



# **The 2016 Internet Security Threat Report: The Good (not much). The Bad (way more of that). And The Ugly (the attacks continue to outpace healthcare)**

**David S. Finn CISA, CISM, CRISC**

Health IT Officer, Symantec

# Agenda

1

The 2016 Internet Security Threat Report

2

The Healthcare Internet Security Threat Report

3

HHS Healthcare Industry Cybersecurity Task Force update

# One of the most comprehensive sources of Internet threat data in the world

- 63.8 million attack sensors
  - Records thousands of events per second
- Monitors threat activity in over 157 countries/territories
- Coupled with one of the most comprehensive vulnerability data bases
  - 74,180 recorded vulnerabilities (20+ years)
  - Over 23,980 vendors representing 71,470 products
- Over 9 billion emails are processed each month
- Over 1.8 billion web requests filtered each day
- Phishing information collected through an extensive anti-fraud community of enterprises, security vendors and more than 52 million consumers on 175 million endpoints
- Symantec secures more than 1 million web servers

# Highlights from the 21<sup>st</sup> Internet Security Threat Report

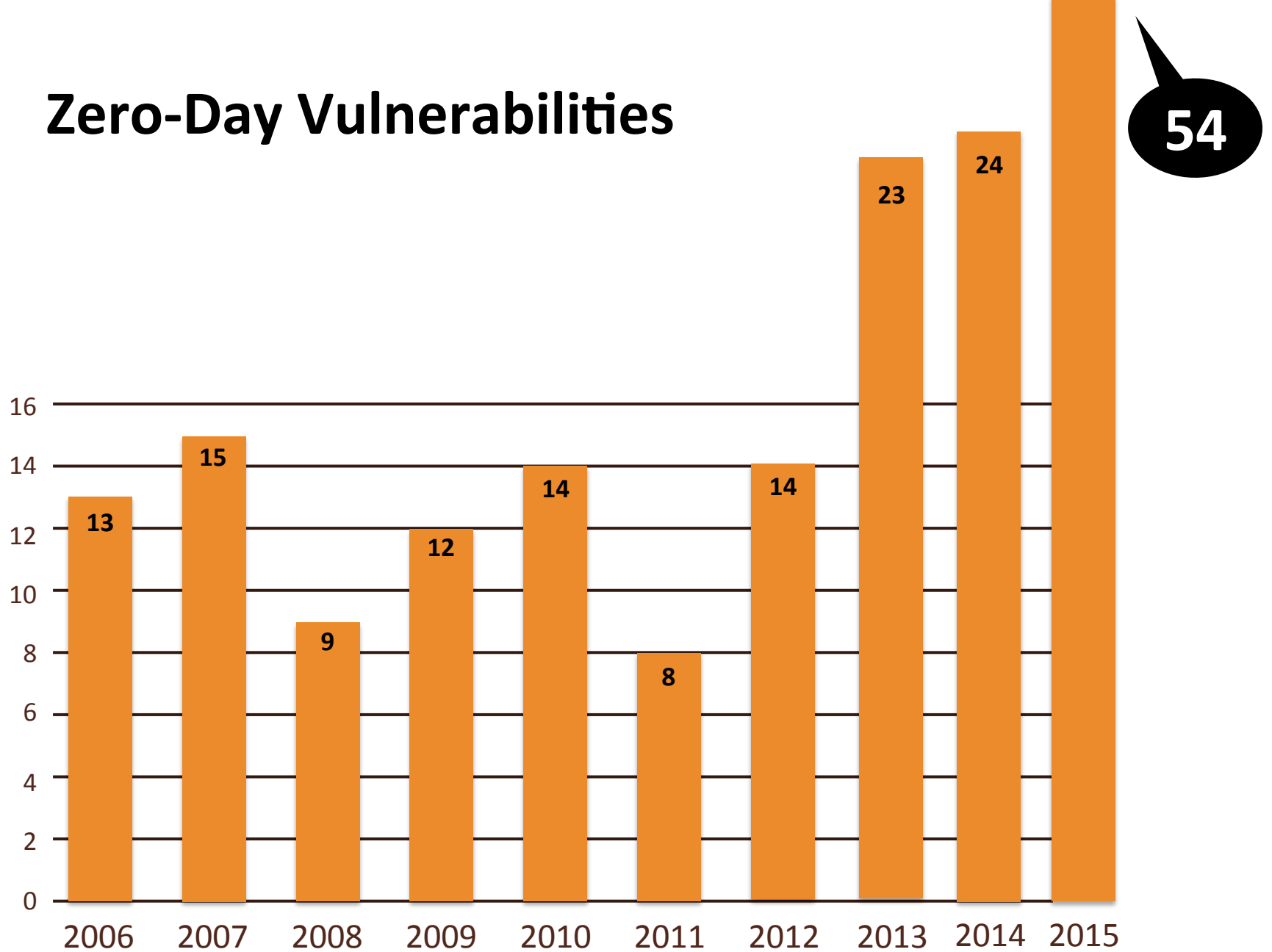
1. On Average, One Zero-day was discovered every week in 2015
2. Over Half a Billion Personal Information Records Lost to Breach
3. Three out of Every Four Websites Put You at Risk
4. Encryption Now Used as a Cyber Weapon to Hold Companies and Individuals' Critical Data Hostage
5. Don't Call Us, We'll Call You: Cyber Scammers Now Make You Call Them to Hand Over Your Cash

In **2009** there were  
**2,361,414**  
**new piece of malware created.**

In **2015** that number was  
**430,555,582**

That's  
**1 Million 179 Thousand**  
**a day.**

# Zero-Day Vulnerabilities

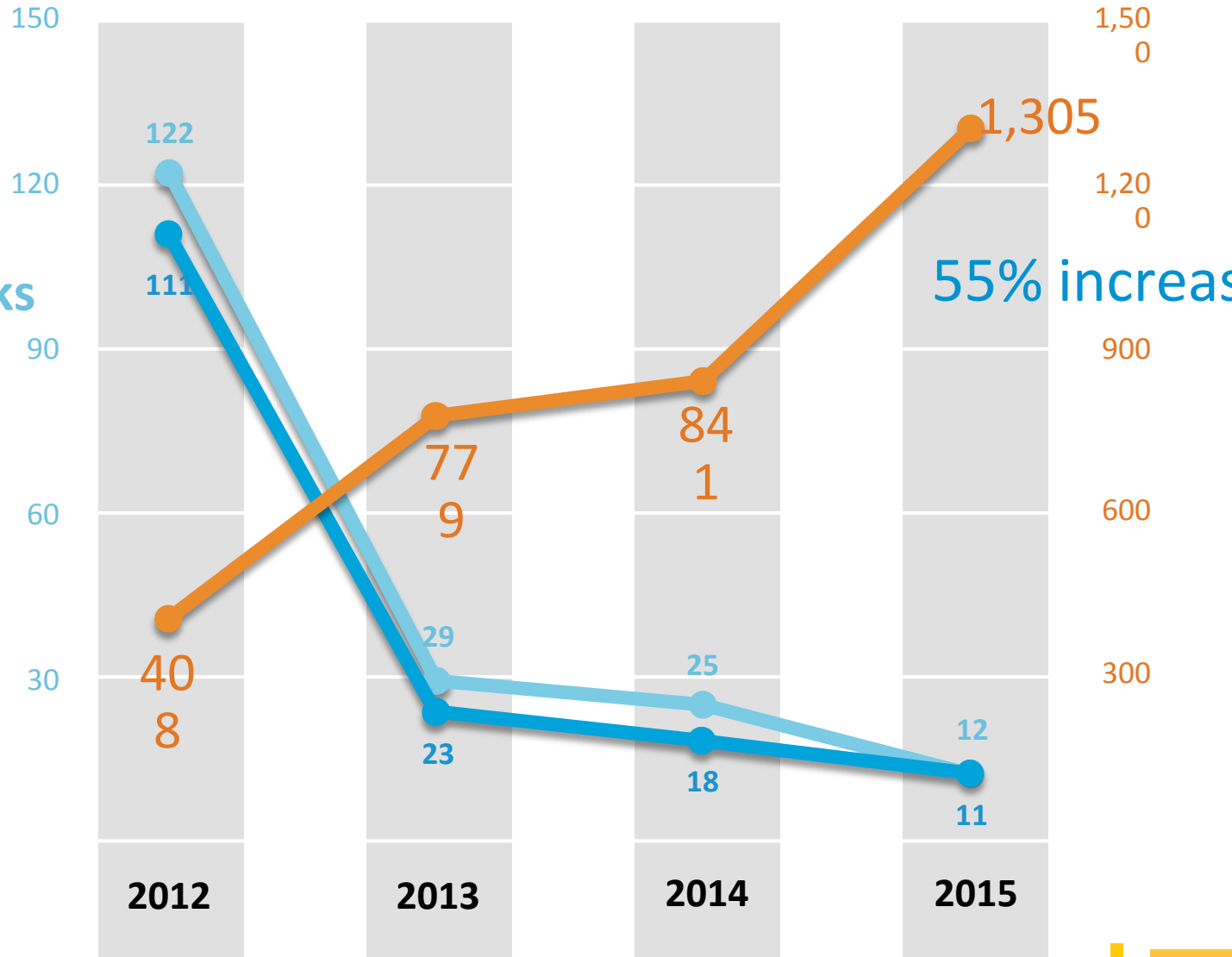


# Targeted Attacks

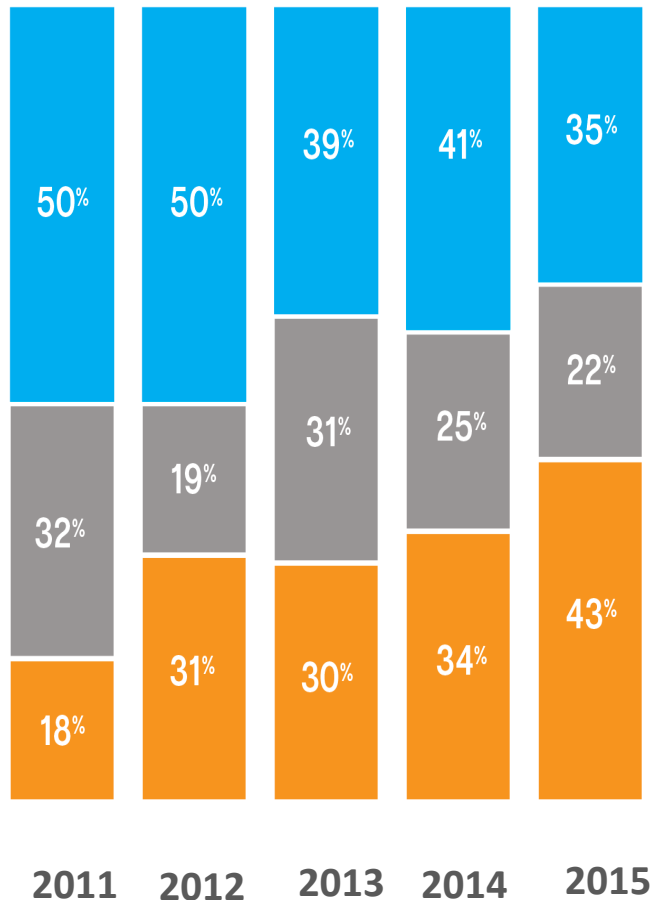
- Average Number of Email Attacks Per Campaign

- Recipients per Campaign

- Campaigns

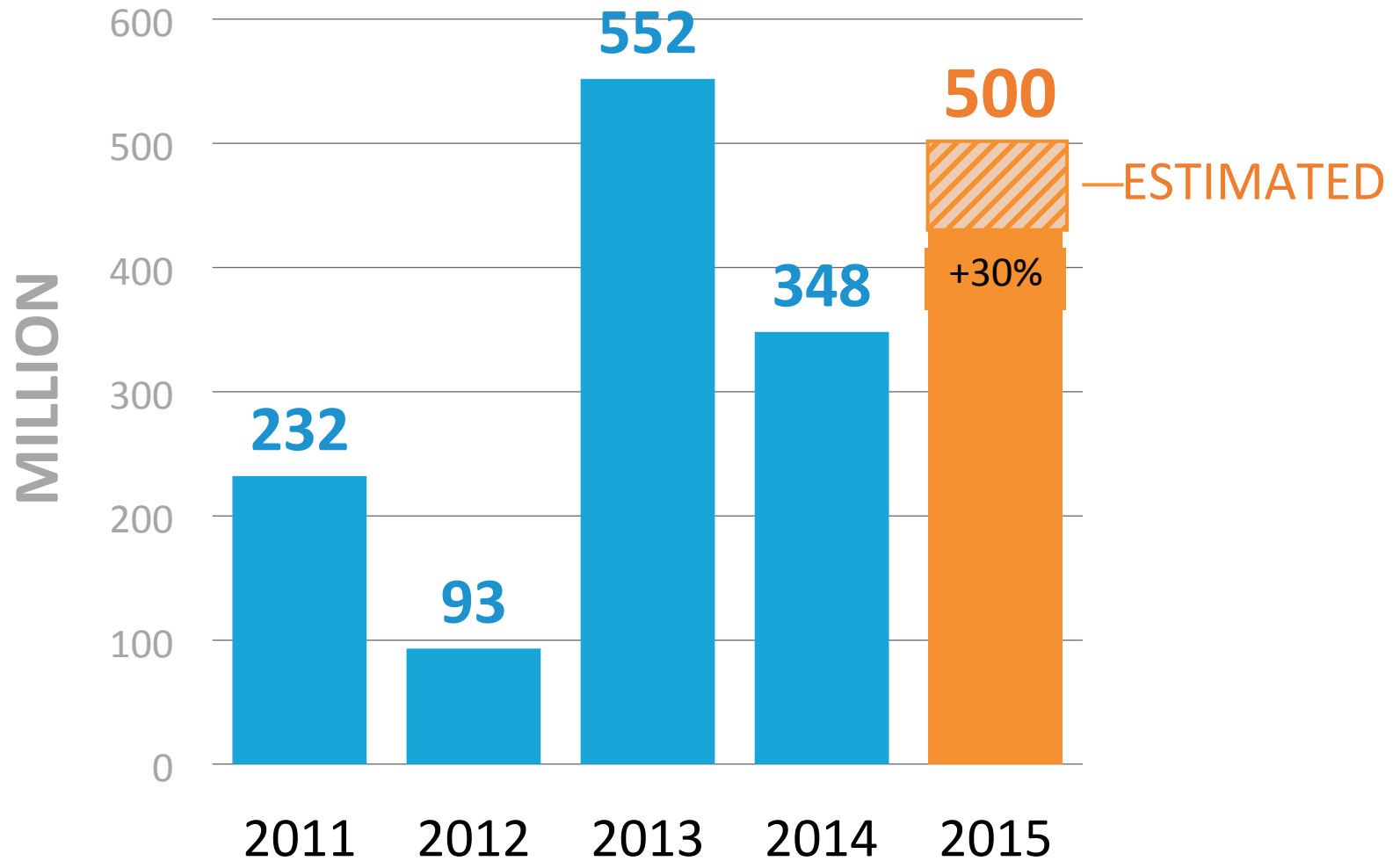


# Spear-Phishing Attacks by Size of Targeted Organization



Org Size	2015 Risk Ratio	2015 Risk Ratio as Percentage	Attacks per Org
Large Enterprises 2,500+ Employees	1 in 2.7	38%	3.6
Medium Business 251-2,500 Employees	1 in 6.8	15%	2.2
Small Business (SMB) 1-250 Employees	1 in 40.5	3%	2.1

# Total Identities Exposed

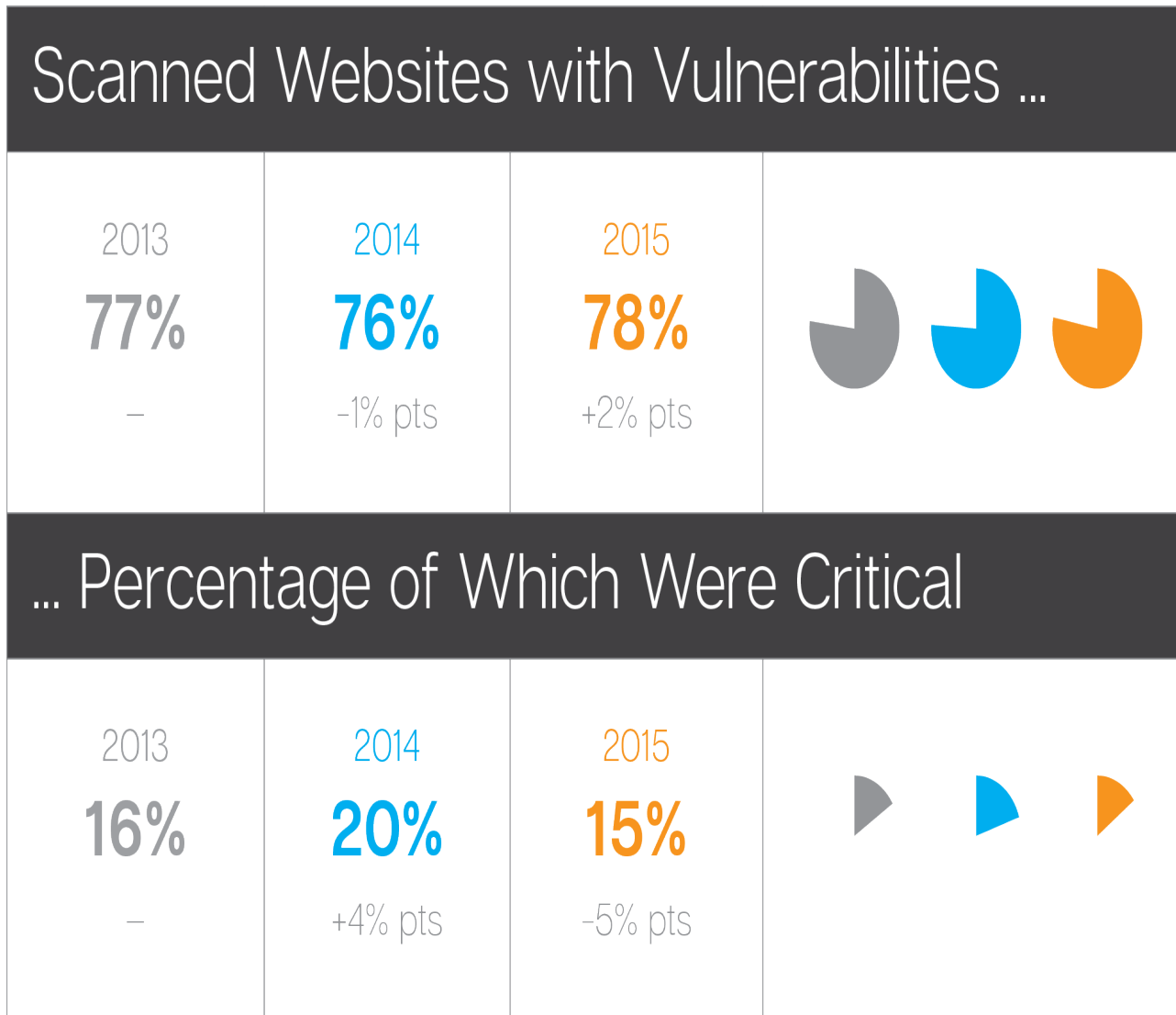




# Mega Breaches 2015



# Vulnerabilities





# Professionalization of Cybercrime

# Hacktool.MultiPurpose

## General options

-----

```
--install: install server on local host and load it
--host <host>: hostname or IP (local host if not set)
--password <password>: server password connection (mandatory)
--forceload: load server on local host without test
```


## Server options

-----

```
--cmd: server command:
  dump: dump stuffz
    --sam: fetch LM/NTLM hashes
    --machines: fetch machines hashes
    --history: fetch history for LM/NTLM hashes
    --sh: fetch logon sessions hashes
    --sp: fetch security packages cleartext passwords
    --accounts: <account list>: with --sam, specify accounts to dump
(comma separated)
    --lsa: fetch LSA secrets
```

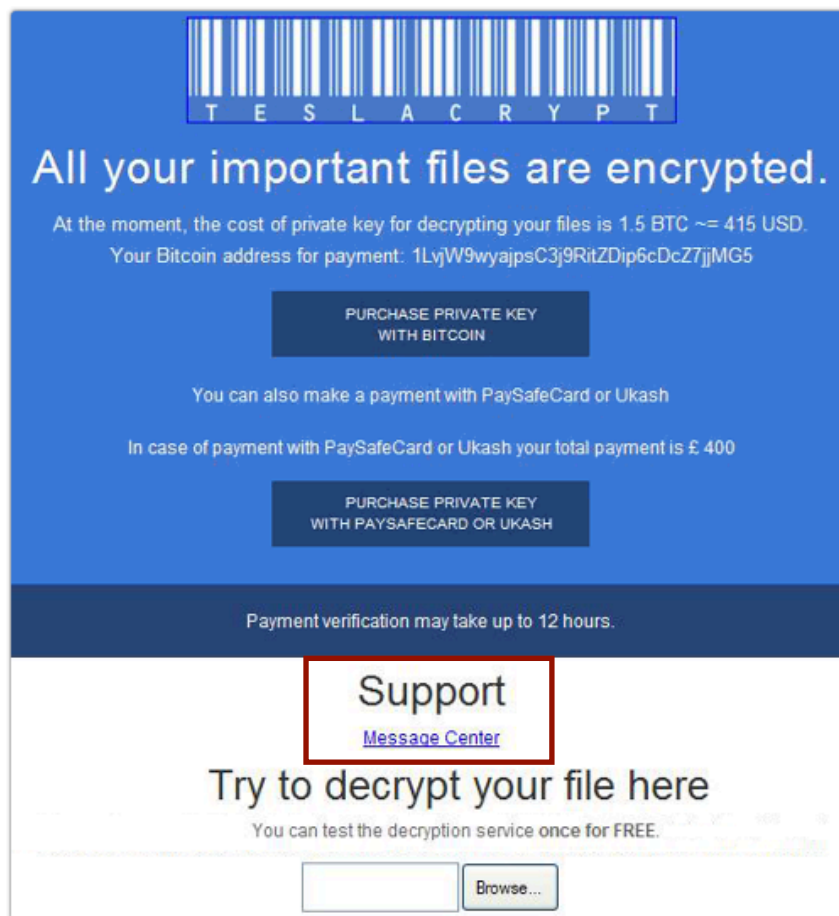


# Tech Support Scams – Outbound Call Centers (Boiler Rooms) to Support the Scam

A black silhouette of a person's head and shoulders in profile, facing left. They are wearing a headset with a microphone. A white speech bubble tail points from the person's mouth to an orange speech bubble on the left. The entire scene is set against a light gray circular background with a subtle orange glow.

Hello sir,  
Your computer is  
infected. Please  
purchase a support  
plan for \$75 so we can  
help you...

# TeslaCrypt Ransomware – Technical Support Available



The screenshot shows a ransomware payment and support interface. At the top, a barcode is displayed above the word "TESLACRYPT" in spaced-out letters. Below this, the text reads "All your important files are encrypted." followed by payment details: "At the moment, the cost of private key for decrypting your files is 1.5 BTC ≈ 415 USD." and "Your Bitcoin address for payment: 1LvW9wyajpsC3j9RitZDip6cDcZ7jjMG5". There are two buttons: "PURCHASE PRIVATE KEY WITH BITCOIN" and "PURCHASE PRIVATE KEY WITH PAYSAFECARD OR UKASH". A note states "In case of payment with PaySafeCard or Ukash your total payment is £ 400". A dark blue bar contains the text "Payment verification may take up to 12 hours." Below this, a "Support" section is highlighted with a red box, containing a "Message Center" link. The main section is titled "Try to decrypt your file here" and includes the text "You can test the decryption service once for FREE." and a "Browse..." button next to an empty input field.

TESLACRYPT

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ≈ 415 USD.  
Your Bitcoin address for payment: 1LvW9wyajpsC3j9RitZDip6cDcZ7jjMG5

PURCHASE PRIVATE KEY  
WITH BITCOIN

You can also make a payment with PaySafeCard or Ukash

In case of payment with PaySafeCard or Ukash your total payment is £ 400

PURCHASE PRIVATE KEY  
WITH PAYSAFECARD OR UKASH

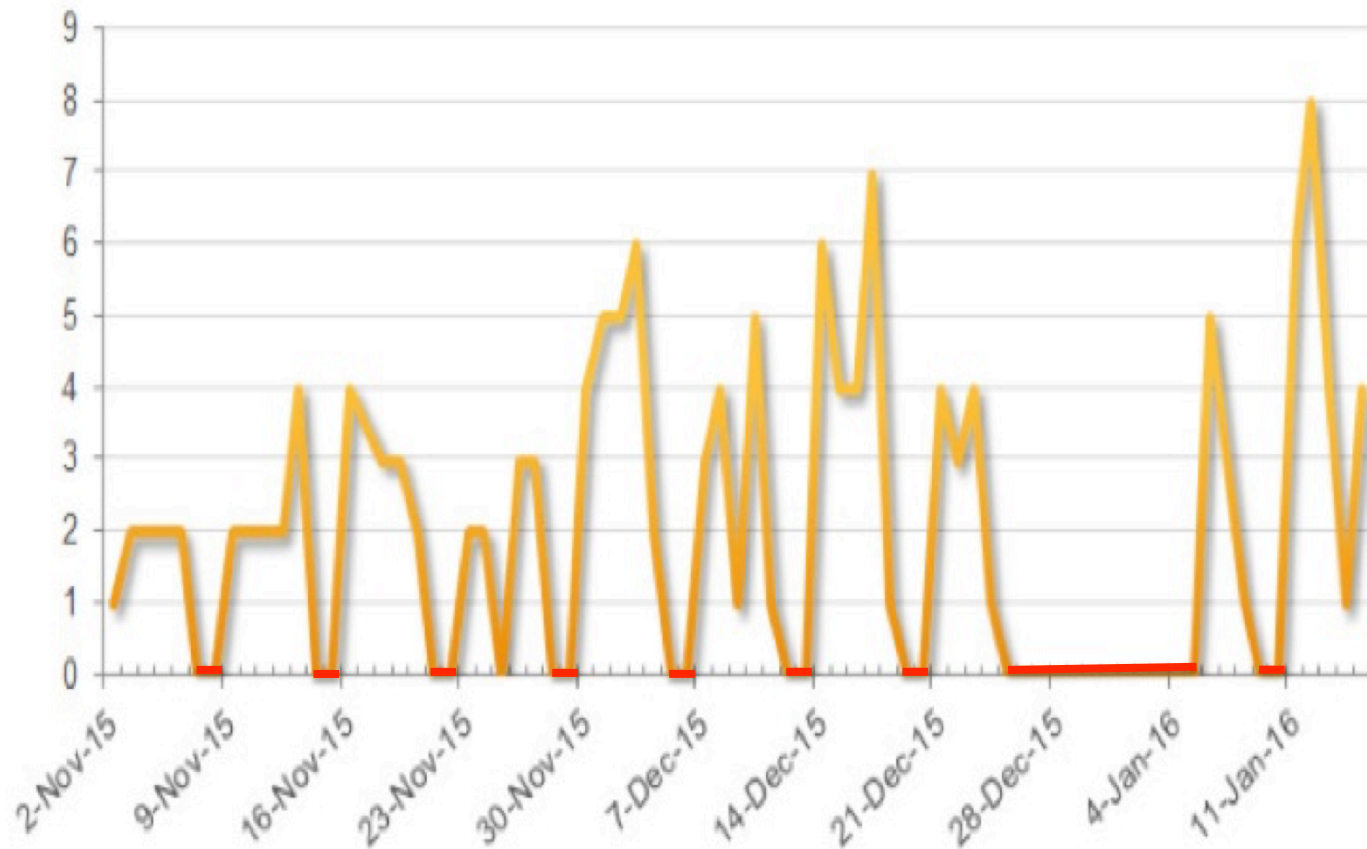
Payment verification may take up to 12 hours.

Support  
[Message Center](#)

Try to decrypt your file here

You can test the decryption service once for FREE.

# Dridex Gang - Number of Known Spam Runs Per Day



# When Cyber Criminals . . .

Work in **Call Centers**, **Write**  
**Documentation**  
and **Take the Weekends Off**

**You Know its a Profession**



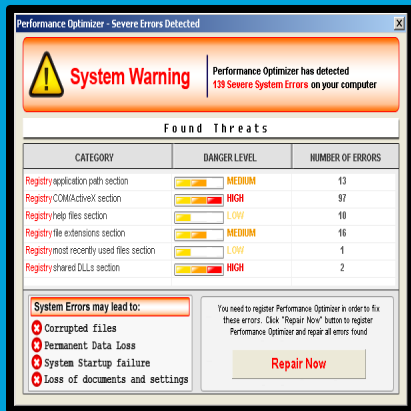


# Ransomware

The biggest news in Healthcare in 2016

# It is not new

## MISLEADING APP



2005-2009

“FIX”

## FAKE AV



2010-2011

“CLEAN”

## LOCKER RANSOMWARE



2012-2013

“FINE”

## CRYPTO RANSOMWARE



2014-2015

“FEE”

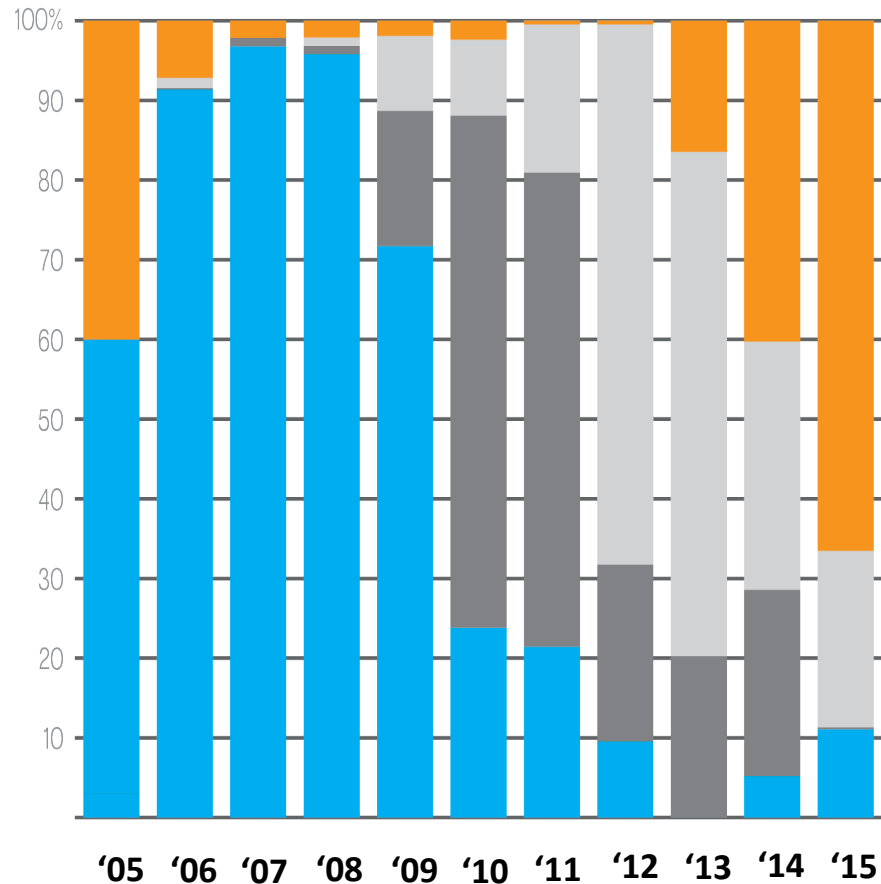
# Growing Dominance of Crypto-Ransomware

MISLEADING APP

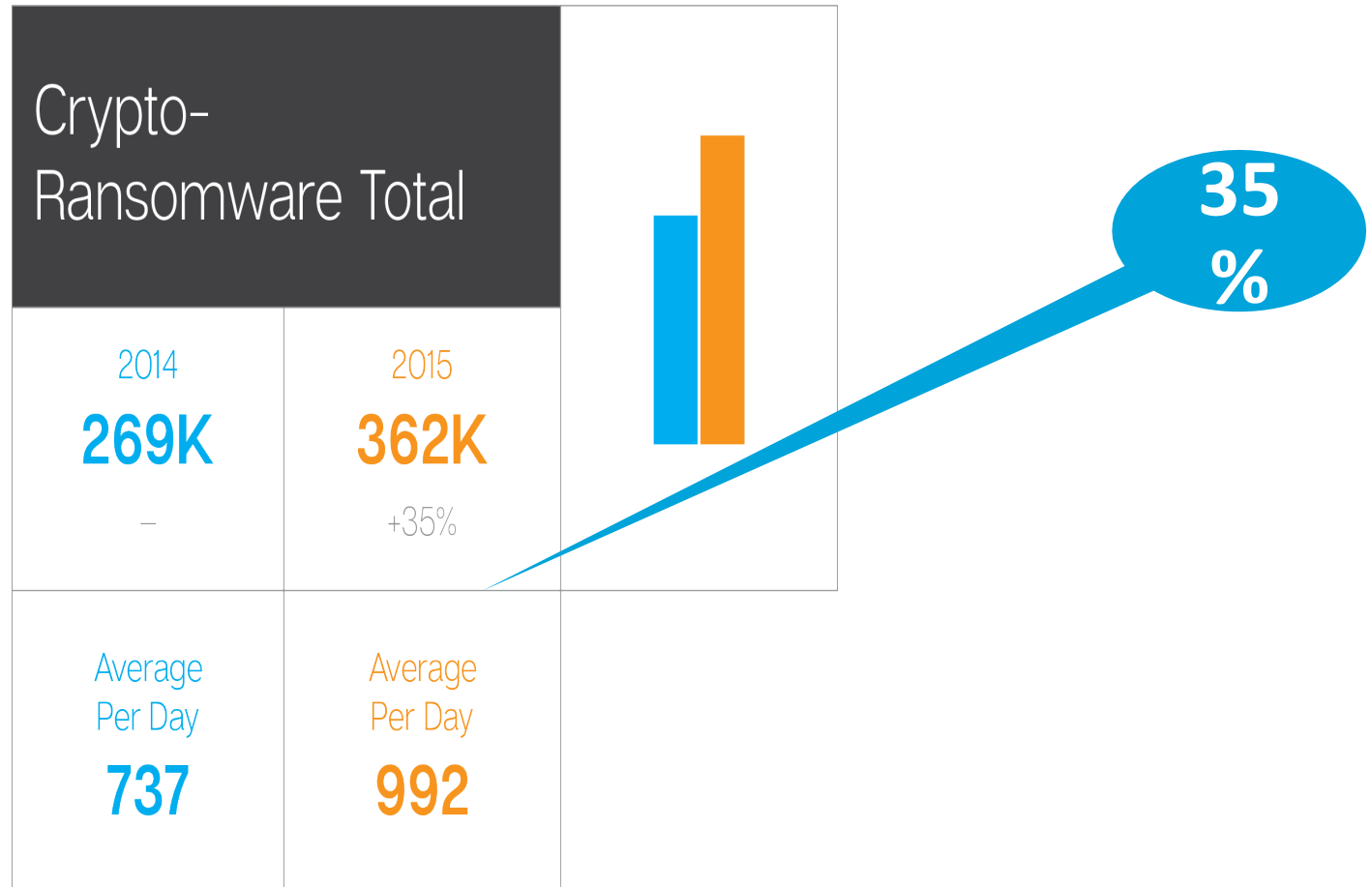
FAKE AV

LOCKER  
RANSOMWARE

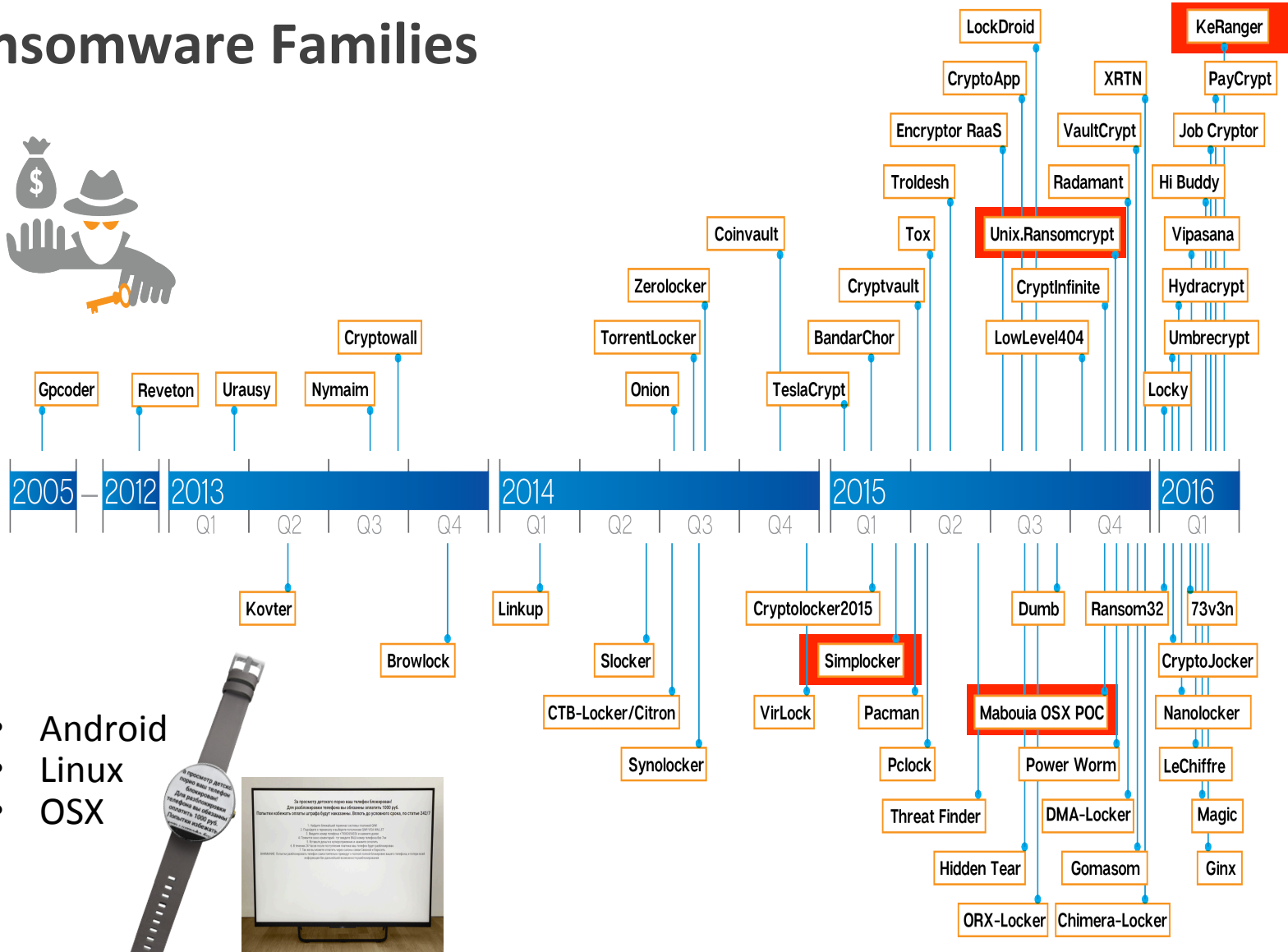
CRYPTO  
RANSOMWARE



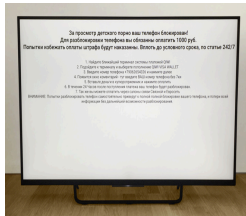
# 35% Increase in Crypto-Ransomware Attacks



# Ransomware Families



- Android
- Linux
- OSX



# Healthcare Cybersecurity - - Not Business as Usual Anymore



# Healthcare Issues



- **Compliance versus Security**
- **Phishing Attacks and Ransomware**
- **Medical Device Security Risks**
- **Resource Challenges**

## Sectors Breached by Number of Incidents

*Healthcare is denoted as a sub-sector within the Services industry, and 120 of the 200 breaches that occurred within the Services sector were attributed to Healthcare.*

Sector/ Sub-Sector	Number of Incidents	% of Incidents	Identities Exposed	% of IDs Exposed
Services	200 (1)	65.6%	259,893,565 (1)	60.6%
Health Services	120 (1)	39.3%	4,154,226 (10)	1.0%



# Healthcare v. Overall

Percentage of Spam in Email by Industry Group	
Health Services	54.1

Phishing Ratio in Email by Industry Group	Phish:Email Ratio
Healthcare/Health Svcs	1 in 2,711

Virus Ratio in Email by Industry Group	Ratio of Malware:Email
Healthcare/Health Svcs.	1 in 396

Overall Email Spam Ratio		
2013	2014	2015
66%	60%	53%
	-6 pts.	-7 pts.

Email Phishing Rate Rate (Overall)		
2013	2014	2015
1 in 392	1 in 965	1 in 1,846

Email Malware Rate (Overall)		
2013	2014	2015
1 in 196	1 in 244	1 in 220



# HHS Healthcare Industry Cybersecurity Task Force

# Purpose

Charged under Title IV, Section 405 of Cybersecurity Information Sharing Act of 2015 (CISA)

- How industries other than the healthcare industry have implemented strategies/ safeguards for addressing cybersecurity threats in their respective industries
- Challenges & Barriers private entities in the healthcare industry faces securing themselves against cyber attacks
- Challenges that HIPAA Covered Entities and Business Associates face in securing networked medical devices and other software or systems that connect to an Electronic Health Record



# Make-up

- 21 members
  - Providers, Payers
  - Data Journalist, Consumer Advocate
  - Security companies
  - EHR-support, Med Device makers
  - Pharma, Labs
  - UL
  - HHS, DHS, NIST, DoD
- Ability to reach back to partners in the broader Healthcare/Public Health Sector
- Developers/Vendors called out specifically in the CISA legislation



# Schedule

Schedule					
5					
2					
3					
4					
2					

✓ Check Schedule

- Eight 2-hour calls
- Four face-to-face meetings
  - April, July, September, December
- ~5 hours month in addition to meetings (Ha!)
- A report to Congress describing the state of cybersecurity within the Healthcare and Public Health (HPH) Sector
- Materials to assist healthcare industry partners in implementing the NIST Cybersecurity Framework



Internet Security Threat Report:

<http://www.symantec.com/security-center/threat-report>

**Q&A**

Healthcare Internet Security Threat Report:

<https://www.symantec.com/solutions/healthcare>



# Thank you!

David S. Finn, CISA, CISM, CRISC

[David\\_Finn@symantec.com](mailto:David_Finn@symantec.com)



@DavidSFinn



832.816.2206

**Copyright © 2015 Symantec Corporation. All rights reserved.** Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.