# Living with compromise: Enterprise Network Survival in tough Russian Environment

Vladimir Kropotov, Vitaly Chetvertakov, Fyodor Yarochkin
HITCON 2014

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

Aug 20, 2014, Taipei

# Outline

# Agenda

- Prerequisites and past Experience share practical experience in an enterprise defense that lead to particular conclusions
- Tools and implemention

demonstrate tools and techniques that improve detection aid incident handling lifecycle

# You are or will be compromised

If you are under attack, your AV,Firewaslls, IDS, etc. are in THE ATTACKER THREATS MODEL. The option you have - read between the lines. When you are compromised, what is the action plan? Are you able to:

- Detect

Properly:

- Categorise
- Mitgate
- Investigate
- ...

# Threat Landscape

- Assumption - Not isolated big networks are (almost) always somehow compromised During the last year about 30% of monitored hosts was attacked by cybercrimes at least once. For Basic setup Host AV, Proxy with AV, firewalls, IPS, etc... Success rate 3-15% If you have 10k hosts network in Russia, about 3k host will be attacked and 90-450 will be compromised on average. Approximate this situation to 40M hosts...

What to do?

# Threat Identification

- Identify threats within detection capabilities of your organisation.
- There always will be threats your org can't detect or handle. You have to accept the risk (or allocate additional resources to mitigate it).

# Examples of an Org. Strength:

- You have Good monitoring team - otherwise *you* can ONLY rely on your security vendors opinion and support in handling security incidents. BAD!


- Defense in Depth: Have multipe independent layers of protection monitoring or mitigation.
- Examples: sinkholes redirect botnet traffic to internal sinkholes. proxy blacklist prevents access to botnet resources. and so on. This also decreases risks of your organization to be blacklisted in public blacklists, such as spamhaus, shadowserver lists (SPB, RSBL).

# Examplies of possible org Limitations:

- No security team, IT operations outsourced :)
- HUGE distributed Not centralized environment. No uniform defense mechanisms.
- Limited ability to control and monitor IT and SECURITY events
- No recording of forensic evidence
- Distributed, uncommunicating IT support teams

# Identify your Attack Surface

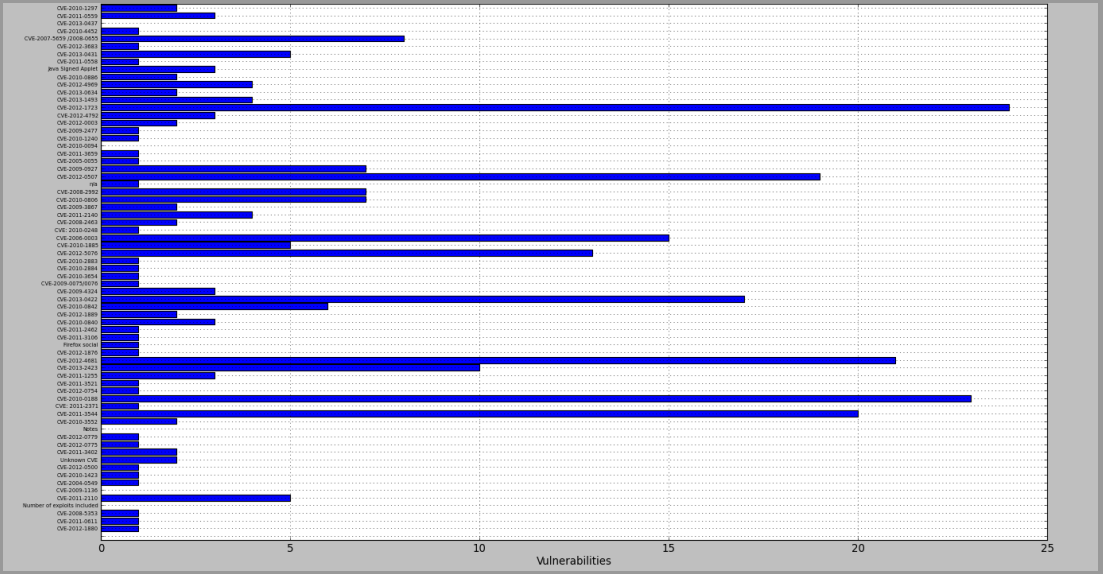
- browser? mail? vpn? rewmovable devices?publically accessable asset? Untrusted vendor?

# Attacker information gathering

- Targetted Attackers want your data.
- They have time.
- Not every javascript serves exploit. Some are just recording information on your environment.

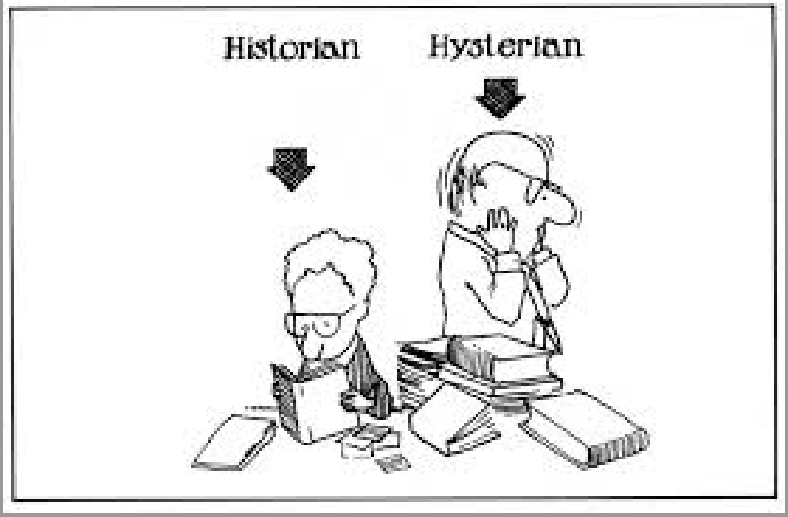
# Attacker exploitation

vuls vs kis (based on Mila/contagiodump repo data):



# Know your history

Incident history datamining.
Case studies of Incident and Incident Response

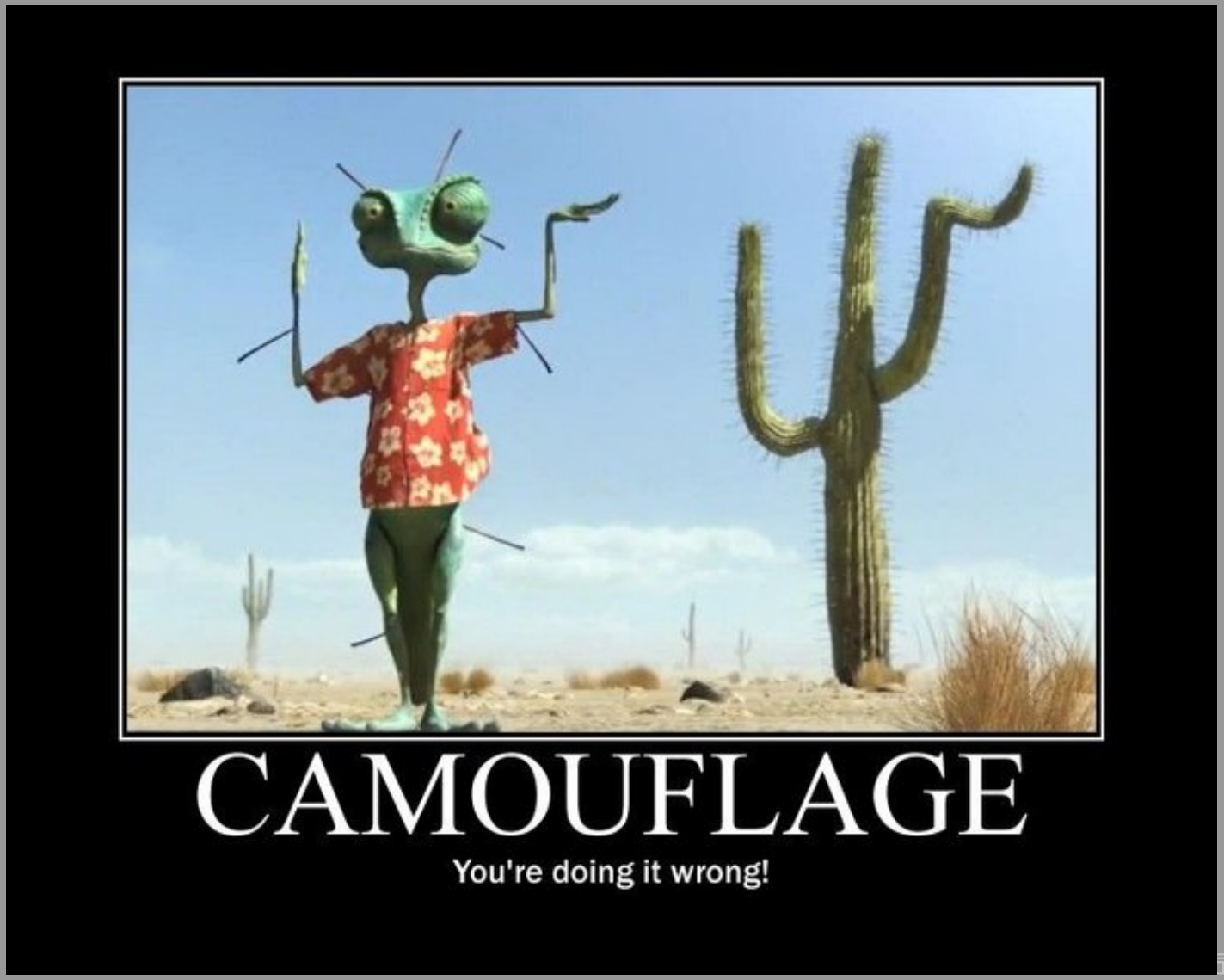


# An Incident Lifestype

stages in life of an incident

- Incident (Almost) Happens
- Incident Detected
- Additional Information Collected
- Short-Term Impact Minimization
- Incident Categorized
- Long-Term Mitigation plan (typical/ not typical)
- Mitigation plan implementation
- QOS (Mitigation assurance): CHECK!
- Indicators of Compromise (IOCs) preservation
- Check for presence of IOCs in other parts of monitoring Environments
- Store incident data, update knowledge base, collect useful stats to speed up future incident handling.

# Be sure that measures are effective.



# Incidents

- Characteristics of incidents
- How to enhance security measures
- How to prevent further recurrence

# Classification of Incidents

Examples:

- Malicious code
- Malicious code, with consequential network activity
- Anomalous activity
- Out of the scope of Enterprise Network Activity
- Untrusted executable
- Direct reputation risk
- Indirect reputation risk
- Targeted Attack (APT)

# Incidents vs Systems(1)

Incidents VS Systems: Usability of various components common belief

| incidents/systems | firewalls | AV | web traf | IPS | DNS Profiling |
|---|---|---|---|---|---|
| Malicious code | | 10 | | | |
| Malicious code, with .. | 1 | 7 | | 2 | |
| Anomalous activity | 5 | | | 5 | |
| Out of the scope .. | 5 | | | 5 | |
| Untrusted executable | | 7 | | 3 | |
| Direct reputation risk | | | | | |
| Indirect reputation risk | | | | | |
| Targeted Attack (APT) | | 8 | | 2 | |

# Incidents vs Systems(2)

Incidents VS Systems: Usability of various components reality

| incidents/systems | firewalls | AV | web traf | IPS | DNS Profiling |
|---|---|---|---|---|---|
| Malicious code | | 4 | 6 | | |
| Malicious code, with .. | 1 | 2 | 4 | 1 | 2 |
| Anomalous activity | 2 | | 3 | 2 | 4 |
| Out of the scope .. | 2 | | 5 | 3 | |
| Untrusted executables | | 1 | 8 | 1 | |
| Direct reputation risk | | | 10 | | |
| Indirect reputation risk | | | 10 | | |
| Targeted Attack (APT) | | 8 | | 2 | |

# Examples: Web Traffic Analysis

Proxy and passive HTTP traffic analysis

Sources:

- proxy logs
- passive web traffic monitoring (including HTTPS)

# Example

| url | ip | mime type | size | code |
|---|---|---|---|---|
| cuba.eanuncios.net/1/zf3z9lr6ac8di6r4kw2r0hu3ee8ad.html | 93.189.46.222 | text/html | 118162 | 200 |
| cuba.eanuncios.net/2909620968/1/1399422480.htm | 93.189.46.222 | text/html | 37432 | 200 |
| cuba.eanuncios.net/2909620968/1/1399422480.jar | 93.189.46.222 | application/java-archive | 18451 | 200 |
| cuba.eanuncios.net/2909620968/1/1399422480.jar | 93.189.46.222 | application/java-archive | 18451 | 200 |
| cuba.eanuncios.net/f/1/1399422480/2909620968/2 | 93.189.46.222 | application/octet-stream | 115020 | 200 |
| cuba.eanuncios.net/f/1/1399422480/2909620968/2/2 | 93.189.46.222 | - | 327 | 200 |


What just happened?

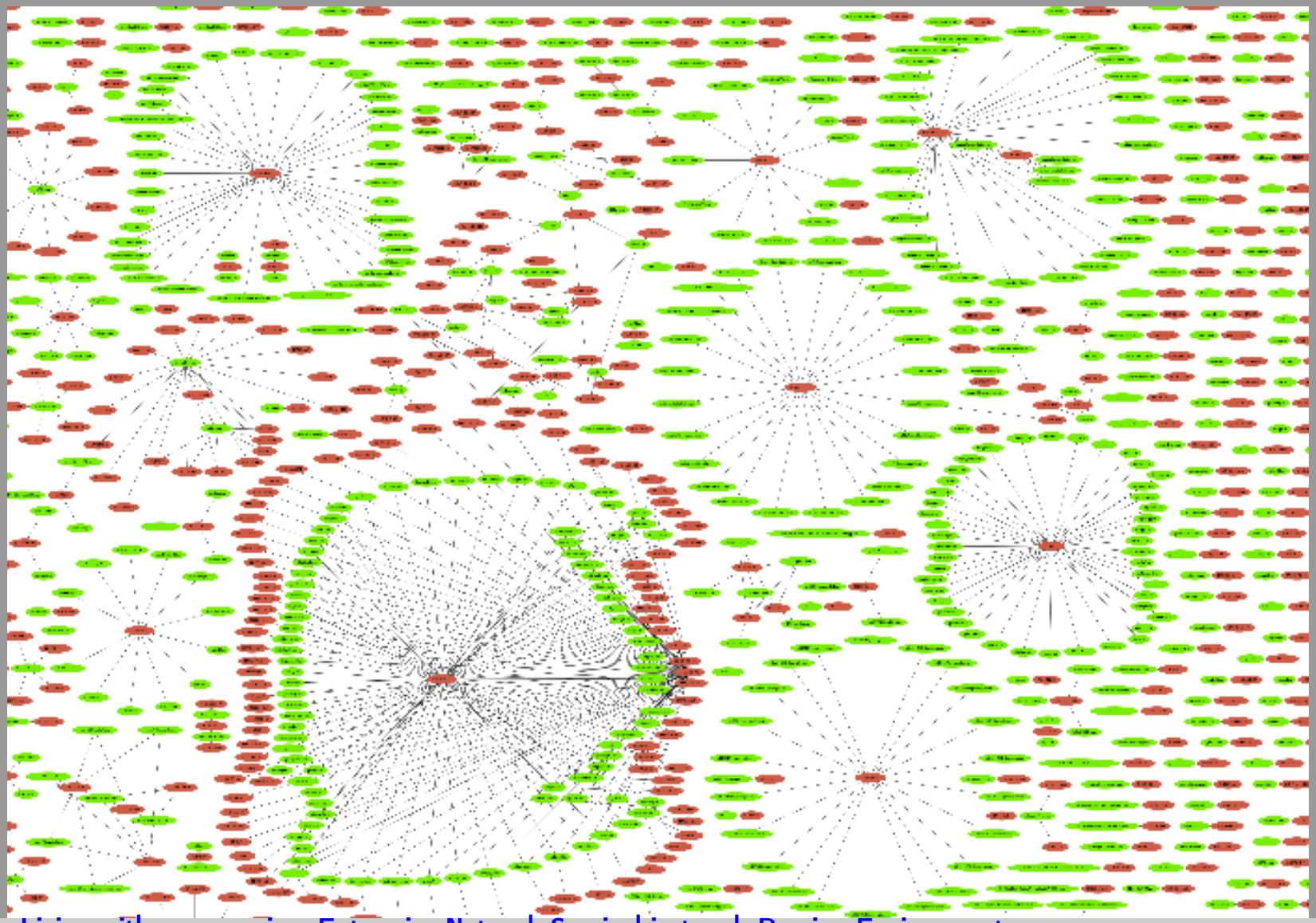
# Examples: DNS

Passive DNS traffic acquisition and analysis
a couple of examples (last week)

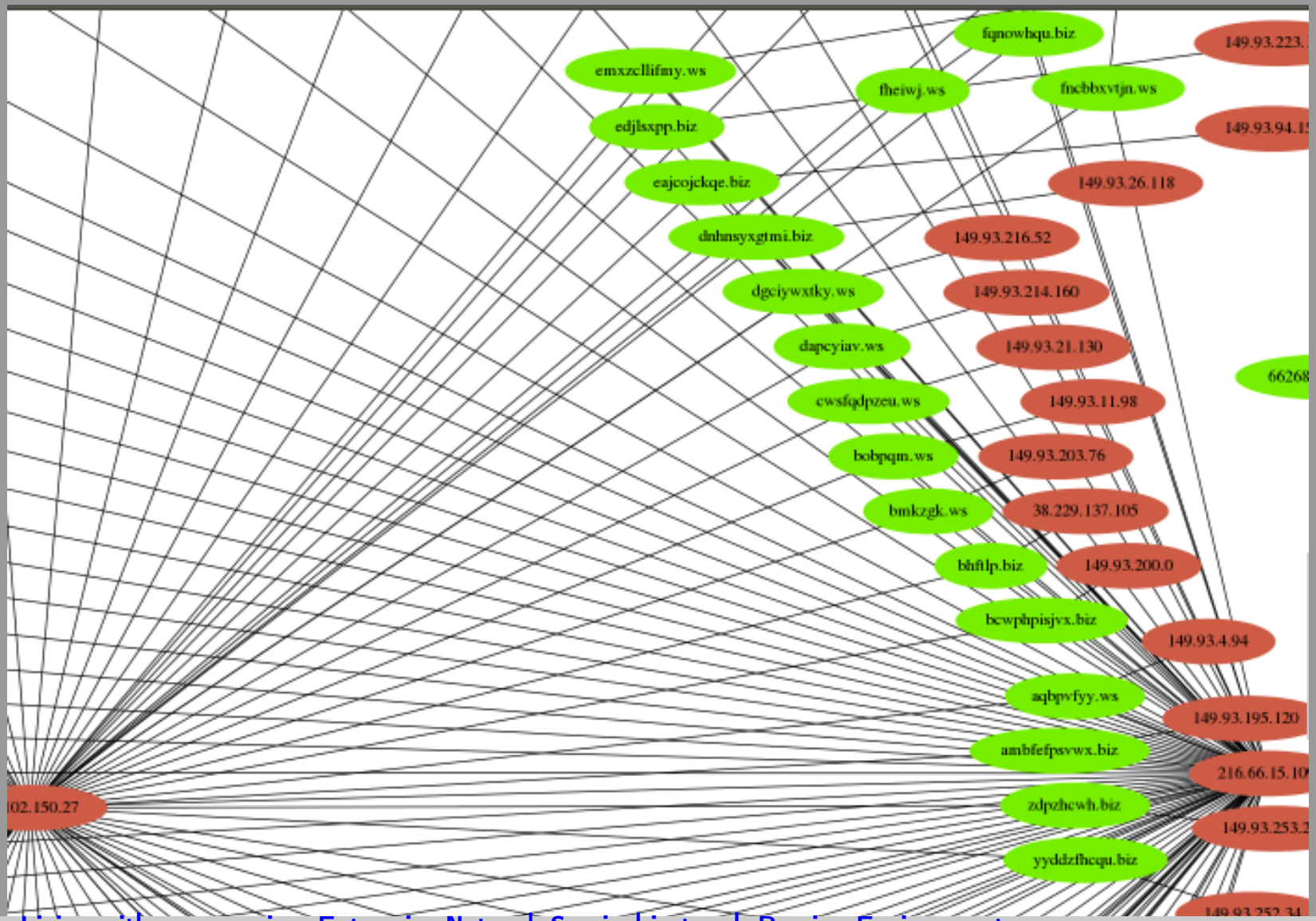
| domain | ip | owner |
|---|---|---|
| rtvwerjyuver.com | 69.164.203.105 | linode |
| tvrstrynyvwstrtve.com | 109.74.196.143 | linode |
| cu3007133.wfaxyqykxh.ru | ... | |

what does your DNS traffic look like..?

# DNS viz01



# DNS viz02


fqnowhqu.biz
emxzcllifmy.ws
fheiwj.ws
fncbbxvtjn.ws
edjlsxpp.biz
eajcojckqe.biz
149.93.26.118
dnhnsyxgtmi.biz
149.93.216.52
dgciywxtky.ws
149.93.214.160
dapcyiav.ws
149.93.21.130
cwsfqdpzeu.ws
149.93.11.98
bobpqm.ws
149.93.203.76
bmkzgk.ws
38.229.137.105
bhftlp.biz
149.93.200.0
bcwphpisjvx.biz
149.93.4.94
aqbpwfyy.ws
149.93.195.120
ambfefpsvwx.biz
zdpzhcwh.biz
yyddzfhcqu.biz

# DNS anonymizer traffc

## Anonimizer

```
8/13/2014 9:59:12 PM - ##.##.##.## - 0s.o53xo.pfxxk5dvmjss4y3pnu.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - o53xo.pfxxk5dvmjss4y3pnu.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - o53xo.pfxxk5dvmjss4y3pnu.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - 0s.om.pf2gs3lhfzrw63i.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - 0s.om.pf2gs3lhfzrw63i.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - nbxxe33tnbuxsllwnn2xg.mjuxultvme.dd
8/13/2014 9:59:12 PM - ##.##.##.## - nbxxe33tnbuxsllwnn2xg.mjuxultvme.dd
8/13/2014 9:59:12 PM - ##.##.##.## - 0s.ne.pf2gs3lhfzrw63i.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - 0s.ne.pf2gs3lhfzrw63i.dd34.ru
8/13/2014 9:59:15 PM - ##.##.##.## - obuwg4y.nruxmzlkn52xe3tbnqxgg33n.d
8/13/2014 9:59:15 PM - ##.##.##.## - obuwg4y.nruxmzlkn52xe3tbnqxgg33n.d
8/13/2014 9:59:15 PM - ##.##.##.## - 0s.o53xo.mzqwgzlcn5xwwltdn5wq.dd34
8/13/2014 9:59:15 PM - ##.##.##.## - 0s.o53xo.mzqwgzlcn5xwwltdn5wq.dd34
Time: Today 09:59:15pm
```

# Covert channel communication

```
8/13/2014 5:49:04 PM - x.x.x.x - 5141017.mtdtzwdhc.mdgtmtmmc
8/13/2014 5:49:04 PM - x.x.x.x - 5141017.mtdtzwdhc.mdgtmtmmc

Time:                          Today          13:19:25
Description:                   REP.bilscz Detected at Today
13:19:25
Interface Name:                bond1.382
Interface Direction:           outbound
```

# Sinkhole in DNS

Credit: domaintools.com

| | |
|---|---|
| Email | thomas@spenglers.biz is associated with ~93,134 domains |
| Registrant Org | Domain Administrator was found in ~4,350,091 other domains |
| Dates | Created on 2014-06-30 - Expires on 2015-06-29 |
| Domain Status | Registered And No Website |
| Whois History | 1 record has been archived since 2014-07-02 |
| Hosting History | 1 change on 2 unique name servers over 0 year |
| Whois Server | whois.biz |

# Sinkhole in DNS

Credit: domaintools.com

| | |
|---|---|
| Email | abuse@bigrock.com is associated with ~265,970 domains<br>gregorygofr@yahoo.com |
| Registrar | BIGROCK SOLUTIONS LIMITED |
| Registrar Status | clientTransferProhibited |
| Dates | Created on 2011-06-26 - Expires on 2015-06-26 - Updated on 2014-06-25 |
| Name Server(s) | NS1.SUSPENDED-DOMIAN.COM (has 306 domains)<br>NS2.SUSPENDED-DOMIAN.COM (has 306 domains) |
| IP Address | 69.164.203.105 - 81 other sites hosted on this server |
| IP Location | - Texas - Dallas - Linode |
| ASN | AS36351 SOFTLAYER - SoftLayer Technologies Inc.,US (registered Dec 12, 2005 |
| Domain Status | Registered And Active Website |
| Whois History | 30 records have been archived since 2011-06-27 Whois History |

# DNS

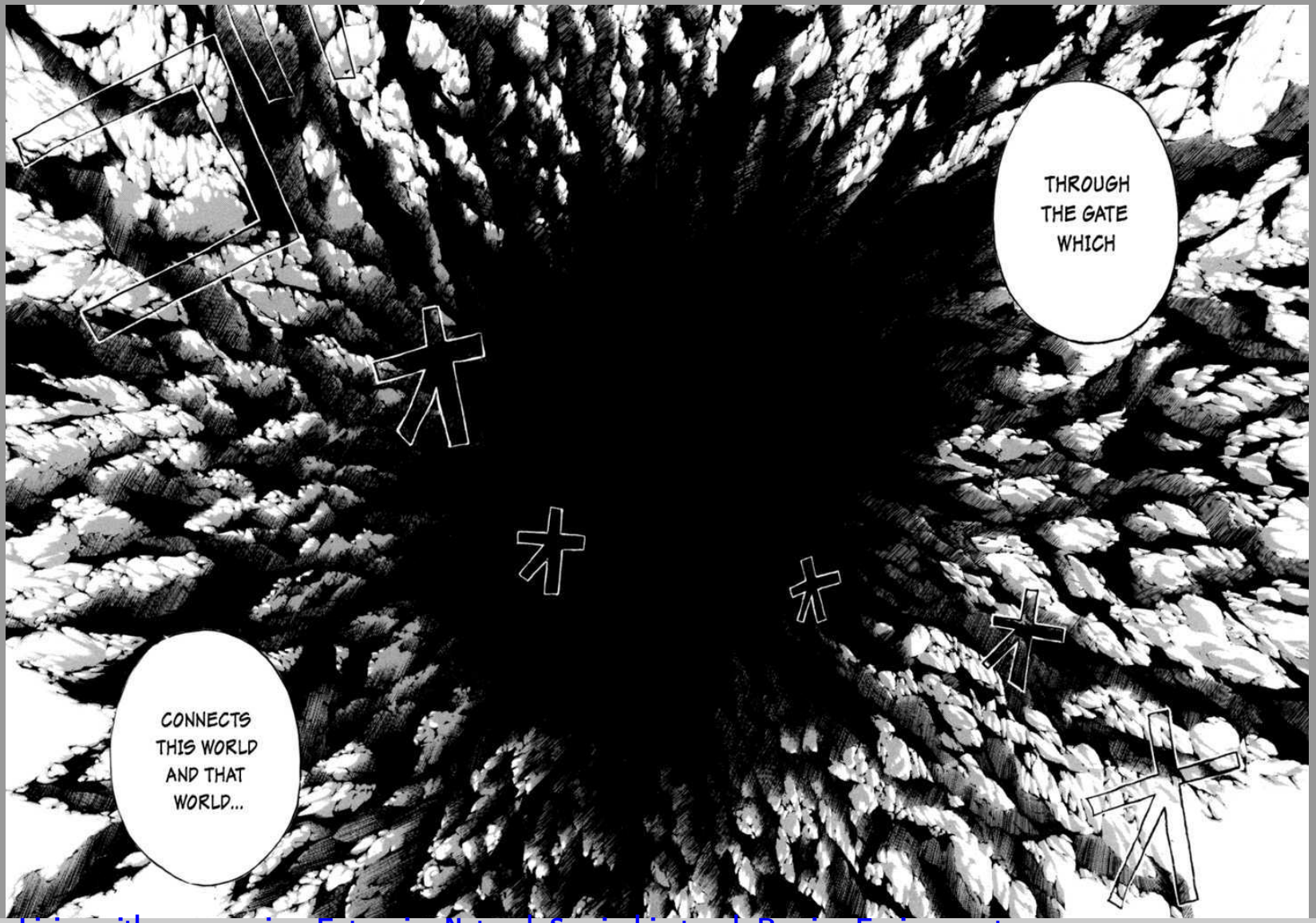
Suspicious activity: DNS lookups: kojxlvfkpl.biz:149.93.207.203
kojxlvfkpl.biz:216.66.15.109
kojxlvfkpl.biz:38.102.150.27

```
found a referral to rwhois.he.net:4321.

%rwhois V-1.5:0012b7:01 ops.he.net (HE-RWHOISd v:r255,m1:r319)
network:ID;I:NET-216.66.15.64/26
network:Auth-Area:nets
network:Class-Name:network
network:Network-Name;I:NET-216.66.15.64/26
network:Parent;I:NET-216.66.0.0/18
network:IP-Network:216.66.15.64/26
network:Org-Contact;I:POC-DC-1125
network:Tech-Contact;I:POC-HE-NOC
network:Abuse-Contact;I:POC-HE-ABUSE
network:NOC-Contact;I:POC-HE-NOC
network:Created:20130823163004000
network:Updated:20130823163004000

contact:ID;I:POC-DC-1125
contact:Auth-Area:contacts
contact:Class-Name:contact
contact:Name:Bart Lathrop
```

# Look for holes :)



# Hole traffic

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2014/08/07 12:15:38 | 7 TWN | 2258 | 38.102.150.27 USA | 80 | 7 | 180 / 590 | moloch |
| 2014/08/07 12:15:44 | 7 TWN | 2502 | 38.102.150.27 USA | 80 | 7 | 180 / 590 | moloch |
| 2014/08/07 12:16:03 | 7 TWN | 3018 | 38.102.150.27 USA | 80 | 7 | 180 / 590 | moloch |
| 2014/08/07 12:16:58 | 7 TWN | 1227 | 38.102.150.27 USA | 80 | 7 | 180 / 590 | moloch |
| 2014/08/07 12:16:58 | 7 TWN | 1229 | 38.102.150.27 USA | 80 | 6 | 156 / 512 | moloch |
| 2014/08/07 12:17:06 | 7 TWN | 1481 | 38.102.150.27 USA | 80 | 7 | 180 / 590 | moloch |
| 2014/08/07 12:17:29 | 7 TWN | 2253 | 38.102.150.27 USA | 80 | 7 | 180 / 590 | moloch |

# Usability of sandboxes

Sandboxes could be helpful to analyze mal. content.
However, they are often not very practical. A few examples (delivery via SMTP)

- 1.zip
- FW supplier data form.msg
- How to Get Thin Quick.msg
- Losing a size within a fortnight It's easy.msg
- $2014_{1308}$.msg

# Problems with Sandboxing

- Known tricks
- matching environment
- code behaves differently depending on: environment, time, user interaction, time-zone, ..
- performance (timeouts, ..)
- Use interaction

# Stages of incident detection

- Before Incident (Security Awareness, Pentests, etc.)
- Access attempt
- Access obtained
- Privilege escalation
- Execution of attack goal
- Post-incident IR (too late))
  Incidents VS Stages of detection ~= how monitoring team operates with current limitations in Environment

# Incidents VS Stages of detection(1)

common belief

| incidents/stages | before | attempt | obtained | escl | impl | late |
|---|---|---|---|---|---|---|
| Malicious code | 5 | 5 | | | | |
| Malicious code, with .. | 5 | 5 | | | | |
| Anomalous activity | 8 | 2 | | | | |
| Out of the scope .. | | | | | | |
| Untrusted executables | 1 | 9 | | | | |
| Direct reputation risk | | | 10 | | | |
| Indirect reputation risk | | | 10 | | | |
| Targeted Attack (APT) | | 8 | 2 | | | |

# Incidents VS Stages of detection(2)

reality

| incidents/stages | before | attempt | obtained | escl | impl | late |
|---|---|---|---|---|---|---|
| Malicious code | 1 | 2 | 2 | | 2 | 3 |
| Malicious code, with .. | 1 | 2 | 2 | | 3 | 2 |
| Anomalous activity | 1 | 3 | 2 | | 2 | 2 |
| Out of the scope .. | | | | | 2 | 8 |
| Untrusted executables | | 2 | 3 | | 3 | 2 |
| Direct reputation risk | | | 2 | 2 | 3 | 3 |
| Indirect reputation risk | | | 2 | 2 | 3 | 3 |
| Targeted Attack (APT) | | 1 | 1 | 1 | 2 | 5 |

# Attack delivery method

| incidents/delivery | web | email | ext.storage | share | services | other |
|---|---|---|---|---|---|---|
| Malicious code | 5 | 2 | 2 | 1 | | |
| Malicious code, with .. | 5 | 2 | 2 | 1 | | |
| Anomalous activity | 1 | 3 | 2 | 1 | 1 | 2 |
| Out of the scope .. | 3 | 3 | 2 | | | 2 |
| Untrusted executables | 4 | | 3 | | 1 | 2 |
| Direct reputation risk | 3 | 2 | | | 3 | 2 |
| Indirect reputation risk | 3 | 2 | 1 | | 2 | 2 |
| Targeted Attack (APT) | 2 | 3 | 1 | | 2 | 2 |

# How can you improve your security posture

Cross-correlate your historical data including data from following sources:

- Incidents
- Detection systems (ips/ids/av/fw/..): map type of incident to component that detects those.
- Stages of detection - and incidents
- Delivery method - which network detection components detect what delivery methods.

use community contributions :)

# Specific incident attributes

- Availability first
- Conflict of interest: flag
- Restrictions on information sharing: limits the quality of teams collaboration
- Manual routing of information sharing for the special cases

# Incidents categorization

- Categorisation based on Vendor knowledge
- Categorisation based on public sources
- Categorisation based on internal intel.
- Categorisation based on limited IOCs sharing to the focused groups
- Attribution

# Tools and Execution

There is a number of tools we can share. Some are developed by us. Other - are just very good open source projects.

- `http://github.com/fygrave/ndf`
- `http://github.com/fygrave/hntp`
- fiddler
- elasticsearch && `http://github.com/aol/moloch` (vm)
- yara (as moloch plugin)
- hpfeeds
- CIF

Indicators of Compromise is one of essential information mediums here to represent facts on incident(s).

# Mining public knowledge

There is a lot of public knowledge you could mine. CIF is a fantastic tool for that. `https://github.com/collectiveintel/cif-v1`

```
[2014-08-20T09:55:12,711Z][INFO][main:312]: processing: /opt/cif/bin/cif-smrt -d
 -r /etc/cif/rules/default/isc_sans_edu.cfg -f domains_medium
[2014-08-20T09:55:12,713Z][INFO][CIF::Smrt:91]: starting at: 2014-08-20T00:00:00
Z
[2014-08-20T09:55:12,717Z][INFO][CIF::Smrt:103]: processing...
[2014-08-20T09:55:12,717Z][DEBUG][CIF::Smrt::Handler::Default:52]: fetching...
[2014-08-20T09:55:12,717Z][DEBUG][CIF::Smrt::Fetcher::Uri:75]: pulling: http://i
sc.sans.edu/feeds/suspiciousdomains_Medium.txt
[2014-08-20T09:55:15,058Z][DEBUG][CIF::Smrt::Fetcher:49]: using log: /var/smrt/c
ache/20140820.log
[2014-08-20T09:55:15,058Z][DEBUG][CIF::Smrt::Fetcher:51]: file: /var/smrt/cache/
isc.sans.edu-domains_medium
[2014-08-20T09:55:15,108Z][INFO][main:324]: nothing [new] to send...
[2014-08-20T09:55:15,108Z][INFO][main:312]: processing: /opt/cif/bin/cif-smrt -d
 -r /etc/cif/rules/default/spamhaus.cfg -f edrop
[2014-08-20T09:55:15,111Z][INFO][CIF::Smrt:91]: starting at: 2014-08-20T00:00:00
Z
[2014-08-20T09:55:15,114Z][INFO][CIF::Smrt:103]: processing...
[2014-08-20T09:55:15,114Z][DEBUG][CIF::Smrt::Handler::Default:52]: fetching...
[2014-08-20T09:55:15,114Z][DEBUG][CIF::Smrt::Fetcher::Uri:75]: pulling: http://w
ww.spamhaus.org/drop/edrop.txt
```

# CIF: example

grabbing shadowserver data:

```
feed = 'http://www.shadowserver.org/ccdns.php'
regex = '^([a-zA-Z0-9.-]+[a-zA-Z0-9]{2,5})$'
regex_values = 'address'
assessment = 'botnet'
description = 'unknown'
alternativeid = 'http://www.shadowserver.org/ccdns.php'
alternativeid_restriction = 'need-to-know'
disabled = true
```

# CIF: example

Searched 5 of 5 shards. 45909 hits. 3.134 seconds

Result Source


```
{
    _index: "cif-2014.08.13",
    _type: "observables",
    _id:
    "edaa72396b4a761122e11c4dc9b6844dd9417c3032150243397e72d68154d8b0",
    _version: 1,
    _score: null,
    ▼ _source: {
        provider: "spamhaus.org",
        ▼ peers: [],
        subdivision: "MOW",
        group: "everyone",
        firsttime: "2014-08-13T08:13:33Z",
        latitude: 55.7522,
        id:
        "edaa72396b4a761122e11c4dc9b6844dd9417c3032150243397e72d68154d8b0",
        altid_tlp: "green",
        lasttime: "2014-08-13T08:13:33Z",
        @timestamp: "2014-08-13T08:13:40Z",
        tlp: "green",
        longitude: 37.6156,
        timezone: "Europe/Moscow",
        lang: "EN",
        observable: "194.1.184.0/24",
        countrycode: "RU",
        ▼ tags: [
            "suspicious",
            "hijacked"
        ],
        @version: 2,
        otype: "ipv4",
        reporttime: "2014-08-13T08:13:33Z",
        citycode: "Moscow",
        confidence: "95",
        altid: "http://www.spamhaus.org/sbl/sbl.lasso?query=SBL148480"
```


| _index | provider | subdivision | group | firsttime |
|---|---|---|---|---|
| cif-2014.08.13 | spamhaus.org | CA | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | CA | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | BC | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | MOW | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | MOW | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | MOW | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | CA | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | CA | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | FL | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | BC | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | NY | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | MA | everyone | 2014-08-13 |
| cif-2014.08.13 | spamhaus.org | BC | everyone | 2014-08-13 |

# 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 unform representation of IOC (now FireEye) `http://www.openioc.org/`

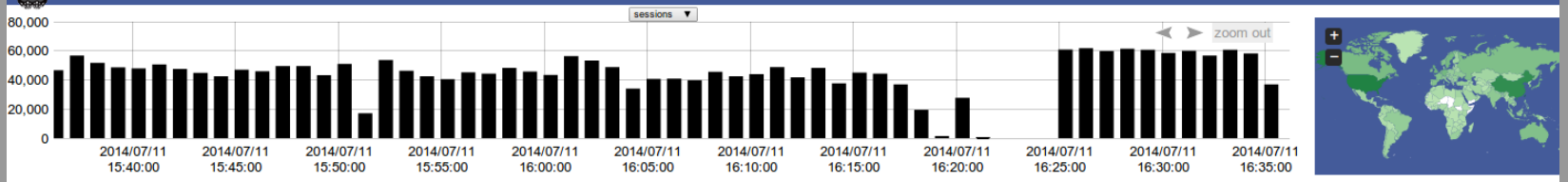

```
-<ioc id="6d2a1b03-b216-4cd8-9a9e-8827af6ebf93" last-modified="2011-10-28T19:28:20">
  <short_description>Zeus</short_description>
  <description>Finds Zeus variants, twexts, sdra64, ntos</description>
  <keywords/>
  <authored_by>Mandiant</authored_by>
  <authored_date>0001-01-01T00:00:00</authored_date>
  <links/>
 -<definition>
  -<Indicator operator="OR" id="9c8df971-32a8-4ede-8a3a-c5cb2c1439c6">
   -<Indicator operator="AND" id="0781258f-6960-4da5-97a0-ec35fb403cac">
    -<IndicatorItem id="50455b63-35bf-4efa-9f06-aeba2980f80a" condition="contains">
       <Context document="ProcessItem" search="ProcessItem/name" type="mir"/>
       <Content type="string">winlogon.exe</Content>
     </IndicatorItem>
    -<IndicatorItem id="b05d9b40-0528-461f-9721-e31d5651abdc" condition="contains">
       <Context document="ProcessItem" search="ProcessItem/HandleList/Handle/Type" type="mir"/>
       <Content type="string">File</Content>
     </IndicatorItem>
    -<Indicator operator="OR" id="67505775-6577-43b2-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>
     -<IndicatorItem id="25ff12a7-665b-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="fea11706-9ebe-469b-b30a-4047cfb7436b" condition="contains">
        <Context document="ProcessItem" search="ProcessItem/HandleList/Handle/Type" type="mir"/>
```

# RAW Data Preservation

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

moloch v0.10.1-G

Last 1 hr | port == 53 && ip.src==140.109.21.163 | Search | Actions




100 | Showing 1 to 100 of 2,543,589 entries (filtered from 27,287,513,073 total entries) | First | Previous | 1 | 2 | 3 | 4 | 5 | Next | Las

| | Start | Stop | Src IP | Src Port | Dst IP | Dst Port | Packets | Bytes | Node | Info |
|---|---|---|---|---|---|---|---|---|---|---|
| udp | 2014/07/11 15:18:43 | 2014/07/11 16:17:39 | 140.109.32.9 TWN | 53 | 8.8.8.8 USA | 53 | 10000 | 946,148 / 1,026,148 | moloch | mixerbox-prod.elasticbeanstalk.com<br>code.jquery.com<br>scontent-b-sin.xx.fbcdn.net<br>11-courier.push.apple.com<br>yl6r032749 |
| udp | 2014/07/11 15:20:06 | 2014/07/11 15:51:20 | 140.109.221.39 TWN | 1067 | 168.95.192.1 TWN | 53 | 437 | 35,580 / 39,076 | moloch | time.nist.gov<br>stdtime.gov.hk<br>time-b.nist.gov<br>furcms.dyndns.tv<br>ntp-nasa.arc.nasa.gov |
| Couldn't look up SPI data, error for session 140711-Y7gLjHiaqwlDAqMyHYXV9nNj Error: Error loading data for session 140711-Y7gLjHiaqwlDAqMyHYXV9nNj | | | | | | | | | | |
| udp | 2014/07/11 15:22:02 | 2014/07/11 15:51:21 | 140.109.229.99 TWN | 32768 | 168.95.1.1 TWN | 53 | 833 | 56,297 / 62,961 | moloch | a628.phobos-apple.com.akadns.net<br>a628.phobos.apple.com.edgesuite.net<br>news.iblinx.com<br>ieonline.microsoft.com<br>clients4.google.com |
| udp | 2014/07/11 15:23:48 | 2014/07/11 16:18:29 | 140.109.54.175 TWN | 13 | 168.95.1.1 TWN | 53 | 2438 | 165,784 / 185,288 | moloch | ntp1.cs.mu.oz.au |
| udp | 2014/07/11 15:24:16 | 2014/07/11 16:18:26 | 140.109.113.52 TWN | 40940 | 198.153.194.22 USA | 53 | 2734 | 321,703 / 343,575 | moloch | sb.l.google.com<br>dx.doi.org<br>wmail1.cc.ntu.edu.tw<br>my.ntu.edu.tw<br>scontent-a.xx.fbcdn.net |

# Moloch as detection tool

# Tools for Dynamic Detection

- Moloch
  - Moloch supports Yara (IOCs can be directly applied)
  - Moloch allows you to develop your own plugins
  - Moloch has awesome tagger plugin:

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

# Extending Moloch

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 model

## moloch_zmq

This ZMQ integration/data explort 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
```

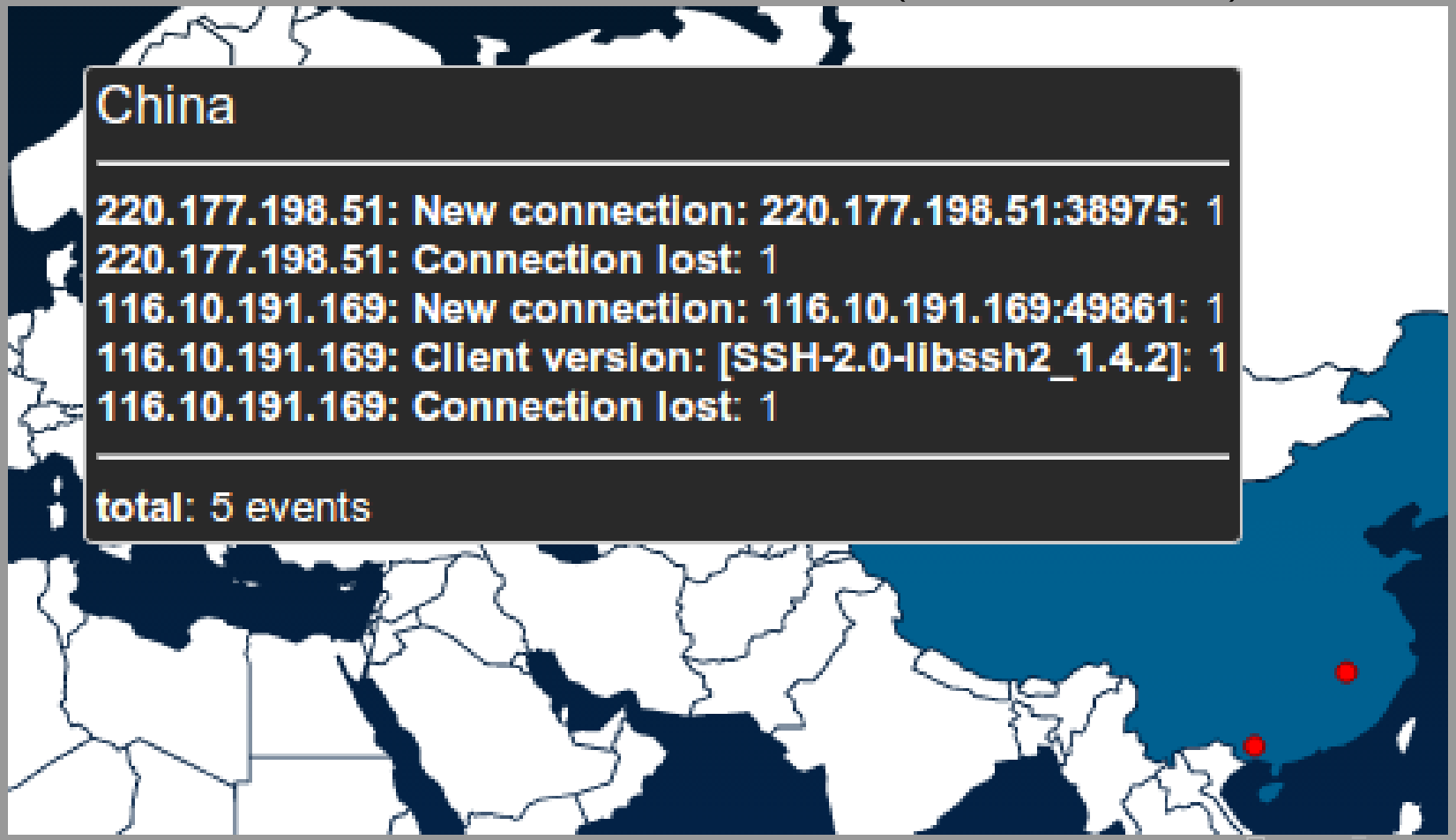
# Moloch ZMQ example

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

```
(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")
(future-call start-counting)
```

# Fake targets

Honeypots are very useful when dealing with unknown threats or when dealing with environments with limited capabilities (VPN, BYOD, ..)



# Honeypot data sharing

HPFeeds could be used to share honeypot data feeds in controlled manner via your own broker.

```
import pygeoip
import hpfeeds
import json

HOST='broker'
PORT = 20000
CHANNELS= ['geoloc.events']
IDENT='ident'
SECRET='secret'
gi = pygeoip.GeoIP('GeoLiteCity.dat')
hpc = hpfeeds.new(HOST, PORT, IDENT, SECRET)
msg = {'latitude':gi.record_by_addr(ip)['latitude'],
       'longitude':gi.record_by_addr(ip)['longitude'],
        'type': 'honeypot hit'}
hpc.publish(CHANNELS, json.dumps(msg))
```

# Last not least :)

Incident response: your availability is impacted by your investigation capabilities.

# Incident Response: some details

- Ways to determine scope (impact)
- Ways to minimize scope (impact)
- Response to the threats with known scope (impact)
- Response to the threats with unknown scope (impact)
- Keep historical record of the process.

# Questions

Q&A

- our slides: `http://www.slideshare.net/burguzbozo/`