HITB LAB: Identifying Threats in Raw Data Events: A Practical Approach for Enterprises

Vladimir Kropotov, Vitaly Chetvertakov, Fyodor Yarochkin
HITB 2014

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

October 16, 2014, Kuala-Lumpur
OUTLINE

Introduction

Criminology: case studies

Detection

Creating own IOCs

EOF
Overview

Introduction

Criminology: case studies

Detection

Creating own IOCs

EOF
LAB

our demo IP 100.123.7.111
Everyone is p0wn3d :)

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 thi
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.
**Statistic speaks**

- 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
Overview

Introduction

Criminology: case studies

Detection

Creating own IOCs

EOF
Forumology - what we can learn by following the trading forums.
Forumology - recent compromise signs

Date: - 01-09-2014
Forumology: targetted attack queries

13.08.2014, 18:51

Нужно получить доступ к определенным компам определенных сотрудников, нескольких организаций.
В наличие мыло, + можно найти профили на LinkedIn
По итогу надо получить доступ и управление удаленным компьютером
Готов платить, или предложить очень выгодное сотрудничество.
Страна Юса + офисы по всем странам..

Сообщение отредактировал gorx - 13.08.2014, 19:22
Forumology: obfuscation patterns

crypto, free service

```
https://cryptjs.com/panel/api

```
Forumology: sensitive data monetization
FORUMOLOGY: SOCIAL GROUPS BUYING REQUEST WITH LEAKED ATTRIBUTION IN SOCIAL NETWORK
Forumology: Google Play Apps Rating Manipulation

| 15.09.2014, 14:20 |

**dimmduh**

Продаю отзывы для платных android приложений

Продаю отзывы для ваших платных и бесплатных андройд приложений на google play.

5 звезд, отличный текст.

**Цена**

Бесплатные - $0.25 за отзыв
Платные - $1 за отзыв (это окончательная цена, цена приложения не важна).

Любой язык, текст сам придумываю или можно ваш.

**Оплата**

paypal - dimmduh@gmail.com
яндекс деньги - 41001666389160 (по текущему курсу)

**Работаю по предоплате**

Для неверующих и ожидающих кидка, можете заказать здесь https://www.fiverr.com/dimmduh/rate...aid-app-5-times или paypal, там всегда можно диспут открыть.

Для оперативной связи dimmduh@gmail.com

Работаю честно, открыто, качественно.
Forumology: shells and traffic w/o direct victims

Attribution

- priority sales to individuals with high forum reputation
- one hands only sale
- reachable trough following contact:

- Людям с отзывами/репутацией предоставляю доступы вперед
- Продаю в одни руки
- Показываю домены по контактам, указанным ниже

Контакты:
ICQ: 673160988
JID: fcntl@jabber.pl
## Campaigns

<table>
<thead>
<tr>
<th>Domain</th>
<th>Category</th>
<th>Campaign dates</th>
<th>Unique hosts/day</th>
</tr>
</thead>
<tbody>
<tr>
<td>ria.ru</td>
<td>news</td>
<td>Summer 2013 – Summer 2014</td>
<td>~ 1 600 000</td>
</tr>
<tr>
<td>rg.ru</td>
<td>news</td>
<td>Autumn 2013</td>
<td>~ 790 000</td>
</tr>
<tr>
<td>newsru.com</td>
<td>news</td>
<td>Winter 2013 – Spring 2014</td>
<td>~ 590 000</td>
</tr>
<tr>
<td>gazeta.ru</td>
<td>news</td>
<td>Spring 2013 - Autumn 2013</td>
<td>~ 490 000</td>
</tr>
<tr>
<td>aif.ru</td>
<td>news</td>
<td>Spring 2013 - Winter 2013</td>
<td>~ 330 000</td>
</tr>
<tr>
<td>mk.ru</td>
<td>news</td>
<td>Summer 2013 - Autumn 2013</td>
<td>~ 315 000</td>
</tr>
<tr>
<td>inosmi.ru</td>
<td>news</td>
<td>Summer 2014</td>
<td>~ 290 000</td>
</tr>
<tr>
<td>3dnews.ru</td>
<td>news</td>
<td>Winter 2013 – Summer 2014</td>
<td>~ 185 000</td>
</tr>
<tr>
<td>vz.ru</td>
<td>news</td>
<td>Winter 2013 – Summer 2014</td>
<td>~ 170 000</td>
</tr>
<tr>
<td>topnews.ru</td>
<td>news</td>
<td>Spring 2013 - Autumn 2013</td>
<td>~ 140 000</td>
</tr>
</tbody>
</table>
### Campaigns (2)

<table>
<thead>
<tr>
<th>Domain</th>
<th>category</th>
<th>When seen</th>
<th>unique hosts/day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Youtube.com</td>
<td></td>
<td>Summer 2013 - Winter 2014</td>
<td>Alexa N 3</td>
</tr>
<tr>
<td>mail.ru</td>
<td>email</td>
<td>Winter 2013 - Spring 2014</td>
<td>Alexa N 40</td>
</tr>
<tr>
<td>auto.ru</td>
<td>Autos</td>
<td>Summer 2014 - Autumn 2014</td>
<td>~320 000</td>
</tr>
<tr>
<td>soccer.ru</td>
<td>Sport</td>
<td>Winter 2014</td>
<td>~220 000</td>
</tr>
<tr>
<td>irr.ru</td>
<td>Ad Boards</td>
<td>Spring 2014 - Autumn 2014</td>
<td>~175 000</td>
</tr>
<tr>
<td>job.ru</td>
<td>HR</td>
<td>Autumn 2014</td>
<td>~140 000</td>
</tr>
<tr>
<td>glavbukh.ru</td>
<td>Accountants</td>
<td>Spring 2013 - Summer 2014</td>
<td>~70 000</td>
</tr>
<tr>
<td>hr-portal.ru</td>
<td>Finance / HR</td>
<td>Winter 2013 - Spring 2014</td>
<td>~55 000</td>
</tr>
<tr>
<td>tks.ru</td>
<td>Finance</td>
<td>Summer 2013 - Spring 2014</td>
<td>~38 000</td>
</tr>
<tr>
<td>Bankir.ru</td>
<td>Finance</td>
<td>Spring 2013 - Autumn 2014</td>
<td>~33 000</td>
</tr>
</tbody>
</table>
Intermediate victims, EDU and forums
INTERMEDIATE VICTIMS, FORUMS
**Intermediate victims, companies (1)**

[China Eastern Airlines Moscow office - Mozilla Firefox]

---

Introduction

Criminology: case studies

Detection

Creating own IOCs

EOF

---

Г. Москва, ул. Королев вал, д. 7, стр. 1
т.п. (495) 935-8828, факс. (495) 935-8829

http://www.flychinaeastern.com
INTERMEDIATE VICTIMS, COMPANIES (2)
Intermediate victims, companies (3)
Intermediate victims, companies (4)
Intermediate victims, companies (5)
INTERMEDIATE VICTIMS, COMPANIES (6)
Intermediate victims, regional gvt related(2)
INTERMEDIATE VICTIMS, REGIONAL GVT RELATED(3)
Intermediate victims, regional gvt related (4)
Intermediate victims, regional govt related (5)
Participants, other (mail delivery service)
Participants, other (anti debugging)
SEEN ON FORUM:

Google redirect:

Сервис р-р-редиректов через google.com/(.*)}, Трастовые, без рефа, https, 150$ за 30к

foxyle  ☻

10.07.2014, 01:27

Вы спрашивали "а можно через google, например?" - теперь, да, можно.

Предлагаю сервис редиректов, где каждый редик имеет вид
https://www.google.com/[а-zА-Я]{112}

Почему так, зачем так, зачем вообще?

Если сравнивать с классическим подходом "много редиков на неизвестном ломе", то у нас:
1) Лом для редиков обычно самый никчемный, перепроданный в десяток рук, никем не про
Participants, other, (known referrers...)
EK/malware serving hosts by country
Target victim traffic costs
**Case studies:**

- commercial crime
- not-monetary-profit oriented crime

Let's take a look at the first type:
Intermediate victims are target too, such as free DNS hostings:

- fbps.1403883.mar2.afraid.org
- ju7a.1403883.mar2.afraid.org
- wzet.1403883.mar2.afraid.org
- gatw.1403883.mar2.afraid.org
- kfzv.1403883.mar2.afraid.org
- oxdo.1403883.mar2.afraid.org
LEGIT DOMAIN ABUSE

domain: SCHOOLOPROS.RU
nserver: ns1.afraid.org.
nserver: ns2.afraid.org.
state: REGISTERED, DELEGATED, VERIFIED
org: LLC "GKShP"
registrar: RU–CENTER–REG–RIPN
admin–contact: https://www.nic.ru/whois
created: 2010.01.25
Domain rotation

http://www.residensea.jp/xuaioxc.php
http://firenzeviaroma.ru/dqryony.php
http://sphynxtoutnu.com/dnqaibb.php
http://www.icmjapan.co.jp/dgttcnm.php
http://www.controlseal.nl/yolelkx.php
http://ural.zz.mu/ledstsn.php
http://www.fotobit.pl/cpjjpeii.php
http://bgcarshop.com/tgghhvy.php
http://www.borkowski.org/fudbqrff.php
http://shop.babeta.ru/puthnkn.php
http://e-lustrate.us/mycbbni.php
http://notarypublicconcept.com/shfvtpx.php
http://www.stempelxpress.nl/vechoix.php
http://64.68.190.53/dqohago.php
http://likos.orweb.ru/oydochh.php
http://wap.warelex.com/parpkeu.php
**Domain rotation**

- over 500 compromised domains
- rotation once every 3 minutes
MALWARE HOSTING, ON LEGIT DOMAINS (STOLEN CREDITS, VULNS, ETC.)
MALWARE HOSTING ON LEGIT DOMAINS
MALWARE HOSTING ON LEGIT DOMAINS

**ZeuS Tracker :: C&C www.colegiuldeadministratie.ro**

The list below shows all ZeuS configs, ZeuS binaries, ZeuS dropzones and FakeURLs which are hosted on www.colegiuldeadministratie.ro.

### Live Information

<table>
<thead>
<tr>
<th>ZeuS C&amp;C:</th>
<th><a href="http://www.colegiuldeadministratie.ro">www.colegiuldeadministratie.ro</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware:</td>
<td>ZeuS</td>
</tr>
<tr>
<td>IP address:</td>
<td>0.36.01.215</td>
</tr>
<tr>
<td>Host status:</td>
<td>online</td>
</tr>
<tr>
<td>Uptime:</td>
<td>185:13:23</td>
</tr>
<tr>
<td>Hostname:</td>
<td>n/a</td>
</tr>
<tr>
<td>SSL:</td>
<td>EU4DE742</td>
</tr>
<tr>
<td>AS number:</td>
<td>35796</td>
</tr>
<tr>
<td>AS name:</td>
<td>ROHOSTWAY-AS HOSTWAY-ROMANIA SRL</td>
</tr>
<tr>
<td>Country:</td>
<td>Romania (RO)</td>
</tr>
<tr>
<td>Level:</td>
<td>2 (hijacked webserver)</td>
</tr>
<tr>
<td>Sponsoring registrar:</td>
<td>Net Design SRL</td>
</tr>
<tr>
<td>Nameserver(s):</td>
<td>ns1.apius.net</td>
</tr>
<tr>
<td>Date added:</td>
<td>2014-09-10</td>
</tr>
<tr>
<td>Last checked:</td>
<td>2014-09-18</td>
</tr>
<tr>
<td>Last updated:</td>
<td>never</td>
</tr>
<tr>
<td>BL status:</td>
<td>This host is being published on the ZeuS Blocklist!</td>
</tr>
</tbody>
</table>
MALWARE HOSTING ON LEGIT DOMAINS
MALWARE HOSTING ON LEGIT DOMAINS
MALWARE HOSTING ON LEGIT DOMAINS
MALWARE HOSTING ON LEGIT DOMAINS

Logiseek Inc. is a US Incorporated AutoCAD Drafting Company based in California.

Logiseek offers cutting-edge CAD drafting services at competitive prices. We can be your reliable partner by providing wide ranging CAD services, right from simple CAD design services to intricate Raster to Vector Conversion, 3D renderings and many more.

Being a leading provider, we have both skill and experience to handle offshore customers from different countries like US, UK, Europe etc. To meet clients’ requirements as per international standards, our team of talented professionals has successfully produced brilliant outputs within quick turnaround time. Our expertise lies in offering BIM Services also. The best thing, you can use our service to convert raster images into vector format effectively. Our raster to vector (R2V) services provides ultimate satisfaction for clients.

We can help you with

- **3D Modeling**
- **Cad Services**
- **Our Team**

Outsource your AutoCAD and CAD drafting projects

Logiseek combines state-of-art infrastructure and
Lurk Campaign

Historical overview

but actually lurk campaign is at least 3 years old. (and mainly targeting .ru IP ranges).
"For purposes of analysis, we selected two information resources which we knew had been used to distribute the malware— http://www.ria.ru/ (a major Russian news agency) and http://www.gazeta.ru/ (a popular online newspaper)." (http://securelist.com/blog/virus-watch/32383/a-unique-bodiless-bot-attacks-news-site-visitors-3/)

Intermediate victims:

- ria.ru
- gazeta.ru
**Lurk in 2011**

Intermediate victims:
- glavbukh.ru
- inosmi.ru
- ria.ru
- riarealty.ru
- ura.ru

<table>
<thead>
<tr>
<th>date</th>
<th>referrer</th>
<th>ip</th>
<th>url</th>
</tr>
</thead>
</table>
Other participants of Winter-Spring 2012 Campaign

Intermediate victims:
- banki.ru
- fas.gov.ru
- glavbukh.ru
- infox.ru
- ino.mn
- inosmi.ru
- klerk.ru
- newsru.com
- pravda.ru
- riarealty.ru
- slon.ru
- ura.ru
Lurk in the news and News distribute Lurk... (2)

Targeted web infections _ Nov 08 2012 (http://securelist.ru/blog/intsidenty/3546/targetirovanny-e-veb-zarazheniya-2/)

Intermediate victims:

- interfax.ru
- Vesti.ru
- gazeta.ru
- vz.ru
- ura.ru
**Timeline of Summer- Autumn 2012 -**

Intermediate victims:

<table>
<thead>
<tr>
<th>date</th>
<th>ref. dom</th>
<th>ip</th>
<th>port</th>
<th>method</th>
<th>url</th>
<th>apptype</th>
<th>bytes out/in</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/17/2012 12:29</td>
<td>3dnews.ru</td>
<td>207.182.136.150</td>
<td>80</td>
<td>GET</td>
<td><a href="http://jiujitrolam.info/2T4T">http://jiujitrolam.info/2T4T</a></td>
<td>text/html</td>
<td>290/58067</td>
</tr>
<tr>
<td>8/17/2012 12:29</td>
<td>rian.ru</td>
<td>207.182.136.150</td>
<td>80</td>
<td>GET</td>
<td><a href="http://jiujitrolam.info/2T4T">http://jiujitrolam.info/2T4T</a></td>
<td>text/html</td>
<td>535/4511</td>
</tr>
<tr>
<td>8/17/2012 13:38</td>
<td>tks.ru</td>
<td>207.182.136.150</td>
<td>80</td>
<td>GET</td>
<td><a href="http://jiujitrolam.info/2T4T">http://jiujitrolam.info/2T4T</a></td>
<td>text/html</td>
<td>370/5972</td>
</tr>
<tr>
<td>9/4/2012 14:16</td>
<td>3dnews.ru</td>
<td>91.216.163.76</td>
<td>80</td>
<td>GET</td>
<td><a href="http://kalmadrezant.info/7GIC">http://kalmadrezant.info/7GIC</a></td>
<td>text/html</td>
<td>339/56870</td>
</tr>
<tr>
<td>9/17/2012 12:50</td>
<td>tks.ru</td>
<td>184.22.165.170</td>
<td>80</td>
<td>GET</td>
<td><a href="http://responsesforemost.org/7GIC">http://responsesforemost.org/7GIC</a></td>
<td>text/html</td>
<td>668/58075</td>
</tr>
<tr>
<td>9/17/2012 13:38</td>
<td>slon.ru</td>
<td>184.22.165.170</td>
<td>80</td>
<td>GET</td>
<td><a href="http://responsesforemost.org/7GIC">http://responsesforemost.org/7GIC</a></td>
<td>text/html</td>
<td>728/194</td>
</tr>
<tr>
<td>9/18/2012 11:54</td>
<td>rian.ru</td>
<td>184.22.165.170</td>
<td>80</td>
<td>GET</td>
<td><a href="http://oggmoreripples.com/7GIC">http://oggmoreripples.com/7GIC</a></td>
<td>text/html</td>
<td>1160/194</td>
</tr>
<tr>
<td>10/10/2012 11:35</td>
<td>vesti.ru</td>
<td>91.121.152.84</td>
<td>80</td>
<td>GET</td>
<td><a href="http://deploypostsale.net/7GIC">http://deploypostsale.net/7GIC</a></td>
<td>text/html</td>
<td>722/58037</td>
</tr>
<tr>
<td>10/12/2012 13:34</td>
<td>gazeta.ru</td>
<td>91.121.152.84</td>
<td>80</td>
<td>GET</td>
<td><a href="http://personallymainframes.net/7GIC">http://personallymainframes.net/7GIC</a></td>
<td>text/html</td>
<td>618/58084</td>
</tr>
<tr>
<td>11/2/2012 14:12</td>
<td>vesti.ru</td>
<td>91.121.152.84</td>
<td>80</td>
<td>GET</td>
<td><a href="http://accuracyuploadonly.net/7GIC">http://accuracyuploadonly.net/7GIC</a></td>
<td>text/html</td>
<td>290/58078</td>
</tr>
</tbody>
</table>

(*) rian.ru + vesti.ru + gazeta.ru + newsru.com + 3dnews.ru + slon.ru > 4,000,000 uniq visitors per day...
CAMPAIN AUTUMN 2012 KNOCKING TO THE MASTER

Proof logs:

<table>
<thead>
<tr>
<th>date</th>
<th>ip</th>
<th>port</th>
<th>method</th>
<th>url</th>
</tr>
</thead>
</table>
Winter 2012-2013 Campaign

- new sigs ISOQ (old sigs 2T4T, 7GIC BVRQ)
- sploit 0ISOQjq
- payload 1ISOQjq
## STATS

<table>
<thead>
<tr>
<th>date</th>
<th>ref. dom</th>
<th>ip</th>
<th>port</th>
<th>method</th>
<th>url</th>
<th>apptype</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.01.2013 16:33</td>
<td>vesti.ru</td>
<td>64.79.67.220</td>
<td>80</td>
<td>GET</td>
<td><a href="http://cetapetrar.info/ISOQ">http://cetapetrar.info/ISOQ</a></td>
<td>text/html</td>
</tr>
<tr>
<td>28.01.2013 15:15</td>
<td>vz.ru</td>
<td>64.79.67.220</td>
<td>80</td>
<td>GET</td>
<td><a href="http://mgsinterviews.biz/ISOQ">http://mgsinterviews.biz/ISOQ</a></td>
<td>text/html</td>
</tr>
<tr>
<td>28.01.2013 15:15</td>
<td>-</td>
<td>64.79.67.220</td>
<td>80</td>
<td>GET</td>
<td><a href="http://mgsinterviews.biz/0ISOQjq">http://mgsinterviews.biz/0ISOQjq</a></td>
<td>application/java-archive</td>
</tr>
<tr>
<td>28.01.2013 15:15</td>
<td>vz.ru</td>
<td>208.110.73.74</td>
<td>80</td>
<td>GET</td>
<td><a href="http://ferpolokas.info/ISOQ">http://ferpolokas.info/ISOQ</a></td>
<td>text/html</td>
</tr>
<tr>
<td>08.02.2013 15:26</td>
<td>3dnews.ru</td>
<td>208.110.73.75</td>
<td>80</td>
<td>GET</td>
<td><a href="http://footmanage.info/XZAH">http://footmanage.info/XZAH</a></td>
<td>text/html</td>
</tr>
<tr>
<td>2/11/2013 16:22</td>
<td>vz.ru</td>
<td>208.110.73.75</td>
<td>80</td>
<td>GET</td>
<td><a href="http://croppingvietnam.biz/XZAH">http://croppingvietnam.biz/XZAH</a></td>
<td>text/html</td>
</tr>
<tr>
<td>19.02.2013 15:13</td>
<td>klerk.ru</td>
<td>208.110.73.75</td>
<td>80</td>
<td>GET</td>
<td><a href="http://interfacesfeaturelimited.org/XZAH">http://interfacesfeaturelimited.org/XZAH</a></td>
<td>text/html</td>
</tr>
<tr>
<td>2/20/2013 12:52</td>
<td>newsru.com</td>
<td>208.110.73.75</td>
<td>80</td>
<td>GET</td>
<td><a href="http://solvesautoplay.info/XZAH">http://solvesautoplay.info/XZAH</a></td>
<td>text/html</td>
</tr>
<tr>
<td>2/20/2013 12:52</td>
<td>-</td>
<td>208.110.73.75</td>
<td>80</td>
<td>GET</td>
<td><a href="http://solvesautoplay.info/0XZAHwj">http://solvesautoplay.info/0XZAHwj</a></td>
<td>application/java-archive</td>
</tr>
<tr>
<td>2/20/2013 12:52</td>
<td>-</td>
<td>208.110.73.75</td>
<td>80</td>
<td>GET</td>
<td><a href="http://solvesautoplay.info/1XZAHwj">http://solvesautoplay.info/1XZAHwj</a></td>
<td>application/octet-stream</td>
</tr>
<tr>
<td>20.02.2013 12:52</td>
<td>newsru.com</td>
<td>208.110.73.75</td>
<td>80</td>
<td>GET</td>
<td><a href="http://solvesautoplay.info/XZAH">http://solvesautoplay.info/XZAH</a></td>
<td>text/html</td>
</tr>
<tr>
<td>20.02.2013 13:22</td>
<td>vz.ru</td>
<td>208.110.73.75</td>
<td>80</td>
<td>GET</td>
<td><a href="http://solvesautoplay.info/XZAH">http://solvesautoplay.info/XZAH</a></td>
<td>text/html</td>
</tr>
<tr>
<td>20.02.2013 13:24</td>
<td>vesti.ru</td>
<td>208.110.73.75</td>
<td>80</td>
<td>GET</td>
<td><a href="http://solvesautoplay.info/XZAH">http://solvesautoplay.info/XZAH</a></td>
<td>text/html</td>
</tr>
<tr>
<td>3/5/2013 13:51</td>
<td>glavbukh.ru</td>
<td>208.110.73.75</td>
<td>80</td>
<td>GET</td>
<td><a href="http://birdsricher.info/XZAH">http://birdsricher.info/XZAH</a></td>
<td>text/html</td>
</tr>
<tr>
<td>3/6/2013 14:32</td>
<td>klerk.ru</td>
<td>74.82.203.10</td>
<td>80</td>
<td>GET</td>
<td><a href="http://comprisefuse.info/XZAH">http://comprisefuse.info/XZAH</a></td>
<td>text/html</td>
</tr>
</tbody>
</table>
**Summer 2013: Landing pattern change to "indexm.html"**

<table>
<thead>
<tr>
<th>date</th>
<th>ref. dom</th>
<th>ip</th>
<th>port</th>
<th>method</th>
<th>url</th>
<th>apptype</th>
<th>bytes out/in</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/Aug/2013:11:53</td>
<td>tks.ru</td>
<td>70.32.39.108</td>
<td>80</td>
<td>GET</td>
<td><a href="http://frilpertesemota.info/054RIwj">http://frilpertesemota.info/054RIwj</a></td>
<td>text/html</td>
<td>4999/0</td>
</tr>
<tr>
<td>03.09.2013 14:12</td>
<td>rg.ru</td>
<td>173.234.60.83</td>
<td>80</td>
<td>GET</td>
<td><a href="http://miopades.info/indexm.html">http://miopades.info/indexm.html</a></td>
<td>text/html</td>
<td>4134/613</td>
</tr>
<tr>
<td>9/20/2013 12:50</td>
<td>gazeta.ru</td>
<td>216.55.166.53</td>
<td>80</td>
<td>GET</td>
<td><a href="http://lpakuwiera.info/indexm.html">http://lpakuwiera.info/indexm.html</a></td>
<td>text/html</td>
<td>4134/613</td>
</tr>
</tbody>
</table>
Debugging of fingerprinting mechanism? Sep 2013

http://ljiartwbvsa.info/indexm.html
text/html

http://ljiartwbvsa.info/054RIdl
application/x-shockwave-flash

http://ljiartwbvsa.info/counter.php?t=f&v=win%202011,7,700,169&a=true
text/html

http://ljiartwbvsa.info/354Rcx
text/html

http://ljiartwbvsa.info/s.php?qt=null&fl=11,7,700,169&sw=null&ar=null&jv=null&sl=5,1,20513,0
text/html

http://ljiartwbvsa.info/054Rcx
## Fresh news from the field

<table>
<thead>
<tr>
<th>date</th>
<th>ref. dom</th>
<th>ip</th>
<th>port</th>
<th>method</th>
<th>url</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/1/2014 12:02</td>
<td>irr.ru</td>
<td>188.165.229.195</td>
<td>80</td>
<td>GET</td>
<td><a href="http://apobda.kiqpoltar2.in/indexm.html">http://apobda.kiqpoltar2.in/indexm.html</a></td>
</tr>
<tr>
<td>1/01/2014 16:54</td>
<td>bankir.ru</td>
<td>188.165.229.195</td>
<td>80</td>
<td>GET</td>
<td><a href="http://snkua.kiqpoltar2.in/indexm.html">http://snkua.kiqpoltar2.in/indexm.html</a></td>
</tr>
<tr>
<td>04/09/2014 12:03</td>
<td>auto.ru</td>
<td>188.165.229.195</td>
<td>80</td>
<td>GET</td>
<td><a href="http://snkua.kiqpoltar2.in/indexm.html">http://snkua.kiqpoltar2.in/indexm.html</a></td>
</tr>
<tr>
<td>04/09/2014 15:26</td>
<td>irr.ru</td>
<td>188.165.229.195</td>
<td>80</td>
<td>GET</td>
<td><a href="http://boreas.gohasellor.info/indexm.html">http://boreas.gohasellor.info/indexm.html</a></td>
</tr>
<tr>
<td>04/09/2014 15:26</td>
<td>irr.ru</td>
<td>188.165.229.195</td>
<td>80</td>
<td>GET</td>
<td><a href="http://boreas.gohasellor.info/3MSKMcx">http://boreas.gohasellor.info/3MSKMcx</a></td>
</tr>
<tr>
<td>04/09/2014 15:26</td>
<td>irr.ru</td>
<td>188.165.229.195</td>
<td>80</td>
<td>GET</td>
<td><a href="http://boreas.gohasellor.info/sxvutirwbfexedbjmqqn.html">http://boreas.gohasellor.info/sxvutirwbfexedbjmqqn.html</a></td>
</tr>
<tr>
<td>04/09/2014 15:56</td>
<td>job.ru</td>
<td>188.165.229.195</td>
<td>80</td>
<td>GET</td>
<td><a href="http://boreas.gohasellor.info/indexm.html">http://boreas.gohasellor.info/indexm.html</a></td>
</tr>
<tr>
<td>05/09/2014 15:46</td>
<td>bankir.ru</td>
<td>188.165.229.195</td>
<td>80</td>
<td>GET</td>
<td><a href="http://snkua.kiqpoltar2.in/indexm.html">http://snkua.kiqpoltar2.in/indexm.html</a></td>
</tr>
</tbody>
</table>
Mitigation experience and aftereffects

- Abusing hosting (you can lose the chain, criminals just pay $50 for other hosting)
- Abusing registrar
- Abusing DNS
- Forensic evidence collection and actor attribution
- Interaction with CERTs and Authorities
- Informing victims directly
MacOS botnet: a Kaiten variant in action

- Kaiten/Tsunami is an open-source irc-controlled DDoS bot
- Observed large infection of MacOS machines in Sept-2014 (starting on 02-09-2014)
- initial infection vector: yet unknown
- Observation: 2014-09-02 - now
- target - mainly .CN (mostly), TW
- small number in KR, NP, JP, MY
- iocs:

Executables:
cbf5a6d2fba422caa5913e48ef68a6ab
http://5.104.106.190/.../cores

98bb67d91476d8ac4e71d39c92564b3b
http://linux.microsoftwindowsupdate.org/poke.sh
IOCs

<table>
<thead>
<tr>
<th>Engine</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td>-</td>
</tr>
<tr>
<td>AegisLab</td>
<td>-</td>
</tr>
<tr>
<td>Agnitum</td>
<td>-</td>
</tr>
<tr>
<td>Avast</td>
<td>ELF:Tsunami-L [Tfj]</td>
</tr>
<tr>
<td>AVG</td>
<td>Linux/Tsunami2.M</td>
</tr>
<tr>
<td>Avira</td>
<td>MACOS/Tsunami.A</td>
</tr>
</tbody>
</table>

File information:

- 2014-09-04 16:33:54  0/55
- 2014-09-04 16:33:53  0/55
- 2014-09-09 15:01:49  21/54
- 2014-09-06 12:07:25  19/55
- 2014-09-07 03:33:47  19/55
- 2014-09-04 21:00:39  16/55
- 2014-09-03 18:36:20  11/50
IOCs

5.104.106.190
- eventuallydown.dyndns.biz
- fastfoodz.dlinkddns.com
- updates.dyndn-web.com

54.68.53.18
- flippinflops.dyndns.tv
Indicators

- Hosted on german IP and Amazon ec2. Hosts an IRC server, DNS server, Web server (used to wget new binaries/updates).
- controlled from an .il IP address

irc servers
192.31.186.4
85.214.45.208
- eichwalde.de
- hortbuntstifte.de
- channel #core
**Kaiten ops:**

- controlled by isee me@rox-9042F9E0.bb.netvision.net.il.
- PRIVMSGs commands, manipulates DNS resolver settings
Kaiten conclusions

- 18247 Unique IP addresses within 3 days
- 3k bots are simultaneously
- Botnet growth limited by IRC server stability
Targeted Campaigns

APT != STATE SPONSORED

- Q: Why so many APT-like activities out of .cn?
- A: A different market structure. (Data worth money)
APT ..?

Interesting correlations:

Kyrgyz president plays risky game with rail bargains

By Rustam Makhmudov Source: Global Times Published: 2014-2-24 19:23:01

Kyrgyz President Almazbek Atambayev recently radically changed his viewpoint on the China-Kyrgyzstan-Uzbekistan railway construction project. At a recent press conference, he said that this project doesn't meet the national interests of Kyrgyzstan.

Illustration: Liu Rui/GT

Submission permanent link 03042a7efbf02bf8bea0347411313330d94b64 (Received 2013-12-20 19:01:36, http://kg.ungov.org/mfa/jq.php?v=webhp)
**Bad guys in your net ;-)**

coming from a KR IP address (bounce), redirecting a shell to CHINANET

[Image of a terminal window showing a反弹SHELL example]
Overview

Introduction

Criminology: case studies

Detection

Creating own IOCs

EOF
Hands ON

- moloch

https://100.123.7.111:8005
user admin
password hitb2014
Detection: tools and techniques
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 (vm)

and our 0mq plugin

- yara
- hpfeeds https://github.com/rep/hpfeeds
- CIF https://github.com/collectiveintel/cif-v1
- https://github.com/STIXProject/-openioc-to-stix converter
- https://github.com/MISP/MISP - malware information sharing platform
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.

AV MODEL BROKEN
Why AV model is broken?
▶ AV detection/monitoring

http://viruscheckmate.com/id/0Byt539VwEcQ
**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>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>RasTls.exe</td>
</tr>
<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/

--<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/>
  <definition>
    --<indicator operator="OR" id="9c8df971-32a8-4ede-8a3a-c5cb2c1439c6">
      --<indicator operator="AND" id="0781258f-6960-4da5-97a0-ec35fb403cac">
        --<indicatorItem id="5045b63-35bf4ef9-f6ae-b2ba2980f80a" condition="contains">
          <context document="ProcessItem" search="ProcessItem/name" type="mir"/>
          <content type="string">winlogon.exe</content>
        </indicatorItem>
      </indicator>
      --<indicatorItem id="b05d9b40-0526-461f-9721-e31d5651abdc" condition="contains">
        <context document="ProcessItem" search="ProcessItem/HandleList/Handle/Type" type="mir"/>
        <content type="string">File</content>
      </indicatorItem>
    </indicator>
    --<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="fe11706-9eb3-469b-b30a-4047cbfa7436b" condition="contains">
        <context document="ProcessItem" search="ProcessItem/HandleList/Handle/Type" type="mir"/>
        <content type="string">\WINDOWS\system32\twext.exe</content>
      </indicatorItem>
    </indicator>
  </definition>
OpenIOCs

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–abeb–73656acb913e.ioc
c32b8af3–28d0–47d3–801f–a2c2b0129650.ioc
2bff223f–9e46–47a7–ac35–d35f8138a4c7.ioc
c71b3305–85e5–4d51–b07c–ff227181fb5a.ioc
2fc55747–6822–41d2–bcc1–387fc1b2e67b.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
7d2eaadf–a5ff–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)**

### News
- Class Materials Now Available for "STIX/TAXII Technical Colloquium" on May 19-20
- Registration Now Closed for "STIX/TAXII Technical Colloquium" on May 19-20
- STIX/TAXII Briefing at Secure 360 Conference
- STIX Version 1.1.1 Now Available
- "Characterizing Malware with MAEC and STIX" White Paper Now Available
- STIX Project Documentation Repository and New "STIX Idioms" Document Now Available on GitHub.com

### Status Report
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,LostTypeEnum=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 to 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', 't3f5y9a2bb3dl7z8gc4o6f.html', 'zf3z9lr6ac8di6r4kw2r0hu3ee8ad.html', 'rx3v'],
        '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']
                }
            }
        }
    }
}
Redirect (example)

http://mysimuran.ru/forum/kZsjOiDMFb/
http://agency.accordinga.pw/remain/unknown.html?mods=8&id=26
Redirect Example

{ '28001': {
  'step1': {
    'directories': ['forum', 'kZsjOiDMFb', 'epygFrFsoU'],
    'arguments': [],
    'files': [''],
    'ip': ['89.111.178.33'],
    'domains': ['mysimuran.ru']},
  'step2': {
    'directories': ['forum', 'kZsjOiDMFb', 'epygFrFsoU', 'kJXshWOMNC'],
    'arguments': ['4231', '7697', '9741'],
    'files': ['js.js', 'cnt.html'],
    'ip': ['89.111.178.33'],
    'domains': ['mysimuran.ru']},
  'step3': {
    'directories': [],
    'arguments': ['i', 'g', 'x'],
    'files': ['hit'],
    'ip': ['89.184.81.35'],
    'domains': ['c.hit.ua']},
  'step4': {
    'directories': ['d1x', '3', '87475b26a521024ce78d7ea73164140a', 'd36eb1fc80ebe9df515d043be1557f57'],
    'arguments': [],
    'files': ['http%3A%2F%2Fagency.accordinga.pw%2Fremain%2Funknown.html%3Fmods%3D8%3Did%3D26', 'http%3A%2F%2Fstruck.looked.africa'],
    'ip': ['46.254.1.209'],
    'domains': ['f-wake.browser-checks.info', 'a-oprzay.browser-checks.pw']}
}
Sourcing External IOCs

- feeds (with scrappers):
**Sourcing External IOCs**

- feed your scrappers:
  - http://malc0de.com/database/
  - https://reputation.alienvault.com/reputation.data...
- VT intelligence

```
rule zero0day
{
  strings:
    $d = "Media.Sound()"
    $dz = "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
HPfeeds, HPfriends and more
HPFeeds Architecture
**HPFeeds API in nutshell:**

```python
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))
```
HPFEEDS INTEGRATION

Welcome to HoneyMap. This is a BETA version! Bug reports welcome :-)  
Note that this is not ALL honeypots of the Honeynet Project, 
only those who voluntarily publish their captures to hpfeeds!

Connection to back-end established
NTP probe collector

```
93.180.5.26:33751 - 2014-05-21 22:04:08.405660
Received 1 packets
Connected from (80.82.64.217, 7678)
NTP scan: 80.82.64.217:7678 - 2014-05-22 01:45:00.678146
INFO:hpfeed:msg:  NTP scan: 80.82.64.217:7678 - 2014-05-22 01:45:00.678146
packet: FwADKgAAAAAAAAAA
NTP scan: 80.82.64.217:7678 - 2014-05-22 01:45:00.679273
INFO:hpfeed:msg:  NTP scan: 80.82.64.217:7678 - 2014-05-22 01:45:00.679273
Received 1 packets
Connected from (93.180.5.26, 55054)
packet: FwADKgAAAAAAA=
Received 1 packets
Connected from (184.105.139.72, 39510)
packet: FgIAAQAAAAAAAA
Version scan
```
HPFeeds and honeymap
Applying IOCs to your detection process

detect detecting moloch moloch moloch :)
Tools for Dynamic Detection of IOC

- Snort
- Yara + yara-enabled tools
- Moloch
- Splunk/Log search
- roll-your-own:p
Moloch

Moloch is awesome:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Src IP/Port: 140.109.221.47:473</td>
<td>TWN</td>
<td>53</td>
<td>68.95.1:53</td>
</tr>
<tr>
<td>Packets</td>
<td>Bytes</td>
<td>Node</td>
<td>Info</td>
</tr>
<tr>
<td>10000</td>
<td>731.919 / 811.919 moloch</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tags: dns:class=IN, dns:type=A, node:moloch, protocols=udp,

DNS

Hosts: 
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/
IOC MAP

iocmap

Indicator of Compromise Mapping Service

Introduction

iocmap is Indicator of Compromise Mapping platform to facilitate Dynamic Threat Intelligence process within an organization.

The main purpose of the project is to provide a service to aim Incident Response Process with fast process of:

- Performing individual IOC characteristic mapping to known/existing Indicators of Compromise. The input can be provided in form of an IP address, a hash, a URL, a process of executable name, and so on.

The output of indicators of compromise can be produced in form of: ..* snort rule(s) ..* Yara rule(s) ..* OpenIOC documents ..* CyBOX ..* Esper rule(s)

- Performing lookup of IOC indicators within raw data sets, such as passiveDNS mappings, passive HTTP traffic, splunk logs, ElasticSearch stored logs and so on.

- Facilitating IOC sharing and implementing IOC sharing policies.
MISP

- https://github.com/MISP
Tools for Dynamic Detection

- Moloch
  - Moloch supports Yara (IOCs 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/

```clojure
(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)
```
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=true

http://liapolasens.info/354R1cx

http://liapolasens.info/054R1cx

What to do?
Investigating using known IOCs

- Investigating Static host based IOCs
- Investigating Dynamic host based IOCs
- Investigating Static network IOCs
- Investigating Dynamic network IOCs
analyzing HTTP traffic

- User agents
- suspicious domains
- static analysis of HTTP headers
Analyzing AV logs

Analyzing AV logs
## Analyzing AV logs

![VirusTotal screenshot]

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet</td>
<td>W32/Shiz.NCF!tr</td>
<td>20131031</td>
</tr>
<tr>
<td>GData</td>
<td>Trojan.Generic.9527504</td>
<td>20131031</td>
</tr>
<tr>
<td>Ikarus</td>
<td>Win32.Refeys</td>
<td>20131031</td>
</tr>
<tr>
<td>Jiangmin</td>
<td></td>
<td>20131031</td>
</tr>
<tr>
<td>K7AntiVirus</td>
<td>Riskware</td>
<td>20131031</td>
</tr>
<tr>
<td>K7GW</td>
<td>Riskware</td>
<td>20131031</td>
</tr>
<tr>
<td>Kaspersky</td>
<td></td>
<td>20131031</td>
</tr>
<tr>
<td>Kingsoft</td>
<td>Win32.Troj.Generic.a.(kcloud)</td>
<td>20130829</td>
</tr>
</tbody>
</table>
# Analyzing AV Logs

[www.virustotal.com](http://www.virustotal.com/en/file/deeee11c34a55901e368db3a715419ae886a33be3f504fd1203076b6eeb625)

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commtouch</td>
<td></td>
</tr>
<tr>
<td>Comodo</td>
<td>UnclassifiedMalware</td>
</tr>
<tr>
<td>DrWeb</td>
<td>Java.Downloader.936</td>
</tr>
<tr>
<td>Emsisoft</td>
<td></td>
</tr>
<tr>
<td>ESET-NOD32</td>
<td>a variant of Java/Exploit.Agent.POO</td>
</tr>
<tr>
<td>F-Prot</td>
<td></td>
</tr>
<tr>
<td>F-Secure</td>
<td></td>
</tr>
<tr>
<td>Fortinet</td>
<td>Java/Agent.POO/Exploit</td>
</tr>
<tr>
<td>GData</td>
<td></td>
</tr>
<tr>
<td>Ikarus</td>
<td></td>
</tr>
<tr>
<td>Jiangmin</td>
<td></td>
</tr>
</tbody>
</table>
## Analyzing AV logs

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Threat Type</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet</td>
<td>W32/Shiz.NCFItr</td>
<td>20130814</td>
</tr>
<tr>
<td>GData</td>
<td>-</td>
<td>20130814</td>
</tr>
<tr>
<td>Ikarus</td>
<td>-</td>
<td>20130814</td>
</tr>
<tr>
<td>Jiangmin</td>
<td>Win32/Virut.bn</td>
<td>20130814</td>
</tr>
<tr>
<td>K7AntiVirus</td>
<td>-</td>
<td>20130813</td>
</tr>
<tr>
<td>K7GW</td>
<td>-</td>
<td>20130813</td>
</tr>
<tr>
<td>Kaspersky</td>
<td>UDS:DangerousObject.Multi.Generic</td>
<td>20130814</td>
</tr>
</tbody>
</table>
Overview

Introduction

Criminology: case studies

Detection

Creating own IOCs
Creating host based IOCs

hashes, mutexes, threatexpert
Use YARA, or tune your own tools

```
rule susp_params_in_url_kind_of_fileless_bot_drive_by
{
    meta:
    date = "oct 2013"
    description1 = "JavaSploit://jdatastorelame.info/054RIw:j:j:j"

    strings:
    $string0 = "http"
    $string1 = "indexm.html"
    $string2 = "054RI"

    condition:
    all of them
}
```
Use Snort to catch suspicious traffic:

# many plugX deployments connect to google DNS when not in use
alert tcp !$DNS_SERVERS any → 8.8.8.8 53 (msg:"APT possible PlugX Google DNS TCP port 53 connection attempt"; classtype:misc−activity; sid:50000112; rev:1;);
GRR: Google Rapid Response:

http://code.google.com/p/grr/

Hunting IOC artifacts with GRR
GRR: Creating rules
GRR: HUNT IN PROGRESS
Honeypots

Learn about attacker as much as you can:

▶ What language does the attacker understand?
▶ What is the attacker keyboard layout?
▶ What tools the attacker uses?
▶ Where those are hosted?
▶ Who are the targets?
▶ Client software information (kippo -> ssh client)
Honeypots

plenty of hosting urls, DDoS targets in hp logs
DNS: Detection

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

<table>
<thead>
<tr>
<th>domain</th>
<th>ip</th>
<th>owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>rtvwerjyuver.com</td>
<td>69.164.203.105</td>
<td>linode</td>
</tr>
<tr>
<td>tvrstrynyvwwstrtve.com</td>
<td>109.74.196.143</td>
<td>linode</td>
</tr>
<tr>
<td>cu3007133.wfaxyqykxh.ru</td>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>

what does your DNS traffic look like..?
DNS viz01
DNS anonymizer traffic

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 - ##.##.##.## - nbxxe33tnbuxsslwnn2xg.mjuxultvme.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - nbxxe33tnbuxsslwnn2xg.mjuxultvme.dd34.ru
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.nruxmlkn52xe3tbnqxgg33n.dd34.ru
8/13/2014 9:59:15 PM - ##.##.##.## - obuwg4y.nruxmlkn52xe3tbnqxgg33n.dd34.ru
8/13/2014 9:59:15 PM - ##.##.##.## - 0s.o53xo.mzqwgzlcn5xwwltdn5wq.dd34.ru
8/13/2014 9:59:15 PM - ##.##.##.## - 0s.o53xo.mzqwgzlcn5xwwltdn5wq.dd34.ru

Time: Today 09:59:15pm

Description: Phishing.bpwh
Confidence Level: High
Covert channel communication

8/13/2014  5:49:04 PM – x.x.x.x –  5141017.mtdtzwdhc.mdgtrammdgtrmmmmdx

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

<table>
<thead>
<tr>
<th>Email</th>
<th><a href="mailto:thomas@spenglers.biz">thomas@spenglers.biz</a> is associated with ~93,134 domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrant Org</td>
<td>Domain Administrator was found in ~4,350,091 other domains</td>
</tr>
<tr>
<td>Dates</td>
<td>Created on 2014-06-30 - Expires on 2015-06-29</td>
</tr>
<tr>
<td>Domain Status</td>
<td>Registered And No Website</td>
</tr>
<tr>
<td>Whois History</td>
<td>1 record has been archived since 2014-07-02</td>
</tr>
<tr>
<td>Hosting History</td>
<td>1 change on 2 unique name servers over 0 year</td>
</tr>
<tr>
<td>Whois Server</td>
<td>whois.biz</td>
</tr>
</tbody>
</table>
Sinkhole in DNS

Credit: domaintools.com

<table>
<thead>
<tr>
<th>Email</th>
<th><a href="mailto:abuse@bigrock.com">abuse@bigrock.com</a> is associated with ~265,970 domains <a href="mailto:gregorygofr@yahoo.com">gregorygofr@yahoo.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrar</td>
<td>BIGROCK SOLUTIONS LIMITED</td>
</tr>
<tr>
<td>Registrar Status</td>
<td>clientTransferProhibited</td>
</tr>
<tr>
<td>Dates</td>
<td>Created on 2011-06-26 - Expires on 2015-06-26 - Updated on 2014-06-25</td>
</tr>
<tr>
<td>Name Server(s)</td>
<td>NS1.SUSPENDED-DOMIAN.COM (has 306 domains) NS2.SUSPENDED-DOMIAN.COM (has 306 domains)</td>
</tr>
<tr>
<td>IP Address</td>
<td>69.164.203.105 - 81 other sites hosted on this server</td>
</tr>
<tr>
<td>IP Location</td>
<td>- Texas - Dallas - Linode</td>
</tr>
<tr>
<td>Domain Status</td>
<td>Registered And Active Website</td>
</tr>
<tr>
<td>Whois History</td>
<td>30 records have been archived since 2011-06-27</td>
</tr>
</tbody>
</table>
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:Bert Lathrop
contact:Company:Farsight Security, Inc
contact:Street-Address:11400 La Honda Rd
Look for holes :)
## Hole Traffic

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Source IP</th>
<th>Port</th>
<th>Type</th>
<th>Byte Count</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Source Country</th>
<th>Annotation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014/08/07</td>
<td>12:15:38</td>
<td>2258</td>
<td>80</td>
<td>7</td>
<td>180 / 590</td>
<td>TCP</td>
<td>7</td>
<td>moloch</td>
<td>USA</td>
<td></td>
</tr>
<tr>
<td>2014/08/07</td>
<td>12:15:44</td>
<td>2502</td>
<td>80</td>
<td>7</td>
<td>180 / 590</td>
<td>TCP</td>
<td>7</td>
<td>moloch</td>
<td>USA</td>
<td></td>
</tr>
<tr>
<td>2014/08/07</td>
<td>12:16:03</td>
<td>3018</td>
<td>80</td>
<td>7</td>
<td>180 / 590</td>
<td>TCP</td>
<td>7</td>
<td>moloch</td>
<td>USA</td>
<td></td>
</tr>
<tr>
<td>2014/08/07</td>
<td>12:16:58</td>
<td>1227</td>
<td>80</td>
<td>7</td>
<td>180 / 590</td>
<td>TCP</td>
<td>7</td>
<td>moloch</td>
<td>USA</td>
<td></td>
</tr>
<tr>
<td>2014/08/07</td>
<td>12:16:58</td>
<td>1229</td>
<td>80</td>
<td>6</td>
<td>156 / 512</td>
<td>TCP</td>
<td>7</td>
<td>moloch</td>
<td>USA</td>
<td></td>
</tr>
<tr>
<td>2014/08/07</td>
<td>12:17:06</td>
<td>1481</td>
<td>80</td>
<td>7</td>
<td>180 / 590</td>
<td>TCP</td>
<td>7</td>
<td>moloch</td>
<td>USA</td>
<td></td>
</tr>
<tr>
<td>2014/08/07</td>
<td>12:17:29</td>
<td>2253</td>
<td>80</td>
<td>7</td>
<td>180 / 590</td>
<td>TCP</td>
<td>7</td>
<td>moloch</td>
<td>USA</td>
<td></td>
</tr>
</tbody>
</table>
**Categorizing Incidents**

It is extremely important to be able to categorize your incidents or threats. There are multiple data sources that could be used to do so.
CATAGORIZATION BASED ON PUBLIC SOURCES

[tbd]
CATAGORIZATION BASED ON HISTORICAL DATA

[tbd]
Categorization based on cross source correlation

- Visualizing the Threats
- Filtering noisy extras
- Making decisions
OVERVIEW

Introduction

Criminology: case studies

Detection

Creating own IOCs

EOF
Questions

@fygrave @vbkropotov @vitalychetvertakov
And answers :)

EOF