



# Compromised?

Paul Black – Asia Pacific & Japan, Incident Response  
Victor Law – Greater China Region, Enterprise Security



# Compromise

## It will happen

No longer an if - but when

## Detection takes too long

229 - Average number of days to discover a breach

## Not enough skills

70% of organizations lack staff to counter cyber security threats

## Time is money

Big money



# Key Themes

## Targeted Attacks

Targeted Attacks Shifted from Economic Espionage to Politically Motivated Sabotage and Subversion

**International Business Times**  
Technology | CyberSecurity

**Ukraine: First power station knocked offline by hackers is harbinger of cyber-warfare future**  
By Anthony Cuthbertson  
Updated January 5, 2016 17:30 GMT

**ars TECHNICA**

RISK ASSESSMENT —  
**Hackers trigger yet another power outage in Ukraine**  
For the second year in a row, hack targets Ukraine during one of its coldest months.

**theguardian**

**DNC head leaked debate question to Clinton, Podesta emails suggests**  
Donna Brazile tipped off Clinton's campaign about Flint water crisis question, according to new emails released by WikiLeaks from John Podesta's account

## Cyber Bank Heists

Attackers Chase the Big Scores, Bigger Ambitions and is Targeting Banks

**FINANCIAL TIMES**  
WORLD US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Bangladesh  
**How cyber criminals targeted almost \$1bn in Bangladesh Bank heist**

## Macros, IT tools & Malware

Attackers Weaponized Commonly Used Software

**appleinsider**

**Microsoft Word macro malware automatically adapts attack techniques for macOS, Windows**  
By Malcolm Owen  
Friday, March 24, 2017, 07:47 am PT (10:47 am ET)



## Internet of Things

Cyber Criminals Harnessed the Processing Power of IoT Devices to Fuel Zombie Army of Devices

**SC MEDIA**  
October 21, 2016  
Mirai botnets linked to massive DDoS attacks on Dyn DNS, Flashpoint says

## Email

Email Became the Weapon of Choice

**Request from CEO**  
Subject: Immediate Wire Transfer  
To: Chief Financial Officer  
High Important  
Please process a wire amount of \$250,000 by COB today. Wire

**SC MEDIA**  
May 27, 2016  
CEO sacked after aircraft company grounded by whaling attack  
Following a successful whaling attack in January which cost FACC €40 million, the company has sacked both its CFO and CEO.

## Ransomware

Ransomware Squeezing Victims with Escalating Demands

**NBC NEWS**  
TECH MAR 23 2016, 5:16 PM ET  
**Three U.S. Hospitals Hit in String of Ransomware Attacks**  
by CONNOR MANNION

TECH JAN 9 2017, 11:51 AM ET  
**Ransomware: Now a Billion Dollar a Year Crime and Growing**  
by HERB WEISBAUM

## Cloud

Cracks in the Cloud: The Next Frontier of Cybercrime is Upon Us

**FINANCIAL EXPRESS**  
**Ransomware: Over 27,000 databases of MongoDB attacked in a day; many other still vulnerable**  
Thousands of MongoDB databases have reportedly been compromised where cyber attackers have wiped data and demanded bitcoins to return them.

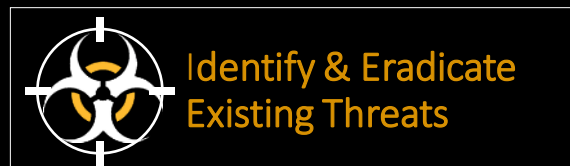
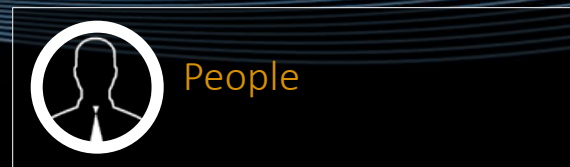
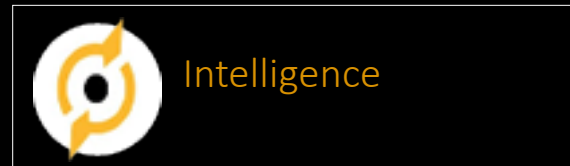
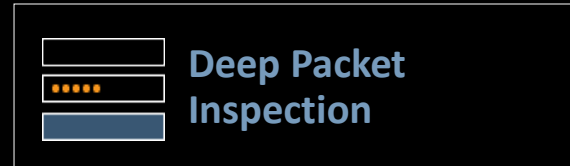


# Quick Wins



# Go Hunting

## Advanced Threat Hunting



## Preventive Incident Response

Regularly hunting for threats helps to establish a consistent, known secure state for your network.

## Don't Wait For an Incident

**Identify** and **eradicate** existing compromises before they become a major data breach.

## Reduce Breach Response Costs

**Compromises** are common and inexpensive to remediate.

Identify threats early to avoid high incident response costs.

# The Importance of Root Cause

Infection vectors don't change between commodity malware and targeted attacks

Know impact and intent, understand the risk and mitigate appropriately

Strengthen detection and prevention as an outcome of every qualified incident

Build trending and metrics into incident reporting

Use actual incident data to drive security awareness

# Quick Wins





**Thank You!**

**Copyright © 2017 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.

