BACKUPS, RANSOMWARE AND SECURITY FOR YOUR CENTRICITY ENVIRONMENT

Design I.T. Solutions,

Moscow Family Medicine

ABOUT US

- Daniel Schwartz – Design I.T. Solutions
- Mary Glaze – Moscow Family Medicine

TOPICS

- Ransomware
- Backups
- Security (prevention)

RANSOMWARE

- Encrypts files it has access to
  - This includes any network resources the active user has modify rights to
- Newer versions have the ability to:
  - Encrypt backups
  - Embed themselves in backups over time and launch when it sees the cycle is complete
  - Destroy shadow copies
  - Put unencrypted copies of files on public websites

RANSOMWARE

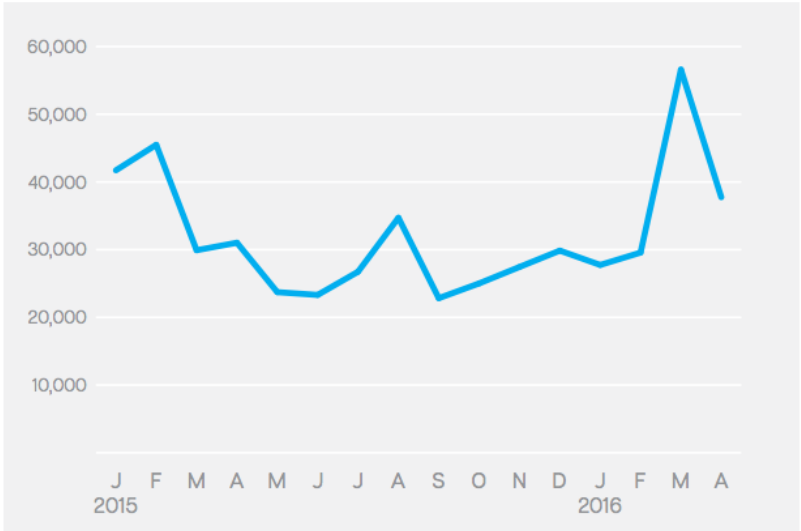
- Gives the user a timeframe to pay for an encryption key
  - Many versions now let you test unencrypting a file to prove the ransom is worth it
  - After a set amount of time, the ransom goes up
  - Files may be released to public domain if no ransom is paid
- White-label, script kiddy friendly
  - Fastest increase in ransomware yet

RANSOMWARE

56,000 ransomware infections in March 2016

Estimates from the FBI put ransomware on pace to be a $1 billion dollar source of income for cyber criminals this year.

Figure 1. Overall Ransomware Infections by Month from January 2015 to April 2016



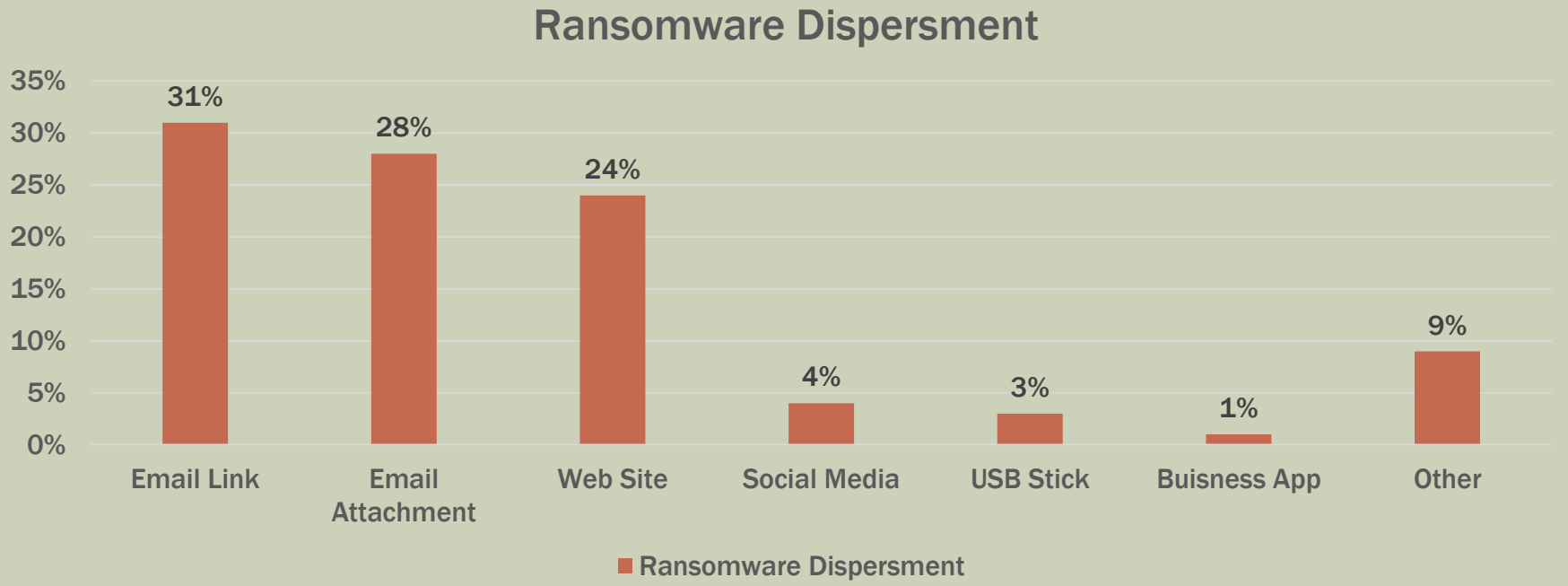
$209 million was paid to ransomware criminals in Q1 2016

Source: Symantec

RANSOMWARE

- **Roughly 80% of all organizations are confident that their backup can provide them with complete recovery**
- **Less than half of ransomware victims fully recover their data, even with backup**
  - Unmonitored and failed backups
  - loss of accessible backup drives that were also encrypted
  - loss of between 1-24 hours of data from the last incremental backup snapshot.

RANSOMWARE



Source: Osterman Research, Inc

WHAT SHOULD YOU BACKUP?

- Centricity Database
  - Backup the SQL backup files
  - Use integrated SQL backup solution
- Docutrack (Document Manager) files
  - PDF, Tiff, txt, etc. that are indexed to a network share
- Docutrack, ESM, Patient Portal and other Databases
- Archives/Scanned documents
- Any other electronic documents worth keeping
- Anything your business needs to function

TYPES OF BACKUPS

- Multiple Backup Options:
  - Automated
  - Offsite
  - Encrypted
  - Compressed
  - SQL Native
  - Dynamic
  - Adaptive
  - Shadow Copies

PROPRIETARY VS NETWORK VISIBLE

- Ransomware can hit anything on the network it has access to
- Using network visible media can allow the backups to be encrypted by ransomware
  - Network visible OS
  - Network share
  - NAS
- Using a backup solution that has a proprietary agent to access backups on each device is the best option
  - Backups are not susceptible to encryption

PROPRIETARY BACKUP AGENTS

- Barracuda
  - Have a hardened appliance that connects to proprietary agent running on servers
  - Can integrate with Vmware, Hyper-v, SQL server and exchange natively to optimize backups
  - De-duplicates, compresses and encrypts data on the appliance before sending a copy to cloud storage
- Carbonite Online Backup
  - Backs up directly to cloud from each computer

BACKUP FREQUENCY

- Daily, or twice a day if bandwidth and server performance can handle it (and volume of data changes is high)
- Keep 8 daily revisions
- Keep 5 weekly revisions
- Keep 6 monthly revisions (Vault to Cloud)
- Keep 2 yearly revisions (Vault to Cloud)

- Ransomware embedded into backups is here

BACKUP REQUIREMENTS

- ANYTHING offsite must be encrypted
  - If you take hard drives/tapes offsite, the media must be encrypted
  - Data leaving premises must be encrypted in transit and at rest
- You must keep records for anywhere between 7 and 21 years
  - Your old EMR/PM system needs to be accusable, back it up too

SECURITY

- Next-Gen Firewall
- Spam Filter
- OS Hardening (Security Updates)
- User Education

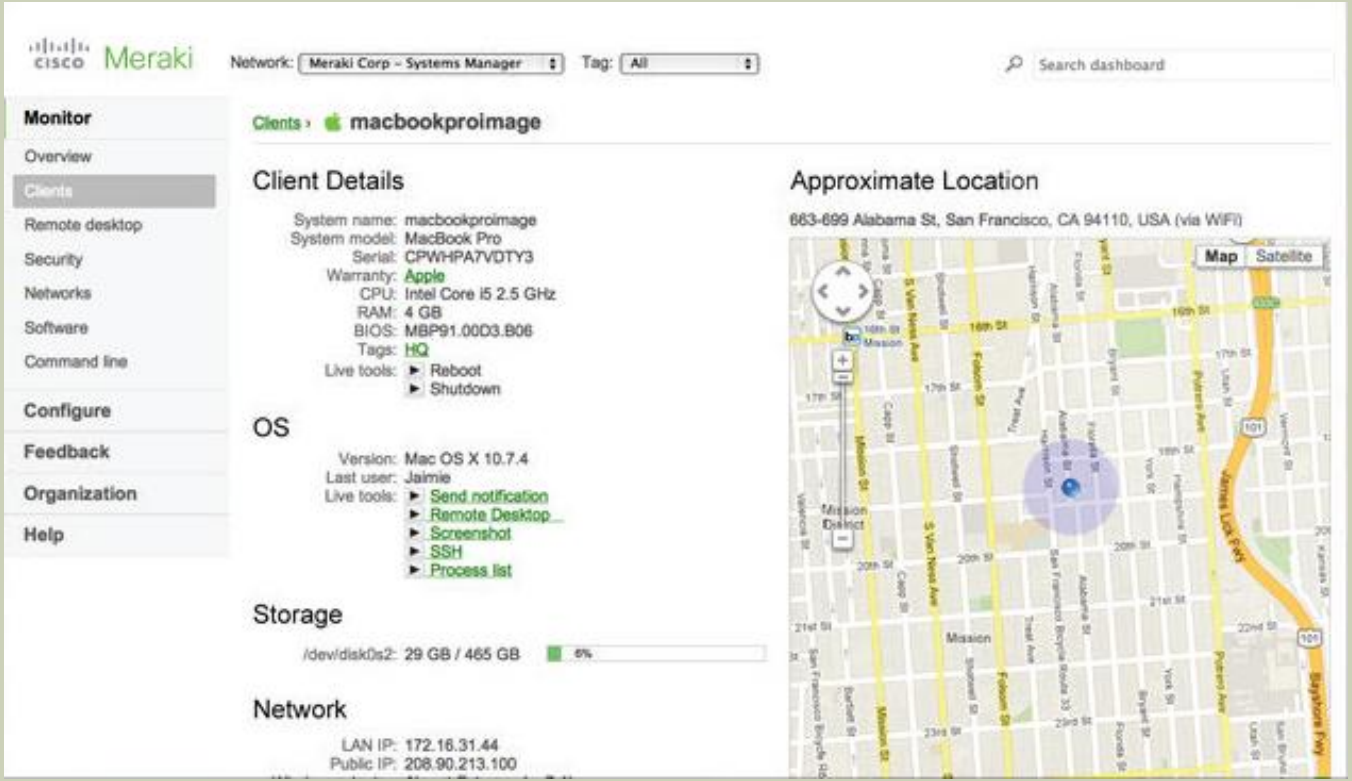
NEXT-GEN FIREWALL

- Contain all the functions of a normal firewall
- Add additional OSI layer (TCP/IP Layer) filtering
  - Layer 7 interaction filtering
  - Policy per group/user/computer
- Can help stop compromised systems from getting out
- If your firewall is 2 or more years old, its time to upgrade
  - Normally firewalls last 5 years, but older than 3 most likely does not have the latest technology
- Routine firewall updates

NEXT-GEN FIREWALL

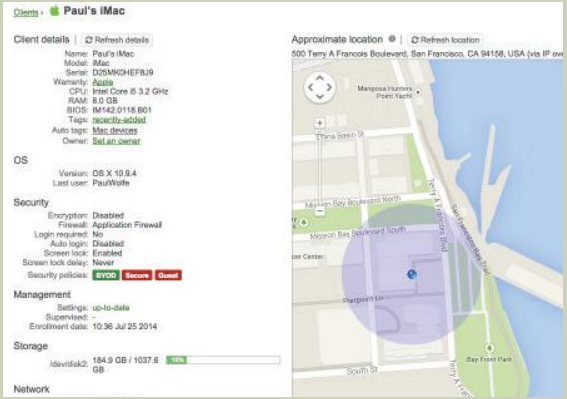
- Depending on the Vendor, it can secure/wipe/monitor remote computers
- Allows for extensive web shaping
  - Control who can get on social media or other potential virus spreading sites
- Has site ratings to block known compromised sites
  - Usually updated daily-weekly.

NEXT-GEN FIREWALL



NEXT-GEN FIREWALL

#	Status	User	OS	Model	RAM	Connectivity	Name	Disk % used	CPU	Tags	Public IP	LAN IP	Phone #	Disk capacity
1		[redacted]@gmail.com	Android 4.4.2	Samsung Galaxy S III	-		[redacted]@gmail.com	95%		employee	76.103.244.38	192.168.1.102	5103881580	12 GB
2		[redacted]@gmail.com	Android 4.4.4	XT1080	-		[redacted]@gmail.com	49%		employee	71.57.60.176	192.168.128.243	4014654007	25 GB
3		[redacted]@gmail.com	Android 4.4.4	XT1060	-		[redacted]@gmail.com	42%		employee	67.161.2.112	192.168.1.50	2622217505	26 GB
4		Admin	OS X 10.6.6	MacBook	2 GB		normal-name	26%	Intel Core 2 Duo	devel	184.23.135.130	192.168.128.2	-	149 GB



Security policies

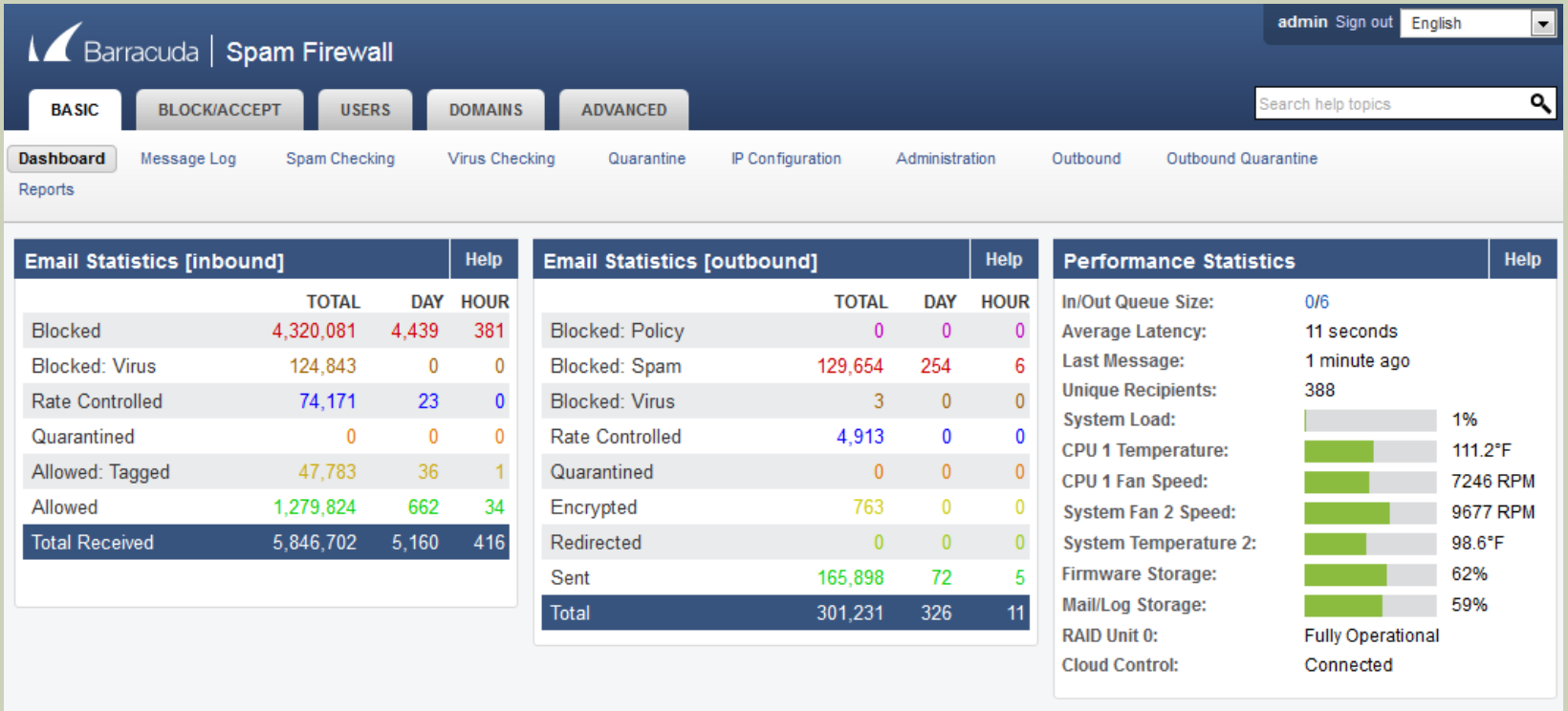
Back to list >

Security policy name	Secure
Desktop	☑ Screen lock after 5 minutes or less. ☑ Login required ☑ Firewall enabled
OS X	☑ Disk encryption
Windows	☑ Antivirus running ☑ Antispyware installed
Mobile devices	☑ Passcode lock ☑ Device is not compromised

SPAM FILTER

- Keep spam filters up to date with latest patches
- Monitor outbound spam filter for possible unknown infections in your network
- New Sandbox technology will execute attachments in the cloud to test for macro/virus/worm payload
  - Currently only available from Barracuda
  - Can be used with all e-mail providers including office 365
  - Currently only Cloud based, in Q1 of 2017 will be available for on premise appliances

SPAM FILTER


Barracuda | Spam Firewall
admin Sign out English
BASIC
BLOCK/ACCEPT
USERS
DOMAINS
ADVANCED
Search help topics
Dashboard
Message Log
Spam Checking
Virus Checking
Quarantine
IP Configuration
Administration
Outbound
Outbound Quarantine
Reports
Email Statistics [inbound]
Help
TOTAL DAY HOUR
Blocked 4,320,081 4,439 381
Blocked: Virus 124,843 0 0
Rate Controlled 74,171 23 0
Quarantined 0 0 0
Allowed: Tagged 47,783 36 1
Allowed 1,279,824 662 34
Total Received 5,846,702 5,160 416
Email Statistics [outbound]
Help
TOTAL DAY HOUR
Blocked: Policy 0 0 0
Blocked: Spam 129,654 254 6
Blocked: Virus 3 0 0
Rate Controlled 4,913 0 0
Quarantined 0 0 0
Encrypted 763 0 0
Redirected 0 0 0
Sent 165,898 72 5
Total 301,231 326 11
Performance Statistics
Help
In/Out Queue Size: 0/6
Average Latency: 11 seconds
Last Message: 1 minute ago
Unique Recipients: 388
System Load: 1%
CPU 1 Temperature: 111.2°F
CPU 1 Fan Speed: 7246 RPM
System Fan 2 Speed: 9677 RPM
System Temperature 2: 98.6°F
Firmware Storage: 62%
Mail/Log Storage: 59%
RAID Unit 0: Fully Operational
Cloud Control: Connected

OS HARDENING

- OS Security Updates (weekly)
- Security updates for applications you use
  - Java
  - Flash (will diminish with HTML5 over time)
  - Acrobat
  - Word/Excel (Macros)
  - JBOSS
  - Sure Scripts Products
- Firewall/VPN software updates

USER EDUCATION

- Users makeup the largest vulnerability in your organization
  - Inexpensive to midigate
- Staff meeting reminders
- Quarterly reminders via prizes
- Network Policies in place to help
  - Change passwords, don't write them down
    - Not to frequent, not to infrequent (no less than 75 days, no more than 120)
  - Have users double short passwords to help them remember long passwords (Caps on the first, number at the end)
    - Passwords should be 10+ characters

LIVE DATA

- Meraki Firewall
- Barracuda Spam Filter
- Barracuda Backup

QUESTIONS?

CONTACT

- Daniel Schwartz
  - Design I.T. Solutions – 509-534-4874 xtn 400
  - dschwartz@designitsolutions.com
- Mary Glaze
  - Moscow Family Medicine - 208-882-7565
  - mglaze@moscowfamilymedicine.com