



VIRUS TRACKER

CHALLENGES OF RUNNING A LARGE SCALE SINKHOLE OPERATION

Kleissner & Associates
Botconf'14, 3–5 Dec 2014, Nancy/France

About

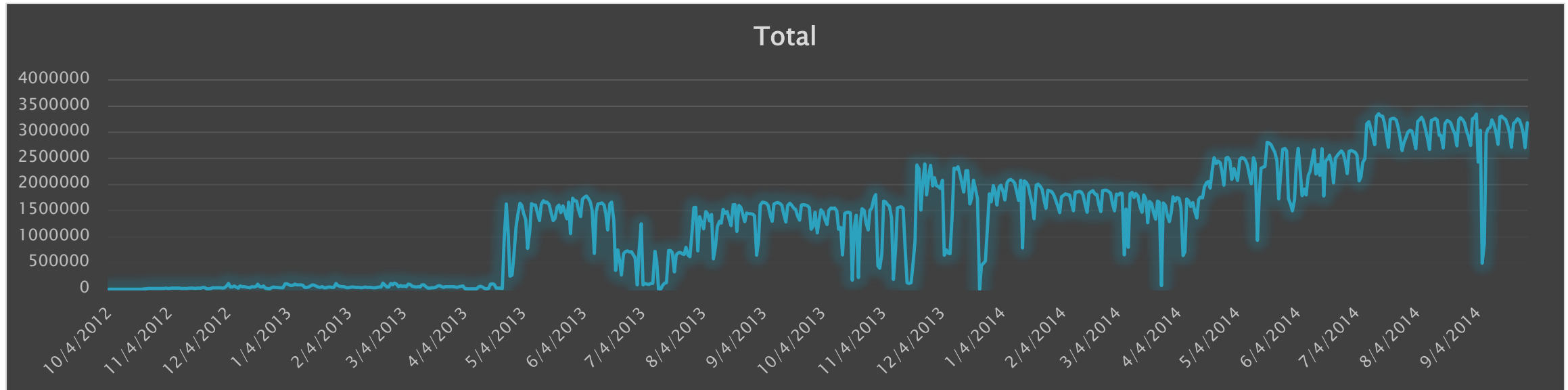
- Worlds largest botnet monitoring system
- Since September 2012
- Originally just to watch banking Trojans, but now we have:
 - Stuxnet and many other APTs in the system
 - A lot banking Trojans and major botnets
 - P2P Crawlers for all major P2P botnets

Objectives:

- Generating statistics such as size, geographical distribution on long-term
- Detecting changes/movements
- Alerting infected organizations

Statistics

- More than 1 billion infection records in our database!
- 3.3 million unique infected machines per day
- More than 7.000 sinkholed domains



Challenges we are facing

- Takedown of our domains
 - For example FBI seized Zeus Gameover domains
 - Microsoft seized Citadel/Zeus domains
- Complaints
 - People mistakenly report our servers and domains as malicious C&Cs
 - -> Appearing on blocklists, domains get suspended
- Cost of domains, average 7.3 USD per domain
 - Adds up when registering hundreds of domains
 - Domains are not always available to register

Challenges we are facing

- Scaling – quite some data!
 - How and what to store, filter it? (with a small budget!)
 - How to inform everyone?
- Different types of botnets
 - HTTP/HTTPS, custom TCP protocols, P2P protocols, IRC..
 - Different protocols and ports used
 - Sometimes no detailed info on the botnets are available
 - Mobile ones – NAT issues, how to calculate unique infections
 - Reversing all DGAs takes time
- Low budget!
 - Only limited resources in terms of time, money, servers etc

Challenges we are facing

- Finding new domains to sinkhole
 - For P2P botnets: Finding initial peers
 - Manual analysis is time consuming
 - Using 3rd party data sources such as ThreatExpert, TotalHash, VirusTotal helps a lot
- IP to geodata correlation
 - Not 100% accurate data, IP ranges get reassigned all the time
 - Very often only telecom provider known – who is really infected?
- Legal considerations
 - Complying with data privacy laws
- Anti-sinkholing techniques: Blacklisting, ddos

The solutions

1. Automate all the things!

1. 100% automated domain registration (including a domain catching system)
2. 100% automated classification of the data
3. 100% automated distribution of the data

2. Create your own distribution network to warn of infections

1. Cooperate with CERTs
2. Security companies
3. Other researchers
(similar to the what Shadowserver Foundation did already)

Data privacy?

- We only store public meta-info!
- No HTTP POST information is analyzed or recorded
- Basically only storing what we really need
 - Kleissner & Associates is the sinkholing company with the most strict data privacy policies!
- Opt-out possibility for providers upon prove of IP range ownership

False positive detection?

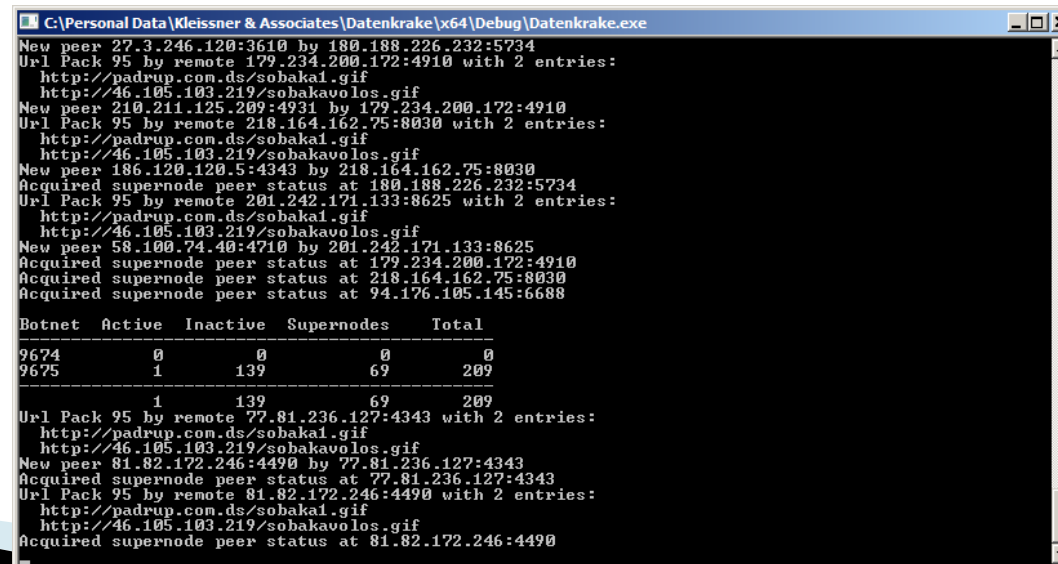
- False positive detection of infection records generated by:
 - Search bots like Googlebot
 - Researchers visiting manually the C&C URL
 - Bots that search for vulnerable admin panels
 - Domain checkers like DomainTools, Websense
 - Online sandboxes/analyzer systems
- Detection via:
 - User Agent
 - Requested Document Path (vs expected one)
 - IP blacklist of known analyzers/bots
- That is especially important for botnets with low infection counts like all APTs!

Massive data?

- Actually storing only the relevant information
- Generating other info (like GeoIP data) on the fly when exporting the data
- Only 1 request per infection per day
- Pregenerating files based on country and day
- Having a nice Windows application to quickly download those packages and analyze it further
- Also providing filters for direct download to reduce the amount of data

P2P Crawlers we wrote

- ZeroAccess 1, ZeroAccess 2, ZeuS Gameover, Sality
- All written from scratch in native C/C++
- Often difficult to finding initial peers
 - Old samples have old inactive embedded peer lists
 - Port scanning can help
 - Or asking other researchers who have active crawlers



```
C:\Personal Data\Kleissner & Associates\Datenkrake\x64\Debug\Datenkrake.exe
New peer 27.3.246.120:3610 by 180.188.226.232:5734
Url Pack 95 by remote 179.234.200.172:4910 with 2 entries:
  http://padrup.com.ds/sobakal.gif
  http://46.105.103.219/sobakavolos.gif
New peer 210.211.125.209:4931 by 179.234.200.172:4910
Url Pack 95 by remote 218.164.162.75:8030 with 2 entries:
  http://padrup.com.ds/sobakal.gif
  http://46.105.103.219/sobakavolos.gif
New peer 186.120.120.5:4343 by 218.164.162.75:8030
Acquired supernode peer status at 180.188.226.232:5734
Url Pack 95 by remote 201.242.171.133:8625 with 2 entries:
  http://padrup.com.ds/sobakal.gif
  http://46.105.103.219/sobakavolos.gif
New peer 58.100.74.40:4710 by 201.242.171.133:8625
Acquired supernode peer status at 179.234.200.172:4910
Acquired supernode peer status at 218.164.162.75:8030
Acquired supernode peer status at 94.176.105.145:6688

Botnet Active Inactive Supernodes Total
9674 0 0 0 0
9675 1 139 69 209
-----
1 139 69 209
Url Pack 95 by remote 77.81.236.127:4343 with 2 entries:
  http://padrup.com.ds/sobakal.gif
  http://46.105.103.219/sobakavolos.gif
New peer 81.82.172.246:4490 by 77.81.236.127:4343
Acquired supernode peer status at 77.81.236.127:4343
Url Pack 95 by remote 81.82.172.246:4490 with 2 entries:
  http://padrup.com.ds/sobakal.gif
  http://46.105.103.219/sobakavolos.gif
Acquired supernode peer status at 81.82.172.246:4490
```

P2P Crawlers we wrote

- Distributed crawlers on multiple geographic locations
- On those locations the crawlers run on one physical machine
- Can handle up to 1 million infections at the same time!
 - Every peer is re-contacted within 10 minutes latest
 - After 1 million peers things are getting slow (network stack exhausted, no available TCP ports, router dislikes tens of thousand concurrent connections as well)
- Windows is awesome!
 - You can set all relevant TCP/socket limits via the API
 - The network stack handles huge traffic really well

P2P Crawlers

Statistics from 4/23/2014:

Botnet	Version	Network / Port	Active	Inactive	Supernode	Total unique infections
ZeroAccess	1	21810	1	0	0	1
		21860	3589	193	85	3867
		22292	7537	534	296	8367
		25700	3978	241	173	4392
		34354	5812	1643	377	7832
		34355	0	0	0	0
		All together	20917	2611	931	24459
	2	16470	55325	16977	3301	75603
		16471	62865	18039	7284	88188
		16464	155400	18259	13990	187649
		16465	66986	14186	3675	84847
		All together	340576	67461	28250	436287
ZeuS Gameover		1028	10	63856	9468	73334
Sality	3	9674	557531	269	4254	562054
	4	9675	117368	193	567	118128
		All together	674899	462	4821	680182
All P2P Botnets						1.214.262 infections

Anti P2P Crawling

Making your life more difficult, ZeuS Gameover:

- To contact a peer you need to know the IP, port and the bot id (20 byte identifier). The bot id is a SHA-1 generated out of the computer name + volume GUID of the first hard disk.
- ZeuS uses random ports, that's why you cannot use port scanning to detect possible infections
- Packets are encrypted (RC4) using the receivers bot id. Without the id you cannot decrypt the packet.
- IDSes cannot make signatures over the packet, as contents, port and size always change. Each packet has a random amount of random bytes appended to randomize the packet.
- Fallback to DGA if no update within 7 days over P2P network (peer list isolation prevention)
- Internal peer list is limited to netmask 255.255.255.128 per entry (IP poisoning prevention)
- Blacklist of subnets in configuration + dynamic blacklist to limit connections to 10 packets/minute.
- Peers only return peers that are xor-nearest to you (to your bot id). So no matter if you contact 10 peers, or 100.000 peers you are likely to always get about the same "neighbour" peers. Because every peer knows you with your bot ID and uses it to encrypt the packet, you cannot simply change it.
- ZeuS GO stores only the internal RC4 keystate => no extraction of the original key

DGA Domain Prediction

1. Some bots use a domain generation algorithm (DGA), here ZeuS Gameover:

```
DNS 102 standard query A euf62bw118168kvjzo51118i35dwlthspylxeq.com
DNS 175 standard query response, No such name
DNS 101 standard query A d30m59muhtgrjugzb58buizk47o41jwouizfu.biz
DNS 163 standard query response, No such name
DNS 99 standard query A gwk37h24pvgtaqnr1u1tp42dsjwcynuhshr.org
```

2. If you know the algorithm, you can predict the domains:

```
11/26/2014,sfthuwrrindskx2gcub1jrayzf.com
11/26/2014,sbltajwonifp12f1xbr1uyhvnd.net
11/26/2014,1g9vqo0vkc18261nn915gmb7u.biz
11/26/2014,go4swb7j8hp41e1dfgsg26d.org
11/26/2014,3as5c7fdevgx373khg1sv07d9.com
11/26/2014,1bwvr5avo237d1p5u76v11m14zf.net
11/26/2014,1vxdeuk589hye5nxtfq1cfy3gv.org
11/26/2014,1wz1ky61aesqhi59rvoroip0q4.net
```

3. And sinkhole them in advance! (below example shows Sinowal sinkholes)

```
Date,Domain,Valid,IP,Owner
11/26/2014,gxwvshhb.com,Weekly,108.61.18.43,Sinkhole by German company
11/26/2014,gxwvshhb.net,Weekly,69.195.129.69,Sinkhole by K&A
```



Anti-sinkholing techniques

Playing the devil's advocate:

Domains:

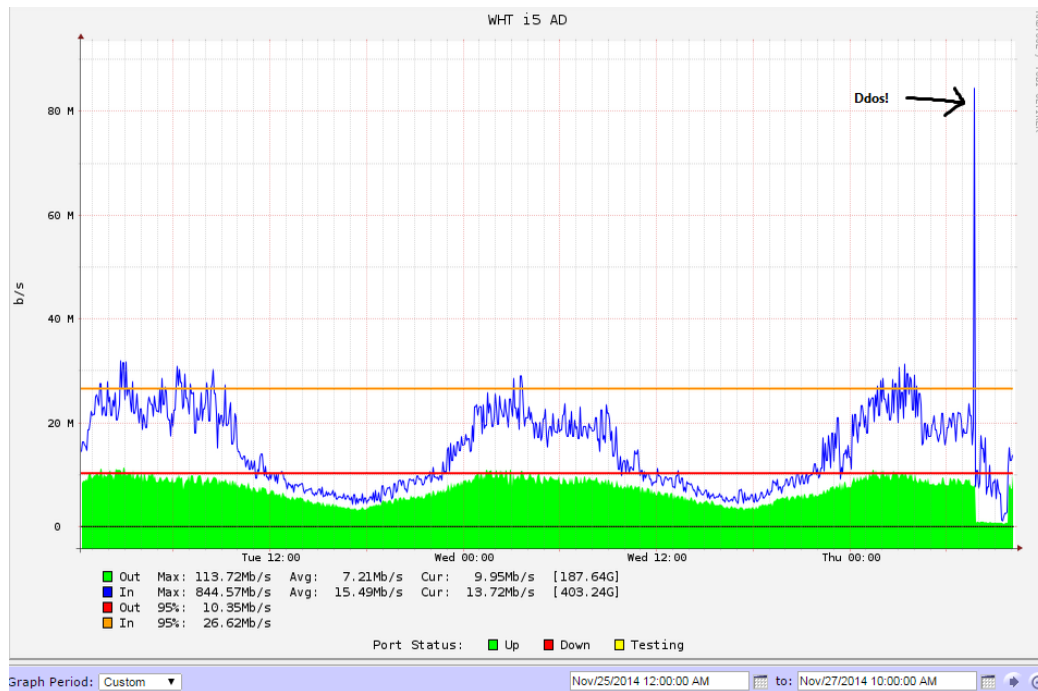
- Blacklisting the sinkhole server domains or IPs (MultiBanker & Sinowal did it)
- Identifying fingerprints in the HTTP header: "X-Sinkhole: malware-sinkhole"

Peer 2 Peer Networks:

- Applying limitations on IPs
- Bot id limitations, tie the bot ids to the IPs; use them like DHT/Kademlia
- Using strong cryptography
- Keeping bot reputations and backup lists

Anti-sinkholing techniques

1 Gbps ddos on 11/27/2014, mixed ICMP / UDP / TCP ddos:



Top 10 flows by bits per second for dst IP: 69.195.129.70

Duration	Proto	Src IP Addr	Src Pt	Dst Pt	Packets	pps	bps
0.067	UDP	178.78.246.45	53	62933	2048	30567	370.2 M
0.008	TCP	[redacted]	54245	80	2048	255999	281.6 M
101.264	UDP	204.145.94.87	47446	80	16.4 M	161794	119.1 M
0.019	ICMP	94.203.140.192	5	0.1	3072	161684	90.5 M
0.340	UDP	178.47.45.22	53	62933	2048	6023	73.0 M
98.668	UDP	209.119.225.25	53	12162	421888	4275	51.8 M
179.829	UDP	162.249.122.2	53	12162	753664	4191	50.8 M
98.318	UDP	209.122.107.49	53	12162	411648	4186	50.7 M
98.282	UDP	80.73.1.1	53	12162	387072	3938	47.7 M
97.400	UDP	216.174.102.25	53	12162	367616	3774	45.7 M

Sinkholing example: Stuxnet



Indicator of compromise

Domain Name: **TODAYSFUTBOL.COM**

Registry Domain ID: 1888818278_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.dynadot.com

Registrar URL: <http://www.dynadot.com>

Updated Date: 2014-05-05T18:11:15.0Z

Creation Date: 2013-10-09T18:50:52.0Z

Registrar Registration Expiration Date: 2014-10-09T18:50:52.0Z

Registrar: DYNADOT LLC

Registrar IANA ID: 472

Registrar Abuse Contact Email: abuse@dynadot.com

Registrar Abuse Contact Phone: +1.6502620100

Domain Status: clientTransferProhibited

Registry Registrant ID:

Registrant Name: Authorized Representative

Registrant Organization: Kleissner & Associates s.r.o.

Registrant Street: Na Strizi 1702/63

Registrant City: Praha

Registrant Postal Code: 140 00

Registrant Country: CZ

Registrant Phone: +420.000000000

Registrant Email: domains@virustracker.info



Data analysis: Stuxnet



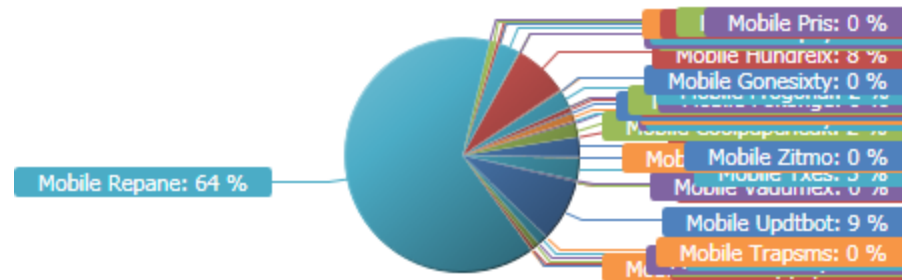
Date ▲	Organization	Botnet	IP	Country ▼	City	User Agent
2013-10-09 20:57:55	Mobinnet WIMAX Network	Stuxnet	5.52.2	Iran, Islamic Republic of		Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Media Center PC 3.0; .NET CLR 1....
2013-10-10 08:58:28	Farahoosh Dena	Stuxnet	94.74	Iran, Islamic Republic of		Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2013-10-10 09:53:04	Iran Telecommunication Compa...	Stuxnet	5.238	Iran, Islamic Republic of		Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CL...
2013-10-11 10:43:19	Information Technology Compan...	Stuxnet	2.178	Iran, Islamic Republic of		Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
2013-10-13 07:38:11	telecommunication of sistan& ba...	Stuxnet	2.181	Iran, Islamic Republic of	Sistan	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.2)
2013-10-13 13:31:11	Static-Pool-TC	Stuxnet	91.98	Iran, Islamic Republic of	Pars	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2013-10-13 13:32:47	Toyserkan Azad University	Stuxnet	217.2	Iran, Islamic Republic of	Azad	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50...
2013-10-13 16:14:43	Static-Pool-TC	Stuxnet	91.98	Iran, Islamic Republic of	Pars	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; AskTbPTV2/5.12.2.16749; M...
2013-10-14 09:00:19	Parsonline	Stuxnet	188.2	Iran, Islamic Republic of	Pars	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2013-11-21 07:22:20	Information Technology Compan...	Stuxnet	2.178	Iran, Islamic Republic of		Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
2013-11-25 12:42:20	Parsonline	Stuxnet	82.99	Iran, Islamic Republic of	Pars	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; AskTbPTV2/5.12.2.16749; M...
2013-11-25 17:02:52	Iran Telecommunication Compa...	Stuxnet	5.238	Iran, Islamic Republic of		Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2013-11-28 10:10:59	SHATEL DSL Network	Stuxnet	94.18	Iran, Islamic Republic of		Mozilla/5.0 (Windows NT 6.1; rv:25.0) Gecko/20100101 Firefox/25.0
2013-12-16 08:04:12	Telecommunication Company of...	Stuxnet	5.234	Iran, Islamic Republic of		Mozilla/5.0 (Windows NT 6.2; rv:25.0) Gecko/20100101 Firefox/25.0 AlexaToolbar/pof...
2013-12-16 20:52:53	Behkoush Rayaneh Afzar Co.	Stuxnet	89.18	Iran, Islamic Republic of		Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

Live analysis of the data following now!



Mobile Botnets

- 33 Android botnets
 - 1-co Symbian botnet with the same C&C!
- 2 Symbian botnets
- 3 Blackberry botnets
- Statistics from 10/8/2014, 14.077 infections total:



Percentage	Absolute	Trojan
63.74	9271	Mobile Repane
8.59	1250	Mobile Updtbot
7.53	1095	Mobile Hundreix
3.01	438	Mobile Yxes
2.89	421	Mobile Kranxpay
2.54	369	Mobile Adrd
2.49	362	Mobile Frogonal

Percentage	Absolute	Trojan
21.7	3055	China
20.46	2880	Russian Federation
15.56	2190	Ukraine
3.86	543	Poland
3.29	463	Venezuela
1.8	253	Iran, Islamic Republic of

Mobile Botnets



Data sent by Mobile Botnets

Often sent by the malware to the C&C:

- IMEI, an unique identifier number of the device
- IMSI, the SIM card identifier
- MSISDN, the telephone number
- SIM operator number
- MAC addresses
- Screen size
- Device model information
- OS and version number

In rare cases the OS or provider adds HTTP fields w/ sensitive data too!

Data sent by Mobile Botnets

Example infection 183.9.187.237 belonging to China Telecom Guangdong with Mobile Stinitier from 2014-08-14 03:01:16:

User Agent:

Dalvik/1.6.0 (Linux; U; Android 4.1.2; HUAWEI Y321-C00 Build/HuaweiY321-C00)

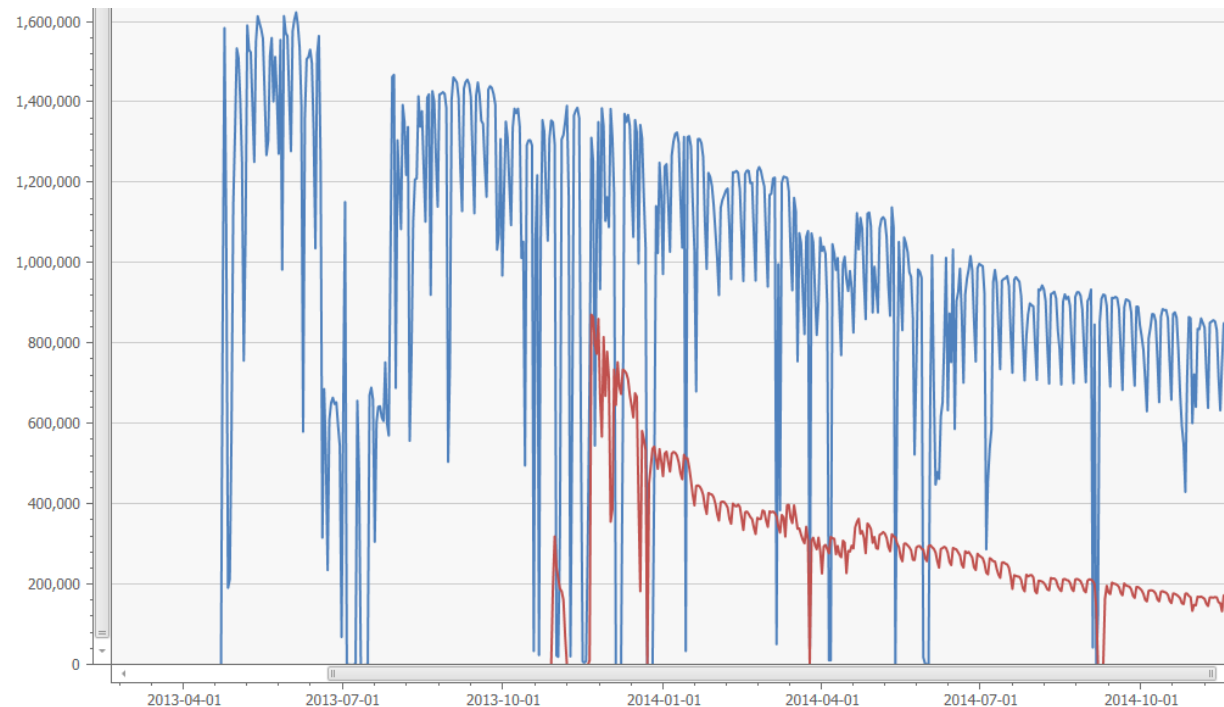
GET request via www.vhunjie.com (= our sinkhole):

/packageApplication/getAppFile/ReportInstallStatus.do?channel_id=35&app_id=48&imei=A000004994B46E&imsi=460036251675324&wifimac=90:4e:2b:d9:67:da&screen_size=480x800&version=1.0.0&model=HUAWEIY321-C00&platform=4.1.2&phone_number=13800138000&os=Android



Dying botnets?

- Abandoned after takedown or media attention
- Conficker (blue), ZeroAccess (red), ...
- Roughly 8% decrease every month



How to make sense of sinkhole data at scale?

- Need the ability to filter, sort and correlate the data
- Run reports on data (for further distribution)
- Generate graphs and visualization
- Quick lookups of IPs / IP ranges
- Our solution: A nice tool that does those jobs

LIVE DEMO

Thanks for attending the presentation! Questions?

For any information please contact:

Email info@kleissner.org

Address Na strži 1702/65
140 00 Praha
Czech Republic

© 2014 Kleissner & Associates s.r.o.

