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
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](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

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CampaignID</td>
<td>Guest16</td>
</tr>
<tr>
<td>Domains</td>
<td>06059600929.ddns.net:1234</td>
</tr>
<tr>
<td>FTPHost</td>
<td></td>
</tr>
<tr>
<td>FTPKeyLogs</td>
<td></td>
</tr>
<tr>
<td>FTPPassword</td>
<td></td>
</tr>
<tr>
<td>FTPPort</td>
<td></td>
</tr>
<tr>
<td>FTPRoot</td>
<td></td>
</tr>
<tr>
<td>FTPSize</td>
<td></td>
</tr>
<tr>
<td>FTPUserName</td>
<td></td>
</tr>
<tr>
<td>FireWallBypass</td>
<td>0</td>
</tr>
<tr>
<td>Gencode</td>
<td>3yHVnheK6eDm</td>
</tr>
<tr>
<td>Mutex</td>
<td>DC_MUTEX-W45NCJ6</td>
</tr>
<tr>
<td>OfflineKeylogger</td>
<td>1</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>#KCMDDC51#</td>
</tr>
</tbody>
</table>
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, CONNEXTION_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, 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, NICK NAME, NetworkSeparator, OS, OfflineKeylogger, Origin, P2PSpread, PLUGIN_EXTENSION, PLUGINS_FOLDER, Password, Perms, Persistence, 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, ahref, 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, linetype, 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_.TEXT, section_.RDATA, section_.RELOC, section_.RSRC, section_.TEXT, section_.TLS, section_AKMBZMH, section_BSS, section_CODE, section_DATA, section_ELTOHVWF, section_VD0JLYFM, section_YRKCHNMU, sha1, sha256, source, sourcetype, splunk_server, splunk_server_group, spybot, super, tag, tag::eventtype, taskmgr, times_submitted, timestamp, 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...

```json
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": "wcniXbslsn",
  "JAR_NAME": "Fresh_Bomb",
  "JAR_REGISTRY": "CopaNwxcFs5",
  "JRE_FOLDER": "UOStKe",
  "NICKNAME": "August24rdBomBing",
  "Origin": "vt",
  "PLUGIN_EXTENSION": "lykYQ",
  "PLUGIN_FOLDER": "LOZQqgmCGJ4",
  "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": "be0f6903b3217c8df94c69dc0e58ee1c07e92ab563bc4015f1a49a1dcf99acf",
  "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]
1 Flights
   1.1 Volga-AviaExpress Flight 1353
   1.2 Siberia Airlines Flight 1047
2 Responsibility
3 Trials
4 References
5 External links
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
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

<table>
<thead>
<tr>
<th>ID</th>
<th>Term</th>
<th>ID</th>
<th>Term</th>
<th>ID</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>24597</td>
<td>Guest16</td>
<td>755</td>
<td>All</td>
<td>337</td>
<td>Kurban</td>
</tr>
<tr>
<td>232</td>
<td>Hacked</td>
<td>181</td>
<td>test</td>
<td>168</td>
<td>Col334</td>
</tr>
<tr>
<td>140</td>
<td>Hack</td>
<td>129</td>
<td>Test</td>
<td>128</td>
<td>Guest</td>
</tr>
<tr>
<td>118</td>
<td>PC</td>
<td>105</td>
<td>new-vict</td>
<td>105</td>
<td>1</td>
</tr>
<tr>
<td>99</td>
<td>Slave</td>
<td>93</td>
<td>Vitima</td>
<td>85</td>
<td>User</td>
</tr>
<tr>
<td>68</td>
<td>all</td>
<td>68</td>
<td>Guest17</td>
<td>66</td>
<td>DOS</td>
</tr>
<tr>
<td>55</td>
<td>hack</td>
<td>53</td>
<td>228</td>
<td>50</td>
<td>apb</td>
</tr>
<tr>
<td>49</td>
<td>Hacker</td>
<td>46</td>
<td>Arkade</td>
<td>44</td>
<td>DC</td>
</tr>
<tr>
<td>42</td>
<td>Steam</td>
<td>41</td>
<td>HACK</td>
<td>40</td>
<td>server</td>
</tr>
<tr>
<td>39</td>
<td>hacked</td>
<td>36</td>
<td>TestGues</td>
<td>36</td>
<td>DhjetoR</td>
</tr>
<tr>
<td>34</td>
<td>123</td>
<td>33</td>
<td>DarkCome</td>
<td>32</td>
<td>user</td>
</tr>
<tr>
<td>32</td>
<td>Rat-1</td>
<td>31</td>
<td>MoyerSK</td>
<td>31</td>
<td>2</td>
</tr>
<tr>
<td>29</td>
<td>trolled</td>
<td>29</td>
<td>MSIL</td>
<td>28</td>
<td>BOT</td>
</tr>
<tr>
<td>27</td>
<td>TEST</td>
<td>25</td>
<td>Rat</td>
<td>24</td>
<td>kurban01</td>
</tr>
<tr>
<td>24</td>
<td>Darkcome</td>
<td>23</td>
<td>Server1</td>
<td>23</td>
<td>CSGO</td>
</tr>
<tr>
<td>22</td>
<td>darkcome</td>
<td>22</td>
<td>Youtube</td>
<td>22</td>
<td>Minecraf</td>
</tr>
<tr>
<td>21</td>
<td>victime</td>
<td>21</td>
<td>test1</td>
<td>21</td>
<td>kurban1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Fidelis Cybersecurity. All rights reserved.
### njRat Campaign IDs

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>ID</th>
<th>Description</th>
<th>ID</th>
<th>Description</th>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>47736</td>
<td>HackEd</td>
<td>632</td>
<td>Hacked</td>
<td>455</td>
<td>Vitima</td>
<td>371</td>
<td>hacked</td>
</tr>
<tr>
<td>175</td>
<td>vitima</td>
<td>162</td>
<td>Victim</td>
<td>156</td>
<td>hacker</td>
<td>123</td>
<td>system</td>
</tr>
<tr>
<td>113</td>
<td>teste</td>
<td>110</td>
<td>svchost</td>
<td>110</td>
<td>1</td>
<td>98</td>
<td>Test</td>
</tr>
<tr>
<td>102</td>
<td>google</td>
<td>101</td>
<td>LpeH</td>
<td>98</td>
<td>HackED</td>
<td>98</td>
<td>89 server</td>
</tr>
<tr>
<td>86</td>
<td>HackEd</td>
<td>79</td>
<td>Vitimas</td>
<td>75</td>
<td>hack</td>
<td>72</td>
<td>HACKEDEI</td>
</tr>
<tr>
<td>67</td>
<td>new</td>
<td>67</td>
<td>HackEd</td>
<td>63</td>
<td>facebook</td>
<td>63</td>
<td>ahmed</td>
</tr>
<tr>
<td>57</td>
<td>Server</td>
<td>52</td>
<td>windows</td>
<td>52</td>
<td>VITIMA</td>
<td>52</td>
<td>Minecraf</td>
</tr>
<tr>
<td>50</td>
<td>Slave</td>
<td>48</td>
<td>ana</td>
<td>48</td>
<td>PB</td>
<td>46</td>
<td>ROOTED</td>
</tr>
<tr>
<td>45</td>
<td>Hack 44</td>
<td>123</td>
<td>ali</td>
<td>110</td>
<td>1</td>
<td>104</td>
<td>victim</td>
</tr>
<tr>
<td>40</td>
<td>alob</td>
<td>40</td>
<td>Facebook</td>
<td>39</td>
<td>svchost.</td>
<td>39</td>
<td>haker</td>
</tr>
<tr>
<td>39</td>
<td>Otario</td>
<td>38</td>
<td>victim</td>
<td>38</td>
<td>explorer</td>
<td>38</td>
<td>Snopi Bi</td>
</tr>
<tr>
<td>37</td>
<td>Skype</td>
<td>36</td>
<td>chrome</td>
<td>36</td>
<td>Windows</td>
<td>35</td>
<td>Hack</td>
</tr>
<tr>
<td>34</td>
<td>HackEd2</td>
<td>34</td>
<td>Google C</td>
<td>34</td>
<td>0</td>
<td>33</td>
<td>PointBla</td>
</tr>
<tr>
<td>32</td>
<td>matrix</td>
<td>32</td>
<td>hhh</td>
<td>32</td>
<td>HackEd</td>
<td>30</td>
<td>win7</td>
</tr>
<tr>
<td>30</td>
<td>Texte</td>
<td>30</td>
<td>New</td>
<td>30</td>
<td>Microsof</td>
<td>30</td>
<td>Fucked</td>
</tr>
<tr>
<td>29</td>
<td>System</td>
<td>29</td>
<td>Cobaia</td>
<td>28</td>
<td>n3aL</td>
<td>28</td>
<td>Anonymou</td>
</tr>
<tr>
<td>27</td>
<td>radar</td>
<td>27</td>
<td>User</td>
<td>27</td>
<td>HackEd B</td>
<td>27</td>
<td>2016</td>
</tr>
<tr>
<td>25</td>
<td>Torrent</td>
<td>25</td>
<td>Dr_Error</td>
<td>24</td>
<td>sadam</td>
<td>24</td>
<td>lol</td>
</tr>
<tr>
<td>24</td>
<td>Hunted</td>
<td>24</td>
<td>HackEd b</td>
<td>24</td>
<td>HackEd B</td>
<td>24</td>
<td>Chrome</td>
</tr>
</tbody>
</table>

© Fidelis Cybersecurity
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.moooo.com
5 arseisa.no-ip.org
4 testando.no-ip.biz
4 shakal2.ddns.net
4 peterpanjack.no-ip.org
4 odjwowjawja0d.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

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

Lammer,,DarkComet
Lammer,,SpyGate
Lammer,,VirusRat
Lammer,,njRat
## Technique can be used to feed DGAs

From Cert.PL malware ripper

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>binary</td>
<td>6eb749c3519e17f4051cbdd1de993cd2</td>
</tr>
<tr>
<td>rc4key</td>
<td>c2Jw73NaoZ837Yhe</td>
</tr>
<tr>
<td>base-domain</td>
<td>g0jdy3826yenz63om.cc</td>
</tr>
<tr>
<td>timestamp</td>
<td>2016-01-11 12:06:07</td>
</tr>
<tr>
<td>post-path</td>
<td>/go8dj37dh672bxj81id/</td>
</tr>
<tr>
<td>cnc</td>
<td>g0jdy3826yenz63om.cc</td>
</tr>
<tr>
<td>botnet</td>
<td>262-N-L</td>
</tr>
<tr>
<td>public_key</td>
<td>-----BEGIN PUBLIC KEY----- MIIIBTANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQBjB1wYUsVbOvAYR+yWQLUp3JvZu1E6p1NepSx+XG6yn71W9yy56dK/Kcml6c6vkc11b8kym/MwLwP+QNZFm77Pa0S9ptS6gk9S89TFtkS51zDk5KvIeYWol74V32dGwjeR2208swcQEOITjRba5IqskpA9N/kS1mU1UWH1Yn1KCyca39xK5zMy4N4bvwSiST0m5SzGvmFTJhANVzdFjUXq2Hw1vvwr6lYhxQsVrPMTf8iiZ567Ju1ARbexJg0ILORz2vVZ57/wScqQ6F+GbhNvjYrLVyn/f0x0NpFJnP5IpSjD602ys/3GVh2fl7ede8BTblRjgQFSMFexAgMBAAE= -----END PUBLIC KEY-----</td>
</tr>
<tr>
<td>type</td>
<td>tinba_dga</td>
</tr>
<tr>
<td>tid</td>
<td>corn.net.in,ru</td>
</tr>
</tbody>
</table>
C2 Details Breakdown

- IP: 14%
- No-Ip: 76%
- DuckDNS: 2%
- Chickenkiller: 3%
- Other DNS: 5%

© Fidelis Cybersecurity
Resolved 29%

NXDOMAIN 67%

RFC 1918 Address 2%

0.0.0.0 2%
## IP GeoLocation

### Countries

<table>
<thead>
<tr>
<th>Country</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Russia</td>
<td>1506</td>
</tr>
<tr>
<td>Brazil</td>
<td>1318</td>
</tr>
<tr>
<td>&quot;United States&quot;</td>
<td>1219</td>
</tr>
<tr>
<td>Turkey</td>
<td>961</td>
</tr>
<tr>
<td>France</td>
<td>857</td>
</tr>
<tr>
<td>Algeria</td>
<td>729</td>
</tr>
<tr>
<td>Egypt</td>
<td>588</td>
</tr>
<tr>
<td>Ukraine</td>
<td>543</td>
</tr>
<tr>
<td>&quot;United Kingdom&quot;</td>
<td>488</td>
</tr>
<tr>
<td>Morocco</td>
<td>373</td>
</tr>
<tr>
<td>Germany</td>
<td>366</td>
</tr>
<tr>
<td>Iraq</td>
<td>321</td>
</tr>
<tr>
<td>&quot;Saudi Arabia&quot;</td>
<td>284</td>
</tr>
<tr>
<td>Netherlands</td>
<td>281</td>
</tr>
<tr>
<td>&quot;Republic of Korea&quot;</td>
<td>228</td>
</tr>
<tr>
<td>Tunisia</td>
<td>220</td>
</tr>
<tr>
<td>Canada</td>
<td>200</td>
</tr>
<tr>
<td>Palestine</td>
<td>151</td>
</tr>
<tr>
<td>United States</td>
<td>1219</td>
</tr>
<tr>
<td>Turkey</td>
<td>961</td>
</tr>
<tr>
<td>France</td>
<td>857</td>
</tr>
<tr>
<td>Algeria</td>
<td>729</td>
</tr>
<tr>
<td>Egypt</td>
<td>588</td>
</tr>
<tr>
<td>Ukraine</td>
<td>543</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>488</td>
</tr>
<tr>
<td>Morocco</td>
<td>373</td>
</tr>
<tr>
<td>Germany</td>
<td>366</td>
</tr>
<tr>
<td>Iraq</td>
<td>321</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>284</td>
</tr>
<tr>
<td>Netherlands</td>
<td>281</td>
</tr>
<tr>
<td>Republic of Korea</td>
<td>228</td>
</tr>
<tr>
<td>Tunisia</td>
<td>220</td>
</tr>
<tr>
<td>Canada</td>
<td>200</td>
</tr>
<tr>
<td>Palestine</td>
<td>151</td>
</tr>
</tbody>
</table>

### Cities

<table>
<thead>
<tr>
<th>City</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cairo</td>
<td>278</td>
</tr>
<tr>
<td>Istanbul</td>
<td>268</td>
</tr>
<tr>
<td>Moscow</td>
<td>242</td>
</tr>
<tr>
<td>&quot;São Paulo&quot;</td>
<td>143</td>
</tr>
<tr>
<td>Baghdad</td>
<td>112</td>
</tr>
<tr>
<td>Jeddah</td>
<td>106</td>
</tr>
<tr>
<td>Riyadh</td>
<td>96</td>
</tr>
<tr>
<td>Paris</td>
<td>94</td>
</tr>
<tr>
<td>Casablanca</td>
<td>91</td>
</tr>
<tr>
<td>Ramallah</td>
<td>89</td>
</tr>
<tr>
<td>Ankara</td>
<td>77</td>
</tr>
<tr>
<td>&quot;Rio de Janeiro&quot;</td>
<td>71</td>
</tr>
<tr>
<td>&quot;Saint Petersburg&quot;</td>
<td>68</td>
</tr>
<tr>
<td>London</td>
<td>67</td>
</tr>
<tr>
<td>Kiev</td>
<td>67</td>
</tr>
<tr>
<td>Amman</td>
<td>67</td>
</tr>
<tr>
<td>Montreal</td>
<td>65</td>
</tr>
<tr>
<td>&quot;Tel Aviv&quot;</td>
<td>65</td>
</tr>
</tbody>
</table>

© Fidelis Cybersecurity
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: qktT87XaVzk
  Mutex: DC_MUTEX-6RS8T6J
  OfflineKeylogger: 1
  Origin: vt
  Port: 1604
  Version: #KCMDCS51#
  compile_date: 2012-06-08 11:12:27
  imphash: B033c11f8a2fdefc317e8655120579933
  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_.TEXT: 7d01b8ff4c5f6f96e21ff89f0f28e5b49
  section_.RELOCS: 4c788dfe6b92b0f0c5f5aeeaf1270f8
  section_.RELOC: 5090ac335a7094d529e15198df1c5920
  section_.RSRC: dae984d74cf7c8d9674bfe8db73d7cfc
  section_.TEXT: c8087ea6a249266ed1db0453229b76c2
  section_.TLS: d41d8cd98f00b204e9800998ecf8427e
  sha1: 5d171467fcbf07bc3be50c019b077b3792dd668
  sha256: 8f507788204bb8842c5a99df6ec2f299828587c5624fabb45e20c317c977c381
  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?

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 3048 -dname "cn=assylias, o=assyliap"
```

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: 6d79c1c3
Certificate Fngerprints:
Signature algorithm name: SHA256withRSA
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=Cincinnati, 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=Cincinnati, 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 Leedey and rest of my team for their effort on this.