After the Attack

The Transformation of EMC Security Operations

Thomas Wood
Senior Systems Engineer, GSNA | CISSP
RSA, The Security Division of EMC
Thomas.WoodJr@rsa.com
Agenda

- Review 2011 Attack on RSA
- Threat Landscape
- Key functions of a Security Operations Center
- The Tyranny of The News Cycle
- Organizational Impact
- RSA ACD & ASOC
The Environment

- ~2,000 security devices
- ~55M security events per hour
- ~60K employees
- 350 sites
- 85 countries
- Core Intellectual Property
EMC “SWAT” – 2005

Basic security tools
- Firewalls
- Anti-virus
- Authentication

Handful of skilled practitioners
- Knows how the tech works
- Understands the different parts of the business / IT
Structure of Pre-Breach CIRC

- Eyes on Glass
- Analysis
- Forensic
- Coordination
- Remediation
- Rule/Report Creation
- Workflow Development
Technology Pre-Breach

Security Operations (RSA Archer)

Security Controls

Data Discovery (RSA DLP)

RSA SIEM

Incident Tracking

Vulnerability Risk Management

Firewall

IPS

Proxy

AV

Windows Clients/Servers

File Servers

Databases

NAS/SAN

Endpoints

Log Analysis

Reporting

Event Forensics

Limited Real-Time Response

Limited Visibility
The Attack

Companies can’t stand against the armies of nation states. Why do we believe we can stand against their cyber army?

*Sam Curry, RSA*
The Initial Vector in the RSA Attack

1. **2 Phishing emails**
   Some clues about the email lead us to believe that this was from some slightly dated research on employees

2. **Launch Zero-day**
   One user opened email attachment (an Excel spreadsheet) which launches a flash zero-day

3. **Attacker gains access to other machines**
   Zero-day exploit installs backdoor (Poison Ivy Rat Variant) which enables extraction of memory resident password hashes
From Compromise to Exfiltration

4 Attacker initiates separate network using credentials obtained from steps 1 - 3

5 Attacker moves laterally through organization, heavily using escalation of privileges, to systems containing disparate information that when combined allowed compromise of RSA SecurID-related information

6 Attacker removes data and stages it on a file share within the network

7 Files are encrypted and attacker tries to ex-filtrate to several servers before finding a successful destination.

External Server
Additional RSA Attack Details

- **Focused and coherent attack**
  - Times of attack were choreographed
  - Attacker moved rapidly to the target: knew what to get and the order to get them
  - **Implication:** Significant reconnaissance and preparation

- **Leveraged Prior Experience**
  - Exploited people and processes more than weaknesses in infrastructure
  - Remote (attacker) hosts were modified to match internal naming structure
  - Very detailed knowledge of the people, process, & infrastructure
  - **Implication:** People continue to be the easiest target

- **Fresh malware was used**
  - Compiled 6 hours before the event
  - **Implication:** Malware was specifically customized; no known signature to block

General list of Command and Control Domains for RSA attack were published in a longer list in the US-CERT EWIN 11-077-01A. The important ones include: *.mincesur.com, *.hopto.org, *.cz88.net
The Business Impact

• $70 Million Write-Down
  – Cost of remediation, IT, investigation, consulting, lost revenue, lost productivity

• Six months focused on remediating authenticators

• All Authentication-related marketing & sales activity stopped for 6 months

• Impact to trust
  – Customers: how could you do this to us? Why didn’t you contact us first (10-15K customers)
  – Lost some customers permanently

• All despite no risk to customers
Present Reality

*The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him.*

- Sun Tzu, *The Art of War*
Traditional Security Is Not Working

99% of breaches led to compromise within “days” or less with 85% leading to data exfiltration in the same time

85% of breaches took “weeks” or more to discover

Source: Verizon 2012 Data Breach Investigations Report
Advanced Threats Are Different

1. TARGETED SPECIFIC OBJECTIVE
2. STEALTHY LOW AND SLOW
3. INTERACTIVE HUMAN INVOLVEMENT

TIME

System Intrusion  Attack Begins  Cover-Up Discovery  Cover-Up Complete
Leap Frog Attacks

1. Decrease Dwell Time
2. Speed Response Time

15

Dwell Time  Response Time

Response

Attack Identified

© Copyright 2014 EMC Corporation. All rights reserved.
What’s Old Is New Again

The consequence of it is, \{215\} that the United States are to a certain extent in the situation of a country precluded from foreign Commerce. They can indeed, without difficulty obtain from abroad the manufactured supplies, of which they are in want; but they experience numerous and very injurious impediments to the emission and vent of their own commodities. Nor is this the case in reference to a single foreign nation only. The regulations of several countries, with which we have the most extensive intercourse, throw serious obstructions in the way of the principal staples of the United States.

Alexander Hamilton
REPORT ON MANUFACTURES
DECEMBER 5, 1791
Online Trust Alliance Guide to Data Protection and Breach Readiness (2013)

- 2,644 Breaches
- 267 Million Records
- $5.5M cost per Breach
- $194 cost per Record
- 99% records lost due to external hacking
- 97% of data breach incidents were avoidable

• Victims
  - 37% financial
  - 24% retail & restaurants
  - 20% manufacturing

• Perpetrators
  - 92% outsiders
  - 19% state-affiliated actors

• Mode
  - 76% exploit weak/stolen credentials
  - 75% financially motivated

• Discovery
  - 69% by external parties
  - 66% took months or more to discover
Verizon Report Recommendations

- Eliminate unnecessary data
- Collect, analyze, share
  - Incident data
  - Threat intelligence
- Focus on better and faster detection
- Evaluate threat landscape
The Adversary

NATION STATE ACTORS
- Nation states
  - Government, defense contractors, IP rich organizations, waterholes

CRIMINALS
- Petty criminals
  - Unsophisticated, but noisy
- Organized crime
  - Organized, sophisticated supply chains (PII, PCI, financial services, retail)

NON-STATE ACTORS
- Insiders
  - Various reasons, including collaboration with the enemy
- Cyber-terrorists / Hacktivists
  - Political targets of opportunity, mass disruption, mercenary
Understanding the threat

Attack Lifecycle

- Recon
- Weaponization
- Delivery
- Exploitation
- Installation
- C2
- Act on Objectives

7-Phase Model for how an adversary engages a victim

Any disruption in the chain will impact their actions

Human intervention is often required for success and failure

All seven steps can be detected, prevented, or minimized

Note/Attribution: 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains'; Hutchins, Cloppert, Amin, Lockheed Martin CIRT; Proceedings of the 6th International Conference on Information Warfare, 2011
## Objective: Affect the Attack Lifecycle

<table>
<thead>
<tr>
<th>Attack Lifecycle</th>
<th>Detect</th>
<th>Deny</th>
<th>Disrupt</th>
<th>Degrade</th>
<th>Deceive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Weaponize</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Delivery</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Exploitation</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security Is Becoming A Big Data Problem

• More determined adversary means more data needed to identify attacks
• More complex IT environment means even simple attacks can hide in plain sight
• Security professionals are struggling to keep up\(^1\)
  – 40% of all survey respondents are overwhelmed with the security data they already collect
  – 35% have insufficient time or expertise to analyze what they collect

\(^1\) EMA, The Rise of Data-Driven Security, Crawford, Aug 2012
Sample Size = 200
Today’s Security Requirements

**Big Data Infrastructure**
“Need a fast and scalable infrastructure to conduct short term and long term analysis”

**Comprehensive Visibility**
“See everything happening in my environment and normalize it”

**High Powered Analytics**
“Give me the speed and smarts to discover and investigate potential threats in near real time”

**Integrated Intelligence**
“Help me understand what to look for and what others have discovered”
Desired State

- Protect organizational mission
- Evolve with the threat environment
- Operational efficiencies & best practices
What SOC/CIRCs Need:

**BROAD VISIBILITY & DETECTION**
Fusing together massive amounts of telemetry data & threat intelligence to detect even the most advanced attacks

**CONTEXT**
Knowing which IT assets are important and the location of sensitive data drives investigative efficiency and prioritization

**FAST INVESTIGATIONS**
Complete investigations in minutes versus hours

**REMEDIATION & OPERATIONS MANAGEMENT**
Workflow driven incident response and SOC/CIRC operations management
People & Process

Technology requires talent and discipline