
# DGAs, DNS and Threat Intelligence

John Bambenek - Fidelis Cybersecurity Threat Research Team

ISC 2015 - September 30, 2015 - Beijing, China

# Intro

- Sr. Threat Analyst for Fidelis Cybersecurity
- Adjunct Faculty in CS Department at the University of Illinois at Urbana-Champaign
- Producer of open-source intel feeds
- Work with companies and LE all over the world to address growth in cybercrime

# 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.

# Malware C2 Network Types

- Static IP / Hostname Lists
- Proxied C2s
- Dynamic DNS
- Fast Flux / Double Flux Networks
- Domain Generation Algorithms
- Tor / i2p hidden services

# Static lists

- Many forms of malware have a simple list of hostnames/IPs and ports that it uses for C2 communications.
- A common example are Remote Access Tools.
- RATs also tend to have configuration items that can also provide a wealth of other intelligence.

# Static Config Extraction

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

- Python scripts that will *statically* rip configurations out of 32 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.

# The next piece of the puzzle

- In order to determine which decoder to use, you need to know which malware it is.

- Yara used for this piece using configs from:
  - https://github.com/kevthehermit/YaraRules
  - Yara Exchange
  - In-House Rules

- Yara results used as “authoritative” for purposes of selecting the decoder.

# Malware Sources

- VirusTotal
- MSFT VIA Program
- Others I haven’t had chance to see if they want recognition
- RAT Traps
- In total, upwards of .25 TB a day (not all RATs)
- If you have malware you want to “trade”, let’s talk

# 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: 1111111111111111
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

# Processing DNS/IP Info

- Config takes FQDN or IP in free-form field.
- The only configuration item any processing is done on is here.
- If RFC 1918 IP, then drop config.
- If FQDN resolves to RFC1918 IP, keep it.
- If it doesn’t resolve, keep it.

# 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,,,,4A2xbJmSqvuc,DC_MUTEX-F54S21D

07ac914bdb5b4cda59715df8421ec1adfaa79cc7,150213,Dark Comet Config,Guest16,alkozor.ddns.net,31.132.106.94,1604,1.ekspert60.z8.ru,######60,######2012,zwd8tECOFOtA,DC_MUTEX-W3VUKQN

NOTE - Redacted entries are username and password for FTP drop

# What if C2 changes?

- Flexibility of DNS is underlying IP can be changed at any time.
- Many C2 hostnames will not resolve or resolve to private IPs unless actively in use.
- Persistent surveillance needed to capture the IP during the small windows it resolves.
- Need to capture IP changes too.

# Domain Generation Algorithms

- Usually a complex math algorithm to create pseudo-random but predictable domain names.
- Now instead of a static list, you have a dynamic list of hundreds or thousands of domains and adversary only needs to have a couple registered at a time.
- Can search for “friendly” registrars to avoid suspension.

# Reverse Engineering DGAs

- Many blog posts about reversing specific DGAs, Johannes Bader has the most online at his blog:
  - Johannesbader.ch

- No real shortcuts except working through IDA/Debugger and reversing the function.
  - Look for functions that iterate many times.
  - There will be at least a function to generate the domains and a function to connect to all of them to find the C2.
  - As with all reverse engineering, be aware of obfuscation and decoy code meant to deceive you.

# Types of DGAs

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

# Other DGA Hardening Techniques

- Choice of gTLD matters.
  - Some doing have WHOIS protection, make it hard to sinkhole
- Rotation of seeds
- Some malware has rudimentary “sinkhole awareness”
- Adversarial objectives: Maintain control, limit surveillance

# Examples of select DGAs - Tinba

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

# Examples of select DGAs - Bedep

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

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

# Examples of Select DGAs – Matsnu and Rovnix

- Matsnu and Rovnix both use wordlists to generate domains that appear like they would be “reasonable”. Rovnix uses the US Declaration of Independence.
- Problem is that sometimes there is collisions with real domains.

teamroomthing.com,Domain used by matsnu DGA for 16 Aug 2015,2015-08-16
transitionoccur.com,Domain used by matsnu DGA for 16 Aug 2015,2015-08-16
windbearboxreceive.com,Domain used by matsnu DGA for 16 Aug 2015,2015-08-16
winner-care-sir.com,Domain used by matsnu DGA for 16 Aug 2015,2015-08-16

theirtheandaloneinto.com, Domain used by Rovnix DGA
thathistoryformertrial.com, Domain used by Rovnix DGA
tothelayingthatarefor.com, Domain used by Rovnix DGA
definebritainhasforhe.com, Domain used by Rovnix DGA
tosecureonweestablishment.com, Domain used by Rovnix DGA

# What the use of DGAs gives the good guys

- Easy ability to sinkhole unused DGA domains to gather additional intelligence.
- Easier ability to do bulk takedowns.
  - *IF* you can predict domains in advance.
- The ability to surveil malicious infrastructure in near real-time.

# What the use of DGAs gives the good guys

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

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

# Sinkholing

- Many security companies do this.
- Many want to hide the fact they do this.
- Most adversaries aren’t stupid enough to not notice.
- Remember, Cryptolocker we had 125 or so sinkholed domain for every 1 malicious domain.

# Feed generation on DGAs

sjuemopwhollev.co.uk,Domain used by Cryptolocker - Flashback DGA for 13 Aug 2015,2015-08-13
meeeqyblgbussq.info,Domain used by Cryptolocker - Flashback DGA for 13 Aug 2015,2015-08-13
ntjqyqhqwcwost.com,Domain used by Cryptolocker - Flashback DGA for 13 Aug 2015,2015-08-13,
nvtvqpjmstuvju.net,Domain used by Cryptolocker - Flashback DGA for 13 Aug 2015,2015-08-13
olyiyhprjuwrsl.biz,Domain used by Cryptolocker - Flashback DGA for 13 Aug 2015,2015-08-13
sillomslltbgyu.ru,Domain used by Cryptolocker - Flashback DGA for 13 Aug 2015,2015-08-13
gmqjihgsfulcau.org,Domain used by Cryptolocker - Flashback DGA for 13 Aug 2015,2015-08-13,

From here you could easily feed this into RPZ or other technology to protect your organization. But we want more.

# How to set up surveillance on a DGA

- Easy to set up with shell scripting and a non-t1.micro AWS instance.
- Requires GNU parallel and adns-tools to handle bulk DNS queries.

# DGA surveillance

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

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

# Tinba Indicator list

quedxvopwvgx.com,151.248.123.41,ns-canada.topdns.com|ns-uk.topdns.com|ns-usa.topdns.com,46.166.189.99|77.247.183.137|85.159.232.241|108.61.12.163|108.61.150.91|109.201.142.225,Master Indicator Feed for tinba non-sinkholed domains
qyyudyfgxqff.com,151.248.123.41,ns-canada.topdns.com|ns-uk.topdns.com|ns-usa.topdns.com,46.166.189.99|77.247.183.137|85.159.232.241|108.61.12.163|108.61.150.91|109.201.142.225,Master Indicator Feed for tinba non-sinkholed domains
rxpgvvlpembu.com,95.163.121.201,ns-canada.topdns.com|ns-uk.topdns.com|ns-usa.topdns.com,46.166.189.99|77.247.183.137|85.159.232.241|108.61.12.163|108.61.150.91|109.201.142.225,Master Indicator Feed for tinba non-sinkholed domains
skrbogdenhub.com,151.248.123.41,ns-canada.topdns.com|ns-uk.topdns.com|ns-usa.topdns.com,46.166.189.99|77.247.183.137|85.159.232.241|108.61.12.163|108.61.150.91|109.201.142.225,Master Indicator Feed for tinba non-sinkholed domains

Seems like a good list to firewall…More on that in a moment.

# DGA Surveillance

- Looking at those four data points you now have solid information to make decisions based on the data.
- You could block domains/IPs.
- You could block nameservers (some times).

# Adversarial Response

- Adversaries know we are doing this.

- In response:
  - They change seeds frequently
  - They have non-DGA communication mechanisms
  - They engage in counterintelligence

# Counterintelligence

- The tactics by which an adversary thwarts attempts to gather information on itself.
- Remember the domain and IP lists before?
- What if an adversary registers domains that they aren’t using?

# Counterintelligence – or worse version

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

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

# Whois Registrar Intel

- Often actors may re-use registrant information across different campaigns.  There may be other indicators too.
- Sometimes **even with WHOIS privacy protection** it may be possible to correlate domains and by extension the actor.
- Most criminal prosecution in cybercrime is due to an OPSEC fail and the ability to map backwards in time of what the actor did to find that fail that exposes them.

# Whois Info

- Many actors will use WHOIS protection… some just use fake information.
- “David Bowers” is common for Bedep.

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

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

# David Bowers

**bfzflqejohxmq.com**,Domain used by bedep (-4 days to today),2015-08-16
**eulletnyrxagvokz.com**,Domain used by bedep (-4 days to today),2015-08-16
**natrhkylqoxjtqt45.com**,Domain used by bedep (-4 days to today),2015-08-16
**nrqagzfcsnneozu.com**,Domain used by bedep (-4 days to today),2015-08-16

But why stop with just known DGAs, what other domains are associated with “David Bowers”?

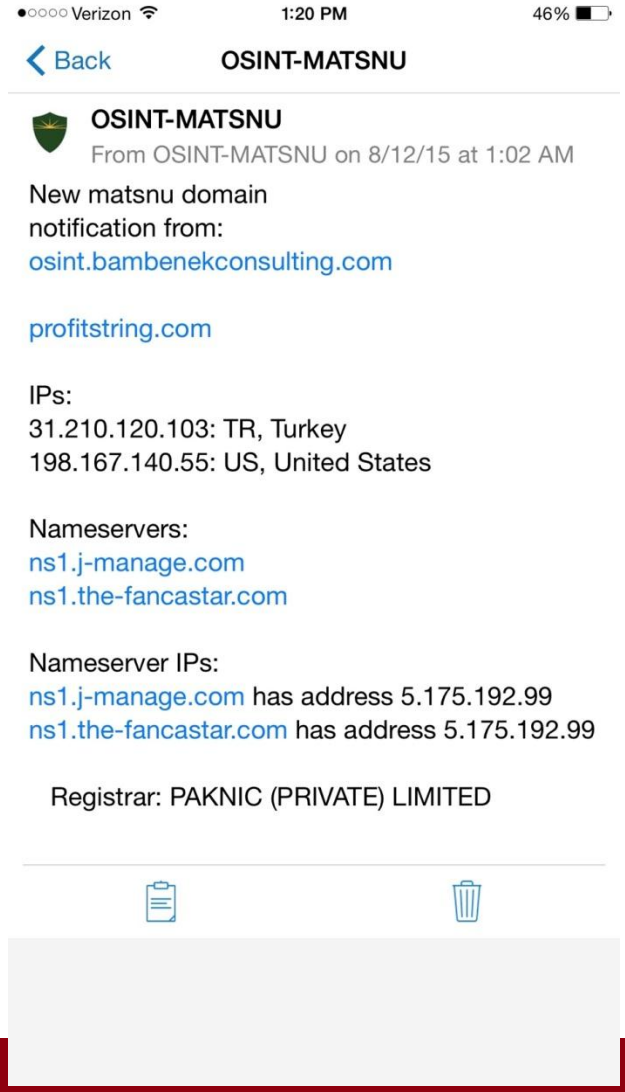
# David Bowers

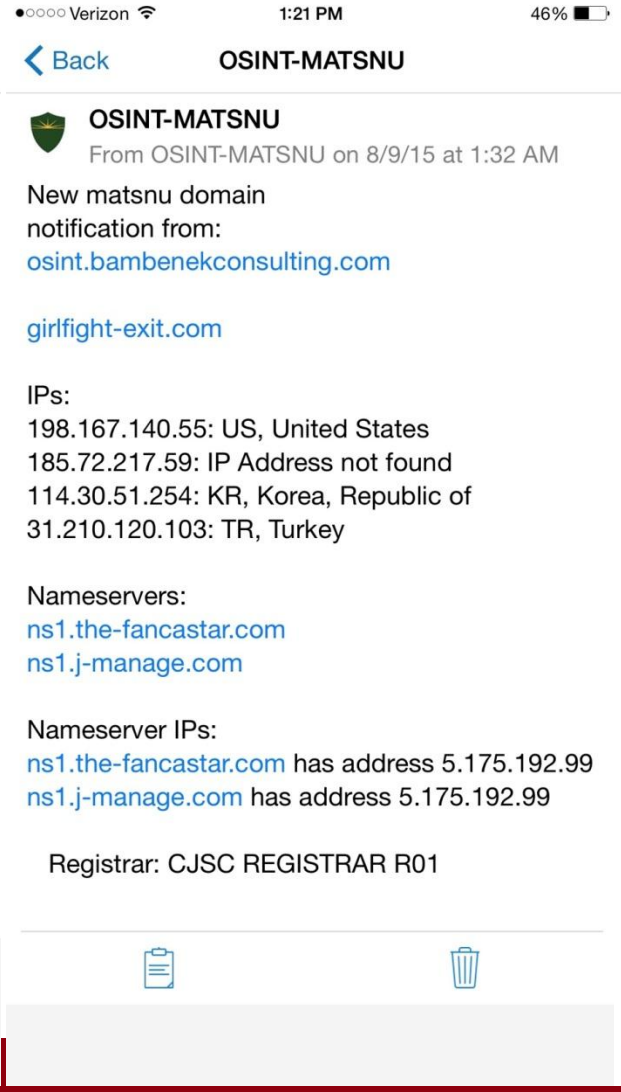
| | | |
|---|---|---|
| 029uhbsdfisjdj4.in | 2015-02-25 | -- |
| 298dkoaldjfiow-yets.in | 2015-03-18 | -- |
| 37aodjdopeoi.in | 2015-03-17 | -- |
| 37kdospwmeop.in | 2015-03-25 | -- |
| 3875jncioeprk.us | 2015-03-31 | -- |
| 394iopwekmcopw.com | 2015-01-19 | DOMAINCONTEXT, INC. |
| 78i2jpaosieu.in |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

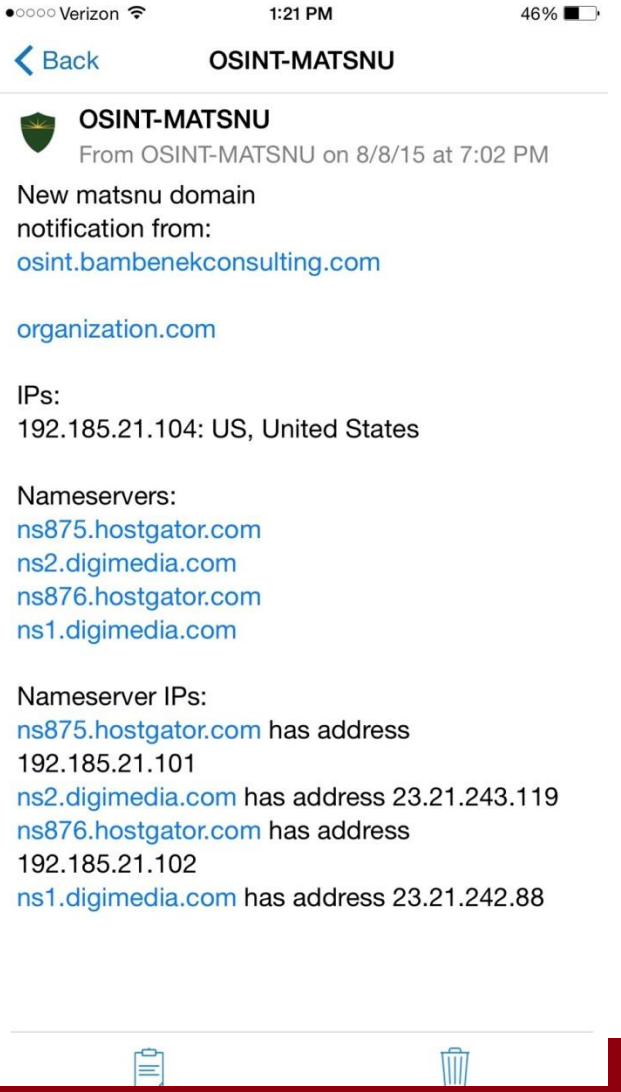
# Surveillance is nice, what about notification?

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

# New Matsnu domains registered



# Pivoting

- Now that I know the-fancastar.com and j-manage.com serve NS for Matsnu, I can see what else is served by those nameservers to find additional intelligence.
- *As of 24 Aug, this has switched to nausoccer.net and kanesth.com*
- Caution is due, this may not always yield results and may yield false positives.  Always correlate with something else before making a final judgement.

# Pivoting

Using IP from Matsnu 31.210.120.103

hostkale.com. IN A 31.210.120.103
ns1.hostkale.com. IN A 31.210.120.103
ns2.hostkale.com. IN A 31.210.120.103
linuxtr.hostkale.com. IN A 31.210.120.103
mobiluzman.com. IN A 31.210.120.103
habertemasi.com. IN A 31.210.120.103
kinghackerz.com. IN A 31.210.120.103
eglencekeyfi.com. IN A 31.210.120.103
ns1.eglencekeyfi.com. IN A 31.210.120.103
nejdetkuafor.com. IN A 31.210.120.103
profitstring.com. IN A 31.210.120.103
sirketrehber.com. IN A 31.210.120.103
actstudy-meat.com. IN A 31.210.120.103
….

# Wrapping it up

- Having all this DNS information for maliciousness is good.
- The ability to pipe it into a resolver and maintain surveillance is key to intelligence and important for defending enterprises.
- Additional benefit is the visibility in knowing when to drop indicators that are no longer valid.

# Questions?

Thanks Daniel Plohmann, April Lorenzen, Andrew Abakumov, Anubis Networks, many others.

And thanks ISC and Yiming Gong!

My feeds: osint.bambenekconsulting.com/feeds/

jcb@bambenekconsulting.com
www.bambenekconsulting.com
+1 312 425 7225


ISC
2015
中国互联网安全大会
360互联网安全中心
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
威胁情报论坛


ISC
2015
中国互联网安全大会
360互联网安全中心
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
威胁情报论坛


ISC
2015
中国互联网安全大会
360互联网安全中心
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
威胁情报论坛