Which rock did you forget to turn over?

MODERN ENTERPRISE INCIDENT RESPONSE

Dave Merkel
Vice President, Products
Reluctant Pitch Man
Security Geek
PKI Nerd
We are MANDIANT

- “Find Evil, Solve Crime.”
- VISA Qualified Incident Response Assessor (QIRA)
- APT and CDT experts
- Located in
  - Washington
  - New York
  - Los Angeles
- Services, software, and education
The threats

Worms and bots
- Indiscriminate Internet users
- Spam, worms, etc.

PII-focused
- Money transfer organizations
- Retailers / POS
- Card issuers
- Equipment manufacturers

Advanced Persistent Threat
- Government / Defense Industrial Base
- Global financial organizations
- Supporting industries
Responding needs a new solution

- Prevent and detect never reach 100%
  - How many incidents start with these alerts?
- Forensic programs aren’t the right tools
  - Can only deep-dive hosts
  - Limited scalability
  - Made for police, not fire
  - Forensically “pulling the thread” not fast enough
- Custom software can be high cost
  - Doesn’t scale from case to case
  - High support cost
MANDIANT Intelligent Response

- Collect indicators from thousands of agents
- Index and search the results
- Live IR on thousands of systems at once
- From disk images to registry keys to live memory forensics
Upcoming events

- **STATE OF THE HACK**
  - Retail Cardholder Data Theft
  - Robbing cash registers over the Internet
- **Thursday, July 9, 2009**
- **At 2 p.m. EDT / 1800 GMT**
- **Presenters:** Michael Graven, Kris Harms and Randy The Customer
- **Register at**
  - [http://www.mandiant.com/](http://www.mandiant.com/)