MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

NETWORK COMPROMISES: WHAT ARE WE LEARNING?

Bill Dean

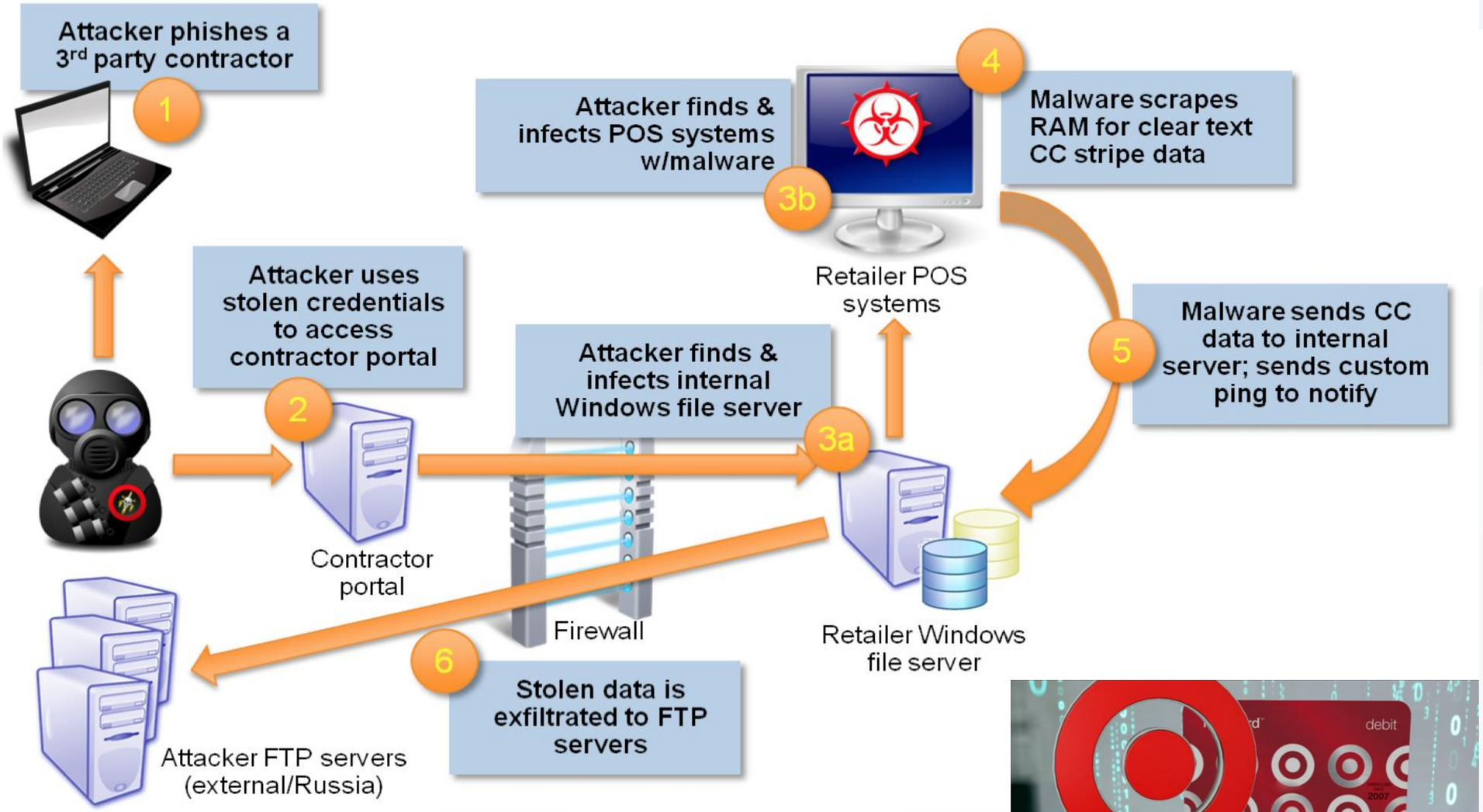
Senior Manager, LBMC Information Security

@billdeancce

AGENDA

- We All Pay Attention to Breach Information
- We All Cringe
- What Are We Learning?
- Do We Test For The Same Attacks?
- Let’s Use This Information To Improve

POS MALWARE


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)


debit
TARGET
DATA BREACH

PUBLISHED MICROSOFT CASE STUDY

Target Development Technologies Group Upgrades Knowledge Base to Microsoft SQL Server 2000, Improves Performance

This case study has been archived.

Published: April 18, 2001

Solution Overview

Company
Target Corporation

Customer Profile
Target Corporation is America's fourth-largest general-merchandise retailer, with combined revenues for 1999 of over $33 billion. The company's store brands include Target, Dayton's, Marshall Field's, Hudson's, and Mervyn's California. Altogether, the company employs more than a quarter of a million team members. It operates 21 distribution centers and more than 1,200 stores in 45 states.

Benefits
By upgrading the company's developer knowledge base server to Microsoft SQL Server 2000 and taking advantage of the improved Full-Text Search capabilities, Target has realized benefits in manipulating and searching on knowledge base entries.

The linked imag

Software and Services
- Microsoft Internet Information Services
- Microsoft SQL Server 2000
- Microsoft Windows 2000 Advanced Server

Country/Region
United States

Solutions
B2C Electronic Commerce

Audiences
Business Decision Makers

LESSONS LEARNED: POS MALWARE

- ✓ Third-Party Vendors
- ✓ Multi-Factor Authentication
- ✓ Proper Segmentation
- ✓ Change Default Credentials
- ✓ Strong Egress Filtering
- ✓ Hardened POS Devices
- ✓ Pay Attention to Alerts
- ✓ Stop Seeking Attention
- ✓ How Did We Pass PCI Compliance?

WHO WASN'T PAYING ATTENTION?

SALLY BEAUTY SUPPLY

Buckle

Verifone

Neiman Marcus

THE HOME DEPOT

SHONEY'S

SONIC

WENDY'S

Arby's

CiCi's PIZZA

Hilton

INTERCONTINENTAL HOTELS & RESORTS

HYATT

kmart

P.F. CHANG'S

AVANTI MARKETS

THIRD-PARTY VENDORS

- ✓ 2017… Seriously
- ✓ Sizable Restaurant Franchise
- ✓ POS Devices Supported by a 3rd Party
- ✓ LogMeIn Credentials Reused Across Customers
- ✓ 3rd Party was Compromised
- ✓ POS Malware Existed for More Than Two Months

VENDOR NOTIFICATION

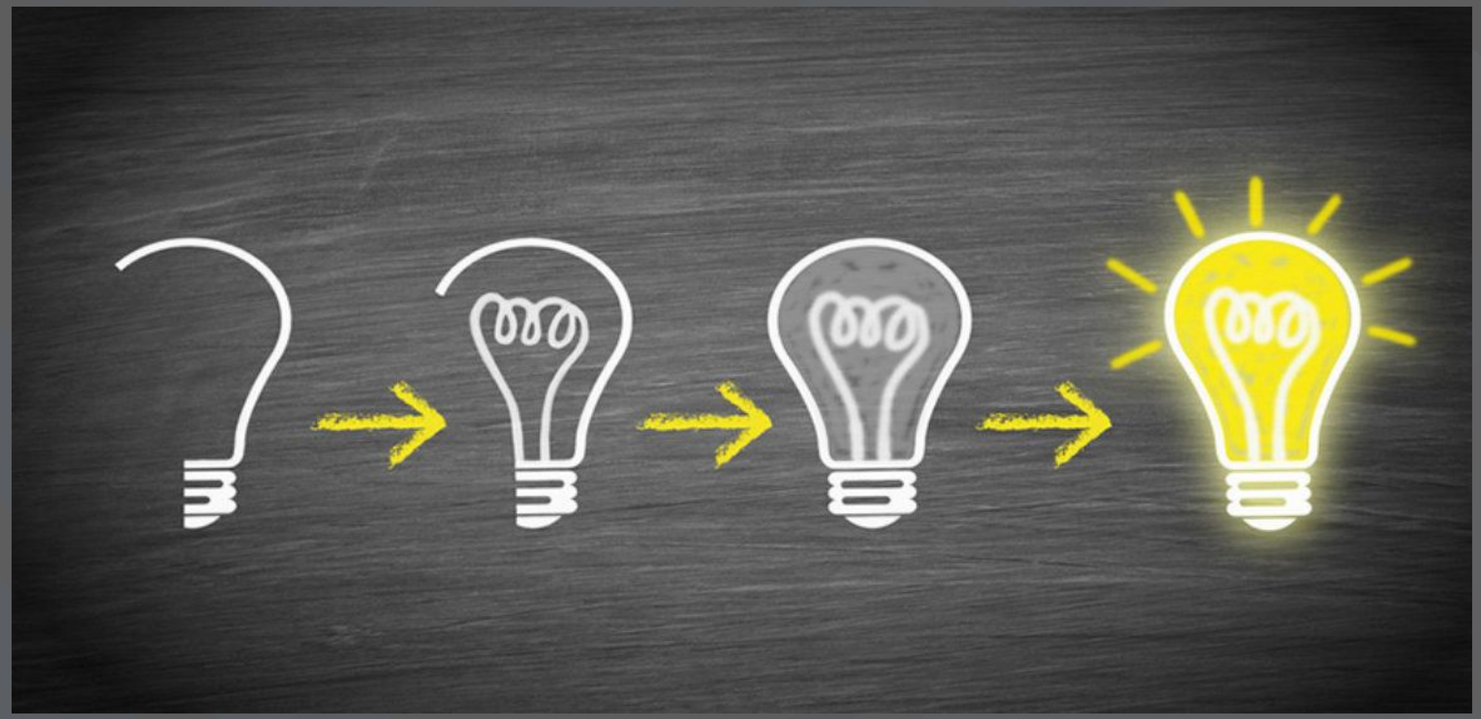
As you are aware, we were recently notified of a potential security incident that may have impacted our network. Upon learning of the issue, our incident response team promptly launched an investigation. As part of our investigation, we have been working very closely with one of the nation's leading cyber security firms that regularly investigates and analyzes these types of incidents.

Our external forensic firm has concluded that as a result of a sophisticated network intrusion through a remote access application, an unauthorized third party gained access to some, but not all, of [redacted] customers' systems and subsequently executed the PoSeidon malware variant. If your systems have been impacted by this malware, your customers' credit card data may be at risk due to the characteristics of this malware.

As part of the forensic investigation, AVG scans were conducted on all merchant systems to determine whether malware was executed on those systems. We have learned that not all merchant systems and terminals were actually logged into by the attacker. Where successful authentication was present, even then the malware was not always executed or created on those authenticated systems. For certain customers, however, authentication was successful and the malware was executed.

LESSONS LEARNED: THIRD PARTY VENDORS

- ✓ Third-Party Vendors
  - ✓ (Often Protect Themselves)
- ✓ Multi-Factor Authentication
- ✓ Proper Segmentation (CDE)
- ✓ No Credential Reuse
- ✓ Strong Egress Filtering
- ✓ Hardened POS Devices
- ✓ Event Monitoring
- ✓ P2PE Is "*Nice*"
- ✓ PCI Compliance Provides Value



WEB APPLICATIONS: EQUIFAX

- ✓ “Severe” Web Application Vulnerability
- ✓ May 2017: Compromise Detected
- ✓ Data at Risk.. Obvious and Severe
- ✓ Response.. Poor (*at best*)

LESSONS LEARNED

- ✓ Maintain Accurate Software Inventories
- ✓ Web Application Assessments
- ✓ Continuous Vulnerability Management
- ✓ Leverage Available Threat Intelligence
- ✓ Diligent Patching Policies

Don’t Work for This Guy → → →

“The human error was that the individual who’s responsible for communicating in the organization to apply the patch, did not,” Smith said in the hearing.

BUSINESS EMAIL COMPROMISE (BEC)

- ✓ Attack On the Wire / Payment Process
- ✓ They Do Their Homework
- ✓ Multiple Schemes (ACH, Payment, PII)
- ✓ Total US Victims – 22,292
- ✓ $5 Billion Dollar Scam

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 04, 2017

Alert Number
I-050417-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

BUSINESS E-MAIL COMPROMISE
E-MAIL ACCOUNT COMPROMISE
THE 5 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to Business E-mail Compromise (BEC) PSAs 1-012215-PSA, 1-082715a-PSA and I-061416-PSA, all of which are posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data as of December 31, 2016.

BUSINESS EMAIL COMPROMISE (BEC)

Office 365 <noreply@noticeoffice365.com>
7/28/2017 2:36:44 PM +0000
[redacted]
You have receive an confidential document

[redacted]

Important Document

A friend has shared an important document with you. You may need to sign in with a Microsoft account to view the document.

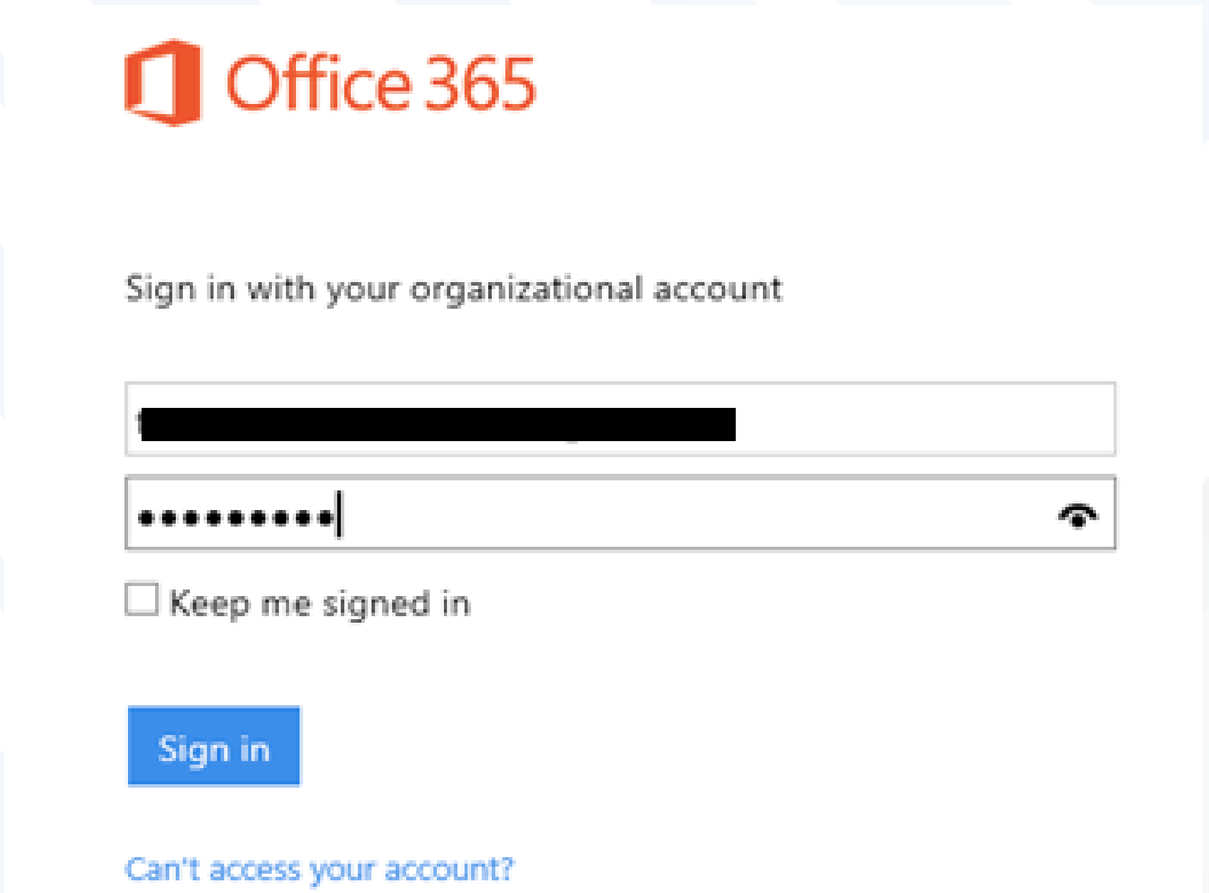
VIEW DOCUMENT

Thanks for subscribing to Office 365. We hope to continue serving you.

Helpful resources

How to reactivate your Office 365 subscription
Already renewed? Verify your subscription here
What happens to my data and access when my subscription expires?
Get help and support for Office 365

BUSINESS EMAIL COMPROMISE (BEC)



BUSINESS EMAIL COMPROMISE (BEC)

Office

Work or school, or personal Microsoft account

[redacted]

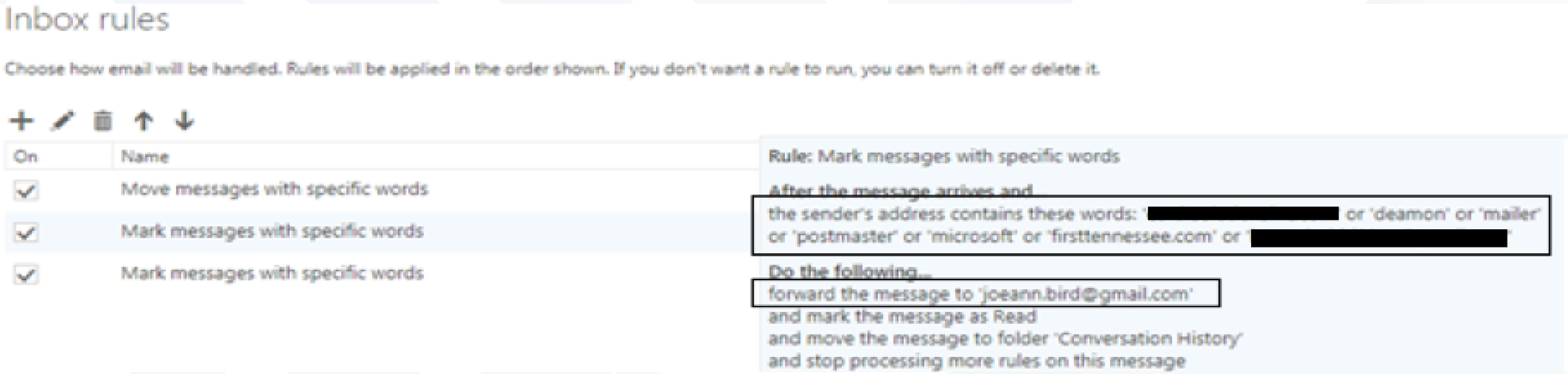
••••••••••

Keep me signed in

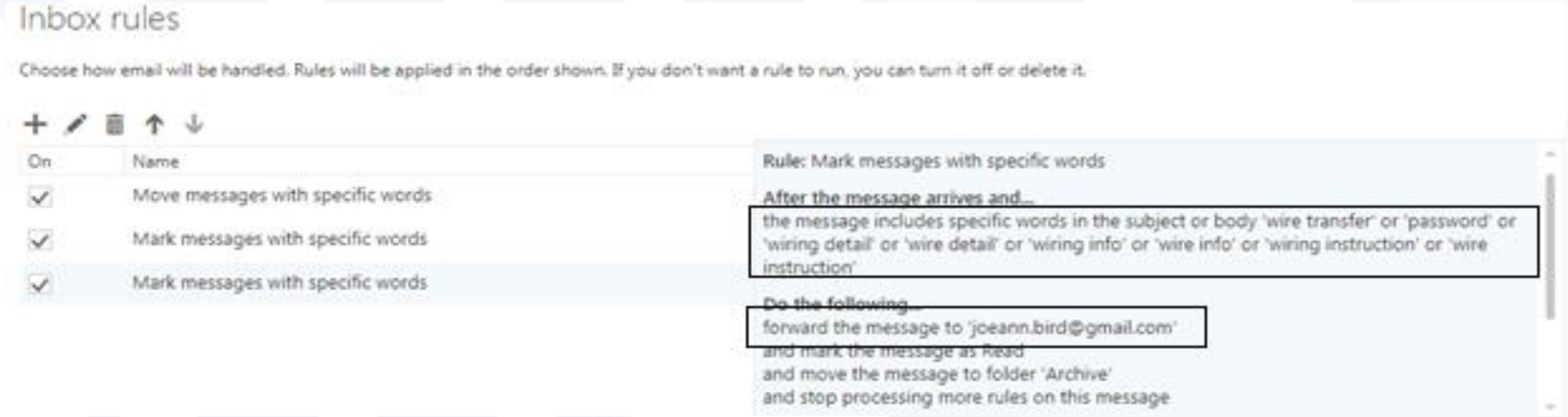
Sign in Back

Can't access your account?

BUSINESS EMAIL COMPROMISE (BEC)



BUSINESS EMAIL COMPROMISE (BEC)



BUSINESS EMAIL COMPROMISE (BEC)

From: Lori [redacted]
To: DUNCAN [redacted]
Subject: RE: RE: [redacted] attached
Date: Wednesday, October 25, 2017 1:29:54 PM

Correct.

See wiring instructions below. Please remember to send the wire confirmation.

Thank you

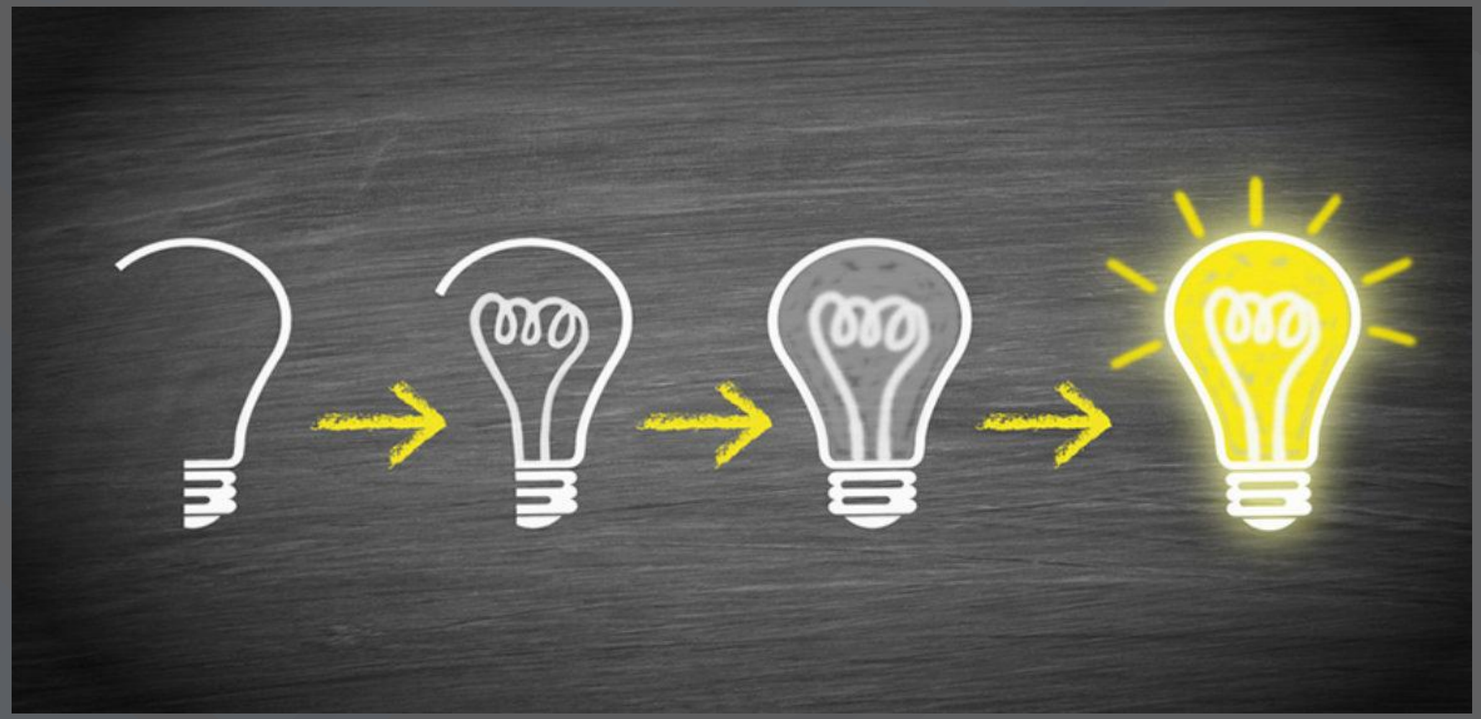
Bank Name: [redacted]
Account Number: [redacted] 337 63339
ABA Routing: 03117[redacted]
Bank Address - [redacted], MN, [redacted]
Account Name: Tripple [redacted]
Beneficiary Address [redacted], CA [redacted]

BUSINESS EMAIL COMPROMISE #2

- ✓ Large Company (Mainly Cloud)
- ✓ “Survey” Phishing Email Sent
- ✓ Attackers Logged into Outlook365
- ✓ 30 People Fell for the Phish
- ✓ 29 People Didn’t Get Paid

LESSONS LEARNED: BUSINESS EMAIL COMPROMISE

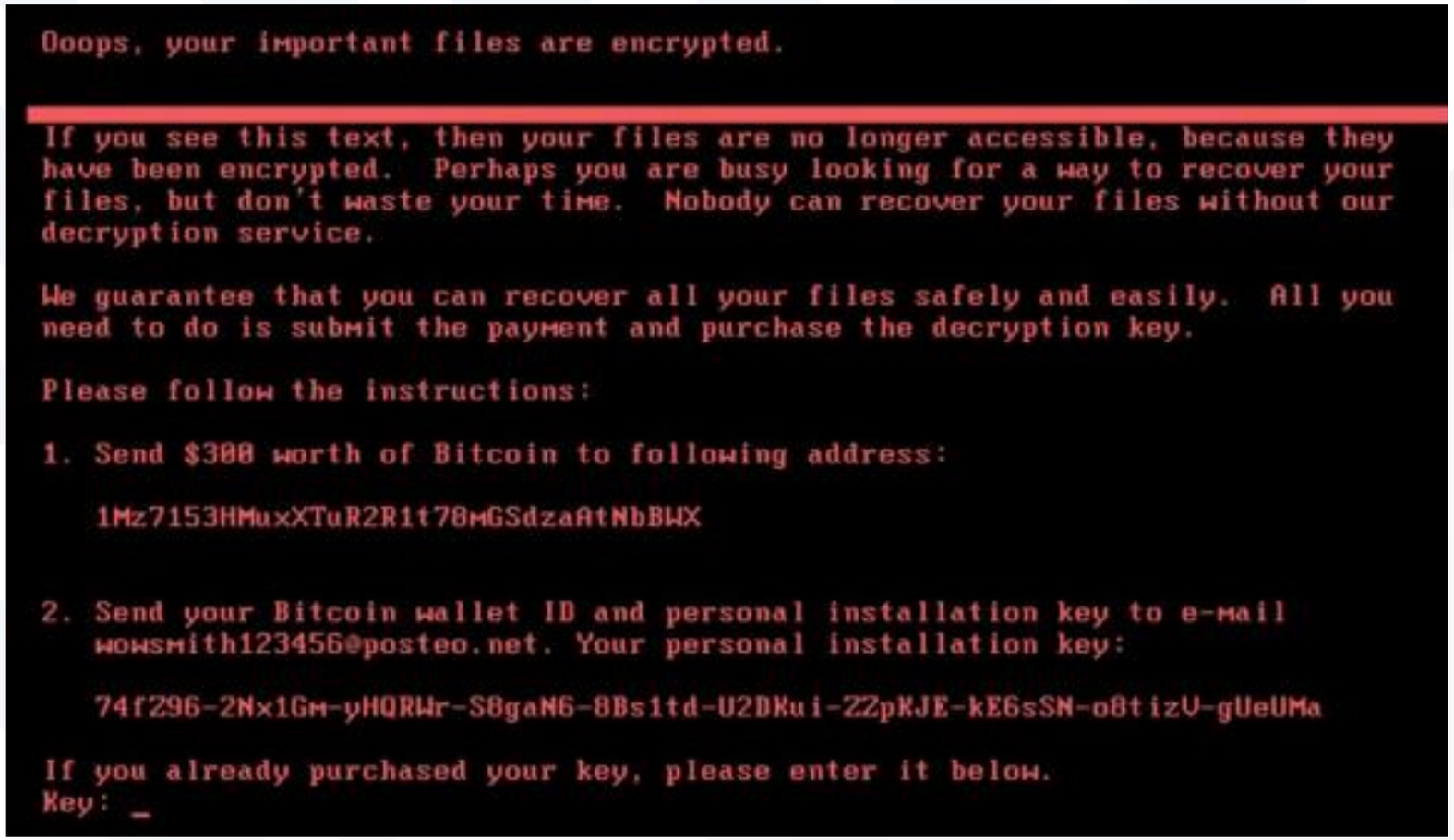
- ✓ Multi-Factor Authentication
- ✓ Turn Off Unneeded Features
- ✓ Geo-Blocking
- ✓ Ensure Extensive Logging
  - Import into SIEM
- ✓ Alert on:
  - Rule Creations
  - Sending “On Behalf” or “Send As”
- ✓ Set [External] Tag for External Emails
- ✓ Phishing Assessments



RANSOMWARE - COMMODITY

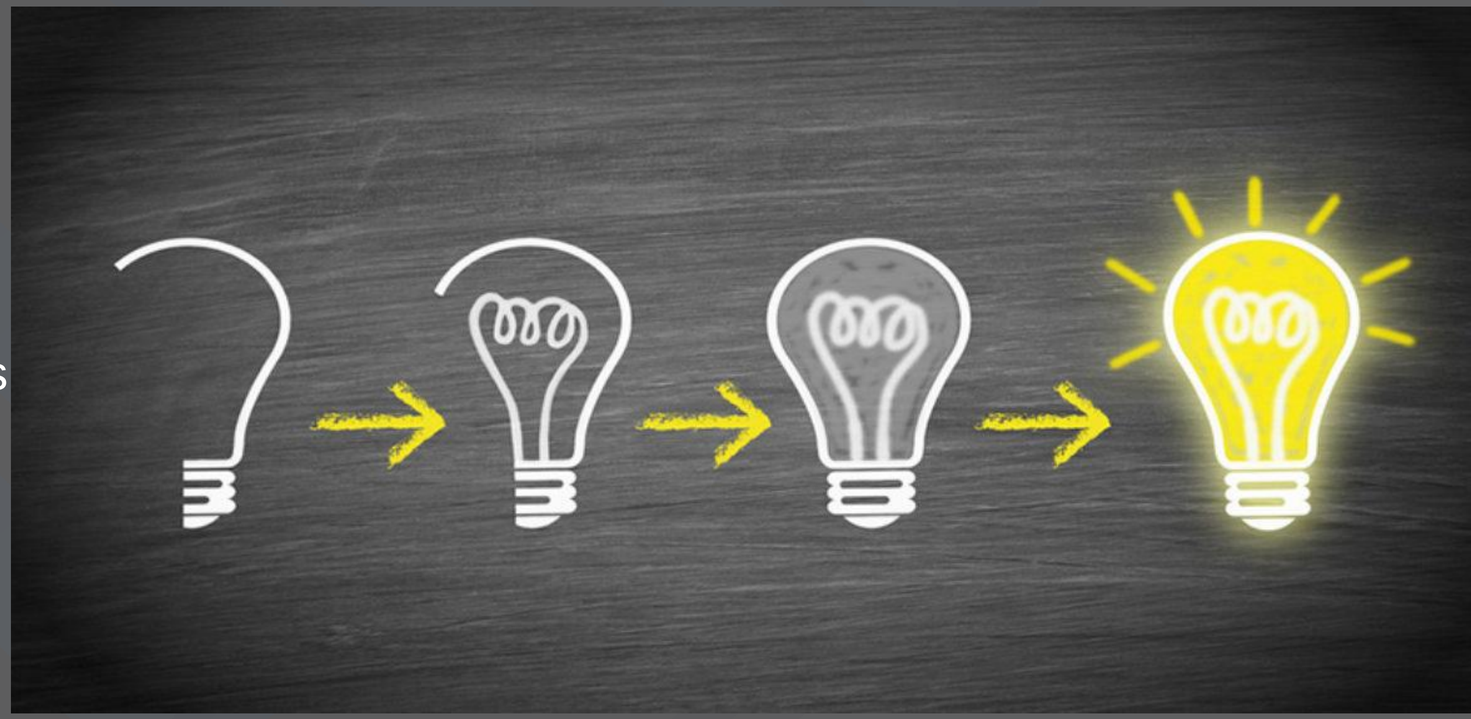
RANSOMWARE - TARGETED

RANSOMWARE - WEAPONIZED



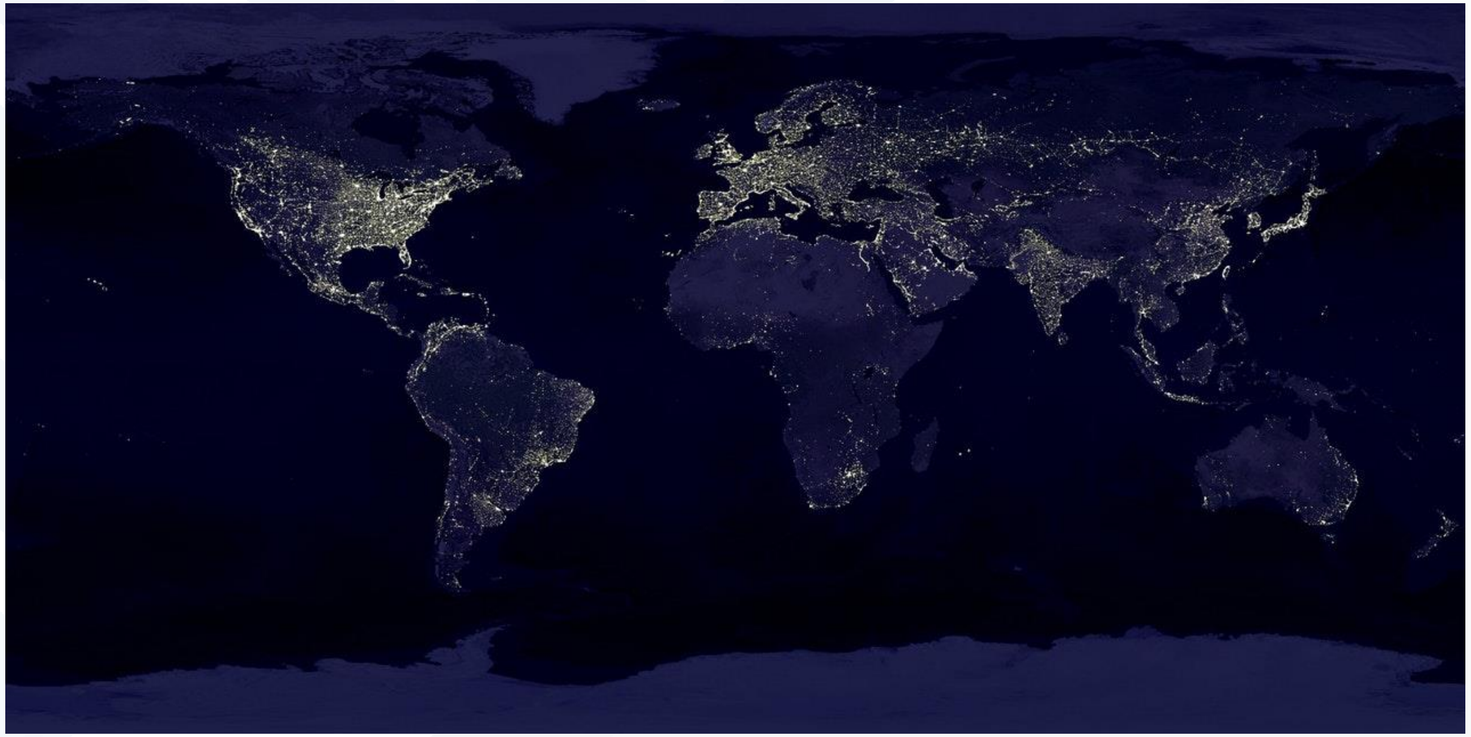
LESSONS LEARNED: RANSOMWARE

- ✓ Mature & Tested Backup Process
- ✓ Vulnerability Management & Patching Processes
- ✓ Disable Active Content in MS Office Documents
- ✓ Implement Least Privilege for Network shares
- ✓ Block TOR & P2P at Perimeter
- ✓ Block Uncategorized & Unknown Websites
- ✓ HIDS/HIPS Where Possible
- ✓ Next-gen AV Controls
- ✓ Security Awareness Training



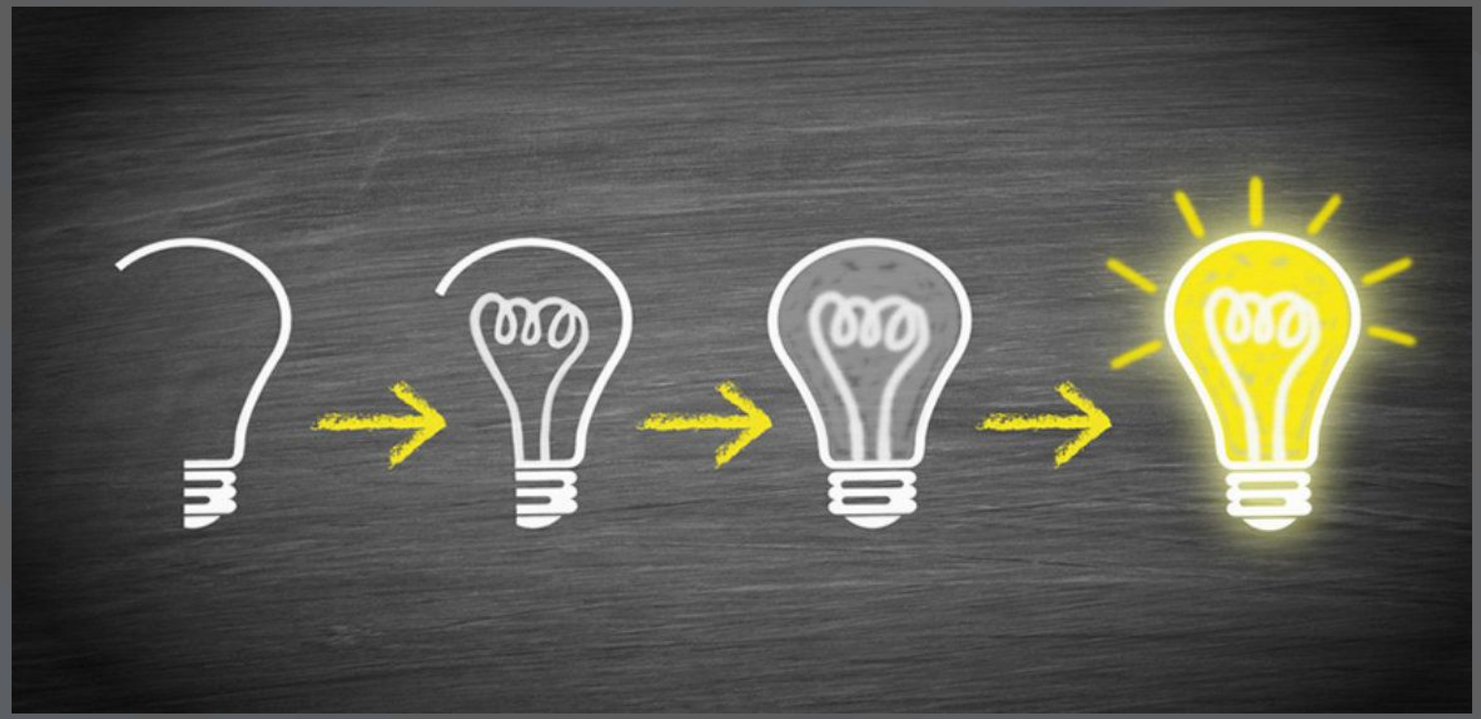
NATION STATE ATTACKS: OPM

- ✓ “Odd” Network Traffic Identified
- ✓ Source Binary was “McAfee” Related
- ✓ Known “Breach” from March 2014..
  - ✓ “No Big Deal”
- ✓ “PlugX” Malware (RAT) Found
  - ✓ “JumpBox” Was Infected
- ✓ Credentials Tied Back to Vendor
  - ✓ That Had a Previous Breach
- ✓ Access to 21 Million Employee Records
    - ✓ 5.6 Million Fingerprints
- ✓ Full Extent of Breach… Unknown
- ✓ Objectives…Concerning



LESSONS LEARNED: OPM

- ✓ Multi-Factor Authentication
- ✓ Partner Breaches Matter
- ✓ Not All Malware is Equal
- ✓ Not All Machines are Equal
- ✓ Look for “Typo-Squatting”
- ✓ We Are in Trouble



YAHOO DATA BREACH

YAHOO DATA BREACH: LESSONS LEARNED

FINAL EXAM

- ✓ What Have We Learned?
- ✓ How Will You Improve?
  - ✓ Controls
  - ✓ Security Testing
- ✓ Credit the Pain of Others

> "DON'T DEPEND ON THE ENEMY NOT COMING; DEPEND RATHER ON BEING READY FOR HIM."
>
> –SUN-TZU

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Bill Dean

Senior Manager, LBMC Information Security

@billdeancce