You don't get to choose the day the enemy decides to show up.
An image from the robbery at US Bank on Carr Street in Lakewood on Sept. 30 (credit: FBI)

Are You Prepared To Face The Enemy?

Are Your Employees Prepared?
FBI Top Ten Most Wanted...

Mylch Jaqory Mason is being sought for his alleged involvement in multiple violent bank robberies and two separate shootings during November 2015 in Colorado.

Mason has tattoos on his chest, both arms, and hands. He has ties to Colorado, Florida, and Nevada.

REWARD: The FBI is offering a reward of up to $100,000 for information leading directly to the arrest of Myloh Jaqory Mason.
"An enemy, Ender Wiggin," whispered the old man. "I am your enemy, the first one you've ever had who was smarter than you. There is no teacher but the enemy. ..." — Orson Scott Card, Ender's Game
Train Like You Fight

Casey Smith
@subTee
Physical Security

Robbery Training, Mock Robberies, Procedures, Alarms, Hold Up Alarms, Cameras, Camera Verification, Vaults, Rapid Response
How We Process Threat Intel

What would that look like if it happened to us?

Are we prepared?
Be the Threat You Hope to Never See
When We Think Assume Compromise...

• It means YOU ARE GOING TO GET ROBBED.
• Prepare for it...
Hunt The Hunter
Quarterly Exercises

Executive Buy In

Short Specific Missions

We Attack to Get Caught
- Spear Phishing
- Weaponized Documents
- Credential Theft
- Command And Control
1 - Spear Phishing

• Some PowerShell @150 LOC
• Cloud Linux Server - $.58 cents per hour...

• This is **NOT** as a test of Users.
• Rather our Security Team’s Response.
<table>
<thead>
<tr>
<th>Time</th>
<th>Website</th>
<th>Disposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:56:42</td>
<td><a href="http://upsdeliveryservice.isaihost.com">http://upsdeliveryservice.isaihost.com</a></td>
<td>Block - URL Cat</td>
</tr>
</tbody>
</table>
Distributed Hunting
Were we detected?
How?
How quickly?
Were we contained?
How did this get through our filters?
What was the impact?

What are the common attributes?
2 - Weaponized Documents

New File On Network
New File Suspicious Parent Process
New File Suspicious Path. Example Path Contains “.zip”
Suspicious Executions
   whoami
   ipconfig
   net use
   quser
   sethc
Instrumentation - Visibility

• Endpoint Executions
• New Unapproved Files
• Network Connections
3 - Credential Theft

This one is very difficult without instrumentation
Some times it can be noisy

• Invoke-Mimikatz.ps1
• InstallUtil.exe – Katz.cs
  • Cross Process Events, Dll Loads
• Have you ever Actually Executed Mimikatz
  • To see the artifacts?

```bash
mimikatz(powershell) # log
Using 'mimikatz.log' for logfile : OK
mimikatz(powershell) # privilege::debug
Privilege '20' OK
mimikatz(powershell) # sekurlsa::minidump \lsass.dmp
Switch to MINIDUMP : \lsass.dmp
mimikatz(powershell) # sekurlsa::logonpasswords
Opening : \lsass.dmp' file for minidump...
```
Delta = FFFFFFFFE23B0000
Loaded ADVAPI32.dll
Loaded CRYPT32.dll
Loaded cryptdll.dll
Loaded NETAPI32.dll
Loaded NTDSAPI.dll
Loaded RPCRT4.dll
Loaded SHLWAPI.dll
Loaded SAMLIB.dll
Loaded Secur32.dll
Loaded SHELL32.dll
Loaded USER32.dll
Loaded HID.DLL
Loaded SETUPAPI.dll
Loaded ntdll.dll
Loaded KERNEL32.dll
Loaded msvcrt.dll
Sometimes It Happens Offline
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MT</td>
<td>crossproc</td>
</tr>
</tbody>
</table>

Opened handle with change access rights to `\windows\system32\lsass.exe` (4faaa369494a207617165dbfd10e34b5)
4 - Command And Control

• Proxy Hunting
  • User-Agent Logging
  • MIME Type Downloads

• DNS Database
  • Extract All Domains From Proxy – QFD (Question-Focused Datasets)
  • “Have we ever seen...” Yes | No
  • 1 row per domain
After Action Reporting 1/2

• Did the defenders detect the attack?
  • If so, how fast did they respond?

• Did the defenders detect the attack in the way the Red Team expected?
  • If not, why not? And was their method of detection more or less successful?

• Walk through the logs together after the exercise to trace the steps of the attack.

Thanks Kai!
After Action Reporting

- Does the data in the logs and/or network traffic meet your expectations? Can you trace the attack as expected?
- What has to be done to react more effectively next time?
  - (Methods, training, tools)
How Do You Know Your Hunting Tactics... Are Working? Are Accurate?

We All Have Lots of Tools Are They Sighted In Properly?
“I fear not the man who has practiced 10,000 kicks once, but I fear the man who has practiced one kick 10,000 times.” – Bruce Lee
References / Resources

Raphael Mudge -- @armitageHacker
https://www.youtube.com/watch?v=Mke74a9guNk

Sean Metcalf – https://adsecurity.org

Lee Holmes – PowerShell For Defenders

HolisticInfosec Blog
http://holisticinfosec.blogspot.com/

Please Read:
“Left of Bang: How the Marine Corps' Combat Hunter Program Can Save Your Life” - Patrick Van Horne

People to Follow:
@jaredcatkinson
@mattifestation
@harmj0y
Questions?

Feedback and Suggestions Welcome.

Casey Smith
@subTee
Special Thanks to A, B, M, K You know who you are.