SANS Forensic Summit
Tactical Incident Response Panel

October 13, 2008

Ken Bradley
Principal Consultant, Federal Services

Kris Harms
Senior Consultant, Commercial Services

Agenda

- How do you answer the following questions from clients after confirming compromise?
  1. How can we quickly determine what type of data was taken?
  2. What are the best ways to determine how the attackers broke into our systems?
  3. Our antivirus is ineffective; how can we detect malware on the hosts on our networks?
- Given the fact that many hackers are versed in anti-forensic techniques…
  1. What anti-forensic techniques are being seen? Which are the most effective?
  2. What are some techniques to aid in the investigation to still gather evidence with this in mind?

How Can We Quickly Determine What Type Of Data Was Taken?

How do you answer the following questions from clients after confirming compromise?

Become Proactive

- **Understand** your *network*
  - Perimeter
  - Internal Separation
  - Authentication
- **Understand** and **Isolate** your *data*
- Maintain log archive
  - Authentications
    - Active Directory
    - VPN Clients
  - Network Requests Traversing Perimeter

What do we own?

Where is it stored?

What access paths exist?

Reactive Assessment

- There is nothing quick about a damage assessment.
- Keep in mind a full quantitative assessment is largely opinion
- Identify $\texttt{VICTIM}^{N}$ → $\texttt{VICTIM}^{0}$ quickly and its connections to the internet
- Timeline analysis
  - MAC times
  - Network Transport Data
- Factor in authentication permissions

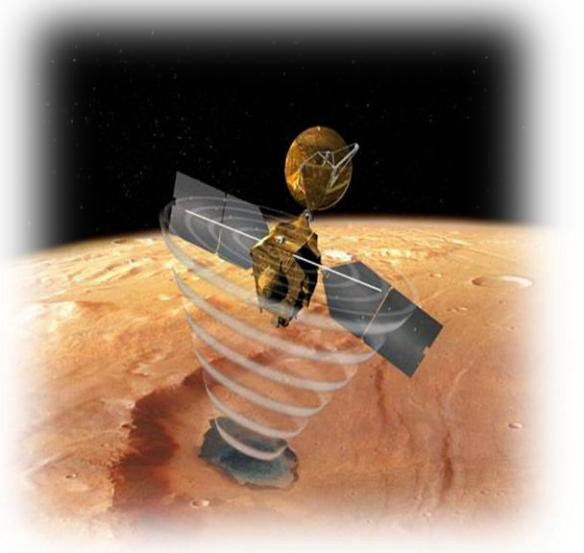
What Are The Best Ways To Determine How The Hackers Broke Into Our Systems?

How do you answer the following questions from clients after confirming compromise?

How *did* they get in?

The quest for Victim 0!

- Understand Your Network
  - Perimeter
  - Authentication Model
  - Internal Segmentation
- Maintain Efficient Log Archives
  - Email
  - Web Applications
  - Databases
- Monitor Network Perimeter Points
  - Netflow
  - Firewall Logs
- Find The Malware



Find Evil. Solve Crime.

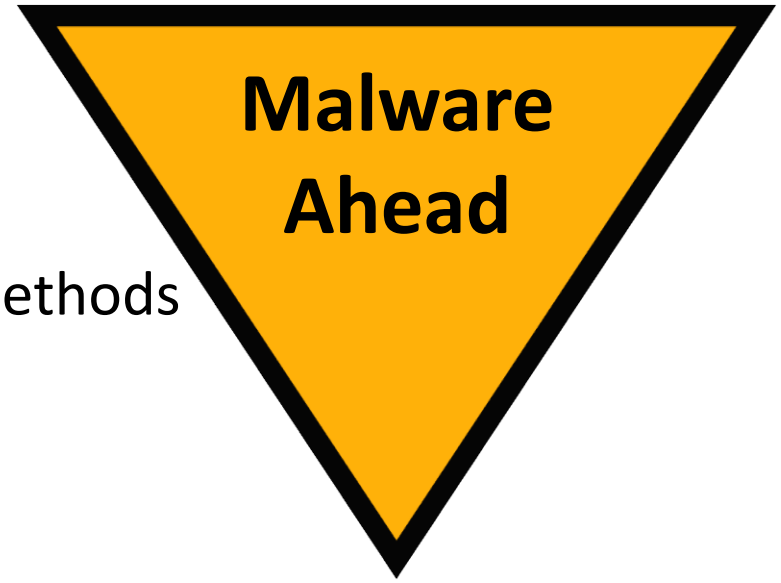
MANDIANT®
INTELLIGENT INFORMATION SECURITY

How Can We Identify Malware On Hosts On Our Network?

How do you answer the following questions from clients after confirming compromise?

Develop and Maintain Effective Indicators

- Balance Network and Host-based Detection
- Enterprise Triage
  - Digital Signatures
  - Entropy Detection
  - Focus on Malware Persistence Methods
- Live Response
  - Agent-based Response
  - Scripts
- Forensic and Malware Analysis
  - Focused on Rapid Indicator Development

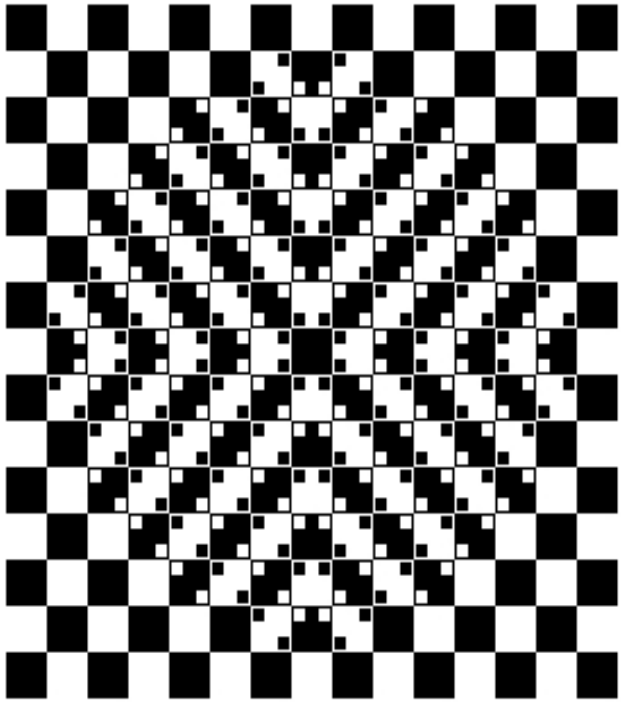


What Anti-forensic Techniques Are Being Seen?

Given the fact that hackers are versed in anti-forensic techniques…

Simplicity, Hiding In Plain Sight

- File Naming Hijacking
  - e.g hinv32.exe
- Process Injection
- Modular Malware
  - Installation
  - Persistence
  - Configuration
- Alternate Data Streams
- Frequent Malware Compilation
  - Armoring
  - Packing
- Dormant Malware Installations



Complexity

- Root Kits?
  - Hacker Defender
  - Custom Driver Performs Hiding
- Custom Command and Control (C2) Protocols
  - Designed to blend into normal HTTP/HTTPS channels
  - VPN split tunnel subversion
  - Internal VPN overlay networks

What Anti-forensic Techniques Are Most Effective?

Given the fact that hackers are versed in anti-forensic techniques…

Effective Evasion Techniques

- Advances in malware persistence
  - Trojaned legitimate system libraries with shell code
  - Typical fport/lsof will ***not*** help
  - Autoruns alone will ***not*** help
- Frequently compiled or configured malware
  - C2 Protocols
  - Host-based signatures
- Custom packing techniques
- Malware that does not touch the disk
- Overwhelm the victim

What Are Some Techniques To Aid The Investigation To Still Gather Evidence With This In Mind?

Given the fact that hackers are versed in anti-forensic techniques…

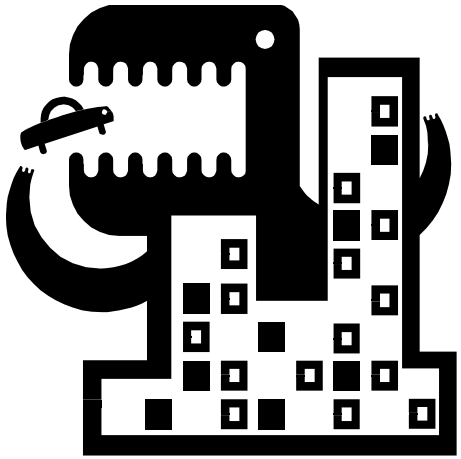
Become Obsessed

- Become an expert
  - Windows Registry
  - Event Log Messages
  - Services / Processes
- Leverage logging mechanisms
  - HIDS
  - Software Management
  - Antivirus
- Develop malware analysis capability
  - Efficient host and network based indicators

MANDIANT®
INTELLIGENT INFORMATION SECURITY

Effective Investigative Techniques

- Focus on the persistence mechanisms
  - Registry
  - Services
- Identify odd PE files
  - Digital Signatures
  - PE Checksum
  - Entropy Detection
- Old-fashioned comprehensive timeline analysis



Questions

MANDIANT®
INTELLIGENT INFORMATION SECURITY

Contact Information

Ken Bradley

Principal Consultant

ken.bradley@mandiant.com

Kris Harms

Senior Consultant

kris.harms@mandiant.com

1.800.647.7020

www.mandiant.com

MANDIANT®

INTELLIGENT INFORMATION SECURITY