Cyber Security Landscape and Challenges

R. Sekar

Evolution of Threats

- Before era of modern crypto (World War II …)
  - Break secret messages during transmission
  - Primarily the domain of nation states
  - Modern cryptography has all but eliminated this threat
- Modern era
  - Focus shifts from altering messages to breaking end-systems that store and process these messages
  - Several culprits
    - Software vulnerabilities
    - Human errors
      - Carelessness or lack of awareness on the part of users
      - Operator errors
    - Emergence of cybercrime and related activities

Evolution of Modern Threats

- First generation
  - break into high-value systems (e.g., banks) through proprietary networks
  - criminal elements as well as rogue nations
- Second generation
  - Malware that spreads due to information sharing
    - Viruses and worms
  - Perpetrated by hackers as a “hobby”
- Third generation
  - Malware that spreads via the Internet
  - Email viruses and Internet worms
  - Still, no evidence of organized or criminal elements

Internet-based threats (3rd generation +)

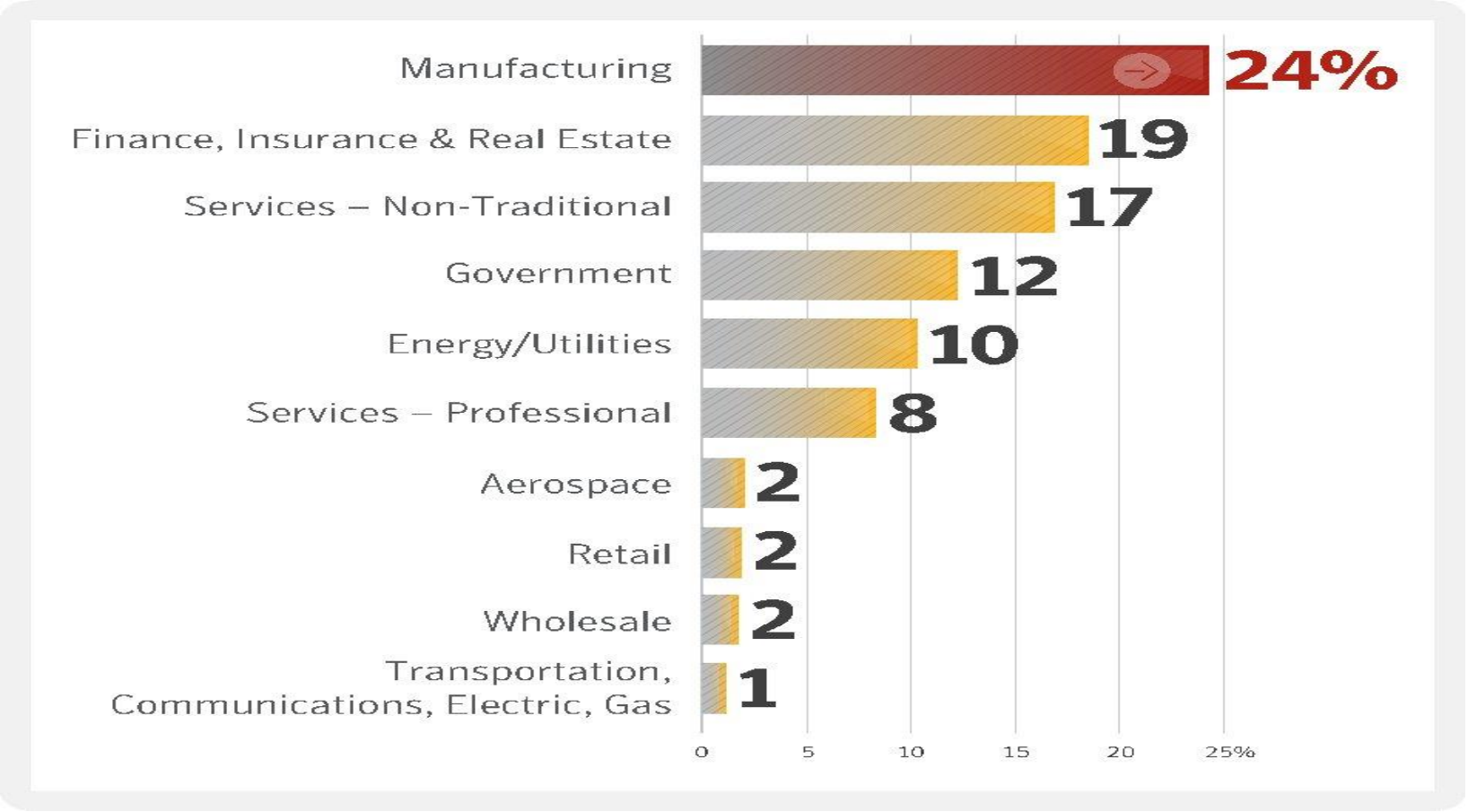
- Initial entry: Software exploit or stealing passwords
  - Increasingly, this step needs some level of user trust
    - Spam, phishing, …
- In some cases, esp. on servers, damage may be effected by the exploit itself
  - More common: exploit installs base for future operation
    - Bots, Trojans, spyware, …
- Goals
  - Steal confidential information
    - Passwords, bank accounts, credit card #s, …
  - Deface property
  - Distribute malware

4th generation: Commercialization of malware

- Hacking for profit, not just fun/fame
  - Thriving black market for exploits and other services
  - Specialization at all levels of cybercriminal enterprise
    - Exploit development, C&C software, Botnet rentals, …
- "Bot"-centric model for cyber crime
  - Relay spam (e-mail scan, phishing)
  - Extortion (using DDoS or targeted attacks)
  - Stealing confidential data (e.g., passwords, trade secrets, IP, …)
- Focus on stealth and obfuscation
  - Rootkits and other cloaking techniques
  - Evasion: match behavior of benign software
  - Anti-analysis techniques
    - Sophisticated packing and metamorphism
    - Detect execution within analysis environment

Current (5th?) Generation

- Major increase in targeted attacks



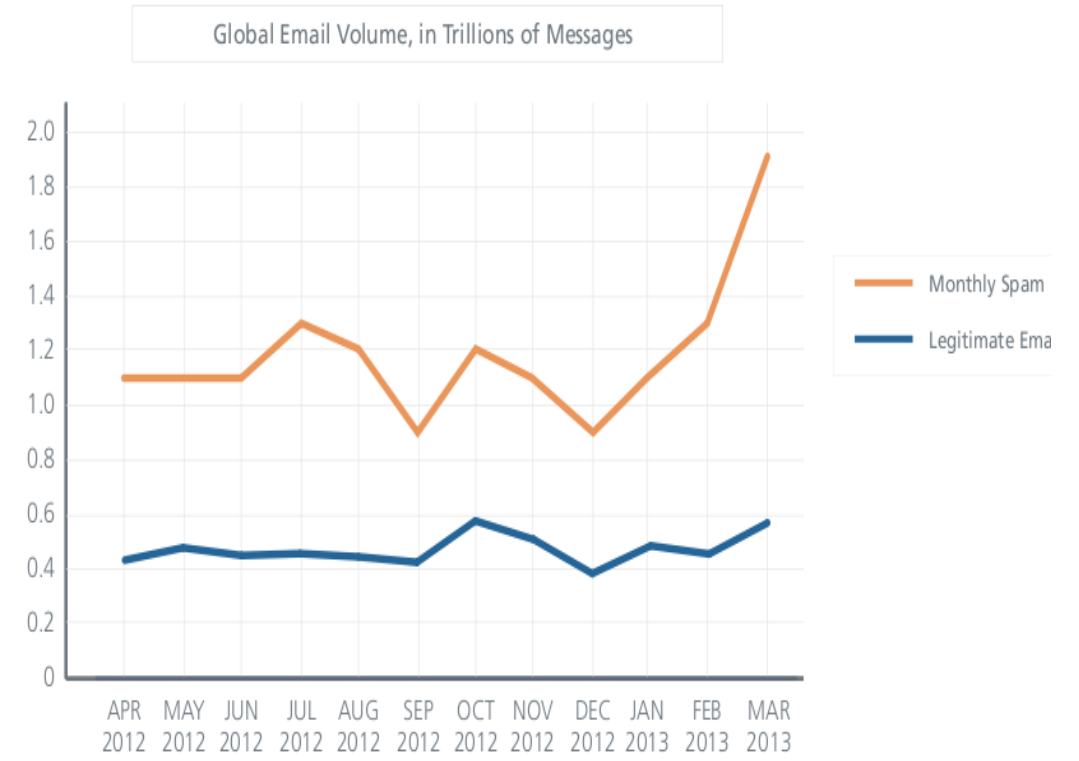
Source: Symantec Threat Report 2013

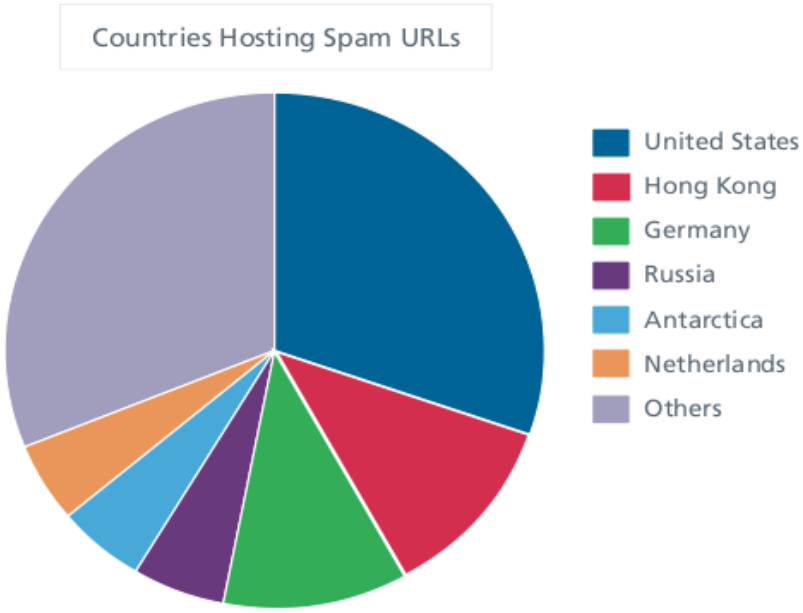
Current (5th?) Generation

- Major increase in targeted attacks
- Advances in exploit development to overcome security improvements on recent OSes
- Sophisticated social engineering techniques
  - Gain user's trust so that he/she may grant the level of access needed for the exploit and/or malware operation
  - Leverage social media
    - Tendency of people to share a lot of personal information
    - Tendency to trust "friends"

Spam

- Spam volumes hold steady
  - After falling from a high of 6T to about 1T/month
- Expands to social networks
  - Facebook, Twitter, Instagram, …





Source: McAfee Threats Report: First Quarter 2013

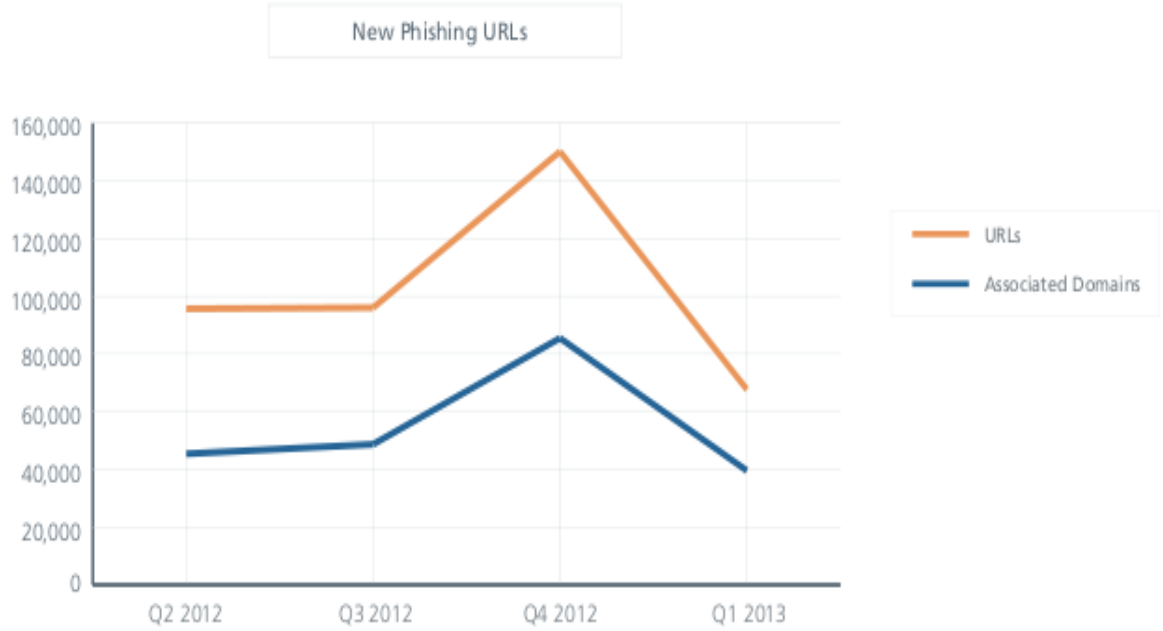
Phishing

- New types of phishing
  - Watering hole
  - Clone phishing
  - Tabnapping

Top 5 Activity for Malware Destination by Geography

Country	1 in
Netherlands	1 in 108
Luxembourg	1 in 144
United Kingdom	1 in 163
South Africa	1 in 178
Germany	1 in 196

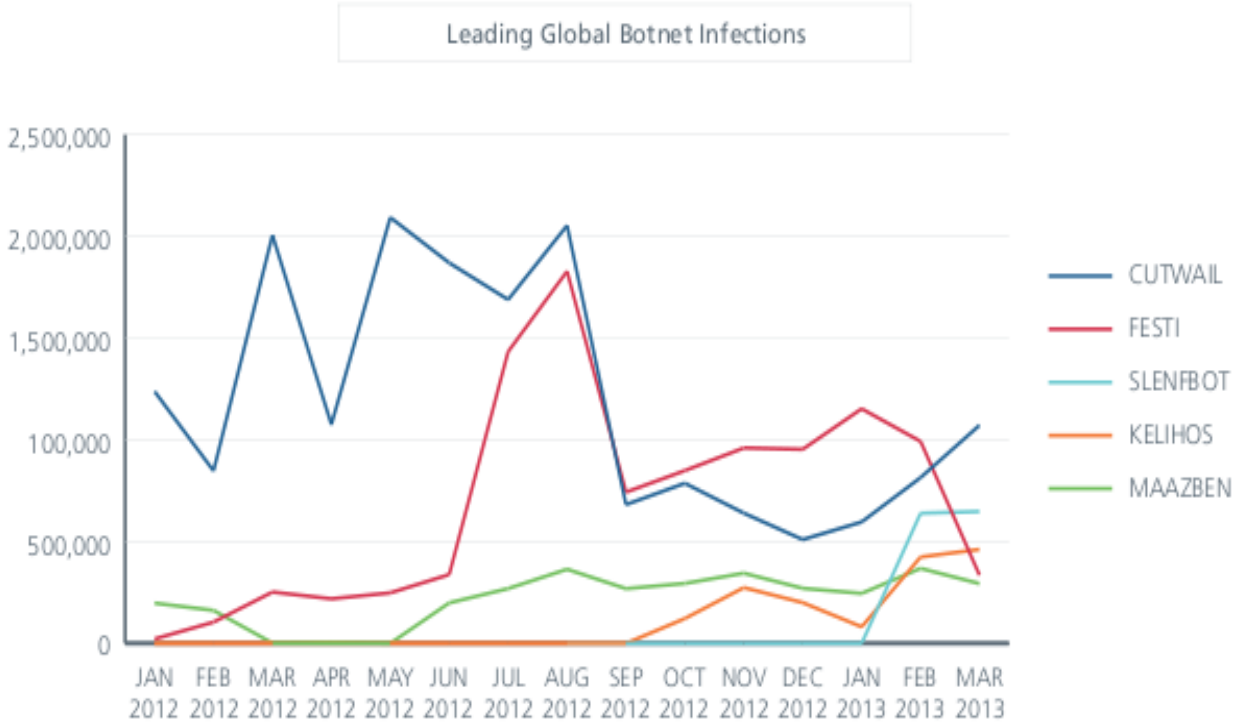
Source: Internet Security Threat Report 2013, Symantec



Source: McAfee Threats Report: First Quarter 2013

Botnets & DDOS

- **Botnets now include mobile devices**
  - **Android botnets**
    - http://mobile.slashdot.org/story/13/01/19/0735259/android-botnet-infects-1-million-plus-phones
- **DDoS used as a diversion**
  - http://www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf



Web Vulnerabilities

Scanned Websites with Vulnerabilities

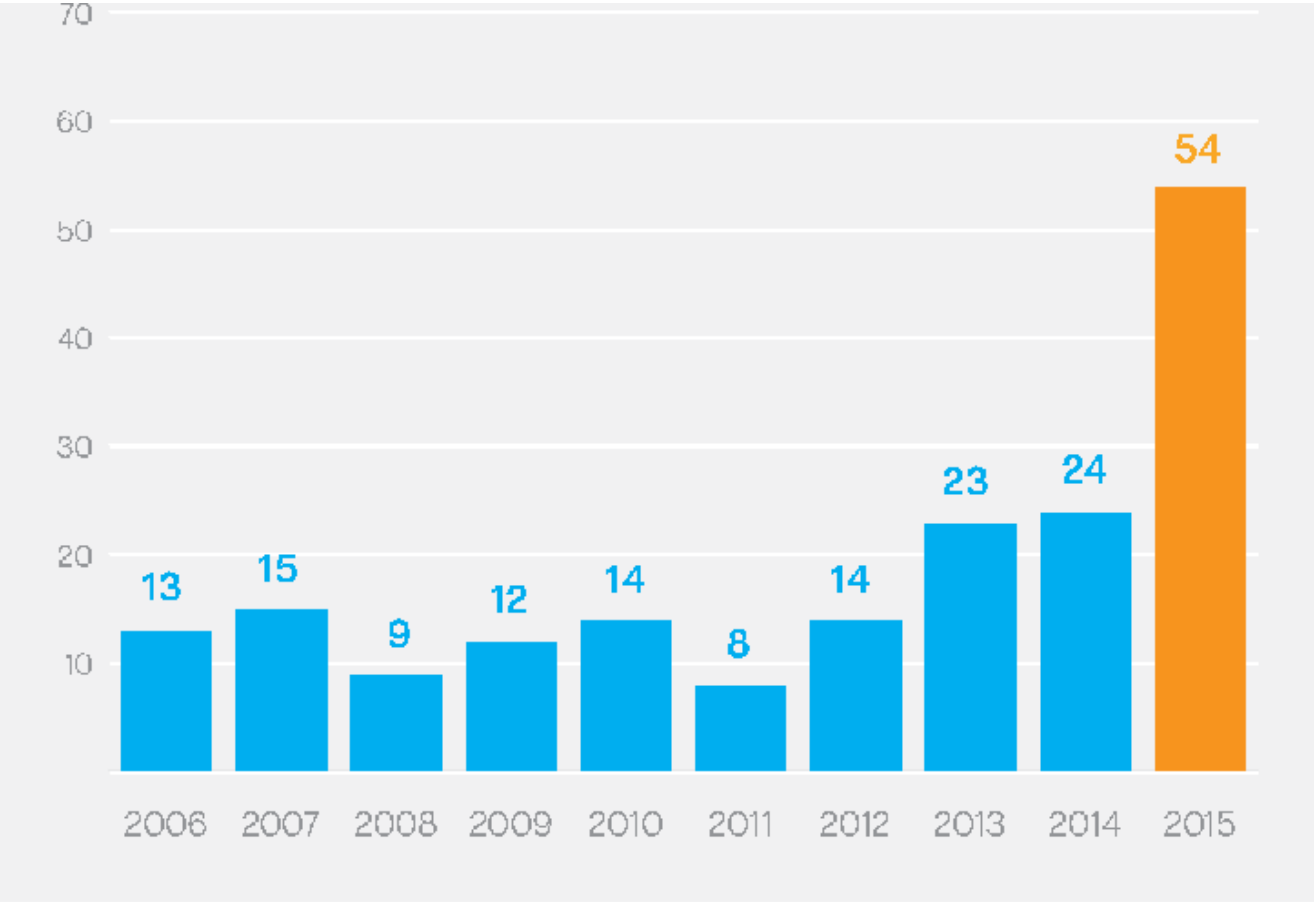
- *A critical vulnerability is one which, if exploited, may allow malicious code to be run without user interaction, potentially resulting in a data breach and further compromise of visitors to the affected websites.*

2013	2014	2015
		
77%	76%	78%
	-1% pts	+2% pts

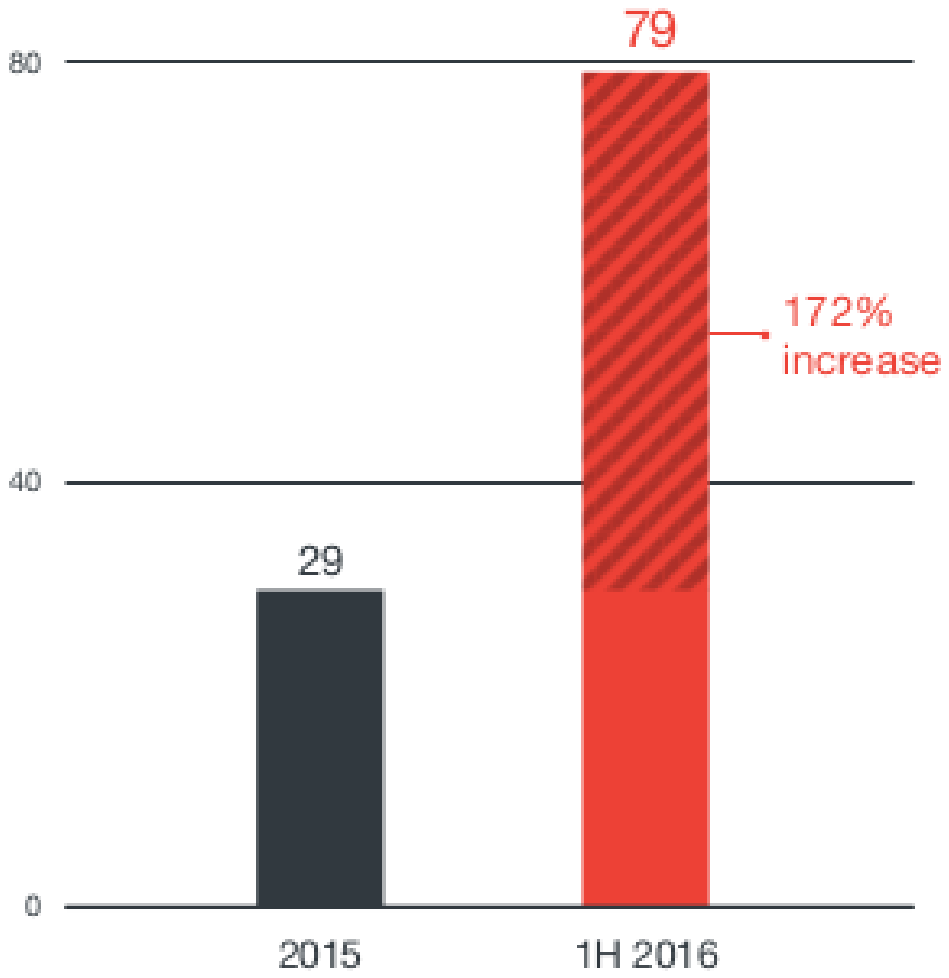
Percentage of Vulnerabilities Which Were Critical

2013	2014	2015
		
16%	20%	15%
	+4% pts	-5% pts

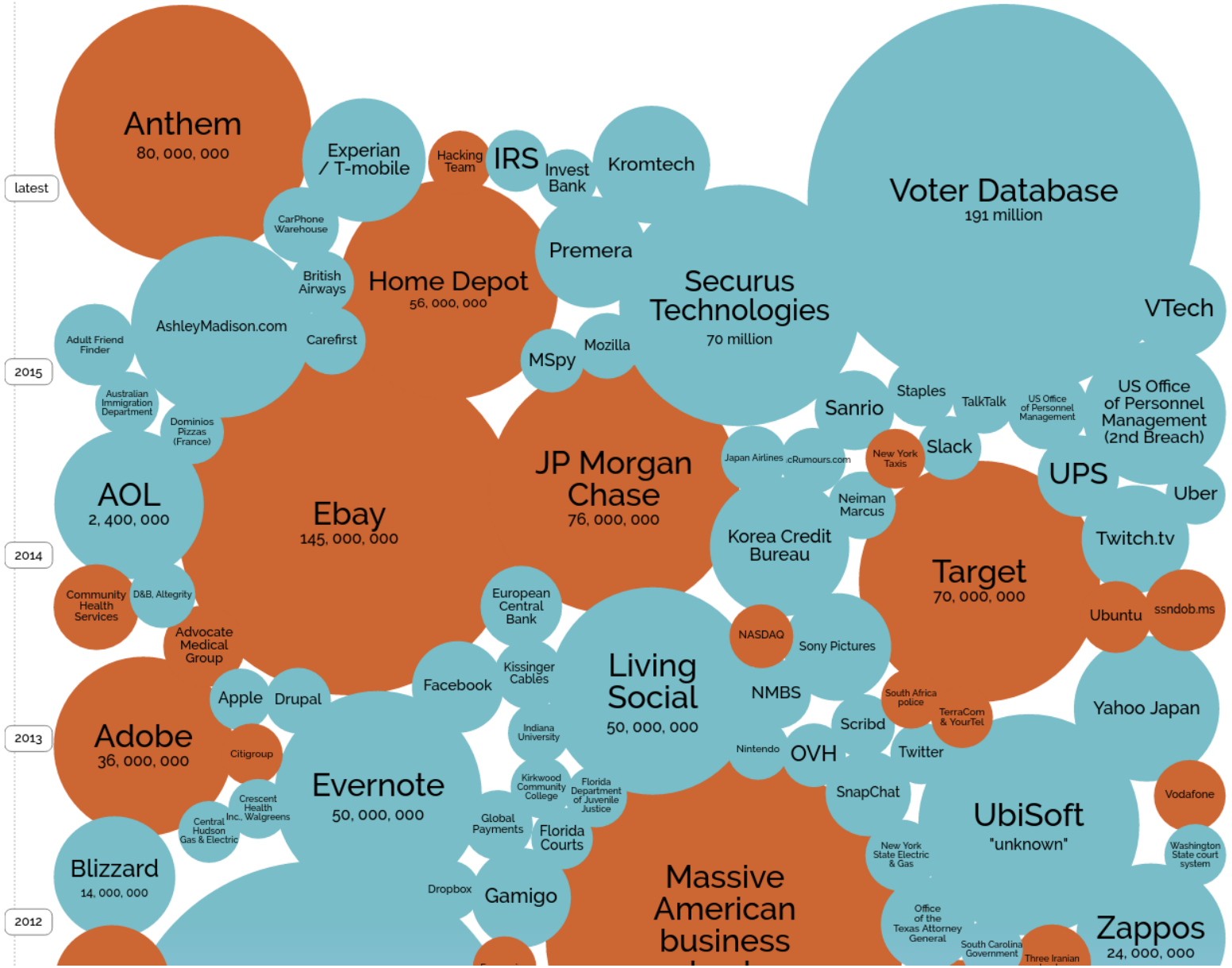
Zero Day Exploits …



Ransomware …



Data Leaks …

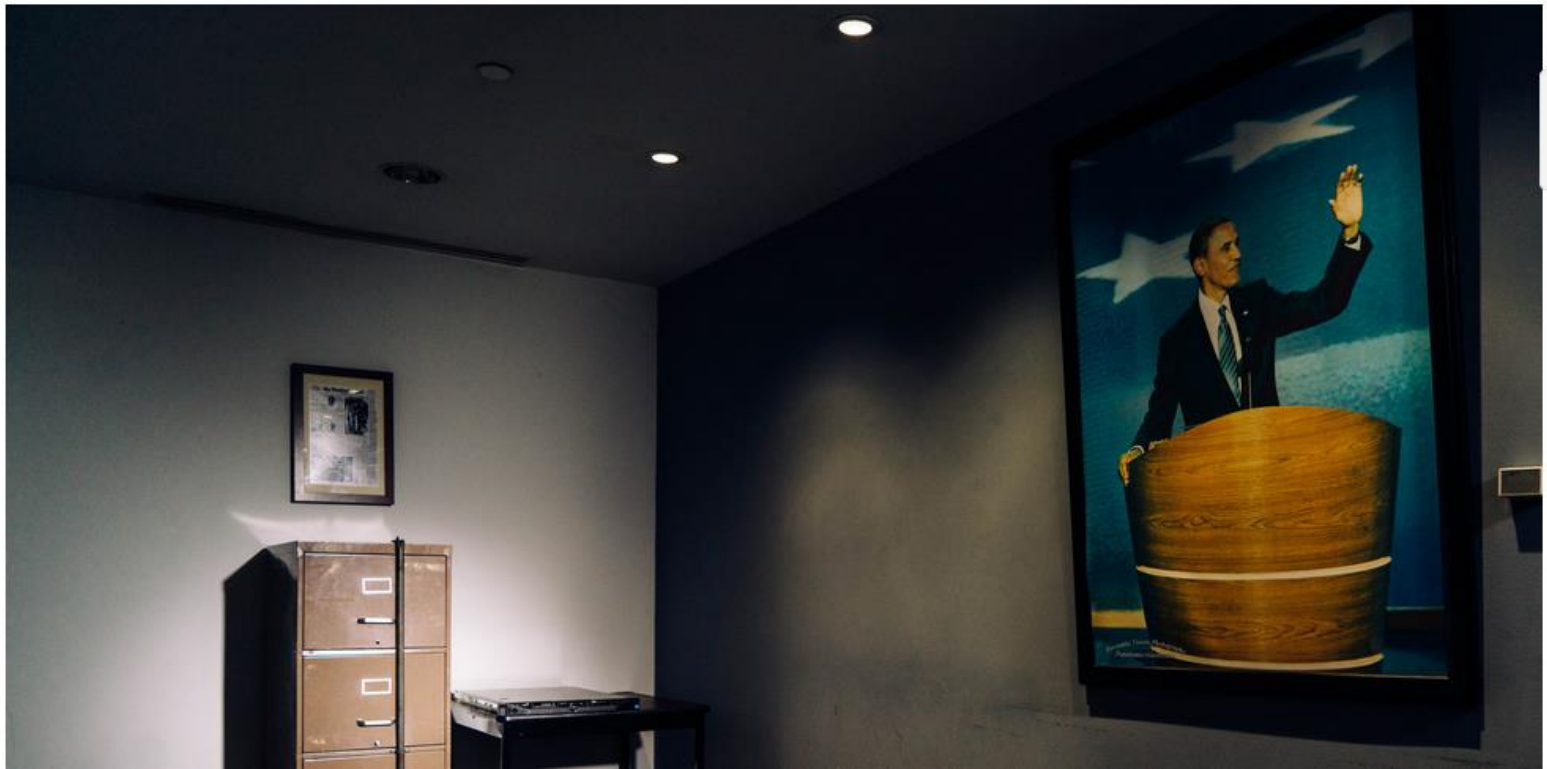

latest
2015
2014
2013
2012
Anthem
80, 000, 000
Experian / T-mobile
Hacking Team
IRS
Invest Bank
Kromtech
CarPhone Warehouse
Premera
Voter Database
191 million
British Airways
Home Depot
56, 000, 000
Securus Technologies
70 million
VTech
AshleyMadison.com
Carefirst
Adult Friend Finder
MSpy
Mozilla
Australian Immigration Department
Dominios Pizzas (France)
Sanrio
Staples
TalkTalk
US Office of Personnel Management
US Office of Personnel Management (2nd Breach)
Japan Airlines
cRumours.com
New York Taxis
Slack
UPS
Uber
AOL
2, 400, 000
Ebay
145, 000, 000
JP Morgan Chase
76, 000, 000
Neiman Marcus
Korea Credit Bureau
Twitch.tv
Target
70, 000, 000
Community Health Services
D&B, Altegrity
Advocate Medical Group
European Central Bank
Ubuntu
ssndob.ms
NASDAQ
Sony Pictures
Facebook
Kissinger Cables
Living Social
50, 000, 000
NMBS
South Africa police
TerraCom & YourTel
Yahoo Japan
Apple
Drupal
Adobe
36, 000, 000
Citigroup
Indiana University
Scribd
Nintendo
OVH
Twitter
Evernote
50, 000, 000
Kirkwood Community College
Florida Department of Juvenile Justice
SnapChat
Vodafone
Crescent Health Inc., Walgreens
Central Hudson Gas & Electric
Global Payments
Florida Courts
UbiSoft
"unknown"
New York State Electric & Gas
Washington State court system
Blizzard
14, 000, 000
Dropbox
Gamigo
Massive American business
Office of the Texas Attorney General
South Carolina Government
Three Iranian
Zappos
24, 000, 000

POLITICS

The Perfect Weapon: How Russian Cyberpower Invaded the U.S.

Читать статью по-русски

By ERIC LIPTON, DAVID E. SANGER and SCOTT SHANE DEC. 13, 2016



Ransomware: See the 14 hospitals attacked so far in 2016 | Healthcare IT News - Mozilla Firefox

www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=1

Healthcare IT News

TOPICS SIGN UP MAIN MENU

Privacy & Security

Ransomware: See the 14 hospitals attacked so far in 2016

By Jessica Davis | October 05, 2016 | 12:13 PM

SHARE Share 25

Ransomware attacks have been steadily increasing in the healthcare industry since the beginning of the year, and with the most recent attacks on New Jersey Spine Center, Marin Healthcare District and Urgent Care Clinic of Oxford, it doesn't look like the target placed on these providers will be shrinking anytime soon. Hospitals are recognizing the threat and are making cybersecurity a top priority. But as cybercriminals gain intelligence - and confidence - it may not be enough to make up for human error, outside vendors and other vulnerabilities.

Read the Analysis: Hollywood Presbyterian hack signals more ransomware attacks to come.

Yahoo says data stolen from 1 billion accounts

by Seth Fiegerman @sfiegerman

December 15, 2016: 4:30 AM ET

Timeline: The rise and fall of Yahoo

Just when you think Yahoo's security issues can't get any worse, the company proves you wrong.

Yahoo (YHOO, Tech30) disclosed a new security breach on Wednesday that may have affected more than one billion accounts. The breach dates back to 2013 and is thought to be separate from a massive cybersecurity incident announced in September.

Yahoo now believes an "unauthorized third party" stole user data from more than one billion accounts in August 2013. That data may have included names, email addresses and passwords, but not financial information.

Social Surge - What's Trending


Yellen: U.S. is near 'maximum employment'


Britain gambles on free trade deal with Europe


JPMorgan Chase accused of paying women less than men