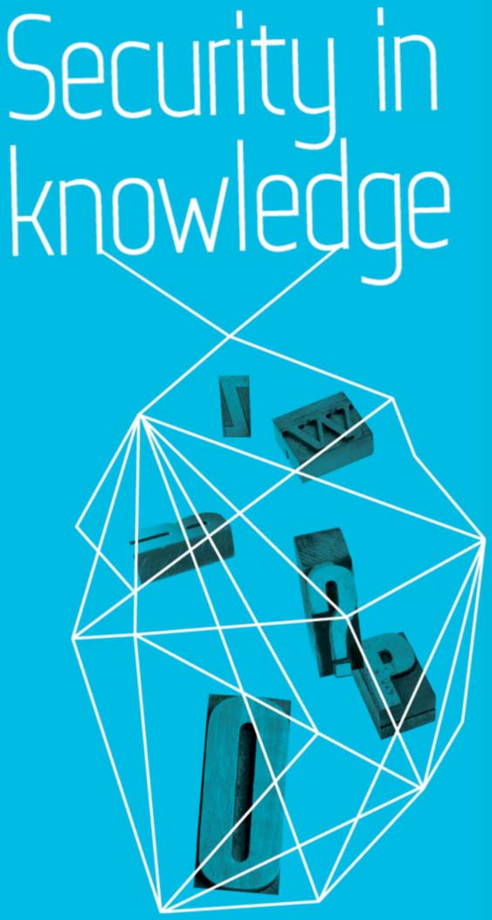
RSACONFERENCE2013



Foolish Zebras: Log-tracking Your Riskiest Users to Find the Bad Guys

Chris Larsen @bc_malware_guy
Blue Coat Systems
www.bluecoat.com/security

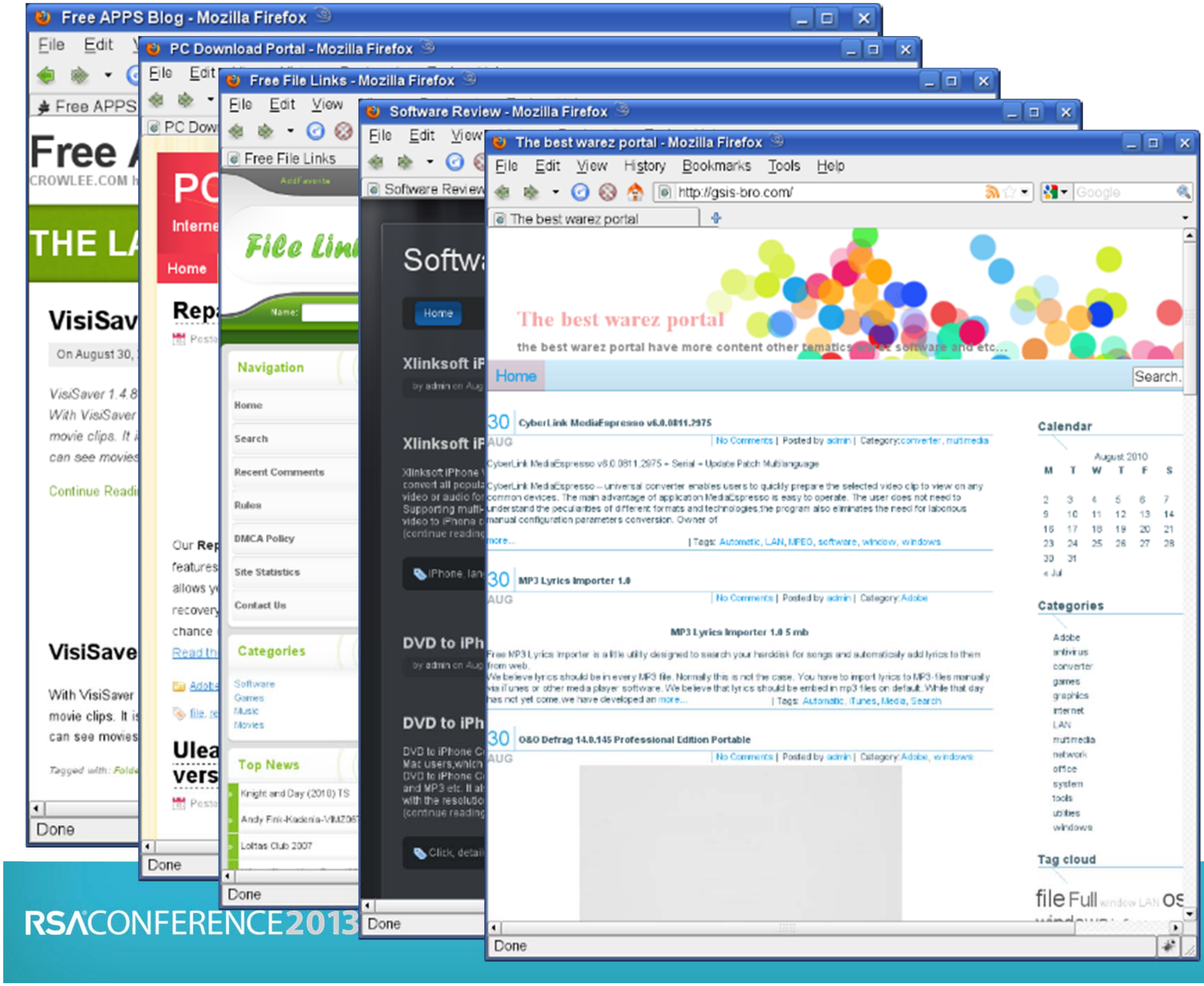
Session ID: BR-F42

Session Classification: Intermediate

Outline

- The "zebra herd" principle
- What to do with your foolish zebras?
  - Get mad at them?
  - Make fun of them?
  - Enlist them as unwitting security researchers!
- How to identify them
- How to track them
  - And what you might find…

Foolish Zebra Story


Free APPS Blog - Mozilla Firefox
PC Download Portal - Mozilla Firefox
Free File Links - Mozilla Firefox
Software Review - Mozilla Firefox
The best warez portal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://gsis-bro.com/
The best warez portal
Home
Search
Navigation
Home
Search
Recent Comments
Rules
DMCA Policy
Site Statistics
Contact Us
Categories
Top News
Calendar
Categories
Tag cloud
Done

The best warez portal

the best warez portal have more content other tematics warez software and etc...

30 AUG **CyberLink MediaEspresso v6.0.0811.2975**

| No Comments | Posted by admin | Category:converter , multimedia

CyberLink MediaEspresso v6.0.0811.2975 + Serial + Update Patch Multilanguage

CyberLink MediaEspresso – universal converter enables users to quickly prepare the selected video clip to view on any common devices. The main advantage of application MediaEspresso is easy to operate. The user does not need to understand the peculiarities of different formats and technologies,the program also eliminates the need for laborious manual configuration parameters conversion. Owner of

more... | Tags: Automatic, LAN, MPEG, software, window, windows

30 AUG **MP3 Lyrics Importer 1.0**

| No Comments | Posted by admin | Category:Adobe

MP3 Lyrics Importer 1.0 5 mb

Free MP3 Lyrics Importer is a little utility designed to search your harddisk for songs and automatically add lyrics to them from web.

We believe lyrics should be in every MP3 file. Normally this is not the case. You have to import lyrics to MP3-files manually via iTunes or other media player software. We believe that lyrics should be embed in mp3 files on default. While that day has not yet come,we have developed an more... | Tags: Automatic, iTunes, Media, Search

30 AUG **O&O Defrag 14.0.145 Professional Edition Portable**

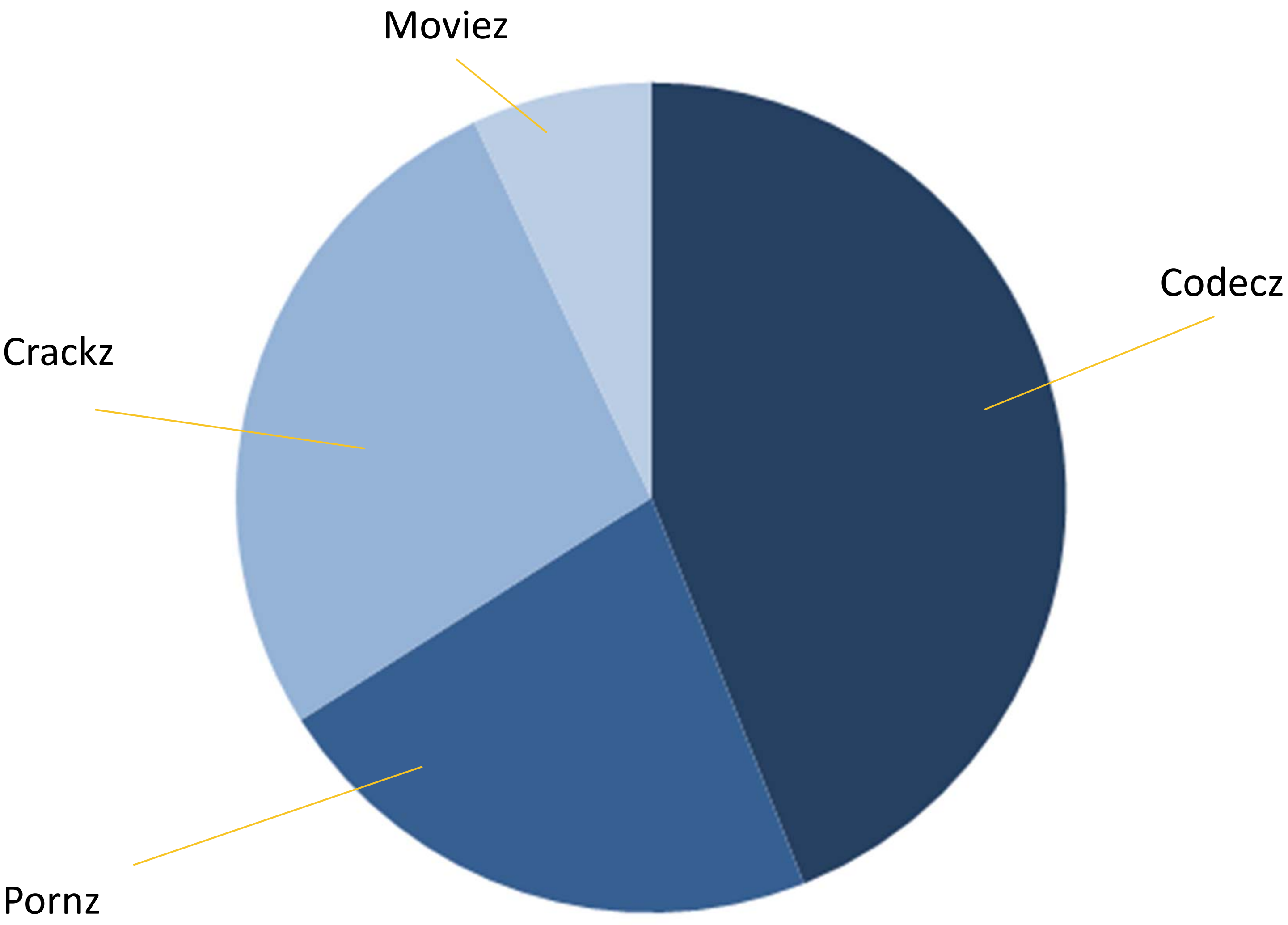
| No Comments | Posted by admin | Category:Adobe, windows

“Dangerous Warez” Network

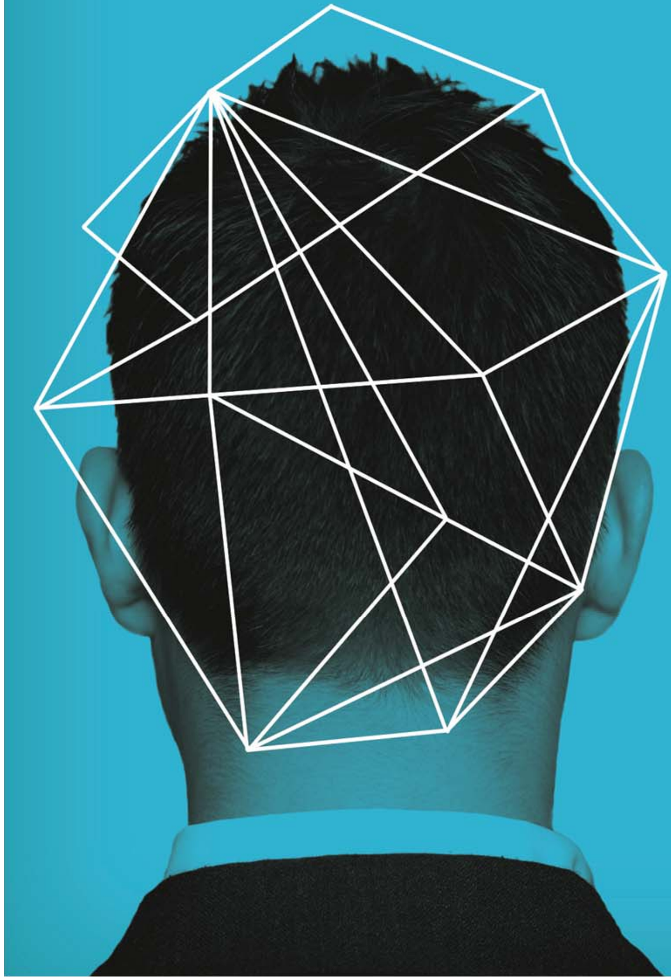
Foolish Zebra Story

- How to save a fence-busting zebra in spite of himself?
- Initial engineer reaction?
  - “We’ve got to build a better fence!”
- Wise researcher reaction?
  - “This noble zebra is sacrificing himself for the good of the herd!”
    - (Let’s radio-collar him and see where else he goes!)
    - (btw, our zebras are anonymous in the logs)

Bonus Slide, Courtesy of “Dangerous Warez” Network



Finding Your Foolish Zebras

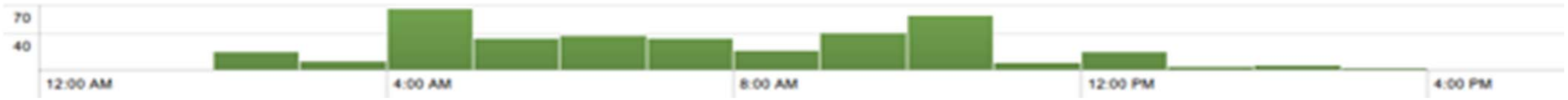


Finding Your Foolish Zebras

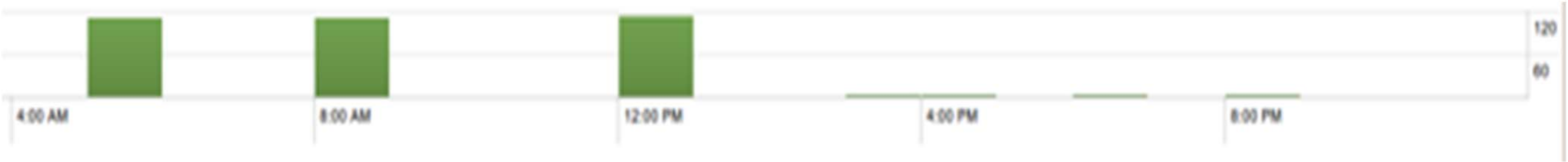
- Basic Idea #1 -- Behavior
  - Zebras with unusually high traffic
  - Zebras with unusual traffic patterns

One-slide tutorial on traffic patterns

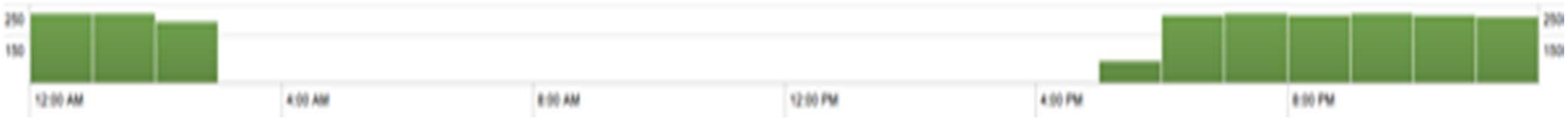
Normal:



Weird Intervals:



Steady/automated:



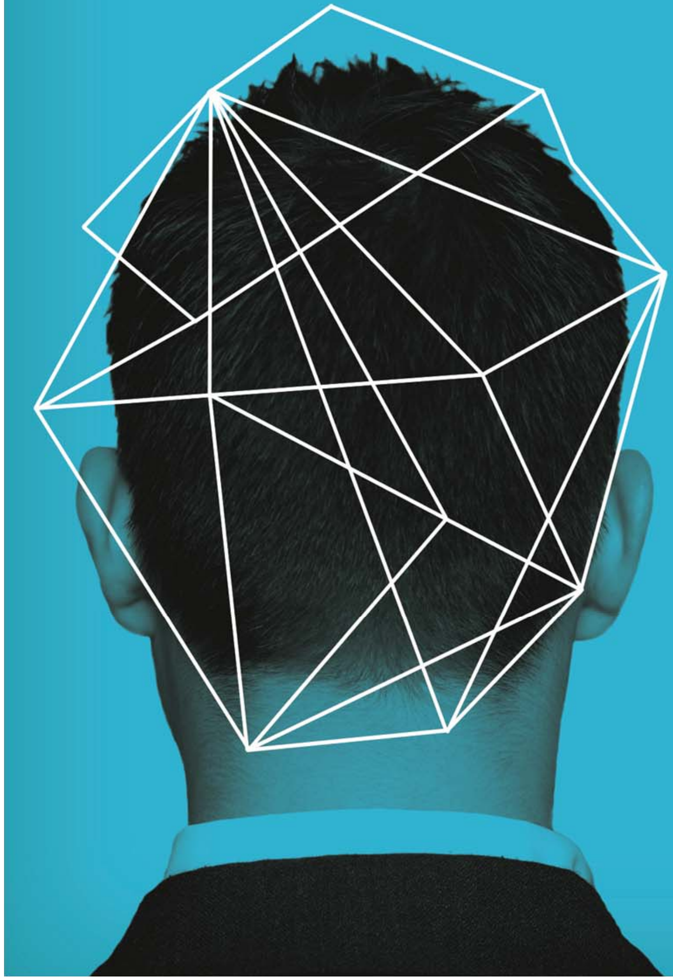
Finding Your Foolish Zebras

- Basic Idea #2 – Risky Areas
  - Identify areas of concern, and start looking there
    - (but zebras are ingenious, so don't just stick to one list!)
  - Security team brainstorming:
    - "If we were Bad Guys, where would we hide our traffic?"
  - Ask your security vendors/consultants for suggestions

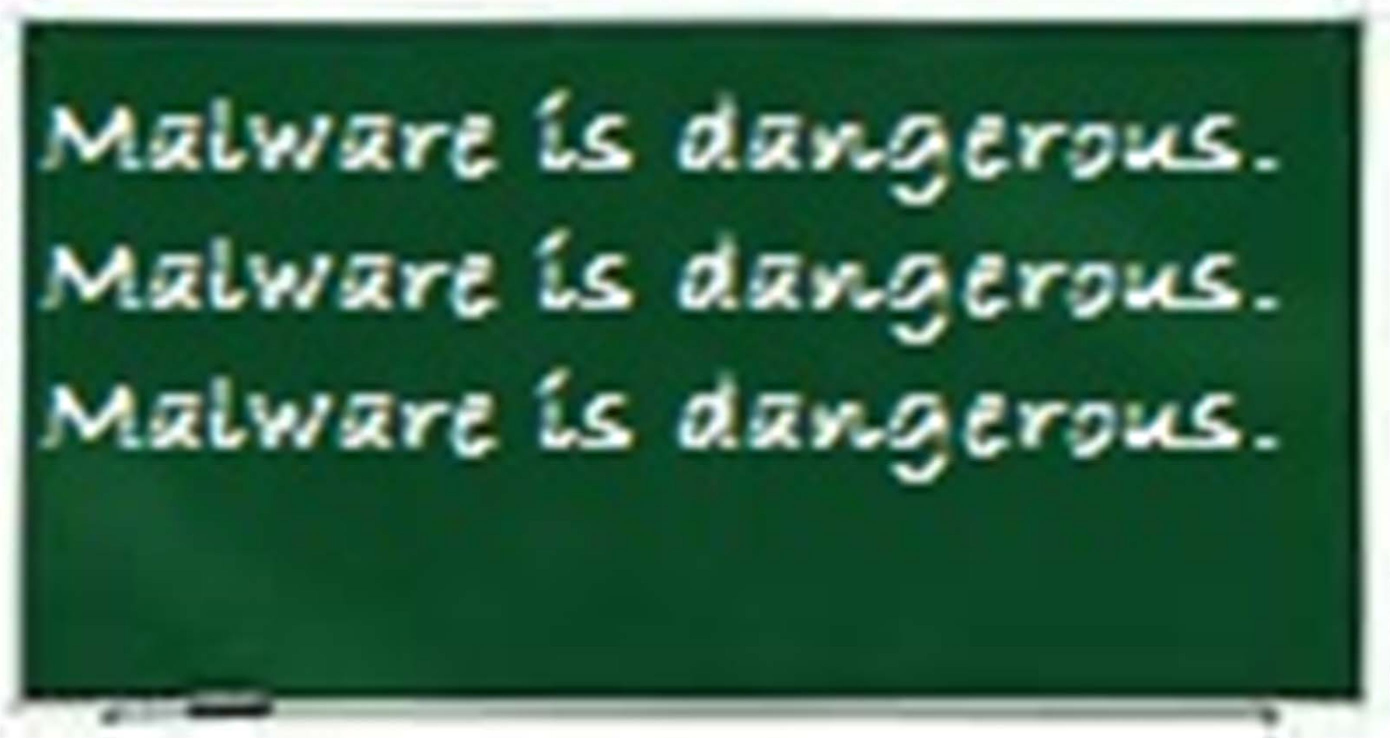
Risky Areas in Web Traffic

- We'll be looking at several areas…
- The Obvious:
  - Malware sites, Botnets, Suspicious…
- The Less-obvious:
  - Porn, Unrated, DynDNS…
- I will provide "Background Radiation" level estimates…
- …"worry level" estimates…
- …and "what you find" examples
- (you will of course need to set your own levels)

Into the bushes we go…



Category of Interest: Malware



Malware is dangerous.
Malware is dangerous.
Malware is dangerous.

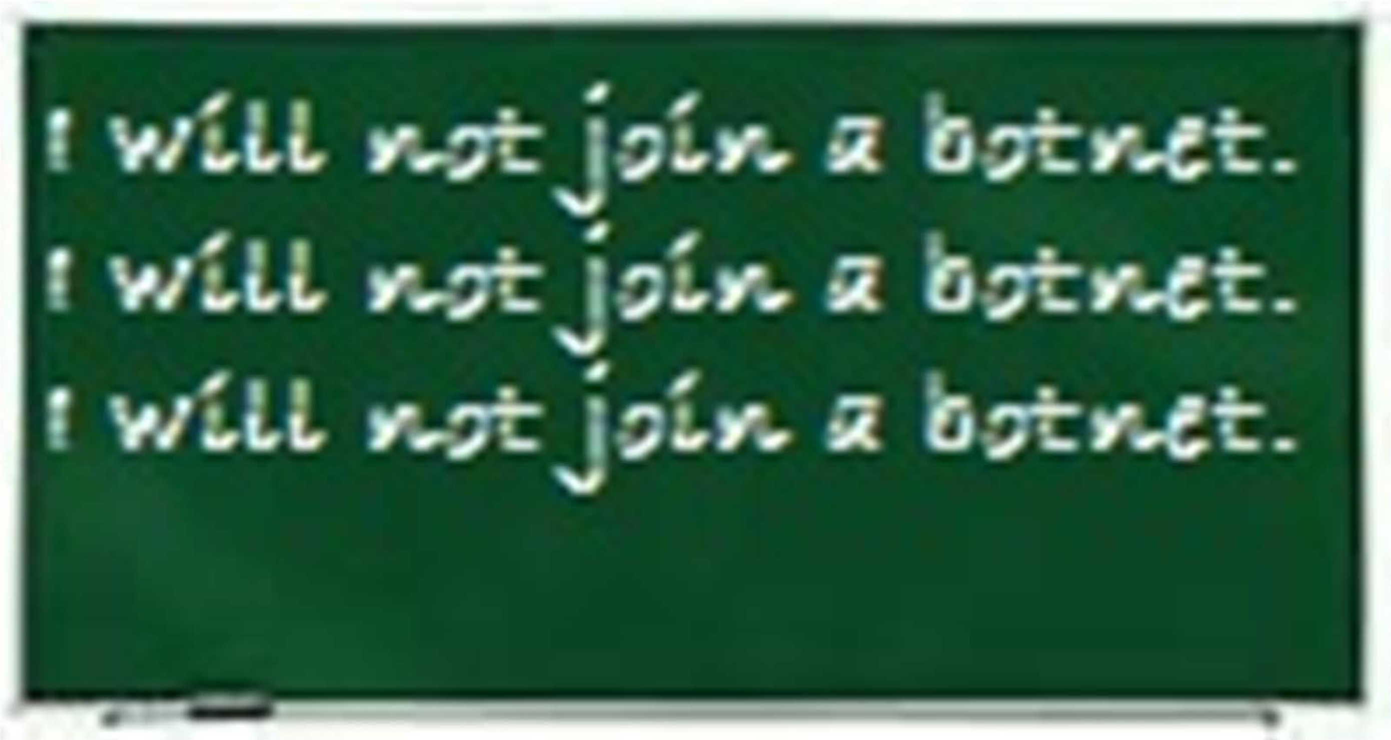
Category of Interest: Malware

- What's in it?
  - Payload hosts, Exkits, "Ecosystem" (relay) sites...
- Why is it interesting?
  - (ok, this one's obvious)
- What's the "Background Radiation" Level? (1-2)
  - Only 785 K9'ers had even 1 hit the day I checked
- What's the "Worry" level?
  - 104 had 3-5 hits; 17 had >5 hits

Zebra Tracking: Malware

- Looked at 9 users with >6 hits
- Most had all hits on 1 attempted visit to a site
  - (1 was spread across 5 visits)
- 1 "scripter" to disable
- 4 looked unscathed (they visited, we blocked)
- But 4 of the 9 looked like they'd been compromised
  - 1 was surfing porn
  - Good stuff to investigate in their other traffic
  - e.g. *suncurrentlytransitstheconstellationoflibrafromoctober.info*
    - Great example of cluster hard to find in whole haystack

Category of Interest: Botnets


I will not join a botnet.
I will not join a botnet.
I will not join a botnet.

Category of Interest: Botnet

- What's in it?
  - Botnet C&Cs, other "Malicious Outbound Traffic"...
- Why is it interesting?
  - Presumably, the best indicator of infection...
- What's the "Background Radiation" Level?
  - 1-2 hits/day for a single surfer
- What's the "Worry" level?
  - 3 and up
  - (and bigger "spikes": 25-230 hits for most foolish zebras)

Zebra Tracking: Botnet

Tip: don't drill in immediately; skim for patterns

- e.g., 10 of top 11 hitters on 12/30 had same site:
  - *ulroyjwchn.cm* (a domain du jour for TDSS botnet)
  - So it occurred a lot, all the way down the list...
- Therefore, the zebra that didn't is automatically more interesting
  - 212.117.177.20 (more shady than malicious)
- A set of junk-domain botnet traffic in the 15-60 hitters
- A set of Conficker sinkhole IPs (5-20 hitter range)
- Unique: *getwinupdates.ru* (quick check: little info, so go deeper)
  - (and then keep an eye on this workstation going forward)

Category of Interest: Suspicious

Category of Interest: Suspicious

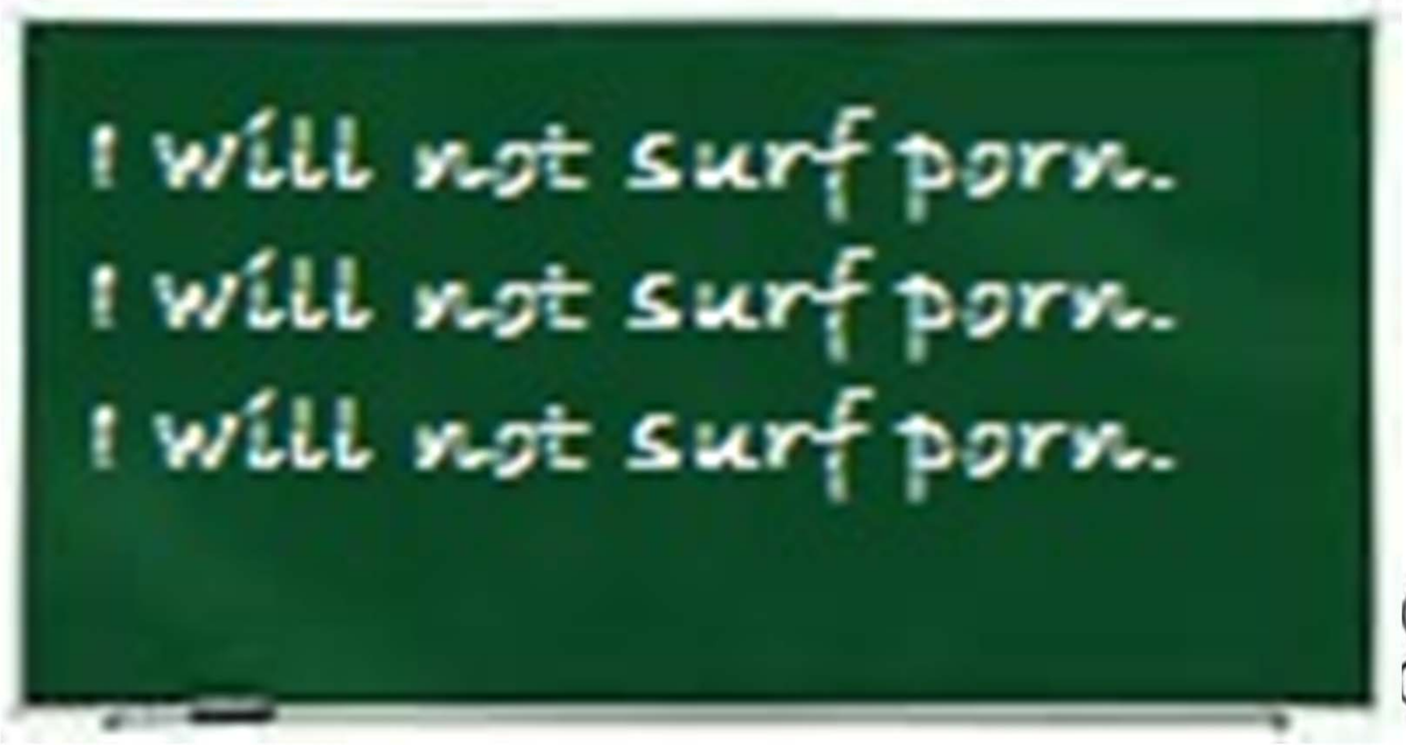
- What’s in it?
  - Sites that are “up to something”
  - Significantly elevated risk areas
  - Stuff not yet confirmed as malicious
- Why is it interesting?
  - The most interesting 1% of the “coolest 5%”
- What’s the “Background Radiation” Level? (1-4)
  - 5985 users had 1-4; 246 had 5-10
- What’s the “Worry” level?
  - 50 had more than 10 hits

Zebra Tracking: Suspicious

- I looked at 10 users with 30+ hits
  - 30 hitter, all to one domain:
    - *www. kindergarten.com.php53-28.dfw1-2.websitetestlink.com*
    - (that many dots is usually a phish; this isn't)
  - 37 hitter, all to one domain:
    - *xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.com*
  - 65 hitter, to an apparently parked domain with weird name (*)
  - 375 hitter: mix of legit, maybe legit, and shady .RU sites
  - 391 hitter: random-ish/botnet-ish domains, never resolving (*)
  - 663 hitter: short-but-ugly domain names, never resolving (*)
- * no "Botnet" traffic, but these are still bots!

(Further) into the bushes we go…

Category of Interest: Porn



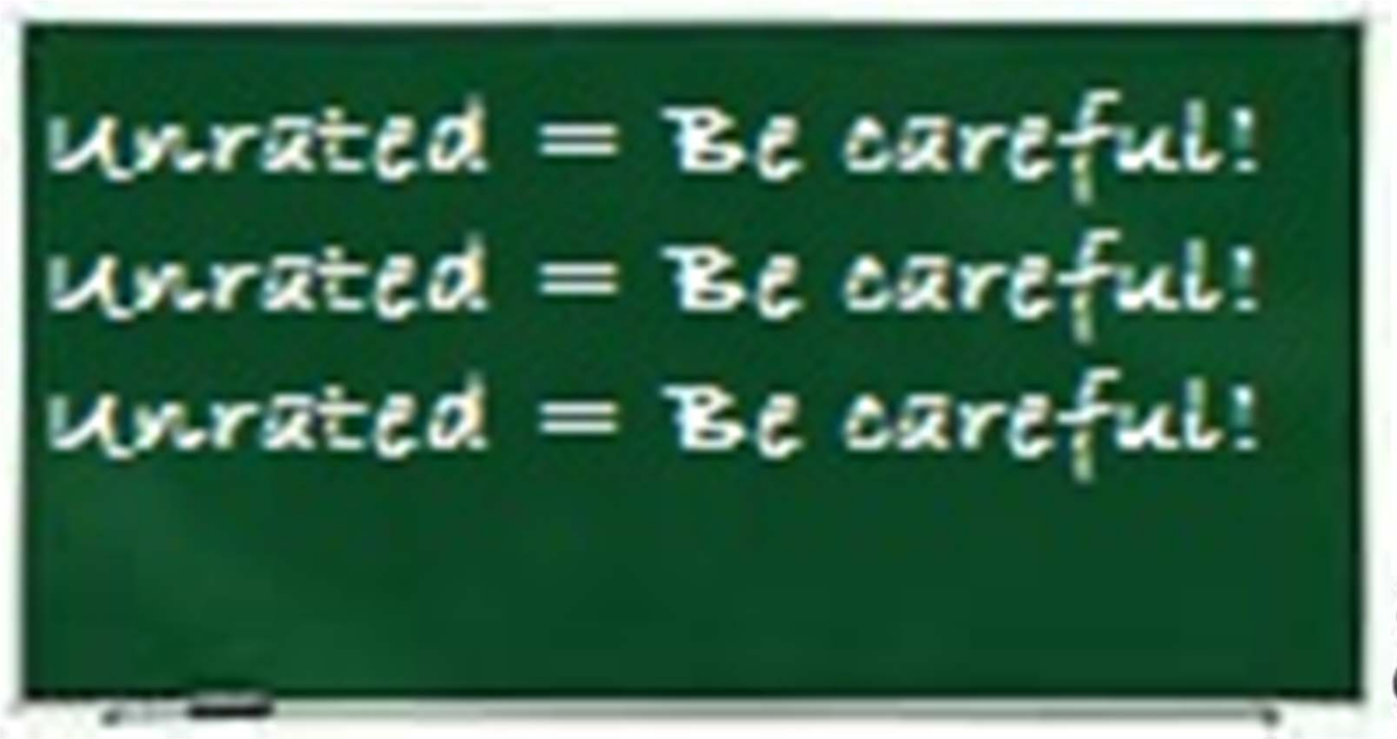
Category of Interest: Porn

- What's in it?
  - The stuff beyond merely "adult"
- Why is it interesting?
  - Well-established lure for spam & malware
- What's the "Background Radiation" Level? (1-3)
  - 83% of K9ers had <4 hits the day I checked
- What's the "Worry" level?
  - Someone above that (4+) is looking for it

Zebra Tracking: Porn

- Most high-count users were trying to find gaps
  - (and ended up showing me where the fence needed repair…)
- One, however, led to something more interesting:
  - 2 huge "shady-search" networks
  - Looked like paid-affiliate type traffic
  - Averaged >5K hits a day, across >50 domains
  - Traffic coming in faster than humans click
    - Definitely shady traffic herding...
- Again, easier to see when tracking one zebra

Category of Interest: Unrated



Unrated = Be careful!

Unrated = Be careful!

Unrated = Be careful!

Category of Interest: Unrated

- What's in it?
  - New and/or small sites we haven't gotten to yet
- Why is it interesting?
  - (Me: "The coolest 5% of the Web!")
- What's the "Background Radiation" Level? (1-5)
  - 150K+ users had at least one; 127,734 of them had 1-5
- What's the "Worry" level? (~ 100-200)
  - 570 users had 100+, 196 users had 200+, 10 had 300+

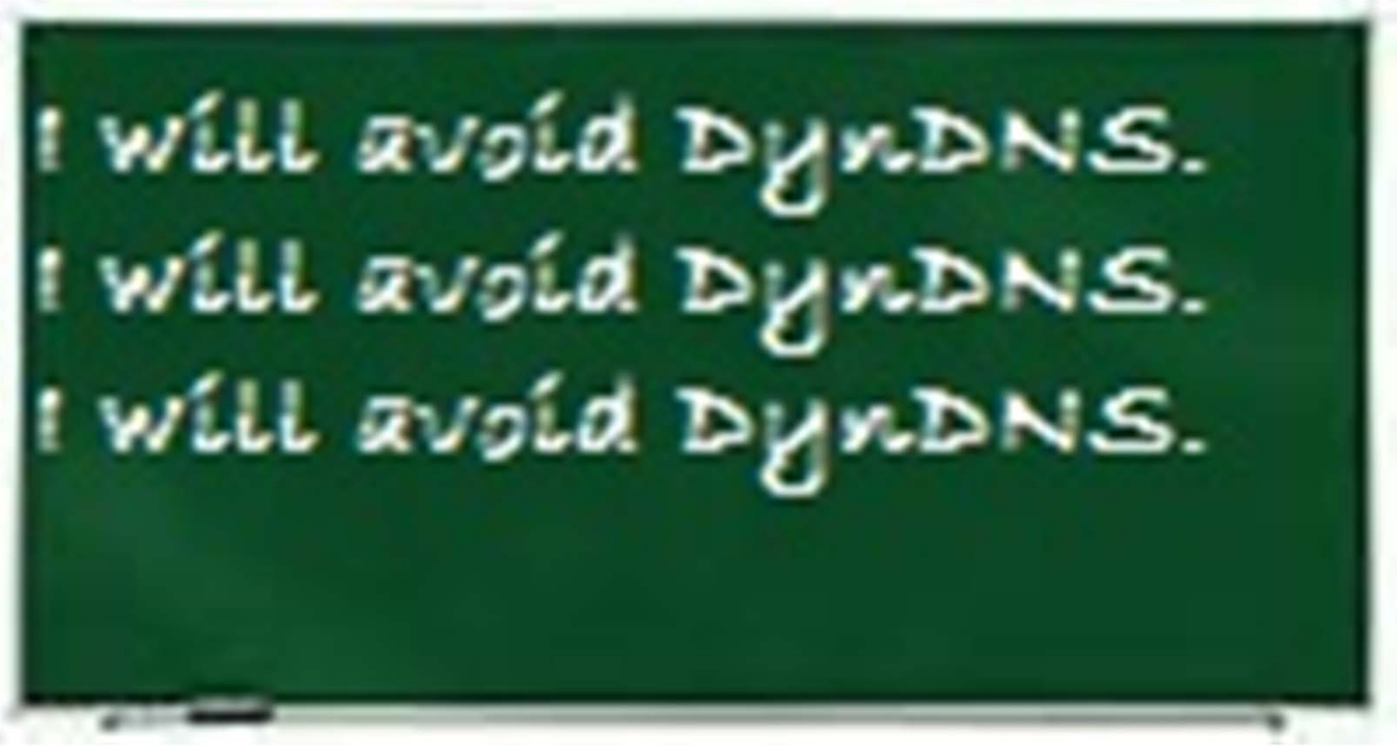
Zebra Tracking: Unrated

- 166 hitter:
  - 2 big ad networks (possibly shady)
  - 1 big relay/tracker network (definitely shady)
- 167 hitter:
  - Porn network (not HTML; Flash video servers)
  - And a shady traffic-driver network
- Then, big hitters: 1557, 1688, 1893, 1921, 1985…
  - 24.119.44.224:8008/machine0-1356049769225?machine=Middleton%2FLibrary%2FDesktop%2FPublicGen4-DTP+%5BWindows+7+Pro+%2C+x86%5D+DF&inuse=2&version=3.11/
  - All at "Middleton Library" running some kind of ancient tech-support package ("SimpleHelp") that kept phoning home...

Zebra Tracking: Unrated

- 201 hitter
  - (also found a lot of Botnet traffic, so worth digging deeper)
- 929 hitter (game traffic for "smeet")
- 1208 hitter (game traffic for "holo.ws")
  - (we had both parent game sites rated, but not these servers)
- 2369 hitter (*ssprovide.com*)
  - (this was only user to hit this; definite botnet-type traffic)

Category of Interest: DynDNS



I will avoid DynDNS.
I will avoid DynDNS.
I will avoid DynDNS.

Category of Interest: DynDNS

- What's in it?
  - "Hosts" allow free subdomains to point anywhere
- Why is it interesting?
  - Even easier to set up than a free host
    - (and you control your server; free hosts may scan for malware, etc.)
  - These have been used in a ***lot*** of APT attacks
- What's the "Background Radiation" Level? (1-3ish)
  - 8804 K9'ers had at least one hit, 1110 had >= 4 hits
- What's the "Worry" level?
  - Probably 3-4 and up
    - (but sometimes much higher is normal)

Zebra Tracking: DynDNS

- General Observations:
  - If you have foolish Russian zebras, I pity you...
    - (ucoz.net family: borderline DynDNS, used like CDNs for free sites)
    - Some zebras have >100 hits on these
    - Most surfing movies, games, and porn
    - Lot of Suspicious and shady-looking sites
  - Also, lots of traffic to *checkip.dyndns.org* (need to filter these)
  - Overall, about 10% of high-hitters had "interesting" traffic
    - (after filtering *ucoz* and *checkip*, it's much better)

Zebra Tracking: DynDNS

- Interesting finds:
  - One zebra: *drirgbqjrgdg.rr.nu, hwpdgbqjrgdg.athissite.com,* etc.
    - (tons of Mac Flashback traffic)
  - Another zebra: lots to *olvvkos.no-ip.info*
    - (looks like spam or traffic-driver network, but if he's the only one…)
    - And, no "Botnet" traffic, so this was the only infection indicator
  - Another zebra: mixed in with the *ucoz* stuff…
    - …was *reffer.chickenkiller.com* (another "standout")
      - *(chickenkiller.com* has been around for years)
    - Quickly found 4 IP's: shady *.info* sites
      - 140+ sites in a week; ~ 6000 hits
      - Some ties to existing malware networks

Zebra Tracking: DynDNS

- More Interesting Finds:
  - *www1 .j3z84ydz34n39.zyns.com* (another “standout” from ucoz)
    - Led to shady porn network
  - *adnanrao.zapto.org* (another oddball)
    - Hiding behind “under construction” page; log shows odd-port traffic
    - Found phishing pages (Western Union, some Forex site)
    - Pakistan IP; nothing else shady in user's traffic
    - But these appeared in stretches of “heartbeat” traffic
      - (so wasn’t part of normal surfing)
    - And, we show 13 K9 users with that traffic
      - (so it looks like they’re infected with something...)

Zebra Tracking: DynDNS

- Still More Interesting Finds:
  - Mixed in with ucoz stuff:
    - *downplay769.dyndns-office.com, fruitarian752.dyndns-free.com*…
    - Led to big tracker/relay network
    - Multiple IP's and DynDNS hosts
  - Again, mixed in with ucoz stuff: *74kfnudh35.dyndns.info*…
    - Lots of sites on that server; looks like a traffic-driver network
  - Interesting: a Spanish user, with very clean traffic…
    - …Facebook, Youtube, Skype, AV updates, K9 checks…
    - …no mystery IPs, no shady trackers, no Suspicious or Unrated!
    - But, two weirdos: *mitoslinares.no-ip.org, blondres.dyndns.org*
    - Not obviously evil, but only this license saw them
    - (and during e-mail use) so keep an eye on that computer!

Other Categories of Interest

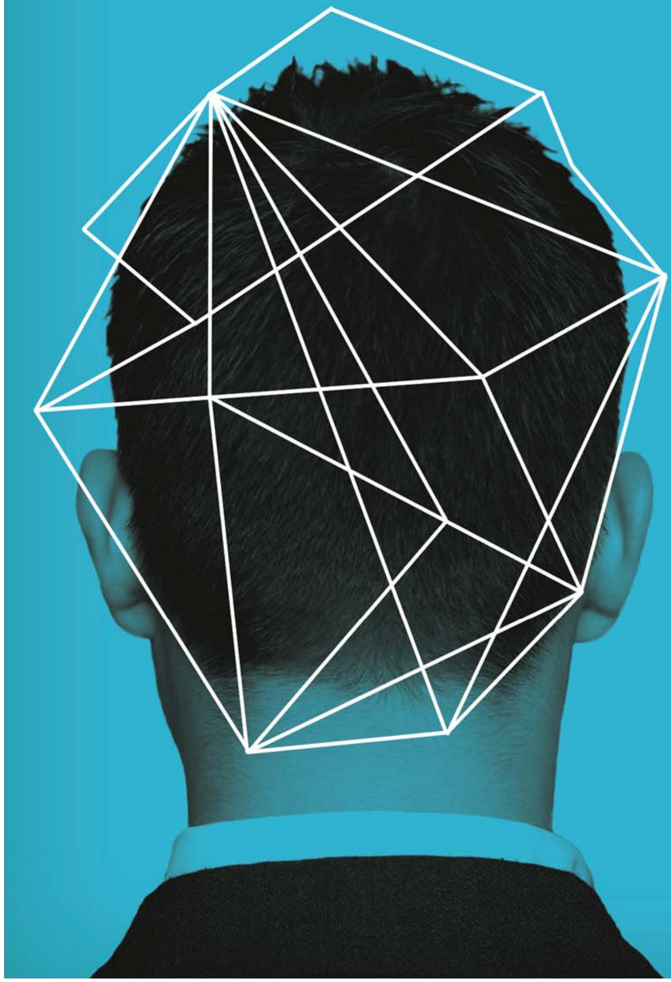
- Spam
- Placeholders
- Adult
- Hacking (Warez)
- Gambling
- Open/Mixed Content
- Online Storage
- … //watch the blog this year for more data!

So go home and get to work!

Action Slide

- Summary of general principles:
    - Identify your foolish zebras to reduce the "haystack size"
        - By areas of concern (e.g., Web site categories)
            - Ask yourself where Bad Guys might hide stuff; look there
        - By behavior (look for outliers)
        - Ask your security vendors and consultants for ideas!
    - Then, do quick initial survey of the mini-haystack
        - What is "normal abnormal"? (e.g., phone-home sites du jour)
            - (spend some time here)
        - What is "abnormal abnormal"? (i.e., different from the du jour stuff)
            - (spend more time here; potential advanced attacks)
- Radio-collar your foolish zebras (check them regularly!)

?



Questions

Chris.Larsen
bluecoat.com/security
@bc_malware_guy