Cyber Security Summit 2015

Threat Intelligence 101: Introduction and Foundations

Matthew J. Harmon
IT Risk Limited, LLC

Matthew J. Harmon

- IT Risk Limited, Principal Consultant
  - DFIR, Pen Testing, Risk Management, IT Audit
- SANS Instructor (401, 464, 504)
  - Security Essentials, Hacker Tools, Techniques, Exploits & Incident Handling), and Hacker Guard, IT Operations Baselining
  - GSEC, GCIH, GCIA, CISSP
- NorSec ISAO, Working Board Member
  - Information Sharing Analysis Organization

What are we going to cover today?

- 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

It could be worse... BUT

Source: PBS Sesame Street, Oscar the Grouch

Breaches are inevitable - against a motivated attacker

...with time and resources

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

but it doesn’t take a super genius

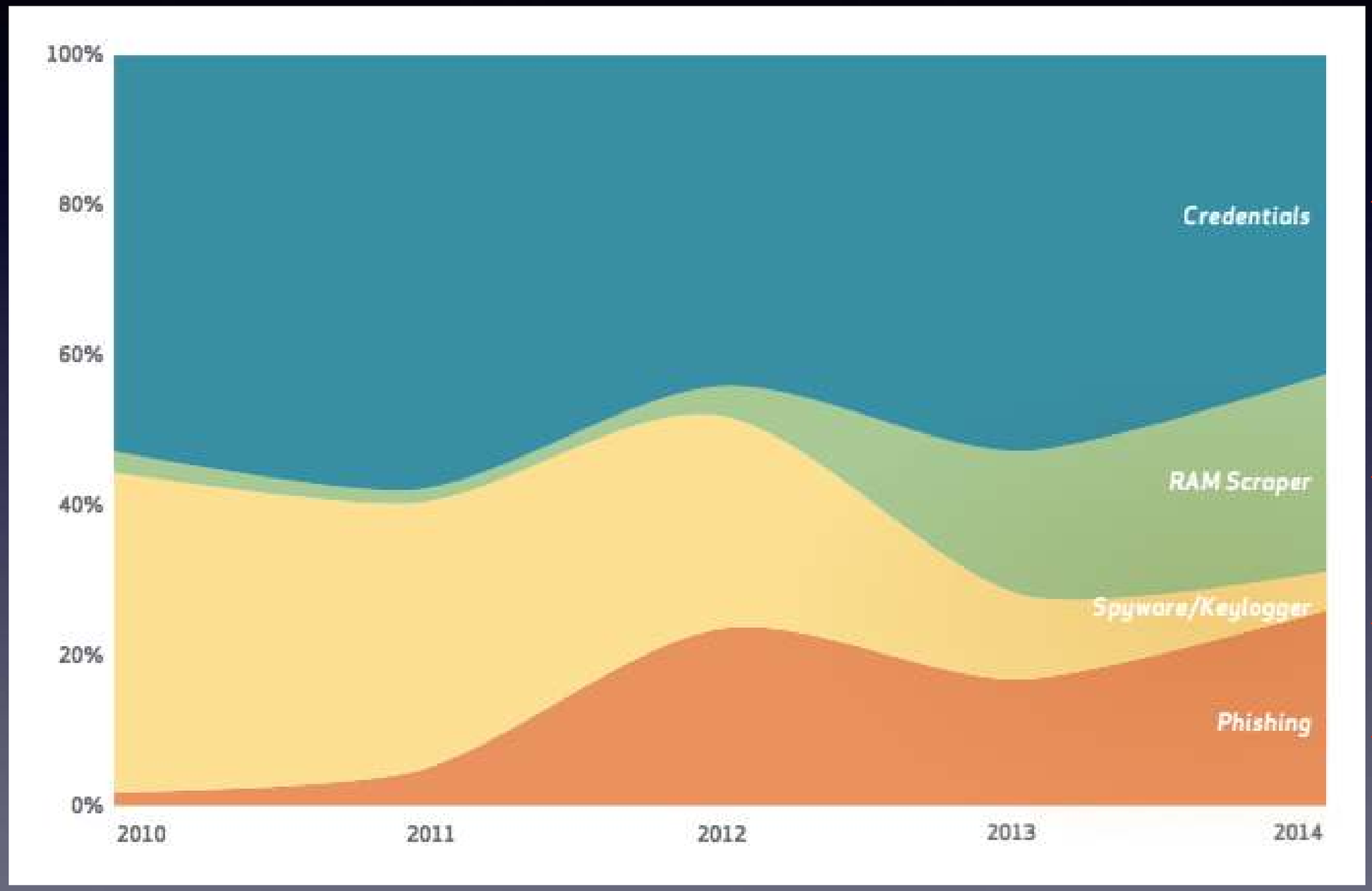
but it doesn't take a super genius

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

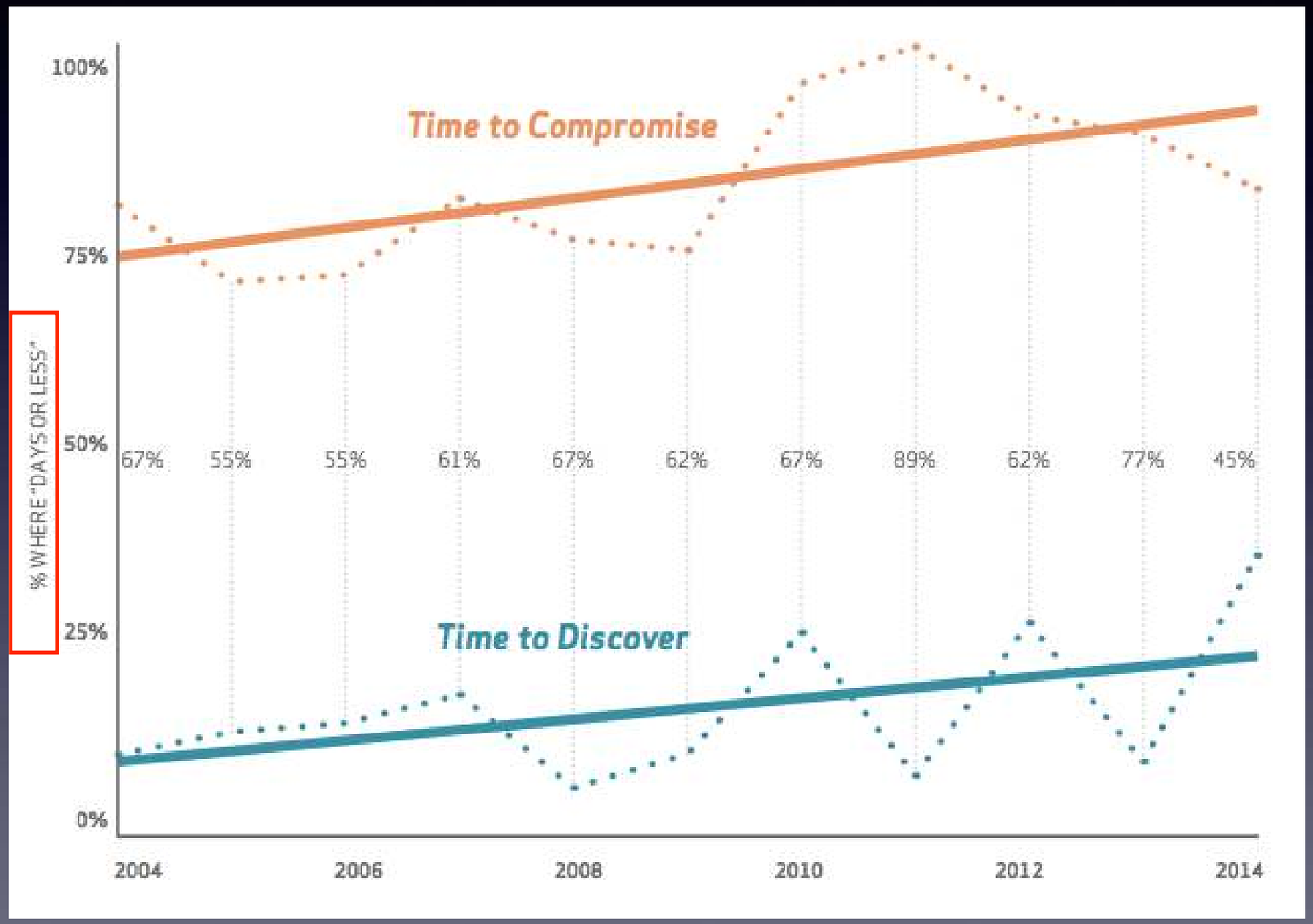
Source: Verizon 2015 Data Breach Investigations Report

Attack Vectors: 2014



Source: Verizon 2015 Data Breach Investigations Report

Time to Discover: 2014



Source: Verizon 2015 Data Breach Investigations Report

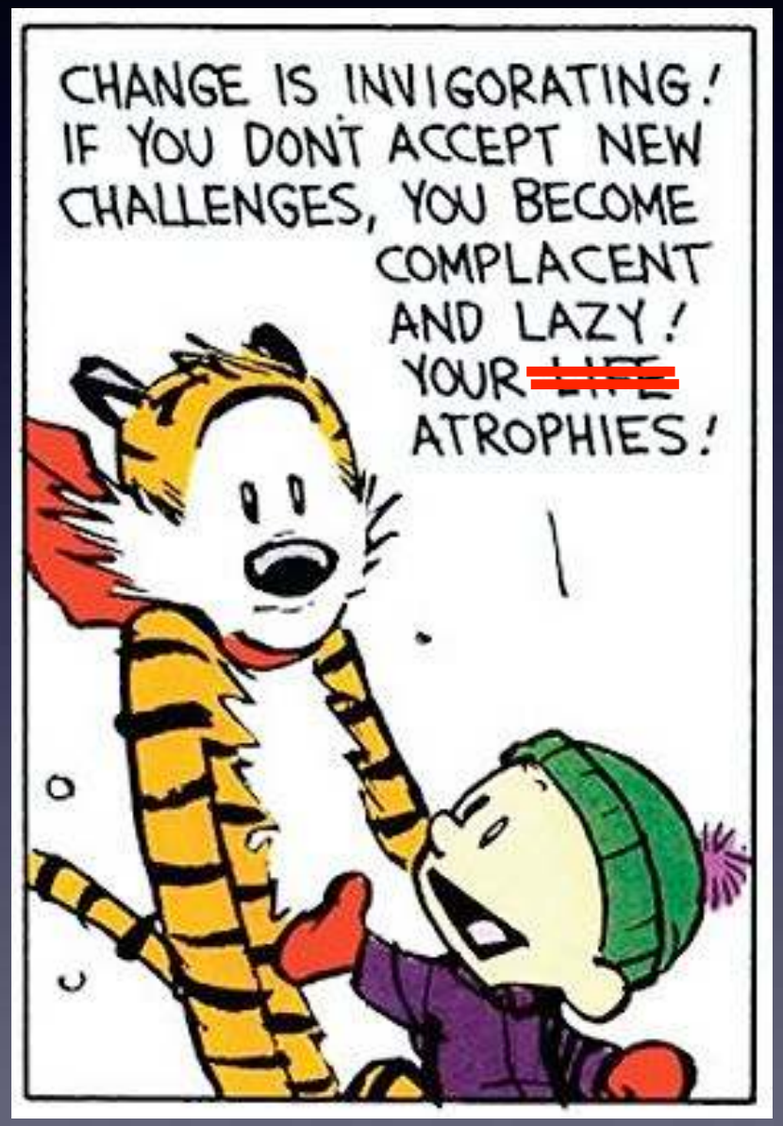
Latest Breaches - Summary

100 Banks, 30 Countries $1B fraudulent transfers (2yrs)
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++
Experian - 15 Million T-Mobile Customers (One file!)
JP Morgan Chase 76 mil houses + 7 mil businesses
... and many, many more.

We really need to get better at this

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

Change is good, Sharing is good



Network

Source: Calvin and Hobbes by Bill Watterson (1995)

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

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

How to share our information?

- Many indicators, 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
    - <u>Structured Threat Information</u>
    - Trusted Automated exchange of Indicator Information
  - Tab Separated Values (Critical Stack + Bro)

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)

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

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

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)

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

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.

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">Indicators - Phishing</stix:Package_Intent>
- </stix:STIX_Header>

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>5d6cbd0a557bb10603bb63b8fe0c4160</c
yboxCommon:Simple_Hash_Value>
<indicator:Indicated_TTP>
<stixCommon:TTP xsi:type="TTP:TTPType">
<TTP:Description>Phishing<TTP:Description></TTP:Attack_Pattern>
```

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">Indicators - 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>
```

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>
```

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>
```

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"/>
```

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-
```

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!

Let's look at some live data.

ThreatConnect Common Community
Demo

Known Adversaries (ThreatConnect)

INDICATORS | ACTIVITY | DOCUMENTS | THREATS | TAGS | ADVERSARIES | VICTIMS | WORKFLOW

Filter

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) 10 1 2

Hacking Team

DETAILS PIVOT

Description:

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

Type: Adversary

Owner: Common Com munity

Added: 02-13-2014

Tags: Advanced Persistent Threat

Indicators of Compromise (ThreatConnect)

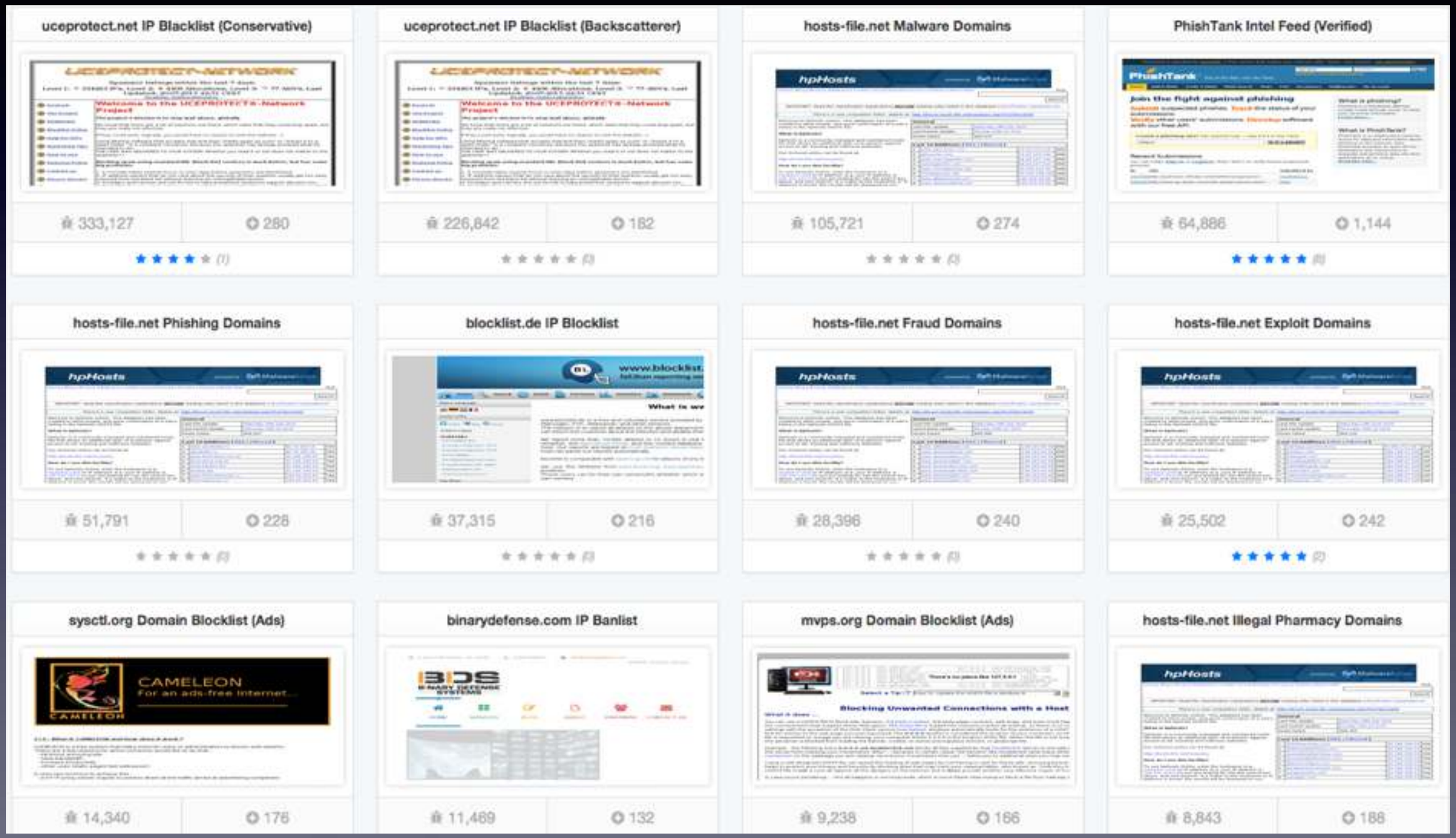
INDICATORS | ACTIVITY | DOCUMENTS | THREATS | TAGS | ADVERSARIES | VICTIMS | WORKFLOW

Filter

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

Feeds (CriticalStack // Intel)



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

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
```

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
```

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/
```

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
```

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        CSjBPN31thrraZMLje      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        CeTSnl3skWGZ8eSaZi      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        CbFlvD3MrPRIZBiv6f      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
```

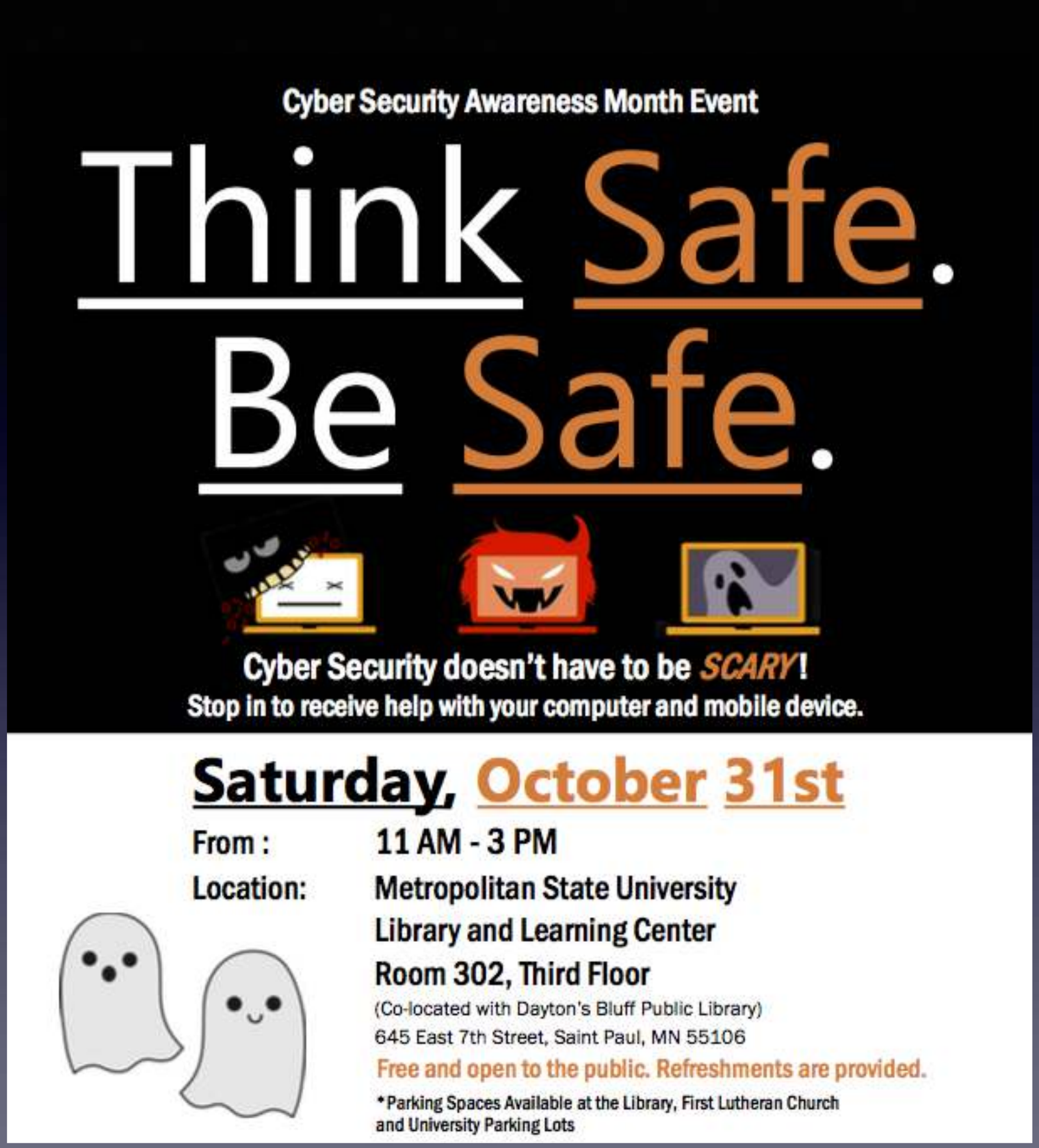
-d = time values human readable

-C = include all headers

Prototyping with Raspberry Pi 2

Want to participate in NorSec?

We need Alpha Testers and First Members
Email us:
info@norsec.org



Contact Matt Weikert at
cv0856mf@metrostate.edu

Chris Crayne at
cz0362yv@metrostate.edu.

Lab

- Install Security Onion
  - 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
  - @Home Throwing Star LAN Tap, NetGear GS108E ($60)

Thank you!

Lab, Resources & Links
http://bit.ly/CSS2015ThreatIntel101

matthew@itriskltd.com