

SANS @ Night

Threat Intelligence: Neighborhood Watch for your Networks & Why Baselining Matters

Wednesday, 20 July 2016 (7:15-8:15)

Matthew J. Harmon
GSEC, GCIH, GCIA, CISSP

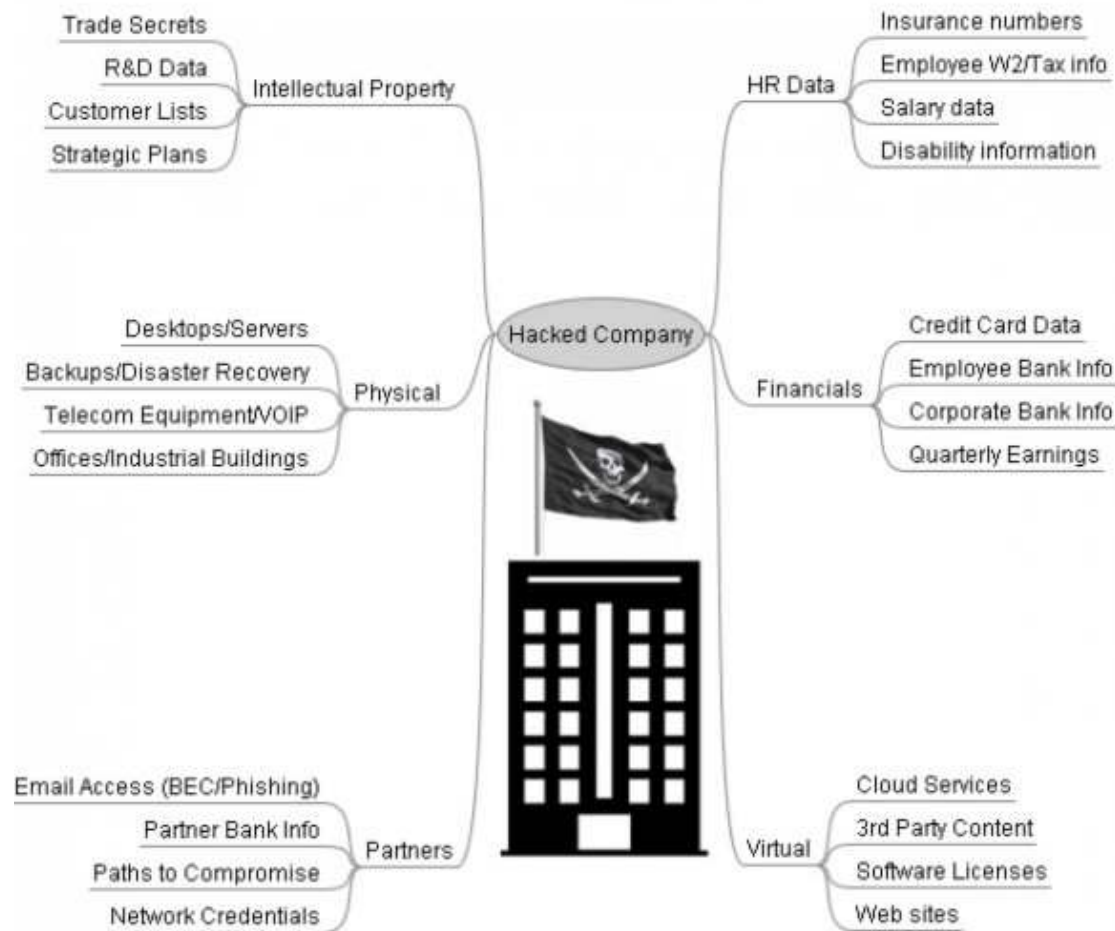
Matthew J. Harmon

- IT Risk Limited, Principal Consultant
 - DFIR, Pen Testing, GRC & Risk Management
- NorSec Foundation, Co-Founder & CTO
 - Information Sharing Analysis Organization (ISAO)
 - “Securing the Internet of Everything” Not for Profit
 - We are looking for alpha/beta testers! Contact me.
- SANS Community & Mentor Instructor
 - Security 401 (Security Essentials), 504 (Hacker Tools, Techniques, Exploits & Incident Handling), 464 (Hacker Guard, IT Operations Baselining)

What are we going to cover tonight?

- State of Cyber Security
 - Short overview of where we are today
- Discuss “What is Threat Intelligence?”
 - Discuss the 15 Axioms of Traditional Intelligence
 - Explain CybOX, STIX & TAXII
 - Real world example structuring CybOX & STIX
- Show three Threat Intelligence exchanges
 - Threat Connect, Critical Stack, YARA
- Show you How to Do It Yourself
 - Lab with Security Onion, Bro, PRADS, and Critical Stack

Reminder: What we're protecting



Source: Team Cymru

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



Year Decade of the big breaches

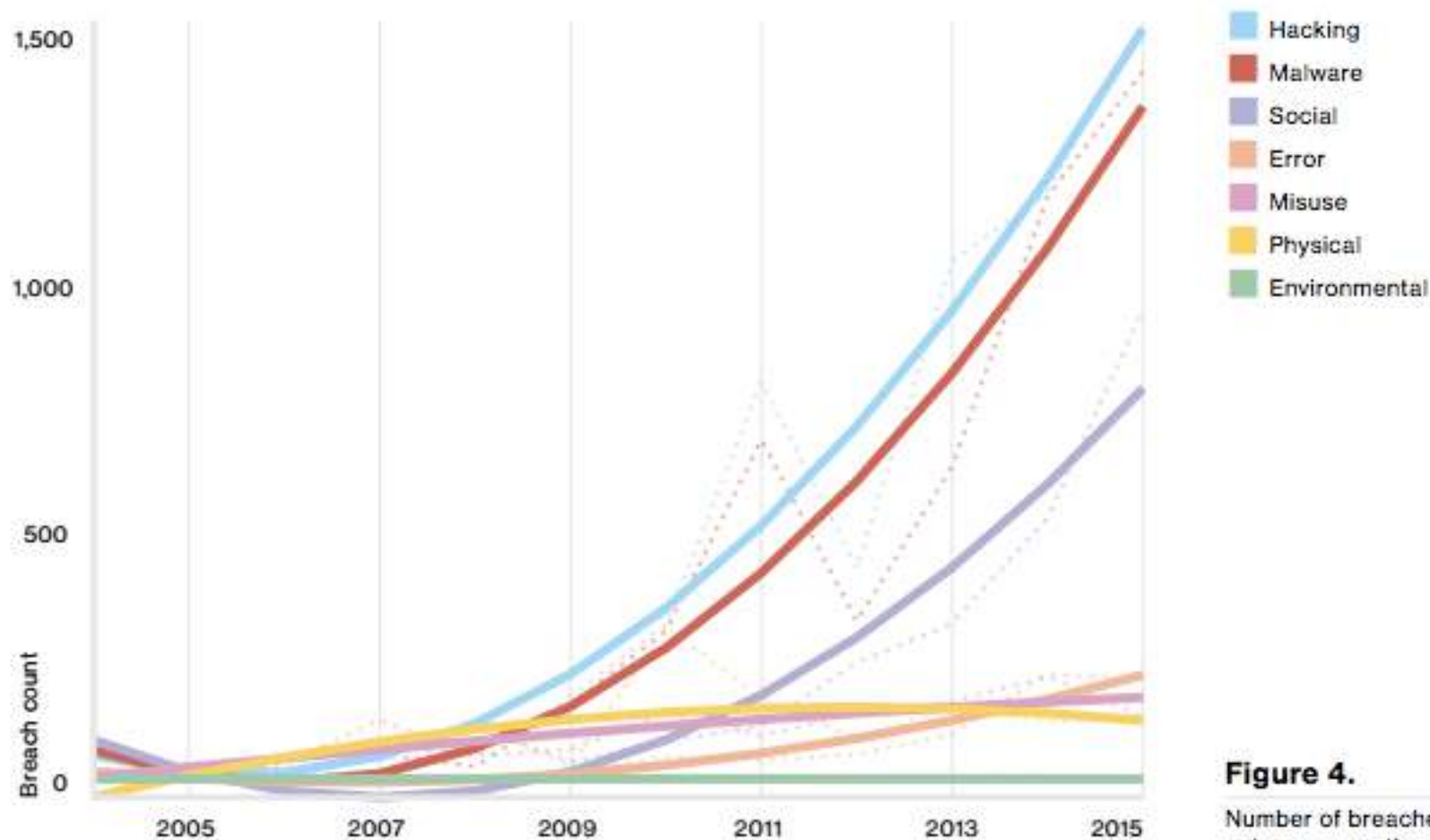


Figure 4.

Number of breaches per threat action category over time, (n=9,009)

Source: Verizon 2016 Data Breach Investigations Report

Attack Vectors: 2016

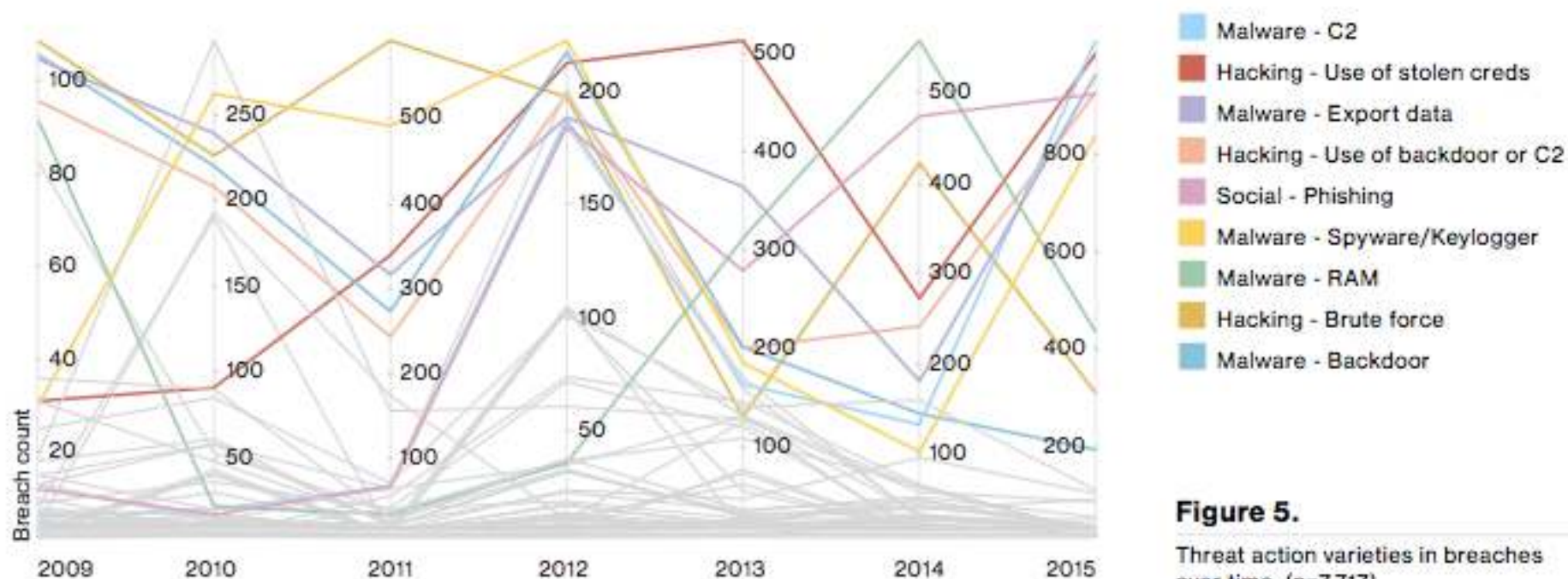


Figure 5.

Threat action varieties in breaches over time, (n=7,717)

Source: Verizon 2016 Data Breach Investigations Report

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)

Sometimes you win the moon shot



Apollo 11 landed 47 years
ago 20 July 1969 20:18 UTC

Photo: NASA "One giant leap for mankind" (Neil Armstrong, Buzz Aldrin [Footprint], Michael Collins [hat tip])

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
 - “ISAO’s”
- Similar to ISAC’s and Cyber Fusion Centers
 - not siloed by sector or industry
- No more re-discovering the same attacks
- Anyone can participate at ISAO.org

Just getting started (ISAO.org)

- ISAO Startup (WG1)
- ISAO Capabilities (WG2)
- Cybersecurity-Related Information Sharing Guidelines (WG3)
- Privacy & Security (WG4)
- ISAO Support Intake Process (WG5)
- Government Programs, Relations and Services to Assist ISAO's (WG6)
- All at v0.2 for document output

Traditional Intelligence - 15 Axioms

- Believe in your own professional judgments.
- Be aggressive, and do not fear being wrong.
- It is better to be mistaken than to be wrong.
- Avoid mirror imaging at all costs.
- Intelligence is of no value if it is not disseminated.
- Coordination is necessary, but do not settle for the least common denominator.

Source: Central Intelligence Agency "Fifteen Axioms for Intelligence Analysts" Tradecraft 2000

Traditional Intelligence - 15 Axioms

- When everyone agrees on an issue, something probably is wrong
- The consumer does not care how much you know, just tell him what is important.
- Form is never more important than substance.
- Aggressively pursue collection of information you need.

Source: Central Intelligence Agency "Fifteen Axioms for Intelligence Analysts" Tradecraft 2000

Traditional Intelligence - 15 Axioms

- Do not take the editing process too seriously.
- Know your Community counterparts and talk to them frequently.
- Never let your career take precedence over your job.
- Being an intelligence analyst is not a popularity contest.
- Do not take your job-or yourself-too seriously.

Source: Central Intelligence Agency "Fifteen Axioms for Intelligence Analysts" Tradecraft 2000

What is Threat Intelligence?

Indicators of Compromise
(IoC's)

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

+

Relevant Threat Activity
(Exchanges)

Campaigns
Malware
Known Adversaries
Situational Awareness
Baselining

=

Crowd Sourced Actionable Cyber Threat
Intelligence Vetted by Expert Analysts with
Local Validation

How to share our information?

- Unvetted IoCs are low confidence (1)
- Live attacks and campaigns are high (5)
- How do we share information? Some examples:
 - Yara (YAML like exchange of malfeasance sigs)
 - XML Based (CybOX, STIX & TAXII, OpenIOC)
 - Cyber Observables
 - Structured Threat Information
 - Trusted Automated exchange of Indicator Information
 - Open IOC (Indicators of Compromise)
 - Tab Separated Values (Critical Stack + Bro)

Yara Signatures

- Yara-Rules
 - https://github.com/Yara-Rules/rules/blob/master/CVE_Rules/CVE-2015-2426.yar

```
31 rule Exploit_MS15_077_078_HackingTeam: Exploit {
32     meta:
33         description = "MS15-078 / MS15-077 exploit - Hacking Team code"
34         author = "Florian Roth"
35         date = "2015-07-21"
36         super_rule = 1
37         hash1 = "ad6bb982a1ecfe080baf0a2b27950f989c107949b1cf02b6e0907f1a568ece15"
38         hash2 = "fc609adef44b5c64de029b2b2cff22a6f36b6bdf9463c1bd320a522ed39de5d9"
39     strings:
40         $s1 = "\\SystemRoot\\system32\\CI.dll" fullword ascii /* PESTudio Blacklist: strings */
41         $s2 = "\\sysnative\\CI.dll" fullword ascii /* PESTudio Blacklist: strings */
42         $s3 = "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/"
43         $s4 = "CRTDLL.DLL" fullword ascii
44         $s5 = "\\sysnative" fullword ascii /* PESTudio Blacklist: strings */
45         $s6 = "InternetOpenA coolio, trying open %s" fullword ascii
46     condition:
47         uint16(0) == 0x5a4d and filesize < 2500KB and all of them
48 }
```

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)

This is continually evolving...

- STIX Specification v2.0 Draft 1
 - Released Monday, July 18th 2016
 - <https://lists.oasis-open.org/archives/cti/201607/msg00051.html>

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">Indic  
ators - 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>5d6cbd0a557bb10603bb63
b8fe0c4160</cyboxCommon: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">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>
```

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>
```

OpenIOC

- Lead by Mandiant
- XML + XML Schema Definition
- <https://github.com/STIXProject/openioc-to-stix>

```
<Indicator operator="OR" id="3cfe6f4c-3276-4e8b-88d5-9b53665da358">
  <IndicatorItem id="0a704ede-840d-4075-a508-3ee5744c332f" condition="is">
    <Context document="DriverItem" search="DriverItem/DeviceItem/DeviceName" type="mir"/>
    <Content type="string">{3093AAZ3-1092-2929-9391}</Content>
  </IndicatorItem>
  <IndicatorItem id="09900e0b-8219-43dc-930b-fabf5324da4e" condition="is">
    <Context document="DriverItem" search="DriverItem/DeviceItem/DeviceName" type="mir"/>
    <Content type="string">{624409B3-4CEF-41C0-8B81-7634279A41E5}</Content>
  </IndicatorItem>
</Indicator>
</Indicator>
<Indicator operator="AND" id="d0f65908-5ala-4936-98e0-cf98ba51037e">
  <IndicatorItem id="b38d3a14-3839-4c62-ae38-3ff48b720add" condition="contains">
    <Context document="RegistryItem" search="RegistryItem/Path" type="mir"/>
    <Content type="string">
      HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
    </Content>
  </IndicatorItem>
  <IndicatorItem id="e415d391-871f-44b9-8fd3-70967644d36f">
    <IndicatorItem id="bcf49307-8362-4f05-998c-a8dd629dbb7d" condition="is">
      <Context document="RegistryItem" search="RegistryItem/ValueName" type="mir"/>
      <Content type="string">CF1D</Content>
    </IndicatorItem>
  </IndicatorItem>
</Indicator>
```

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
 - Many Feeds, easy to read Tab Separated Values, easy client integration with Bro!

Known Adversaries (ThreatConnect)

The screenshot displays the ThreatConnect interface with a top navigation bar containing icons for Indicators, Activity, Documents, Threats, Tags, Adversaries (selected), Victims, and Workflow. Below the navigation bar is a search filter. The main content area shows a table of known adversaries. The 'Hacking Team' entry is highlighted, and a details panel is open on the right.

Name	Owner	Date Added
Song Yubo	Common Community	02-27-2015
l fe	Common Community	11-18-2014
john.felder@hotmail.com	Common Community	09-30-2014
tommy.bluber1234321@ddd.com	Common Community	09-30-2014
Li Ning	Common Community	04-18-2014
Hacking Team	Common Community	02-13-2014
Sergoy Tarasov	Common Community	01-21-2014
Jack White	Common Community	01-02-2014
rootert	Common Community	12-20-2013
Wang Zhong Yun	Common Community	12-11-2013

Details for Hacking Team:

Hacking Team

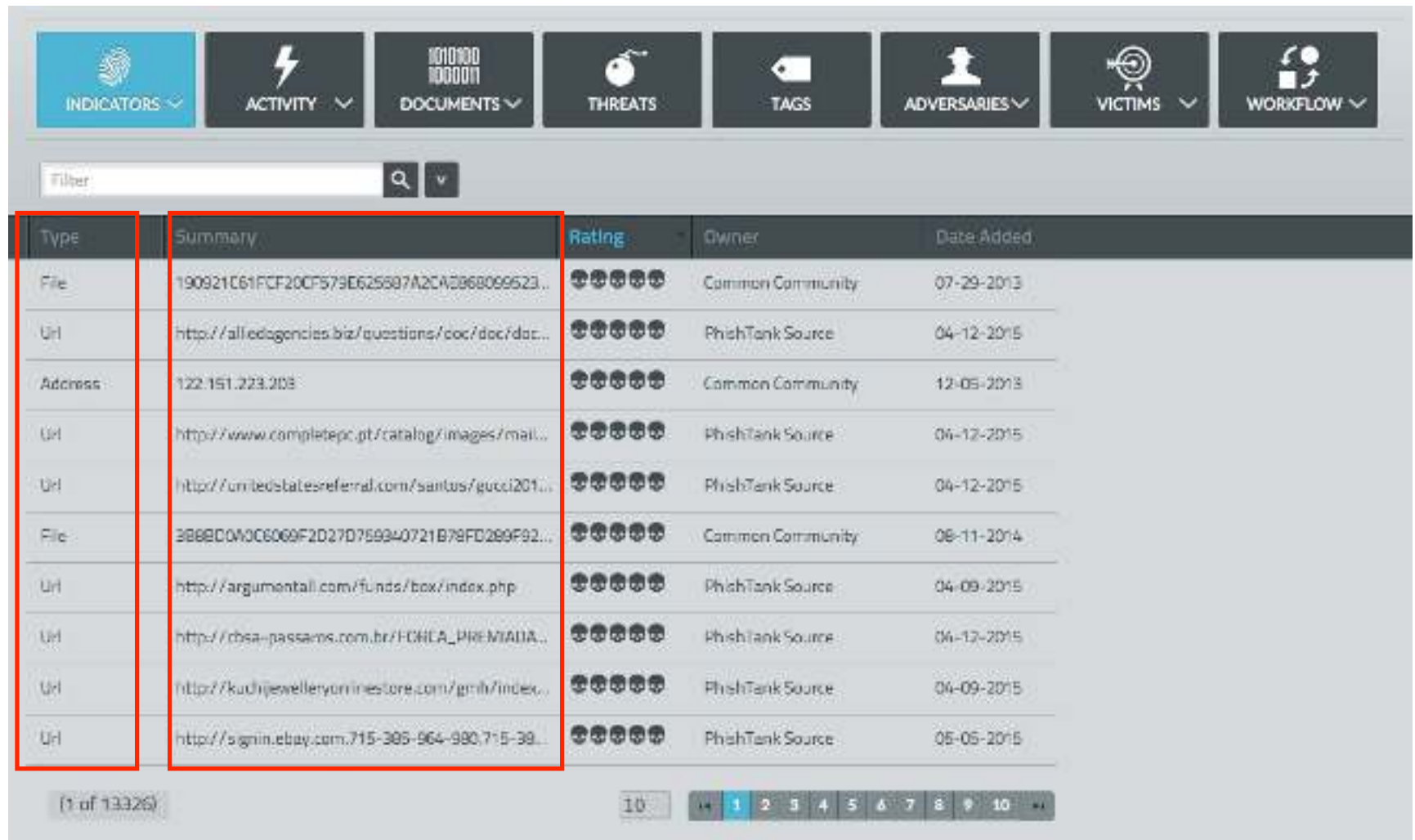
[DETAILS](#) [PIVOT](#)

Description:
Hacking Team, also known as H.T.S.R.I, 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

Indicators of Compromise (ThreatConnect)















The screenshot displays the ThreatConnect Indicators interface. At the top, there is a navigation bar with icons and labels for INDICATORS, ACTIVITY, DOCUMENTS, THREATS, TAGS, ADVERSARIES, VICTIMS, and WORKFLOW. Below this is a search bar labeled 'Filter'. The main content area is a table with the following columns: Type, Summary, Rating, Owner, and Date Added. A red box highlights the first 10 rows of the table. The table shows various indicators, including files, URLs, and addresses, with their respective ratings and owners.

Type	Summary	Rating	Owner	Date Added
File	190921C61FCF20CF573E625697A2CA0868099523...	★★★★★	Common Community	07-29-2013
Url	http://alliedgenies.biz/questions/coc/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/santus/gucci201...	★★★★★	PhishTank Source	04-12-2015
File	368ED0A0C6069F2D27D759340721B78FD269F92...	★★★★★	Common Community	08-11-2014
Url	http://argumentall.com/funds/box/index.php	★★★★★	PhishTank Source	04-09-2015
Url	http://cbsa-passaros.com.br/FCNLA_PREMIADA...	★★★★★	PhishTank Source	04-12-2015
Url	http://kudijewelleryonlinestore.com/gnfr/index...	★★★★★	PhishTank Source	04-09-2015
Url	http://signin.ebay.com.715-385-964-980.715-39...	★★★★★	PhishTank Source	05-05-2015

(1 of 13326)

10 1 2 3 4 5 6 7 8 9 10

Feeds (CriticalStack // Intel)

<p>uceprotect.net IP Blacklist (Conservative)</p>  <p>★ 333,127 ⌚ 280</p> <p>★★★★★ (7)</p>	<p>uceprotect.net IP Blacklist (Backscatterer)</p>  <p>★ 226,842 ⌚ 182</p> <p>★★★★★ (7)</p>	<p>hosts-file.net Malware Domains</p>  <p>★ 105,721 ⌚ 274</p> <p>★★★★★ (7)</p>	<p>PhishTank Intel Feed (Verified)</p>  <p>★ 64,886 ⌚ 1,144</p> <p>★★★★★ (7)</p>
<p>hosts-file.net Phishing Domains</p>  <p>★ 51,791 ⌚ 228</p> <p>★★★★★ (7)</p>	<p>blocklist.de IP Blocklist</p>  <p>★ 37,315 ⌚ 216</p> <p>★★★★★ (7)</p>	<p>hosts-file.net Fraud Domains</p>  <p>★ 28,396 ⌚ 240</p> <p>★★★★★ (7)</p>	<p>hosts-file.net Exploit Domains</p>  <p>★ 25,502 ⌚ 242</p> <p>★★★★★ (7)</p>
<p>sysctl.org Domain Blocklist (Ads)</p>  <p>★ 14,340 ⌚ 176</p> <p>★★★★★ (7)</p>	<p>binarydefense.com IP Banlist</p>  <p>★ 11,469 ⌚ 132</p> <p>★★★★★ (7)</p>	<p>mvps.org Domain Blocklist (Ads)</p>  <p>★ 9,238 ⌚ 166</p> <p>★★★★★ (7)</p>	<p>hosts-file.net Illegal Pharmacy Domains</p>  <p>★ 8,843 ⌚ 188</p> <p>★★★★★ (7)</p>

Bro for parsing full packet captures

- 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

Critical Stack 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-110-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  | vxxvault.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-Blacklist                            | 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 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/rbl/dnsd-all/ips.backscatterer.org
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/rbl/dnsd-all/ips.backscatterer.org
g.gz via intel.criticalstack.com
2015-07-21T13:41:21-0500 CXIfwxL9df9YjRqRh 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 CgOpR922fUUYJtlqig 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 CBFivX3MfPR1ZBivbf 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/rbl/dnsd-all/ips.backscatterer.org
g.gz via intel.criticalstack.com
```

-d = time values human readable

-C = include all headers

# SGUIL Analysis

RealTime Events | Enabled Events

| ET | ENT | Source      | Alert ID | IP             | SPort | Dest IP        | DPort | Pt | Event Message                                                               |
|----|-----|-------------|----------|----------------|-------|----------------|-------|----|-----------------------------------------------------------------------------|
| ET | 1   | doug-wrt... | 3.1114   | 192.168.23.129 | 1066  | 58.51.91.107   | 80    | 5  | ET CURRENT_EVENTS Possible Bad Bot Exploit Kit Single Character JAR Request |
| ET | 1   | doug-wrt... | 3.1115   | 108.23.129     | 1064  | 58.53.91.102   | 80    | 6  | ET MALWARE Possible Malicious Applet Access (justexploit kit)               |
| ET | 11  | doug-wrt... | 3.1117   | 58.51.102      | 80    | 192.168.23.129 | 1064  | 5  | ET JMRD JAVA - Java Archive Download by Vulnerable Client                   |
| ET | 2   | doug-wrt... | 3.1128   | 58.51.102      | 80    | 192.168.23.129 | 1066  | 5  | ET POLICY PE EXE or DLL Windows file download                               |
| ET | 27  | doug-wrt... | 3.1130   | 58.51.102      | 80    | 192.168.23.129 | 1067  | 6  | ET INFO EXE - Served Inline HTTP                                            |
| ET | 14  | doug-wrt... | 3.1144   | 58.51.102      | 80    | 192.168.23.129 | 1067  | 5  | ET POLICY Java EXE Download                                                 |
| ET | 14  | doug-wrt... | 3.1158   | 58.51.102      | 80    | 192.168.23.129 | 1067  | 6  | ET TROJAN Java EXE Download by Vulnerable Version - Likely Driveby          |
| ET | 1   | doug-wrt... | 3.1185   | 192.168.23.129 | 1069  | 212.252.32.20  | 80    | 5  | ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)          |
| ET | 1   | doug-wrt... | 3.1185   | 192.168.23.129 | 1069  | 212.252.32.20  | 80    | 5  | ET TROJAN SpyEye Bot Checkin                                                |
| ET | 1   | doug-wrt... | 3.1187   | 108.23.129     | 1069  | 212.252.32.20  | 80    | 6  | ET TROJAN SpyEye C&C Check in URI                                           |
| ET | 1   | doug-wrt... | 3.1188   | 192.168.23.129 | 1069  | 212.252.32.20  | 80    | 5  | ET TROJAN Bamke (PWS/InfoStealer) HTTP GET Checkin                          |
| ET | 2   | doug-wrt... | 3.1189   | 10.10.10       | 4444  | 10.10.10.70    | 1096  | 6  | ET POLICY PE EXE or DLL Windows file download                               |
| ET | 4   | doug-wrt... | 3.1190   | 10.10.10       | 4444  | 10.10.10.70    | 1096  | 5  | ET SHELLCODE Possible Call with No Offset TOP shellcode                     |
| ET | 2   | doug-wrt... | 3.1191   | 10.10.10       | 4444  | 10.10.10.70    | 1096  | 5  | GRE SHAPI CODE x86/x64 NOP                                                  |
| ET | 1   | doug-wrt... | 3.1197   | 172.16.150.20  | 1294  | 66.32.119.38   | 80    | 6  | ET INFO Executable Download from dotted quad Host                           |
| ET | 1   | doug-wrt... | 3.1198   | 172.16.150.20  | 1294  | 66.32.119.38   | 80    | 5  | ET POLICY SUSPICIOUS *.doc.exe in HTTP URL                                  |
| ET | 1   | doug-wrt... | 3.1199   | 66.32.119.38   | 80    | 172.16.150.20  | 1294  | 6  | ET POLICY PE EXE or DLL Windows file download                               |

IP Resolution | Agent Status | Sensor Statistics | System Maps | User Maps

| Sl | Net | Hostname | Type | Last     | Status |
|----|-----|----------|------|----------|--------|
| 1  |     |          |      | 15:10:15 | UP     |
| 2  |     |          |      | 15:00:25 | UP     |
| 3  |     |          |      | 15:11:45 | UP     |
| 4  |     |          |      | 15:11:47 | UP     |
| 5  |     |          |      | 15:12:11 | UP     |
| 6  |     |          |      | 15:11:45 | UP     |

Update Interval (secs): 15 NOW

Show Packet Data | Show Rule

Alert top SHOME\_NET any > EXTERNAL\_NET \$HTTP\_PORTS (msg:"ET POLICY SUSPICIOUS \*.doc.exe in HTTP URL"; flowto\_server,established; content:".doc.exe", http\_uri; nocase; dsstype:bad unknown; sid:2013475; rev:1)

| IP            | Source IP    | Dest IP | Src | Len | Prot | Seq  | Win | Flags | Offset | TTL   | Checksum |
|---------------|--------------|---------|-----|-----|------|------|-----|-------|--------|-------|----------|
| 172.16.150.20 | 66.32.119.38 | 4       | 5   | 0   | 378  | 8716 | 2   | 0     | 128    | 50326 |          |

U A P R S F

| Source | Dest | R R R C S S Y I | Seq #     | Adj #    | Offset | Rec Window | Urp   | Checksum |
|--------|------|-----------------|-----------|----------|--------|------------|-------|----------|
| Port   | Port | T O D K H I N N |           |          |        |            |       |          |
| 1794   | 80   |                 | 257060136 | 95006116 | 5      | 0          | 12500 | 0        |

DATA

|                                                 |                   |
|-------------------------------------------------|-------------------|
| 47 45 54 20 2f 74 69 62 65 22 73 2f 42 73 61 6f | GET /images/brand |
| 64 5f 6f 49 5e 67 65 2f 64 69 61 67 6f 5f 73 74 | donImage/brand    |
| 69 63 73 2f 73 77 69 5e 67 70 60 65 63 58 61 6f | ica/wing-mechan   |
| 69 63 73 2f 64 6f 63 2f 65 70 64 20 40 54 56 56 | ica.doc.exe HTTP  |
| 2f 31 2f 31 00 04 41 63 63 65 70 70 3a 20 69 6f | /1.1...Accept: im |
| 61 67 65 2f 67 69 66 20 20 69 60 61 67 65 2f 70 | age/gif, image/x  |
| 70 78 65 69 74 65 61 70 2f 70 66 65 61 67 65 70 | -shman; source/   |

Search Packet Payload | Dec | Text | NoCase

Source: Doug Burks of Security Onion Solutions

# PRADS for Baselining

---

```
Example
prads -i eth0 -l prads.log
```

If you run the prads service, the assets it sees will be dumped into /var/log/prads.log and look like this:

```
10.43.2.181,0,54354,6,SYN,[65535:64:1:64:M1460,N,W2,N,N,T,S,E,E:P:MacOS:iPhone OS 3.1.3
(UC) ethernet/modem:uptime:1574hrs],0,1300882012
10.43.2.181,0,0,0,ARP (Apple),C8:BC:C8:48:65:CA,0,1300882017
```

This information can be further processed, inserted into an SQL database etc.

the general format fo this data is:

```
asset,vlan,port,proto,service,[service-info],distance,discovered
```

```
asset = The ip address of the asset.
vlan = The virtual lan tag of the asset.
port = The port number of the detected service.
proto = The protocol number of the matching fingerprint.
service = The "Service" detected, like: TCP-SERVICE, UDP-SERVICE, SYN, SYNACK,MAC,.....
service-info = The fingerprint that the match was done on, with info.
distance = Distance based on guessed initial TTL (service = SYN/SYNACK)
discovered = The timestamp when the data was collected
```

May it sniff your network for a while and you will be able to do anomaly detection.

Source: Edward Fjellskål (<https://github.com/gamelinux/prads>)



# LOKI for IOC Checking

```
LOKI

Simple IOC Scanner

(C) Florian Roth - BSK Consulting GmbH
Jan 2015
Version 0.2

DISCLAIMER - USE AT YOUR OWN RISK

[INFO] LOKI - Starting Loki Scan on PROMETHEUS
[INFO] File Name Characteristics initialized with 32 regex patterns
[INFO] Malware Hashes initialized with 43 hashes
[INFO] False Positive Hashes initialized with 8 hashes
[INFO] Scanning C:\ ...
-[ALERT] Malware Hash TYPE: SHA256 HASH: b12c7d57507286bbbe36d7acf9b34c22
c96606ffd904e3c23008399a4a50c047 FILE: C:\$Recycle.Bin\S-1-5-21-949666807
-3097873-177000209-1000\src7v2pz.sys DESC: Regin Malware Sample
[ALERT] Yara Rule MATCH: Regin_APT_KernelDriver_Generic_B FILE: C:\$Recyc
le.Bin\S-1-5-21-949666807-3097873-177000209-1000\src7v2pz.sys
```

Source: Florian Roth (<https://github.com/Neo23x0/Loki>)

# LOKI for IOC Checking

---

Loki currently includes the following IOCs:

- Equation Group Malware (Hashes, Yara Rules by Kaspersky and 10 custom rules generated by us)
- Carbanak APT - Kaspersky Report (Hashes, Filename IOCs - no service detection and Yara rules)
- Arid Viper APT - Trendmicro (Hashes)
- Anthem APT Deep Panda Signatures (not officialy confirmed) (krebsonsecurity.com - see Blog Post)
- Regin Malware (GCHQ / NSA / FiveEyes) (incl. Legspin and Hopscotch)
- More than 180 hack tool Yara rules - Source: APT Scanner THOR
- More than 600 web shell Yara rules - Source: APT Scanner THOR
- Numerous suspicious file name regex signatures - Source: APT Scanner THOR
- Much more ..

Source: Florian Roth (<https://github.com/Neo23x0/Loki>)

# Getting Started

---

- Threat Intel is pointless without baselining
- Explore the Intelligence Axioms
- You must know what is correct before you can detect deviations
- Bro and PRADS for baselining and asset identification
- SGUIL for alert analysis
- LOKI for IOC detection
- Doug Burks' Security Onion makes it easy

# Now what? Do it yourself!





# How to Do It Yourself

---

- Install Security Onion on a 2+1 NIC box
  - <https://github.com/Security-Onion-Solutions/security-onion/wiki/Installation> Comes with bro & prads preconfigured
- Sign up at Critical Stack // Intel
  - <https://intel.criticalstack.com/>
- Follow the setup instructions
  - Setup your first client to add Bro and Yara rules to Security Onion
- Setup a span, mirror or network tap
  - NetGear GS108E (\$60) + RaspberryPi or better
- Bonus: Document every authorized device to win!

# Thank you!

---

Email for a copy of the slides and/or to get involved  
with the NorSec Foundation ISAO Program



Full Contact Details



matthew@itriskltd.com