Barncat:
Mining Malware at Scale to Create an Encyclopedia of Malware

John Bambenek, Manager of Threat Systems
Fidelis Cybersecurity

28th Annual First Conference: Seoul, Korea

Fidelis™ Cybersecurity

Introduction

- Manager of Threat Systems with Fidelis Cybersecurity
- Part-Time Faculty at University of Illinois in CS
- Provider of open-source intelligence feeds
- Run several takedown oriented groups and surveil threats

Shorter Version

How this all began…

- Effectively took a break from security for ~2 years.
- Came back in 2013 with some fresh perspective to solve problems.
- First “big thing” I worked on was ransomware, Cryptolocker specifically.

DGA Surveillance

- Cryptolocker solely used a DGA to find C2s. This made takedown possible.

- Used DGA to resolve all current domains to find those that resolved, eliminated sinkholes, rest was bad. Surveillance was born.

- Other indicators were useful too (nameservers, registrant info, etc).

DGA Surveillance

- Now 42 families are tracked and almost a million domains a day.

- Have historical info on every family and can watch “interesting” connections and how the adversary moves.
  - And when they screw up. (**important**)

DGA Surveillance

- “Free” to use: http://osint.bambenekconsulting.com/feeds
  - But consider donating to my charity: http://www.thetumainifoundation.org

- More added when I’m not traveling and have time to implement/RE new DGAs (or get them from Johannes Bader).

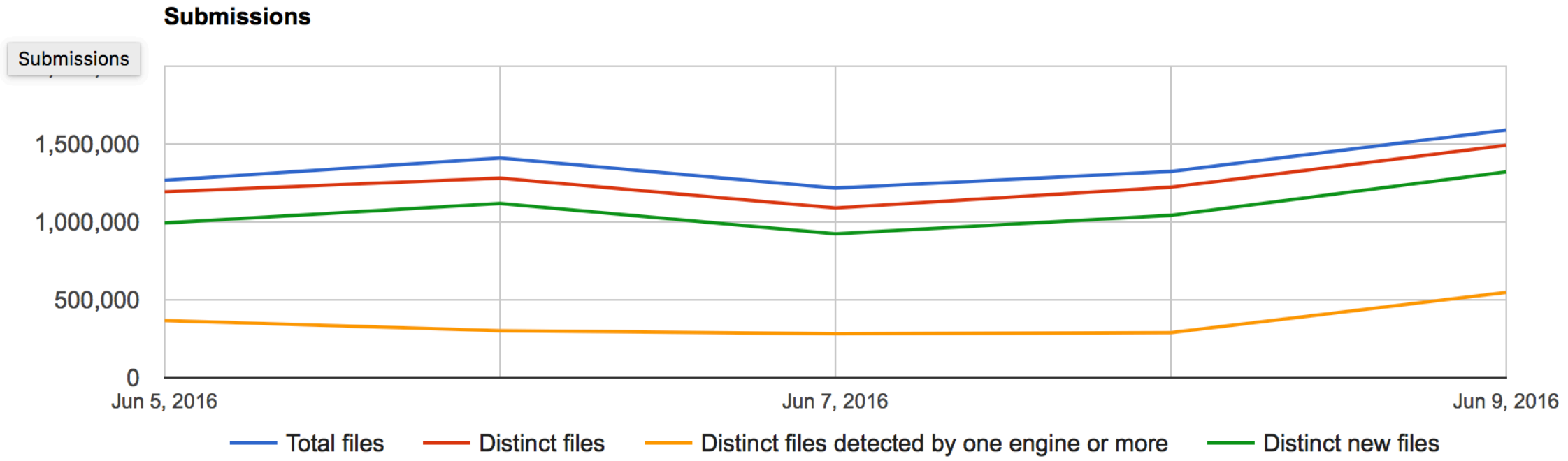
But this talk isn't about DGAs

- This started me down a road of what else can be surveilled and creating databases of badness to correlate activity.
- What if you had configuration data from 10 years of malware? What connections/correlations can you find?
- **Every successful criminal prosecution involves creating a timeline of the actor and finding the one time they screwed up.**

Problem Statement

- We are on the losing end of an arms race.
  - Too much malware
  - Not enough analysts
  - We're "open", they can operate privately
  - "Global" law enforcement is hard
  - …

The Problem Illustrated (from Virustotal)



About Threat Intelligence

- 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.

About Threat Intelligence

- Most CTI vendors give you indicators… context is often lacking. Much of the information “isn’t valuable” so it’s discarded.

- I’m a vendor, but not a feed vendor. My interest is creating dataset that can be actioned and make a difference.

How to Deal with 1M+ Samples/Day

- Full RE most expensive but most thorough.
- Dynamic analysis is good, but bin may not run correctly and sandboxing is resource intensive.
- Static analysis can be very fast… if you know how to pull the information out.
- Key is to automate such that you can do as much static analysis as possible, dynamic for much of the rest and RE only for the items where there is no other alternative.

Malware Config Extraction

- There are almost 1 million distinct new malware samples seen by just VirusTotal every day.

- Given a large corpus of malware, you can mine all of that for configs and other data.

- Can provide up-to-date data of in-the-wild (i.e. relevant) malware.

Malware Config Ripping

- Dynamic analysis is good, but bin may not run correctly and is resource intensive.
- Static analysis can be very fast… if you know how to pull the information out.
- Key is to automate such that you can do as much static analysis as possible, dynamic for much of the rest and RE only for the items where there is no other alternative.

Your Starter Kit

- Start with a feed of binaries, VT is fine or whatever you have. (Your own spam folders)
- Use Yara and/or AV names to preselect family.
- Run appropriate malware decoder
  - Put in whatever database makes sense to you.
  - Internally we use splunk, external sharing via MISP.
- All of this (Except the feed of malware*) is open-source and you can start doing this today.

What can you do with malware configs?

- 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.

These tools help…

- https://github.com/kevthehermit/RATDecoders

- Python scripts that will *statically* rip configurations out of ~three dozen different flavors of malware.

- Actively developed and you can see in action at malwareconfig.com

- Disclaimer: I had nothing to do with the development of these tools; they just fit my need and Kevin Breen deserves mad props.

Malware Sources

- VirusTotal
- MSFT VIA Program
- Other malware sharing programs
- Internal sources (most important)

Malware Configs

- Every malware 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 Data

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

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

07998ff3d00d232b6f35db69ee5a549da11e96d1,150213,Dark Comet Config,test1,192.116.50.238,90,4A2xbJmSqvuc,DC_MUTEX-F54S21D

07ac914bdb5b4cda59715df8421ec1adfaa79cc7,150213,Dark Comet Config,Guest16,alkozor.ddns.net,31.132.106.94,1604,1.ekspert60.z8.ru,#######60,#######2012,zwd8tEC0F0tA,DC_MUTEX-W3VUKQN

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

All the fields…

ActivateKeylogger,ActiveXKey,ActiveXStartup,AddToRegistry,AntiKillProcess,BypassUAC,CONNECTION_TIME,Campaign,ChangeCreationDate,ClearAccessControl,ClearZoneIdentifier,ConnectDelay,CustomRegKey,CustomRegName,CustomRegValue,DELAY_CONNECT,DELAY_INSTALL,Date,DebugMsg,Domain,EnableDebugMode,EnableMessageBox,EncryptionKey,Error,ExeName,FTPDirectory,FTPHost,FTPInterval,FTPKeyLogs,FTPPassword,FTPPort,FTPRoot,FTPServer,FTPSize,FTPUser,FireWallBypass,FolderName,Gencode,GoogleChromePasswords,Group,HKCU,HKLM,HideFile,ID,INSTALL,INSTALL_TIME,Injection,InstallDir,InstallDirectory,InstallFileName,InstallFlag,InstallFolder,InstallMessageBox,InstallMessageTitle,InstallName,JAR_EXTENSION,JAR_FOLDER,JAR_NAME,JAR_REGISTRY,JRE_FOLDER,KeyloggerBackspace=Delete,KeyloggerEnableFTP,KillAVG2012-2013,MPort,MeltFile,MessageBoxButton,MessageBoxIcon,MsgBoxText,MsgBoxTitle,Mutex,NICKNAME,NetworkSeparator,OS,OfflineKeylogger,Origin,P2PSpread,PLUGIN_EXTENSION,PLUGIN_FOLDER,Password,Perms,Persistance,Port,PreventSystemSleep,PrimaryDNSServer,ProcessInjection,RECONNECTION_TIME,REGKeyHKCU,REGKeyHKLM,RegistryValue,RequestElevation,RestartDelay,RetryInterval,RunOnStartup,SECURITY_TIMES,ServerID,SetCriticalProcess,StartUpName,StartupPolicies,TI,TimeOut,USBSpread,UseCustomDNS,VBOX,VMWARE,Version,_raw,_time,adaware,ahnlab,baidu,bull,clam,comodo,compile_date,date_hour,date_mday,date_minute,date_month,date_second,date_wday,date_year,date_zone,escan,eventtype,fprot,fsecure,gdata,host,ikarus,immunet,imphash,index,k7,linecount,magic,malw,mc,mcshield,md5,nano,norman,norton,outpost,panda,product,proex,prohac,quickheal,rat_name,resys,run_date,section_,section_.BSS,section_.DATA,section_.IDATA,section_.ITEXT,section_.RDATA,section_.RELOC,section_.RSRC,section_.TEXT,section_.TLS,section_AKMBCZMH,section_BSS,section_CODE,section_DATA,section_ELTQHVWF,section_VDOJLYFM,section_YRKCHNMU,sha1,sha256,source,sourcetype,splunk_server,splunk_server_group,spybot,super,tag,tag::eventtype,taskmgr,times_submitted,timestamp,trend,uac,unique_sources,unthreat,vendor,vipre,windef,wire

Data Storage

- Operational data is made available via MISP:
  - https://barncat.fidelissecurity.com

- E-mail me for access. (Need name, email and affiliation)

- Or give me a business card after this talk and write barncat on it.

Why store all that data?

- VT doesn’t keep configuration information. You MAY get pieces of it if the malware runs.

- More importantly, if you knew what you where looking for at the time the sample was seen, you’d already have a rule in place.

- Ability to correlate backwards to find the OPSEC fail.

Why store all that data?

- Three basic things to look for:
- When DNS points to a new IP address
- When config data maps to previous samples
- When config data matches future samples

Configuration Items

Most RATs have either free-form text configuration items or randomly generated configuration items:

- Campaign ID, File Paths, Mutex, Registry Keys

Some have authentication information or FTP server information.

All can be correlated to link seemingly disparate attacks or to learn something about the attacker.

What can you do with this?

- If you receive a sample, check the configuration items against the balance of former samples to find a pattern of behavior.

- Hunt for interesting data and actors.

So let's say you get this malware…

9/2/15
5:27:06.000 AM


```
{ [-]
   DELAY_CONNECT: 1
   DELAY_INSTALL: 1
   Date: 2015-09-02 05:27:06
   Domain: nikresut015js.zapto.org
   INSTALL: true
   JAR_EXTENSION: fqLw1v
   JAR_FOLDER: wcnLIxbslsn
   JAR_NAME: Fresh_Bomb
   JAR_REGISTRY: COpaNxwcFs5
   JRE_FOLDER: UOStKe
   NICKNAME: August24rdBombing
   Origin: vt
   PLUGIN_EXTENSION: lykYQ
   PLUGIN_FOLDER: L0ZQqgmCGJ4
   Port: 2014
   SECURITY_TIMES: 5
   VBOX: true
   VMWARE: true
   magic: Zip archive data, at least v2.0 to extract
   md5: a1c9d4b1e522cfab79982917d7930cd6
   rat_name: JSocket
   run_date: 2015-09-03
   sha1: af9c898da3faa02e5d9ae25c5f9ced5ded7c603e
   sha256: be0f6903b3217c8df94c69dc0ea58ee1c07e92ab563bc4015f1a49a1dcf99acf
   times_submitted: 2
   unique_sources: 1
}
```

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]

Background

- Now dead, but was Java-based multiplatform RAT, has a strong LatAm user base but at least one user may have Hezbollah ties.
- There is a strong “RATtng” presence in Middle East attackers.
- There can be some laterally communication/knowledge sharing among “support” entities in terrorist groups.

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

,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

Beating a Dead Norse

- Often what drives intelligence (at least for vendors) is marketing combined with the need to “SAY SOMETHING ANYTHING RIGHT NOW”.

- Despite initial data points that says this could be terrorism related, access to an historical database was able to disprove the notion quickly.

- The biggest byproduct of big data is spurious conclusions.

Dark Comet Campaign IDs

24597	Guest16	2747	Guest16_	755		406	All	337	Kurban
232	Hacked	193	HF	181	test	168	Col334	145	Solis
140	Hack	135	lol	129	Test	128	Guest	121	Victim
118	PC	118	Guest1	105	new-vict	105	1	102	kurban
99	Slave	96	No-IP	93	Vitima	85	User	70	HACKED
68	all	68	Server	68	Guest17	66	DOS	58	okay
55	hack	55	Kurbanla	53	228	50	apb	50	B--L--A-
49	Hacker	47	KURBAN	46	Arkade	44	DC	43	Opfer
42	Steam	41	Victime	41	HACK	40	server	40	hak
39	hacked	39	RAT	36	TestGues	36	DhjetoR	35	vitima
34	123	33	LOL	33	DarkCome	32	user	32	Trolld
32	Rat-1	31	MoyerSK	31	2	30	SPY	30	LucidsVi
29	trolled	29	teste	29	MSIL	28	BOT	27	WinUpdat
27	TEST	25	Rat	24	kurban01	24	Omegle	24	DeadPrez
24	Darkcome	23	Server1	23	Gerek po	23	CSGO	22	deneme
22	darkcome	22	Youtube	22	New	22	Minecraf	22	Bot
21	victime	21	test1	21	kurban1	21	Noob	21	M2BOB

njRat Campaign IDs

47736 HacKed	632 Hacked	455 Vitima	371 hacked	199 Lammer
175 vitima	162 Victim	156 hacker	123 system	119 Hacker
113 teste	113 test	110 svchost	110 1	104 victim
102 google	101 LpeH	98 Test	98	89 server
86 HacKeD	79 Vitimas	75 hack	72 HACKED	69 Teste
67 new	67 HacKed	63 facebook	63 ahmed	62 Lammer
57 Server	52 windows	52 VITIMA	52 Minecraf	51 server.e
50 Slave	48 ana	48 PB	46 ROOTED	46 HacKer
45 Hack 44	123	42 ali	42 Hackeado	41 Victime
40 alosh	40 Facebook	39 svchost.	39 haker	39 VicTim
39 Otario	38 victime	38 explorer	38 Snopi Bi	38 HacKed1
37 Skype	36 chrome	36 Windows	35 HacK	35 !~HaCKeD
34 HacKed2	34 Google C	34 0	33 PointBla	33 AZiiiiiZ
32 matrix	32 hhh	31 HackeD	30 win7	30 skype
30 Texte	30 New	30 Microsof	30 Fucked	29 mandi
29 System	29 Cobaia	28 n3aL	28 Anonymou	27 yahoo
27 radar	27 User	27 HacKed B	27 2016	26 Crossfir
25 Torrent	25 Dr_ERror	24 sadam	24 lol	24 PC
24 Hunted	24 HacKed b	24 HacKed B	24 Chrome	24 2015

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" ue16-data-pruned.csv…

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

C2 hostnames with multiple RAT families

```
5 pooi222.no-ip.biz
5 deli34.zapto.org
5 brixsus.mooo.com
5 arseisa.no-ip.org
4 testando.no-ip.biz
4 shakal2.ddns.net
4 peterpanjack.no-ip.org
4 odjwowjawjai0d.ddns.net
4 netwed.ddns.net
4 mrmoney.no-ip.biz
4 malouzimbra.no-ip.biz
4 kayocharlex.no-ip.org
4 jmkrar.no-ip.biz
4 hamudi1997.no-ip.biz
4 fahad26smsm.zapto.org
```

```
5 mods5153135.no-ip.org
5 darkdoser87.ddns.net
5 biga.zapto.org
5 192.168.56.1
4 souhila.no-ip.biz
4 server10169.ddns.net
4 oreidostrojans.no-ip.org
4 ngokhong.ddns.net
4 myinfinity.ddns.net
4 microwaveone.ddns.net
4 kroneeeee.no-ip.org
4 kamelayad22.ddns.net
4 host21.no-ip.org
4 gethackedscammed.no-ip.biz
4 doni123.ddns.net
```

```
pooi222.no-ip.biz,CyberGate
pooi222.no-ip.biz,LuxNet
pooi222.no-ip.biz,SpyGate
pooi222.no-ip.biz,VirusRat
pooi222.no-ip.biz,njRat
```

Campaign IDs re-used in different RATs

23	6 test	6 Hacked	6 1	5 hacked
5 Test	5 Slave	5 Server	5 Microsof	5 Lammer
5 HacKed	4 xd	4 windows	4 test1	4 svchost.
4 server	4 photo	4 new	4 chrome	4 admin
4 Vitima	4 Victim	4 Unknown	4 System	4 RAT
4 Lucas	4 LOL	4 Hacker	4 Game	4 Chrome
4 123	3 xxxxx	3 x	3 win32	3 vitima
3 victime	3 vic	3 v1	3 user	3 tt
3 teste	3 test2	3 svchost	3 ss	3 slave
3 sexy	3 serveur	3 serv	3 s	3 rus
3 qwe	3 qq	3 prueba1	3 ok	3 name
3 microsof	3 meow	3 memo	3 main	3 lucas
3 love	3 lool	3 lol	3 kkk	3 king

```
Lammer,,DarkComet
Lammer,,SpyGate
Lammer,,VirusRat
Lammer,,njRat
```

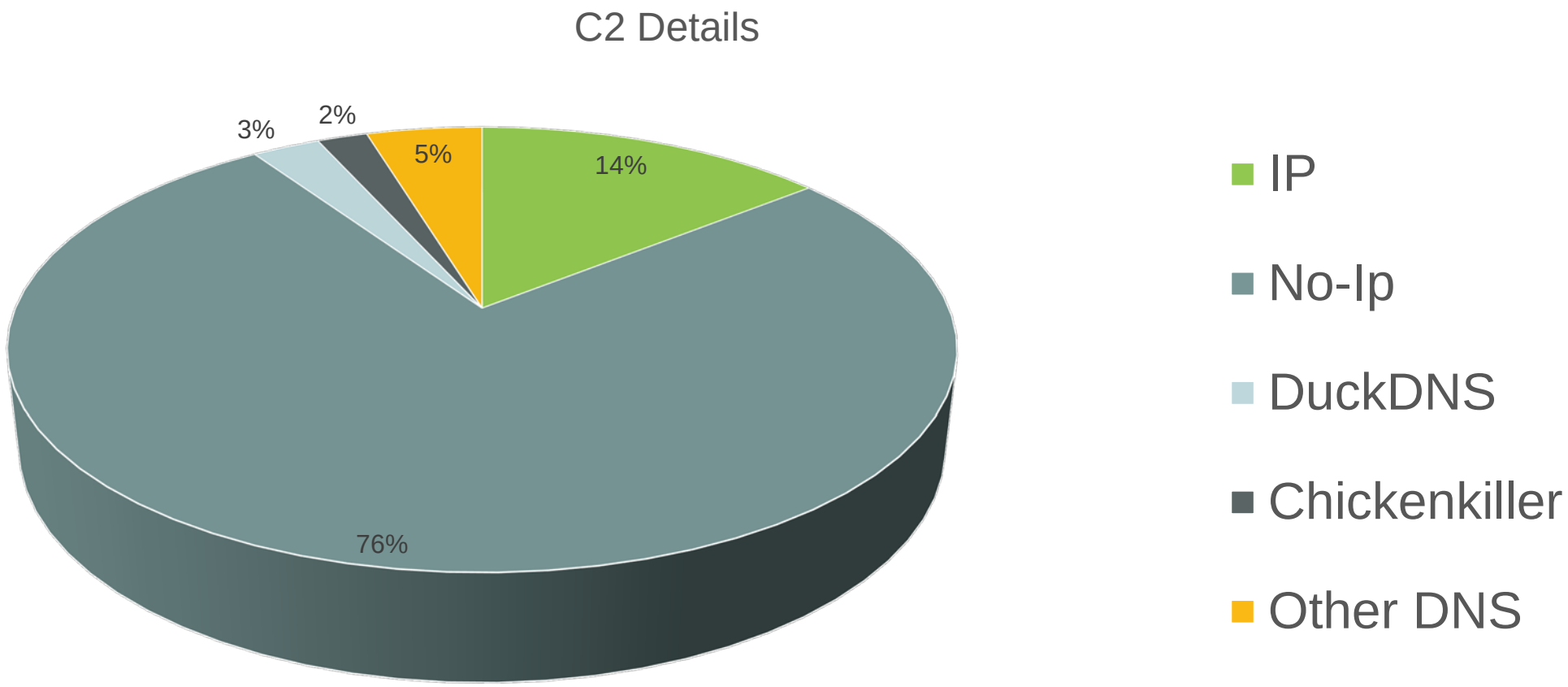
Technique can be used to feed DGAs

From Cert.PL malware ripper

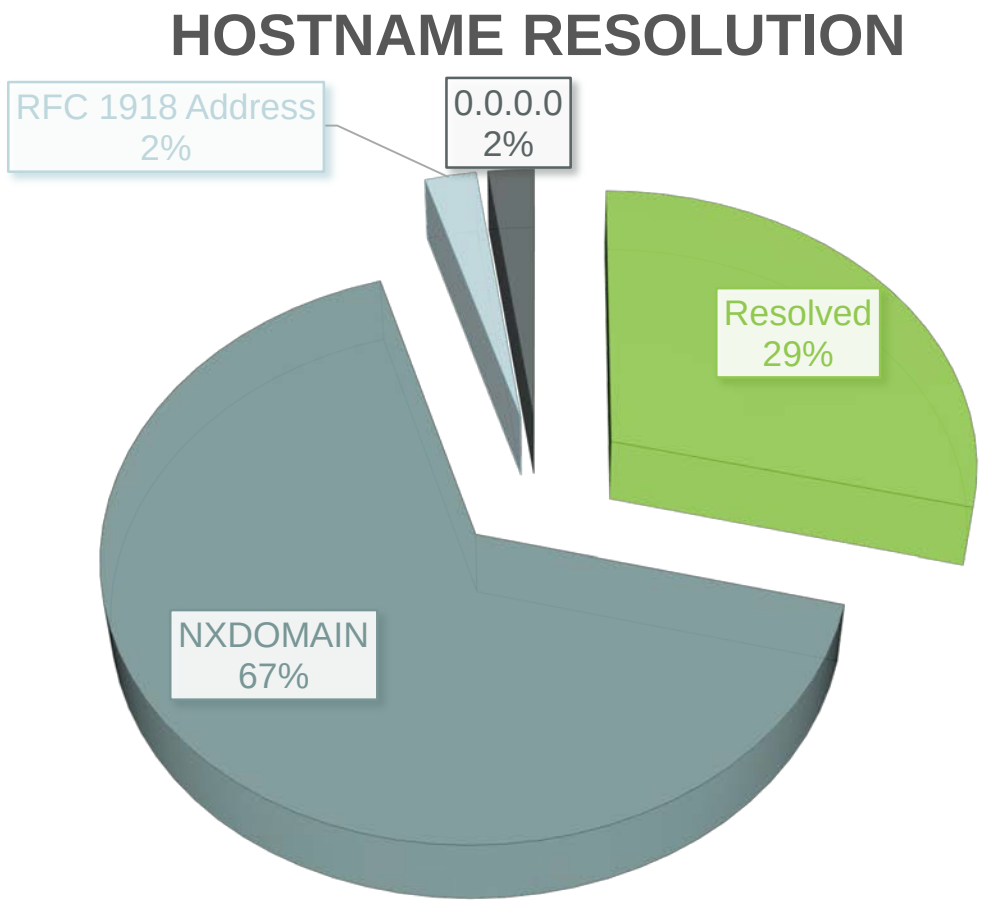
Old Configs

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/kS51zDKkMvIeYOwIg7v43ZrdGwjeR22O8swcQE0TxRba5l skpaP6N/kStuM1UtWHYmIKCycaj9lxK5izMy4N4bvwb1ST0M5SzGvmT9JnA/VzFf iJXqZHw1vvnwSiYHxQsVirPMTl9iliZ56Tu1ARbsxJg0iLORn2vVZ57/wScQiF+G bhNxjylrLVVvm/be0n0NpFJNpfSjD6D02ysl/GVn2fif7edxeBTbhRjigQFSMFex AgMBAAE= -----END PUBLIC KEY-----
type	tinba_dga
tld	com,net,in,ru

C2 Details Breakdown



Resolving Hostnames (May 2015 - now)



IP GeoLocation

Countries

1506 Russia
1318 Brazil
1219 "United States"
961 Turkey
857 France
729 Algeria
588 Egypt
543 Ukraine
488 "United Kingdom"
373 Morocco
366 Germany
321 Iraq
284 "Saudi Arabia”
281 Netherlands
228 "Republic of Korea"
220 Tunisia
200 Canada
151 Palestine

Cities

278 Cairo
268 Istanbul
242 Moscow
143 "São Paulo"
112 Baghdad
106 Jeddah
96 Riyadh
94 Paris
91 Casablanca
89 Ramallah
77 Ankara
71 "Rio de Janeiro"
68 "Saint Petersburg"
67 London
67 Kiev
67 Amman
65 Montreal
65 "Tel Aviv"

Resolving hostnames

- It seems most RATs aren't actively resolving (and not actively controlling victims).
- Passive DNS also misses a fair bit of these hostnames.
- Sophisticated attackers, however, will only have a dynamic hostname resolve when they are active and then have it non-resolve or point to RFC 1918 space when not actively working on victims.
- Most RATs don't use HTTP, so hostname is not in traffic.

Counter-intelligence

- Attacks know that we do this and actively throw mud in the water.
- Attacks could just as easily submit binaries to VT with fake information. Some indication people used VT to test detection.
- Just because a C2 is in a given country, attacker may be somewhere else.

Example #1

11/20/15
2:12:42.000 PM


```
{ [-]
   Campaign: All
   Date: 2015-11-20 14:12:42
   Domain: 8.8.8.8
   FireWallBypass: 0
   Gencode: qkttTB7XaVzk
   Mutex: DC_MUTEX-6R5BT6J
   OfflineKeylogger: 1
   Origin: vt
   Port: 1604
   Version: #KCMDDC51#
   compile_date: 2012-06-08 11:12:27
   imphash: 8033c11f8a2fdfc317e8655120579933
   magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
   md5: ffe6d90760977305d01a346a25995efe
   rat_name: DarkComet
   run_date: 2015-11-21
   section_.BSS: d41d8cd98f00b204e9800998ecf8427e
   section_.DATA: cb210a12278fc6b67accee22c52b9ad1
   section_.IDATA: 80655c280fee15e63402a8fc93041c3c
   section_.ITEXT: 7d01b8ffc56f096e211f89f0f28e5b49
   section_.RDATA: c1788dfeb92bbf0cff5aeaeaf1270ff8
   section_.RELOC: 590aac335a7094d529e15198df1c5920
   section_.RSRC: dea984d74cf7c8d9674bfe8db73d7cfc
   section_.TEXT: c8087ea6a249266ed1db0453229b76c2
   section_.TLS: d41d8cd98f00b204e9800998ecf8427e
   sha1: c5d171467fcbf07bc3be50c019b077b3792dd668
   sha256: 8f507788204bb8843c7a59ddf6ec2f29982587c5624fabb45e20c317c977c381
   times_submitted: 1
   unique_sources: 1
}
```


Show as raw text

Example #2

Remember Kevin Breen's decoders from before?

JSocket author changed encryption key between version 1.1 and version 1.2 to break that decoder.

- JSocket v2 uses RC6 encryption now.

Everything we do is public and disruptive. Attackers can and will adapt.

Counter-intelligence

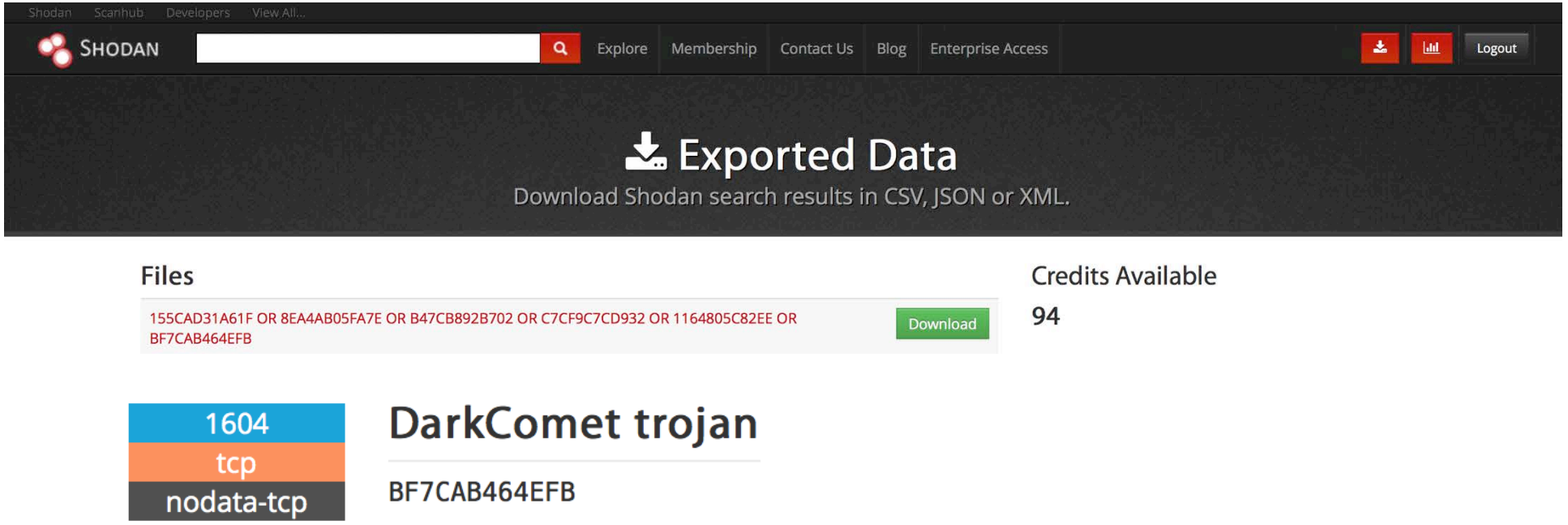
- DNS resolution is point-in-time.
- Some attackers will have their hostnames resolve when actively in operation but have them point “elsewhere” when not in use.
- Some attackers may upload samples to VT with “wrong” configuration items.
- .

Edge cases

- A decoder exists for Cryptowall (at least for v3) but Cryptowall uses compromised domains.
- They aren’t the only one who is not the only malware family that uses compromised domains.
- Similar problem with word-list-based DGAs.
- What about encoded DNS resolution?

Finding C2s without binaries

Using the data above, it also becomes possible to proactively hunt C2s even without having malware configs.



Not perfect but did find C2s I was unaware of.

Data not in configuration

Some aspects of the malware might be relevant but not present in the configuration itself.

JSocket uses the same SSL certificate for all C2 communications.

Data:

Version: 3 (0x2)

Serial Number: 522427837 (0x1f239dbd)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=FR, O=assylias.Inc, CN=assylias

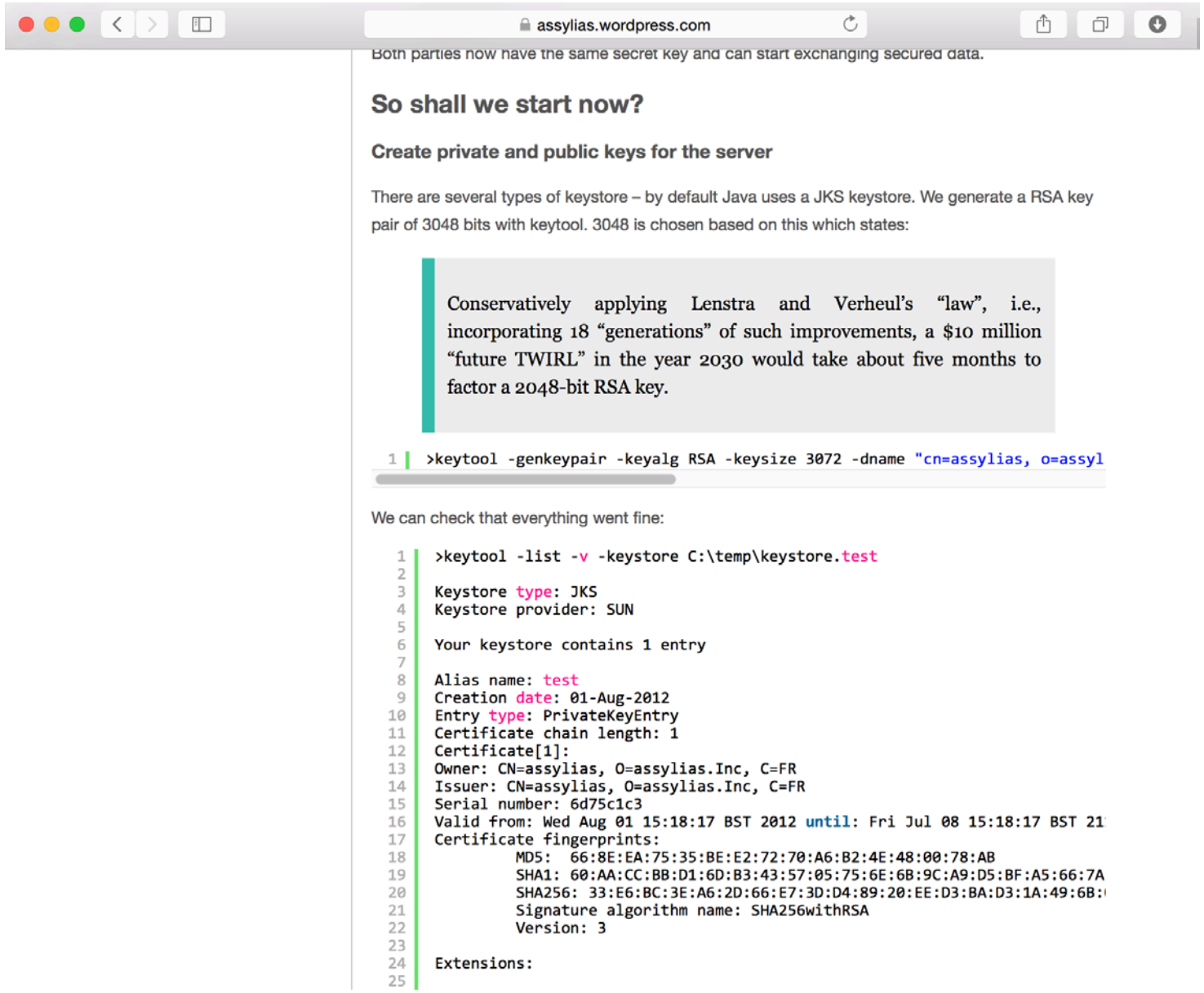
Validity

Not Before: Jan 17 05:26:19 2015 GMT

Not After : Dec 24 05:26:19 2114 GMT

Subject: C=FR, O=assylias.Inc, CN=assylias

Assylias?



JSocket Certificate Validation

- JSocket builders phone home to verify valid subscription. Builder will not run unless it is presented the correct cert.

- JSocket builder itself has a cert which is used to verify the builder (all builders use same one, the Assylias cert).

- Attacker changed keystore password from “storepass” ☹

Certificates continued

- Some families of RATs also produce mobile malware. Android specifically needs to have all APKs “signed”.

- An exercise to the attacker to find a way to get the malware on the phone (allow unverified signers, get to phone around store).

- JSocket binds itself to an existing APK so makes it “easy” to masquerade on an existing and legitimate app.

JSocket APK Cert

Certificate:

Data:

Version: 1 (0x0)

Serial Number:

fa:21:6b:2c:8e:6c:35:f6

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=EU, ST=Oregon, L=Cincinati, O=Oracle Corporation, OU=Oracle, CN=Oracle Developer/emailAddress=admin@oracle.com

Validity

Not Before: Jan 6 16:33:13 2015 GMT

Not After : May 23 16:33:13 2042 GMT

Subject: C=EU, ST=Oregon, L=Cincinati, O=Oracle Corporation, OU=Oracle, CN=Oracle Developer/emailAddress=admin@oracle.com

JSocket APK Cert

- Searching based on that cert did not find many samples in VT retrohunt.
- However, some samples were found in the wild.
- Appears multiple families are using the same CN information.
- Could not find “instructions” that attackers used, yet.
- Opens up possibilities of scanning malicious APKs by signing cert for finding malware.

So what's next?

Once a given hostname is seen, it needs to be persistently surveilled.

- Resolving hostname (and feeding to pDNS)
- Checking to see if C2 is actually up (syn() check)

Process historical malware. (If you have a zoo that you'll let me process, let's talk)

Checking for things that resolve to RFC 1918 then go back to "real IPs"

Burn/Sink all the things.

Barncat Demo

- Time permitting…
- For access, e-mail me with your name, email address and affiliation (or give me a business card and write Barncat on it).
- https://barncat.fidelissecurity.com
- Bring data local (Splunk, ES, whatever), MISP interface not as useful in this specific case.

Questions & Thank You!

John Bambenek / john.bambenek@fidelissecurity.com

Special thanks to Kevin Breen and many others for their research.

Thanks to Tim Leedy and rest of my team for their effort on this.

Fidelis™ Cybersecurity