Examples of Two Ways to Engage the Enemy

1. Off Horizon - Collect and Analyze Telemetry

2. Hand To Hand Combat - Mitigations
Whitelisting is a fight
I actually want whitelisting to work.

I worry defenders are not talking about its efficacy.

...Why Not?
“...use your opening strategy to push your opponent into uncomfortable territory.”

-- Garry Kasparov
Classes Of Adversary

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

- Naïve
  - These attackers are not equipped to handle all security measures they may encounter.
Defenders need to hear the positive results

IMPLEMENTING APPLICATION WHITELISTING

Download ACSC Protect Notice, Implementing Application Whitelisting (PDF), April 2012
First published 2012; updated April 2016

INTRODUCTION

1. Application whitelisting is the most effective strategy in the Australian Signals Directorate Incidents.
Microsoft Ignite 2017 Talk (Aaron & Chris)

Trust by Default
All software is good until proven bad

APPS

Trust by Exception
All software is bad until proven good
What Techniques Are Mitigated By Whitelisting?

MITRE ATT&CK

92 Techniques Descriptions or Mitigations list whitelisting

For example: Whitelisting prevents ALL unauthorized DLLs from executing.
Perhaps you haven’t had a major incident, because no one has tried…
What Really Is Whitelisting?

Some use different names, like Application Control

Deny unapproved software the opportunity to execute
CIS Control 2:

Inventory and Control of Software Assets
Better Security Through Better Hygiene
Unwanted Software - Everyone has this problem...

High Prevalence

Difficult to control

AWL doesn’t have this problem. Your policy is actually now enforceable....
Most Challenges For Application Control Are Not Technical
How does software enter your organization?

Who approves software for your organization?

How quickly does software need to be approved?

What causes urgent deployments, besides updates and patches?

How is software removed from your environment?
What Difficulties Will You Likely Face?

Dynamic Developer Environments

IT Admins

Dynamic Software (Some .NET patterns for example)

Disconnected Systems

Urgent Approvals
State Of The Art For Bypassing

1. Exploitation of Trusted Software
   ~AWL kills exploit/drop & execute pattern

1. Misplaced Trust / Dual Use Binaries
2. Misconfiguration abuse
3. Memory Residence / Migration
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.
Bypasses Exist - Doesn’t Mean Dismiss

There is NO Perfect Defense
Actual Effect Of Mitigations

Source: @halvarflake | https://twitter.com/halvarflake/status/911503262284689408
Fact - It is difficult

Takes coordination and dialogue and cooperation with several teams

For Example:

Help Desk / Support Needs To Know How To TShoot This

Client Software Deployment Needs To Know How This Works
Cross Team Training

“This whitelisting stuff is …”

You will get blamed for problems and blocks

Be prepared to de-conflict
Where do we start?

Audit Mode

Report Monitor new software and how it enters your environment

Isolate teams and similar configurations
Phases Of Deployment
Organizational Commitment
Evaluation

Multiple Teams need to provide input.

Good sample representation of the organization

Gauge level of effort required
Selection

You better set requirements and objectives.

Don’t let vendors do this for you.
Example Week One - Collecting Execution Inventory

Audit Mode

Tight loop

Study Blocked applications
Week Two

Move small set of machines to a blocking mode
Week N

Rinse and Repeat
Blocking legitimate apps

This will probably happen.

Prepare, Train, and Learn From it when it does
Crisis/Urgent Blocks
Legitimate Blocks - Malware/Unwanted Software
Mass Deployment approvals
Metrics On Effectiveness

Track

1. Blocking Malicious Software
2. Blocking Unapproved Software
3. Disruptive Blocks
Case Study - Overview
But I mean, Does it work?

Red October ( For Us ;-) ) - October 22, 2013

Whitelisting Full Enforcement, April 2014. Yes, even DLLs. It is possible.

Was it difficult, YES.

Did it work? YES.

Are there bypasses? YES.
Closing thoughts

Whitelisting, even in audit mode, gives you tremendous insight into what is actually executing.

You have some of the best organizational telemetry to work with.

You need a quick way to lower enforcement, or you will be doomed to fail.

This can be done, at scale
Questions? Challenges? Discussion?
Help make whitelisting a new normal
Drive out commodity and opportunistic attacks
Questions? Feedback?

Casey Smith
@subTee