Building Better Castles

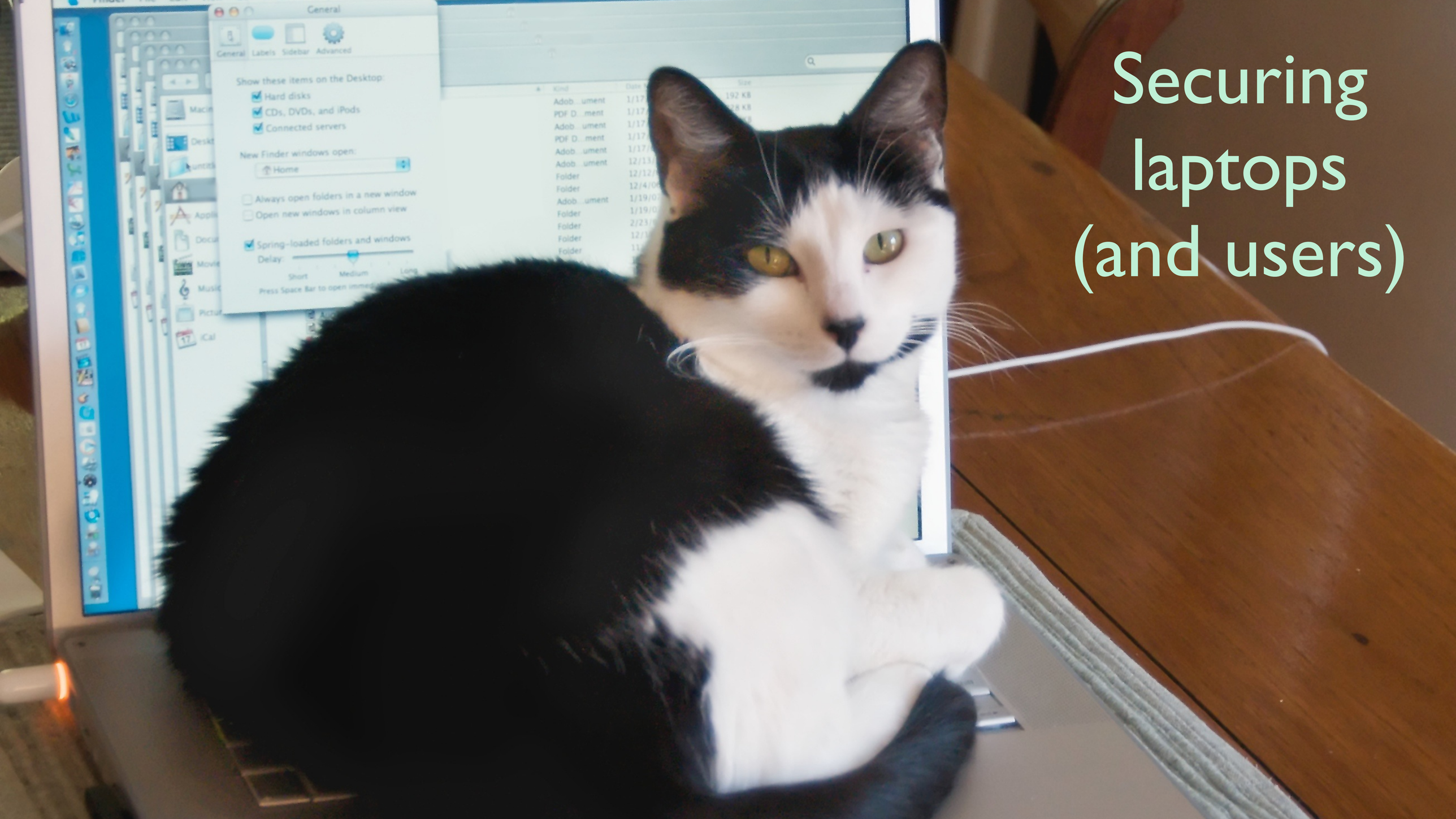
Ben Hughes
Etsy
@benjammingh

Building better sand castles

- I work at Etsy, yes that Etsy.
- Yes we have a seemingly large security team.
- We do “some” webops, arguably devops some days too.
- My German is terrible.
- No one cares about this slide.

Building better sand castles

- Intro (we're here)
- Users/laptops/the two people with "workstations".
- Servers/systems.
- Data - that small topic.
- Conclusions


General
Labels
Sidebar
Advanced
Show these items on the Desktop:
Hard disks
CDs, DVDs, and iPods
Connected servers
New Finder windows open:
Home
Always open folders in a new window
Open new windows in column view
Spring-loaded folders and windows
Delay:
Short
Medium
Long
Securing
laptops
(and users)

The landscape has changed.

https://www.flickr.com/photos/andraspasztor

The landscape has changed.

https://www.flickr.com/photos/andraspasztor

chrome

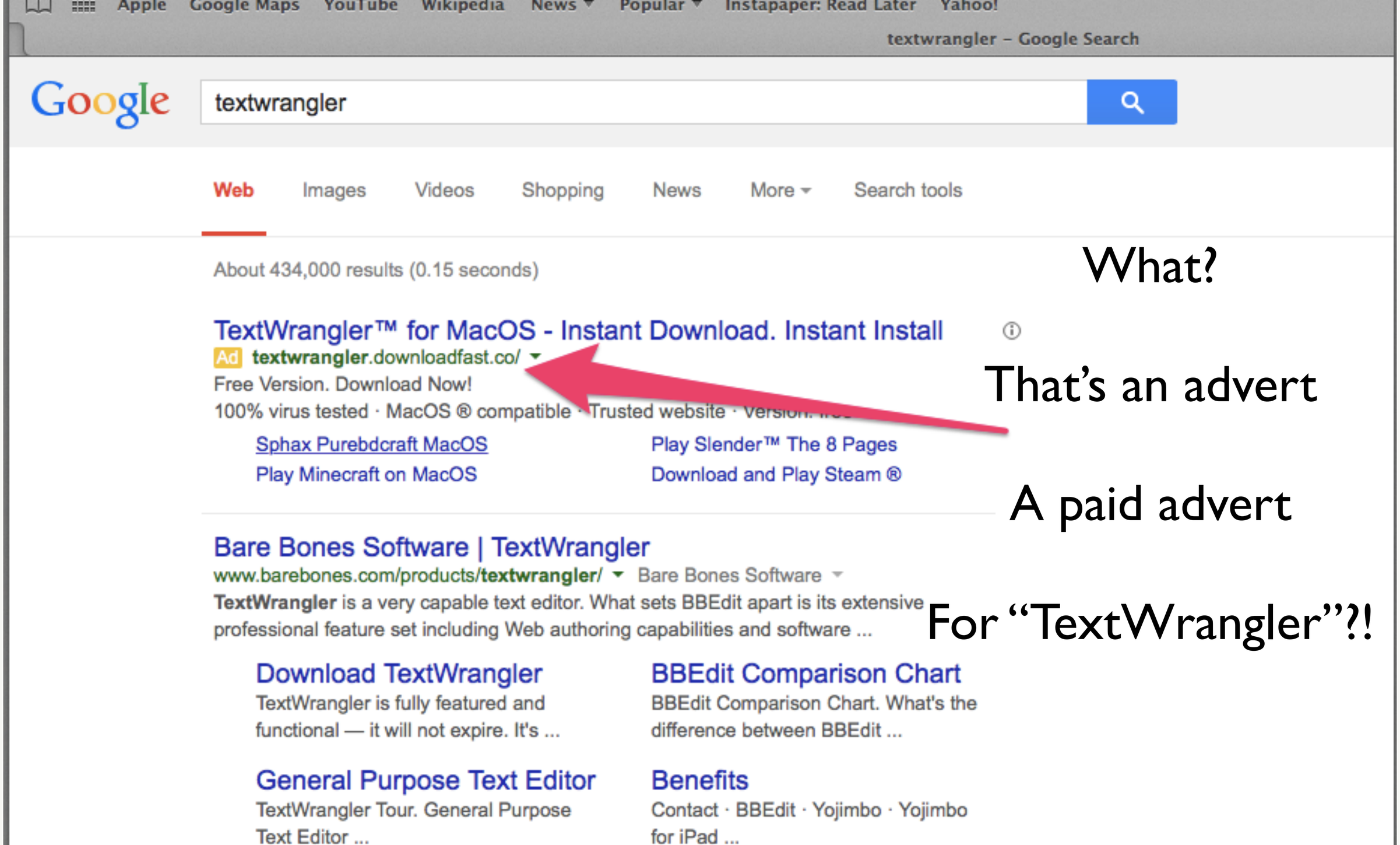
Danger: Malware Ahead!

Google Chrome has blocked access to this page on hbdpomandigafcibbmofojjchbcdagbl.

Content from twitpic.com, a known malware distributor, has been inserted into this web page. Visiting this page now is very likely to infect your computer with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more

Go back Advanced



What?

That's an advert

A paid advert

For "TextWrangler"?!


Sink holes!

```
[ben@laptop:default][1]% grep -A 6 downloadfast.co named.sinkhole
zone "downloadfast.co" IN {
  type master;
  file "/etc/named.sinkhole.zone";
  allow-update {
    none;
  };
};
[ben@laptop:default][1]% cat named.sinkhole.zonefile
@       IN      SOA     localhost       root ( 2 3H 15M 1W 1D )

        24H IN NS               @

        24H IN AAAA             ::1
*       24H IN AAAA             ::1
@       24H IN AAAA             ::1

        24H IN A                127.0.0.1
*       24H IN A                127.0.0.1
@       24H IN A                127.0.0.1
```

IPv6

(it's big outside of America)

Building better sand castles

- http://labs.neohapsis.com/2013/07/30/picking-up-the-slaac-with-sudden-six/
- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-15-2mt-book/ip6-ra-guard.html
- http://resources.infosecinstitute.com/slaac-attack/
- https://github.com/Neohapsis/suddensix

Building better sand castles

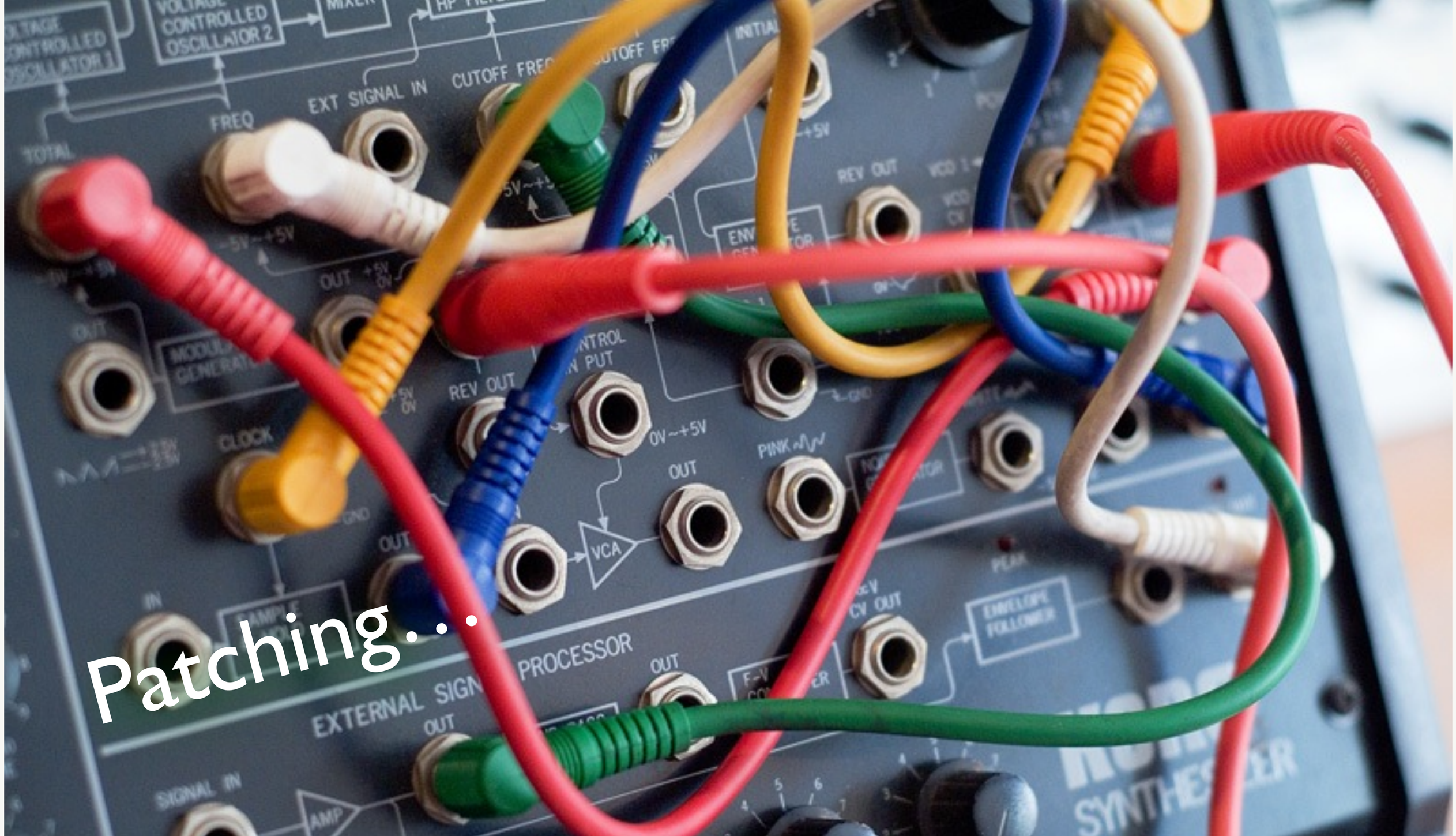
Oprah says “And you get an IDS….”

- On most desktop OSes (Linux/OSX/Windows… I have no idea about Windows) you can use the firewall like an IDS.
- PF example:

```
pass log quick proto { tcp, udp } to any port { 6881, 31337, $badport }
```

Servers!

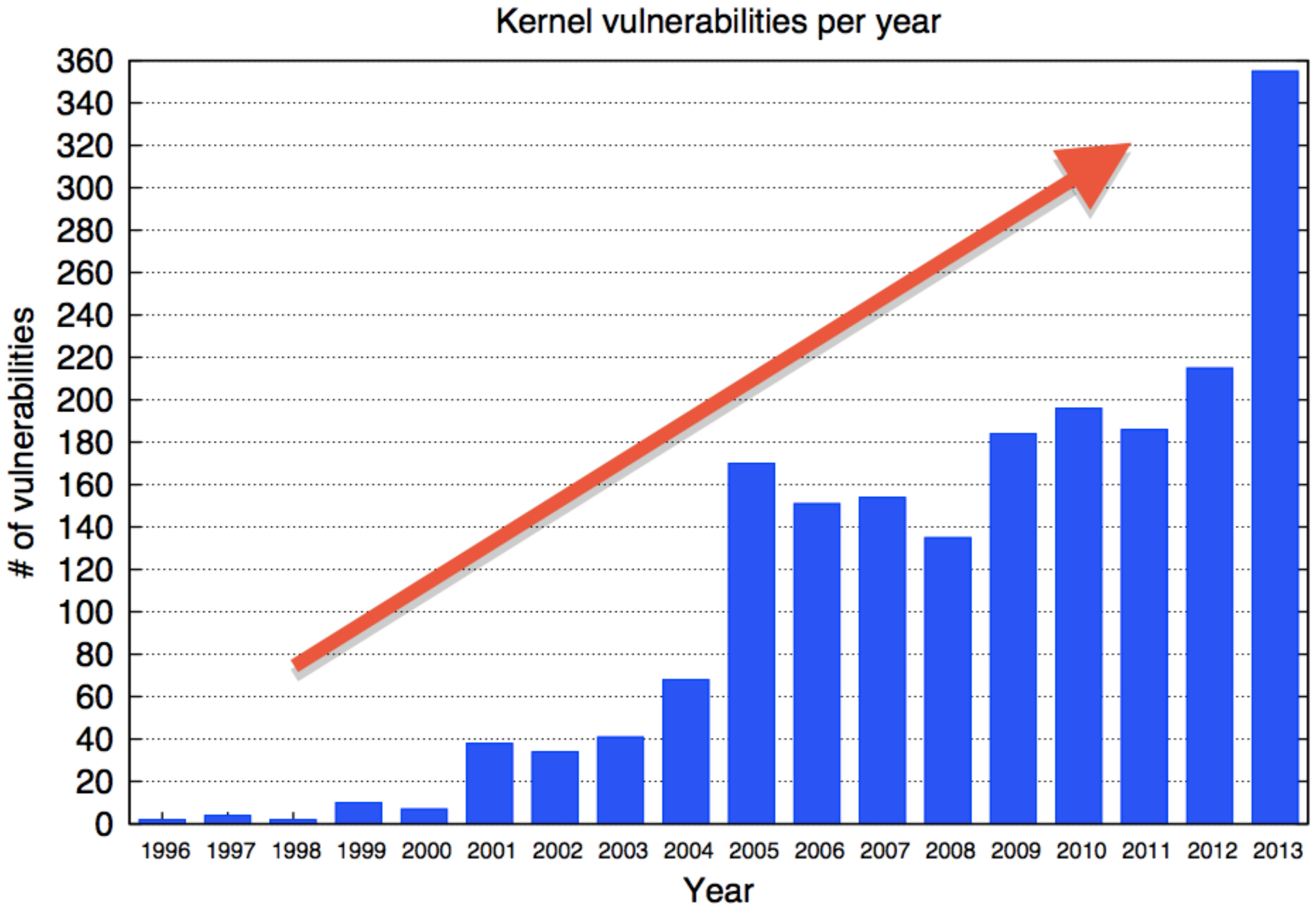
https://www.flickr.com/photos/stalker_cz/


Patching…

TimDenike
@TimDenike

(MUD:timmy@dbticket1:~)$ uptime
18:53:09 up 2129 days, 16:32, 3 users,
load average: 0.33, 0.28, 0.21
10:53

https://twitter.com/TimDenike/status/162973991034826752



Source: National Vulnerability Database (http://nvd.nist.gov)

https://www.blackhat.com/docs/eu-14/materials/eu-14-Kemerlis-Ret2dir-Deconstructing-Kernel-Isolation.pdf

“Zero-Day” Attack

& timthumb.php

Building better sand castles

Uptime security solutions!

Building better sand castles

Uptime security solutions!

- SELinux - ‘setenforce 0’ as it’s also known as.
  - http://stopdisablingselinux.com/

Building better sand castles

Uptime security solutions!

- SELinux - ‘setenforce 0’ as it’s also known as.
  - http://stopdisablingselinux.com/
- grsecurity - set of hardening patches to Linux.
  - http://grsecurity.net/features.php

Building better sand castles

Uptime security solutions!

- SELinux - ‘setenforce 0’ as it’s also known as.
  - http://stopdisablingselinux.com/
- grsecurity - set of hardening patches to Linux.
  - http://grsecurity.net/features.php
- Ksplice - https://www.ksplice.com/ scariest fix ever.

Building better sand castles

Realities of the situation:

- There will always be un-patched machines.

Building better sand castles

Realities of the situation:

- There will always be un-patched machines.
- Breeches will occur.

Building better sand castles

Realities of the situation:

- There will always be un-patched machines.
- Breeches will occur.
- Knowing they happened is much better than not knowing.

Building better sand castles

Bundesdatenschutzgesetz warning!

ALL EVENTS

Query Ran For **0.024 Seconds**

0 to **100** of 500 available for paging

host	message.user	message.comm	message.arguments	message.succe
deploytest	root	sh	sh -c '/usr/bin/gmetric --name=syslog-ng_d_log01_0...	yes
deploytest	root	awk	awk '{print $3}'	yes
deploytest	root	grep	grep 'Total requests'	yes
deploytest	root	gmetric-syslog-	/usr/bin/env ruby /usr/etsy/bin/gmetric-syslog-ng-...	yes
deploytest	root	which	which gmetric	yes
deploytest	root	ruby	ruby /usr/etsy/bin/gmetric-syslog-ng-client.rb	yes
deploytest	root	awk	awk '{print $NF}'	yes
deploytest	root	awk	awk '{print $6}'	yes
deploytest	root	tail	tail -1	yes
deploytest	root	gmetric	/usr/bin/gmetric -n entropy_available	yes

Building better sand castles

- Linux kernel auditd events.
  - http://people.redhat.com/sgrubb/audit/ (driest page ever)
- Mangled with some python because auditd is awful.
  - (will open source this, once the bugs are out. Pinkie swear)
  - Use Mozilla's https://github.com/mozilla-it/audit-cef
  - Pay https://www.threatstack.com/ if you "Cloud".
- Throw in ELK/syslog/giant file to grep through.

Building better sand castles

More awesome auditd stuff purely for people downloading the slides:

- http://security.blogoverflow.com/2013/01/a-brief-introduction-to-auditd/
- http://blog.threatstack.com/labs/2014/8/21/threat-stack-vs-redhat-auditd-showdown
- http://www.slideshare.net/MarkEllzeyThomas/

Data

https://www.flickr.com/photos/jdhancock

Backups

Building better sand castles

Backups

- Don't ship your DB backups off unencrypted.
- Don't use symmetric encryption, because the key will live with the backup (probably).

Canaries

Building better sand castles

"Animal sentinel"

- Put obvious "fake" data in data stores, use IDS to detect them in places they should never go.

Building better sand castles

"Animal sentinel"

- Put obvious "fake" data in data stores, use IDS to detect them in places they should never go.
- Operational uses too. Spotting non-TLS LDAP traffic.

Building better sand castles

"Animal sentinel"

- Put obvious "fake" data in data stores, use IDS to detect them in places they should never go.
- Operational uses too. Spotting non-TLS LDAP traffic.
- Load Balancer Canary

To Conclude

Building better sand castles

Conclusions

- Laptops/users trust the environment. This isn't always good.

Building better sand castles

Conclusions

- Laptops/users trust the environment. This isn't always good.
- Servers don't have to run so blindly, there's a wealth of information in the Linux kernel.

Building better sand castles

Conclusions

- Laptops/users trust the environment. This isn't always good.
- Servers don't have to run so blindly, there's a wealth of information in the Linux kernel.
- Be careful with data. Help it be careful with you.

Building better sand castles

Questions?

(Hah! As if we have time...)

https://www.codeascraft.com/

https://github.com/etsy/

https://www.etsy.com/