Cyber Security 2015 – Welcome

TeleTrusT/GABA Symantec – Security Solutions Showcase April 20th 2015

Office of the CTO

Thomas Hemker, CISSP, CISM – Security Strategist

Symantec and TeleTrusT

- Worldwide Engineering
  - E.g. Germany: Hamburg and Frankfurt
  - Symantec Access Management Gateway
  - Encryption Core Functions
- TeleTrusT Membership
  - Partner for German IT Security Industry
  - OEM and Affiliate Program
- Threat Intelligence
  - Worldwide coverage
  - Reports and Data provided to partners and customers

Symantec Security Intelligence

Global Data Collection

Signals

Attack Quarantine System

Malware Protection

Gateways

Phishing Detections

Global Sensor Network

3rd Party Affiliates

Human

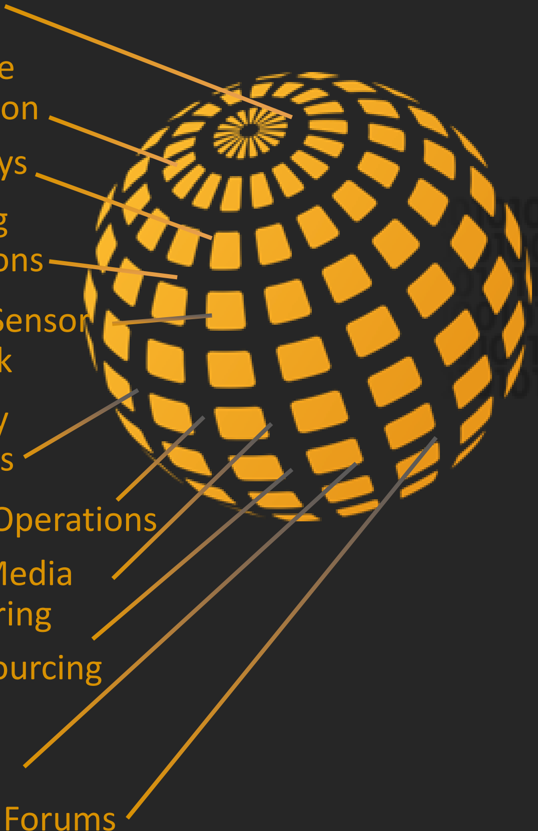
Online Operations

Social Media Monitoring

Open Sourcing Mining

Liaisons

Sharing Forums



Big Data Analysis

Data Fusion Warehouse

Analytics

Intelligence Analysts

DeepSight

Portal

1001010110100101010
↓ ↓ ↓ ↓ ↓
1001010110100101010

DataFeeds

Directed Research

Global Intelligence Network

Symantec

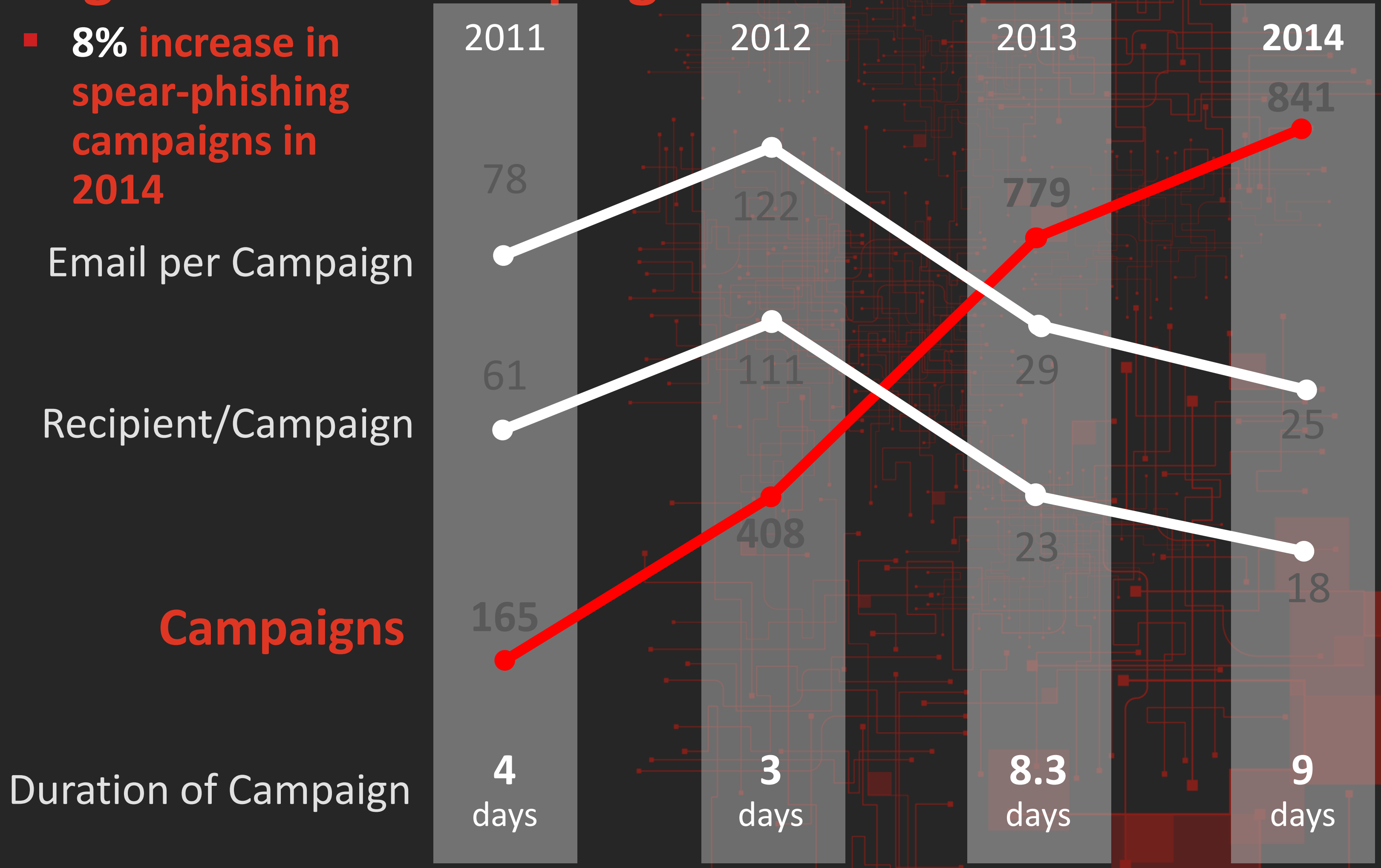
ISTR20

INTERNET SECURITY THREAT REPORT

Attackers are moving faster, defenses are not

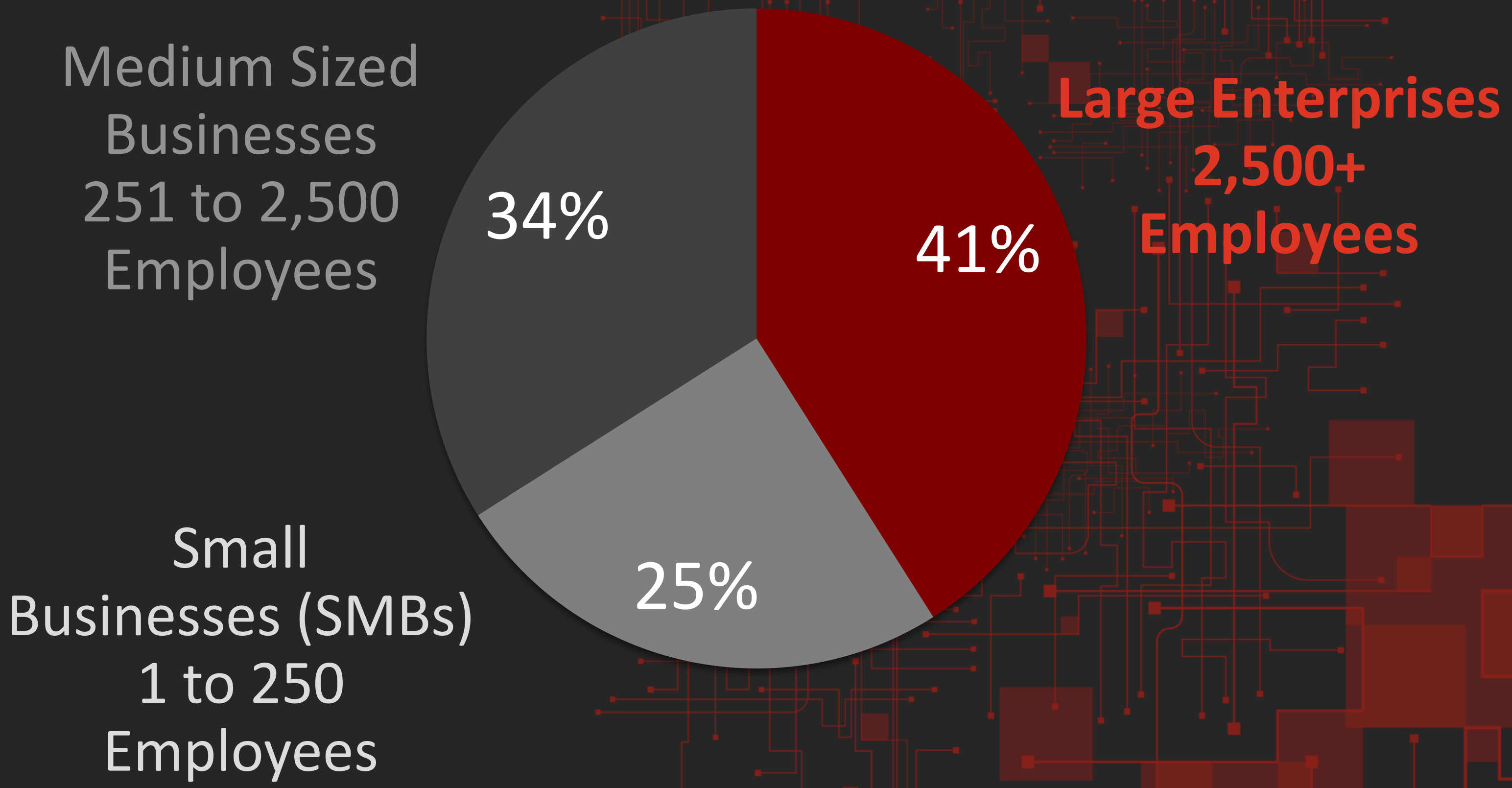
Targeted Attack Campaigns

- **8%** increase in spear-phishing campaigns in 2014

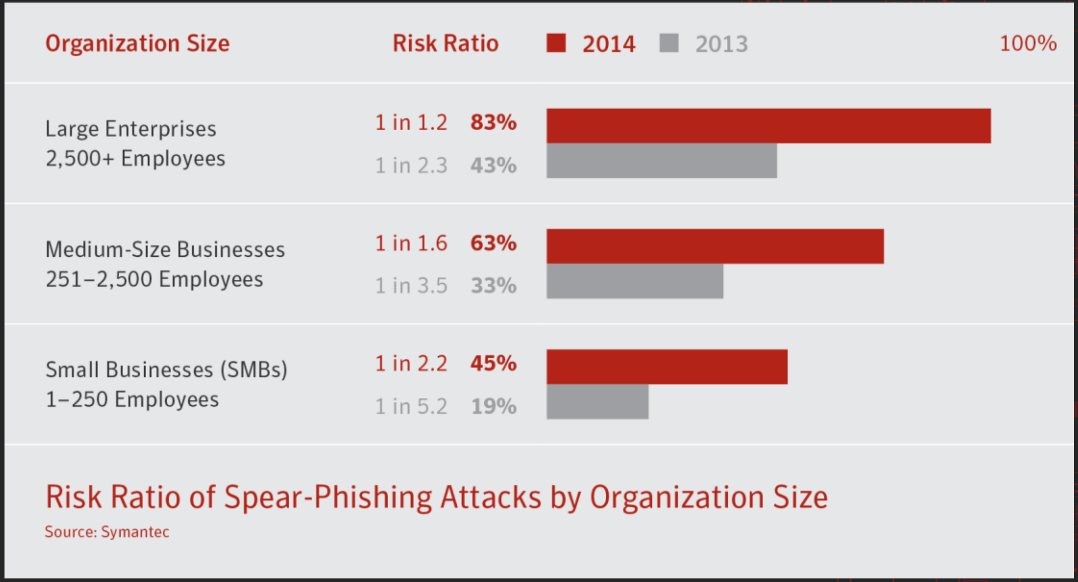


Distribution of Spear-Phishing Attacks by Org Size

2014



Risk Ratio of Spear-Phishing Attacks by Org Size



Organization Size	Risk Ratio	
Large Enterprises 2,500+ Employees	1 in 1.2 1 in 2.3	83% 43%
Medium-Size Businesses 251–2,500 Employees	1 in 1.6 1 in 3.5	63% 33%
Small Businesses (SMBs) 1–250 Employees	1 in 2.2 1 in 5.2	45% 19%

Risk Ratio of Spear-Phishing Attacks by Organization Size

Source: Symantec

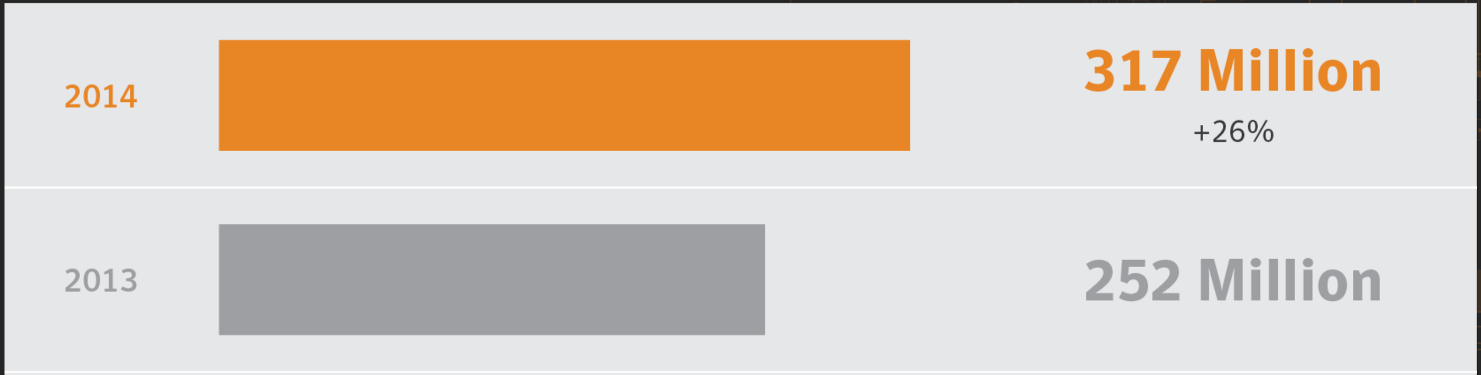
40% pt increase

30% pt increase

26% pt increase

- 5 out of 6 Large Businesses Targeted (83%)

New Malware Variants

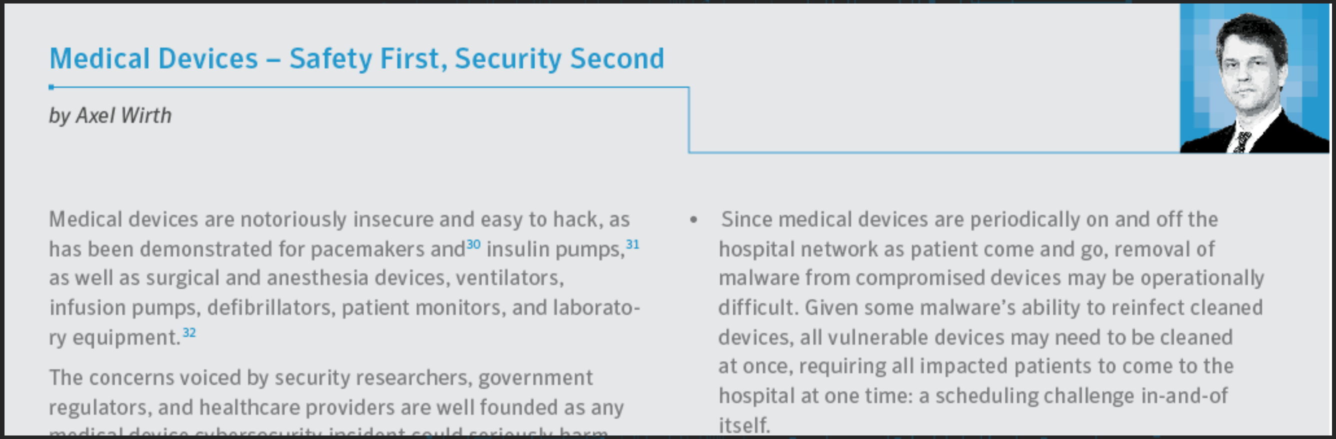


New Malware Variants (Added in Each Year)

Source: Symantec

- Almost 1 million new threats created each day in 2014

The 2015 ISTR contains essays on security risks to Cars and Medical Devices



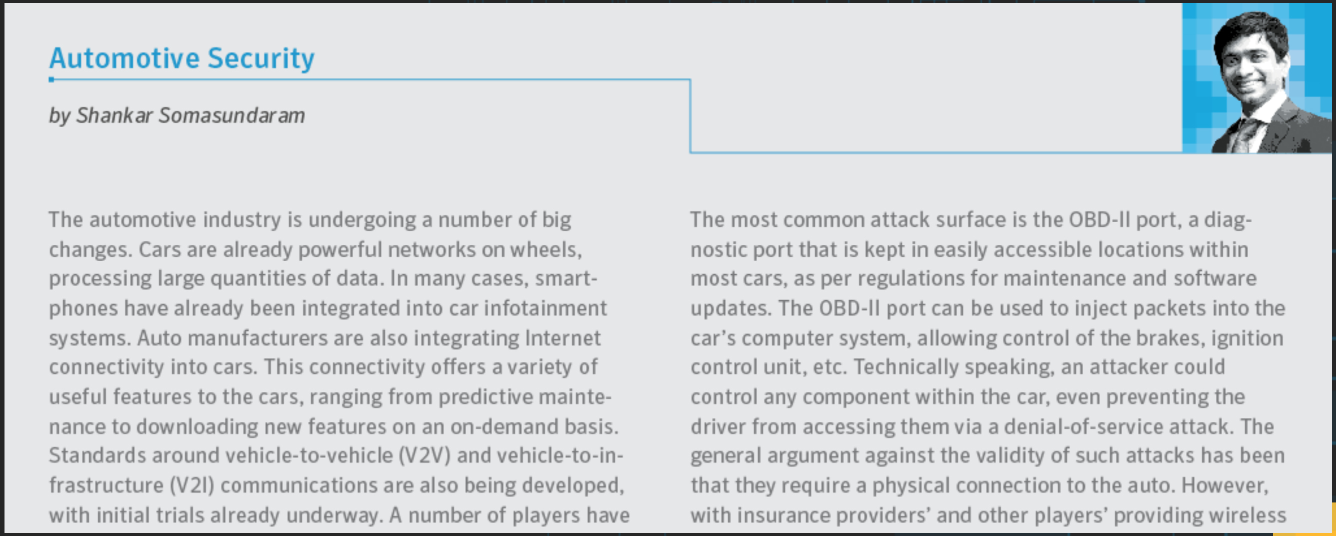
Medical Devices – Safety First, Security Second

by Axel Wirth

Medical devices are notoriously insecure and easy to hack, as has been demonstrated for pacemakers and[30] insulin pumps,[31] as well as surgical and anesthesia devices, ventilators, infusion pumps, defibrillators, patient monitors, and laboratory equipment.[32]

The concerns voiced by security researchers, government regulators, and healthcare providers are well founded as any medical device cybersecurity incident could seriously harm

- Since medical devices are periodically on and off the hospital network as patient come and go, removal of malware from compromised devices may be operationally difficult. Given some malware's ability to reinfect cleaned devices, all vulnerable devices may need to be cleaned at once, requiring all impacted patients to come to the hospital at one time: a scheduling challenge in-and-of itself.



Automotive Security

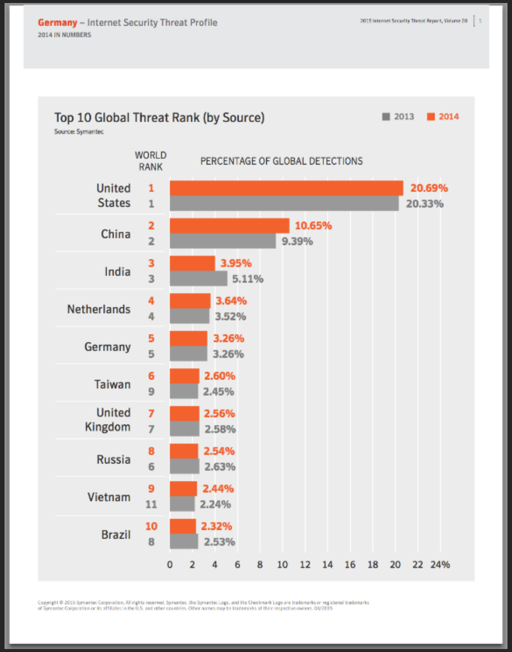
by Shankar Somasundaram

The automotive industry is undergoing a number of big changes. Cars are already powerful networks on wheels, processing large quantities of data. In many cases, smartphones have already been integrated into car infotainment systems. Auto manufacturers are also integrating Internet connectivity into cars. This connectivity offers a variety of useful features to the cars, ranging from predictive maintenance to downloading new features on an on-demand basis. Standards around vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications are also being developed, with initial trials already underway. A number of players have

The most common attack surface is the OBD-II port, a diagnostic port that is kept in easily accessible locations within most cars, as per regulations for maintenance and software updates. The OBD-II port can be used to inject packets into the car's computer system, allowing control of the brakes, ignition control unit, etc. Technically speaking, an attacker could control any component within the car, even preventing the driver from accessing them via a denial-of-service attack. The general argument against the validity of such attacks has been that they require a physical connection to the auto. However, with insurance providers' and other players' providing wireless

ISTR 20

- symantec.com/threatreport
- German ISTR webcast – 6th May at 2pm https://www.brighttalk.com/webcast/5691/152209



Germany – Internet Security Threat Profile

2014 IN NUMBERS

2015 Internet Security Threat Report, Volume 20 | 1

Top 10 Global Threat Rank (by Source)

Source: Symantec