You are making whitelisting difficult

Casey Smith

Two Ways to Engage the Enemy

Off Horizon - Collect and Analyze Telemetry

Hand To Hand Combat - Mitigations (User/Kernel/Hypervisor)

Whitelisting is a street fight

Disrupt/Degrade Adversary Capabilities

Classes Of Adversary

These attackers are aware of your defense and are **actively** working to bypass those controls.

Enlightened

Naïve

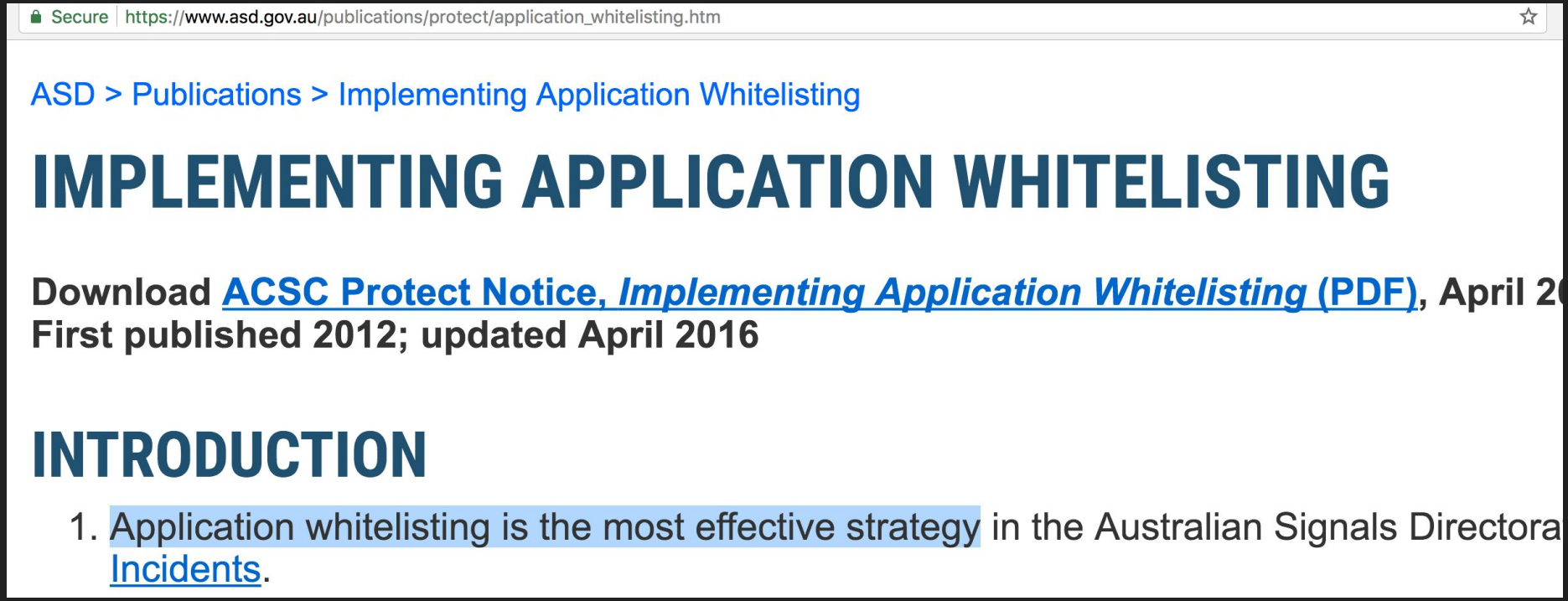
These attackers are not equipped to handle all security measures they may encounter.

Three Problem Statements

1.

admins often do not know where or how to begin to deploy whitelisting

Defenders need to hear the positive results



I actually want whitelisting to work.

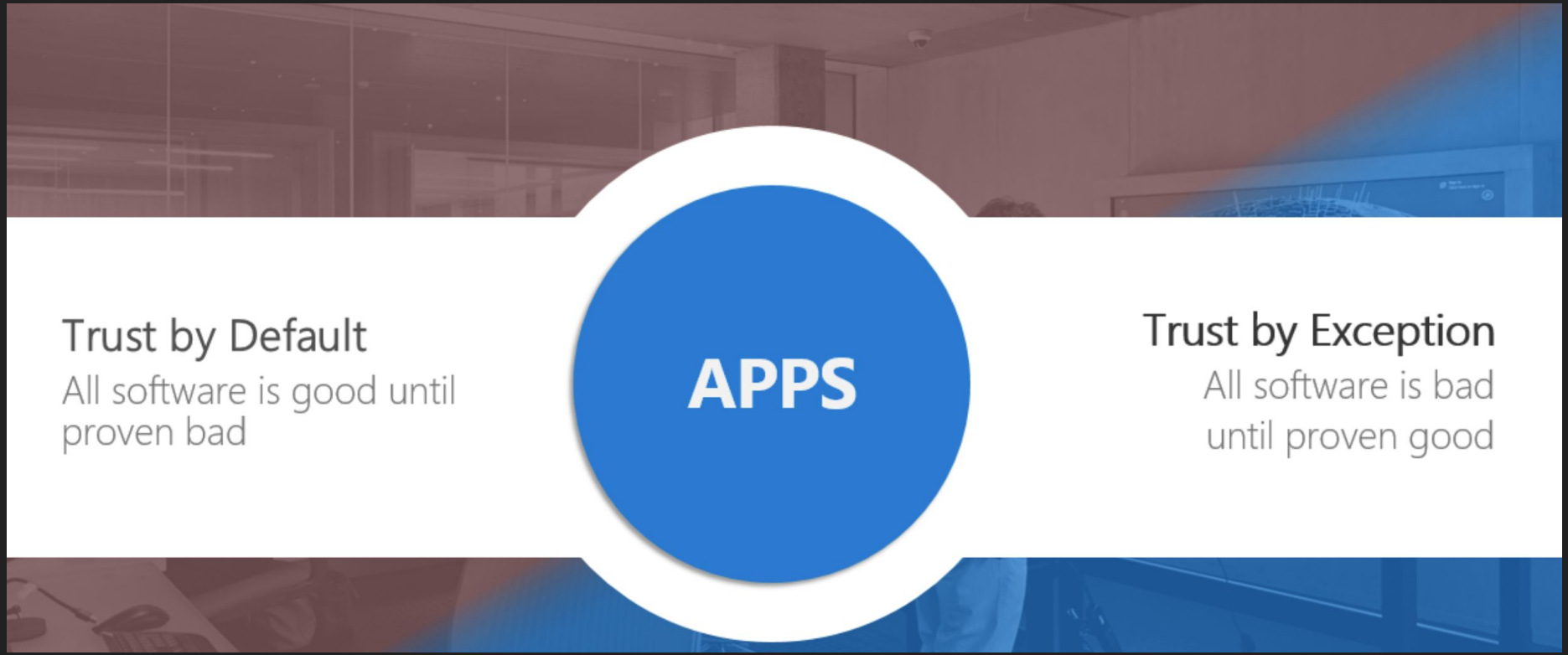
I worry defenders are not talking about its efficacy.

...for fear attackers will switch tactics?

2.

trust by default
instead of
trust by exception

More of this please...Ignite 2017 Talk (Aaron & Chris)



Trust Decisions made on... publisher…?

- Was this the intent of code signing?
- Verifies Identity and Integrity
  - Not Intent

3.

trusted signed tools can lead to compromise

My experience with bypasses

IEExec - Jan 16, 2014 (Proved my theory Trusted Things Can Execute Things)

InstallUtil - October 31, 2014

RegAsm/RegSvcs - November 6, 2015

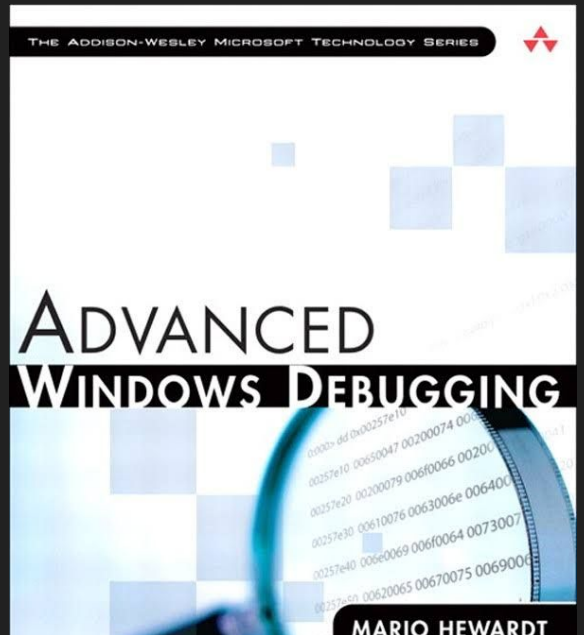
Regsvr32 - April 19, 2016

MSBuild - May 27, 2016 - Device Guard Bypass.

dbghost.exe

Discovered accidentally by …

Reading MSDN & :)



Honestly need all need a better

methodology to find these...

Using Custom Analysis Scripts

The analysis module in DebugDiag is extensible. You can also use existing analysis scripts to extract more data or
using the objects exposed by Dbghost.exe. Additionally, you can create new analysis scripts to address specific are

Does keeping a blacklist for whitelisting even make sense?

Current Published Device Guard Bypass Tools

- bash.exe
- bginfo.exe[1]
- cdb.exe
- csi.exe
- dbghost.exe
- dbgsvc.exe
- dnx.exe
- fsi.exe
- fsiAnyCpu.exe
- kd.exe
- ntkd.exe
- lxssmanager.dll
- msbuild.exe[2]
- mshta.exe
- ntsd.exe
- rcsi.exe
- system.management.automation.dll
- windbg.exe

How are new bypasses...

Discovered?

Serviced?

Announced?

Call To Action

Three Things We Need

1.

Acknowledge whitelisting is a boundary. ;-)

2.

“sign everything same way”, needs to be evaluated

notepad.exe == windbg.exe ?

3.

more .NET visibility

Closing Thoughts

Questions? Feedback?

Casey Smith