NAIC National Association of Insurance Commissioners & The Center for Insurance Policy and Research

Insurance SUMMIT

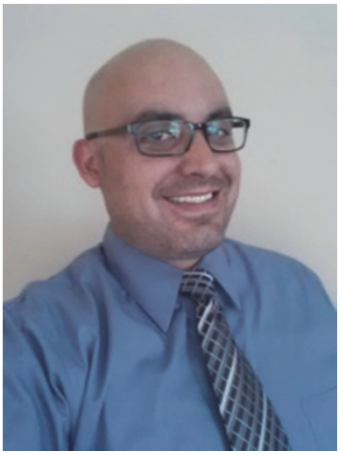
The Cybersecurity Landscape

Walt Powell CISSP, CISM
Sr. Solution Architect Optiv Security

OPTIV

Introduction

Walt Powell CISSP CISM
Sr. Solution Architect
Optiv Security



Agenda

- Biggest breaches of the 3 last years
- Anatomy of breaches
- Common factors
- Who are the modern threat actors
- What are the future threat vectors
- Cost of Breaches
- Cost Reduction Techniques
- How to combat modern threats
- Breach detection techniques
- Summary

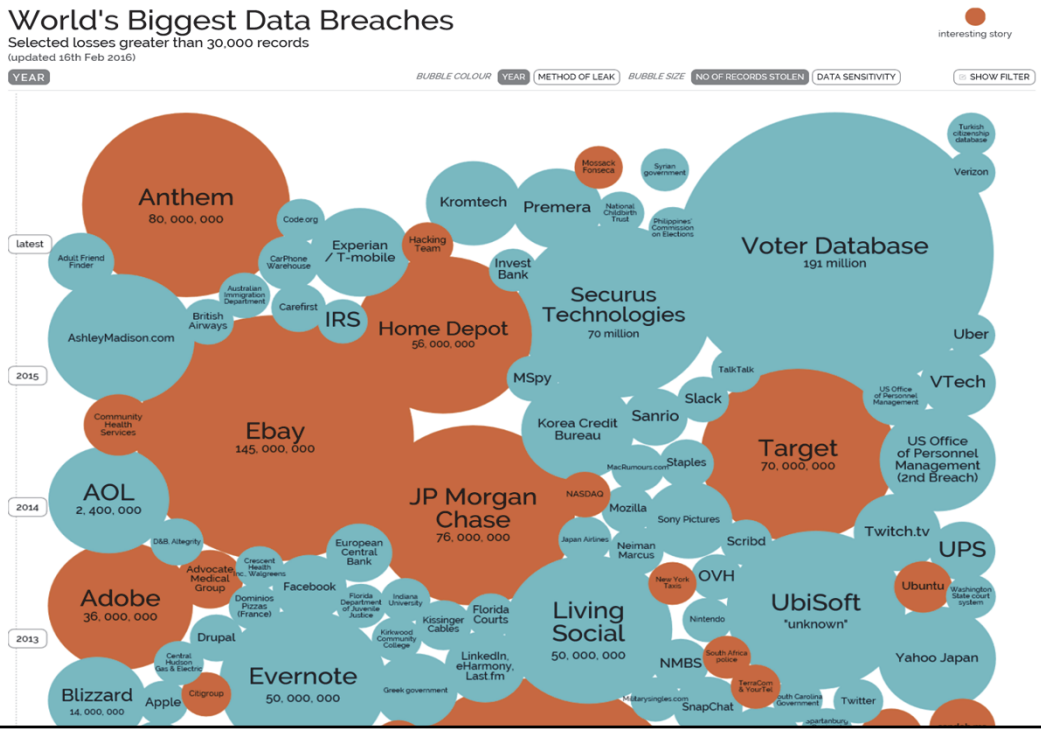
NAIC Insurance Regulator
Professional Designation Program

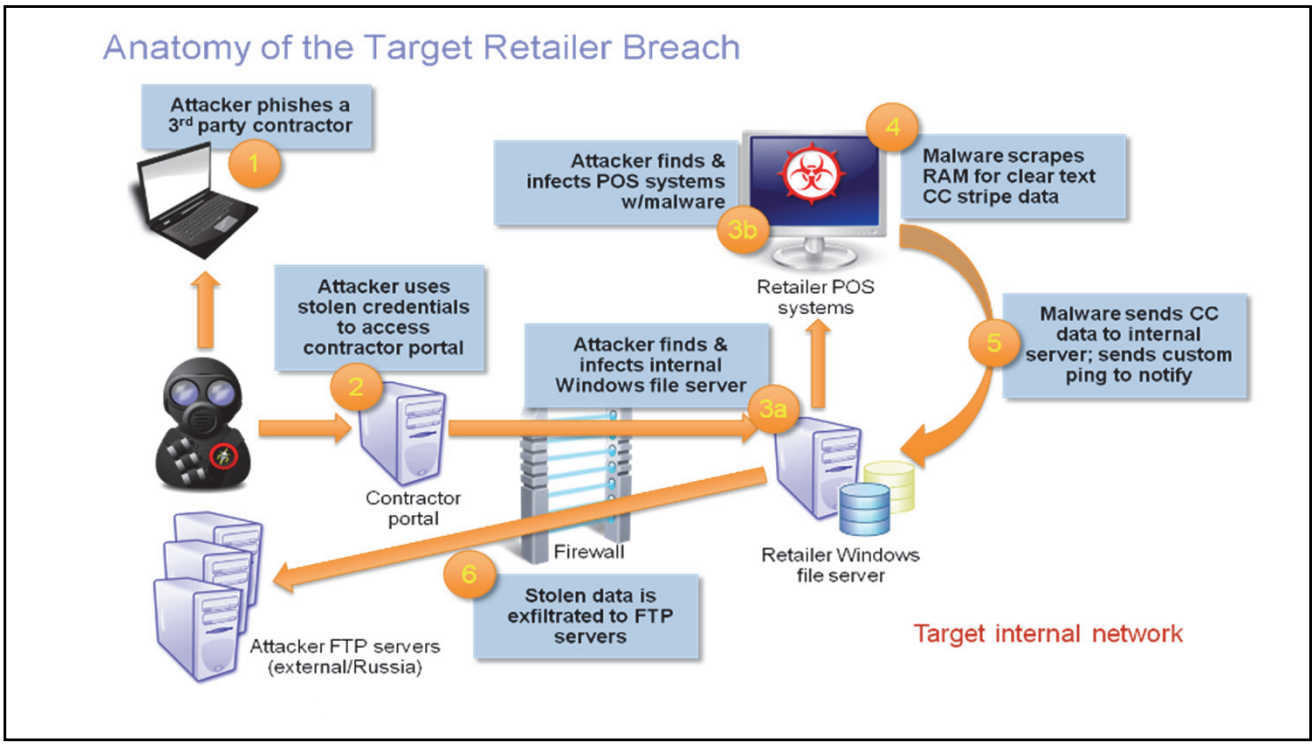
Attention APIR, PIR, or SPIR Designees…

This presentation is pre-qualified for NAIC Designation Renewal Credits (DRCs). If you currently hold an NAIC APIR, PIR, or SPIR designation and are pursuing continuing education credit to maintain it, you may be awarded credits for your participation. To receive credit, you must be in attendance for the duration of the presentation.

Learning Objectives

- Understand the common anatomy of breaches
- Identify common threats and threat actors
- Understand the average cost of breaches
- Develop an understanding of threat and cost reduction techniques and strategies



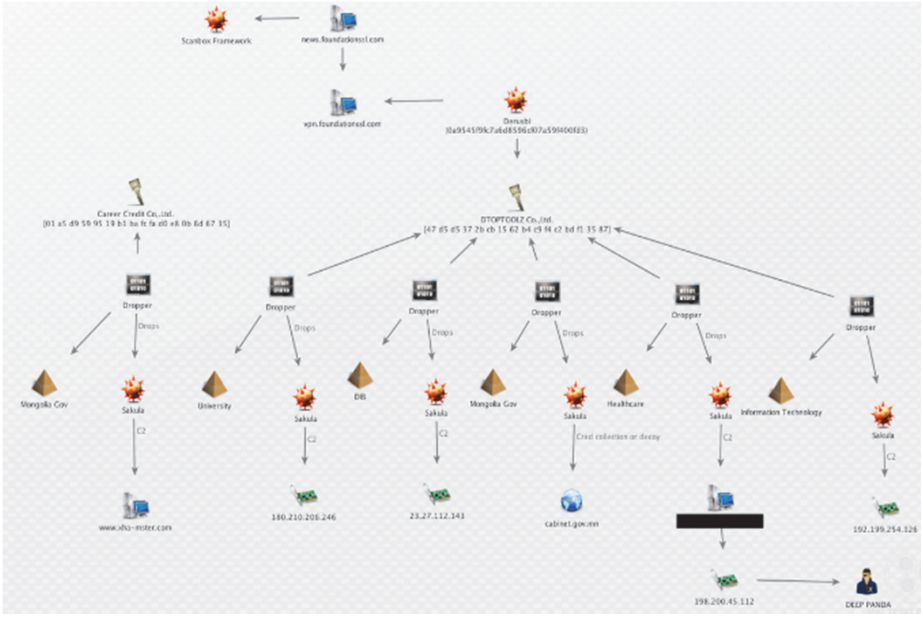

Anatomy of the Target Retailer Breach
Attacker phishes a 3rd party contractor
1
Attacker uses stolen credentials to access contractor portal
2
Contractor portal
Attacker finds & infects internal Windows file server
3a
Attacker finds & infects POS systems w/malware
3b
Retailer POS systems
4
Malware scrapes RAM for clear text CC stripe data
5
Malware sends CC data to internal server; sends custom ping to notify
Firewall
Retailer Windows file server
6
Stolen data is exfiltrated to FTP servers
Attacker FTP servers (external/Russia)
Target internal network


TARGET
P.F. CHANG'S
CHINA BISTRO
THE HOME DEPOT
SALLY
SALLY BEAUTY SUPPLY

Anthem Attack

Doppelganger Domains

- We11Point.com
- Me.we11point.com
- Prennera.com



PASSWORD

DATA BREACH

Ebay and JP Morgan Chase

The origin of the breach comes from hackers compromising a small number of employee log-in credentials, which gave access to eBay's corporate network. –Forbes.com

JPMorgan's security team had apparently neglected to upgrade one of its network servers with the dual password scheme -New York Times

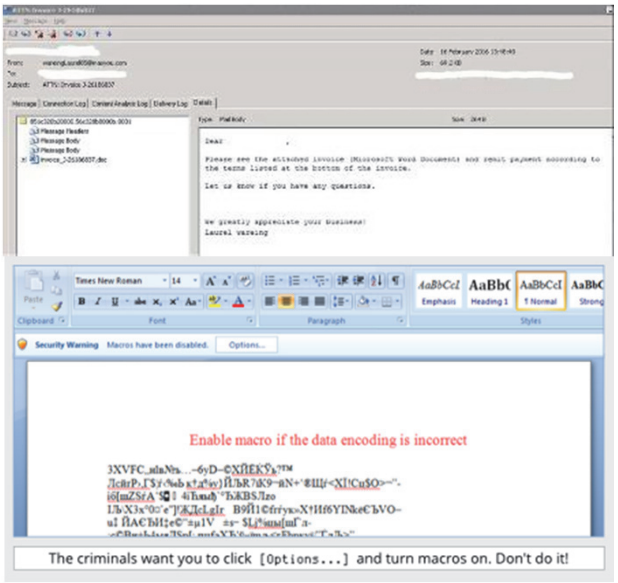
Sony Pictures Entertainment

Attack details are shrouded in lies

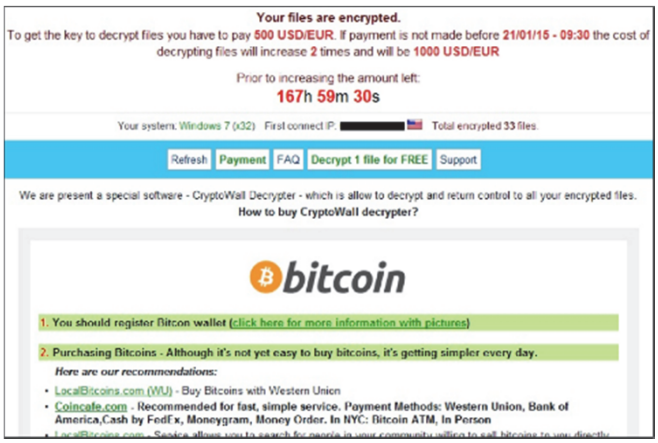
- "The FBI now has enough information to conclude that the North Korean government is responsible for these actions."

- "The attack on Sony was unprecedented and that the malware used was "undetectable by industry standard antivirus software." -Kevin Mandia (Mandiant Security)
- "Norse Corporation researchers are claiming that a group of six people, including at least one former Sony Pictures employee, was behind the recent breach at Sony Pictures Entertainment."

Ransomware

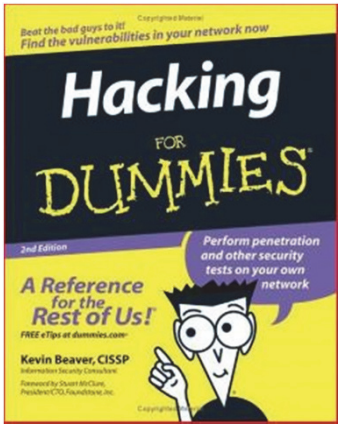


Cryptowall was responsible for 406,887 attempted infections and accounted for approximately $325 million in damages since its discovery in January 2015. -Lavasoft



What the Biggest Breaches Have in Common

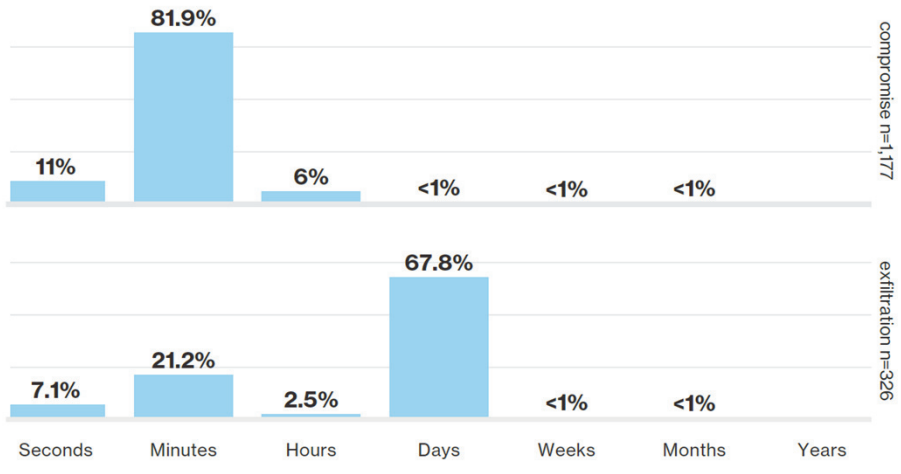
- No 0 Day Exploits or Advanced Techniques
- Most used Phishing attacks and legitimate credentials
- All attacks were persistent and progressive
- Hackers spent months inside networks undetected
- Most of the exploited vulnerabilities were compromised more than a year after the associated CVE was published
- Used old, derivative or common malware
  - Zeus
  - Black POS / Kaptoxa
  - Fakem RAT
  - Wiper



Cyber Kill Chain

Reconnaissance	• Harvesting Email Addresses, Social Networking, Passive Search, IPs, Port Scans
Weaponization	• Developing Exploit with Payload Creation, Malware, Delivery system, Decoys
Delivery	• Spear Phishing, Infected Website, Service Provider, USB
Exploitation	• Activation, Execute Code, Establish Foothold, 3rd Party Exploitation
Installation	• Trojan or Backdoor, Escalate Privileges, Root Kit, Establish Persistence
Command & Control	• Command Channel, Lateral Movement, Internal Recon, Maintain Persistence
Actions on Target	• Expand Compromise, Consolidate Persistence, Identify Targets, Data Ex-filtration

The timeline is accelerating



Attack Types

Malware	Software that is intended to damage or misuse a system
Exploit	Taking advantage of a flaw in a computer system
Active	Deploying Metasploit payload
Passive	Waiting for malware to call home for C&C
Persistent	Remote Access Trojan (RAT) installed to maintain rouge access
Targeted	Phishing or vulnerability scanning
Non-Targeted	Spammed or shared malware
Blended	Most modern attacks will utilize multiple attack types

Modern Malware is Polymorphic

Zero Day Exploit vs. Zero Day Malware

Commonly Mixed Up Terms:

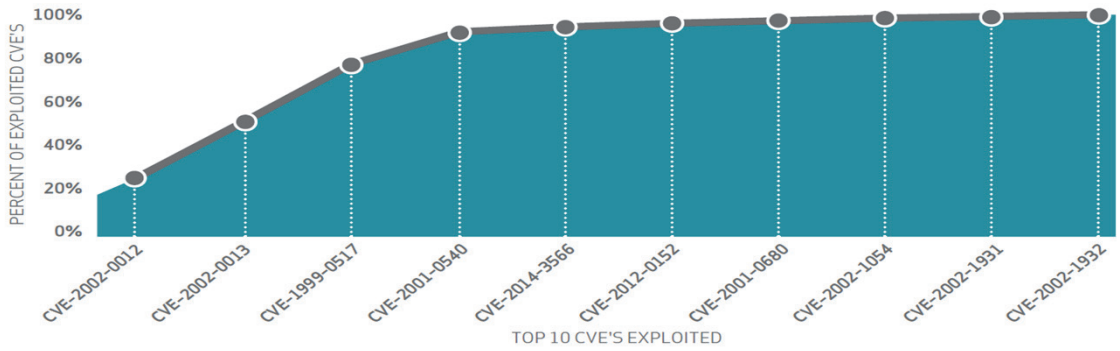
Vulnerability – Weakness or flaw in a system

Threat – Anything that can intentionally or accidentally, and obtain, damage, or destroy an asset. (ie; Hackers, Terrorists, Tornados)

Exploit – An exploit is the way or tool by which an attacker uses a vulnerability

-Buffer Overflow
-Heap Spray
-XSS

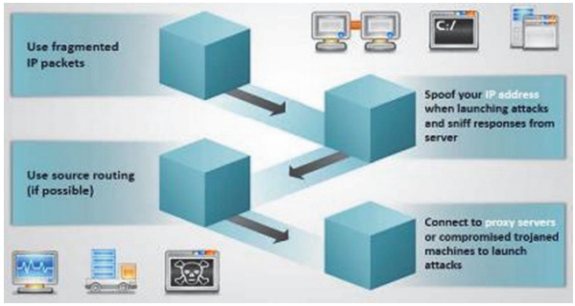
Malware Changes Exploits Don't



1. Windows Log Clear
2. XSS via java
3. Slash Dot ..\ Dir Traversal
4. HP AIF Gain DB Privileges
5. RDP Terminal Server DoS
6. SSL "POODEL"
7. RDP Memory Exhaustion
8. Missing SMTP Name
9.&10. SMTP remote privileges

Evasion techniques add to the challenge

- Address Spoofing
- Packet Fragmentation
- Polymorphism of malware per machine instead of per organization circumventing most host and network based detection methods.



- Malware circumventing network detection by using SSL and Domain Generation Algorithm (DGA)
- Multi-vector Malware attacks in layers creating distraction and chaos while allowing unauthorized access, performing massive data exfiltration, and leading to extortion and data loss:
  - ***Visits malicious website → Endpoint Compromised → Stolen Credentials → Privilege Escalation***
  - ***W32.Changeup → Zeus → Cryptolocker → Data Loss***
  - ***Compromise of Computer + Phone for Financial Attacks***

Phishing

23%
OF RECIPIENTS NOW OPEN PHISHING MESSAGES AND 11% CLICK ON ATTACHMENTS.
-Verizon DBIR 2015

Almost all of the Biggest breaches of the last several years are the result of a phishing attacks

- Strong recon makes Spearfishing difficult to detect
- Doppelganger domains and obfuscation techniques can mask malicious links
- Dark Hotel, phone pre-texting, etc move phishing attacks out of email

Modern Threat Actors

- Organized Crime
  - Russian and Ukrainian based
    - CyberBerkut, Innovative Marketing Inc
  - Corporatized, Big money
- State Sponsored / Nation States
  - North Korea
  - China (Great Cannon)
  - Deep Panda
  - NSA
- Hacktivists
  - Anonymous
  - Lulz Sec
- Terrorist Groups
  - ISIS

КИБЕРБЕРКУТ
МЫ НЕ ЗАБУДЕМ
МЫ НЕ ПРОСТИМ

ANONYMOUS

DEEPPANDA

Future Attack Vectors

- **IPv6**
  - The Zeus Botnet is IPv6 Compliant
  - Most modern malware can tunnel IPv6 C&C traffic
- **Internet of Things**
  - Things are IP'd that were never designed to be connected
  - How do we secure, Thermostats, Switches, Light Bulbs, etc?
- **Big Data**
  - Internet of things requires Big Data, which is still in its infancy
  - Our ability to compute is rapidly out stripping our ability to secure
- **Cloud**
  - Blurred Edge makes securing the Perimeter impossible
  - Sanctioned Service Challenges vs Shadow Cloud Challenges
  - How do you Secure disjointed memory spaces or remote processing and computation?

Common Problem

Security threats have evolved… Security spending hasn't!
The response no longer fits the threat!

2001

Threats

Script Kiddies, Web defacement, Bragging Rights, Backdoors in open source

Sub7 Code Red Klez NTDaddy NetBus Back Orifice Nimda Anna Kournikova

Security Spending

- Anti-virus
- Firewall/VPN
- Content Filtering
- IDS/IPS

2015

Threats

Crime Syndicates, Nation States, Identity Theft, Targeted Malware

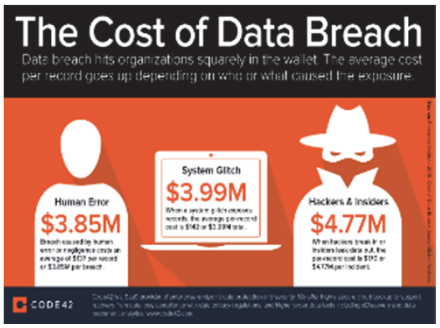
Mobile phone attacks Night Dragon APT Targeted attacks Black POS Zeus 232 million identities stolen

Security Spending

- Anti-virus
- Firewall/VPN
- Secure Email/Web
- IDS/IPS

Cost of Data Breaches

- $3.79 million is the average total cost of data breach
  - 23% increase in total cost of data breach since 2013
- $170 is the average cost per lost or stolen record
  - The cost of data breach varies by industry.
    - Healthcare breaches can have an average per record cost high as $363.
- Data breaches cost the most in the US
  - The average per capita cost of data breaches in the US is $217
  - 12% percent increase in per capita cost since 2013



-Ponemon 2015 Cost of Data Breach Study

Cost of Settlements

Company	Date of Breach/ Settlement	# Records	Type of Records	Settlement Fund	Basis
AvMed (Florida)	2010/Jan 2014	1 million	Social Security Numbers and Health records	$3.1M	Partial refund of insurance premiums (up to $30 per individual) for not receiving the level of security promised
Stanford University (CA)	2009/April 2014	20,000	Health records	$4.1M	Patients will receive $100 each and the hospital will have to fund a program for 2 years that trains medical professionals to protect patient records.
Schnucks (MO)	2012/July 2014	2.4 million	Credit Cards	$2.1M	Up to $200 for expenses plus up to $10,000 for individuals who actually lost money
Vendini	2013/July 2014	3 million	Credit Cards and other PII	$3M	Unreimbursed Identity Theft Losses up to $3,000 or compensation for Unreimbursed Expenses up to $1,000 related to the breach
Sony	2011/July 2014	77 million	Login Credentias, PII and Some Credit Cards	$15M	Class members who didn't take advantage of a 2011 "Welcome Back" package of games and memberships will receive one of 14 PS3 games, as well as three of six PS3 themes or a three-month PlayStation Plus subscription. Qriocity users will get one month of free access.
LinkedIn	2012/August 2014	6.4 million (incl 800,000 premium subscribers)	PII (login credentials only)	$1.25M	Of the 800,000 premium LinkedIn subscribers from March 2006 to June 2012, only 20,000 to 50,000 looked at LinkedIn's privacy policy long enough to be influenced by their representations and eligible for up to $50 from the settlement fund

The 3 major factors contributing to a rising cost of breaches

- Cyber attacks have increased in frequency and in the cost to remediate the consequences.
  - The cost of data breaches due to malicious or criminal attacks increased from an average of $159 to $170 per record.
  - Cyber attacks were the root cause of 42% of Data loss in 2013 but have increased to over 50% in 2015.
- The consequences of lost business are having a greater impact on the cost of data breach.
  - The average cost of business impact increased from $1.33 million last year to $1.57 million in 2015.
  - That cost includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill.
- Data breach costs associated with detection and escalation increased.
  - This total average cost increased from $.76 million last year to $.99 million in 2015.
  - These costs typically include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors.

-Ponemon 2015 Cost of Data Breach Study

Ways to lower the cost

- **Cyber Insurance**

Exposure Category		Description
Privacy Liability		Provides liability coverage for failure to protect electronic or non-electronic information in your care custody and control. Can include coverage for acts of vendors as well.
Network Security Liability		Provides liability coverage if an Insured's Computer System fails to prevent a Security Breach, becomes inaccessible to those who need it or unintentionally transmits a virus to a 3rd party.
Media Content Liability		Provides liability coverage for Intellectual Property and Personal Injury lawsuits stemming from your website or social media content under your direct control.
Regulatory Liability		Defense coverage for legal proceedings or investigations by Federal, State, or Foreign regulators relating to Privacy Laws.
Crisis Management	Legal Assistance Expense	Expenses incurred to hire an attorney to help navigate the breach response process in accordance with the multitude of State and federal laws.
	Forensic Expense	Expenses incurred to hire a firm to conduct IT forensics investigations following a data breach.
	Notification Expense	Expenses incurred to notify members of a breach in accordance with State and Federal laws.
	Credit Monitoring Expense	Expenses incurred to provide donors with access to identity protection services.
	Public Relations Expense	Expenses incurred to hire a public relations consultancy, media expenses, etc. in the wake of a data breach.
Data Recovery/Restoration		Expenses incurred to re-create data that is damaged as a result of a cyber incident.
Business Interruption		The reduction of business income as a result of an interruption or use of a computer system as a result of a network breach to their system.
Cyber Extortion		Expenses incurred resulting from threats to introduce a system hack, virus, etc. or from threats to disseminate or use information contained in your computer systems to destroy or alter your computer systems.
Fines and Penalties		Where permissible by law, expenses incurred as a result of a State, Federal or other (PCI DSS) fine or penalty resulting from a data breach.

Under Insurance is state of the market

- **Target Corp.** announced that its 2013 data breach will cost an estimated **$252 million** in expenses.
  - After its expected **$90 million** insurance compensation that still leaves **$162 million**.
- **Home Depot** expects **$100 million** in cyber insurance payments toward **$232 million** in expenses from its 2014 breach.
  - Which leaves **$132 million** is uncovered costs.
- **Anthem** ran into difficulties renewing its coverage after an attack early this year that compromised some **79 million** customer records.
  - Renewal rates were "prohibitively expensive".
  - Anthem managed to get **$100 million** in coverage by agreeing to pay the first **$25 million** in costs for any future attacks.

AIG CEO Peter D. Hancock said that cyber insurance "lags behind other types of insurance in the amount of coverage providers offer."

-"The largest coverage I'm aware of is for a bank that has about $400 million in coverage which is very small when you think about it." -Jim Finkle Rueters.com

Ways to REALLY lower the cost

- **Board involvement can reduce the cost of a data breach.**
  - Positive consequences can result when boards of directors take a more active role when an organization had a data breach.
    - Board involvement reduces the cost by $5.5 per record.
- **Time to identify and contain a data breach affects the cost.**
  - How quickly an organization can identify and contain data breach incidents has great financial consequences.
    - Malicious attacks can take an average of 256 days to identify.
    - Data breaches caused by human error take an average of 158 days to identify.
- **Business continuity management plays an important role in reducing the cost of data breach.**
  - Research reveals that having business continuity management involved in the remediation of a breach can reduce the cost by an average of $7.1 per compromised record.

-Ponemon 2015 Cost of Data Breach Study

Threat reduction strategies

Goals

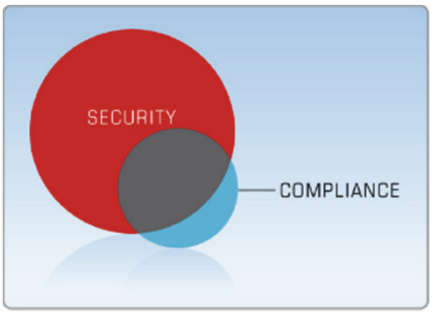
- **Programmatic Approach**
  - Documented
  - Risk Based
  - Business Aligned
- **Layered Defenses**
  - Visibility, prevention, detection, response
  - Spread across kill chain
- **Operationalize**
  - Plan, Build, Run, Audit, Repeat

Challenges

- **Programmatic Approach**
  - Lack of head count / qualified talent
  - Lack of Funding / Budget
- **Layered Defenses**
  - Lack of visibility/network blind spots/unmanaged environments/insecure apps
  - Large numbers of ingress/egress points and unmanaged devices
- **Operationalize**
  - Enterprises often have no IR infrastructure or it is not properly utilized

Compliance vs Security

- Nobody is immune to compliance. But it's more than just checking a box.
  - Everyone needs to be compliant with a policy, regulation or legal requirement: PCI, HIPAA, SOX, GLBA, FTC, NERC, FERC…
  - Are you secure or just compliant?
  - You can be completely compliant and totally insecure.
  - Promote compliance through security. It does not come in a can or clip board.



Problems We Face

- Lack of head count / qualified talent
- Lack of Funding / Budget
- Enterprises often have no IR infrastructure or it is not properly utilized
- Lack of visibility/network blind spots/unmanaged environments/insecure apps
- Large numbers of ingress/egress points and unmanaged devices

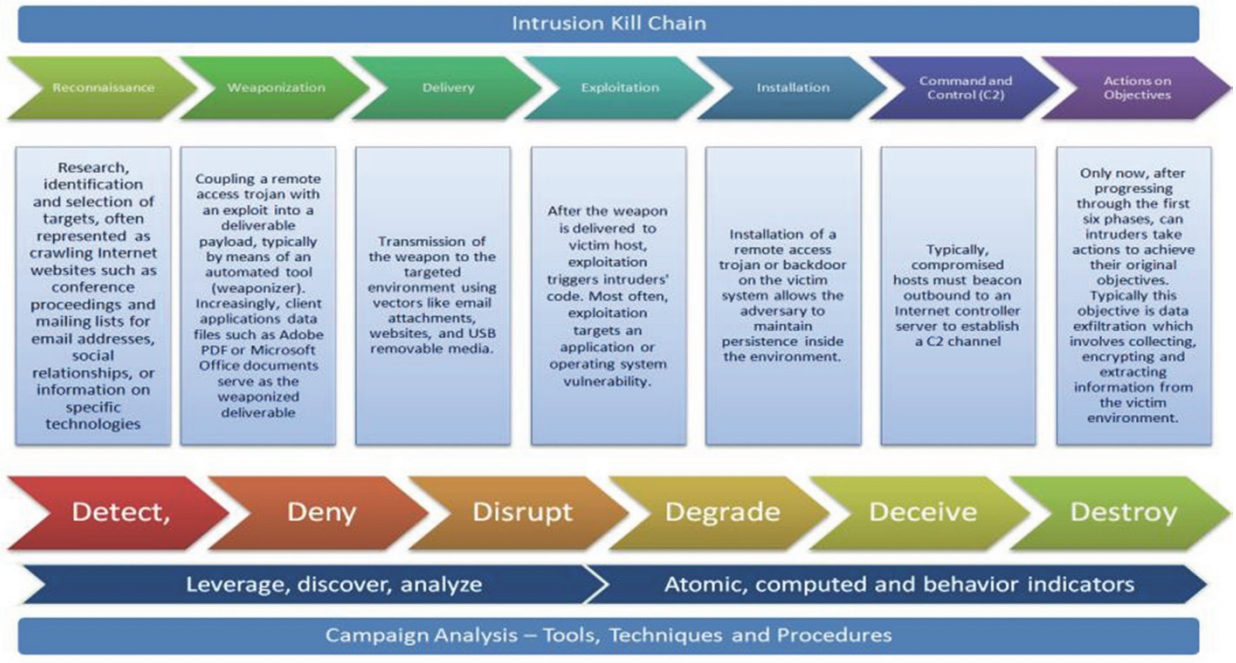
Hard Truths

- Bastion Model no longer works
- Most breaches are still due to lack of basics
- Once we get good at the basics the “next gen” of advanced attacks already exist.
- Behavior, heuristics and statistics will become “table stakes”.
- The future of Security will include AI style algorithms that can understand North/South and East/West Traffic in real time.
- Until then we need to Operationalize IR and take on a reactive “Breach Detection” model. To supplement out prevention techniques.

What should we be looking for?

- Know indicators of endpoint compromise
- Queries for suspicious or known bad domain names
- Connection is to known botnets, C&C servers or bad IPs
- Domain Fluxing (DGA)
- Tunneling
- Proxy connection attempts
- Network traffic IOCs and anomalies
- High quantity of egress connection attempts
- High volume of traffic or data egress (chatty cathy's)
- Suspicious binary downloads
- Non-human / automated behavior

Modern Malware needs to be addressed in a more holistic way and all along the Kill Chain



PASSWORD

MALWARE

Modern Detection Techniques

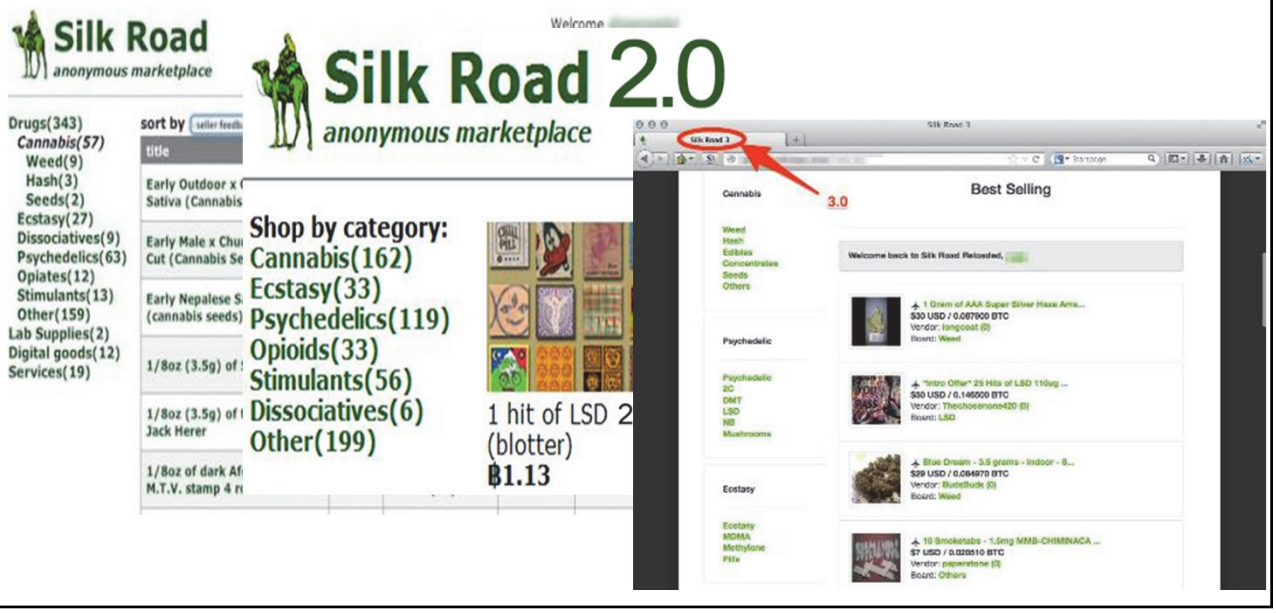
Modern Malware and Breach detection requires a blended approach to detect all along the Kill Chain.

- Dynamic Code Analysis (Sandboxing)
- Whitelisting /Threat Intelligence
- Machine Learning
- Data Mining
- Heuristics
- Static Code Analysis
- SSL decryption
- Next gen traffic inspection
  - App ID
  - User ID
  - Content ID

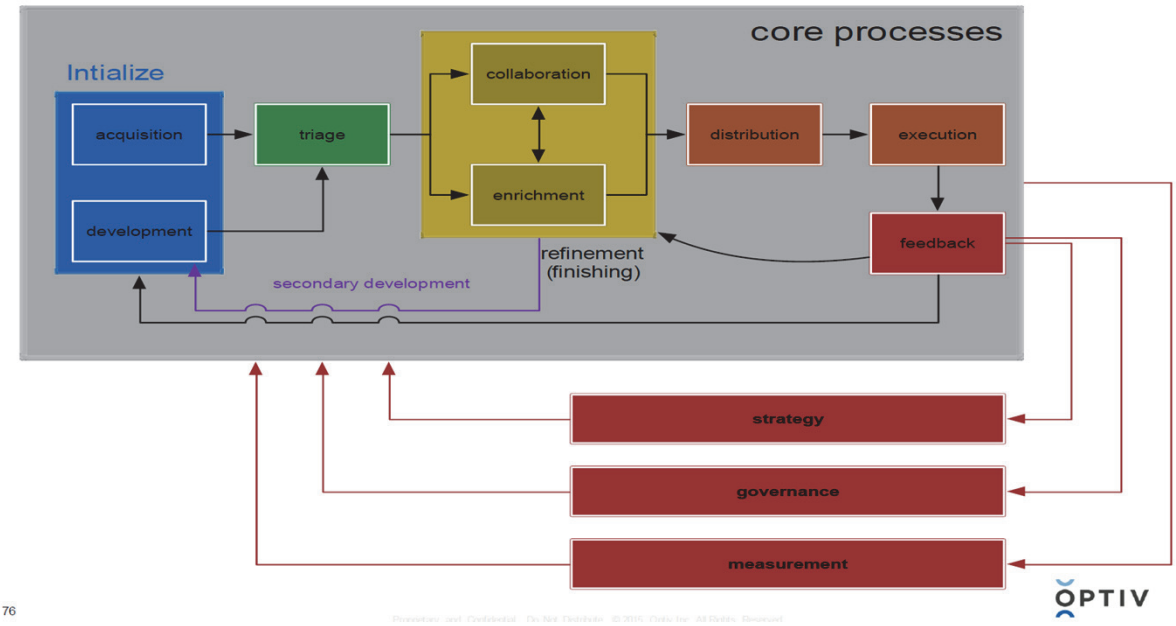
Controls for Combatting Modern Threats

- **Quick Wins and Low Hanging Fruit**
  - Patch Management
  - Security Awareness Training
  - Credential Management
- **Advanced Controls**
  - Endpoint Anti-Malware & APT
  - Network Anti-Malware & APT
  - Email Anti-Malware & APT
- **Visibility & Attribution Tools**
  - SEIM
  - Endpoint Forensics
  - Network Packet Capture
  - Cloud Security
- **Programmatic Answers**
  - Operationalize IR and Forensics
  - Align Security program with Business practices and drivers

The Problem With Gathering Threat Intel



The Problem With Operationalizing Threat Intel



76

Summary

- All the major breaches of the last 3 years have been perpetrated the same ways; utilizing phishing and well known attack techniques, methods and exploits.
- The costs and frequency of data breaches are on the rise.
  - Averaging $3-$4 Million per breach
- The best way to lower the costs of data breaches is to:
  - Elevate board level visibility and buying
  - Take a programmatic approach to enterprise security
  - Operationalize Incident Response
  - Build trusted partnerships with firms that can manage, operationalize, or supplement your practice

OPTIV

Credit and Thanks to:

- DataBreachToday.com
- Kreb On Security
- Verizon DBIR 2015 & 2016
- Trend Micro
- Norse
- CrowdStrike
- FBI
- Forbes
- New York Times
- Kevin Mandia and Mandiant
- Lockheed Martin
- Proofpoint.com
- Forcepoint.com
- Rueters.com
- Ponemon.com
- Ponemon 2015 Cost of Data Breach Study
- Jim Finkle
- Colby Clark Principle Sec Architect Kaiser Perm
- Jeff Horne Optiv Dir of IR
- Raf Los Optiv Dir of Solutions R&D
- NigeSecurityguy
- Countaponsecurity.com
- Google.com
- Code 42
- Trustwave Global Security Report 2015
- Kevin Beaver and For Dummies Publishing

OPTIV

NAIC National Association of Insurance Commissioners

& The Center for Insurance Policy and Research

insurance SUMMIT

Thank You
For Attending

Walt Powell CISSP, CISM

OPTIV