# Anatomy of a Breach

Lessons Learned

Susan Ramsey, Security Engineer

NCAR

# Attack

In February of 2014, an intruder broke into an NCAR webserver and exfiltrated 47,333 mailing list user accounts.

# The Open Door

Webserver Running:
Solaris 10
Apache
MySQL
Old OPeNDAP cgi script

# Discovery

Bro Reported High CPU Loads on the host

Staff Logged in and found active intruder
…exfiltrating data, exec’ing scripts

# Response

Immediate (Pulled the Plug)

- +5 Hours (Logs)
- +15 Hours (Staff)
- +17.5 Hours (SEG)
- +18.5 Hours (SEG Responds)
- +20 Hours (Victims Notified)
- +More Than 1 Day Later (Executive)

# What Went Right

Event Alerting Worked
The Attack was Confined
The Vulnerability was Identified

# What Went Right

Security Playbook Referenced

...Mostly Followed

Members Contacted Within 24 Hours

...Advised to Change Passwords

# The culprit? ...OPeNDAP cgi script

OPeNDAP is a framework that simplifies all aspects of scientific data networking.

OPeNDAP provides software which makes local data accessible to remote locations regardless of local storage format.

OPeNDAP also provides tools for transforming existing applications into OPeNDAP clients (i.e., enabling them to remotely access OPeNDAP served data).

OPeNDAP software is freely available.

# What Went Wrong

Old Code - Never Updated or Patched

OPeNDAP Script Never Identified as Risk

Logs Analyzed _5_ Hours Later

# What Went Wrong

Security Was Contacted _18_ Hours Later
Legal and Media Relations _NOT_ Contacted
Executive Board Not Consulted _Before_
...Notification Sent to Affected Users

# Follow Up

Security Playbook Updated to Notify

- Executive Management
- Legal
- Media/Communications

Still Concerns Over Legacy Scripts

...i.e. Not Detected by Nessus Scans

# But, You Say, It’s Just a Mailing-List…

MD5 Hashed Passwords are Easily Cracked
People Re-Use Passwords
Nice Start for a Spear-Phishing Campaign
…or Two ….or Three
It’s Still a Failure to Protect Privacy

# More Risks…

Members' Addresses Were in the Database

...Snailmail Phishing/Spam

Members' Affiliate Type (MIL, GOV, LAB)

...Can be used to guess other accounts

Department Name, and Profession

...More phishing, Org knowledge