Introduction

- Bejtlich ("bate-lik") biography
  - General Electric, (07-present)
  - TaoSecurity (05-07)
  - ManTech (04-05)
  - Foundstone (02-04)
  - Ball Aerospace (01-02)
  - Captain at US Air Force CERT (98-01)
  - Lt at Air Intelligence Agency (97-98)
- Author
  - Tao of Network Security Monitoring: Beyond Intrusion Detection (solo, Addison-Wesley, Jul 04)
  - Extrusion Detection: Security Monitoring for Internal Intrusions (solo, Addison-Wesley, Nov 05)
  - Real Digital Forensics (co-author, Addison-Wesley, Sep 05)
  - Contributed to Incident Response, 2nd Ed and Hacking Exposed, 4th Ed
  - TaoSecurity Blog (http://taosecurity.blogspot.com)
Lessons from The Cuckoo’s Egg

Originally published in 1989
In 1990, PBS’ “Nova” aired “The KGB, the Computer, and Me.”
Cliff Stoll was a Lawrence Berkeley National Laboratory astronomer assigned to be a Unix system administrator in his lab.
It Started with 75 Cents

In August 1986, Stoll’s supervisor Dave Cleveland asked Stoll to resolve a $0.75 accounting error.
Hunter

Stoll determined the user “Hunter” was responsible for the $0.75 discrepancy.
Stoll deleted the Hunter account.
Third Party Notification

Shortly thereafter Stoll’s boss received an external notification from the owner of NSA’s “dockmaster” computer that someone from LBNL was trying to log into dockmaster.
Engage the Incident Response Team

Cleveland passed the issue to Stoll. Stoll realized that user “Sventek” was trying to log into dockmaster.
The First Intrusion Detection System for LBNL

Stoll programmed his terminal to beep every time someone logs in!
After 100s of Logins

Stoll caught user Sventek logging into the LBNL network.
Engage the Network Team

Working with the network team to trace the line associated with Sventek’s login, they determined it is an outside connection with 50 possible lines.
Instrumenting the Network

To instrument the network, Stoll borrowed 50 printers from LBNL users and attached one to each of the 50 lines he needed to monitor.
Surrounded by printers, Stoll stayed overnight hoping to catch Sventek logging into LBNL.
During the night, Sventek logged in and generated eighty feet of logged activity!
Local Privilege Escalation

Reading the logged activity, Stoll realized the intruder exercised a local privilege escalation vulnerability to become root. The problem resided in the movemail function in GNU Emacs.
Improving the Instrumentation

Stoll bought equipment for monitoring at Radio Shack (of course).
Serial Line Intrusion Detection System

Stoll and colleague Lloyd Bellknap attached a logic analyzer to the lines, and programmed it to activate a dialer that will call Stoll.
Watch for Sventek

The logic analyzer watched for “sventek” on the serial lines.
Rather than assuming the system just works, Stoll validated the alerting mechanism before Sventek returned.
24x7 Coverage

Now Stoll can wait for his LBNL IDS to call him at home when Sventek logs in.
Stoll programmed a pager to sound when Sventek logs in. His girlfriend Martha disapproved.
Sventek logged in again and Stoll analyzed the activity.
LBNL Is a Stepping Stone

Stoll observed logins to .mil and .gov computers.
The intruder consistently created several accounts on compromised computers.
Accounts Created by Intruder
Accounts Created by Intruder

Jaeger
Accounts Created by Intruder
Get the ISPs Involved

LBNL relies on Tymnet for connectivity, so Stoll asked them for help.
More ISPs

Tymnet turned to Pacific Bell for assistance.
Tracing the Next Login

Stoll enlisted the Oakland District Attorney to authorize tracing the calls to try to determine who is logging into LBNL.
When Sventek returned, Stoll and company began tracing him.
Manual Effort

At least six parties were on the phone trying to determine the origin of the call.
Stymied

Pacific Bell traced the call to VA, but the phone company said Stoll’s search warrant is only good in CA. They wouldn't tell Stoll the origin of the phone call!
Frustrated, Stoll decided to review the logs to identify affected parties.
Enter the CIA

Stoll noticed names, phone numbers, and email addresses of CIA netblocks in WHOIS data.
Stoll decided to call the CIA points of contact directly to tell them Stoll has seen illicit activity involving CIA computers.
Officials from the CIA visited LBNL, but neither they nor the FBI offered help.
Stoll and friends tried to measure latency to determine the intruder’s physical location. They measured 3 seconds RTT.
Statistical analysis of intruder login times showed he preferred accessing LBNL computers at mid-day, Pacific time.
During one trace of Sventek activity, Stoll and friends identified activity originating from outside the US.
The West German Connection

The trace lead to ITT, then to the Bundespost network in West Germany.
Unfortunately the Bundespost network used antique rotary switches from the 1950s.
Rotary Switches

Checking all of the rotary switches to determine the origin of a call required at least an hour!
The intruder spent too little time online. Stoll needed a way to keep the intruder online longer so the Bundespost could complete their manual trace.
Building the Honeypot

Stoll’s girlfriend Martha suggested creating fake documents to lure the intruder into wasting time reading and downloading them, thereby staying connected to LBNL longer.
The ploy worked! In addition to downloading data, a Hungarian spy in the US wrote to an address planted by Stoll in friends, requesting information on the fake “SDINet.”
Six months after starting the investigation, Stoll kept the intruder online long enough for the Bundespost to trace the call to Hannover, West Germany.
Eventually the FBI became interested, but noted at that time there was no extradition treaty with West Germany.
Three years after starting his investigation, Stoll went to Germany for a court case against the intruders.
Dirk Brezinski (programmer) and Peter Carl (contact with KGB) were two of the group conducting espionage on behalf of the KGB.
Karl Koch, aka Hagbard, was a third member of the group. He died in May 1989 under suspicious circumstances after being charged. He supposedly committed suicide in a forest by setting himself on fire.
Markus Hess, the fourth member of the group, was the intruder Stoll tracked.

The German court found the three survivors guilty but the defendants served less than two years probation.
Watch the Show Online!

http://www.youtube.com/watch?v=v1swbLfrP6g
Lessons: Monitoring and Analysis

- “Build visibility in” with local accounting application
- Don’t rely on a single “source of truth”
- Centralized logging defeats intruders deleting local logs
- Passive full content monitoring captures all details without alerting intruder
- Document analysis in log book
- Key questions: scope of intrusion, depth of intrusion?
- Monitoring using discarded gear is better than nothing
- Writing custom tools for monitoring and alerting
- Someone cares: analysis by a person who took the intrusion personally!
Lessons: Nature of the Intrusion

• Intruder exploits weak credentials to gain access
• Intruder leverages local privilege escalation vulnerability
• Intruder exploits trust relationships
• Intruder exploits poor configurations deployed by vendor
• Intruder exploits system monoculture (Unix in the ’80s!)
• Sensitive data accessible from normal network, e.g., cancer treatment equipment
• Systems owners repeatedly told Stoll an intrusion was “impossible – our systems are secure!”
• Recover by reimaging, rebuilding, restore backup?
• External notification is most common detection method
Lessons: Enduring Truths

- Of at least 80 victims, only 2 noticed (LBNL, NSA)
- Agencies ask for information but provide little back
- Users communicate about intrusion compromise opsec
- Intruders violate assumptions held by network owners
- When to monitor intruder, and when to contain him?
- How much is stolen data worth? What is incident cost?
- A variety of analysis techniques provides best results
- Cannot trust endpoints to defend themselves nor report their security state
- Intruders can be creative and persistent
Watch Cliff Stoll’s TED Appearance

http://www.youtube.com/watch?v=Gj8IA6xOpSk
Questions?

KNOW YOUR NETWORK BEFORE AN INTRUDER DOES

Richard Bejtlich
richard@taosecurity.com
taosecurity.blogspot.com