MANDIANT®

Beyond ‘Check The Box’

Powering Intrusion Investigations

PRESENTED BY: Jim Aldridge

27 MARCH 2014

Five Important Capabilities

- Mapping an IP address to a hostname
- Identifying the systems to which a specified account authenticated
- Determining the systems that communicated with a specified Internet IP address
- Tracking domain name resolution attempts
- Identifying indicators of compromise across the environment

Big-Picture Incident Response Questions

1. What information was exposed?
2. Do I need to notify regulators or customers?
3. What is the extent of the compromise?
4. How much money did we lose?
5. How did the attacker gain entry?
6. How do we effectively stop the attack and remove the attacker?

Investigative Questions

- When and what was the earliest evidence of compromise?
- How did the attacker gain entry?
- What is the latest evidence of attacker activity?
- What systems are (or were previously) under the attacker's control?
- What systems did the attacker access?
- What actions did the attacker execute on the systems with which he interacted?
- How does the attacker maintain access to the environment?
- How does the attacker operate inside of the environment?
- What tools has the attacker deployed?
- What accounts did the attacker compromise?

#1: Mapping an IP address to a hostname

- Ensure the logs are enabled
  - DHCP audit logs are located by default at %windir%\System32\Dhcp (Win2k8)
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters\DhcpLogFilesMaxSize (max size in MB)
  - Reference: http://technet.microsoft.com/en-us/library/cc726869(v=ws.10).aspx
- Absent logs, leverage config management software or antivirus to log the changing IP address to hostname mappings
- Collect logs, make searchable, and archive
  - SIEM (ideal)
  - Scheduled task to copy log files off and compress to a central file share daily
    - PowerGREP is your friend

#2: Systems to which a specified account authenticated

- Log authentication events
  - On all systems!
  - Successful more important than failed
  - Very important, even if you do not have a way to search or aggregate them
- At a minimum, push domain controller logs into a SIEM
  - Or copy off logs to a central location for manual searching
  - This will enable querying Kerberos Service Tickets
  - Realize that you don't have visibility into local account activity
    - Can make up for that by querying data on individual systems, under Capability #5, but only if you have been logging the data already

Authentication-related Logging Recommendations

Audit	Setting	Scope	Important EIDs
Account Logon: Audit Credential Validation	Success Failure	All	4776 (Account validated)
Account Logon: Audit Kerberos Authentication Service	Success	Domain Controllers	4768 (Kerberos TGT requested)
Account Logon: Audit Kerberos Service Ticket Operations	Success	Domain Controllers	4769 (Kerberos service ticket requested)
Account Logon: Audit Other Account Logon Events	Success	All	4778 (session reconnected to window station)
Logon/Logoff: Audit Account Lockout	Success	All	4625 (account locked out)
Logon/Logoff: Audit Logoff	Success	All	4634, 4647 (account logged off)
Logon/Logoff: Audit Logon	Success / Failure	All	4624, 4648 (account logged on, explicit credentials logon)

*Windows 7/2008; reference: http://technet.microsoft.com/en-us/library/dd772662(v=ws.10).aspx
*Also reference Randy Franklin Smith's UltimateWindowsSecurity.com site for great descriptions of event IDs: http://www.ultimatewindowssecurity.com/Default.aspx

#3: Determining the systems that communicated with a specified Internet IP address

- Log firewall “accepts” or NetFlow for outbound traffic
- If the volume of data becomes prohibitive
  - Filter out events associated with the most common legitimate destinations
    - Avoid filtering out ranges associated with open-to-the-public hosting environments, could be used for hosting C2
- Test the scenario where you query this data to identify communications with an IP address
  - Ensure you have DHCP logs and can determine the source host name
- Implement alerting capability

#4: Tracking domain name resolution attempts

- If the volume of data becomes prohibitive
  - Filter out events associated with internal name lookups and top known-good domains
- Block resolution of dynamic DNS names

#5: Identifying indicators of compromise across the environment

- Host-based or network-based artifacts
- May be artifacts associated with a specific attacker or intrusion
- May be general conditions indicating malicious activity
- Without a purpose-built tool to fulfill this need:
  - Antivirus
  - System/configuration management software
  - Email system logs
  - NIDS
  - SIEM
  - Vulnerability scanners
  - PowerShell/WMI

Conclusions

- Develop IR use cases, conduct simulations
  - Determine what capabilities _you_ need in your environment for the types of threats you face
- Define requirements for new roles, processes, and tools
- Ensure you are measuring something useful
  - Mean-time-to-remediate
  - Mean-time-to-detect

Contact information:

- E-mail:
  Jim.Aldridge@Mandiant.com

- Twitter:
  @jimaldridge