Data Mining for Fun and Profit:

Building an Historical Database of Adversary Information

John Bambenek, Threat Research Team, Fidelis Cybersecurity

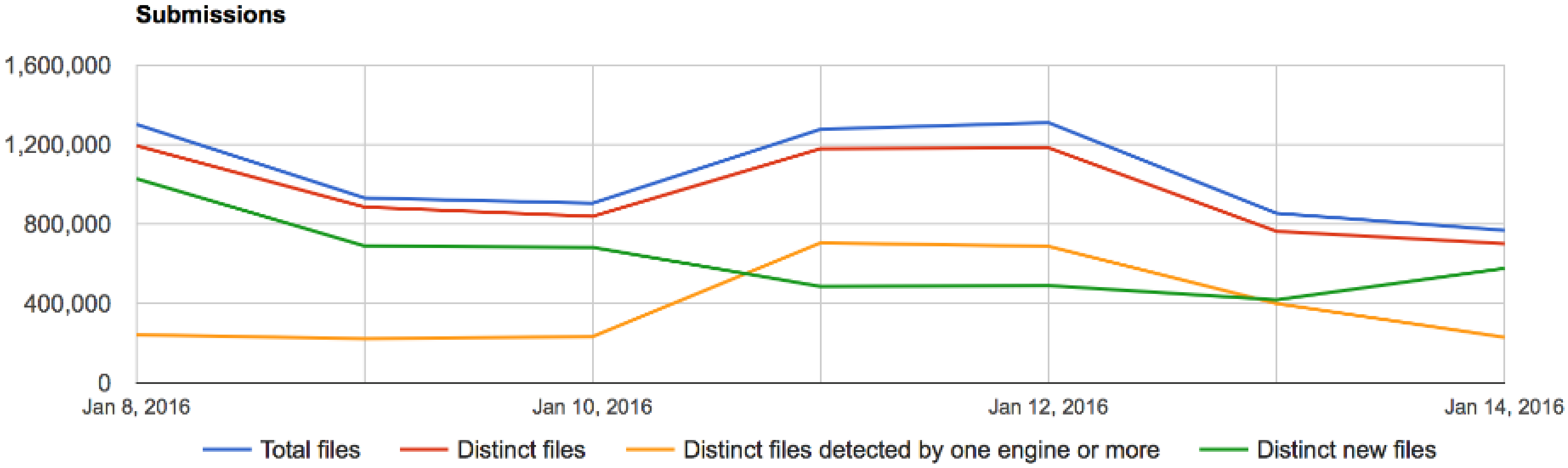
SANS Threat Intelligence Summit, 2016

Introduction

- Threat Instigator with Fidelis Cybersecurity
- CS Faculty at the University of Illinois
- Producer of open-source intelligence feeds
- Run several takedown-oriented groups for various malware families

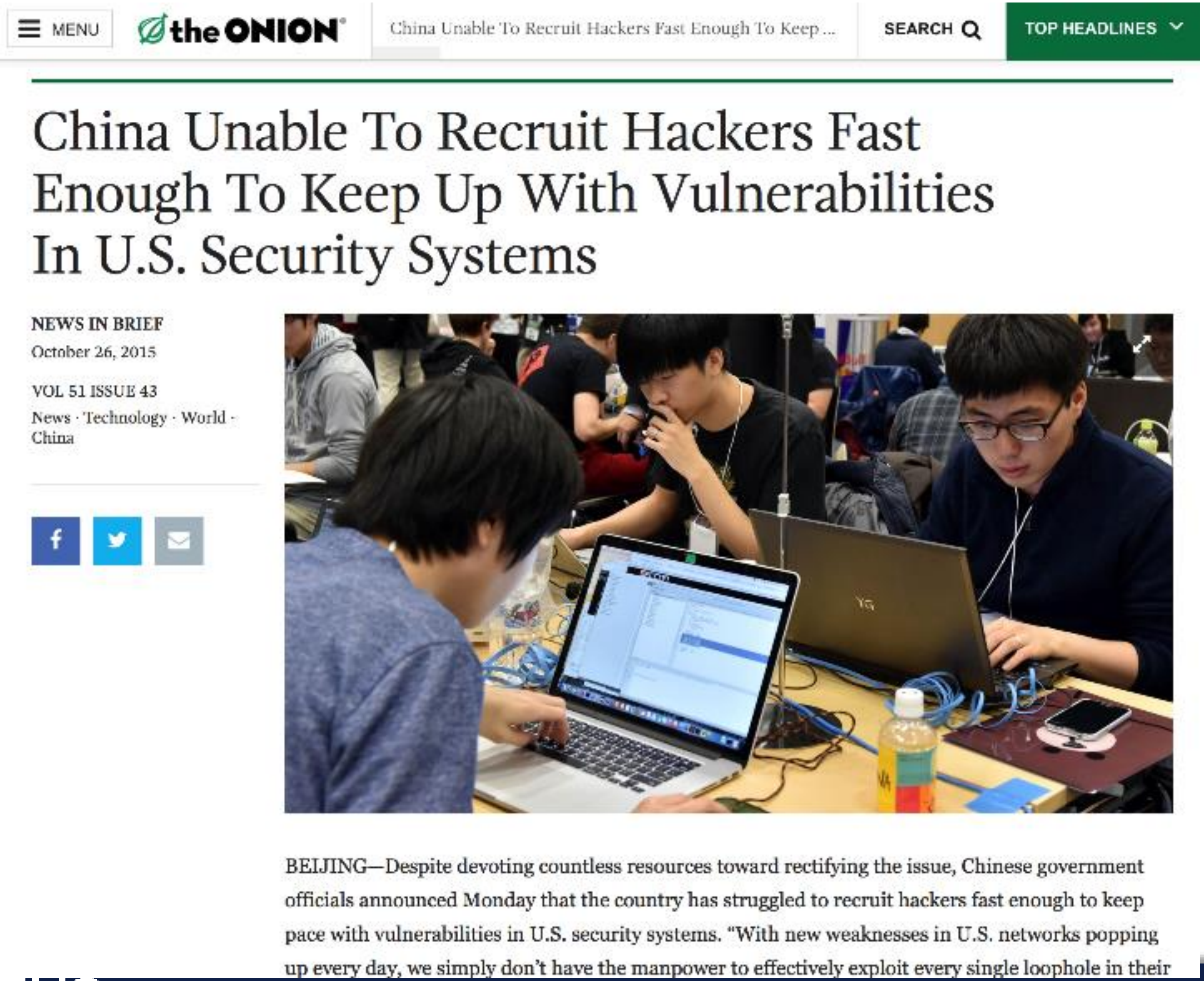
Shorter Version

The Problem… Illustrated



Virustotal Statistics taken at Jan 16, 2016

TL;DR



China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems

NEWS IN BRIEF

October 26, 2015

VOL 51 ISSUE 43

News · Technology · World · China

BEIJING—Despite devoting countless resources toward rectifying the issue, Chinese government officials announced Monday that the country has struggled to recruit hackers fast enough to keep pace with vulnerabilities in U.S. security systems. "With new weaknesses in U.S. networks popping up every day, we simply don't have the manpower to effectively exploit every single loophole in their

TL;DR

Bad News: We’re Doomed

Good News: Unlimited Job Security

Threat hunting

- Lots of talk about hunting threats in your network, but…

- The threats keep coming…
  - Good for vendors, bad for enterprises.

I prefer to hunt the attackers…

My intelligence objective

- I prefer to run operations designed to end a given threat and hopefully put someone in prison.

- This creates intelligence biases that are important to note.
  - i.e. Direct operationalization of data has issues that need resolved.

- Sources of data are external to a given enterprise
  - But we'll use internal sources too and so should you.

Putting the Intelligence back in Threat Intel

- Information is a set of unprocessed data that may or may not contain actionable intelligence.

- Intelligence is the art of critically examining information to draw meaningful and actionable conclusions based on observations and information.

- Involves analyzing adversary capabilities, intentions and motivations.

- Problem: Threat intel is sold based on quantity, not quality. Intel is hard and takes time.

How to win at VC…

- VirusTotal generally has C2 information (assuming sample runs).
- If vt > 1/55 then dump all network info, apply whitelist (maybe), call it a threat intel feed….
- Collect your $50 million in VC funding.
- Create pew-pew map.
- Apply logo.

How to not suck

- Point-in-time data is of limited use.
  - Data can “expire”
  - Can’t derive any context
  - Can’t determine motivations, capabilities
  - Can’t forecast off a data point

- Need to know when data is no longer any good?
  - Domains suspended
  - Hosting companies clean up compromised sites
  - Infrastructure changes

Two case studies

- Data mining malware
  - Can process about 30 families (many decoders open source)
  - Can correlate off configuration items to find related campaigns

- DGA surveillance
  - Currently running DGA feeds, running for over 2 years
  - Bulk resolving of all domains for information

What can you do with malware configs?

- In fullness of time, I plan to provide a feed to LE and CERTs for remediation.
- Sinkholing for victim notification is a possibility.
- Mining the data for correlations.
- Mine historical database for indicators that didn’t seem important at the time but became important later.

Open source magic sauce…

- https://github.com/kevthehermit/RATDecoders by Kevin Breen
- Python scripts that will *statically* rip configurations out of ~three dozen different flavors of RATs.
- Actively developed and you can see in action at malwareconfig.com
- Most malware has artifacts and many can be recovered statically.

Malware Sources

- VirusTotal
- MSFT VIA Program
- Other malware sharing programs
- Your own spam **IMPORTANT**
- In total, I process upwards of .25 TB a day
- If you have malware you want to trade, let’s talk.

Malware Configs

- Every malware family has different configurable items.

- Not every configuration item is necessarily valuable for intelligence purposes, some items may have default values.

- Free-form text fields provide interesting data that may be useful for correlation.

- Mutex can be useful for correlating binaries to the same actor.

Sample DarkComet config

```
Key: CampaignID         Value: Guest16
Key: Domains      Value: 06059600929.ddns.net:1234
Key: FTPHost      Value:
Key: FTPKeyLogs         Value:
Key: FTPPassword        Value:
Key: FTPPort      Value:
Key: FTPRoot      Value:
Key: FTPSize      Value:
Key: FTPUserName        Value:
Key: FireWallBypass     Value: 0
Key: Gencode      Value: 3yHVnheK6eDm
Key: Mutex        Value: DC_MUTEX-W45NCJ6
Key: OfflineKeylogger   Value: 1
Key: Password     Value:
Key: Version      Value: #KCMDDC51#
```

Sample njRat config

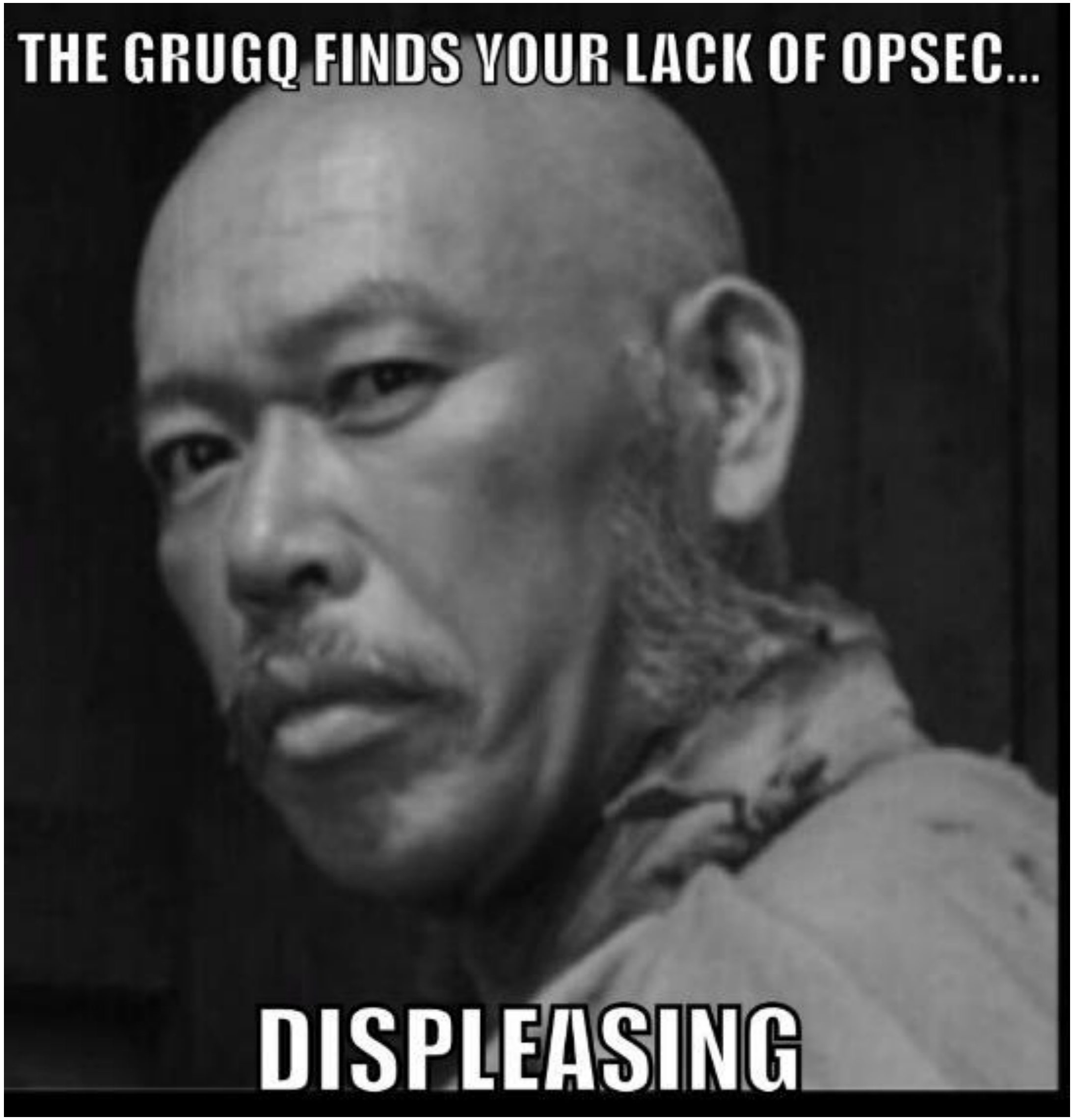
Key: Campaign ID   Value: 1111111111111111111
Key: Domain Value: apolo47.ddns.net
Key: Install Dir   Value: UserProfile
Key: Install Flag   Value: False
Key: Install Name   Value: svchost.exe
Key: Network Separator   Value: |'|'|
Key: Port   Value: 1177
Key: Registry Value Value:
5d5e3c1b562e3a75dc95740a35744ad0
Key: version   Value: 0.6.4

Sample Output

```
0739b6a1bc018a842b87dcb95a73248d3842c5de,150213,Dark Comet
Config,Guest16,lolikhebjegehackt.ddns
.net,1604,o1o5GgYr8yBB,DC_MUTEX-4E844NR

0745a4278793542d15bbdbe3e1f9eb8691e8b4fb,150213,Dark Comet
Config,Guest16,ayhan313.noip.me,1604
,aWUZabkXJRte,DC_MUTEX-TX61KQS

07540d2b4d8bd83e9ba43b2e5d9a2578677cba20,150213,Dark Comet Config,FUDDDDD,bilalsidd43.no-
ip.biz,
204.95.99.66,1604,qZYsyVu0kMpS,DC_MUTEX-8VK1Q5N

07560860bc1d58822db871492ea1aa56f120191a,150213,Dark Comet Config,Victim,cutedna.no-
ip.biz,1604
,sfAEjh4m1lQ7,DC_MUTEX-F2T2XKC

07998ff3d00d232b6f35db69ee5a549da11e96d1,150213,Dark Comet Config,test1,192.116.50.238,90,4A
2xbJmSqvuc,DC_MUTEX-F54S21D

07ac914bdb5b4cda59715df8421ec1adfaa79cc7,150213,Dark Comet
Config,Guest16,alkozor.ddns.net,31.13
2.106.94,1604,1.ekspert60.z8.ru,######60,######2012,zwd8tEC0F0tA,DC_MUTEX-W3VUKQN
```

NOTE – Redacted entries are username and password for FTP drop for

OPSEC? What OPSEC?



Dark Comet Campaign IDs

11510 Guest16	40 Slave	18 KURBAN	12 Admin
1563	36 Hack	18 BITS	12 111
Guest16_min	36 DOS	16 lol	11 victime
924	34 Guest17	16 Victime	11 NEW
125 Kurban	32 DC	15 Rat	11 Facebook
108 All	31 HACKED	15 HACK	10 svchost
102 HF	27 Steam	15 Bot	10 new
100 Hacked	27 RAT	14 vitima	10 hacker
96 No-IP	26 server	14 hak	10 Vitimas
95 test	26 Server	14 VK	10 USER
84 Col334	24 hack	14 Solis	10 Trolld
58 Guest1	23 all	14 LOL	10 Testing
53 kurban	23 DarkComet	13 user	10 TestGuest
51 Victim	23 BOT	13 slave	10 Skype
51 Test	22 darkcomet	13 CSGO	10 Omegle
49 User	21 Hacker	12 hot	10 Minecraft
48 Guest	20 hacked	12 TEST	10 LucidsVictim
47 Vitima	20 123	12 HACKER	10 Infected
46 1	18 PC	12 Gurban	10 Guest15

Sometimes interesting things come up

- JSocket Unique Campaign IDs by count

418 JSocket (DEFAULT)

6 order

6 lion

6 amendmentcopy

3 ThePunisher

3 August24rdBombing

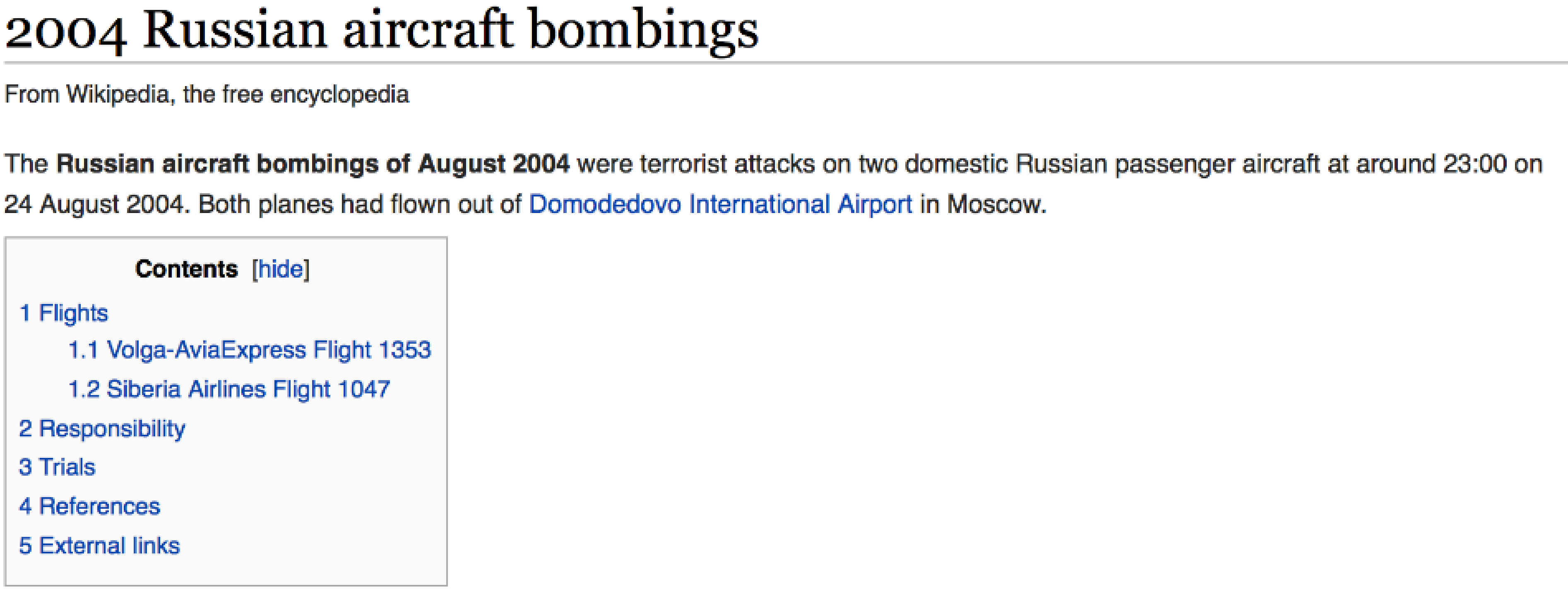
2 quotation

2 onlyali

2 festus

2 admi

Sometimes interesting things come up



2004 Russian aircraft bombings

From Wikipedia, the free encyclopedia

The **Russian aircraft bombings of August 2004** were terrorist attacks on two domestic Russian passenger aircraft at around 23:00 on 24 August 2004. Both planes had flown out of Domodedovo International Airport in Moscow.

Contents [hide]

Digging deeper

```
,1,1,2015-08-10
06:31:43,nikresut015js.zapto.org,true,fqLw1v,wcnLIxbslsn,Fresh_Bomb,COpaNxwcFs5,UOStKe,AugustBombing,vt,lykYQ,L0ZQqgmCGJ4,
2014,5,true,true,{PLUGIN_EXTENSION: lykYQ, JAR_NAME: Fresh_Bomb, INSTALL: true, JAR_EXTENSION: fqLw1v
,1,1,2015-07-02
09:52:30,nikresut015js.zapto.org,true,qSFai7,NfK3deVgu9o,1stJulyBombing,M1mDo7Mh4VF,gVJ0uD,JSocket,vt,SBVUC,aVCrh3IPVFP,2014
,5,true,true,{PLUGIN_EXTENSION: SBVUC, JAR_NAME: 1stJulyBombing, INSTALL: true, JAR_EXTENSION: qSFai7
,2015-09-03 17:55:59,nikresut015js.zapto.org,,vt,2014,{PLUGIN_EXTENSION: lykYQ, JAR_NAME: Fresh_Bomb, INSTALL: true,
JAR_EXTENSION: fqLw1v, times_submitted: 1, DELAY_CONNECT: 1, run_date: 2015-09-04, SECURITY_TIMES: 5, VBOX: true, Date: 2015-
09-03 17:55:59, JRE_FOLDER: UOStKe, sha256: 422fc0d4c7286db9b16fe86fb420e255de96a88bc4b316af96060894cb548913,
PLUGIN_FOLDER: L0ZQqgmCGJ4, unique_sources: 1, JAR_FOLDER: wcnLIxbslsn, JAR_REGISTRY: COpaNxwcFs5, NICKNAME:
Sep3rdtBombing,
,2015-09-02 05:27:06,nikresut015js.zapto.org,,vt,2014,{PLUGIN_EXTENSION: lykYQ, JAR_NAME: Fresh_Bomb, INSTALL: true,
JAR_EXTENSION: fqLw1v, times_submitted: 2, DELAY_CONNECT: 1, run_date: 2015-09-03, SECURITY_TIMES: 5, VBOX: true, Date: 2015-
09-02 05:27:06, JRE_FOLDER: UOStKe, sha256: be0f6903b3217c8df94c69dc0ea58ee1c07e92ab563bc4015f1a49a1dcf99acf,
PLUGIN_FOLDER: L0ZQqgmCGJ4, unique_sources: 1, JAR_FOLDER: wcnLIxbslsn, JAR_REGISTRY: COpaNxwcFs5, NICKNAME:
August24rdBombing
,2015-09-02 05:23:35,nikresut015js.zapto.org,,vt,2014,{PLUGIN_EXTENSION: lykYQ, JAR_NAME: Fresh_Bomb, INSTALL: true,
JAR_EXTENSION: fqLw1v, times_submitted: 1, DELAY_CONNECT: 1, run_date: 2015-09-03, SECURITY_TIMES: 5, VBOX: true, Date: 2015-
09-02 05:23:35, JRE_FOLDER: UOStKe, sha256: a985f8803080c8308d6850de4be9a9f096f7733ca1f98c14074b65be1051447f,
PLUGIN_FOLDER: L0ZQqgmCGJ4, unique_sources: 1, JAR_FOLDER: wcnLIxbslsn, JAR_REGISTRY: COpaNxwcFs5, NICKNAME:
August24rdBombing
,2015-09-02 01:15:43,nikresut015js.zapto.org,,vt,2014,{PLUGIN_EXTENSION: lykYQ, JAR_NAME: Fresh_Bomb, INSTALL: true,
JAR_EXTENSION: fqLw1v, times_submitted: 1, DELAY_CONNECT: 1, run_date: 2015-09-03, SECURITY_TIMES: 5, VBOX: true, Date: 2015-
09-02 01:15:43, JRE_FOLDER: UOStKe, sha256: 2723bfc312cb05b4f5d8460286e18c1834381a6d216e95ab22ef779ce5150ad2,
PLUGIN_FOLDER: L0ZQqgmCGJ4, unique_sources: 1, JAR_FOLDER: wcnLIxbslsn, JAR_REGISTRY: COpaNxwcFs5, NICKNAME:
August24rdBombing
,1,1,2015-07-02
09:52:30,nikresut015js.zapto.org,true,qSFai7,NfK3deVgu9o,1stJulyBombing,M1mDo7Mh4VF,gVJ0uD,JSocket,vt,SBVUC,aVCrh3IPVFP,2014
,5,true,true,{PLUGIN_EXTENSION: SBVUC, JAR_NAME: 1stJulyBombing, INSTALL: true, JAR_EXTENSION: qSFai7, times_submitted: 2,
DELAY_CONNECT: 1, run_date: 2015-08-19, SECURITY_TIMES: 5, VBOX: true, Date: 2015-07-02 09:52:30, JRE_FOLDER: gVJ0uD,
sha256: d448763f6f2b1e6fab1d00a2e87d6f88d6706853b6078b97d72518fb5c07afa3, PLUGIN_FOLDER: aVCrh3IPVFP, unique_sources: 2,
JAR_FOLDER: NfK3deVgu9o, JAR_REGISTRY: M1mDo7Mh4VF, NICKNAME: JSocket
```

Digging deeper

```
host nikresut015js.zapto.org
nikresut015js.zapto.org has address 50.7.199.164

30058   | 50.7.199.164     | 50.7.192.0/19       | US | arin     |
2010-10-18 | FDCSERVERS - FDCservers.net,US

RRset results for nikresut015js.zapto.org/ANY

bailiwick          zapto.org.
count   11
first seen         2015-09-30 00:24:21 -0000
last seen          2015-10-08 11:37:34 -0000
nikresut015js.zapto.org.         A         50.7.199.164
```

Digging deeper

- What’s the biggest byproduct of Big Data?
- Despite the ominous name, likely no connection to the bombing on 24 August.
- Without further review, marketing may have spun up a new “APT campaign” blog post.
- Just as important to have a large historical dataset to create and correlate backwards is the ability to prove an initial conclusion is wrong.

Correlating with Mutexes

- Some malware families randomly generate a mutex via the builder. Needed to prevent multiple copies of the same malware from running.

- 1867 ***MUTEX***
- 755 Pluguin
- 445 DC_MUTEX-F54S21D
- ……
- 26 DC_MUTEX-KT2FTNQ
- 23 DC_MUTEX-R0FHB8M
- 20 E4JR7ST81TYT8U
- 18 DC_MUTEX-V76C9X6
- 18 ***CryptoSuite***
- 17 DC_MUTEX-CNAFSEW
- 16 DC_MUTEX-RJ62AL7
- **16 DC_MUTEX-1FBMSBT**

Correlating with Mutexes

```
# grep "DC_MUTEX-1FBMSBT" fullratdump.csv | awk -F "," '{print $3,$5,$7}’
```

```
DOS 12/12/15 20:46 asdssaaassss.ddns.net
DOS 12/9/15 18:03 91.225.73.26
DOS 11/28/15 17:07 46.119.218.223
DOS 11/14/15 16:11 46.119.218.223
DOS 11/14/15 11:48 46.119.227.6
DOS 11/13/15 12:59 46.119.227.6
DOS 11/3/15 13:10 134.249.20.28
DOS 11/2/15 2:50 134.249.20.28
DOS 11/1/15 15:53 134.249.20.28
DOS 9/30/15 2:01 sattorov.ddns.net
DOS 9/13/15 19:19 aleksej-morozov.noip.me
 8/18/15 6:38 pingvin.ddns.net
DOS 8/5/15 16:39 draken.zapto.org
DOS 7/23/15 9:18 zhbrcbnhfh.no-ip.org
DOS 7/15/15 10:17 test777test.ddns.net
DOS 7/7/15 8:31 5.248.21.138
```

The Ashley Madison Correlation Trick

- Password can authenticate victim and server, so often they change less even when other settings change. Unique password by count with PoisonIvy:

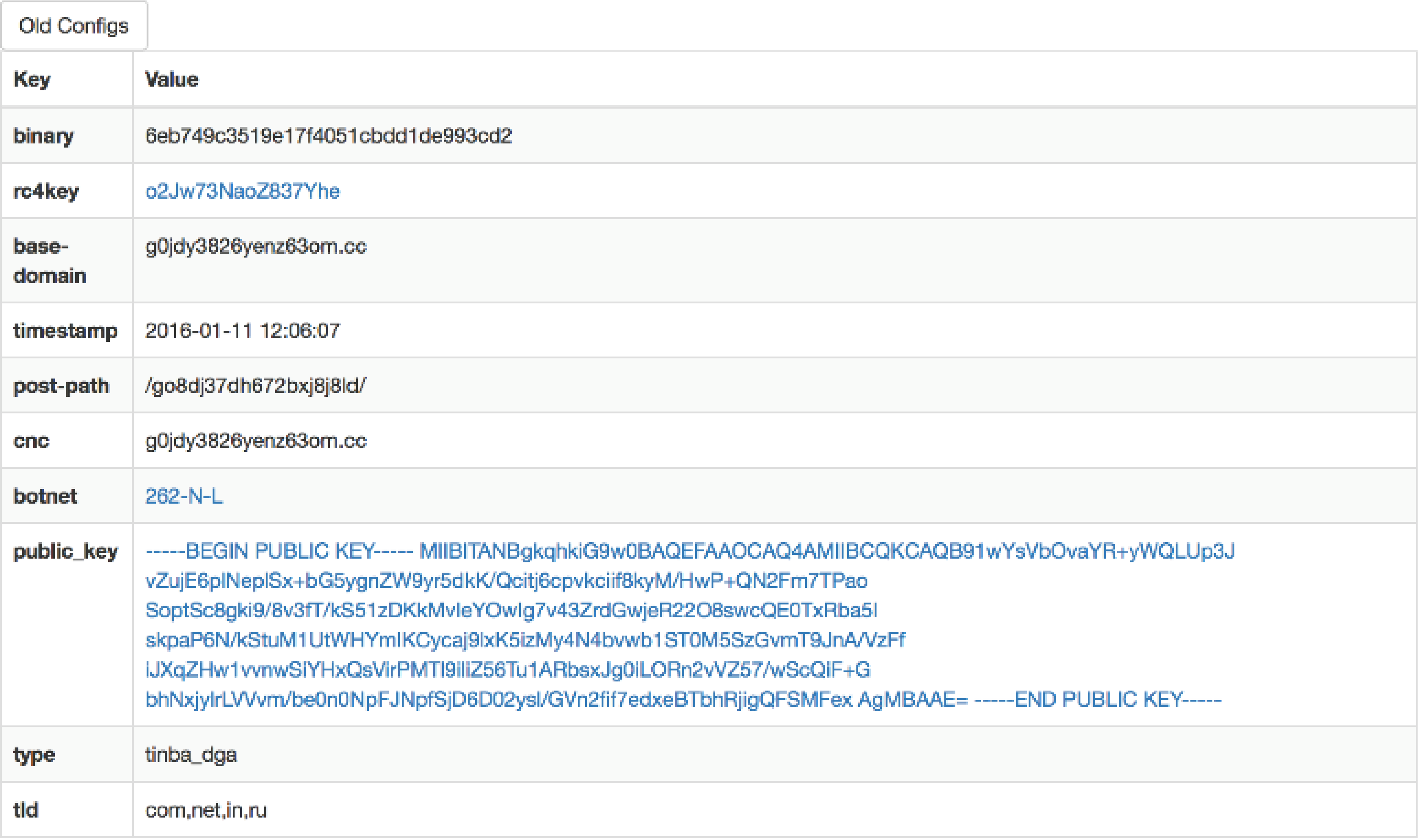
```
824  ""@client$321$""
228  ""admin""
 20  ""radministrator""
  9  ""80012345678""
  9  ""13800138000""
  9  ""13644713530""
  9  ""12345678901""
  6  ""version2013""
  6  ""teleport""
  5  ""sdjnga""
  4  ""boyyzj""
  3  ""dani10010""
  3  ""anonymous""
  3  ""80A80B80C80D""
  3  ""170077""
  2  ""pass@C2SV""
```

PoinsonIvy (password Version2013)

- Points to three C2s:
  - popkaka.xicp.net
  - popkaka.xicp.net has address 174.128.255.227
  - Running off Sharktech in US
  - sg3appstore.net
  - sg3appstore.net has address 121.127.234.170
  - Running off Sun Network in Hong Kong
  - us3appstore.net
  - us3appstore.net has address 121.127.234.170

Technique can be used to feed DGAs

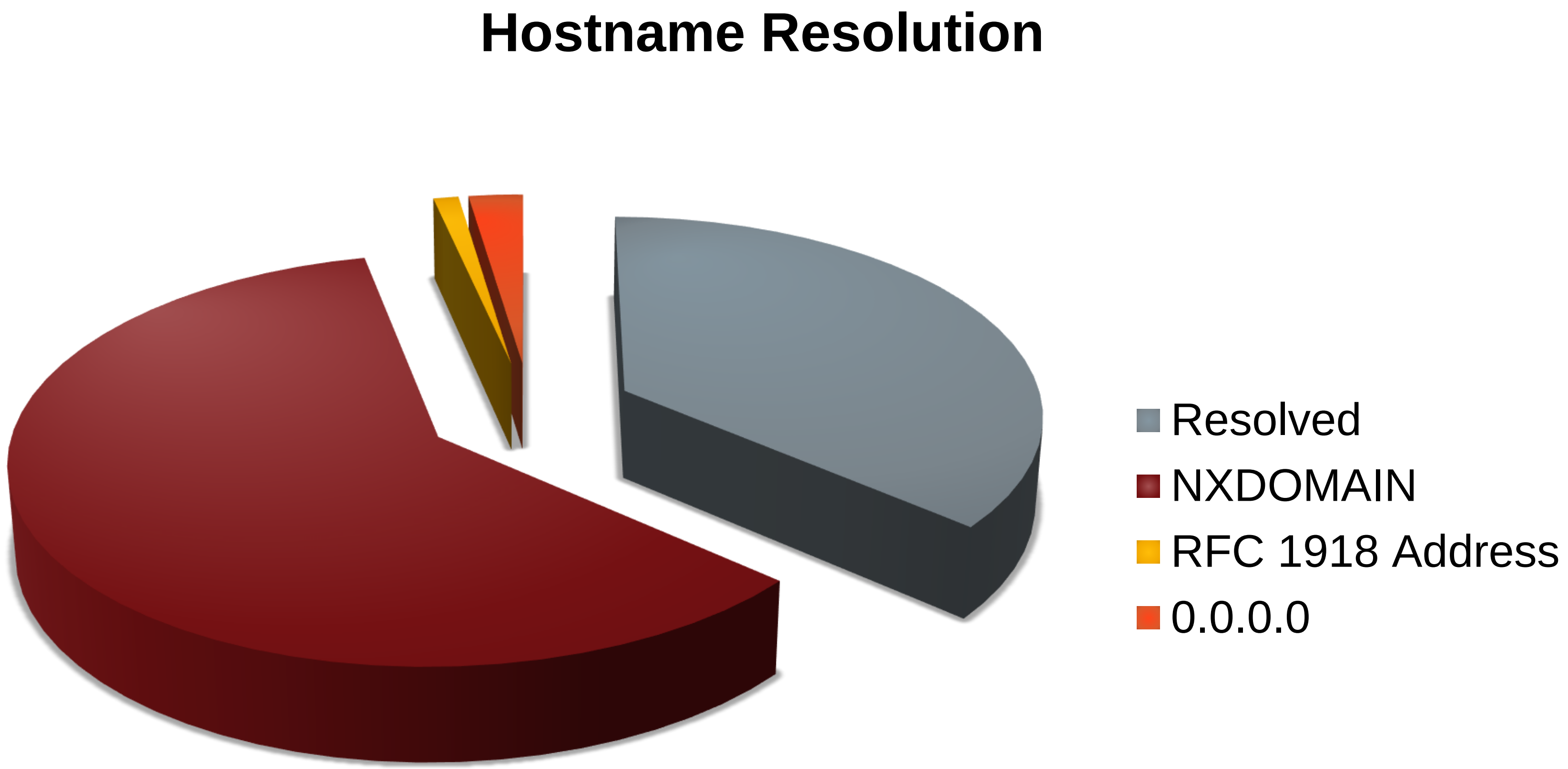
From Cert.PL malware ripper



Old Configs

Key	Value
binary	6eb749c3519e17f4051cbdd1de993cd2
rc4key	o2Jw73NaoZ837Yhe
base-domain	g0jdy3826yenz63om.cc
timestamp	2016-01-11 12:06:07
post-path	/go8dj37dh672bxj8j8ld/
cnc	g0jdy3826yenz63om.cc
botnet	262-N-L
public_key	-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB91wYsVbOvaYR+yWQLUp3J vZujE6plNeplSx+bG5ygnZW9yr5dkK/Qcitj6cpvkciif8kyM/HwP+QN2Fm7TPao SoptSc8gki9/8v3fT/kS51zDKkMvleYOwlg7v43ZrdGwjeR22O8swcQE0TxRba5l skpaP6N/kStuM1UtWHYmlKCycaj9lxK5izMy4N4bvwb1ST0M5SzGvmT9JnA/VzFf lJXqZHw1vvnwSlYHxQsVirPMTl9iliZ56Tu1ARbsxJg0iLORn2vVZ57/wScQlF+G bhNxjylrLVVvm/be0n0NpFJNpfSjD6D02ysl/GVn2fif7edxeBTbhRjigQFSMFex AgMBAAE= -----END PUBLIC KEY-----
type	tinba_dga
tld	com,net,in,ru

Resolving Hostnames (May 2015 - now)



The need for constant surveillance

- DNS resolving is point-in-time, may resolve sometimes and sometimes not.
  - The fact that it doesn’t resolve in and of itself is not a contraindication.
- Some configs may be garbage.
  - Some RATs, for instance, were configured to beacon to the IP 8.8.8.8
- DNS is under control of attacker, even if they engage in deception, detecting that has intelligence value.
- Some malware uses encoded IPs.
  - i.e. resolved IP is then “converted” to real IP.

Domain Generation Algorithms

- Usually a complex math algorithm to create pseudo-random but predictable domain names.

- Now instead of a static lists, you have a dynamic list of hundreds or thousands of domains and adversary only needs to have a couple registered at a time.

- Can search for “friendly” registrars to avoid suspension.

- Can engage in counter-intelligence.

Counterintelligence – or worse version

- What if adversary knows you resolve these DGA domains and put directly into your firewall (and I know people do this with my feeds)?
- Anyone recognize these IP addresses? They are the DNS Root Servers

198.41.0.4
192.228.79.201
192.33.4.12
199.7.91.13
192.203.230.10
192.5.5.241
192.112.36.4
128.63.2.53
192.36.148.17
192.58.128.30
193.0.14.129
199.7.83.42
202.12.27.33

Counterintelligence – or worse version

- Taking action on information without analysis is generally a bad idea, especially when the information is under the complete control of the adversary.

- This is why intelligence analysis is so important.

- (I whitelisted the root servers after I noticed an adversary tried to do an attack similar to this.)

Types of DGAs

- Almost all DGAs use some time of “Seed”.
- Types:
  - Date-based
  - Static seed
  - Dynamic seed
- Seed has to be globally consistent so all victims use the same one at the same time.

Other DGA Hardening Techniques

- Choice of gTLD matters.
  - Some doing have WHOIS protection, make it hard to sinkhole

- Rotation of seeds

- Some malware has rudimentary “sinkhole awareness”

- Adversarial objectives: Maintain control, limit surveillance

Examples of select DGAs - Cryptolocker

- Used 1000 domains a day across 7 gTLDs. Order domains are queries in based on GetTickCount()
- Eerily similar to DGA described in Wikipedia article on DGAs.
- Used previously by Flashback OSX Worm.
- Never changed during the life of the malware campaign.
- Successfully taken down in June 2014

Examples of select DGAs - Tinba

- Generated 1,000 domains a day, not date-seeded.
- Seeded by an initial hostname and a defined gTLD (one or more).
- Changes seeds often and tends to update already infected machines.
  - At least sinkholing tended to be ineffective for more than a few days.

Examples of select DGAs - Bedep

- Uses a dynamic seed – currency exchange values for foreign currency
  - European Central Bank produces daily feeds of the rates, this is used as source data.

- Impossible to predict in advance even though code to generate the domains is publicly available.
  - http://asert.arbornetworks.com/bedeps-dga-trading-foreign-exchange-for-malware-domains/

What the use of DGAs gives the good guys

- Easy ability to sinkhole unused DGA domains to gather additional intelligence.

- Easier ability to do bulk takedowns.
    - *IF* you can predict domains in advance.

- The ability to surveil malicious infrastructure in near real-time.

What the use of DGAs gives the good guys

- The use of DNS in malware severely limits the ability of the adversary to play games.
  - They need the world to be able to find their infrastructure in order to control victim machines.

- Even when DGA changes, the adversary **tends** not to immediately change their infrastructure too.
  - Allows for the use of passive DNS to see the extent of DGA changes.

DGA surveillance

- Pre-generate all domains 2 days before to 2 days in future.
- Pipe all those domains into adnshost using parallel to limit the number of lines.
- Able to process over 700,000 domains inside 10 minutes (and I’m not done optimizing).

```
parallel -j4 --max-lines=3500 --pipe adnshost -a -f < $list-of-domains | fgrep -v nxdomain  >> $outputfile
```

Example

2n2qlh5hqcwrvo.net,8.5.1.40,dns1.name-services.com|dns2.name-services.com|dns3.name-services.com|dns4.name-services.com|dns5.name-services.com,98.124.192.1|98.124.193.1|98.124.194.1|98.124.196.1|98.124.197.1,Master Indicator Feed for bebloh non-sinkholed domains,http://osint.bambenekconsulting.com/manual/bebloh.txt

lvzyjwj1fakh55i.com,208.91.197.113,ns1.dynadot.com|ns2.dynadot.com,54.164.135.208|54.164.162.213|54.165.100.140|54.68.142.171|54.68.143.189|54.68.145.110|54.68.55.168|54.88.182.181,Master Indicator Feed for bebloh non-sinkholed domains,http://osint.bambenekconsulting.com/manual/bebloh.txt

evtzxdehixfrktsjy.com,188.138.25.129,ns1.regway.com|ns2.regway.com,109.70.27.118|194.226.96.118,Master Indicator Feed for bedep non-sinkholed domains,http://osint.bambenekconsulting.com/manual/bedep.txt

ifamvhlimcaezy.com,188.138.125.65,ns1.regway.com|ns2.regway.com,109.70.27.118|194.226.96.118,Master Indicator Feed for bedep non-sinkholed domains,http://osint.bambenekconsulting.com/manual/bedep.txt

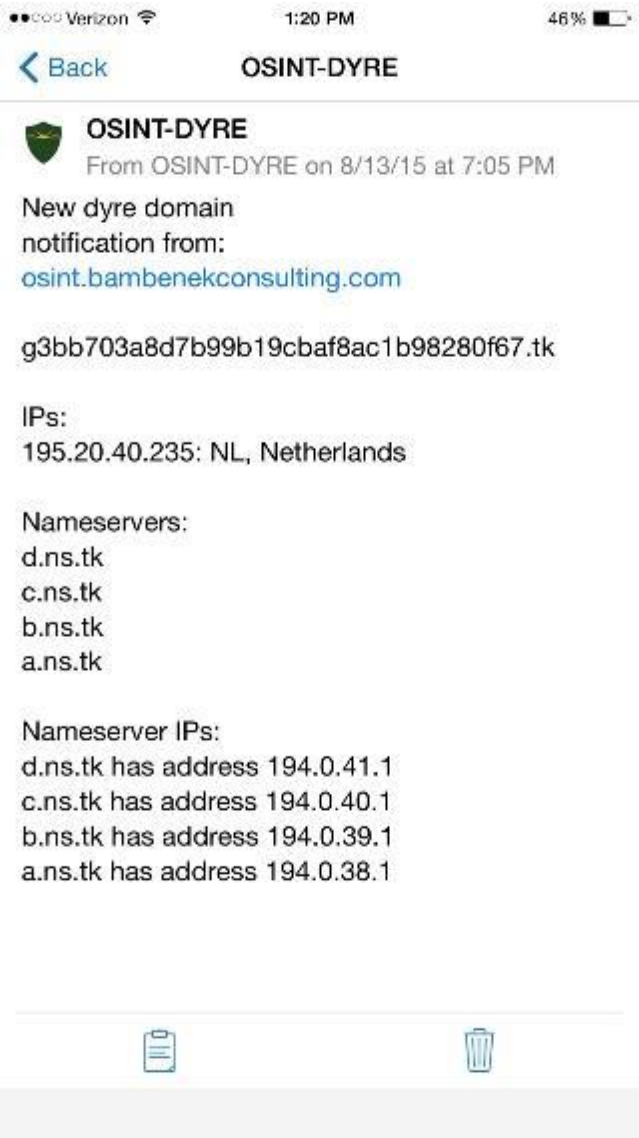
Public Feeds at: http://osint.bambenekconsulting.com/feeds

This is the C2-Master feed.

Surveillance is nice, what about notification?

- Creation of feeds and intake is still a passive tactic.
- It is all possible to automate notifications when key changes happen to allow for more near-time actions.
- This uses the Pushover application (Apple and Google stores) which has a very simple API.

New Dyre domain registered



OSINT-DYRE

From OSINT-DYRE on 8/13/15 at 7:05 PM

New dyre domain
notification from:
osint.bambenekconsulting.com

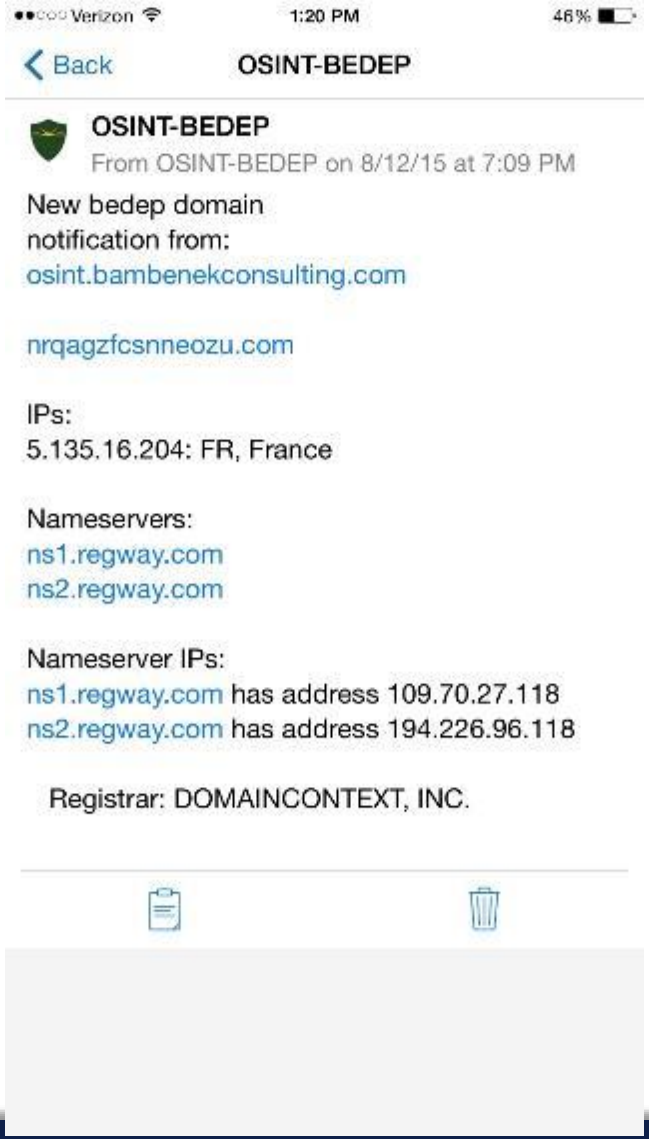
g3bb703a8d7b99b19cbaf8ac1b98280f67.tk

IPs:
195.20.40.235: NL, Netherlands

Nameservers:
d.ns.tk
c.ns.tk
b.ns.tk
a.ns.tk

Nameserver IPs:
d.ns.tk has address 194.0.41.1
c.ns.tk has address 194.0.40.1
b.ns.tk has address 194.0.39.1
a.ns.tk has address 194.0.38.1

New Bedep Domain Registered



OSINT-BEDEP

From OSINT-BEDEP on 8/12/15 at 7:09 PM

New bedep domain
notification from:
osint.bambenekconsulting.com

nrqagzfcsnneozu.com

IPs:
5.135.16.204: FR, France

Nameservers:
ns1.regway.com
ns2.regway.com

Nameserver IPs:
ns1.regway.com has address 109.70.27.118
ns2.regway.com has address 194.226.96.118

Registrar: DOMAINCONTEXT, INC.

Whois Registrar Intel

- Often actors may re-use registrant information across different campaigns. There may be other indicators too.

- Sometimes **even with WHOIS privacy protection** it may be possible to correlate domains and by extension the actor.

- Most criminal prosecution in cybercrime is due to an OPSEC fail and the ability to map backwards in time of what the actor did to find that fail that exposes them.

Whois Info

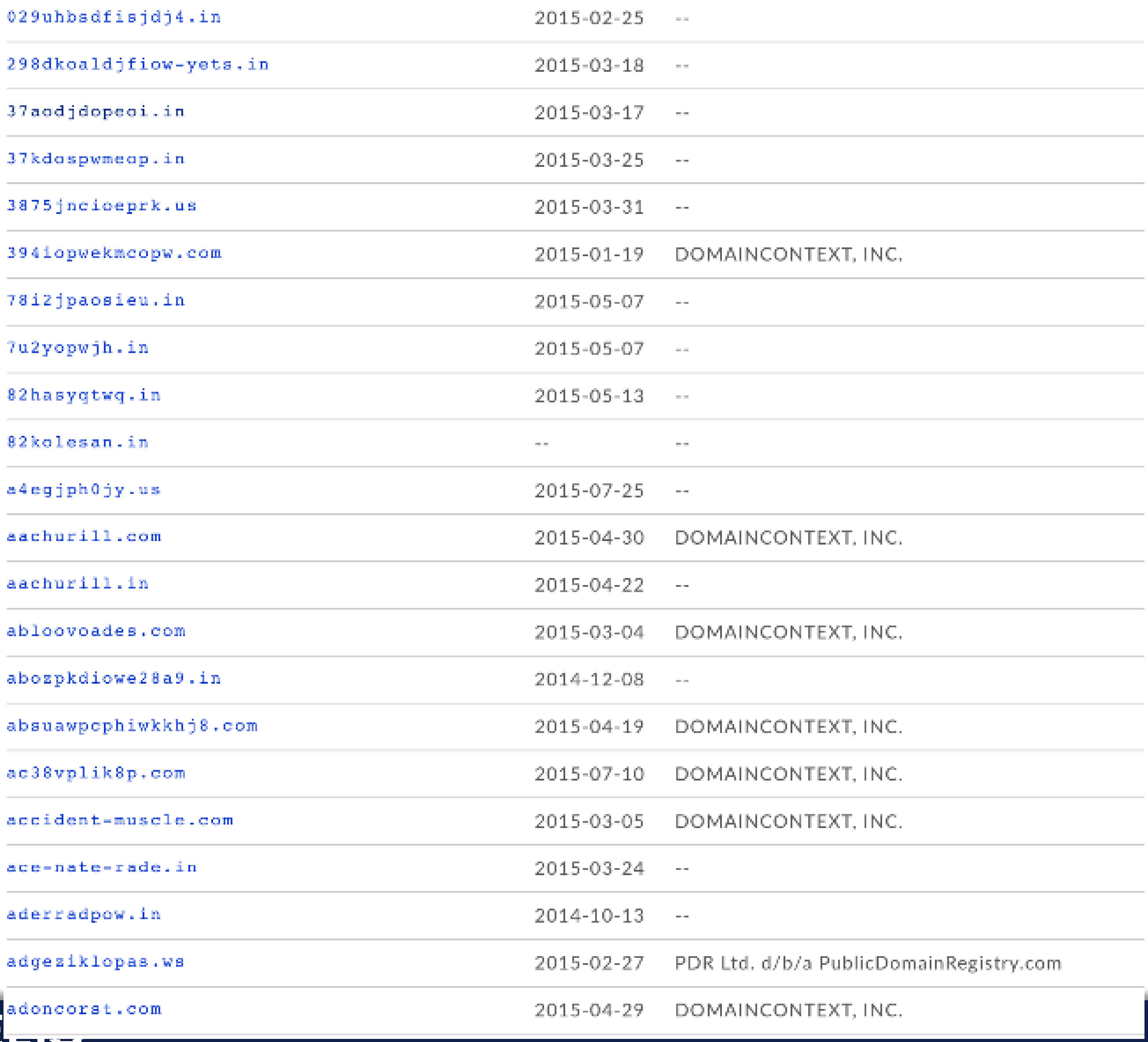
- Many actors will use WHOIS protection… some just use fake information.

- “David Bowers” is common for Bedep.

- ubuntu$ grep "David Bowers" *.txt | grep Registrant

- whois-bfzflqejohxmq.com.txt:**Registrant** Name: David Bowers
- whois-demoqmfritwektsd.com.txt:**Registrant** Name: David Bowers
- whois-eulletnyrxagvokz.com.txt:**Registrant** Name: David Bowers
- whois-lepnzsiqowk94.com.txt:**Registrant** Name: David Bowers
- whois-mhqfmrapcgphff4y.com.txt:**Registrant** Name: David Bowers
- whois-natrhkylqoxjtqt45.com.txt:**Registrant** Name: David Bowers
- whois-nrqagzfcsnneozu.com.txt:**Registrant** Name: David Bowers
- whois-ofkjmtvsnmy1k.com.txt:**Registrant** Name: David Bowers

David Bowers



029uhbsdfisjdj4.in	2015-02-25	--
298dkoaldjfiow-yets.in	2015-03-18	--
37aodjdopeoi.in	2015-03-17	--
37kdospwmeop.in	2015-03-25	--
3875jncioeprk.us	2015-03-31	--
394iopwekmcopw.com	2015-01-19	DOMAINCONTEXT, INC.
78i2jpaosieu.in	2015-05-07	--
7u2yopwjh.in	2015-05-07	--
82hasyqtwq.in	2015-05-13	--
82kolesan.in	--	--
a4egjph0jy.us	2015-07-25	--
aachurill.com	2015-04-30	DOMAINCONTEXT, INC.
aachurill.in	2015-04-22	--
abloovoades.com	2015-03-04	DOMAINCONTEXT, INC.
abozpkdiowe28a9.in	2014-12-08	--
absuawpcphiwkkhj8.com	2015-04-19	DOMAINCONTEXT, INC.
ac38vplik8p.com	2015-07-10	DOMAINCONTEXT, INC.
accident-muscle.com	2015-03-05	DOMAINCONTEXT, INC.
ace-nate-rade.in	2015-03-24	--
aderradpow.in	2014-10-13	--
adgeziklopas.ws	2015-02-27	PDR Ltd. d/b/a PublicDomainRegistry.com
adoncorst.com	2015-04-29	DOMAINCONTEXT, INC.

Wrapping it up

- Both techniques can be used to observe adversary behavior outside an organization to get a fuller picture of what they are involved in.

- Using this you can proactively have elements needed to proactively block potential adversaries or to end feed a hunt team.

- Techniques can be used to disrupt their operations even if they aren’t actively targeting you.

- Key is to remember to go through the time consuming exercise of doing real intelligence work instead of pumping into firewalls/IPS.

QUESTIONS?

THANKS TIM LEEDY AND THE REST OF MY TEAM. KEVIN BREEN, MANY OTHERS.

JOHN BAMBENEK
JOHN.BAMBENEK@FIDELISSECURITY.COM
/JCB@PEOPLE.OPS-TRUST.NET
+1 217 493 0760

DGA FEEDS:
OSINT.BAMBENEKCONSULTING.COM/FEEDS/