Escaping Alcatraz

Breaking out of Application Sandboxed Environments

By: Kirk Hayes
whoami

Kirk Hayes
Senior Security Consultant

Avid Coffee Drinker, Wannabe Ukulele Player

Scripts/Tools:
https://github.com/I0gan
https://github.com/MooseDojo
Outline

History of “Alcatraz”
Escape – “Can I play, Daddy?”
Escape – “Don’t hurt me”
Escape – “Bring ‘em on!”
Escape – “I am Death incarnate!”
Mitigation Techniques
Alcatraz 101

Alcatraz:
- Opened in 1934
- 1.5 miles to nearest shore
- 14 Escape Attempts
- 29 Years
- 36 Prisoners
- 5 unaccounted for
“Alcatraz” 101

Technologies:
● Microsoft Remote Desktop (Formerly Terminal Services)
● vmWare Horizon View
● Citrix Access Gateway
● Kiosk PCs
“Alcatraz” 101

Purpose:
- Simplified Management
- Remote Access to Company Resources
- Deliver applications to any device
- Bring Your Own Device (BYOD)
- Centralize control of applications
Escape Plan

Alcatraz Escape Map

[Map showing various escape attempts with details such as dates and locations]
Escape Plan

1. Obtain Access to “Alcatraz” (Get arrested?)
2. Discover Security Level (Recon and Prepare for Escape)
3. Setup Attack Infrastructure (Build Escape Rafts)
4. Escape Application (Escape Alcatraz)
5. Profit! (Freedom!)
Escape - “Can I Play Daddy?”

How tough are you?

Can I play, Daddy?
Don't hurt me.
Bring 'em on!
I am Death incarnate!
Escape - “Don’t Hurt Me.”

How tough are you?

Can I play, Daddy?
Don’t hurt me.
Bring ’em on!
I am Death incarnate!
Escape - “Don’t Hurt Me.”
Escape - “Bring ‘em on!

How tough are you?

Can I play, Daddy?
Don’t hurt me.
Bring ‘em on!
I am Death incarnate!
Escape - “Bring ‘em on!”
Escape - “I am Death Incarnate!”

How tough are you?

Can I play, Daddy?  
Don’t hurt me.  
Bring ’em on!  
I am Death incarnate!
Escape - “I am Death Incarnate!”
Demo
Mitigation Techniques

● Secure your login portals
  ○ Use Multi-Factor Authentication
  ○ Strong Passphrases

● Secure your Operating Systems
  ○ Prevent access to management tools
  ○ Restrict the use of macros
  ○ Limit internet access to only approved sites

● Monitor, Monitor, Monitor!
Kirk Hayes
- @kirkphayes
- Kirk_Hayes@Rapid7.com
- kirk.paul.hayes@gmail.com

https://github.com/MooseDojo/myBFF
https://github.com/MooseDojo/backHack
https://github.com/I0gan

QUESTIONS???