Network Intrusions and Detection. Cloud?

Vladimir Kropotov, Fyodor Yarochkin
ISGC 2017

Affiliations: Academia Sinica, o0o.nu, chroot.org

March 5/2017, Taipei
OUTLINE

Introduction

Detection Techniques and Tools

EOF
Overview

Introduction

Detection Techniques and Tools

EOF
Everyone gets compromised :)

Safe Browsing
Diagnostic page for google.com

What is the current listing status for google.com?
This site is not currently listed as suspicious.

Part of this site was listed for suspicious activity 77 time(s) over the past 90 days.

What happened when Google visited this site?
Of the 438781 pages we tested on the site over the past 90 days, 1603 page(s) resulted in malicious softw
last time Google visited this site was on 2014-05-18, and the last time suspicious content was found on th
Malicious software includes 546 trojan(s), 185 exploit(s), 105 scripting exploit(s). Successful infection resu
Malicious software is hosted on 230 domain(s), including bissnes.org/, webevangelista.blogspot.com/, fyw
234 domain(s) appear to be functioning as intermediaries for distributing malware to visitors of this site, inc
webevangelista.com/.

This site was hosted on 4 network(s) including AS15169 (GOOGLE), AS36040 (YOUTUBE), AS43515 (YO

Has this site acted as an intermediary resulting in further distribution of malware?
Over the past 90 days, google.com appeared to function as an intermediary for the infection of 63 site(s) ir
CHALLENGES

Main Assumption: All networks are compromised
The difference between a good security team and a bad security team is that with a bad security team you will never know that you’ve been compromised.
Cloud security
Cloud Security = Sever Security
▶ some issues could be cloud specific
THREAT LANDSCAPE WITH CLOUD

Server security plus more!

- issues in cloud hosting software
- issues in hypervisor/virtualization software
- issues with using shared system
- issues with using shared IP addresses

and more
Cloud: headache for forensic examiners

Several Polish banks hacked, information stolen by unknown attackers

badcyber / February 3, 2017 / Crime, Investigation / banking, malware, Poland
**Why is it a problem?**

```
www.eye-watch.in. IN A 54.204.17.89
www.eye-watch.in. IN A 23.23.104.162
www.eye-watch.in. IN A 23.21.237.3
www.eye-watch.in. IN A 50.16.223.43
www.eye-watch.in. IN A 23.21.237.3
www.eye-watch.in. IN A 50.16.223.43
www.eye-watch.in. IN A 107.20.190.149
www.eye-watch.in. IN A 23.21.237.3
www.eye-watch.in. IN A 50.19.231.17
www.eye-watch.in. IN A 23.21.237.3
www.eye-watch.in. IN A 107.20.190.149
www.eye-watch.in. IN A 23.21.251.12
www.eye-watch.in. IN A 54.221.226.150
www.eye-watch.in. IN A 23.23.163.122
www.eye-watch.in. IN A 50.19.215.86
www.eye-watch.in. IN A 23.23.194.85
www.eye-watch.in. IN A 54.225.70.157
www.eye-watch.in. IN A 50.16.240.106
www.eye-watch.in. IN A 107.21.242.98
www.eye-watch.in. IN A 54.204.38.131
www.eye-watch.in. IN A 54.243.79.224
www.eye-watch.in. IN A 54.225.70.157
www.eye-watch.in. IN A 54.243.234.197
www.eye-watch.in. IN A 54.225.70.157
www.eye-watch.in. IN A 75.101.145.157
www.eye-watch.in. IN A 54.225.94.231
www.eye-watch.in. IN A 54.225.158.177
```
Your site matters!

File information

- Identification
- Details
- Content
- Analyses
- Submissions
- ITW
- Behaviour
- Comments

URL: http://120.113.173.207:8080/View.jsp?action=BaseUrl&u=12817620835722
TYPE: POST
USER AGENT: WinHttpClient

URL: http://120.113.173.207:8080/View.jsp?action=What&u=12817620835722
TYPE: GET
USER AGENT: WinHttpClient

TCP connections
120.113.173.207:8080

UDP communications
MACHINE DNS SERVER 50
ANOTHER ASPECT OF THE CLOUD

lots of machines :)}
Botnet guys invented cloud :) 

- about 40,000,000 internet users in Russia
- for every 10,000 server hosts 500 hosts trigger redirects to malicious content per week
- about 20-50 user machines (full AV installed, NAT, FW) get affected
ACADEMIC NETWORKS

- past few months - a number of breaches
- Academic Networks tend to have trust relationships: exploited by attackers
- lots of experimental gear
Overview

Introduction

Detection Techniques and Tools

EOF
Good thing to assume

If you are under attack, your AV, Firewalls, IDS, are in THE ATTACKER THREATS MODEL. The option you have - read between the lines. When you are compromised, what is the action plan?
Some Useful tools

Developed by us:

- http://github.com/fygrave/ndf
- http://github.com/fygrave/hntp

3rd party:

- fiddler
- elasticsearch && http://github.com/aol/moloch
- yara
- hpfeeds https://github.com/rep/hpfeeds
- IntelMQ https://github.com/certtools/intelmq
- https://github.com/STIXProject/ - openioc-to-stix converter
- https://github.com/MISP/MISP - malware information sharing platform. Also helpful for incident tracking
Introduction: terminology

Indicators of Compromise

Indicator of compromise (IOC) in computer forensics is an artifact observed on network or in operating system that with high confidence indicates a computer intrusion.

**Why Indicators of compromise**

Indicators of Compromise help us to answer questions like:

- is this document/file/hash malicious?
- is there any past history for this IP/domain?
- what are the other similar/related domains/hashes/..?
- who is the actor?
- am I an APT target?!;-)
An Example

A Network compromise case study:

- Attackers broke via a web vuln.
- Attackers gained local admin access
- Attackers created a local user
- Attackers started probing other machines for default user ids
- Attackers launched tunneling tools – connecting back to C2
- Attackers installed RATs to maintain access
Indicators

So what are the compromise indicators here?

- Where did attackers come from? (IP)
- What vulnerability was exploited? (pattern)
- What web backdoor was used? (pattern, hash)
- What tools were uploaded? (hashes)
- What users were created locally? (username)
- What usernames were probed on other machines
## Good or Bad?

<table>
<thead>
<tr>
<th>File Name</th>
<th>RasTls.exe</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Size</td>
<td>105 kB</td>
</tr>
<tr>
<td>File Modification Date/Time</td>
<td>2009:02:09 19:42:05+08:00</td>
</tr>
<tr>
<td>File Type</td>
<td>Win32 EXE</td>
</tr>
<tr>
<td>MIME Type</td>
<td>application/octet−stream</td>
</tr>
<tr>
<td>Machine Type</td>
<td>Intel 386 or later, and compatibles</td>
</tr>
<tr>
<td>Time Stamp</td>
<td>2009:02:02 13:38:37+08:00</td>
</tr>
<tr>
<td>PE Type</td>
<td>PE32</td>
</tr>
<tr>
<td>Linker Version</td>
<td>8.0</td>
</tr>
<tr>
<td>Code Size</td>
<td>49152</td>
</tr>
<tr>
<td>Initialized Data Size</td>
<td>57344</td>
</tr>
<tr>
<td>Uninitialized Data Size</td>
<td>0</td>
</tr>
<tr>
<td>Entry Point</td>
<td>0x3d76</td>
</tr>
<tr>
<td>OS Version</td>
<td>4.0</td>
</tr>
<tr>
<td>Image Version</td>
<td>0.0</td>
</tr>
<tr>
<td>Subsystem Version</td>
<td>4.0</td>
</tr>
<tr>
<td>Subsystem</td>
<td>Windows GUI</td>
</tr>
<tr>
<td>File Version Number</td>
<td>11.0.4010.7</td>
</tr>
<tr>
<td>Product Version Number</td>
<td>11.0.4010.7</td>
</tr>
<tr>
<td>File OS</td>
<td>Windows NT 32−bit</td>
</tr>
<tr>
<td>Object File Type</td>
<td>Executable application</td>
</tr>
<tr>
<td>Language Code</td>
<td>English (U.S.)</td>
</tr>
<tr>
<td>Character Set</td>
<td>Windows, Latin1</td>
</tr>
<tr>
<td>Company Name</td>
<td>Symantec Corporation</td>
</tr>
<tr>
<td>File Description</td>
<td>Symantec 802.1x Supplicant</td>
</tr>
<tr>
<td>File Version</td>
<td>11.0.4010.7</td>
</tr>
<tr>
<td>Internal Name</td>
<td>dot1xtray</td>
</tr>
</tbody>
</table>
**IT REALLY DEPENDS ON CONTEXT**

RasTls.DLL
RasTls.DLL.msc
RasTls.exe


_Dynamic-Link Library Search Order_
IOC representations

Multiple standards have been created to facilitate IOC exchanges.

- Madiant: OpenIOC
- Mitre: STIX (Structured Threat Information Expression), CyBOX (CyberObservable Expression)
- Mitre: CAPEC, TAXII
- IODEF (Incident Object Description Format)
**STANDARDS: OpenIOC**

OpenIOC - Mandiant-backed effort for uniform representation of IOC (now FireEye) http://www.openioc.org/

```xml
<loc id="6d2a1b03-b216-4cd8-9a9e-8827af6ebf93" last-modified="2011-10-28T19:28:20">
    <short_description>Zeus</short_description>
    <description>Finds Zeus variants, twexts, sdra64, ntos</description>
    <keywords/>
    <authored_by>Mandiant</authored_by>
    <authored_date>0001-01-01T00:00:00</authored_date>
    <links/>
</loc>

--<indicator operator="OR" id="9c8df971-32a8-4ede-8a3a-c5cb2c1439c6">
    --<indicator operator="AND" id="0781258f-6960-4da5-97a0-ec35fb403cac">
        --<indicatorItem id="50455b63-35bf-4ef3-9f06-aea2980f80a" condition="contains">
            <context document="ProcessItem" search="ProcessItem/name" type="mir"/>
            <content type="string">winlogon.exe</content>
        </indicatorItem>
    </indicator>
    --<indicatorItem id="b05db40-0526-461f-9721-e31d5651abdc" condition="contains">
        <context document="ProcessItem" search="ProcessItem/HandleList/Handle/Type" type="mir"/>
        <content type="string">File</content>
    </indicatorItem>
    --<indicatorItem id="6755775-6577-43b2-bccd-74603223180a">
        --<indicatorItem id="c5ae706f-c032-4da7-8acd-4523f1dae9f6" condition="contains">
            <context document="ProcessItem" search="ProcessItem/HandleList/Handle/Name" type="mir"/>
            <content type="string">system32\sdra64.exe</content>
        </indicatorItem>
    </indicator>
    --<indicatorItem id="25f12a7-665b-4e45-8b0f-6e5ca7b95801" condition="contains">
        <context document="ProcessItem" search="ProcessItem/HandleList/Handle/Name" type="mir"/>
        <content type="string">system32\twain_32\user.ds</content>
    </indicatorItem>
    --<indicatorItem id="feaa1706-9ebe-469b-b30a-4047cfb7436b" condition="contains">
        <context document="ProcessItem" search="ProcessItem/HandleList/Handle/Type" type="mir"/>
        <content type="string">\WINDOWS\system32\twext.exe</content>
    </indicatorItem>
</indicator>
```
Open IOCs

Digital Appendices/Appendix G (Digital) – IOCs$ ls
0c7c902c–67f8–479c–9f44–4d985106365a.ioc
ad521068–6f18–4ab1–899c–11007a18ec73.ioc
12a40bf7–4834–49b0–a419–6abb5fe2b291.ioc
af5f65fc–e1ca–45db–88b1–6ccb7191ee6a.ioc
2106f0d2–a260–4277–90ab–edd3455e31fa.ioc
Appendix G IOCs README.pdf
26213db6–9d3b–4a39–abebe73656acb913e.ioc
c32b8af3–28d0–47d3–801f–a2c2b0129650.ioc
2bf223f–9e46–47a7–ac35–d35f8138a4c7.ioc
c71b3305–85e5–4d51–b07c–ff227181fb5a.ioc
2fc55747–6822–41d2–bccc1–387fc1b2e67b.ioc
c7fa2ea5–36d5–4a52–a6cf–ddc2257cb6f9.ioc
32b168e6–dbd6–4d56–ba2f–734553239efe.ioc
d14d5f09–9050–4769–b00d–30fce9e6eb85.ioc
3433dad8–879e–40d9–98b3–92ddc75f0dcd.ioc
d1c65316–cddd–4d9c–8efe–c539aa5965c0.ioc
3e01b786–fe3a–4228–95fa–c3986e2353d6.ioc
d4f103f8–c372–49d1–b9f4–e127d61d0639.ioc
6bd24113–2922–4d25
70b5be0c–8a94–44b4
7c739d52–c669–4d51
7d2eaadfa5ff–4199
7f9a6986–f00a–4071
806beff3–7395–492e
84f04df2–25cd–4f59
8695bb5e–29cd–41b9
86e9b8ec–7413–453b
STANDARDS: MITRE

Mitre CybOX: `http://cybox.mitre.org/`
`https://github.com/CybOXProject/Tools`
`https://github.com/CybOXProject/openioc-to-cybox`

Mitre CAPEC: `http://capec.mitre.org/`

Mitre STIX: `http://stix.mitre.org/`

Mitre TAXII `http://taxii.mitre.org/`
Mature: stix

STIX™ is a collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information. The STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible. All interested parties are welcome to participate in evolving STIX as part of its open, collaborative community.

Trusted Automated exchange of Indicator Information (TAXII™) is the main transport mechanism for cyber threat information represented as STIX. Through the use of TAXII services, organizations can share cyber threat information in a secure and automated manner.

Related Efforts
- Cyber Observables (CybOX)
- Malware (MAEC)
- Attack Patterns (CAPEC)

STIX Version 1.1.1 is an update release of the STIX language that can be utilized for practical operational use and integration into other standards efforts. Version 1.1.1 includes the following updates:
- Corrected the indicator --> Campaign reference mechanism from using an incorrect type; fixed a typo in Availability; lost Type enum = 1.0; made the Description, Type, and Specification fields in GenericTestMechanism optional rather than required; and fixed several cases where a Source element was not set in InformationSourceType. View the
Indicators of Compromise

- Complex IOCs covering all steps of attack
- Dynamic creation of IOCs on the fly
- Auto-reload of IOCs, TTLs
- Dealing with different standards/import export
# EXPLOIT PACK TRACE

<table>
<thead>
<tr>
<th>url</th>
<th>ip</th>
<th>mime type</th>
<th>ref</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://cuba.eanuncios.net/1/zf3z9lr6ac8di6r4kw2r0hu3ee8ad.html">http://cuba.eanuncios.net/1/zf3z9lr6ac8di6r4kw2r0hu3ee8ad.html</a></td>
<td>93.189.46.222</td>
<td>text/html</td>
<td><a href="http://www.smeysyatut.ru/">http://www.smeysyatut.ru/</a></td>
</tr>
<tr>
<td><a href="http://cuba.eanuncios.net/2909620968/1/1399422480.htm">http://cuba.eanuncios.net/2909620968/1/1399422480.htm</a></td>
<td>93.189.46.222</td>
<td>text/html</td>
<td><a href="http://cuba.eanuncios.net/">http://cuba.eanuncios.net/</a></td>
</tr>
<tr>
<td><a href="http://cuba.eanuncios.net/2909620968/1/1399422480.jar">http://cuba.eanuncios.net/2909620968/1/1399422480.jar</a></td>
<td>93.189.46.222</td>
<td>application/java-archive</td>
<td>-</td>
</tr>
<tr>
<td><a href="http://cuba.eanuncios.net/2909620968/1/1399422480.jar">http://cuba.eanuncios.net/2909620968/1/1399422480.jar</a></td>
<td>93.189.46.222</td>
<td>application/java-archive</td>
<td>-</td>
</tr>
<tr>
<td><a href="http://cuba.eanuncios.net/f/1/1399422480/2909620968/2">http://cuba.eanuncios.net/f/1/1399422480/2909620968/2</a></td>
<td>93.189.46.222</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><a href="http://cuba.eanuncios.net/f/1/1399422480/2909620968/2/2">http://cuba.eanuncios.net/f/1/1399422480/2909620968/2/2</a></td>
<td>93.189.46.222</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Nuclearsploit pack

{
'Nuclearsploitpack':{
  'step1': {
    'files': ['wz3u6si8e5lh7k2tk5ox4ne6d8g.html', 't3f5y9a2bb3d1l7z8gc4o6f.html', 'zf3z9lr6ac8di6r4kw2r0hu3ee8ad.html', 'rx3v8m9z9lr6ac8di6r4kw2r0hu3ee8ad.html'],
    'domains': ['father.ferremovil.com', 'thai.alohatransllc.com', 'cuba.eanuncios.net', 'duncan.disenocorporativo.com.ar'],
    'arguments': [],
    'directories': ['1'],
    'ip': ['93.189.46.201', '93.189.46.203', '93.189.46.222', '93.189.46.224', '93.189.46.233'],
  },
  'step2': {
    'files': ['1399422480.htm', '1399704720.htm', '1399513440.htm', '1399514040.htm', '1399773300.htm'],
    'arguments': [],
    'directories': ['2909620968', '1', '507640988', '940276731', '3957283574', '952211704'],
    'ip': ['93.189.46.222', '93.189.46.224', '93.189.46.233'],
  },
  'step3': {
    'files': ['1399422480.jar', '1399513440.jar'],
    'domains': ['cuba.eanuncios.net', 'homany.collectiveit.com.au'],
    'arguments': [],
    'directories': ['2909620968', '1', '940276731'],
    'ip': ['93.189.46.222', '93.189.46.224'],
  },
  'step4': {
    'files': ['2'],
    'domains': ['cuba.eanuncios.net'],
    'arguments': [],
    'directories': ['f', '1', '1399422480', '2909620968', '2'],
    'ip': ['93.189.46.222']
}
}
Sourcing External IOCs

- feeds (with scrappers):

```sql
<table>
<thead>
<tr>
<th>type</th>
<th>_id</th>
<th>_score</th>
<th>avdetect</th>
<th>url</th>
</tr>
</thead>
<tbody>
<tr>
<td>malwr</td>
<td>26c7885b95501a4da13fa621f7</td>
<td>24</td>
<td><a href="http://malwr.com/analysis/Nzg5MMe2">http://malwr.com/analysis/Nzg5MMe2</a></td>
<td></td>
</tr>
<tr>
<td>malwr</td>
<td>eb31b69055e25ccb52150453c558db05a</td>
<td>1</td>
<td><a href="http://malwr.com/analysis/OWEzIIMa">http://malwr.com/analysis/OWEzIIMa</a></td>
<td></td>
</tr>
<tr>
<td>malwr</td>
<td>1d0756d0a8c9928fba3a4325f839e727</td>
<td>1</td>
<td><a href="http://malwr.com/analysis/NTcwZG9u">http://malwr.com/analysis/NTcwZG9u</a></td>
<td></td>
</tr>
<tr>
<td>malwr</td>
<td>e26b0fe694b9e2503e</td>
<td>3</td>
<td><a href="http://malwr.com/analysis/M2E2ZG9u">http://malwr.com/analysis/M2E2ZG9u</a></td>
<td></td>
</tr>
<tr>
<td>malwr</td>
<td>8321f0fe694b9e2503e</td>
<td>12</td>
<td><a href="http://malwr.com/analysis/MWYzIIMa">http://malwr.com/analysis/MWYzIIMa</a></td>
<td></td>
</tr>
<tr>
<td>malwr</td>
<td>0105566c6b6a346284da5355</td>
<td>1</td>
<td><a href="http://malwr.com/analysis/NTU3MMe2">http://malwr.com/analysis/NTU3MMe2</a></td>
<td></td>
</tr>
<tr>
<td>malwr</td>
<td>02506992dedeff0cd5c17857829</td>
<td>1</td>
<td><a href="http://malwr.com/analysis/MzMyYzg5">http://malwr.com/analysis/MzMyYzg5</a></td>
<td></td>
</tr>
<tr>
<td>malwr</td>
<td>0003f0fe694b9e2503e</td>
<td>1</td>
<td><a href="http://malwr.com/analysis/Nzg5MMe2">http://malwr.com/analysis/Nzg5MMe2</a></td>
<td></td>
</tr>
<tr>
<td>malwr</td>
<td>048c405438cab8df6a31</td>
<td>41</td>
<td><a href="http://malwr.com/analysis/ZTcxM">http://malwr.com/analysis/ZTcxM</a></td>
<td></td>
</tr>
<tr>
<td>malwr</td>
<td>0321f0fe694b9e2503e</td>
<td>1</td>
<td><a href="http://malwr.com/analysis/NTU3MMe2">http://malwr.com/analysis/NTU3MMe2</a></td>
<td></td>
</tr>
<tr>
<td>malwr</td>
<td>048c405438cab8df6a31</td>
<td>41</td>
<td><a href="http://malwr.com/analysis/ZTcxM">http://malwr.com/analysis/ZTcxM</a></td>
<td></td>
</tr>
</tbody>
</table>
```
Automating with IntelMQ

github.com/certtools/intelmq
Sourcing External IOCs

- feed your scrappers:
  https://zeustracker.abuse.ch/blocklist.php?download=badips
  http://malc0de.com/database/
  https://reputation.alienvault.com/reputation.data...
- VT intelligence

```
rule zero0day
{
    strings:
    $d = "Media.Sound()"
    $d2 = "flash.Media.Sound()"
    condition:
    any of them
}
```
Sourcing IOCs Internally

- honeypot feeds
- log analysis
- traffic analysis
**Where to look for IOCs internally**

- Outbound Network Traffic
- User Activities/Failed Logins
- User profile folders
- Administrative Access
- Access from unusual IP addresses
- Database IO: excessive READs
- Size of responses of web pages
- Unusual access to particular files within Web Application (backdoor)
- Unusual port/protocol connections
- DNS and HTTP traffic requests
- Suspicious Scripts, Executables and Data Files
**Challenges**

Why we need IOCs? because it makes it easier to systematically describe knowledge about breaches.

- Identifying intrusions is hard
- Unfair game:
  - defender should protect all the assets
  - attacker only needs to 'poop' one system.
- Identifying targeted, organized intrusions is even harder
- Minor anomalous events are important when put together
- Seeing global picture is a mast
- Details matter
- Attribution is hard
**Use honeypots**

- Running honeypots gives enormous advantage in detecting emerging threats
- Strategically placing honeypots is extremely important
Applying IOCs to your detection process

moloch moloch moloch :)

Sessions | SPI View | SPI Graph | Connections | Files | Stats | Settings

Last 24 hrs ▼ port.src==53 && port.src==53 && port.src==53

Showing 1 to 100 of 1,988,776 entries (filtered from 25,958,928,807 total entries)
TOOLS FOR DYNAMIC DETECTION OF IOC

- Snort
- Yara + yara-enabled tools
- Moloch
- Splunk/Log search
- roll-your-own:p
Moloch is awesome:
OPEN-SOURCE TOOLS

OpenIOC manipulation
https://github.com/STIXProject/openioc-to-stix
https://github.com/tklane/openiocscripts

Mantis Threat Intelligence Framework
https://github.com/siemens/django-mantis.git
Mantis supports STIX/CybOX/IODEF/OpenIOC etc via importers:
https://github.com/siemens/django-mantis-openioc-importer

Search splunk data for IOC indicators:
https://github.com/technoskald/splunk-search

Our framework: http://github.com/fygrave/iocmap/
MISP

- https://github.com/MISP
TOOLS FOR DYNAMIC DETECTION

- Moloch
  - Moloch supports Yara (IOC can be directly applied)
  - Moloch has awesome tagger plugin:

```bash
# tagger.so
# provides ability to import text files with IP and/or hostnames
# into a sensor that would cause autotagging of all matching
plugins=tagger.so
taggerIpFiles=blacklist,tag,tag,tag...
taggerDomainFiles=domainbasedblacklists,tag,tag,tag
```
Moloch plugins

Moloch is easily extendable with your own plugins

- https://github.com/fygrave/moloch_zmq - makes it easy to integrate other things with moloch via zmq queue pub/sub or push/pull

**moloch_zmq**

This ZMQ integration/data exploit plugin for Moloch (http://github.com/aol/moloch/). The current implementation acts as ZMQ PUB(lisher), which you need to connect to using your client(s) and perform additional real-time analysis of network data.

Presently only HTTP traffic (src ip, dst ip, ports, url and X-Forwarded-For headers are sent). The plugin could be further extended to hook into other protocols as well.

Only two 0MQ patterns are supported on the moment. Push/Pull and Pub/Sub.

**Requirements:**

0MQ 3.x or later.

```
add-apt-repository ppa:chris-lea/zeromq
apt-get update
apt-get install libzmq3-dev
```
**Moloch ZMQ example**

CEP-based analysis of network-traffic (using ESPER):
https://github.com/fygrave/clj-esptool/

```lisp
(esp :add "create context SegmentedBySrc partition by src from WebDataEvent")
(esp :add "context SegmentedBySrc select src, rate (30) as rate, avg(rate (30)) as avgRate from WebDataEvent.win: time (30) having rate (30) < avg(rate (30)) * 0.75 output snapshot every 60 sec")
```

```lisp
(future -call start -counting)
```
Sources of IOCs

- ioc bucket:
  http://iocbucket.com

- Public blacklists/trackers could also be used as source:
  https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist
  https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist

- Eset IOC repository
  https://github.com/eset/malware-ioc
  more coming?
WHERE TO MINE IOC

- passive HTTP (keep your data recorded)
- passive DNS

These platforms provide ability to mine traffic or patterns from the past based on IOC similarity

show me all the packets similar to this IOC

We implemented a whois service for IOC look-ups

whois -h ioc.host.com attribute:value+attribute:value
MINING IOCs FROM YOUR OWN DATA

- find and investigate incident
- Or even read paper
- determine indicators and test it in YOUR Environment
- use new indicators in the future
  see IOC cycle we mentioned earlier
Example

If event chain leads to compromise

http://liapolasens[.]info/indexm.html

http://liapolasens[.]info/counter.php?t=f&v=win%202011.7,700,169&a=\texttt{true}

http://liapolasens[.]info/354RIcx

http://liapolasens[.]info/054RIcx

What to do?
Overview

Introduction

Detection Techniques and Tools

EOF
Questions

@fygrave @vbkropotov
And answers :)