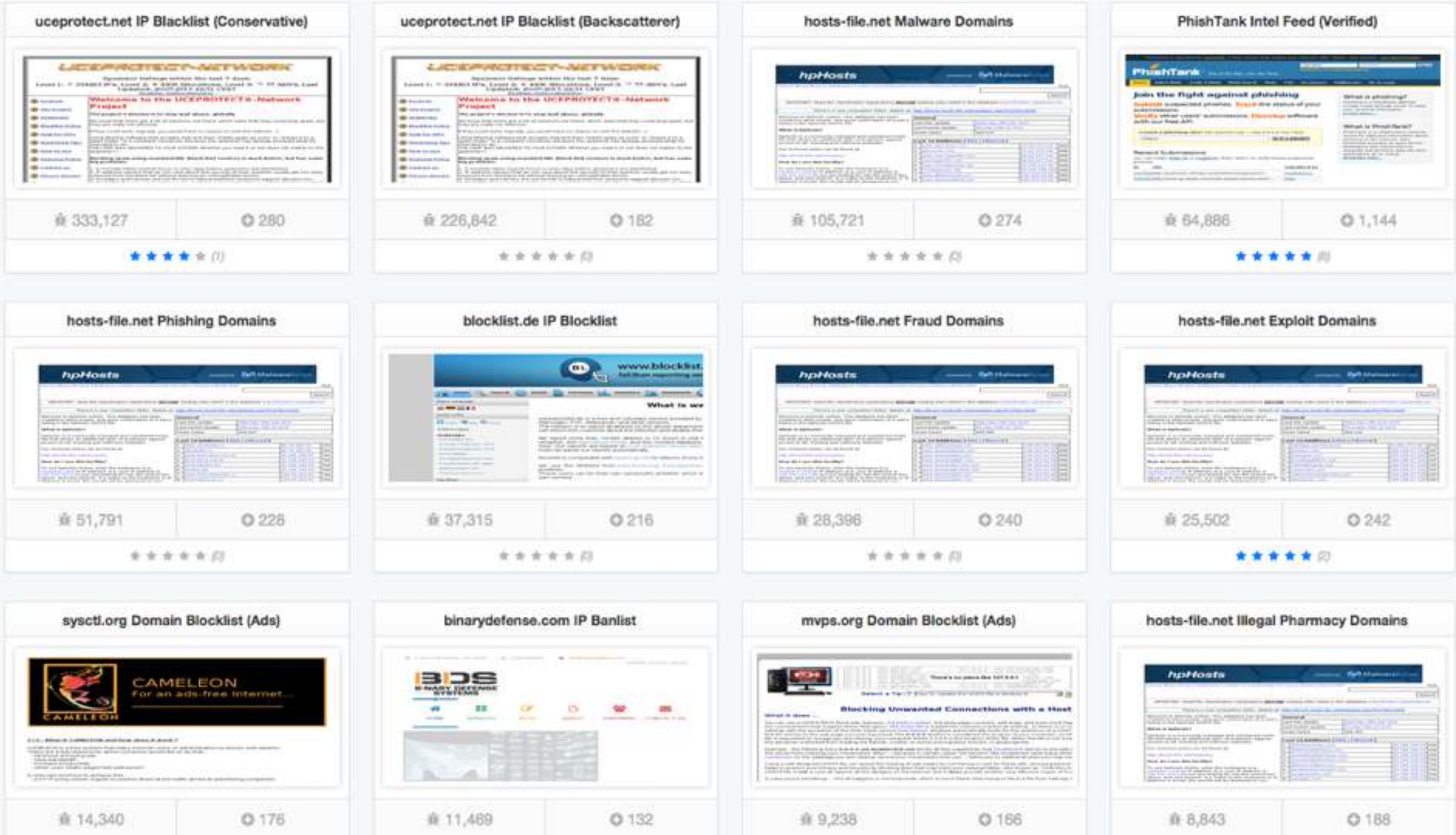
Thursday, July 23, 15

In this case we have file hashes, URLs that are known, and hostile addresses

Feeds (CriticalStack // Intel)

Now let’s take a closer look at Critical Stack, their intel feeds are extensive

Feeds (CriticalStack // Intel)



uceprotect.net IP Blacklist (Conservative)
333,127 · 280
★★★★☆ (1)

uceprotect.net IP Blacklist (Backscatterer)
226,842 · 182
☆☆☆☆☆ (0)

hosts-file.net Malware Domains
105,721 · 274
☆☆☆☆☆ (0)

PhishTank Intel Feed (Verified)
64,886 · 1,144
★★★★★ (6)

hosts-file.net Phishing Domains
51,791 · 228
☆☆☆☆☆ (0)

blocklist.de IP Blocklist
37,315 · 216
☆☆☆☆☆ (0)

hosts-file.net Fraud Domains
28,396 · 240
☆☆☆☆☆ (0)

hosts-file.net Exploit Domains
25,502 · 242
★★★★★ (2)

sysctl.org Domain Blocklist (Ads)
14,340 · 176

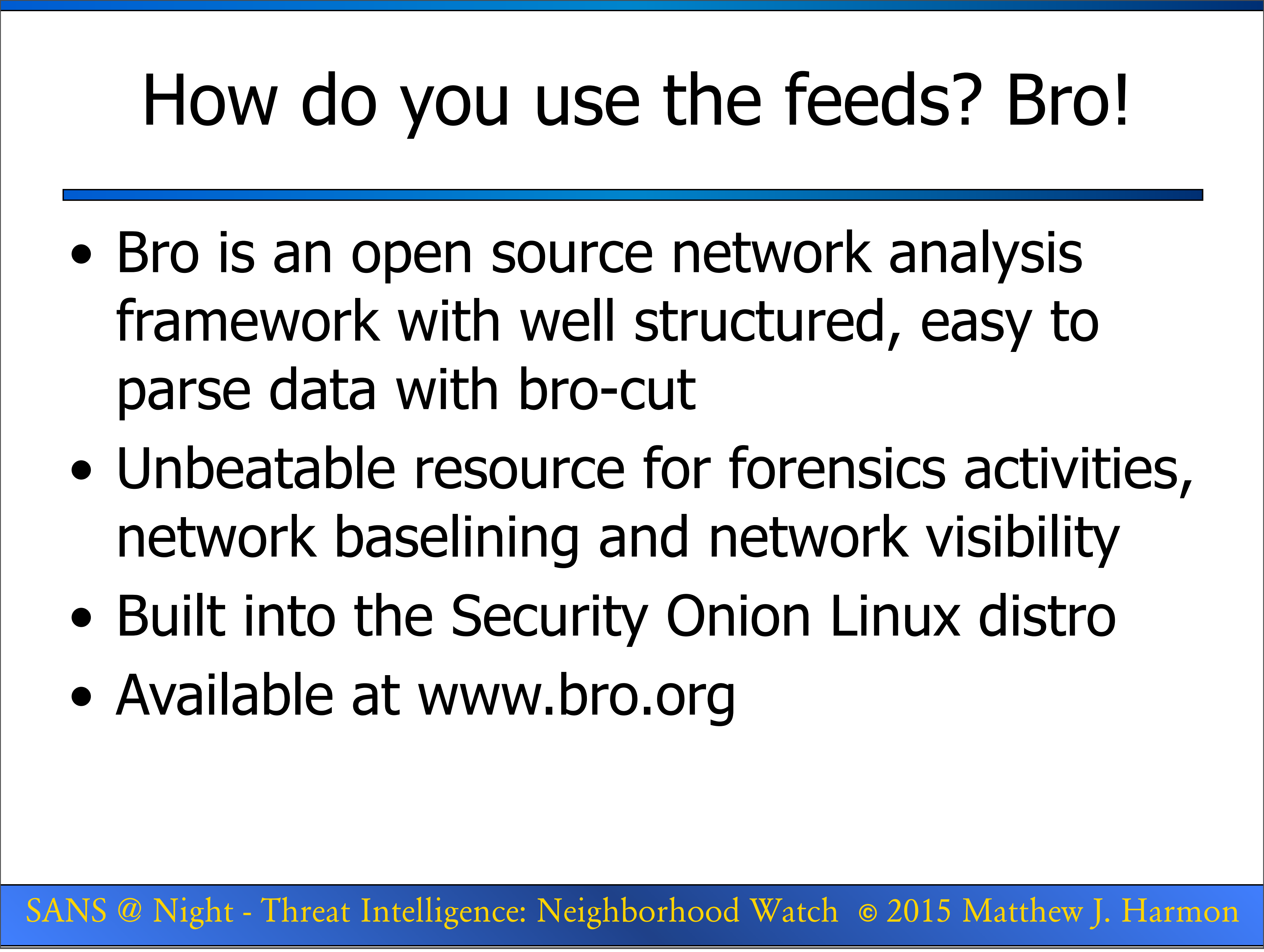
binarydefense.com IP Banlist
11,469 · 132

mvps.org Domain Blocklist (Ads)
9,238 · 166

hosts-file.net Illegal Pharmacy Domains
8,843 · 188

Thursday, July 23, 15

They have aggregated over 100 specific block lists, known fraudulent domains, hostile ads, botnet IPs and exploit hosting domains



How do you use the feeds? Bro!

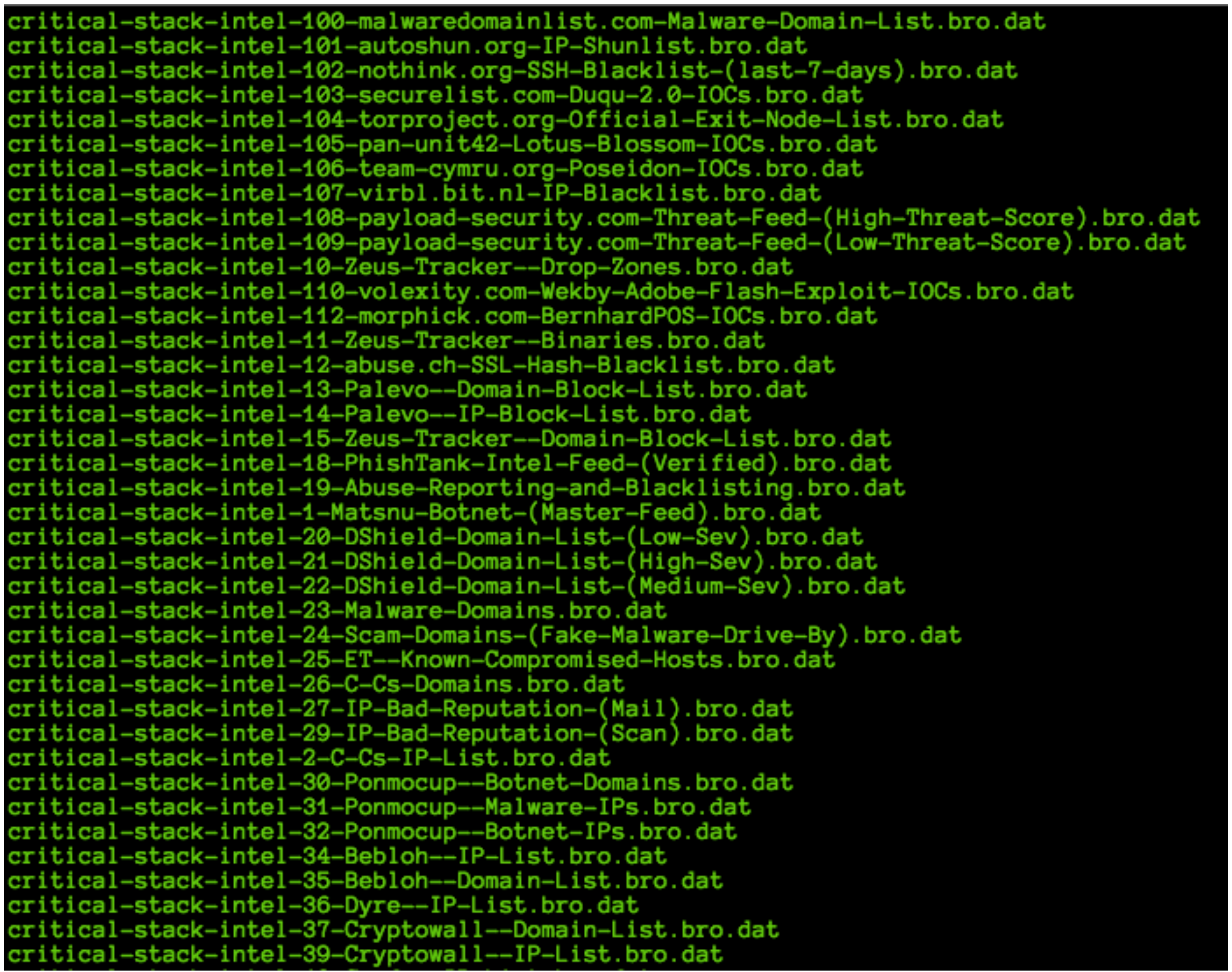
- Bro is an open source network analysis framework with well structured, easy to parse data with bro-cut
- Unbeatable resource for forensics activities, network baselining and network visibility
- Built into the Security Onion Linux distro
- Available at www.bro.org

We mentioned earlier that we can integrate the Critical Stack Intel feed with Bro, but what it Bro?

Feeds (.bro.dat)

Once you download the Critical Stack Intel Feeds, you get a long list of files ending in .bro.dat

Feeds (.bro.dat)



```
critical-stack-intel-100-malwaredomainlist.com-Malware-Domain-List.bro.dat
critical-stack-intel-101-autoshun.org-IP-Shunlist.bro.dat
critical-stack-intel-102-nothink.org-SSH-Blacklist-(last-7-days).bro.dat
critical-stack-intel-103-securelist.com-Duqu-2.0-IOCs.bro.dat
critical-stack-intel-104-torproject.org-Official-Exit-Node-List.bro.dat
critical-stack-intel-105-pan-unit42-Lotus-Blossom-IOCs.bro.dat
critical-stack-intel-106-team-cymru.org-Poseidon-IOCs.bro.dat
critical-stack-intel-107-virbl.bit.nl-IP-Blacklist.bro.dat
critical-stack-intel-108-payload-security.com-Threat-Feed-(High-Threat-Score).bro.dat
critical-stack-intel-109-payload-security.com-Threat-Feed-(Low-Threat-Score).bro.dat
critical-stack-intel-10-Zeus-Tracker--Drop-Zones.bro.dat
critical-stack-intel-110-volexity.com-Wekby-Adobe-Flash-Exploit-IOCs.bro.dat
critical-stack-intel-112-morphick.com-BernhardPOS-IOCs.bro.dat
critical-stack-intel-11-Zeus-Tracker--Binaries.bro.dat
critical-stack-intel-12-abuse.ch-SSL-Hash-Blacklist.bro.dat
critical-stack-intel-13-Palevo--Domain-Block-List.bro.dat
critical-stack-intel-14-Palevo--IP-Block-List.bro.dat
critical-stack-intel-15-Zeus-Tracker--Domain-Block-List.bro.dat
critical-stack-intel-18-PhishTank-Intel-Feed-(Verified).bro.dat
critical-stack-intel-19-Abuse-Reporting-and-Blacklisting.bro.dat
critical-stack-intel-1-Matsnu-Botnet-(Master-Feed).bro.dat
critical-stack-intel-20-DShield-Domain-List-(Low-Sev).bro.dat
critical-stack-intel-21-DShield-Domain-List-(High-Sev).bro.dat
critical-stack-intel-22-DShield-Domain-List-(Medium-Sev).bro.dat
critical-stack-intel-23-Malware-Domains.bro.dat
critical-stack-intel-24-Scam-Domains-(Fake-Malware-Drive-By).bro.dat
critical-stack-intel-25-ET--Known-Compromised-Hosts.bro.dat
critical-stack-intel-26-C-Cs-Domains.bro.dat
critical-stack-intel-27-IP-Bad-Reputation-(Mail).bro.dat
critical-stack-intel-29-IP-Bad-Reputation-(Scan).bro.dat
critical-stack-intel-2-C-Cs-IP-List.bro.dat
critical-stack-intel-30-Ponmocup--Botnet-Domains.bro.dat
critical-stack-intel-31-Ponmocup--Malware-IPs.bro.dat
critical-stack-intel-32-Ponmocup--Botnet-IPs.bro.dat
critical-stack-intel-34-Bebloh--IP-List.bro.dat
critical-stack-intel-35-Bebloh--Domain-List.bro.dat
critical-stack-intel-36-Dyre--IP-List.bro.dat
critical-stack-intel-37-Cryptowall--Domain-List.bro.dat
critical-stack-intel-39-Cryptowall--IP-List.bro.dat
```

Thursday, July 23, 15

Here we see the feeds after downloading via the API, they include the malwaredomainlist, tor project exit node list Team Cymru's PoSeidon IOCs, Zeus Tracker, DShield, known Scam Domains, known compromised hosts and the CryptoWall domain and IP lists

Feed Content (CryptoWall Malware)

- CryptoWall Ransomware Domains
  - `# cd /opt/critical-stack/frameworks/intel/.cache; cat critical-stack-intel-37-Cryptowall--Domain-List.bro.dat`

```
#fields  indicator indicator_type  meta.source
adolfforua.com  Intel::DOMAIN   http://example.com/feeds/
cryptowall-domlist.txt
babamamama.com  Intel::DOMAIN   http://example.com/feeds/
cryptowall-domlist.txt
craspatsp.com   Intel::DOMAIN   http://example.com/feeds/
cryptowall-domlist.txt
crynigermike.com        Intel::DOMAIN   http://example.com/
feeds/cryptowall-domlist.txt
```

Let’s take a look at what these files look like, opening them is as easy as reading a text file. As compared to the much more complex XML and Schema Definitions of CybOX & STIX

This is a the feed content for a small portion of the CryptoWall Ransomware Domains

Feed Content (PoSeidon Malware)

- Point of Sale system malware
- PoSeidon Domains
  - **# cd /opt/critical-stack/frameworks/intel/.cache; cat critical-stack-intel-106-team-cymru.org-Poseidon-IOCs.bro.dat**

```
#fields  indicator indicator_type  meta.source
askyourspace.com/ldl01aef/viewtopic.php Intel::URL
https://example.com/link
46.30.41.159    Intel::ADDR     https://blog.team-cymru.org/
46.166.168.106  Intel::ADDR     https://blog.team-cymru.org/
164af045a08d718372dd6ecd34b746e7032127b1
Intel::FILE_HASH       https://blog.team-cymru.org/
d5ac494c02f47d79742b55bb9826363f1c5a656c
Intel::FILE_HASH       https://blog.team-cymru.org/
```

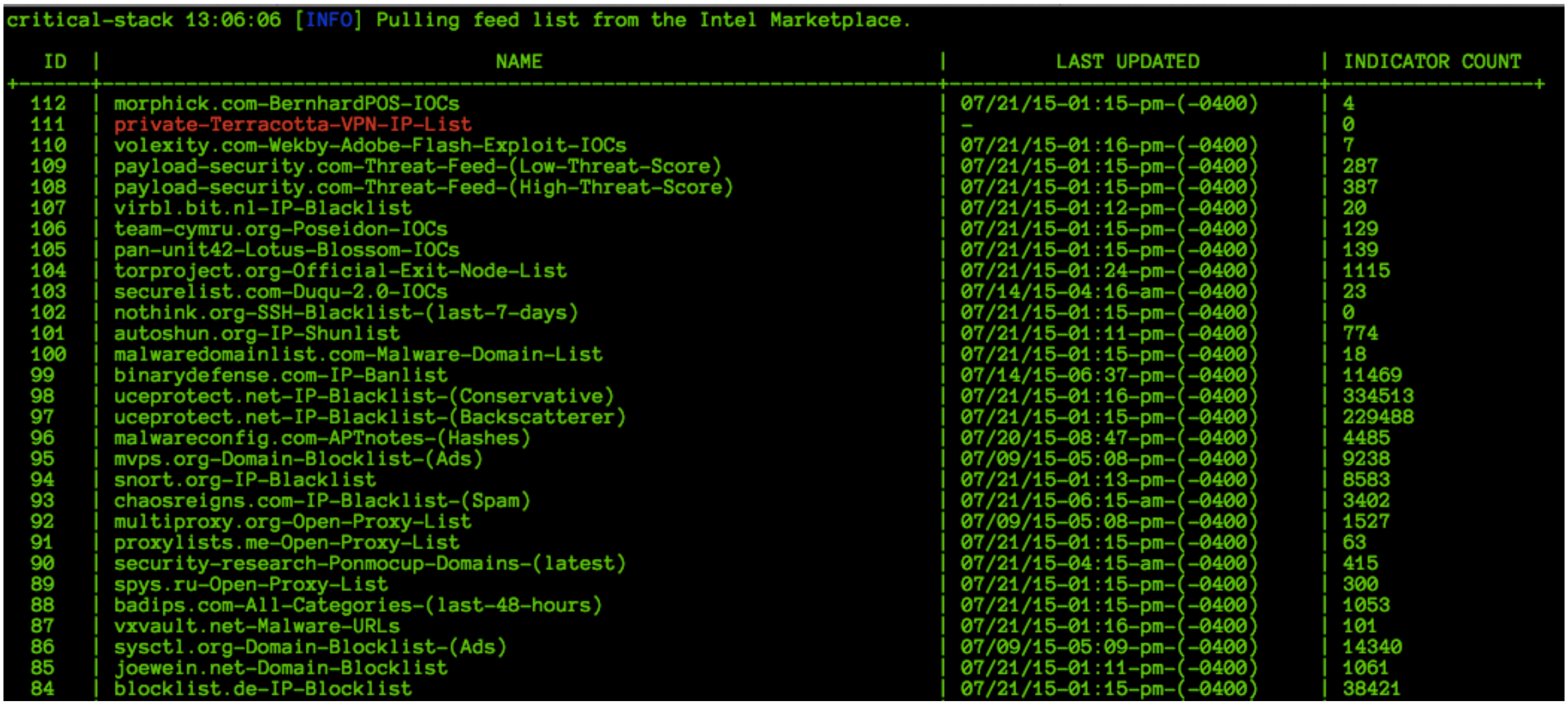
This is a portion of the PoSeidon domains

As you can see, this formatting is a bit less detailed than the CybOX and STIX formats, just the bare necessities to load into bro

critical-stack-intel list

After loading into Bro, you can use the critical-stack-intel client to list your subscribed feeds

critical-stack-intel list



```
critical-stack 13:06:06 [INFO] Pulling feed list from the Intel Marketplace.

   ID  |                            NAME                                   |              LAST UPDATED           | INDICATOR COUNT
+------+-------------------------------------------------------------------+-------------------------------------+-----------------+
  112  | morphick.com-BernhardPOS-IOCs                                     | 07/21/15-01:15-pm-(-0400)           | 4
  111  | private-Terracotta-VPN-IP-List                                    | -                                   | 0
  110  | volexity.com-Wekby-Adobe-Flash-Exploit-IOCs                       | 07/21/15-01:16-pm-(-0400)           | 7
  109  | payload-security.com-Threat-Feed-(Low-Threat-Score)               | 07/21/15-01:15-pm-(-0400)           | 287
  108  | payload-security.com-Threat-Feed-(High-Threat-Score)              | 07/21/15-01:15-pm-(-0400)           | 387
  107  | virbl.bit.nl-IP-Blacklist                                         | 07/21/15-01:12-pm-(-0400)           | 20
  106  | team-cymru.org-Poseidon-IOCs                                      | 07/21/15-01:15-pm-(-0400)           | 129
  105  | pan-unit42-Lotus-Blossom-IOCs                                     | 07/21/15-01:15-pm-(-0400)           | 139
  104  | torproject.org-Official-Exit-Node-List                            | 07/21/15-01:24-pm-(-0400)           | 1115
  103  | securelist.com-Duqu-2.0-IOCs                                      | 07/14/15-04:16-am-(-0400)           | 23
  102  | nothink.org-SSH-Blacklist-(last-7-days)                           | 07/21/15-01:15-pm-(-0400)           | 0
  101  | autoshun.org-IP-Shunlist                                          | 07/21/15-01:11-pm-(-0400)           | 774
  100  | malwaredomainlist.com-Malware-Domain-List                         | 07/21/15-01:15-pm-(-0400)           | 18
  99   | binarydefense.com-IP-Banlist                                      | 07/14/15-06:37-pm-(-0400)           | 11469
  98   | uceprotect.net-IP-Blacklist-(Conservative)                        | 07/21/15-01:16-pm-(-0400)           | 334513
  97   | uceprotect.net-IP-Blacklist-(Backscatterer)                       | 07/21/15-01:15-pm-(-0400)           | 229488
  96   | malwareconfig.com-APTnotes-(Hashes)                               | 07/20/15-08:47-pm-(-0400)           | 4485
  95   | mvps.org-Domain-Blocklist-(Ads)                                   | 07/09/15-05:08-pm-(-0400)           | 9238
  94   | snort.org-IP-Blacklist                                            | 07/21/15-01:13-pm-(-0400)           | 8583
  93   | chaosreigns.com-IP-Blacklist-(Spam)                               | 07/21/15-06:15-am-(-0400)           | 3402
  92   | multiproxy.org-Open-Proxy-List                                    | 07/09/15-05:08-pm-(-0400)           | 1527
  91   | proxylists.me-Open-Proxy-List                                     | 07/21/15-01:15-pm-(-0400)           | 63
  90   | security-research-Ponmocup-Domains-(latest)                       | 07/21/15-04:15-am-(-0400)           | 415
  89   | spys.ru-Open-Proxy-List                                           | 07/21/15-01:15-pm-(-0400)           | 300
  88   | badips.com-All-Categories-(last-48-hours)                         | 07/21/15-01:15-pm-(-0400)           | 1053
  87   | vxvault.net-Malware-URLs                                          | 07/21/15-01:16-pm-(-0400)           | 101
  86   | sysctl.org-Domain-Blocklist-(Ads)                                 | 07/09/15-05:09-pm-(-0400)           | 14340
  85   | joewein.net-Domain-Blocklist                                      | 07/21/15-01:11-pm-(-0400)           | 1061
  84   | blocklist.de-IP-Blocklist                                         | 07/21/15-01:15-pm-(-0400)           | 38421
```

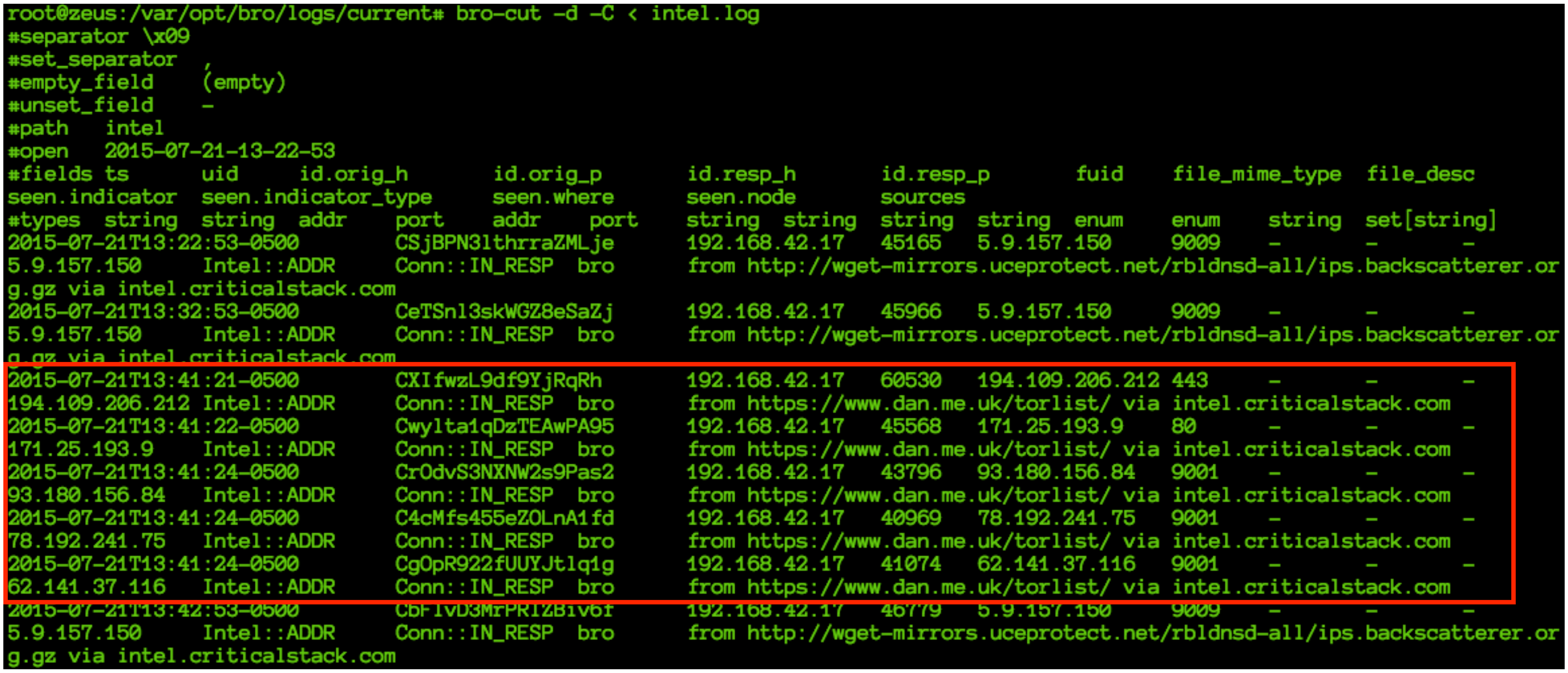
Thursday, July 23, 15

Here we see a similar breakdown as before of the associated names with the feeds and how many indicators are being tracked

bro-cut -d -C < intel.log

Now that we’ve got them loaded and verified the indicators, let’s generate some TOR traffic and see what matches!

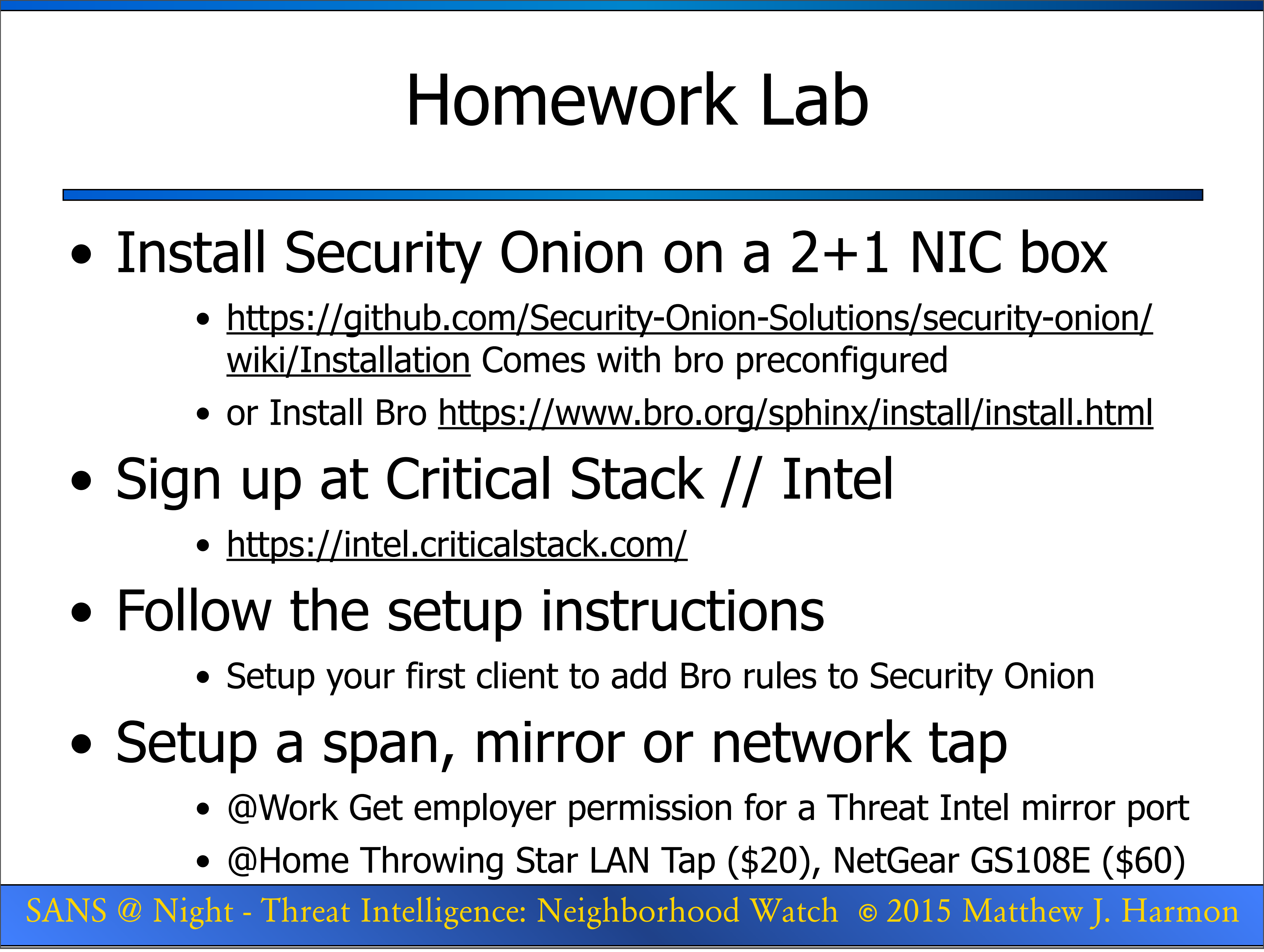
bro-cut -d -C < intel.log



```
root@zeus:/var/opt/bro/logs/current# bro-cut -d -C < intel.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   intel
#open   2015-07-21-13-22-53
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       fuid    file_mime_type  file_desc
seen.indicator  seen.indicator_type     seen.where      seen.node       sources
#types  string  string  addr    port    addr    port    string  string  string  string  enum    enum    string  set[string]
2015-07-21T13:22:53-0500        CSjBPN3lthrraZMLje      192.168.42.17   45165   5.9.157.150     9009    -       -       -
5.9.157.150     Intel::ADDR     Conn::IN_RESP   bro     from http://wget-mirrors.uceprotect.net/rbldnsd-all/ips.backscatterer.or
g.gz via intel.criticalstack.com
2015-07-21T13:32:53-0500        CeTSnl3skWGZ8eSaZj      192.168.42.17   45966   5.9.157.150     9009    -       -       -
5.9.157.150     Intel::ADDR     Conn::IN_RESP   bro     from http://wget-mirrors.uceprotect.net/rbldnsd-all/ips.backscatterer.or
g.gz via intel.criticalstack.com
2015-07-21T13:41:21-0500        CXIfwzL9df9YjRqRh       192.168.42.17   60530   194.109.206.212 443     -       -       -
194.109.206.212 Intel::ADDR     Conn::IN_RESP   bro     from https://www.dan.me.uk/torlist/ via intel.criticalstack.com
2015-07-21T13:41:22-0500        Cwylta1qDzTEAwPA95      192.168.42.17   45568   171.25.193.9    80      -       -       -
171.25.193.9    Intel::ADDR     Conn::IN_RESP   bro     from https://www.dan.me.uk/torlist/ via intel.criticalstack.com
2015-07-21T13:41:24-0500        CrOdvS3NXNW2s9Pas2      192.168.42.17   43796   93.180.156.84   9001    -       -       -
93.180.156.84   Intel::ADDR     Conn::IN_RESP   bro     from https://www.dan.me.uk/torlist/ via intel.criticalstack.com
2015-07-21T13:41:24-0500        C4cMfs455eZOLnA1fd      192.168.42.17   40969   78.192.241.75   9001    -       -       -
78.192.241.75   Intel::ADDR     Conn::IN_RESP   bro     from https://www.dan.me.uk/torlist/ via intel.criticalstack.com
2015-07-21T13:41:24-0500        CgOpR922fUUYJtlq1g      192.168.42.17   41074   62.141.37.116   9001    -       -       -
62.141.37.116   Intel::ADDR     Conn::IN_RESP   bro     from https://www.dan.me.uk/torlist/ via intel.criticalstack.com
2015-07-21T13:42:53-0500        CbFlvD3MrPRIZB1v6f      192.168.42.17   46779   5.9.157.150     9009    -       -       -
5.9.157.150     Intel::ADDR     Conn::IN_RESP   bro     from http://wget-mirrors.uceprotect.net/rbldnsd-all/ips.backscatterer.or
g.gz via intel.criticalstack.com
```

-d = time values human readable
-C = include all headers

We can see five connects to known TOR exit nodes and a hostile domains we visited



Homework Lab

- Install Security Onion on a 2+1 NIC box
  - https://github.com/Security-Onion-Solutions/security-onion/wiki/Installation Comes with bro preconfigured
  - or Install Bro https://www.bro.org/sphinx/install/install.html
- Sign up at Critical Stack // Intel
  - https://intel.criticalstack.com/
- Follow the setup instructions
  - Setup your first client to add Bro rules to Security Onion
- Setup a span, mirror or network tap
  - @Work Get employer permission for a Threat Intel mirror port
  - @Home Throwing Star LAN Tap ($20), NetGear GS108E ($60)

Thursday, July 23, 15

I hope that this overview of Threat Intelligence, including the components of ThreatConnect and CriticalStack Intel was useful for you. As a final item, in order to tie all of this together I highly recommend this Homework Lab

As we don’t have time for a lab today in our short session, I’ve put together a quick Homework Lab for you!

First, install Bro manually or install Security Onion on a system. If you’re doing a real threat intel box, get a 2+1 NIC: one port for ingress, one for egress and one for management

Sign up at Critical Stack, it’s quick and easy

Follow the client setup instructions at Critical Stack, subscribe to some feeds, and load the client and those feeds into your Bro instance

If you’re doing this at work, get your employers permission to setup a passive mirror port for network traffic and explore the wonders of Bro and Security Onion with your Threat Intel feeds!

If at home, get a throwing star LAN tap or a cheap gigabit switch that supports a port mirror - the NetGear GS108E is relatively inexpensive (around $60) and comes with the Port Mirror capability!

Thank you!

Homework Lab, Resources & Links:

http://bit.ly/SANSMpls2015MJH

mjh@itys.net

I’ve posted the Homework Lab in addition to many additional resources and links mentioned in this slide to a Google Spreadsheet, you can find that at:

http:// bit . ly / SANSMpls2015MJH

Or scan the QR Code