FIDELIS CYBERSECURITY™

Mining Malware for Intelligence at Scale

John Bambenek / Sr. Threat Analyst / Threat Research Team

DEEPSEC ‘15 / Vienna, Austria

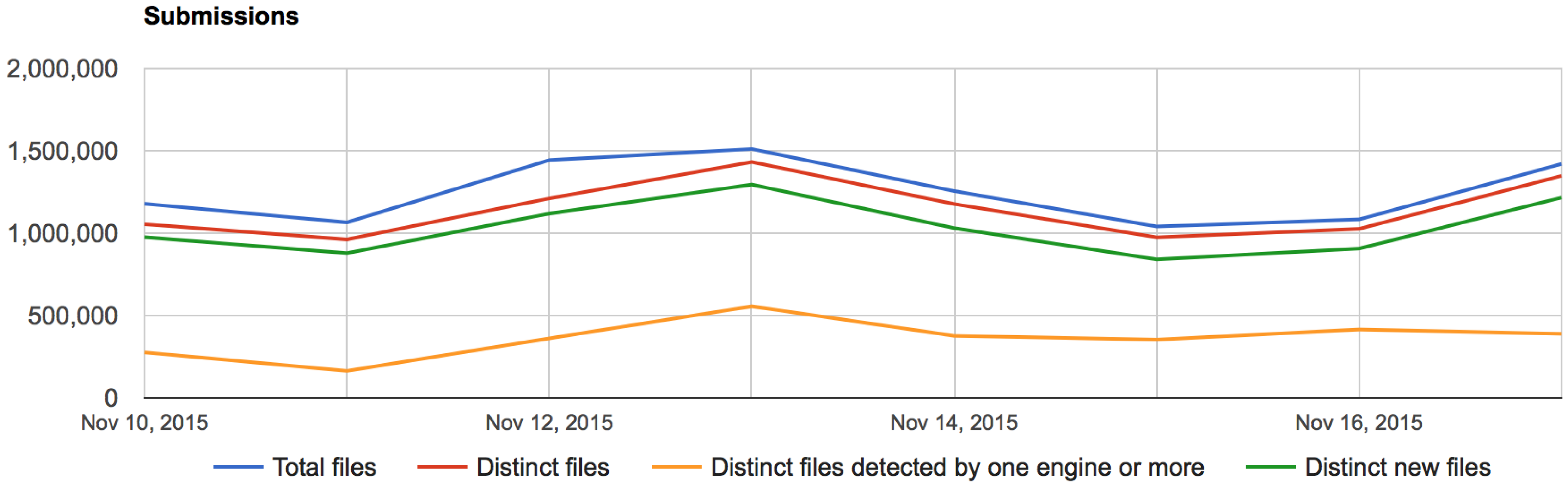
Introduction

- Sr. Threat Researcher with Fidelis Cybersecurity
- Faculty at the University of Illinois at Urbana-Champaign
- Producer of open-source intelligence feeds
- Run several takedown-oriented groups for various malware families
- Important note: in this presentation is no use of the word “cyber” except for my company name ⏪

Problem Statement

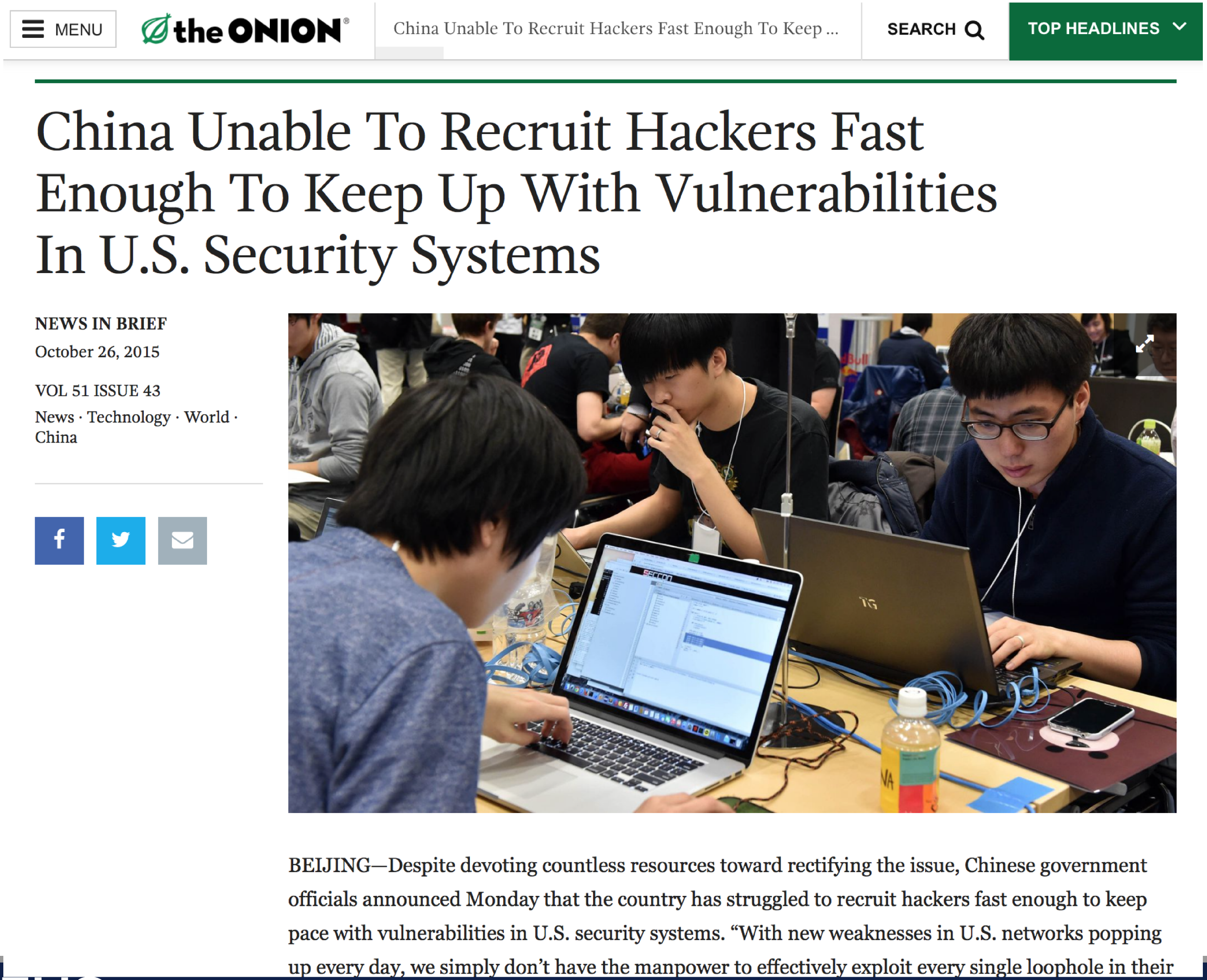
- We are on the losing end of an arms race
  - The adversaries produce more malware than we can possible analyze.
  - We have to operate in the open while they operate in secret.
  - Their core business is exploitation, security for us is a cost center.
  - We operate in a global economy without an effective means of global law enforcement.

The Problem… Illustrated



Virustotal Statistics taken at 18 Nov 2015

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

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.

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 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 RAT binaries, VT is fine or whatever you have.

- Use Yara and/or AV names to preselect family.

- Run appropriate RAT decoder

- Put in whatever database makes sense to you.
  - Internally use splunk, external sharing via MISP.

- All of this (Except the feed of malware*) is open-source and you can start doing this today.

Why RATs?

- Single stage malware will generally always have full configuration in the binary itself.
- Used not just by skiddies but by advanced attackers also such as nation-states and terrorist affiliated entities.
- Dozens of RAT types all well-known to deal with.
- Gotta walk before you can run.
- That said, Dridex/Cridex integrated too now.

What can you do with RAT configs?

We don’t need another whitepaper. What we need is bodies in the street.

What can you do with RAT 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.

Also, there is this magic sauce…

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

- 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

- 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
- In total, upwards of .25 TB a day (not all RATs)
- If you have malware you want to trade, let’s talk.

Malware Configs

- Every RAT 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
```

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

Why store all that data?

- VirusTotal generally has C2 information (assuming sample runs).
- If vt > 1/55 then dump all network info, apply whitelist, call it a threat intel feed… PROFIT
- VT doesn’t keep configuration information.
- 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?

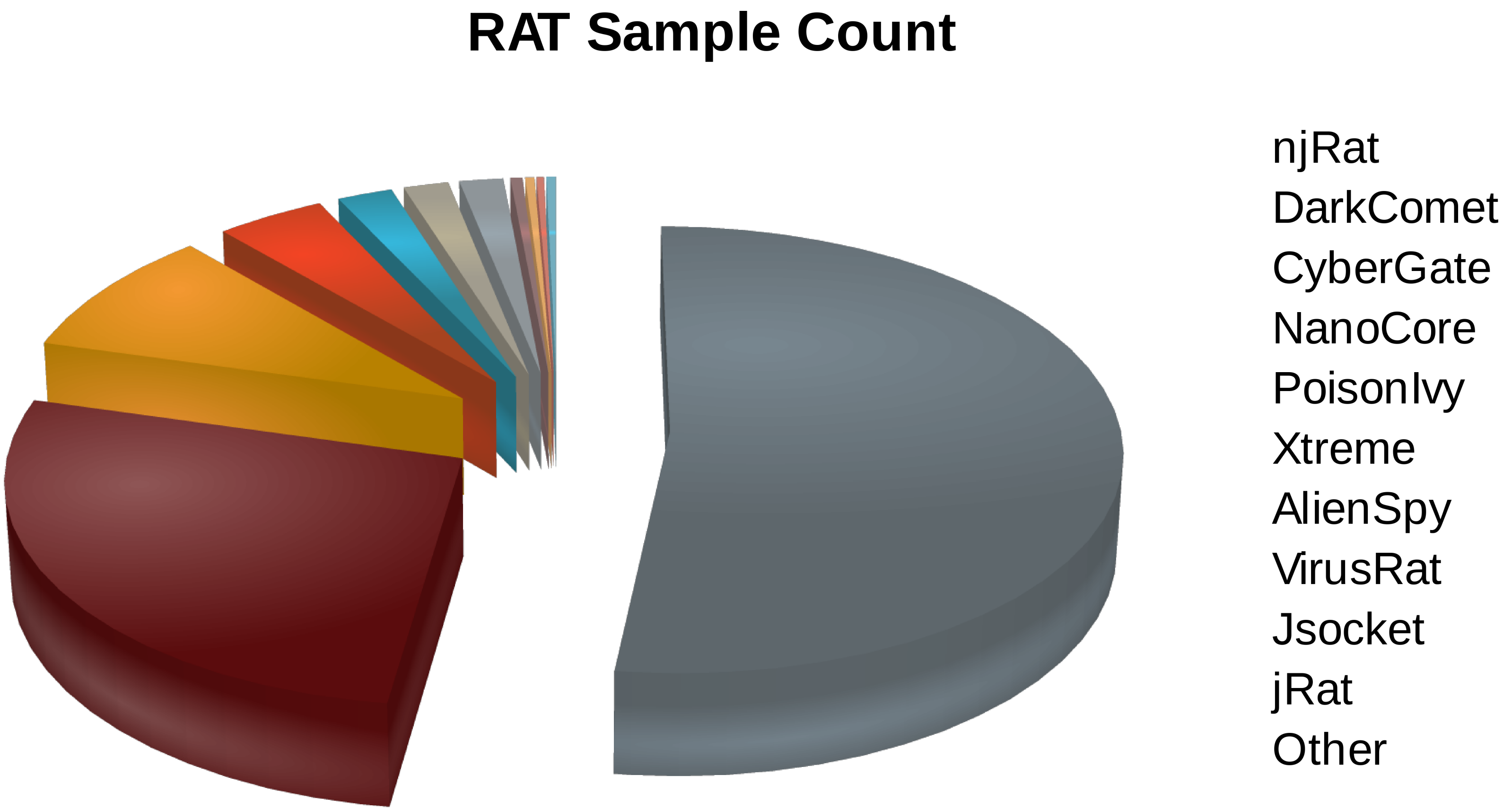
- As a more network-oriented researcher, I ignored many config fields at first.

- Host-based researchers turned this into a big database of IOCs that they used to hunt/block infections.
  - Works even if C2 isn't online (more on that soon).

- Now can take host-based IOCs and backtrace it to initial attack/MD5 and then correlate to other attacks.

- Internally stored in Splunk so we can cross-correlate with our telemetry.

Family Breakdown



Configuration Items

- Most RATs have either free-form text configuration items or randomly generated configuration items:
  - Campaign ID
  - Paths
  - Mutex
  - Registry Keys
- Some have authentication information or FTP server information.
  - This is a great source of temptation for me…
- All can be correlated to link seemingly disparate attacks or to learn something about the attacker.

Dark Comet Campaign IDs

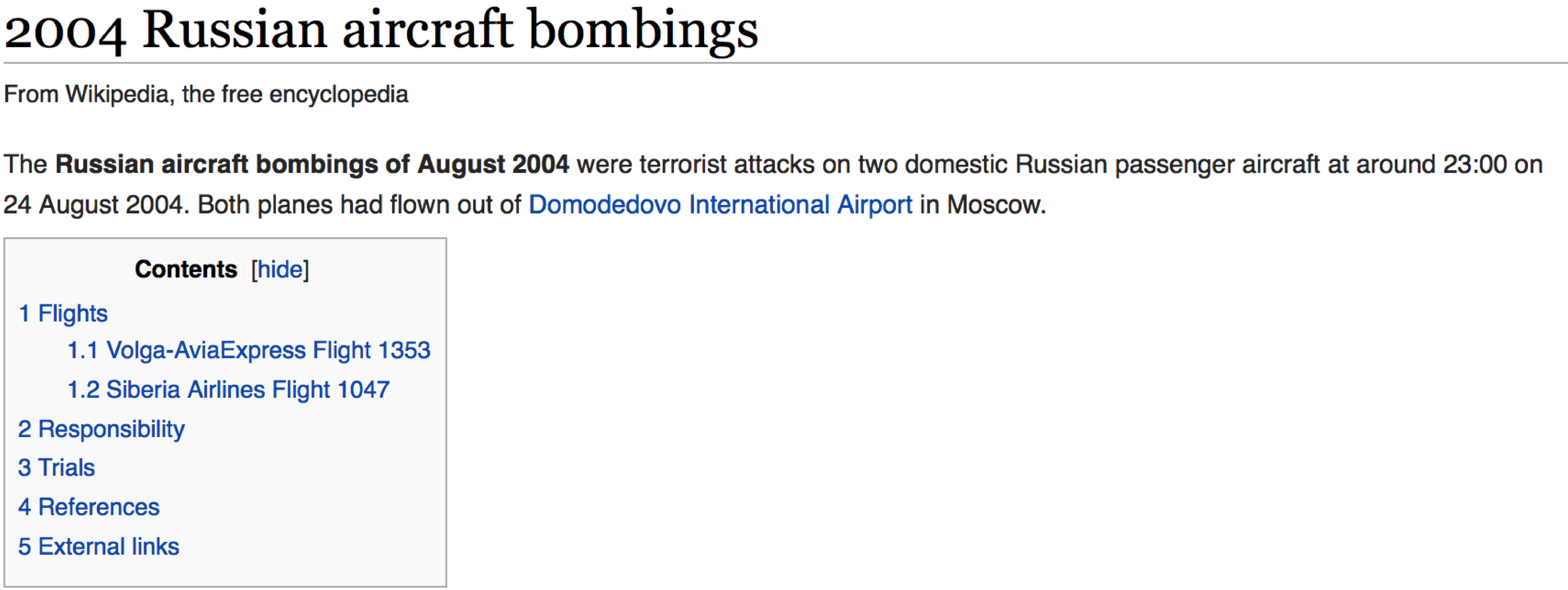
7483	Guest16
967	"Guest16_min"
484	
168	Col334
117	Kurban
102	Solis
102	"new-victims 2.0"
96	"No-IP"
64	Hack
63	okay
55	test
46	Test
46	Hacked
46	Arkade
44	HF
41	Vitima
41	"B--L--A--Y"
38	Guest1
35	Victim
34	HACKED
33	trolled
33	Guest
33	DOS
32	MoyerSK
31	Server
30	LucidsVictim
27	1
26	PC
25	Slave
24	kurban0101
24	Steam
24	DeadPrezidents
23	kurban
23	"Gerek port"
21	MSIL
20	darkcomet
20	Xodiak
20	User
20	SPY
20	DC
19	KURBAN
18	csgolounge
18	Wh1te
18	Rat
18	BITS
17	RAT
17	IronMan
17	HOERTJE
17	All
16	hot
16	hak
16	"CSGO COOLDOWN BYPASSER"
15	Preface
15	LOL
15	Kurbanlar
15	"_2015_F_csgo"
15	"Pack v1.1"
14	hacked
14	HACKER
14	HACK
14	DarkComet
14	Cliente
14	BAMBAM
13	White
13	NewServer
13	Guest17
13	2015
13	"Mommu\y"
13	"???”
12	user

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]

1 Flights
- 1.1 Volga-AviaExpress Flight 1353
- 1.2 Siberia Airlines Flight 1047

2 Responsibility

3 Trials

4 References

5 External links

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,tru
e,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.

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

Network Details

C2 Breakdown

Hostnames
IP addresses

Network Details

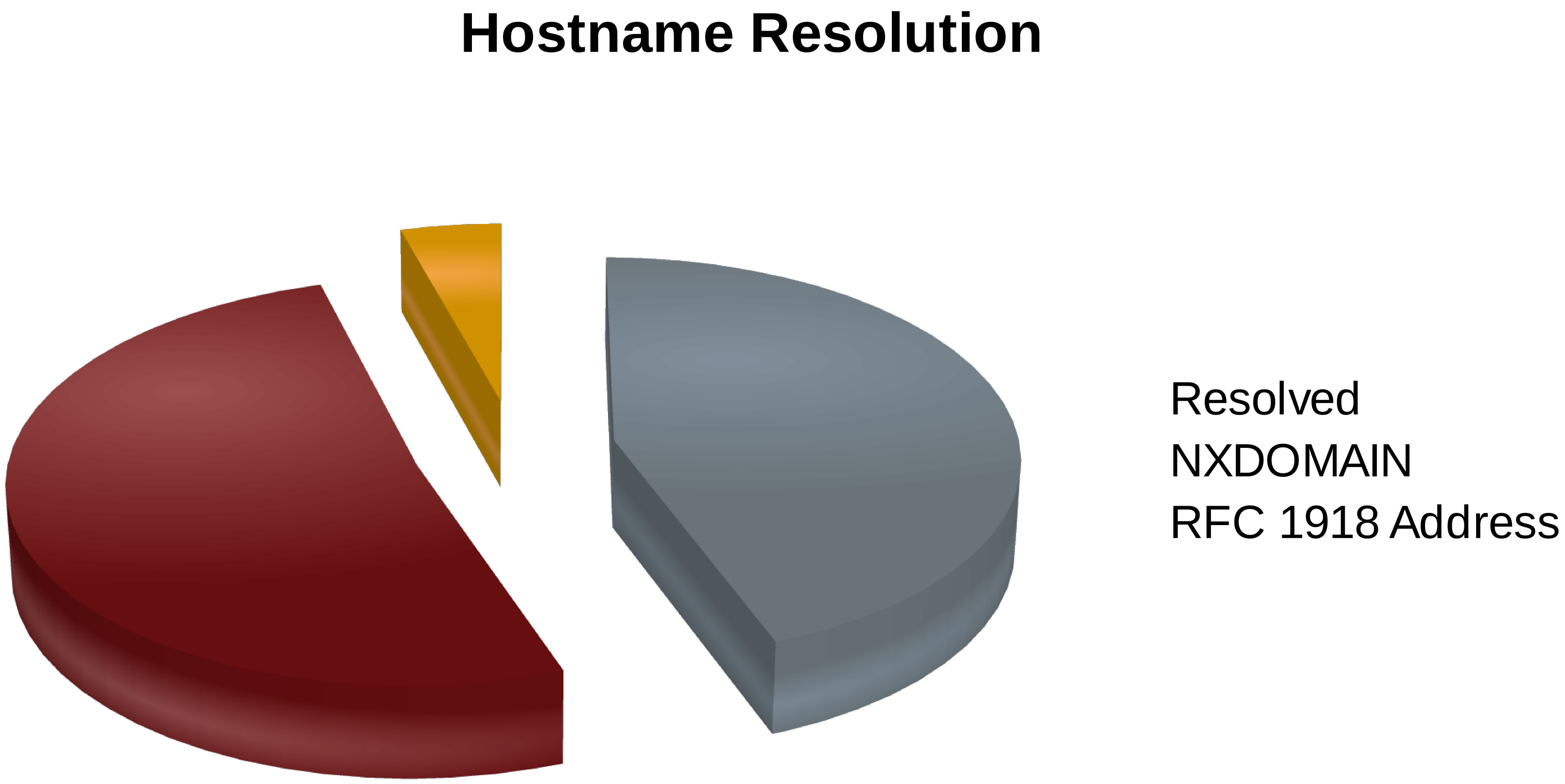
DNS Provider Breakdown

No IP Hostnames
Duck DNS Hostnames
Other DNS Hostnames
IP address only

DNS Services for Malware

- No real surprise that No-IP is common for malware.
- Dyn has all but disappeared now that they charge.
- Duck DNS is new (I only noticed it preparing for this)
- There are other open-source tools to do roll-your-own Dynamic DNS that have cropped up for specific attacks.

Resolving Hostnames (1 June – 1 Oct 2015)



Resolving hostnames

- It seems most RATs aren’t actively resolving (and not actively controlling victims).

- Passive DNS also misses a far bit of these hostnames (~25%, but kept running into query limits ◀◀)

- 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.

Where do RAT C2s live?

Top Cities

- 1723 NO CITY FOUND
- 222 Cairo
- 183 Baghdad
- 112 Istanbul
- 77 Moscow
- 76 Riyadh
- 75 Jeddah
- 71 Amman
- 66 São Paulo
- 65 Casablanca
- 59 Ramallah
- 57 Alexandria
- 47 Paris
- 45 London
- 44 Tel Aviv
- 37 Erbil
- 35 Izmir
- 35 Rio de Janeiro
- 34 Los Angeles
- 30 Kiev
- 30 Ankara
- 30 Agadir
- 30 Chişinău

Top Countries

- 630 United States
- 586 Brazil
- 579 Algeria
- 519 Russia
- 453 Egypt
- 434 Turkey
- 434 France
- 417 Iraq
- 264 Morocco
- 211 United Kingdom
- 201 Ukraine
- 186 Saudi Arabia
- 172 Tunisia
- 146 Netherlands
- 136 Germany
- 107 Palestine
- 96 Canada
- 81 Sweden
- 78 India
- 77 Republic of Korea
- 76 Hashemite Kingdom of Jordan
- 75 Pakistan
- 72 Israel

Counter-intelligence

- Attacks know that we do this and actively throw mud in the water.
- My DGA feeds have seen attackers (or someone else) register a DGA domain and point it to an obvious good IP address.
- 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.

Counter-intelligence

- 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.

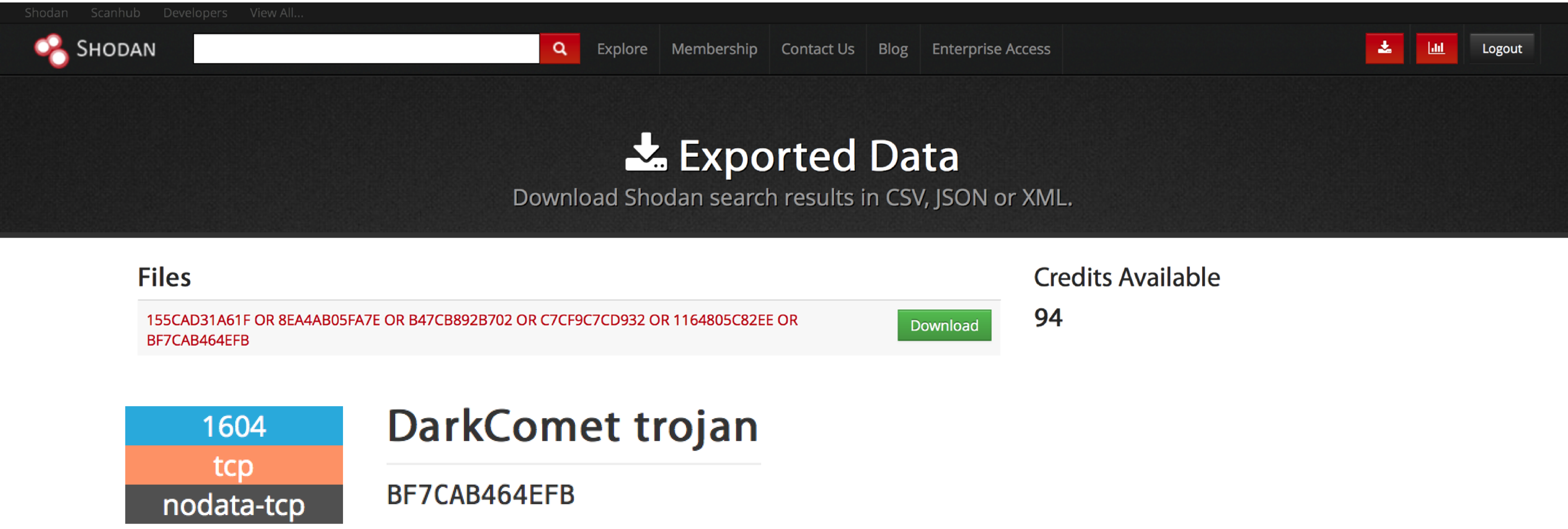
- Additional correlation is needed then just mining VT and becoming Yet-Another-Feed-Vendor.

Edge cases

- A decoder exists for Cryptowall (at least for v3).
- Cryptowall initially calls a compromised domain to get [1-5].php as part of the process to get the encryption key.
- Cryptowall is not the only malware family that uses compromised domains.
- Do you put those into blocklists / indicator lists?
- Similar problem with word-list-based DGAs.

Finding C2s without binaries

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



Exported Data

Download Shodan search results in CSV, JSON or XML.

Files

155CAD31A61F OR 8EA4AB05FA7E OR B47CB892B702 OR C7CF9C7CD932 OR 1164805C82EE OR BF7CAB464EFB

Credits Available

94

1604
tcp
nodata-tcp

DarkComet trojan

BF7CAB464EFB

- Not perfect but did find C2s I was unaware of.

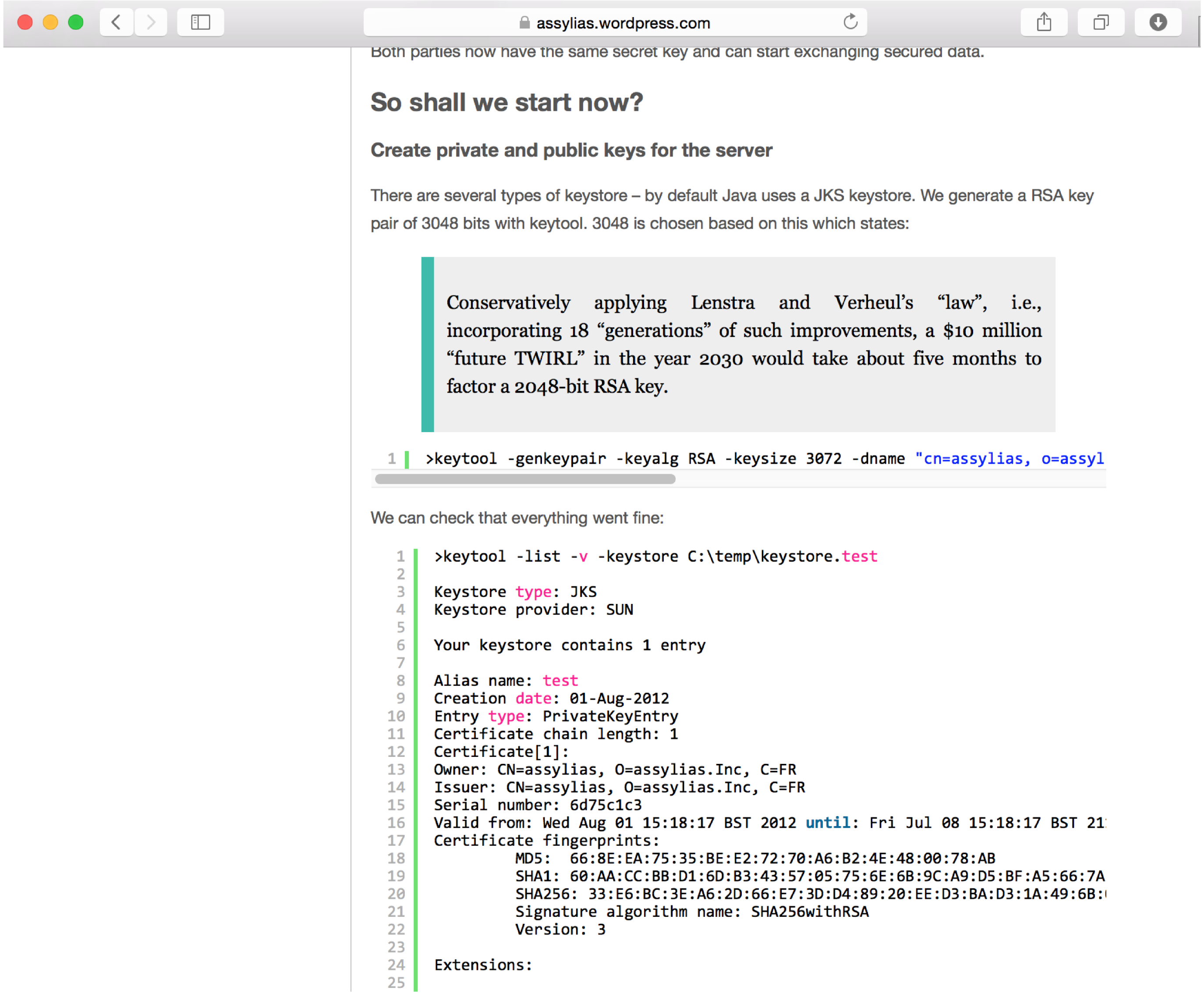
Data not in configuration

- 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?



Both parties now have the same secret key and can start exchanging secured data.

So shall we start now?

Create private and public keys for the server

There are several types of keystore – by default Java uses a JKS keystore. We generate a RSA key pair of 3048 bits with keytool. 3048 is chosen based on this which states:

> Conservatively applying Lenstra and Verheul's "law", i.e., incorporating 18 "generations" of such improvements, a $10 million "future TWIRL" in the year 2030 would take about five months to factor a 2048-bit RSA key.

```
>keytool -genkeypair -keyalg RSA -keysize 3072 -dname "cn=assylias, o=assyl
```

We can check that everything went fine:

```
>keytool -list -v -keystore C:\temp\keystore.test

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: test
Creation date: 01-Aug-2012
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=assylias, O=assylias.Inc, C=FR
Issuer: CN=assylias, O=assylias.Inc, C=FR
Serial number: 6d75c1c3
Valid from: Wed Aug 01 15:18:17 BST 2012 until: Fri Jul 08 15:18:17 BST 21
Certificate fingerprints:
         MD5:  66:8E:EA:75:35:BE:E2:72:70:A6:B2:4E:48:00:78:AB
         SHA1: 60:AA:CC:BB:D1:6D:B3:43:57:05:75:6E:6B:9C:A9:D5:BF:A5:66:7A
         SHA256: 33:E6:BC:3E:A6:2D:66:E7:3D:D4:89:20:EE:D3:BA:D3:1A:49:6B:
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

```

JSocket Certificate Validation

- JSocket builders phone home to verify valid subscription. Builder will not run unless it is presented the correct cert (SSL intercept won’t work).

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

- Some of my other tricks also weren’t able to intercept actually HTTPS traffic.

- Attacker changed keystore password from “storepass” [redacted]

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).

- Or is it?

- 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
- Process historical malware.
- Sharing data out via MISP (will announce when I finally get this up).
- Checking for things that resolve to RFC 1918 then go back to “real IPs”
- Mobile App scanning for malicious signatures.
- Burn/Sink all the things.

Final point

- If you want to share malware or otherwise collaborate on this or other things I work on (ransomware, DDoS, spam malware, DGAs) please get in touch:
  - jcb@people.ops-trust.net

- Let’s burn things ⏪

QUESTIONS?

THANKS KEVIN BREEN, MANY OTHERS.

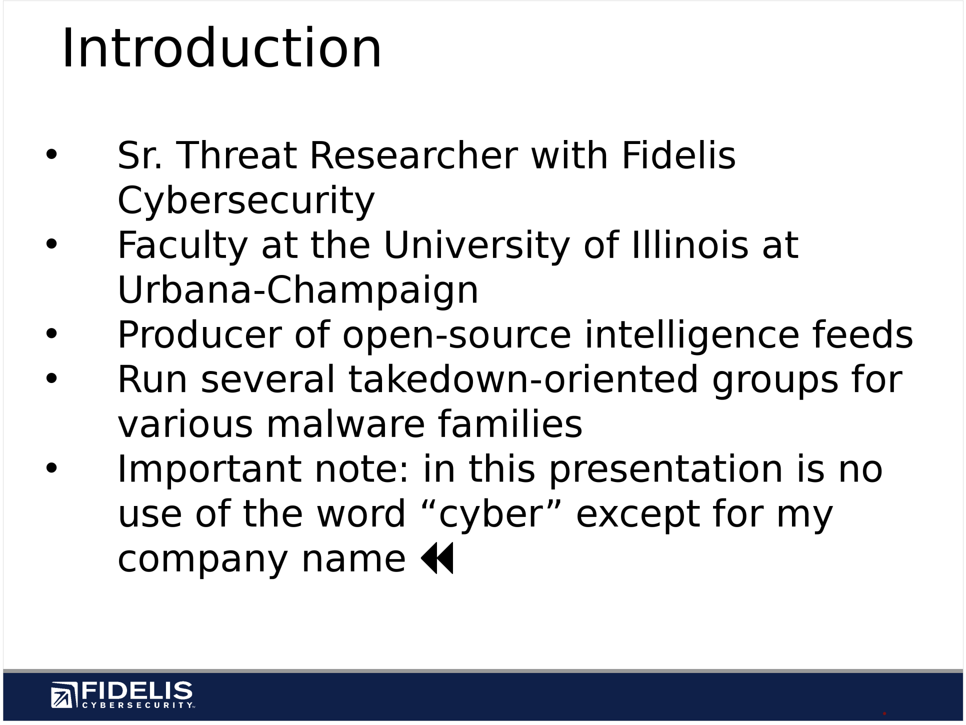
JOHN BAMBENEK
JOHN.BAMBENEK@FIDELISSECURITY.COM
/JCB@PEOPLE.OPS-TRUST.NET
+1 217 493 0760

DGA FEEDS:
OSINT.BAMBENEKCONSULTING.COM/FEEDS/

Mining Malware for Intelligence at Scale

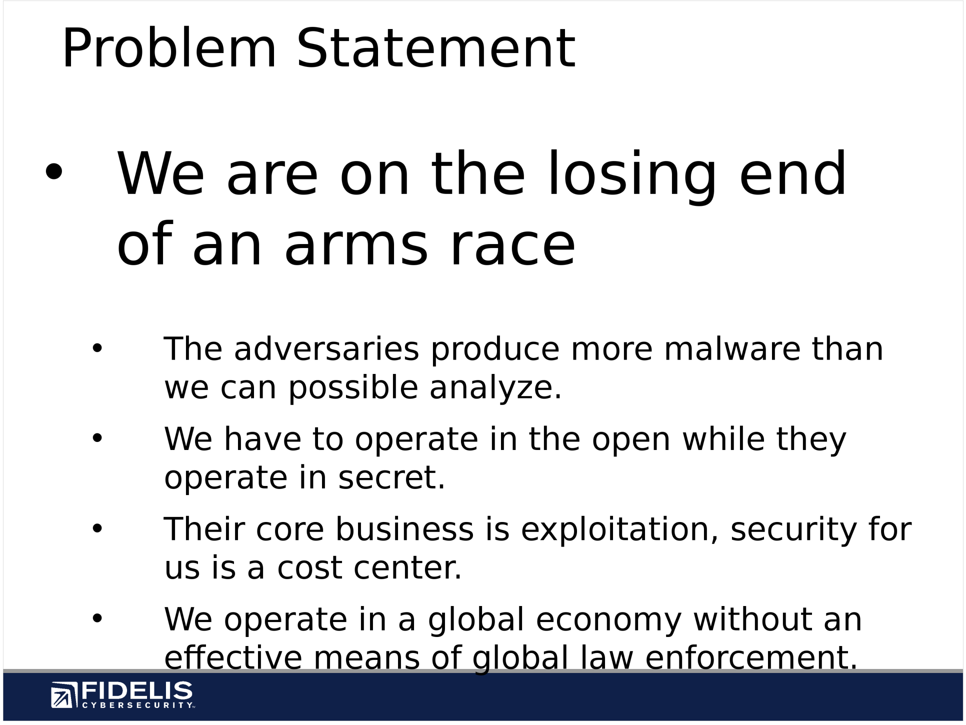
John Bambenek / Sr. Threat Analyst / Threat Research Team

DEEPSEC ‘15 / Vienna, Austria



Introduction

- Sr. Threat Researcher with Fidelis Cybersecurity
- Faculty at the University of Illinois at Urbana-Champaign
- Producer of open-source intelligence feeds
- Run several takedown-oriented groups for various malware families
- Important note: in this presentation is no use of the word “cyber” except for my company name ⏪

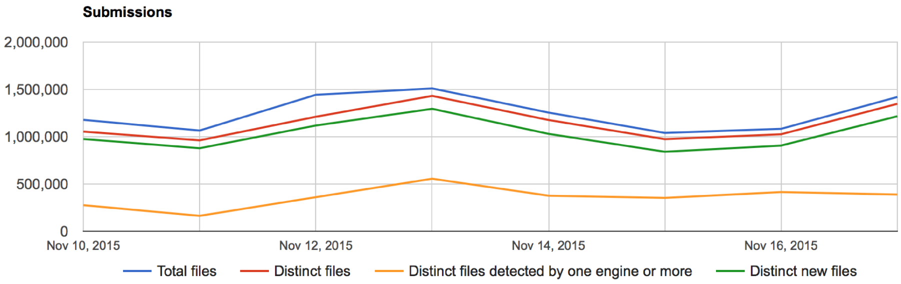


Problem Statement

- We are on the losing end of an arms race
  - The adversaries produce more malware than we can possible analyze.
  - We have to operate in the open while they operate in secret.
  - Their core business is exploitation, security for us is a cost center.
  - We operate in a global economy without an effective means of global law enforcement.

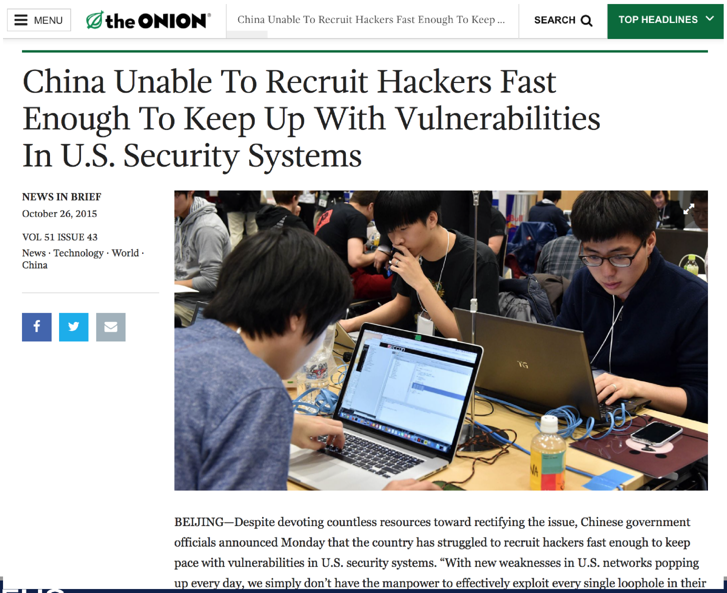
FIDELIS
CYBERSECURITY

The Problem… Illustrated



Virustotal Statistics taken at 18 Nov 2015

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

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.

How to deal with 2M+ samples/day

- Full RE most expensive but most thorough.
- 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 RAT binaries, VT is fine or whatever you have.
- Use Yara and/or AV names to preselect family.
- Run appropriate RAT decoder
- Put in whatever database makes sense to you.
  - Internally use splunk, external sharing via MISP.
- All of this (Except the feed of malware*) is open-source and you can start doing this today.

Why RATs?

- Single stage malware will generally always have full configuration in the binary itself.

- Used not just by skiddies but by advanced attackers also such as nation-states and terrorist affiliated entities.

- Dozens of RAT types all well-known to deal with.

- Gotta walk before you can run.

- That said, Dridex/Cridex integrated too now.

What can you do with RAT configs?

We don’t need another whitepaper. What we need is bodies in the street.

What can you do with RAT 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.

Also, there is this magic sauce…

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

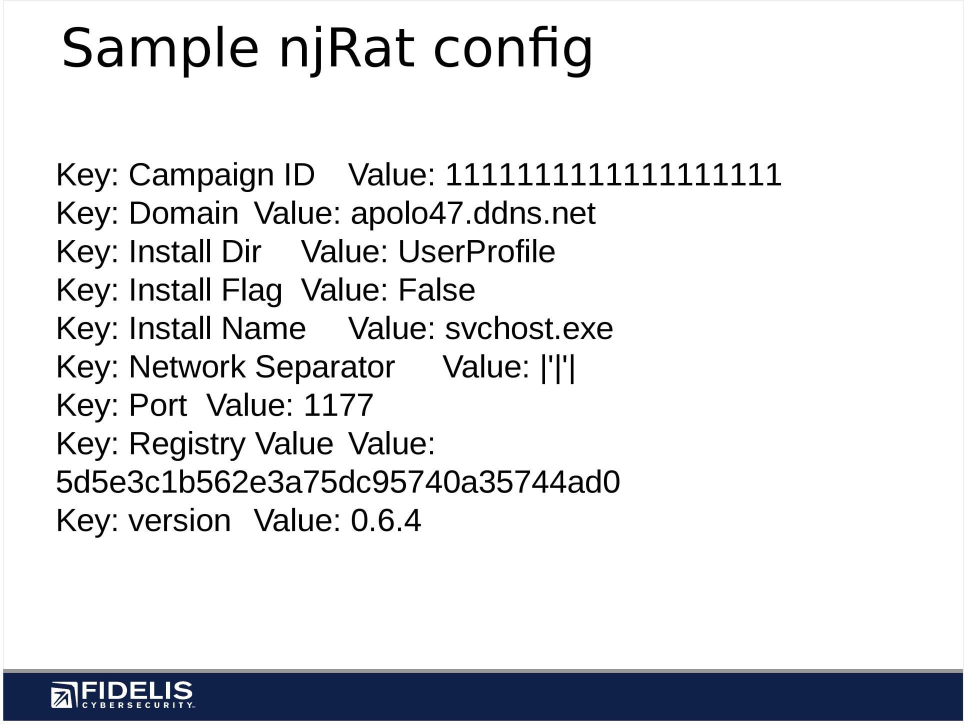
- VirusTotal
- MSFT VIA Program
- Other malware sharing programs
- Internal sources
- In total, upwards of .25 TB a day (not all RATs)
- If you have malware you want to trade, let’s talk.

Malware Configs

- Every RAT 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
```

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

Why store all that data?

- VirusTotal generally has C2 information (assuming sample runs).

- If vt > 1/55 then dump all network info, apply whitelist, call it a threat intel feed… PROFIT

- VT doesn’t keep configuration information.

- 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?

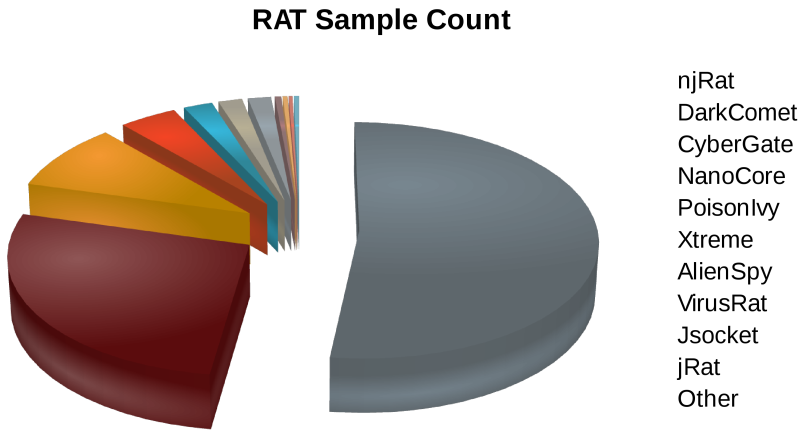
- As a more network-oriented researcher, I ignored many config fields at first.

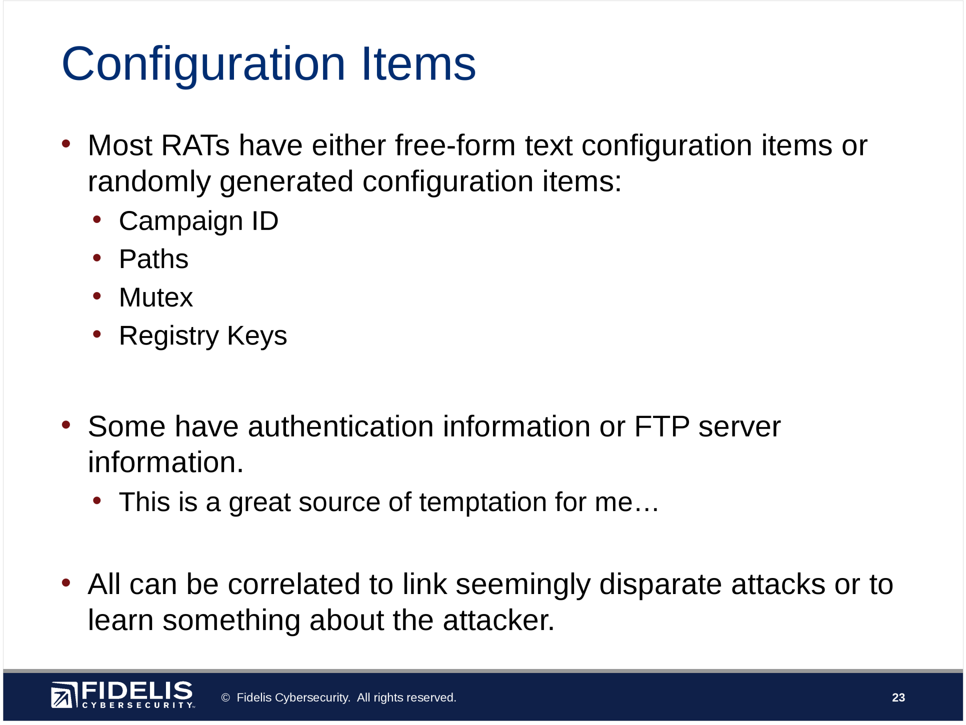
- Host-based researchers turned this into a big database of IOCs that they used to hunt/block infections.
  - Works even if C2 isn't online (more on that soon).

- Now can take host-based IOCs and backtrace it to initial attack/MD5 and then correlate to other attacks.

- Internally stored in Splunk so we can cross-correlate with our telemetry.

Family Breakdown





Configuration Items

- Most RATs have either free-form text configuration items or randomly generated configuration items:
  - Campaign ID
  - Paths
  - Mutex
  - Registry Keys

- Some have authentication information or FTP server information.
  - This is a great source of temptation for me…

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

Dark Comet Campaign IDs

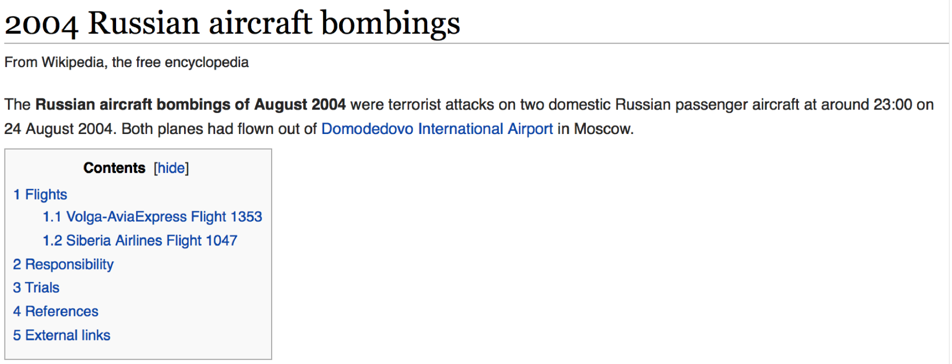
7483	Guest16
967	"Guest16_min"
484	
168	Col334
117	Kurban
102	Solis
102	"new-victims 2.0"
96	"No-IP"
64	Hack
63	okay
55	test
46	Test
46	Hacked
46	Arkade
44	HF
41	Vitima
41	"B--L--A--Y"
38	Guest1
35	Victim
34	HACKED
33	trolled
33	Guest
33	DOS
32	MoyerSK
31	Server
30	LucidsVictim
27	1
26	PC
25	Slave
24	kurban0101
24	Steam
24	DeadPrezidents
23	kurban
23	"Gerek port"
21	MSIL
20	darkcomet
20	Xodiak
20	User
20	SPY
20	DC
19	KURBAN
18	csgolounge
18	Wh1te
18	Rat
18	BITS
17	RAT
17	IronMan
17	HOERTJE
17	All
16	hot
16	hak
16	"CSGO COOLDOWN BYPASSER"
15	Preface
15	LOL
15	Kurbanlar
15	"_2015_F_csgo"
15	"Pack v1.1"
14	hacked
14	HACKER
14	HACK
14	DarkComet
14	Cliente
14	BAMBAM
13	White
13	NewServer
13	Guest17
13	2015
13	"Mommu\y"
13	"???”
12	user

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.

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

Network Details

C2 Breakdown

Hostnames
IP addresses

Network Details

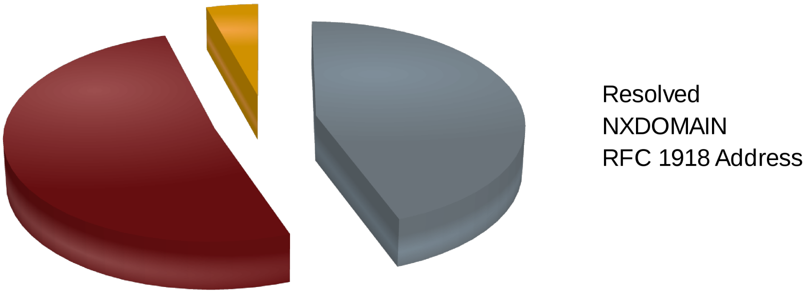
DNS Provider Breakdown

No IP Hostnames
Duck DNS Hostnames
Other DNS Hostnames
IP address only

DNS Services for Malware

- No real surprise that No-IP is common for malware.
- Dyn has all but disappeared now that they charge.
- Duck DNS is new (I only noticed it preparing for this)
- There are other open-source tools to do roll-your-own Dynamic DNS that have cropped up for specific attacks.

Resolving Hostnames (1 June – 1 Oct 2015)



Resolving hostnames

- It seems most RATs aren’t actively resolving (and not actively controlling victims).
- Passive DNS also misses a far bit of these hostnames (~25%, but kept running into query limits ◀◀)
- 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.

Where do RAT C2s live?

Top Cities

- 1723 NO CITY FOUND
- 222 Cairo
- 183 Baghdad
- 112 Istanbul
- 77 Moscow
- 76 Riyadh
- 75 Jeddah
- 71 Amman
- 66 São Paulo
- 65 Casablanca
- 59 Ramallah
- 57 Alexandria
- 47 Paris
- 45 London
- 44 Tel Aviv
- 37 Erbil
- 35 Izmir
- 35 Rio de Janeiro
- 34 Los Angeles
- 30 Kiev
- 30 Ankara
- 30 Agadir
- 30 Chişinău

Top Countries

- 630 United States
- 586 Brazil
- 579 Algeria
- 519 Russia
- 453 Egypt
- 434 Turkey
- 434 France
- 417 Iraq
- 264 Morocco
- 211 United Kingdom
- 201 Ukraine
- 186 Saudi Arabia
- 172 Tunisia
- 146 Netherlands
- 136 Germany
- 107 Palestine
- 96 Canada
- 81 Sweden
- 78 India
- 77 Republic of Korea
- 76 Hashemite Kingdom of Jordan
- 75 Pakistan
- 72 Israel

Counter-intelligence

- Attacks know that we do this and actively throw mud in the water.

- My DGA feeds have seen attackers (or someone else) register a DGA domain and point it to an obvious good IP address.

- 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.

Counter-intelligence

- 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.

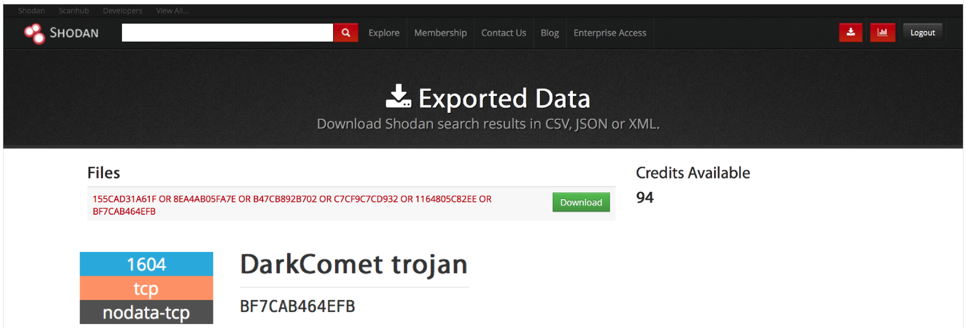
- Additional correlation is needed then just mining VT and becoming Yet-Another-Feed-Vendor.

Edge cases

- A decoder exists for Cryptowall (at least for v3).
- Cryptowall initially calls a compromised domain to get [1-5].php as part of the process to get the encryption key.
- Cryptowall is not the only malware family that uses compromised domains.
- Do you put those into blocklists / indicator lists?
- Similar problem with word-list-based DGAs.

Finding C2s without binaries

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



Exported Data

Download Shodan search results in CSV, JSON or XML.

Files

155CAD31A61F OR 8EA4AB05FA7E OR B47CB892B702 OR C7CF9C7CD932 OR 1164805C82EE OR BF7CAB464EFB

Credits Available

94

1604
tcp
nodata-tcp

DarkComet trojan

BF7CAB464EFB

- Not perfect but did find C2s I was unaware of.

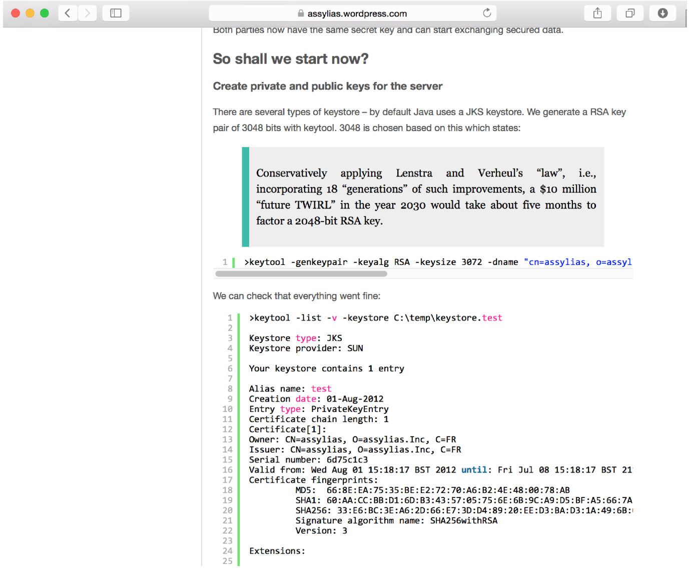
Data not in configuration

- 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?



Both parties now have the same secret key and can start exchanging secured data.

So shall we start now?

Create private and public keys for the server

There are several types of keystore – by default Java uses a JKS keystore. We generate a RSA key pair of 3048 bits with keytool. 3048 is chosen based on this which states:

> Conservatively applying Lenstra and Verheul's "law", i.e., incorporating 18 "generations" of such improvements, a $10 million "future TWIRL" in the year 2030 would take about five months to factor a 2048-bit RSA key.

```
>keytool -genkeypair -keyalg RSA -keysize 3072 -dname "cn=assylias, o=assyl
```

We can check that everything went fine:

```
>keytool -list -v -keystore C:\temp\keystore.test

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: test
Creation date: 01-Aug-2012
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=assylias, O=assylias.Inc, C=FR
Issuer: CN=assylias, O=assylias.Inc, C=FR
Serial number: 6d75c1c3
Valid from: Wed Aug 01 15:18:17 BST 2012 until: Fri Jul 08 15:18:17 BST 21
Certificate fingerprints:
         MD5:  66:8E:EA:75:35:BE:E2:72:70:A6:B2:4E:48:00:78:AB
         SHA1: 60:AA:CC:BB:D1:6D:B3:43:57:05:75:6E:6B:9C:A9:D5:BF:A5:66:7A
         SHA256: 33:E6:BC:3E:A6:2D:66:E7:3D:D4:89:20:EE:D3:BA:D3:1A:49:6B:
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

```

JSocket Certificate Validation

- JSocket builders phone home to verify valid subscription. Builder will not run unless it is presented the correct cert (SSL intercept won’t work).
- JSocket builder itself has a cert which is used to verify the builder (all builders use same one, the Assylias cert).
- Some of my other tricks also weren’t able to intercept actually HTTPS traffic.
- Attacker changed keystore password from “storepass” [redacted]

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).
- Or is it?
- 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
- Process historical malware.
- Sharing data out via MISP (will announce when I finally get this up).
- Checking for things that resolve to RFC 1918 then go back to “real IPs”
- Mobile App scanning for malicious signatures.
- Burn/Sink all the things.

Final point

- If you want to share malware or otherwise collaborate on this or other things I work on (ransomware, DDoS, spam malware, DGAs) please get in touch:
  - jcb@people.ops-trust.net

- Let’s burn things ⏪

QUESTIONS?

THANKS 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/