SMB's vs. Ransomware

Tim Ashford
April 2017
GIAC GSEC, GCIH, GCIA

Ransomware: A Story

SMB's in the Cross Hairs

- 43 percent of 2015 cyber attacks: SMB's
- Ransomware is easily automated
- Ransomware is financially rewarding
- Assumption: SMB's highly vulnerable

. . . But Are They?

- How are SMB's disadvantaged?
- What are their cyber strengths?
- How are they similarly positioned?

Giving SMB's A Level Field

- Educate SMB's about highest risks
- Equip them with big business tools
- Enlist available strategies

A Word From Australia

- ASD: The Top Four
  - Patch apps
  - Harden Java, Flash, and the like
  - Disable untrusted MS Office macros
  - Use Application Whitelisting

More From Australia

- ASD: The Essential Eight
  - Restrict admin privileges
  - Patch OS
  - Use multi-factor authentication
  - Perform daily backups

Final Thought from ASD

- 85% of threats mitigated by Top Four
- Here's confidence:

"Any organisation that has been compromised despite properly implementing these [eight] mitigation strategies is encouraged to notify ASD."

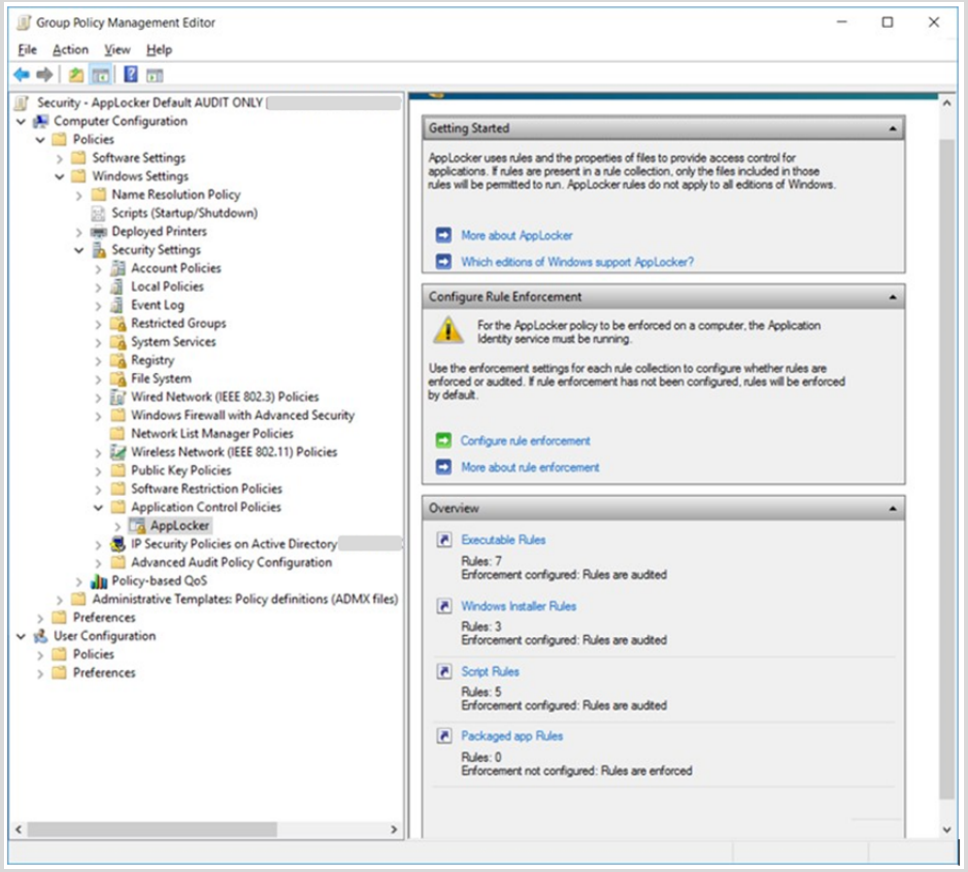
Why AppLocker?

- Whitelisting: Top 4 recommended
- SMB's best handle known good
- Ransomware rarely targeted
- AppLocker best: Free in Windows

Application Whitelisting

- SMB's have the advantage!
  - AppLocker = free (Windows Servers)
  - SMB's can easily inventory software
  - SMB's have fewer apps to manage

AppLocker Walk-Through



AppLocker Assumptions

- Users are not local Admins
- UAC settings are in place
- Link AppLocker object to correct OU
- Start slow
  - Create a Global Security Group
  - Add users
  - Apply Security Filtering, under Scope

AppLocker Limitations

- Does not include robust logging
- Path rules invite risk
- Whitelisting MS can be dangerous
  - Allows Regsvr32 example
  - Leaves room to invoke PowerShell

Containing PowerShell

- File-less attacks utilize PowerShell
- PowerShell is hard to tame
  - Not a single .exe
  - Cannot simply be "turned off"
  - Some constraints easy to bypass

Summary

- Stop ransomware with "Essential Eight"
- Application Whitelisting crucial for SMB's
- AppLocker is logical way to implement
- Well worth time and effort
- Ideally suited to SMB's
- Discussion/Q&A