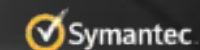


Ransomware Threat Environment in the Context of Digital Identity

Adam Madlin CISSP – Strategist: Public Sector Identity Management

Symantec



Copyright 2016, Symantec Corporation

2016 Internet Security Threat Report

- Symantec's Global Intelligence Network is made up of more than **63.8 million attack sensors** and records **thousands of events per second**. The network monitors threat activity in more than **157 countries and territories**
- Symantec's vulnerability database includes more than **74,180 recorded vulnerabilities** from more than **23,980 vendors**

Ransomware Evolution

Evolution path

MISLEADING APP



2005-2009

“FIX”

FAKE AV



2010-2011

“CLEAN”

LOCKER RANSOMWARE



2012-2013

“FINE”

CRYPTO RANSOMWARE



2014-2015

“FEE”

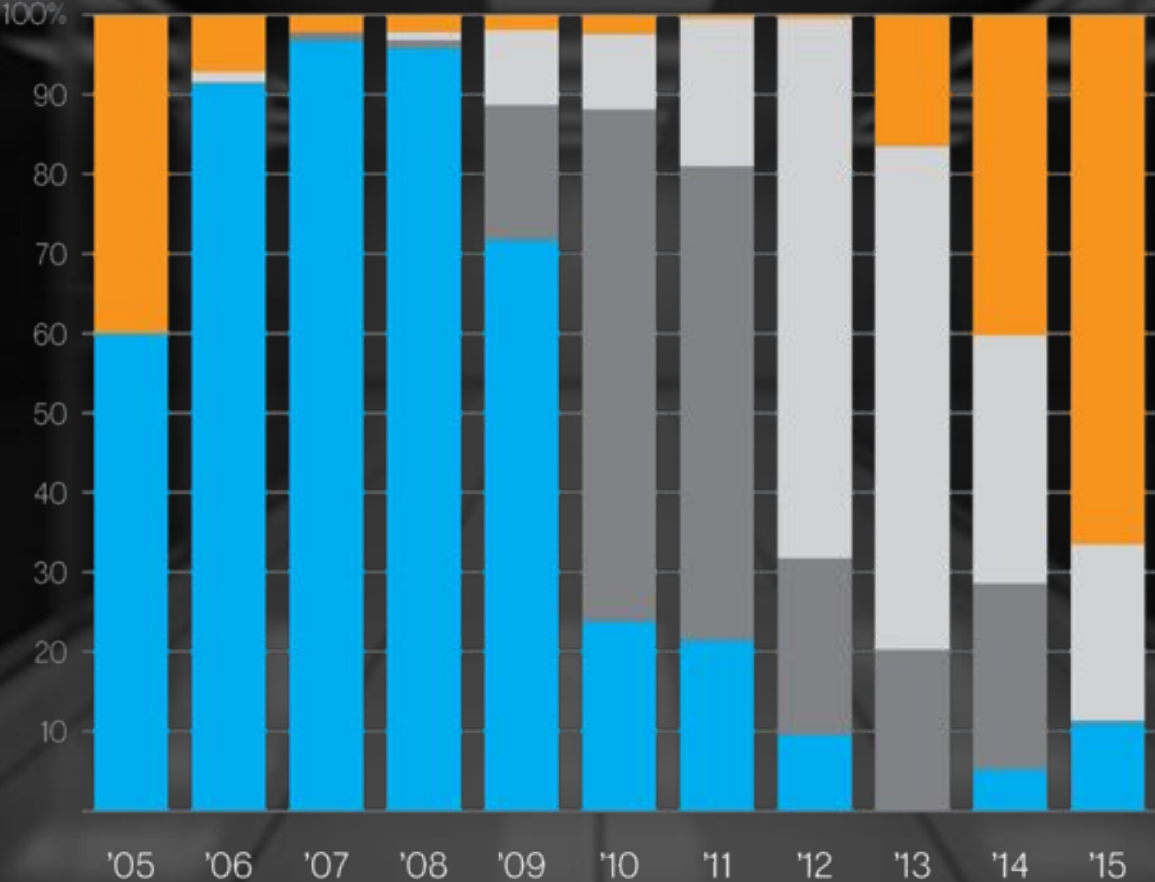
Growing Dominance of Crypto-Ransomware

MISLEADING APP

FAKE AV

LOCKER RANSOMWARE

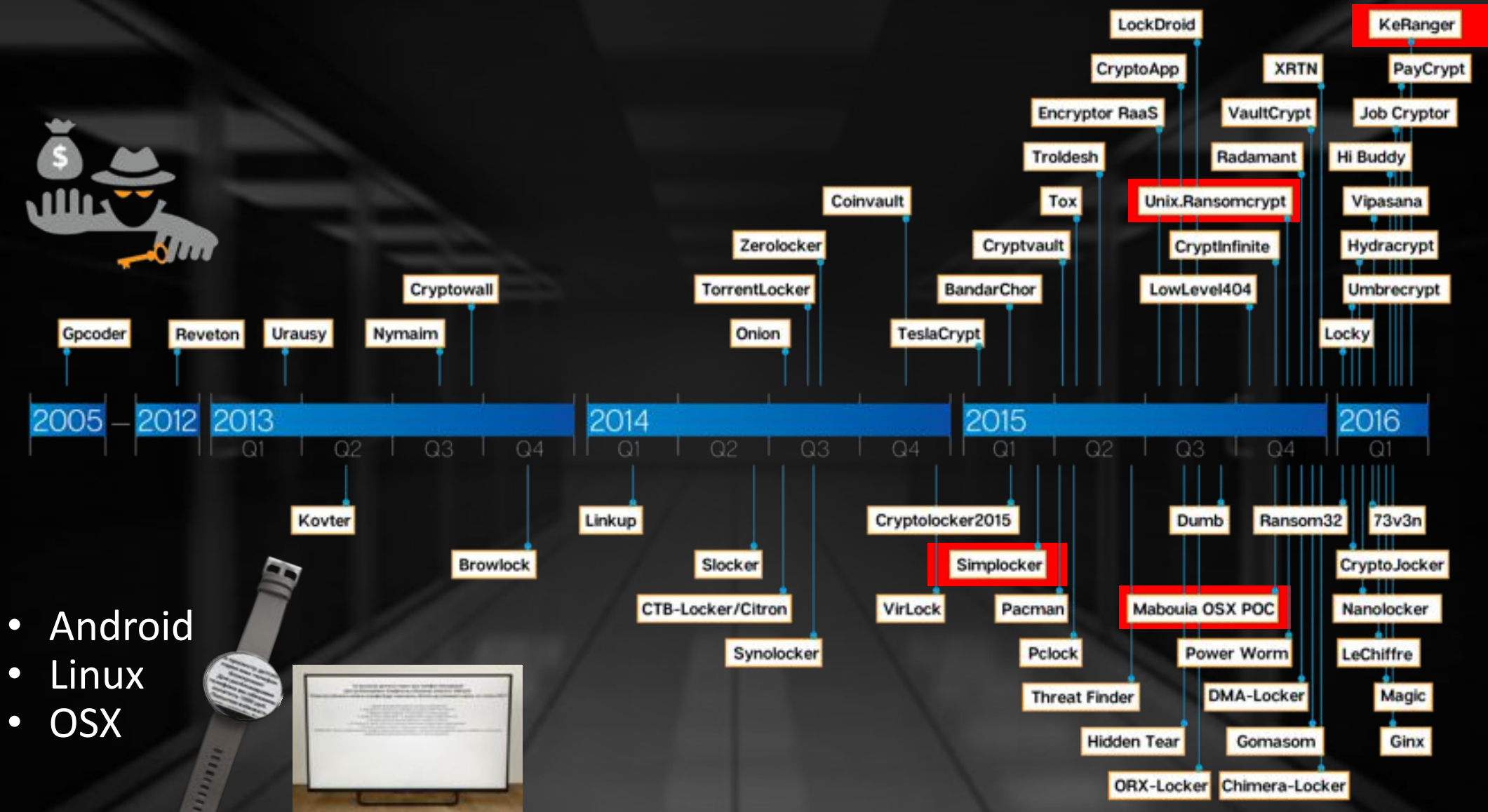
CRYPTO RANSOMWARE



35% Increase in **Crypto-Ransomware** Attacks



Ransomware Families



- Android
- Linux
- OSX



What's new?

Use of **scripting languages** to evade detection

A number of new strains using languages such as JavaScript, PHP, PowerShell and Python

Add-on features

CryptXXX steals Bitcoin wallet data. Cerber adds machines to botnet to carry out DDoS attacks.

New threats added to ransom note

In addition to encryption, Chimera threatens to post personal data online

Ransomware Key Findings

Ransomware and Business 2016

Key findings

- Record year for new ransomware
100 new families identified in 2015. In 2014 that number was 77.
- Ransoms are increasing. Average ransom demand is now \$679
- Businesses are firmly in the sights of attackers
Employees in organizations represent 43% of infections
There are ransomware families designed to infect organizations
Organizations are being targeted by ransomware attackers
- Targeted ransomware attacks use advanced attack techniques

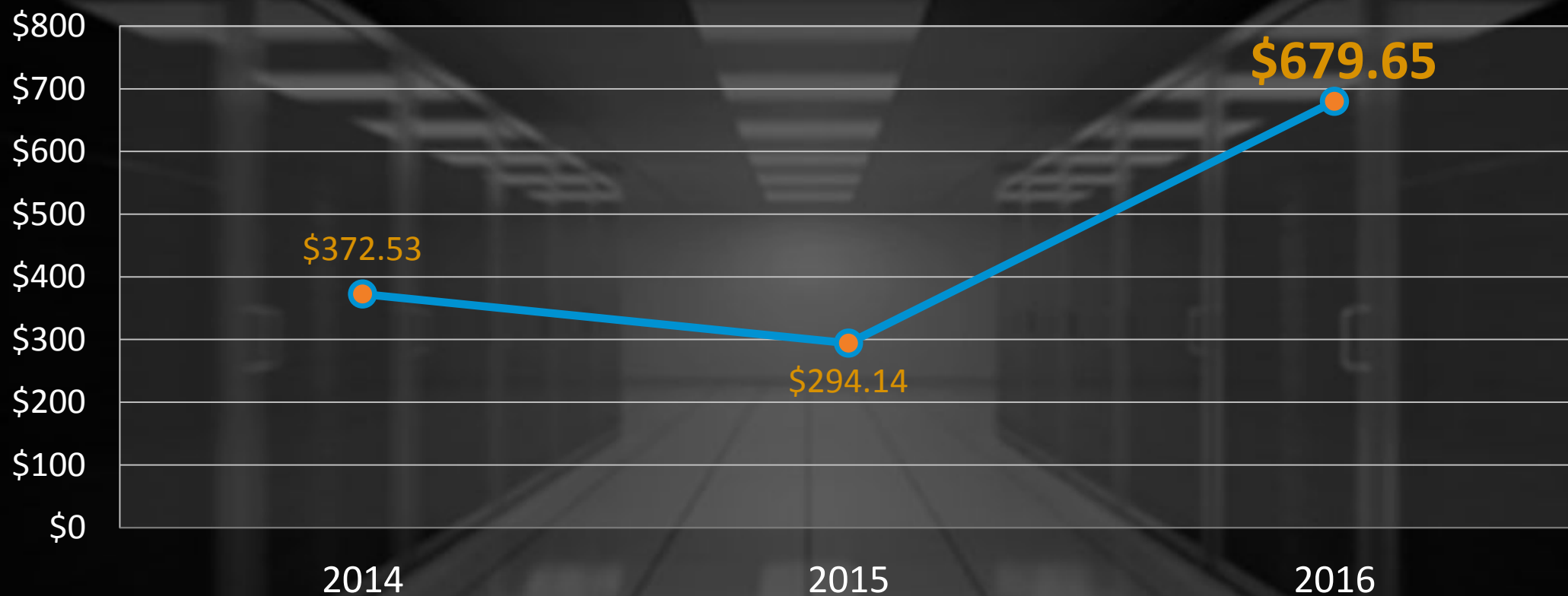
Growth factors



- Easy access to encryption
- Effective infection vectors
- Adoption of advanced attack techniques
- Ransomware as a service

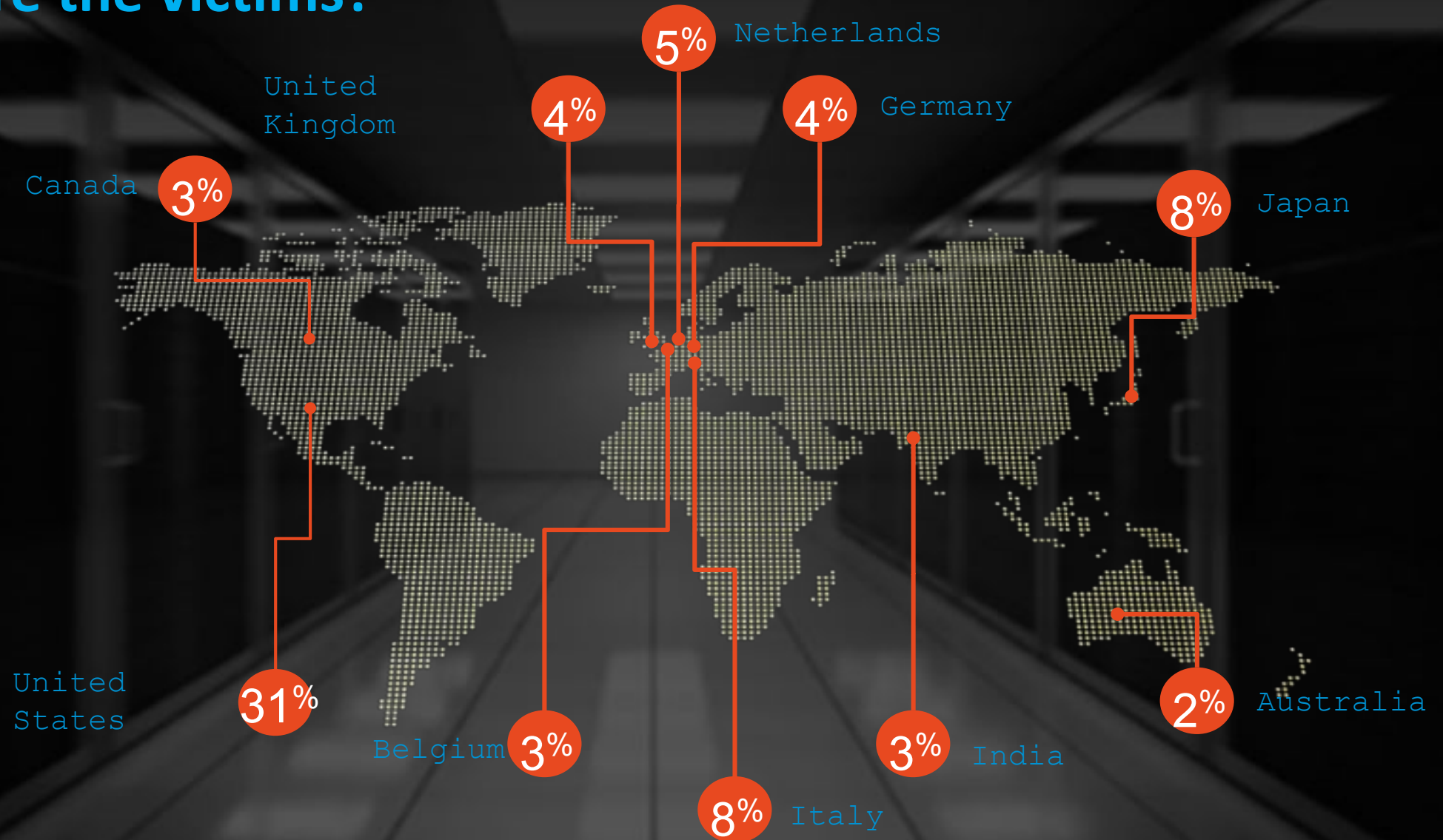
100 new families identified in 2015 compared to 77 in 2014

Ransom demands



Average ransom demand has **more than doubled**

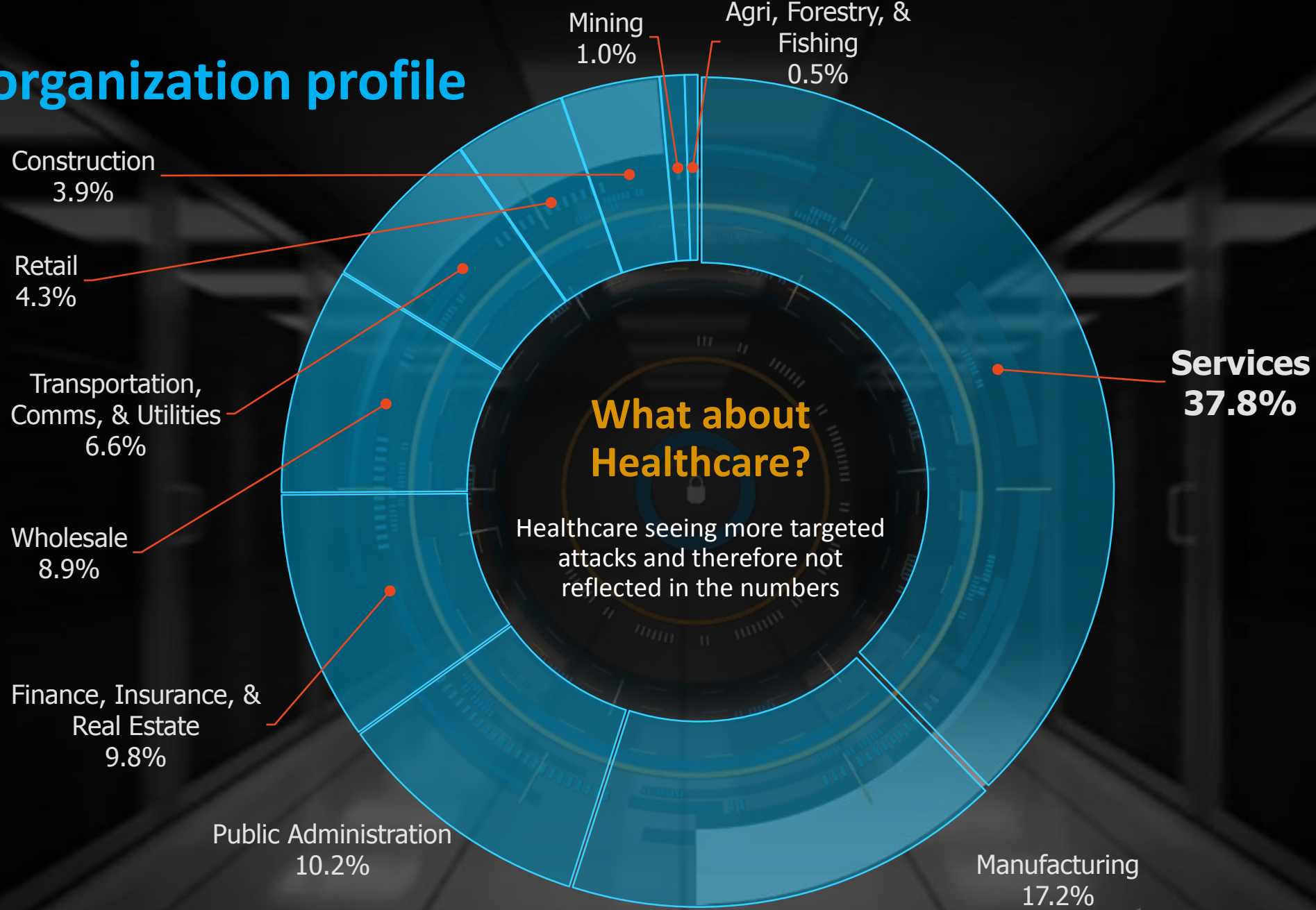
Where are the victims?



Businesses as a target

- Cybercrime is **not just an end-user problem**
 - BEC, financial and data theft and ransomware are all impacting organizations
- **43% of ransomware** infections occur inside organizations
- Corporate-specific features
 - SamSam ransomware exploits **server vulnerabilities** to spread
- Organizations are being **targeted** in advanced attacks

Victim organization profile




Ransomware in Canada

- Canadian organizations are more likely (75%) to pay ransom as compared to US, UK, Germany
- More than 24% of Canadian companies suffered a ransomware attack in past year
- Canada ranked highest for ransomware penetration, those moving beyond the initial compromised endpoint
- Cost is much higher in Canada than US, 65% averaging more than \$1,000
- Canadians have a false sense of security. 51% confident in ability to stop ransomware



TeslaCrypt Ransomware – Technical Support Available



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: 1LvjW9wyaipsC3j9RtZDip6cDcZ7jjMG5

**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.

How are they getting in?



Email

- Distributed through large spam runs
- Masquerades as invoice, unpaid bill or delivery notice
- Attached directly to email
- Attachment launches downloader which installs ransomware
- Link to exploit kit



Exploit Kits

- Hosted on compromised websites and exploit vulns in popular software
- Links sent through email, social media or malvertisements
- Angler was most popular kit in 2015 but is now believed to be offline



Other Vectors

- Malvertisements
- Other malware
- Brute-force attacks
- Server-side vulnerabilities
- Worm techniques
- SMS messages and app stores (Android)

What about Identity

- The next big ransomware threat vector
- We believe that identity is a growing attack vector
 - Stolen credentials
 - Ineffective passwords
 - Lack of two factor authentication
- Why?
 - Ransomware is more profitable
 - Direct threat opportunity – don't need to exfiltrate identities and re-sell them
 - Can move around the network and attack servers
 - Privileged user accounts are suspect and need to be protected

Password attacks are piling pp

Ad hacked, 3 million
acc

The r
card r
custo

OPM: Total of 22.1M people

Total records
breached
since 2005

930m

Median avg. no.
of records across
all data breaches

2,300

Year since '05 with
most breaches
over 50k records

2006

Sector with most
records breached
since 2005

Financial

Data source: Privacy Rights Clearinghouse

By Jose P.

employees and contractors.

Web Security Tool Is Flawed, Researchers Say

JANNY YADRON

Updated April 8, 2014 7:29 p.m. ET

October 6th, 2014

Summary

- Ransomware has evolved from an “annoyance” into a serious threat

The number of Ransomware families continue to grow in number and sophistication

As a result the Ransom Demand has also grown

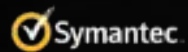
- No one is immune, but Businesses are firmly in the sights of attackers
- Attackers use “persistent” techniques across several Threat Vectors
- To reduce your Risk to Ransomware attacks you need to:
 - Reduce the Attack Surface, Prevent Known Threats & ID and Block Unknown Threats
- Information Sharing amongst trusted peers is essential to quickly address emerging threats

ISACs

DHS Automated Information Sharing Program

Private Sector Cyber Threat Alliance

Thank you!



Adam Madlin
adam_madlin@Symantec.com

Copyright © 2016 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.



Ransomware Infographic

<https://goo.gl/w1F8QY>

