

Security, Viruses, Malware

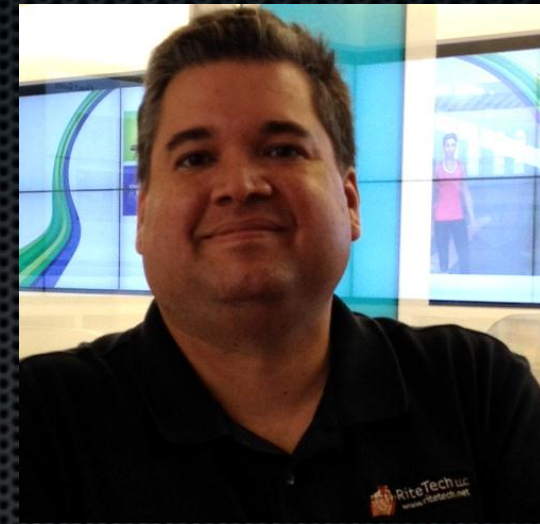


“It’s Real; It’s Now...
You need to take it seriously”

Dave Bainum 
@dbainum; @ritetechllc



Dave Bainum, PMP, CSM

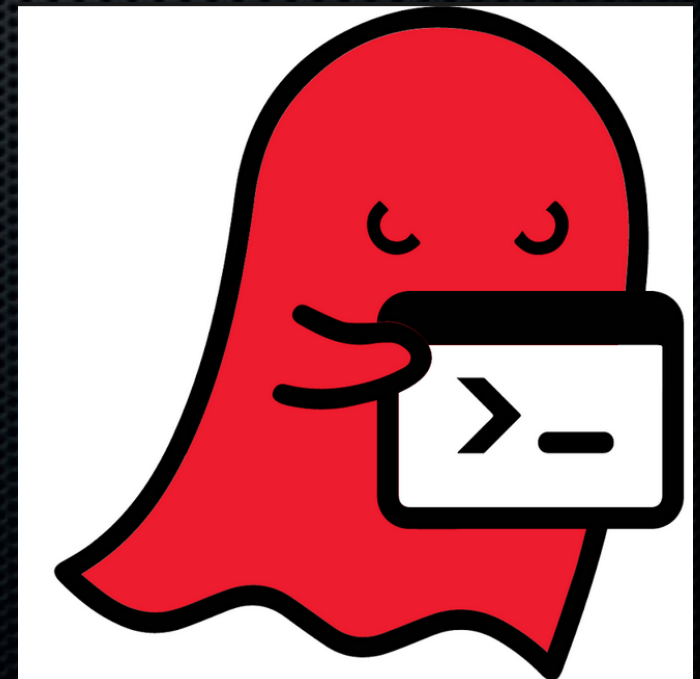


- IT Project Mgmt. of various InfoSec, Upgrade, Deployment, Data Center, & Disaster Recovery projects for Org's of all sizes/types
- IT Security Projects; Endpoint & 0-Day Protection
- Ex-Microsoft Certified Trainer & ex-HOA Prez.
- Spoken at: MacTech, ITExpo, SMBNation, others...
- RiteTech: Founded in '07; in ACN since late 2012
- Creator of the www.CrashScreens.com and www.HOAsGoneWild.com blogs/web sites

Security, Viruses, Malware...

What we'll cover

- Why are we doing this & why do we care?
- Concepts / Definitions / Best Practices
- Sample Tools, Tips, Techniques
- Some Perspective / “Experts Weigh In” on Mac vs. PC Security (and why it’s a moot point now!)
- Group Discussion(s) / Q & A

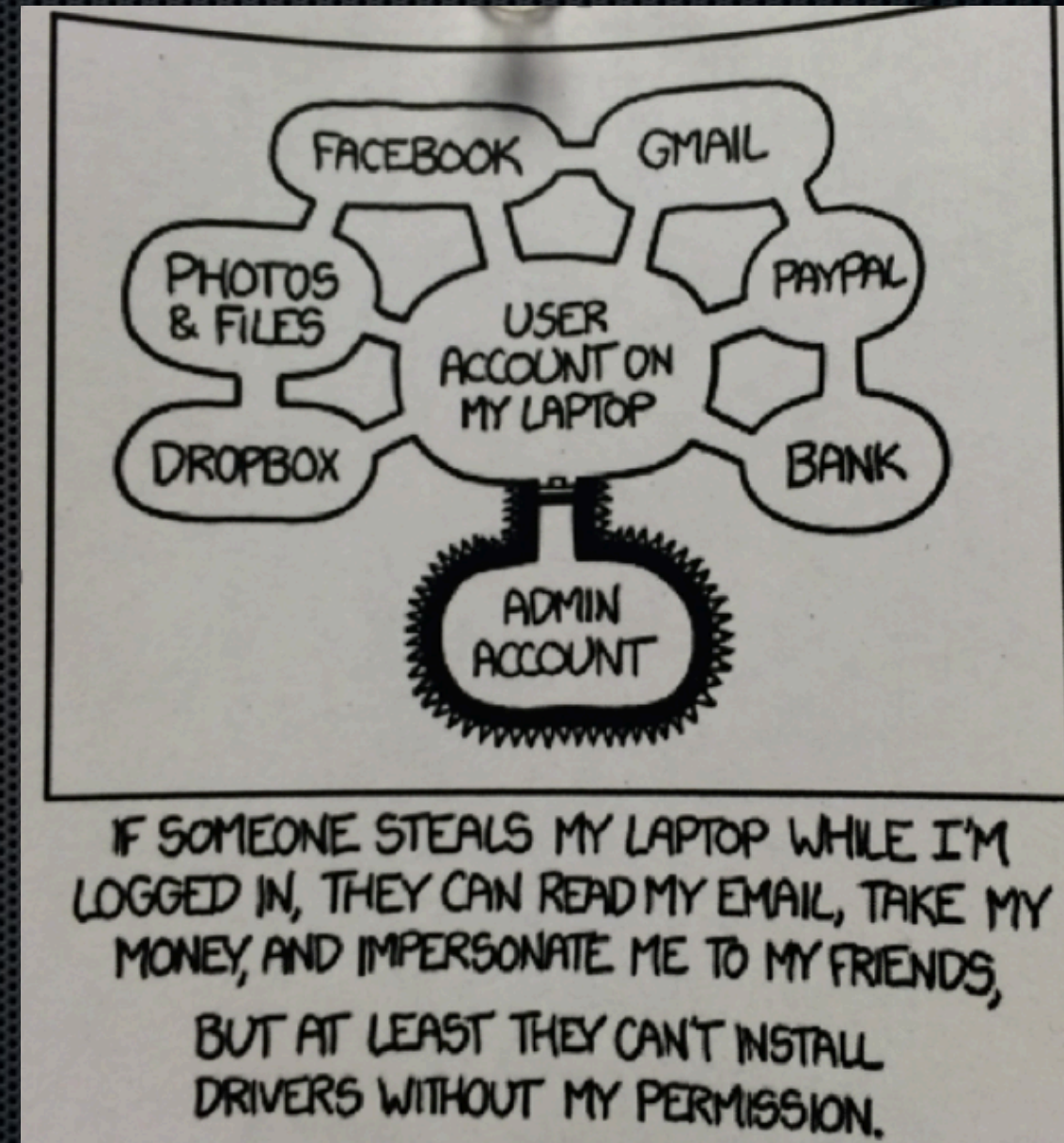


Before we get “into it...”

- Who here (regularly) ...
- ... Sells, uses, or deploys...
- ... AntiVirus software?
- ... Firewalls?

SEIM ? (Splunk?)

- How about InfoSec consulting? Policy development?



Some Definitions...

- **Virus** = a piece of programming code that is capable of copying itself, and typically has a detrimental effect, such as corrupting the system, or stealing/destroying data.
- We'll just say that it's **infectious, unwanted, intrusive, unauthorized software**.
- **Malware** = Umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, **scripts, active content**, etc.
- Zero-Day (0-Day) = (Will explain).
- There's also PUP's = Potentially Unwanted Programs ... but all of these are **InfoSec (Information Security) concerns**



InfoSec: Why Should We Care?

- IT Security *IS* **C.I.A.** =
- **C**onfidentiality....
- **I**ntegrity...
- **A**vailability...



Some More Examples...

- **C**onfidentiality...

Applying proper permissions, protocols, encryption, etc. to protect data & apps to maintain confidentiality.

- **I**ntegrity...

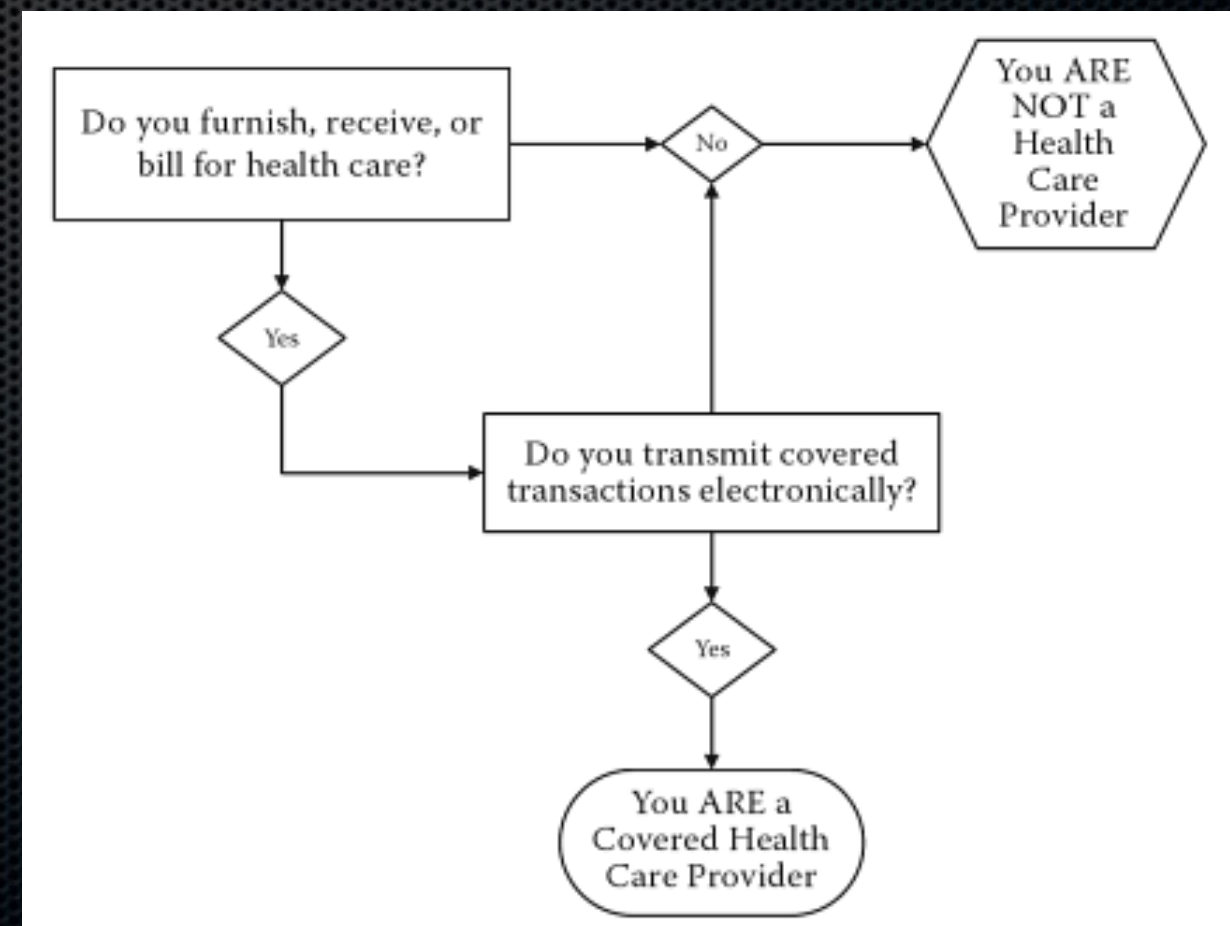
Operates faithfully & as expected; harmful data changes or other bad things are prevented (or at least, detected).

- **A**vailability...

Taking precautions to ensure system uptime, and availability of critical app's and data.

Other Reasons To Care (a lot?)..

- Compliance: “Hungry, Hungry HIPAA?”
(also PCI, GLB, SOX, others...)
 - Reputation, Safety..
 - Performance...
- Contract requirement?
- Audit requirements?



To preserve InfoSec & CIA...

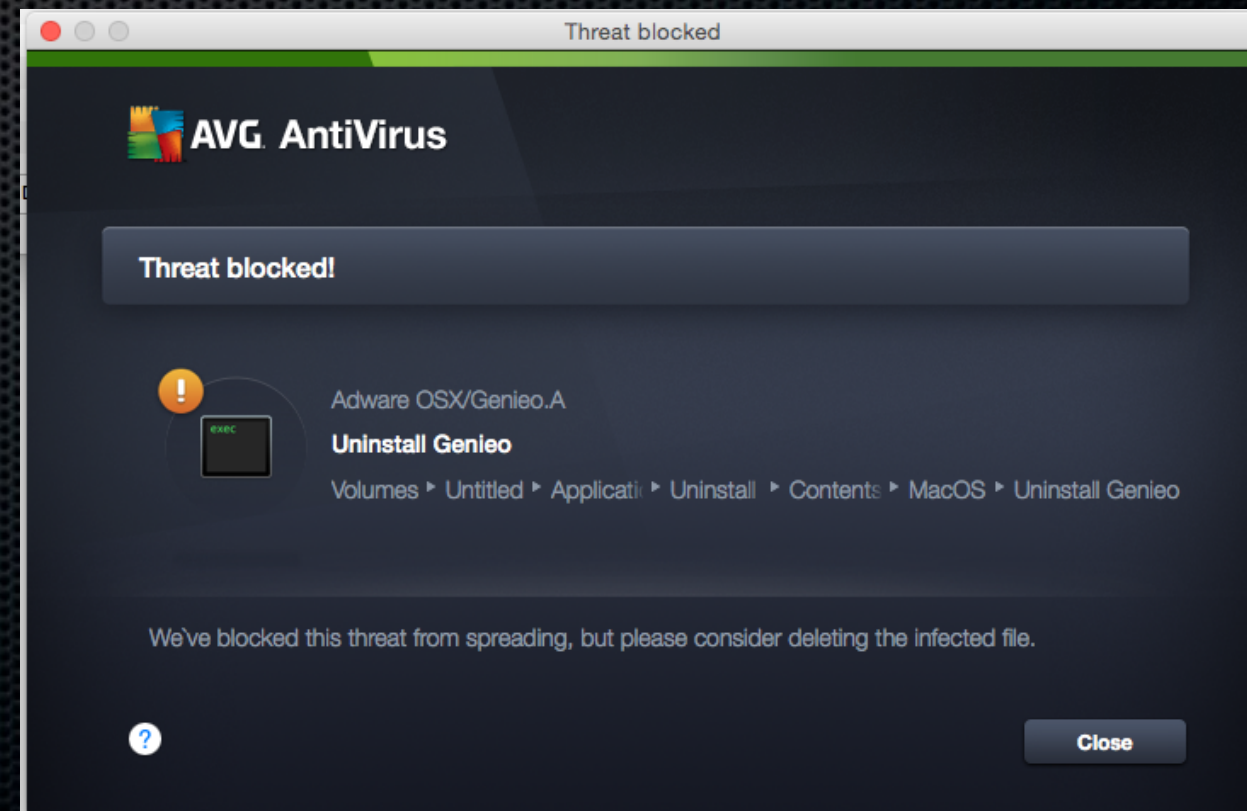
- A basic IT security policy & awareness – even if it's just a few pages w/ basics like password tips, & how to handle lost/stolen BYO devices
- An incident response and management plan –to help monitor trends & know if the specific **organization(s) or individual(s) are being targeted**
- A good, solid HW/SW inventory that's **kept up to date**
- Good, solid firewalls, switches, & wireless - & **physical security**
- Some sort of strategy & mechanism to monitor IT security events
- Good, solid data backups and/or B.C.P., that's periodically *tested*
- A functional patch & update management approach (how to handle all of those Adobe and Java updates? Other updates?)
- Some sort of endpoint protection (ideally, a centrally managed one)

Why it matters...

- Viruses, malware, 0-Day's & PUP's can drastically undermine the "CIA Triad", or even attack other systems
- However, other factors or incidents can, too
- Such **as physical security**, environmental, and/or denials of service (downtime/outages)
- Or even, hostile actors convincing employees (or users) to do things or reveal info. that they shouldn't
- Changing attack trends, common software & application platforms – as well as regulation - is all starting to render the "PC vs. Mac: What's the safer OS platform?" argument obsolete – particularly for endpoint protection

Endpoint protection options...

- Symantec / SEP
- Sophos, McAfee
- E-Set, AVG
- Intego, BitDefender, ...
- Kaspersky
[may provide
most frequent
updates (?)]



How to pick? “Best Fit”...

- Budget
- Performance / User Experience
- Options / Customization
- Central Management / “Defense in Depth”

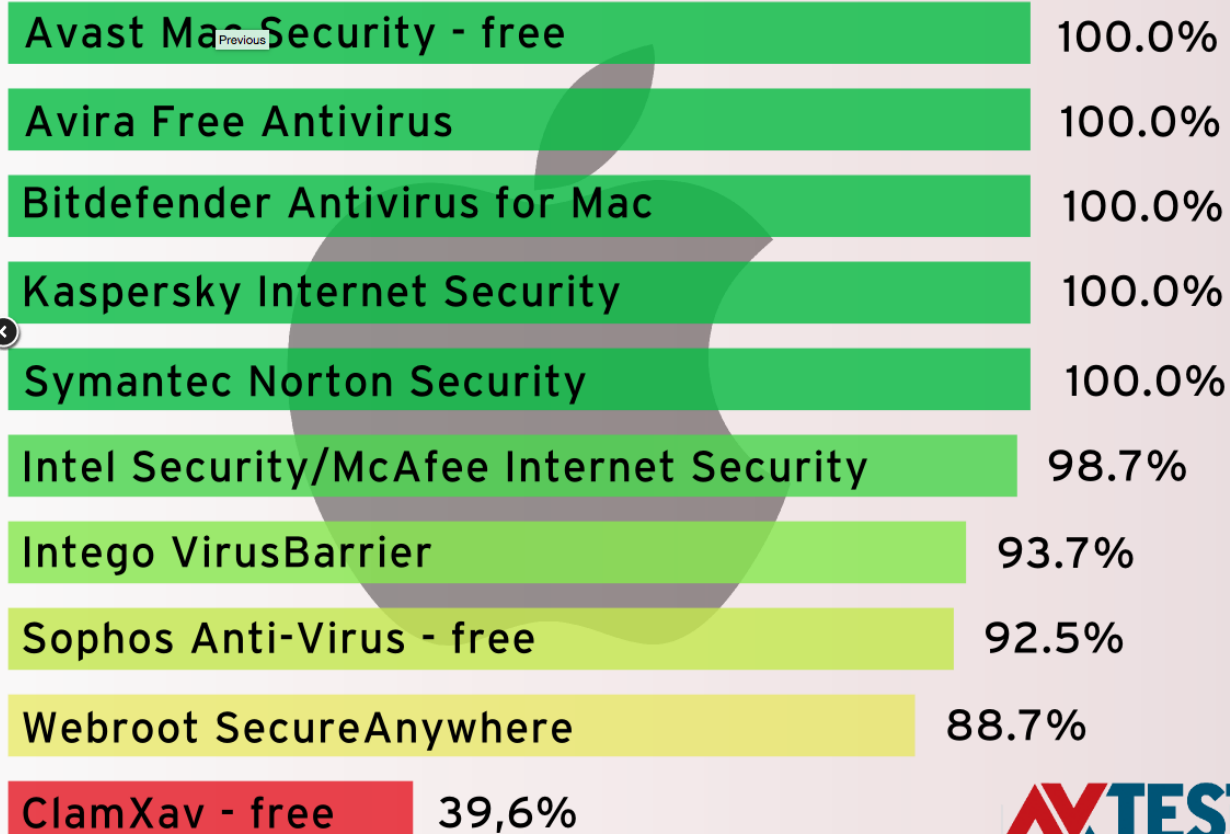


Possible integration with SEIM (e.g. Splunk)

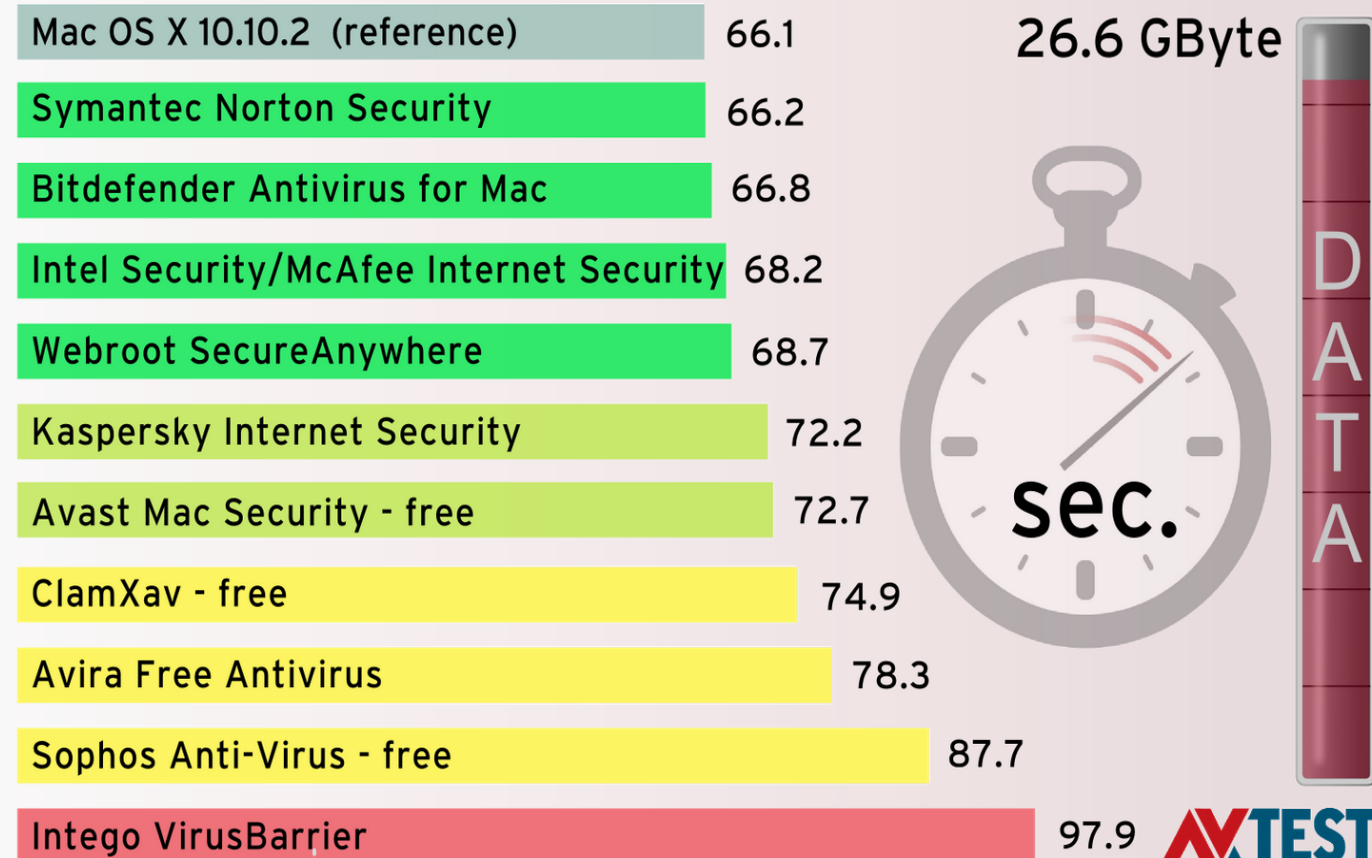
- Ramp-Up and Training Time; Ease of use
- Tuning; Sensitivity; User Experience; “Uniqueness?”

Some sample research...

Test: 10 Security Suites for Mac OS X (On-Demand Test):



This is how security packages slow down Mac OS X when copying



Network protection options...

- Get a **real** firewall; and a FAST one; not the \$50 one (please)
- It should ideally support:
- Geographic blocking, application blocking and/or throttling, event log aggregation (Syslog, splunk, etc.), Deep Inspection
- Even better if it shows realtime graphs of activity, attacks, exceptions, etc.
- Please get **managed switches** wherever possible
- Consider VLAN's, MAC address filtering, 802.1x Auth, and/or DHCP reservations



But... A Riddle...

- Can a modern IT system be kept secure with a firewall (or other security sensors, or devices) that are NOT being actively monitored?
- ... Or with IT systems and critical data that end-users can change and modify at their own whim?
- ...Or better yet, if all of this was happening without the business management or owner(s) even knowing that these changes occurred?
- How would you even know without some form of Endpoint mgmt.?



What to do about Wireless...

- Convenient? Yes!
Hard to secure?
You Betcha!
- Many organizations consider it “untrusted”
- Be careful how to handle guest devices
- Please don't get the \$50 AP for any mission-critical or security-critical applications.
- Consider MAC address filtering or other advanced security options (this doesn't protect against eavesdropping or MITM, though)



Some other suggestions...

- User Training & Awareness is very important – particularly to combat Phishing & targeted attacks
- Many attacks may involve con-artistry (“social engineering”), particularly via phone call(s)
- Application and/or Developer/Publisher Whitelisting (can potentially be a pain)
- Consider encryption (and/or encrypting backups)
- Only grant account access level(s) absolutely needed
- Passwords continue to be a “weak link”...
Two-Factor Authentication (2FA) helps in some scenarios.
- Use RMM tools & reports (Casper, Watchman, etc.)

“Experts Weigh In on Mac vs. PC Security”...

- <http://www.cnet.com/news/in-their-words-experts-weigh-in-on-mac-vs-pc-security>:
- “In reality, all technologies are subject to security vulnerabilities, including...**browsers, common plug-ins, and common applications that run on top of the OS**. So in reality, consumers can fall victim to online threats regardless of the OS they’re using.”
- “Both [OS X & Windows] are particularly vulnerable to client-side application exploitation...and **the content that most people want to view or process is often from unknown sources & requires a fair amount of control of the system for ‘proper’ execution – e.g. Flash, etc.**”

Some Perspective...

- > 48 Million new unique Malware Samples in start of 2015*
- < 5K new viruses were written for MacOS X*
- Apple's 2015-Q1 USA Market share was #3: **12%** (**1.67M New Macs!**); behind HP (26.1%), Dell (23.2%)**
- Apple continues to buck the trend of **-5.2% overall** PC shipments decline**
- Sources: *Andreas Marx, CEO of Independent AntiVirus Research Institute AV-Test

** : Gartner Estimates, April '15



Let's consider that...

- More market share = more visibility = more lines of code in use by more people = more ppl. online = larger attack surface(s) = more potential exposure
- The PC world, Microsoft, and large organizations have learned (often, painfully ... at times, begrudgingly) how to deal with patch/vulnerability management & many IT security threats.
- The Apple world has enjoyed “security by obscurity” for a while – but with increasing market share, the platform will get more attention from hackers/attackers/etc. as time goes on.
- That said, the actual OS used is becoming less relevant every day. Most newer attacks now target user behavior, specific applications (e.g. Adobe, Java, web browsers, plug-in's, E-Mail clients, infected codec's, scripting attacks), or even specific companies, industries, and/or individuals.

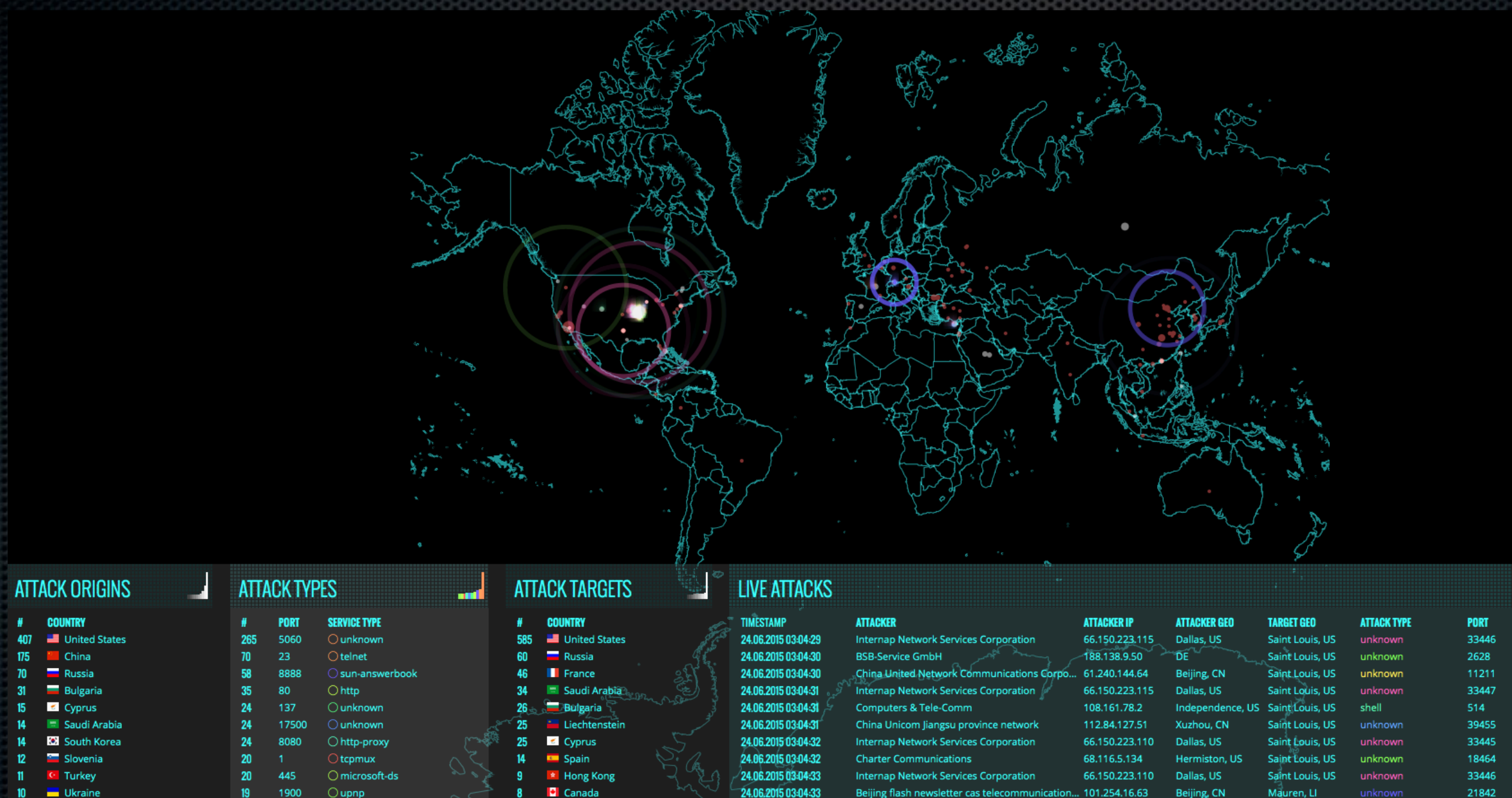
So, who does these things?

- Nation-states (particularly China)
- Industrial Espionage (competitors)
- (Dis)-gruntled (Ex)-Employees
- Unsupervised kids who don't know any better
- Your cousin Vinnie (or your child playing on a work PC)
- Hackers for Hire and/or Hackers of opportunity
(most elaborate attacks, online theft, fraud are financially motivated)
- Existing employee(s) and/or contractors
- Other infected computers that are already out there



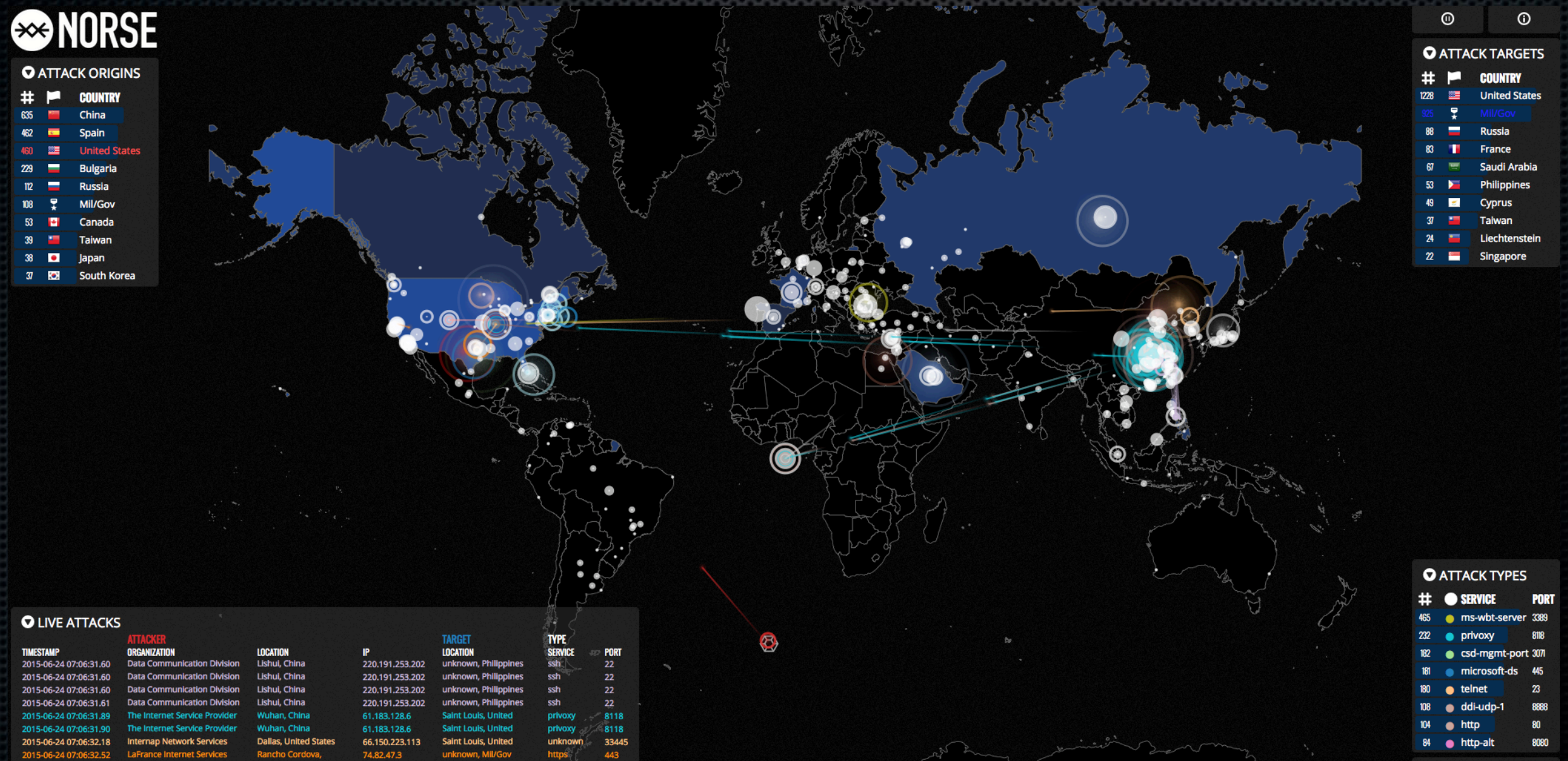
Still Not Convinced?

- Check out <http://www.norse-corp.com> (click on “Live Attacks”) or <http://map.ipviking.com> (Norse)



Still Not Convinced? (#2)

- Check out <http://www.norse-corp.com> (click on “Live Attacks”) or <http://map.ipviking.com> (Norse)



References / Takeaway's / Etc.

- If you go to only one link on this topic, seriously:
- <http://www.cnet.com/news/in-their-words-experts-weigh-in-on-mac-vs-pc-security>
- AVTest (AntiVirus research test labs)
- InfoSec Vendor Web Sites (Symantec, Kaspersky, etc.)
- Google HIPAA and related compliance / security standards
- Keep an eye on Bromium & other emerging protection techniques

Questions?



Dave Bainum



@dbainum; @ritetechllc

www.HOAsGoneWild.com

www.CrashScreens.com