Post-Intrusion Problems

Pivot, Persist, and Property
Your Hosts

Cory Altheide

Morgan Marquis-Boire
Our Mission

A framework for thinking about post-intrusion and response to targeted attacks.
Firefighters or Police?
Neither! Counter-intelligence
State Of The Art - Level 1

Most responders focus on "Vulnerabilities & Exploits"

• You can assume 0-day
• These will always exist
• These will continue to change
• Have fun fighting your last battle
State of the Art - Level 2

"Tools, Techniques, and Procedures" - TTP

Usually Tool-Focused

(Understanding the tools is important, but tools don't steal data, actors steal data)

Techniques & Procedures left by the wayside
State of the Art - Level 2

Tools are easy to modify or abandon!

"Don't let yourself get attached to anything you are not willing to walk out on in 30 seconds flat if you feel the heat around the corner."
Defense as a Product
Anti-Virus
Intrusion Detection
Vulnerability Assessment
The "Kill Chain"

http://computer-forensics.sans.org/blog/2010/06/21/security-intelligence-knowing-enemy
Our Approach

Focus on things the attacker *must* do, not things they *happen* to do.

- Pivoting
- Persistence
- Property Crimes

This presupposes a motivated attacker.
Motivation
Focus

Focus on the adversary's goal

Focus on the things they must do to achieve that goal

For opportunistic discovery - focus on what they *generally* do in an operation.
Pivot
Pivoting

Once you're "in", you need to identify and reach your target

Two activities: enumeration & lateral movement

Generally done in parallel (both provide feedback useful to the other)
Enumeration

Mapping the hosts

Identifying users and privileges

Mapping the data
Lateral Movement

Machine -> Machine transition

"Searching for malware identifies only 54% of systems compromised in an incident." - Mandiant M-Trends 2012

Not necessarily a straight line to the "target."
Artifacts Created While Pivoting

Victim Host Artifacts:

- Process / Socket
- Shell history
- Event Logs (logon)
- User profile directory creation
Artifacts Created While Pivoting

Attacker Host Artifacts:

- RDP / SSH / Other related artifacts
- Registry keys (MRUs, mounted shares)
- Various memory-only artifacts - command buffers, IPs, hostnames
Artifacts Created While Pivoting

Network Artifacts:

• Domain Controller / LDAP / Kerberos Logs
• Internal DNS logs
• Internal Netflow
• Internal IDS
Persistence

THE ARMS RACE
A Brief History of Persistence

Trojaned Binaries

Userland backdoors

Hiding in plain sight
A Brief History of Persistence

MBR

VBR

Kernel Rootkits
A Brief History of Persistence

Hypervisor

NIC Firmware

BIOS

Keyboard Firmware
Maintaining Access

Esoteric is not always better (or necessary).
Maintaining Access

Even detecting 'Basic' persistence techniques is done poorly.
Property
"Property"

A catch-all for what the motivated attacker wants to attack

Can be intellectual or actual

Three broad activities:
• Destruction
• Modification
• Theft
Destruction

Virtual:
- `rm -rf /*`
- `dd if=/dev/zero of=/dev/sda`
- secure delete

Physical:
- Stuxnet
- DHS tests
- Soviet gas pipeline sabotage (1982)
Destruction - Investigation

In some cases, destruction is obvious (especially physical)

In some cases, destruction may simply be a distraction from the real goal.

If your attacker's goal was simply destruction, consider yourself lucky.
Modification

Preparing the battlefield: Logic Bombs

Can be used to hide persistence/lateral movement.

Any non-destructive modification of data:
• Addition
• Alteration
• Selective deletion

End Goal: Backdoor addition
Modification - Investigation

File content modification (hashes)

File system time stamps

Revision control logs/verification

Comparison w/ unaltered originals

Backups/snapshotting file systems
Stealing - Who / What

Chinese Hackers
Russian/Ukrainian Financial Hackers
Other Intelligence-focused attacks

Can be focused on:
- Subset of data
- ALL the data
- Continued access to data
A Brief History of Data Exfiltration

File Transfer:
• UUCP
• FTP / SMTP / SCP

Old Skool Obfuscation:
• Base64 + Terminal
• serial line logging
• screen

Tunneling:
• RDP / DNS / ICMP / NTP
A Brief History of Data Exfiltration

Cloud Data Services:
• Dropbox/Box/Google Drive
• MegaUpload/RapidShare/YouSendIt
• Webmail/Webmail Drafts

Flame & USB
P2P
Stealing - Investigation - 1

Network Indicators:
- Netflow
- Network signals (IDS) - outbound compressed data
- DNS logs
- Data Leakage Prevention
Stealing - Investigation - 2

Host Indicators:

- Process executions:
  - Archivers, especially CLI
  - File transfer applications

- Archive files/remnants on-disk

- SQL history files, etc.

- Wall o' A-Times*
Winning the Fight
You are fighting intelligent adversaries
They have a job they need to do
But they are fighting in your house
Aggressive Defense
Hunting Primitives

Ability to generate & log enough network artifacts

Ability to immediately (or automatically) pull relevant host artifacts

Correlation of host & network artifacts into logical events
Effective Hunting

At Google we do this using GRR
• open source incident response framework
• http://code.google.com/p/grr/

Prepare not for what *could* come, but what you know *will* come.
FIN

NOW HIRING

Incident Responders: Zurich

cory@google.com  mmb@google.com