Mock Incident Walk-through:

All your networks r belong to us (muwhahahaha!)

(ISC)2®
SECURITY TRANSCENDS TECHNOLOGY®

Agenda

- A Brief Introduction
- What is ISC2?
- What is an Incident and how do I know I’m having one?
- 2014 Reddit-Apocalypse
- Questions

A Brief Introduction

- Joe Daw - Information Security Manager for Jones Day, (ISC)2 Chapter President
- Christopher Robinson aka CRob –InfoSec Architect for the Westfield Group, (ISC)2 Education Officer
- Combined over 30 years Enterprise Engineering/Operations, Management, Strategic Planning, and Security experience

What is ISC2 and what's a CISSP?

- International Information Systems Security Certification Consortium
    - A global non-profit recognized as a leader in educating and certifying security professionals
- Certified Information Systems Security Professional

The recognized "Gold Standard" for confirming security experience and knowledge. The CISSP has worldwide recognition of competence

(ISC)²
SECURITY TRANSCENDS TECHNOLOGY

Why should I care about “Incidents”

- Anyone can be a target. No, you’re not too small and no you don’t not have anything of value.
- 80% of all attacks in 2012 were a result of password guessing/reusing valid credentials.
- Phishing (attacks via email) are the go-to attack vector; chances are if you have email, you’ve been phished.
- Most breaches (62%) take months or years to discover. Sadly, 70% of those breaches are reported back to you via an external entity.
- 2012 had 855 documented incidents involving over 174 millions compromised records. - 2012 Verizon Breach Report

Krebs on Security tells us….

YOU ARE A TARGET

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- *Your bank or financial accounts, where they can steal or transfer your money.*
- *Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.*
- *Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.*
- *Your UPS or Fedex accounts, where they ship stolen goods in your name.*

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- *All the names, email addresses and phone numbers from your contact list.*
- *All of your personal or work email.*

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- *Your online gaming characters, gaming goods or gaming currencies.*
- *Any software licenses, operating system license keys, or gaming licenses.*

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- *Sending out spam to millions of people.*
- *Launching Denial of Service attacks.*

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

www.securingthehuman.org/ouch

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- *Your Facebook, Twitter or LinkedIn account.*
- *Your email accounts.*
- *Your Skype or other IM accounts.*

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- *Hosting phishing websites to steal other people's usernames and passwords.*
- *Hosting attacking tools that will hack people's computers.*
- *Distributing child pornography, pirated videos or stolen music.*

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- *Your credit card information.*
- *Your tax records and past filings.*
- *Your financial investments and retirement plans.*

Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- *Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.*
- *Encrypting all the data on your computer and demanding payment to decrypt it.*
- *Tracking all websites you visit and threatening to publish them.*

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com

The Cyber-Incident

The Stages of an Incident

- Preparation
- Identify
- Containment
- Eradicate
- Recover
- Lessons Learned

Who are we?

We will be playing the part of technology and business people from:

The Great Rivers Brewery (GRB) makers of

- Gruss Von Krampus – a delightful winter ale
- The Bear Hunter – a nutty and sweet brown ale
- Bear Attack! – a crisp Belgian Ale
- Cthulhu-weizen – an insanely good Hefeweisen

The Players

The Players

- The “Ops” Team – technologists who manage the infrastructure and implement the software that helps run the company.
- The Security Team – policy and process focused, no direct contact with impacted systems.
- Senior Management/HR – The leadership of the company, no technical skills, focused on the business.

And our VERY special guest….

Kathy Nagy – Contingency Planners of Ohio - Vice President , Business Continuity Manager

WAT?

Kathy takes a moment to explain the differences between:

- BCP – Business Continuity Planning
- DR – Disaster Recovery
- IR – Incident Response

The Incident….

Oh Reddit, you're such a scamp!

You are contacted by a client that "GRB data" was found in the same location as recently-leaked "provocative celebrity selfies"

Externalizing Circumstances…

While reviewing access to the data, it is noted that 4 employees and 1 3rd Party contractor had recently touched the data.

Login of “External_Karl” from “We Do Stuff Consulting Inc.”

E.T. Phone Home

During the investigation, as the Ops team is in the server room……

the distinct sound of a modem connecting is heard

SIEM's shady to me….

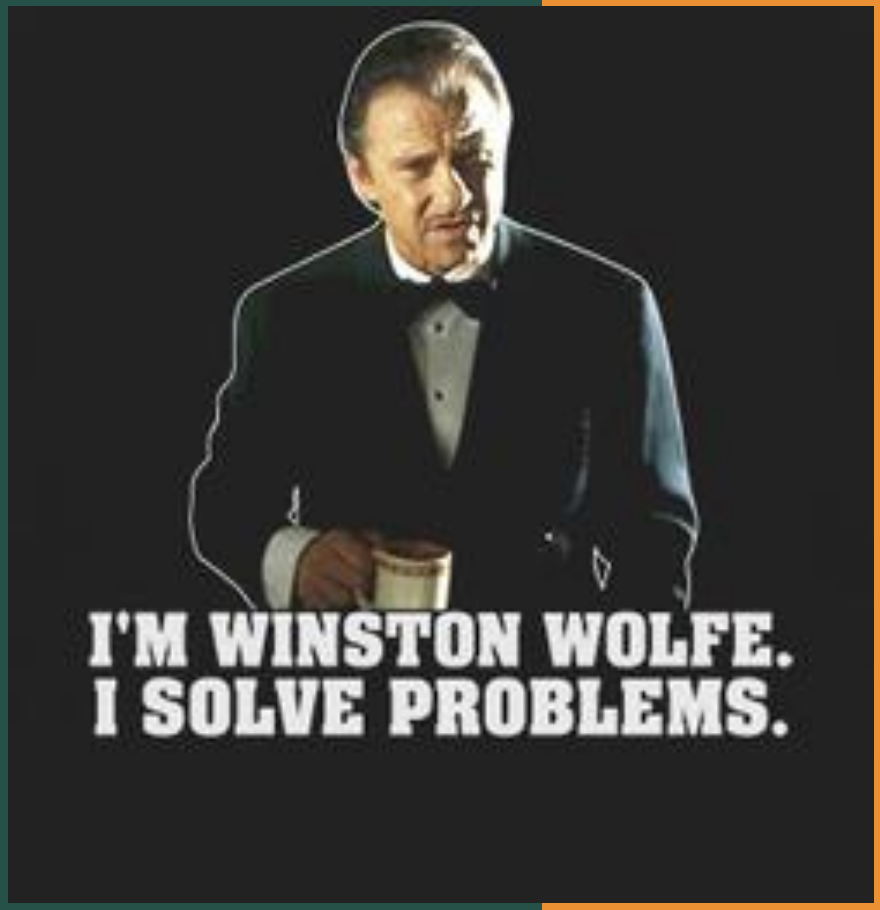
- Review of data in SIEM shows data leaving via "webservice" service.
- Karl created the service account.
- The ID is still enabled and is running on executive's laptop.

Call the Cleaner

What path do we take: prosecution or eradicate?

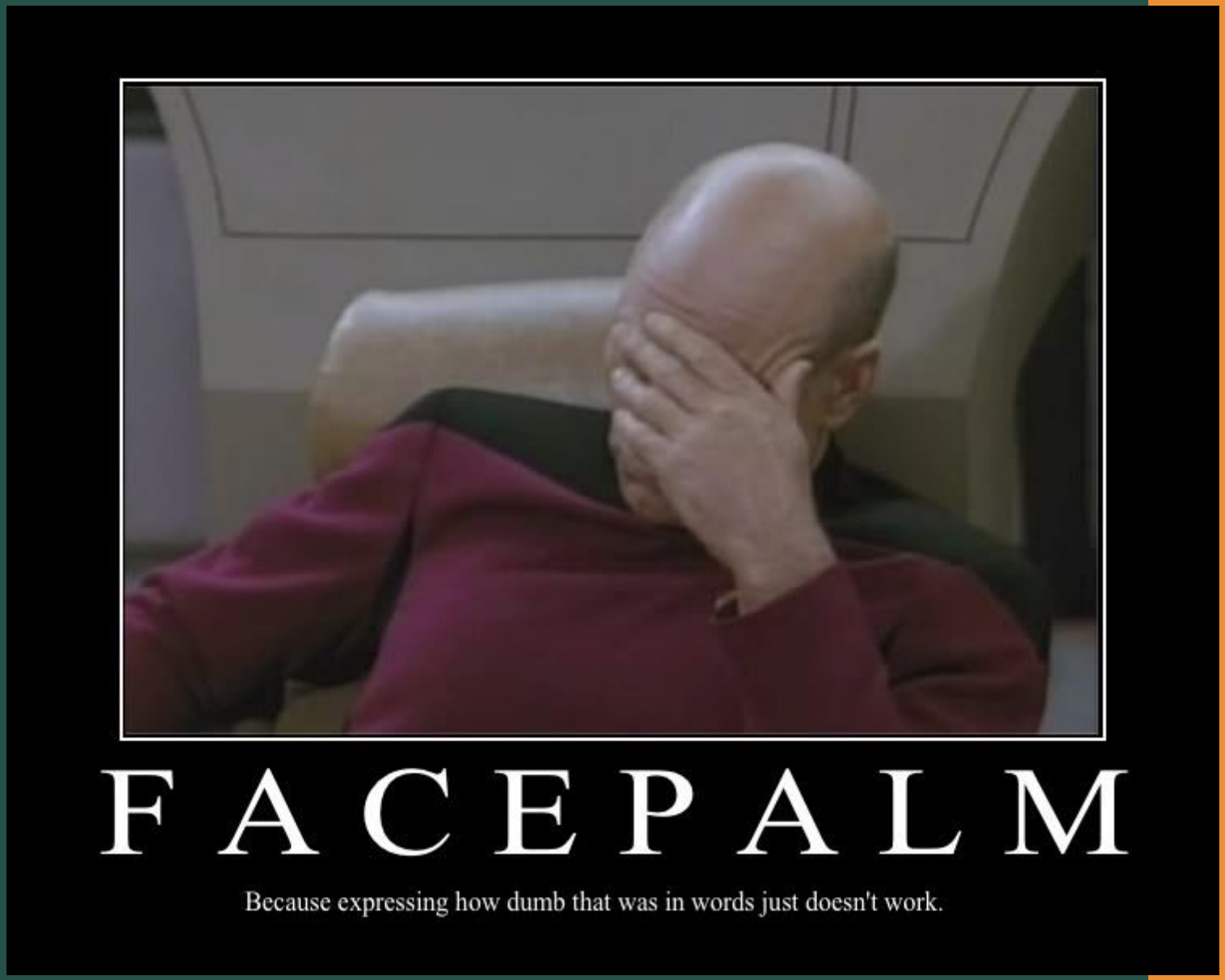
Who should do this?

What needs done?



Overzealous Response

We have an issue though: Nick Burns, from Desktop, decided to eradicate any risk to the compromised box, he already wiped and rebuilt it.



Lessons Learned?

The 10 Principles of Incident Response

1.) Assign an executive responsible for the plan.

2.) Develop a taxonomy of risks, threats, potential failure modes.

3.) Develop easily accessible quick-response guides for likely scenario.

4.) Establish processes for making major decisions.

5.) Maintain relationships with key external stakeholders, such as law enforcement.

6.) Maintain SLAs and relationships with breach-remediation providers/experts.

7.) Ensure the documented response plan is available to the entire organization.

8.) Make sure staff members understand their roles and responsibilities.

9.) Identify individuals who are critical for incident response and ensure redundancy.

10.) Train, practice, and run simulated breaches.

An Incident Handling Process for Small and Medium Businesses

http://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791

Cleveland ISC2 Chapter

- Our Goal – To Educate, Inspire, and Entertain
  - Focused on the entire InfoSec Professional
  - We meet the last Tuesday of every* month at 5:30pm at varying locations (generally in/near Independence, Ohio)
  - Great guest speakers from Security, Business, Education and other fields.
  - Excellent peer-to-peer conversations on relevant InfoSec issues.

Visit http://www.isc2chapter-cleveland.us/ for more details!

*every month, mostly

(ISC)² SECURITY TRANSCENDS TECHNOLOGY

ThankYouThankYouThankYouThankYou

Thanks to Drayton Graham, Robert Netgen, Chris Bush, Kathy Nagy

Questions?