How Was that Breach Detected?

Jeff Hamm, Technical Director

Mandiant
Introduction

- Mandiant has done thousands of IR investigations across multiple industry types and networks. In each case, the customer was either altered by a third party about the breach or discovered something “not quite right” in the network. In several cases the alerts the customer discovered led to discovery of a targeted attacker in the environment - and a subsequent incident response investigation.

- In this presentation, we will use international case examples Mandiant investigated to take a closer look at how the breach was discovered and what security lessons can be learned from the alerts - for example how a performance monitor on a domain controller spiked which led to discovery of credential harvesting. The take away will include actionable items in many environments.
Targeted Attack Life Cycle

- **INITIAL RECONNAISSANCE**
  - Open source intelligence gathering
  - Network and application reconnaissance
  - Remote access identification

- **INITIAL COMPROMISE**
  - Social engineering
  - Internet-based attack
  - Leverage service provider

- **ESTABLISH FOOTHOLD**
  - Backdoors
  - Remote access subversion

- **ESCALATE PRIVILEGES**
  - Credential harvesting
  - Password cracking
  - Pass-the-Hash

- **INTERNAL RECONNAISSANCE**
  - Critical system identification
  - System enumeration
  - Account and password enumeration

- **COMPLETE MISSION**
  - Data staging
  - Data exfiltration
  - Data modification
  - Data destruction

- **MAINTAIN PRESENCE**
  - Command and control
  - Remote access subversion
  - Account abuse

- **MOVE LATERALLY**
  - Remote command execution
  - Remote administration
Introduction

• IR consultant with Mandiant since 2010
  • Technical Director and IR function lead in Europe since 2014
  • Adjunct lecturer at NTNU (Norwegian University of Science and Technology) since 2011
  • Deputy Sheriff/Detective/Sergeant at Oakland County Sheriff’s Office, Michigan 1997-2008
  • Co-Author “Digital Forensics” 2017, Wiley
Agenda

• Introduction
• Case Studies
  • LE On The Frontlines
  • Buy One Get Many Free
  • Set that CPU to Warp Speed
  • FTP in the DMZ
  • Broadcast Denied
  • "OPT" Out
  • SWIFT Transfer
  • APTx2
• Compiled Lessons Learned
Case Studies
LE On The Frontlines

• In 2016, law enforcement provided a notification to a biotechnology company that metadata belonging to them was found on a monitored hop point.
  • The story was written before the investigation began
    • https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
  • Phishing email that caused the download of a malicious Adobe Flash Player SWF file and an FLV file
  • Payload included “SHOTPUT” backdoor
  • APT3
    • Additional tools
    • C2 (command and control) infrastructure
    • Dates of active spear phishing campaign
LE On The Frontlines

Phish Email with “hp.swf”
Command shell “ctf.exe.gif”

Quarks PWDUMP
PSExeSVC
Scheduled Tasks

Domain Controller
VSS> NTDS.DIT

SHOTPUT
RDP Listener
Credential Harvesters
Lesson Learned:

- Ingest public intelligence and reporting into your alerting platforms
- Protect LSASS memory
- Prevent service accounts from interactive logins
Buy One Get Many Free

- Another biotechnology firm received an external notification
  - Their managed service provider alerted them of a problem
    - The managed service provider’s “jump host” into the customer’s environment was compromised by an attacker
  - The provider and the customer tried to remediate
    - Attacker changed tactics and tools
    - The investigation subsequently took months
    - Proper eradication of the attacker then took place
Service Provider’s Jump Host Credentials for the customers network

Attacker installed the backdoor
Reset the C2 Channel
Customer removed the backdoor

C2 Channel Known
Domain Administrator Account Used
Credentials Harvested
Customer reset the Administrator Account Password
Attacker returned the next day
Installed a new backdoor
Tried to steal data out of the C2
Ended up sending new credential harvest output to Dropbox
Buy One Get Many Free

• Lessons Learned:
  • Don’t remediate too soon while conducting an investigation
  • Ensure that all managed service providers are secure and proper controls are in place.
  • Protect LSASS memory
  • Prevent service accounts form interactive logins
Set that CPU to Warp Speed

• Performance Logs on a DC Spiked
  • An AD manager noticed the spike
  • The investigation revealed that an external attacker was interacting with systems
    • A credential harvester was being run on the system to dump all credential hashes
Customer noticed DC performance dropped

Attacker logged in while we were monitoring the system

Attacker was able to access /usr/games/PSEXEC.EXE

Lateral movement went across another geographic border

An SMB server connected to the workstation

Attacker saw lateral movement from a geographically removed network segment
Set that CPU to Warp Speed

• Lessons Learned:
  • Baseline domain controller performance logs
    • https://morgansimonsen.com/2011/01/03/establishing-a-performance-baseline/
  • Feed performance logs of your AD infrastructure into your security solution
  • Do not have domain controllers perform any additional tasks
  • Perform regular penetration tests on your DMZ
FTP in the DMZ

• Login to a database via unsecured FTP
  • A service account logged into a database and changed language settings
  • Attacker targeted the PUM (Privileged User Management) server
  • Attacker actively additional compromised systems daily while the investigation was ongoing
FTP in the DMZ

Attacker probed and found a vulnerable FTP Server in the DMZ
Attacker moved laterally to a privileged account management server
Attacker had the keys to the kingdom and accessed several systems most everyday during the investigation
FTP in the DMZ

• Lessons Learned:
  • Prevent service accounts form interactive logins
  • Know when you know enough to eradicate the attacker
    • Don’t let the attacker overwhelm your ability to investigate
  • Update Powershell
  • Log Powershell
Broadcast Denied

• Television Broadcasting Company had their repeaters crash just prior to an annual special event broadcast
  • Proprietary systems were sent a remove network devices command.
  • The host name of the system sending the command was found early on
    • The IP address was unknown
    • The IP address assignment was DHCP and was not logged
    • A backup server had the mapping of the IP address, but the system was never located
Broadcast Denied

ManagementConsole# rm -fr /etc/network
Broadcast Denied

• Lessons Learned:
  • Ensure inventory control is part of the security posture of the company
  • Have a disaster recovery plan to bring critical, remote devices up automatically
    • Customer had to send a technician to every remote relay site to reinstall from a backup
“OPT” Out

• Private bank had a server’s “opt” directory continually using up its quota.
  • Attacker was downloading tools and scripts to this directory
“OPT” Out

Database001# df -h /opt
Filesystem Size Used Avail Capacity iused ifree %iused Mounted on
/dev/sda5 200Gi 200Gi 0Gi 100% 2271542 4292695737 0% /opt
“OPT” Out

• Lessons Learned:
  • Ensure that all managed service providers are secure and proper controls are in place
  • Have play book guides for critical systems acting ’unusual’
  • Use malware detection capabilities – even on Linux / UNIX
SWIFT Transfer

• Public bank had their SWIFT servers crash.
  • Attacker deleted files and formatted volumes to cover their tracks
  • No traditional backdoors were found
  • Powershell and Metasploit scripts were located in memory of servers only
SWIFT Transfer

Investment Banking

SWIFT Environment (Segmented)
SWIFT Transfer

• Lessons Learned:
  • Ensure that proper controls are in place between network segments
  • Ensure critical systems configurations are hardened
  • Update Powershell
  • Log Powershell
• A large International company alerted on an Encrypted RAR file in their defense industrial business unit.
  • The RAR file transmission was blocked by IPS
  • A full scope IR revealed an additional APT group in the Mining and Gas business unit.
    • The attacker targeted the Mining and Gas infection with a spear-phishing campaign
    • The company believed they remediated the phishing emails but did not validate their actions
  • The attacker moved further into the environment as a result
APTx2

• Lessons Learned:
  • Rebuild workstations believed to have been affected by malware
  • Validate that any remedial actions were successful
Compiled Lessons Learned

- Don’t remediate too soon while conducting an investigation
- Ensure that all managed service providers are secure and proper controls are in place
- Protect LSASS memory
- Prevent service accounts from interactive logins
- Baseline domain controller performance logs
- Feed performance logs of your AD infrastructure into your security solution.
- Do not have domain controllers perform any additional tasks
- Perform regular penetration tests on your DMZ
- Know when you know enough to eradicate the attacker
- Don’t let the attacker overwhelm your ability to investigate
- Update Powershell
- Log Powershell
- Ensure inventory control is part of the security posture of the company
- Have a disaster recovery plan to bring remote critical devices up automatically
- Ensure that proper controls are in place between network segments
- Rebuild workstations believed to have been affected by malware
- Validate that the remedial actions were successful
- Have play book guides for critical systems acting ‘unusual’
- Ensure critical systems configurations are hardened
- Use malware detection capabilities – even on Linux / UNIX
Questions?

- Jeff Hamm
  - Technical Director
  - Mandiant
    - jeff.hamm@mandiant.com
    - hammjd@yahoo.com