Assessing Risk in a Breached World

The Role of the Compromise Assessment

Presented by

Chris Gerritz
CEO & Co-founder, Infocyte
The “New” Bank Heist

Central Bank of Bangladesh
February 2016

Hackers made off with $81MM they infiltrated the bank and initiated $931MM in SWIFT transfers from their Federal Reserve Bank of New York account.

Hackers were key logging for “several weeks” before initiating the attack - FireEye Report

Malware took control of the banks Swift Alliance Access (SAA) servers and operator workstations
Speaker History

Previously established the Air Force’s Enterprise Hunt Team

Chris Gerritz  
CEO & Founder of Infocyte, Inc.

Previously:  
*Chief, Counter-Cyber Operations*  
*Air Force CERT*
Measuring Security Risk

Current State of Network Security Assessments
Types of IT Risk Assessments

**Compliance Assessment**
Identifies an organizations’ state of compliance with various regulatory requirements and policies. i.e. NIST Cybersecurity Framework.

**Vulnerability Assessment**
Identifies known security weaknesses in targeted systems.
- External Network
- Internal Network
- Application

**Penetration Test**
Attempts to duplicate the actions of an attacker with the goal of finding weaknesses that could allow an attacker to access the enterprise environment.
Vulnerable Software

13,073
Vulnerabilities discovered in 2013.

Unintended Features
What it wasn’t designed to do, but it does

Missing Features
What it was designed to do, but it doesn’t

Intended Design

Final Result

Limited Resources + Deadlines = Software Vulnerabilities

Sources: Secunia 2014 Vulnerability Review
Ok so we’re vulnerable. What are we missing?
Persiant Compromises

Michaels – Jan 2014
“Payments at their stores were potentially exposed between May 8, 2013 and January 27, 2014 [8 Months]” – Forbes, Jan 2015

Home Depot – Sept 2014
“The malware [...] swiped account information of unsuspecting customers for five (5) months before detection” – US News, Nov 2014

Sony – Nov 2014
“It’s unclear when the hack began. One interview with someone claiming to be with [the hacker group] said they had been siphoning data from Sony for a year” – Wired, Dec 2014

Office of Personnel Management (OPM) – June 2015
“OPM Hack [...] went undetected for more than a year, Sources Say” – ABC News, 11 Jun 2015

Trump Hotels – Sept 2015
“criminals lurked [within their network] for a year” – UK Telegraph
The median time to discover a breach after one has occurred.

Intrusions discovered by internal security processes.

Sources: 2015 Mandiant M-Trends
## Motives for Persistence

### Persistence & Stealth
- Spying
- Corporate Espionage
- Blackmail
- Credit Card Theft
- Botnet Operations
- False Flag Attacks
- Posturing for Future Attack
- Military - Operational Preparation of the Environment (OPE)

### Transient & Loud
- Crypto-Locker
- Web Defacement
- “Smash and Grab” Theft
- Denial of Service
- Destructive Worms

---

VS.
The Problem

- Networks always have a degree of vulnerability
- Organizations are struggling to prevent determined attackers from getting in their networks.
- Skilled attackers can remain hidden for months, sometimes years, before detection.

Without determining the current state of compromise, we have an incomplete picture of information risk.
“Instead of conducting a penetration test to confirm that an attacker can compromise your environment, similar to confirming that water is indeed wet, you should conduct an assessment to determine which adversaries are already operating within your environment. “

- Rick Holland, Forrester (1/26/16)
An objective survey of a network and its’ devices to discover presence of malware and unauthorized access.

To be effective, the assessment should be:

• **Fast** - Assess a large network within hours/days

• **Affordable** - The average organization should be able to conduct it proactively and regularly

• **Independent** - Does not rely on existing security tools
Methods

Some approaches to breach discovery in use today are:

1. **Anomaly Detection & Analytics** on existing logs, connection, and event data to catch what the analysts might have missed (i.e. Splunk queries)

2. **Monitor** the network with new/different security sensors. (i.e. passive DNS monitoring)

3. **Actively scan devices** for indications of compromise, multiple AV engines, artifacts & malicious behavior (i.e. Hunt/IR solutions)
Case Study: Banking & Finance

Organization
- The **acquirer** is a major financial institution based in the US with over a trillion dollars in assets.
- The **acquiree** is a ~50 employee wealth management firm in the US serving high net worth clients and managing over a Billion dollars in assets.

Challenge
- As part of M&A due diligence, the acquirer needed to independently verify the integrity of the acquiree's IT systems and ensure no breaches had occurred.

Solution
- Compromise Assessment

Results
- Remotely scanned, analyzed, and validated 54 workstations and servers. Five (5) days from install to delivery of final report.
- Showed the acquiree had strong technical controls, regular security hygiene (i.e. nightly reboots), and IT policies in place to protect the network.
- Provided an overall **clean bill of health** for the network ensuring confidence for the transaction to progress.
- Evidence of suspicious foreign remote access to the network was verified as an authorized technical support organization.
Use Cases

**Data Breach Insurance**  
Pre-existing conditions check

**Mergers & Acquisitions**  
Due Diligence

**Vendor Management**  
Independent 3rd party verification

**GRC / IT Audit**  
Annual/Quarterly