ROVNIX 攻击平台分析

—— 利用 WordPress 平台传播的多插件攻击平台

安天安全研究与应急处理中心(Antiy CERT)

首次发布时间：2015 年 07 月 24 日 14 时 30 分

目 录

1 背景介绍

近期，安天安全研究与应急处理中心（安天 CERT）的安全研究人员在跟踪分析 HaveX 家族样本的过程中，意外地发现了 Rovnix 家族（Trojan/Win32.Rovnix）在建立其恶意代码下载服务器时，也开始使用类似 HaveX 的方式，即：使用 WordPress 搭建的网站，或入侵第三方由 WordPress 搭建的正常网站（HaveX 的 C&C 服务器地址都是通过入侵由 WrdPress 搭建的网站得到的）。因此，安天 CERT 的研究人员对 Rovnix 家族展开分析。

2 威胁概述

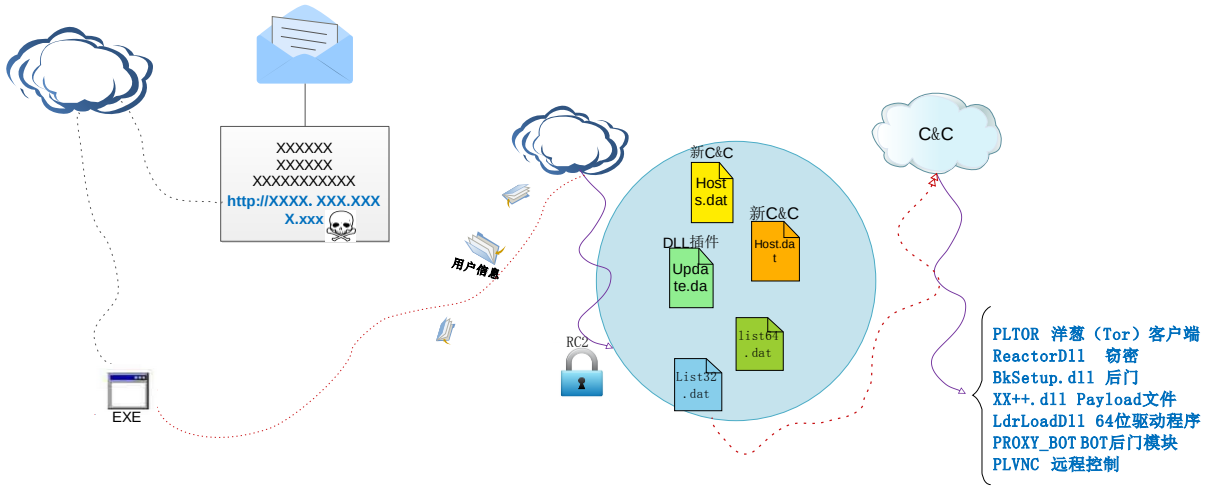


图 1 威胁图示

Rovnix 家族于 2011 年首次被发现，至今依然十分活跃。该家族恶意代码插件众多，具有反调试、反虚拟机、反沙箱、安装 VBR-BootKit（VBR 全称 *Volume Boot Record*，卷引导记录）等技术手段，同时具有收集用户信息、盗取比特币、盗取银行密码、远程控制等功能。

该家族主要通过电子邮件传播，通过诱使用户点击邮件正文中的链接地址下载 Rovnix 主程序（安天 CERT 迄今共发现了 300 多个恶意代码下载地址）。主程序在执行后会搜集、回传用户系统信息，其中，信息回传地址以硬编码形式加密保存在主程序内部。随后，主程序根据 DGA（Domain Generation Algorithm）计算出配置文件的下载地址。配置文件使用 RC2 算法加密，每个配置文件功能各不相同。例如：配置文件 Host.dat 存放插件下载服务器地址。主程序根据当前系统版本下载对应的插件列表，再下载该插件列表中的恶意插件，这些插件即是上述具有安装洋葱（Tor）客户端、盗取比特币、盗取银行密码、远程控制等功能的插件。

3 样本功能分析：

3.1 主程序分析

样本标签

病毒名称	Trojan/Win32.Rovnix
MD5	6EB761EA46A40AD72018D3CEE915C4CD
处理器架构	X86-32
文件大小	207960 字节
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2015-05-11 10:40:37
数字签名	NO
加壳类型	无
编译语言	Microsoft Visual C++
VT 首次上传时间	2015-05-11 14:33:00
VT 检测结果	32 / 56

Rovnix 主程序的主要功能是回传用户系统信息、释放其他插件、安装 Bootkit 以及加载插件。

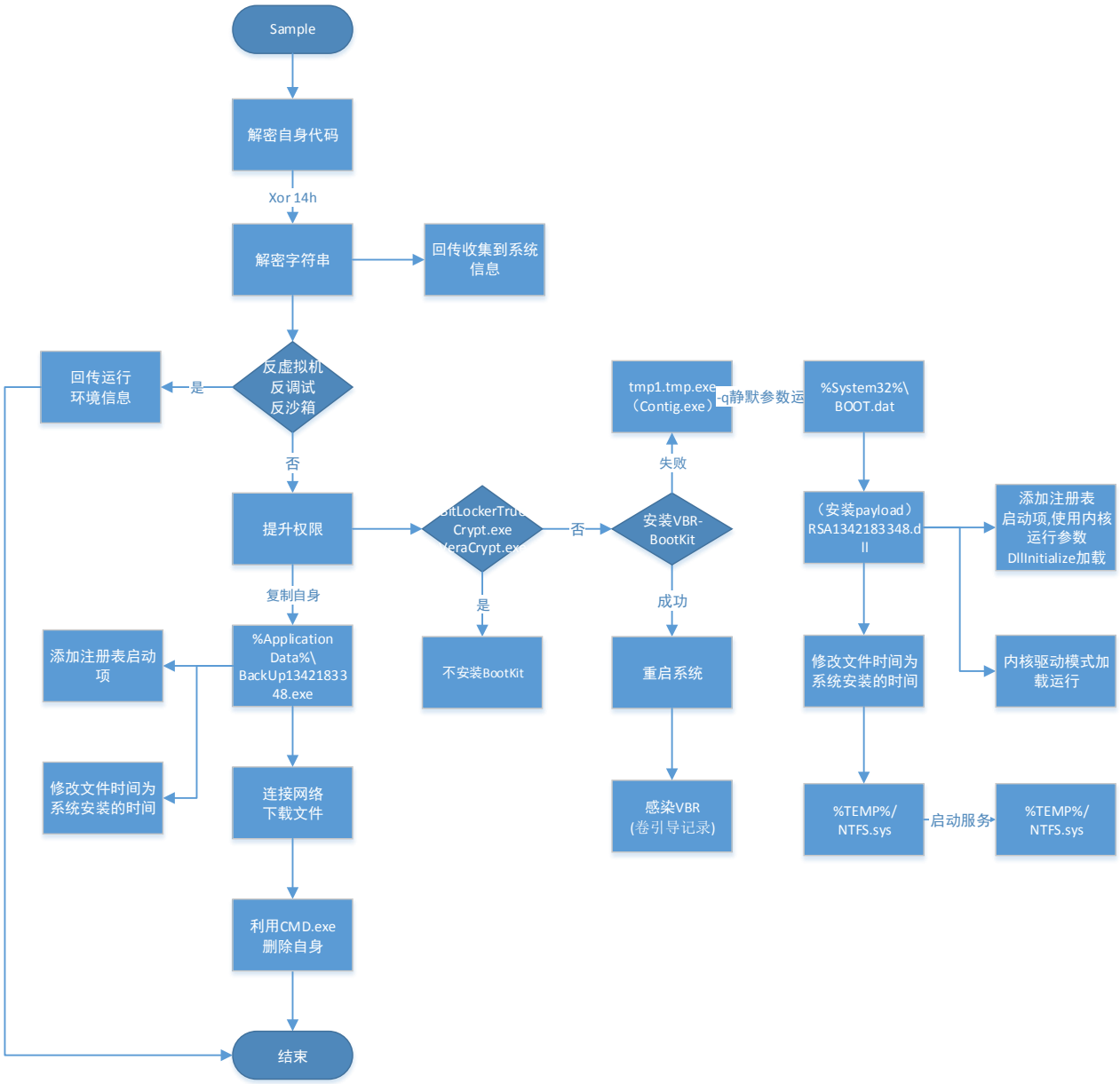


图 2 主程序流程图

1、样本运行后首先解密出自身代码，将地址 401000 处的数据清 0，再重新写入解密后的代码。

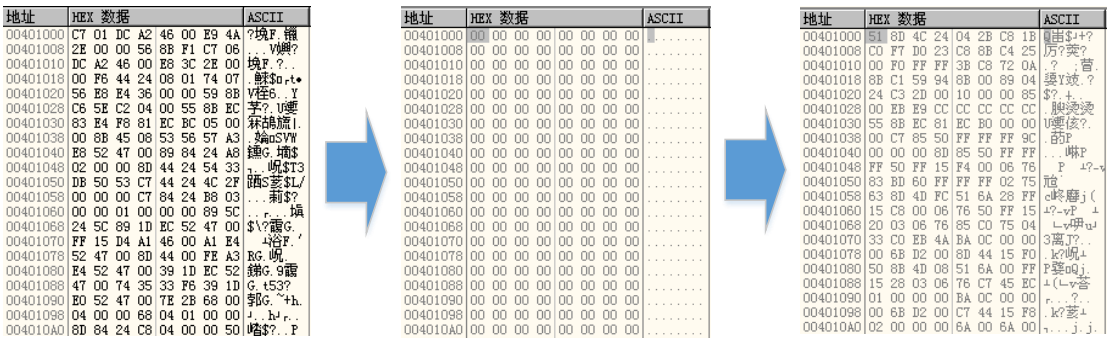


图 3 解密自身代码

2、进入代码空间后，使用 Xor 0x14h 解密对应的字符串。

```
for ( i = 0; i < a2; ++i )
{
  *(_WORD *)(a1 + 2 * i) ^= a3;                 // a3 = 14h
  result = i + 1;
}
```

3、随后检测样本运行环境，包括是否运行于虚拟机环境、沙箱环境。样本使用的异常处理机制并非常见的 SHE（Structure Exception Handler，结构化异常处理），而且采用了 VEH（Vectored Exception Handler，向量化异常处理）。样本检测当前运行环境是否支持脚本语言（如：Python、perl 等），并检查样本执行路径及文件名中，是否包含 sample、virus 等字样（这通常是反病毒厂商在其动态分析平台所使用的文件名），从而判断是否运行于恶意代码分析环境。同时，这些环境信息也会上传到 C&C 服务器。

```
v2 = Length(L"xagqf", 6, &v1);                  // 校验字符串长度
if ( !v2 )
  Xor_14h(L"xagqf", v1, 20);                    // luser
v2 = Length(L"dqfx", 5, &v1);
if ( !v2 )
  Xor_14h(L"dqfx", v1, 20);                     // perl
v2 = Length(L"dm`|{z", 7, &v1);
if ( !v2 )
  Xor_14h(L"dm`|{z", v1, 20);                   // python
v2 = Length(L"`fuwq", 6, &v1);
if ( !v2 )
  Xor_14h(L"`fuwq", v1, 20);                    // trace
v2 = Length(L"payd", 5, &v1);
if ( !v2 )
  Xor_14h(L"payd", v1, 20);                     // dump
v2 = Length(L"guydxq", 7, &v1);
if ( !v2 )
  Xor_14h(L"guydxq", v1, 20);                   // sample
v2 = Length(L"guyd%q", 7, &v1);
if ( !v2 )
  Xor_14h(L"guyd%q", v1, 20);                   // samp1e
v2 = Length(L"b}fag", 6, &v1);
if ( !v2 )
  Xor_14h(L"b}fag", v1, 20);                    // virus
result = Length(L"yuxcuf", 7, &v1);
v2 = result;
if ( !result )
  result = Xor_14h(L"yuxcuf", v1, 20);          // malwar
return result;
```

4、该样本随后执行提权（WIN7 利用漏洞提权、XP 利用普通提权）、复制自身到其他目录、修改文件时间、自删除、检测反病毒软件、回传系统信息、安装 VBR-BootKit 等一系列操作。

5、样本运行后会释放 4 个文件：

%Application Data%\Microsoft\Crypto\RSA\RSA1342183348.dll	**payload 文件**
%Temp%\tmp1.tmp.exe	**正常文件 contig.exe**
%system32%\BOOT.dat	**BOOT 加密引导数据**
%Temp%\NTFS.sys	**正常引导文件**

RSA1342183348.dll 是 payload 程序。样本会将文件时间修改为系统文件 svchost.exe 的时间（即系统安装时间），添加注册表启动项，利用 rundll32.exe 加载并启动，而它的启动参数是利用内核驱动模式加载的“DllInitialize”参数。

RSA1342183348"="C:\\WINDOWS\\system32\\rundll32.exe \"C:\\Documents and Settings\\"用户目录"\\Application Data\\Microsoft\\Crypto\\RSA\\RSA1342183348.dll\",DllInitialize"

tmp1.tmp.exe 是微软 Contig 程序，当样本因为卷没有足够的自由空间导致安装 VBR-BootKit 失败时，它将运行 Contig.exe 程序来调整文件数据。

注：Contig 是一个单个文件碎片整理程序，其目的是使磁盘上的文件保持连续。对于持续被碎片化的文件，或者如果您希望确保碎片数量尽量少，它可以完美地迅速优化文件。

恶意代码释放 Contig V1.7 版本使用如下静默方式运行，整理%system32%\BOOT.dat 文件碎片，执行命令为：

Tmp1.tmp.exe -q -n "C:\WINDOWS\system32\BOOT.dat" 256000

Rovnix 的关键功能是安装内核模式文件 VBR-BootKit。样本判断系统是否存在加密软件，决定是否安装 BootKit 并执行，检查系统是否使用 BitLocker 加密，遍历进程查看是否有 TrueCrypt.exe 和 VeraCrypt.exe（这两个进程都是加密软件），如果 Rovnix 发现系统使用上述加密，它将不安装 BootKit，未发现则安装 VBR-BootKit。如果 Rovnix 成功安装 VBR-BootKit，会产生蓝屏，并导致系统重新启动；安装 VRB-BootKit 失败，则加载 Payload 程序。

6、Rovnix 连接网络，下载文件，下载地址已经失效：

http://heckwassleftran.ru/R3_QACBABON/up.bin

C&C：

http://heckwassleftran.ru/cgi-bin/050515/post.cgi

3.2 插件分析

安天 CERT 研究人员对 Rovnix 的插件进行分析，发现若干其他插件，这些插件均从相关恶意服务器下载执行，其中包括具有 TOR 功能的洋葱匿名网络服务的客户端程序、后门程序、驱动程序、虚拟网络等，详情见如下列表：

插件名称	插件功能
PLTOR	洋葱（Tor）客户端，可以用来进行匿名访问网络，更好的隐藏自身。
ReactorDll	该模块具有后门功能，收集系统信息进行回传，使用 POST 方式与服务器进行通信，接收指令并执行。如：cookie 删除、开启 VNC、开启 socket 通信等等。
BkSetup.dll	获取系统版本，提升进程权限，然后在系统中安装后门模块，并设置自启动，当所有操作完成后，进行自删除。
XX++.dll	该模块与 Payload 功能相同，是 Rovnix 早期版本的 Payload 文件。
LdrLoadDll	该模块为 64 位驱动程序。用来检测系统中是否存在杀毒软件，主要功能是加载 DLL 模块，并调用其导出函数。

PROXY_BOT	BOT 后门模块，获取系统详细版本信息，使用 HTTP、FTP 多种方式与服务器进行通信，可用来执行多种命令。
PLVNC	该模块可以用来对机器进行远程控制，可以获取屏幕截图、系统信息，并对系统进程多种操作。
Payload	该模块在前面有比较详细的分析，主要功能是下载其它模块，并在内存中进行加载执行，添加自启动项等。
loader32.bin	收集系统信息，使用 HTTP POST 的方式与服务器进行通信，加载配置文件，根据配置文件，执行相应的操作。

Rovnix 的插件较多，目前安天 CERT 研究人员仅对以上 9 个重要插件进行了初步的定性分析。并对 Payload 进行了较详细的分析。

3.3 Payload 插件分析

样本标签

病毒名称	Trojan[Downloader]/Win32.Rovnix
原始文件名	RSA2095805845.dll
MD5	DED8BB2AD12B2317F1DB3265B003DCB5
处理器架构	X86-32
文件大小	79872 字节
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2015-06-19 10:50:15
数字签名	NO
加壳类型	无
编译语言	Microsoft Visual C++
VT 首次上传时间	2015-06-25 15:02:31
VT 检测结果	31 / 55

该插件为主程序释放的 DLL 插件，该 DLL 将大量字符串与 API 进行加密处理，解密后的主要功能包括更新 C&C 地址、创建命名管道、下载更多插件等。详细分析流程图与描述如下：

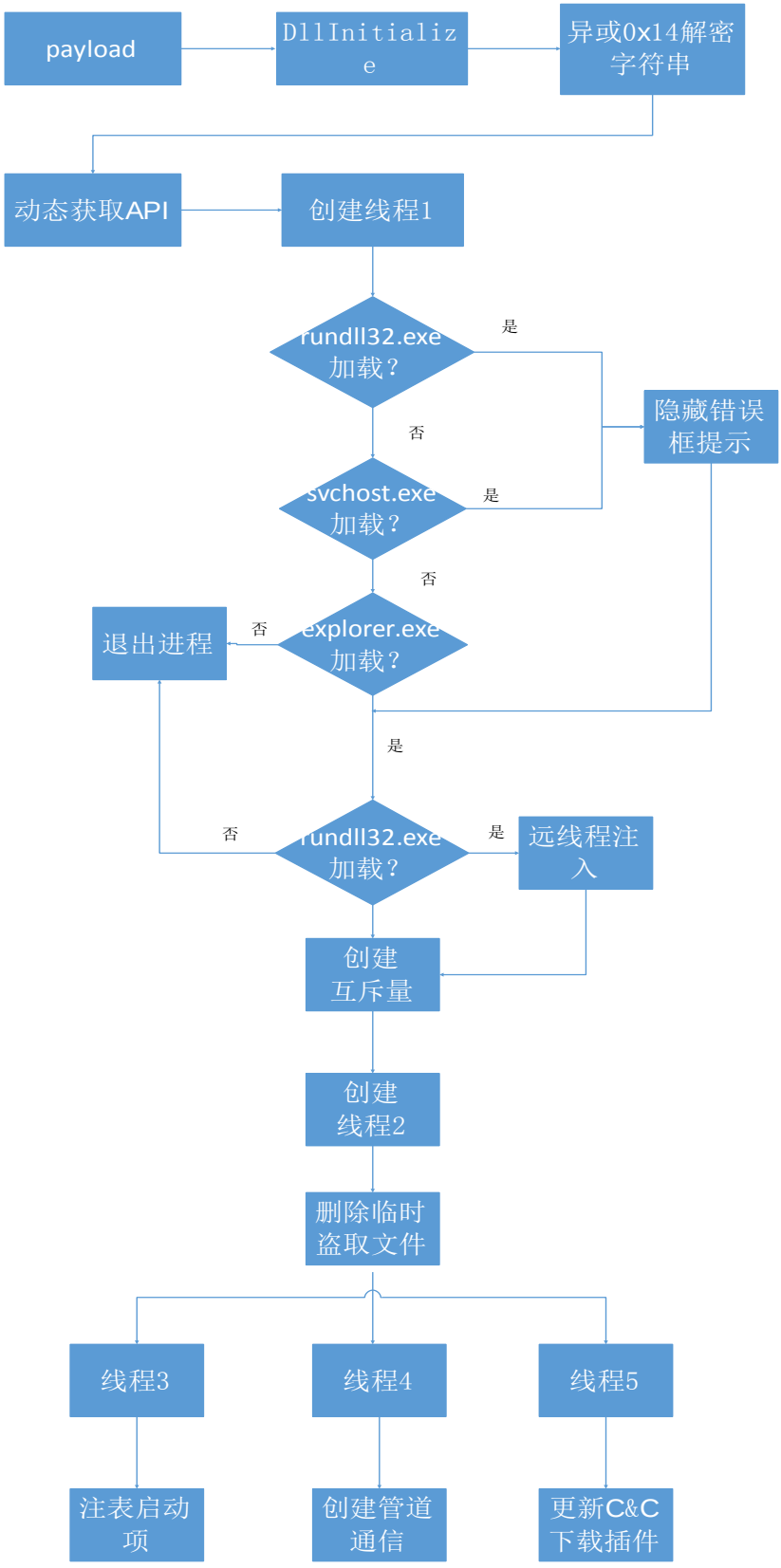


图 4 Payload 流程图

1、解密字符串：样本运行后首先将该样本中所使用到的系统中的 DLL、要操作的注册表键值、进程名称均使用异或 0x14 的方式进行了加密。其中，对于窄字节形式字符串，将以 BYTE 为单位异或 0x14，对于宽字节形式字符串将以 WORD 为单位异或 0x14。

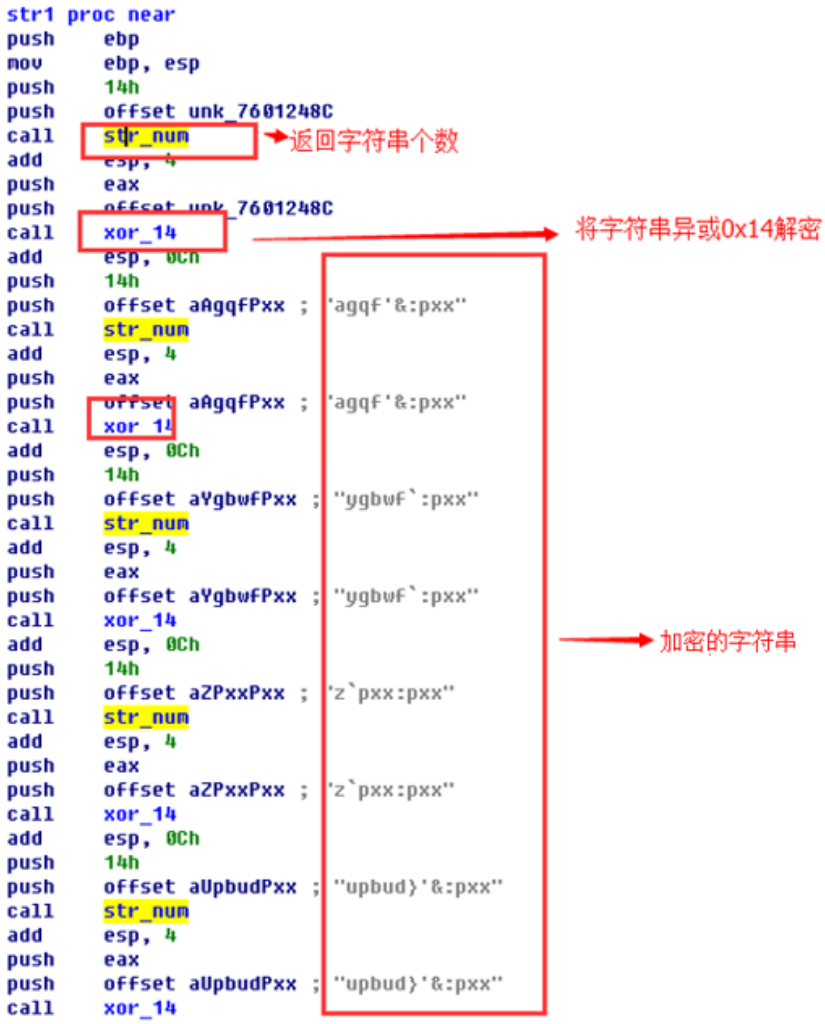


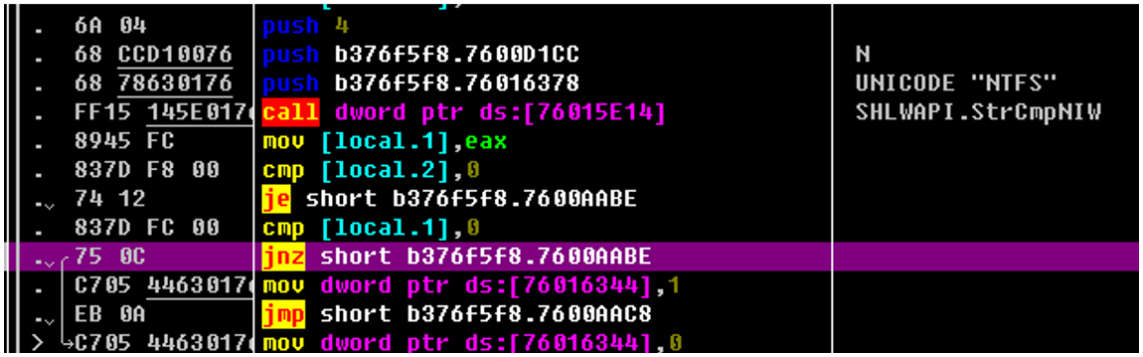
图 5 解密字符串

2、随后样本创建线程，进行加载样本进程的判断，并置位对应的内存标志，样本判断如下 4 个加载自身的程序。

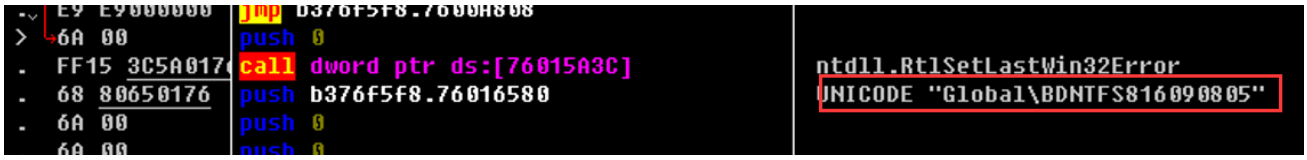
进程名称	标志位
winlogon.exe	0x7601634C
svchost.exe	0x76016348
explorer.exe	0x76016350
rundll32.exe	0x76016354

对不同的加载程序，做相应的处理，如：在线程 1 中，若样本运行在 svchost.exe 或 rundll32.exe 进程中，会调用 SetErrorMode(0x8003)设置系统不显示 Windows 的多种错误对话框，隐藏运行。如果不是上述 4 种中的一种加载自身，则进程退出。

3、样本获取系统文件路径并提取卷标、磁盘类型等信息。如果样本是 NTFS 类型，则置位 76016344 内存为 1



并根据磁盘信息创建互斥量字符串



互斥量的组成 Global\BD（文件系统类型\卷序列号），如：Global\BDNTFS816090805。

4、样本创建线程 2，进行临时文件夹下的文件删除操作。目的是删除主程序释放的盗取系统信息的临时文件。

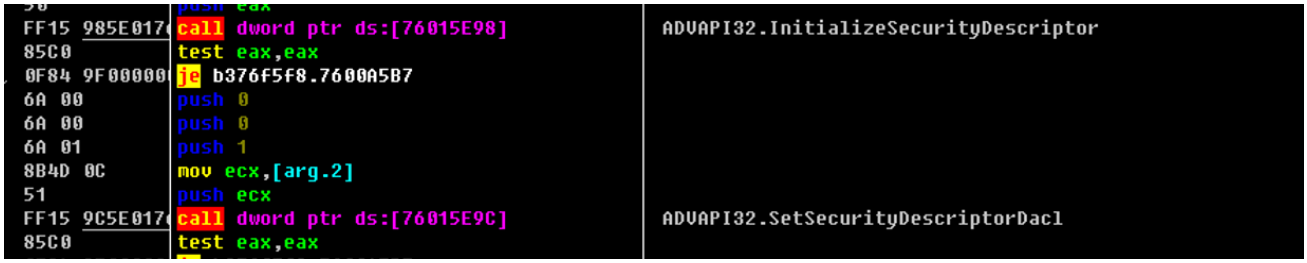
5、随后样本进入主要功能阶段，创建了三个线程：

线程 3：

样本会遍历注册表 HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run 中的所有模块，查看当前模块是否存在，如果不存在，则会添加到启动项中。

线程 4：

通过创建命名管道的方式与其他恶意进程进行通信。



```
6A 02          push 2
68 E0760176    push b376f5f8.760176E0          UNICODE "\\.\pipe\vhost816090805"
FF15 C45B017(  call dword ptr ds:[76015BC4]    kernel32.CreateNamedPipeW
8945 FC        mov [local.1],eax
837D FC FF     cmp [local.1],-1
0F84 8500000(  je b376f5f8.7600A6C7
6A 00          push 0
8B55 FC        mov edx,[local.1]
52             push edx
FF15 C05B017(  call dword ptr ds:[76015BC0]    kernel32.ConnectNamedPipe
85C0           test eax,eax
```

管道的命名也与卷序列号有关，\\.\pipe\vhost（卷序列号），如：\\.\pipe\vhost816090805

线程 5：

线程 5 的主要作用是更新 C&C 服务器并下载插件执行。

在样本中 C&C 域名有 3 个，均经过异或 0x14 后，键名称分别为：SH1、SH2、SH3，保存到注册表中，地址为：HKCU（或 HKLM）\\Software\\Microsoft\\Product\\B（卷序列号）。样本读取该键值，判断是否有数据，如果有，则更新到样本中；如果没有，则使用样本中硬编码的三个 C&C 域名。当连网获取到新的 C&C 后，会更新到注册表中。

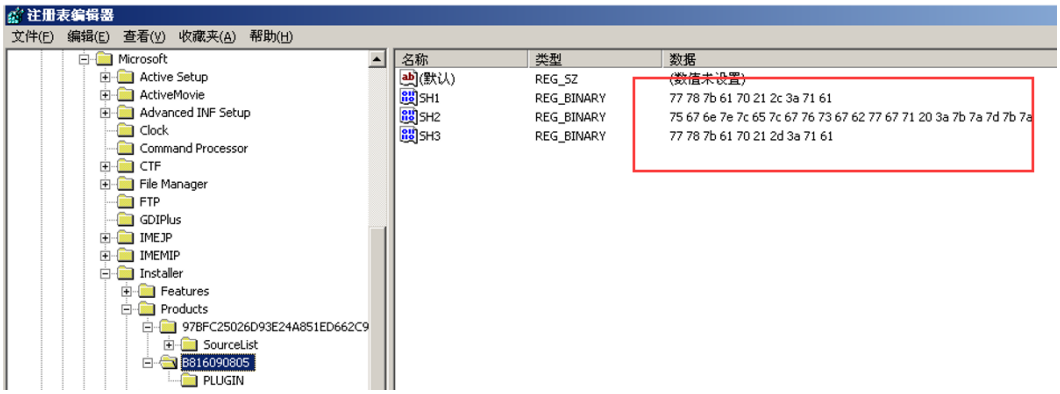


图 6 存储在注册表中的加密域名数据

根据DGA解密后的域名：

cloud58.eu
aszjhqhsbgsvcse4.onion
cloud59.eu

3.4 Yara 规则提取（payload）

通过安天 CERT 提取的 Payload 插件相应特征，编写 Payload Yara 规则如下：

```
rule Rovnix_Payload_Plugins
{
    meta:
        author = " AntiyCert"
        date = "2015/07/20"
```

```
        ref = "http://www.antiy.com"
        maltype = "Rovnix_Payload_Plugins"
        filetype = "dll"

    strings:
        $PE32 = {55 8B EC 83 EC 08 C7 45 FC 00 00 00 00 8B 45 08 0F BE 08 89 4D F8 8B 55 08 83 C2 01 89 55 08 83 7D F8 00 74 0B 8B 45 FC 83 C0 01 89 45 FC EB DD 8B 45 FC 8B E5 5D C3}
        $PE64 = {48 89 4c 24 08 48 83 ec 18 48 c7 44 24 08 00 00 00 00 48 8b 44 24 20 0f be 00 89 04 24 48 8b 44 24 20 48 ff c0 48 89 44 24 20 83 3c 24 00 74 0f 48 8b 44 24 08 48 ff c0 48 89 44 24 08 eb d3 48 8b 44 24 08 48 83 c4 18 c3}
        condition:
        1 of them
    }
```

4 传播 URL 分析

2015 年，安天 CERT 共发现了 300 多个恶意代码下载地址，URL 对应的 IP 地理位置涉及 34 个国家，其中数量最多的国家是美国，占总数量的一半以上。这些 URL 有一个共同的特点，如下图所示：

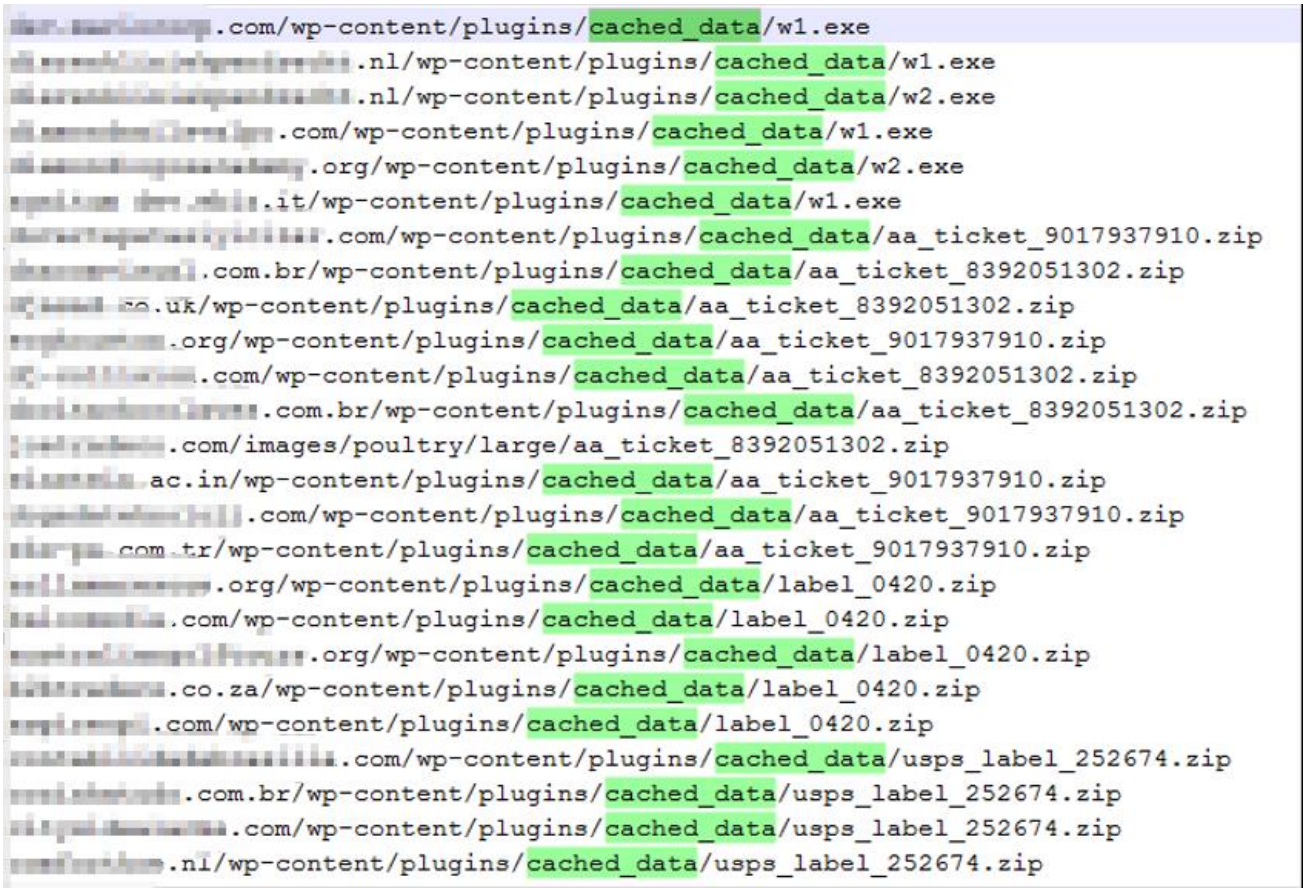


图 7 Rovnix 下载地址结构

与此同时，安天 CERT 又发现了另一个家族的样本也是使用类试的 URL 结构形式如下图：

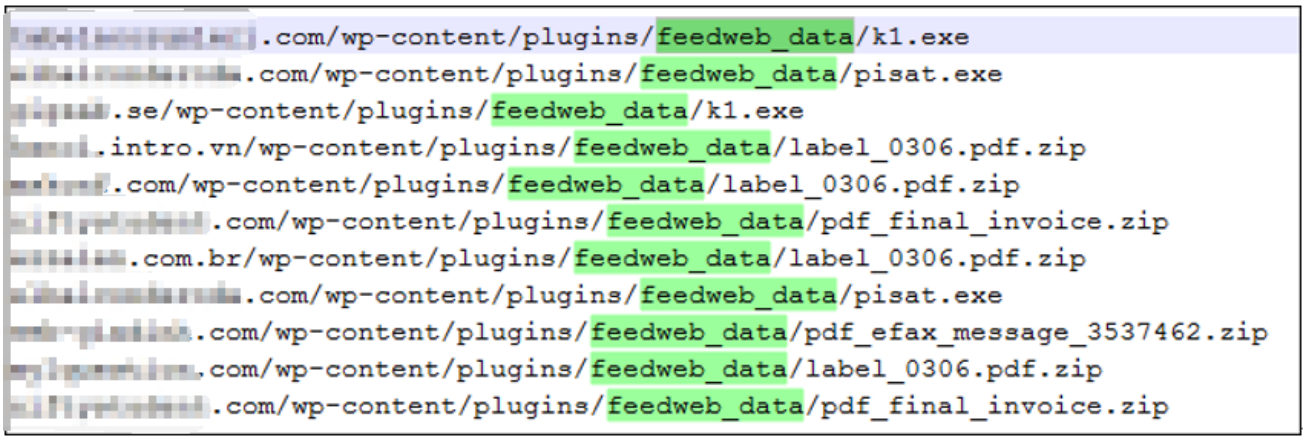


图 8 另一个家族的地址结构

从 URL 结构上来看，两个家族之间是有一定联系的，都是通过邮件正文中的链接点击下载并执行，并且从传播时间上看也都是在 2015 年开始出现。

通过以上统计出的 URL 地址，安天 CERT 联想到了 2014 年出现的 APT 事件 Havex，Havex 的 C&C 服务器都是通过入侵由 WordPress 搭建的正常网站得到的。Rovnix 中也有一部分的 URL 下载地址是入侵由 WordPress 搭建的正常网站得到的。Rovnix 在后期回传数据时用使用了其它的 C&C 服务地址。

注：WordPress 是一种使用 PHP 语言开发的博客平台，用户可以在支持 PHP 和 MySQL 数据库的服务器上架设属于自己的网站，也可以把 WordPress 当作一个内容管理系统（CMS）来使用。

5 总结

Rovnix 是一个喜欢使用冷门技术的恶意代码家族，具有如下特性：它喜欢使用 VEH 异常处理机制，BootKit 使用的是 VBR-BootKit；支持众多的 Windows 版本，根据环境投放 32 位或 64 位的插件；定制化的插件支持多种恶意功能。这些特性让安天 CERT 的研究人员将其归类为专业化的攻击平台，是有可能被用来进行定向攻击的武器之一。

附录一：插件 Hash 列表

插件名	MD5
PLTOR	F17F3F7610E60B7A9B9F243CF437062B 2e2d3ef681f085672655c805412907c7
ReactorDll	1f895c237b131c1739985e2851dc5236 bb91c8c65b8c4664a8099e064535463c 43fb37ffd4415cbaa20ca1e38736d12d

BkSetup	60b36b16a2dc6482f7cc1f29a07b2c04
XX++	e2cb2233a8670bdbc0cd98a7d5d5aeda 7b462550b69471f3417aef8d85398eba 742e30b5ba7793bea18b3972292d139e
LdrLoadDll	acebb8d92c7d8529f84d9a22280f3f21 98e70439a6922e06e24636779456b2b8
PROXY_BOT	52de1fa8c96e09e2389cef45ba9e1775
PLVNC	c78ebe1395615d39350e5155fc8486e8
Payload	ecbc8b7a52e0417d8c13ead5c8c9d1e3 31f84e39a7b48eca73f7e6635d7d2a14 ecbc8b7a52e0417d8c13ead5c8c9d1e3 9b116c78b89a1a619c831290f2ff553c 13998bcd28a3064b99cdeaf339335bf9 68bc8e20123c1f061e11cc4e606e058e f90203eb1300f21fcffc9abaf8d8e9a6 0a40bfd79530bbdd2a16bf5d1f01a68a 92d548ac911c61551a979284c384d792 92d548ac911c61551a979284c384d792 0a40bfd79530bbdd2a16bf5d1f01a68a 6206d4ef511899fe52d152713c27d392 6206d4ef511899fe52d152713c27d392 48af0025c9705a9e8ac0ea9fee77af08 48af0025c9705a9e8ac0ea9fee77af08 c58e0867fbbd229ca578858cd2ec25b3 4c3dfbbf8652f5ce8139f2aa12f48adf f26da54810d7d9a0ee211a5459b1d566 3b05cfea114da145e1e64a2c0eeb8b45 6fdcbee2d35e5107ac2cc098ecffffef 30c085758a7ef457f9a8ebbd99da0052 94aa008846ba49fb257e9414159879af 8e3ed59de1e8ad138a84e0a44373fdd7 9a4f5d950b45ed4e9d744c56c99edfb2 5bc6658f23594d74e26bdf680715925e a584e0d5775a38e4cc0eda2a4180a09e 5844bb74e5e030828322ee68bafc86be c9f371cae74ed398cbe81bbf71ec0747 a963aa496ae69f84500d4cba366fa3e9 a8804a7038347348a69a4ee3cde6d6ae f95ee1c40857199a7d54e72ece5719a9 61229fbaabd4caf3c6ca53dd0512353c 65be747958aad1e2d3b3120ff0478551 f95ee1c40857199a7d54e72ece5719a9 a8804a7038347348a69a4ee3cde6d6ae

	f45776b77224c246b123da4d3864159d 2be91034a5c264eb48a260ea8f2b404d ded8bb2ad12b2317f1db3265b003dcb5 ebf3c9c13c6c9536f378e7fa2cd755be 8e3ed59de1e8ad138a84e0a44373fdd7 2be91034a5c264eb48a260ea8f2b404d a82300b6ba656b64efbbcd56b8948095 c89c4cd8aa4fa1476eaadcebc89fb083 ebf3c9c13c6c9536f378e7fa2cd755be 94aa008846ba49fb257e9414159879af c89c4cd8aa4fa1476eaadcebc89fb083 a04645d8cbfd2f8d1225a1a6ebacd3ac
loader32.bin	97aa9fbf54b6dbd12020e8fc78536348 5988fffc9367e5d8ab2d228425706597 e16066f20df36bfdf07d7fe6a02baec2 8ac63eee20fa1054211f868ee0b6906f 8e8c618e21125e4602163eedb2778b8f 44dac1521674daf87c507f00862a4e3e 778d40df0747c3356dc4f249f80724e8 5aba1da0813fbb99a27dfd15702ac7e6 e8d835b9c6e5ed9f52c13f1f0e3db66a d7dde4320c34052bb4b836cbdffee9ed 5ec1574874959ed7535e0df2a5588317 b3ea8f269c9681d0845c7d2fe7683625 01629b695811c1df38e17e40987fb8cc 7517e5a5894fb571e682533b34dc6bdc bbb8b345bfd264c0c42364508e0b2e3d 23a52a86711d148029b26a5d8ace5b07 9a70ce19c64bb19d825a912db544e4df 11df67f371d40aacdc72f2c389186d3f 95d88acbe7d9a35937f8be72654bac07 ba7c0d35a9d2ecadd26585d76f6a637e 821e2e37335c62093d6fc2b771fb9cef f82386c935195228aaacfbdc3f56bc4f 9ac383b7f8c605e566c7b2327f5a8b6f 9f2325435b28e20f4da92b99191a4af3 a1bafd0a17f198f0769bc009b2105358 756c0f0a16c35c3e9c1b5ef43a30ffee 3b7b26453f21890bdac2c2bc1edf26b4 953d50901a86f837ed9d994d46449018 e3eb6ffd78bb6a157c41ec0c7a95be55 123d5278b61caad9cf70e59f6606b006 eb5106f41a851c630a7de7cb9b14e90f 423a07c16f29c5649060ae4eaf517ba0

	1b114b24647adf49afd86e28e29ac7fd da2a943b87945d8c7938542e164f5d73 c83f6d378eb1dfd012dc1c06cfcaf428 21791ca18692c9a170d9a45ea83438a4 7a6295e93a17e14b407becf443357889 1fd00c73d18f46bb6abd7285a84a20fd d8ed3e957606651e1e2139fbfaa29467 12a12cc9858280a0f52bca4a25c25b91 8c894c6e4bf45c0c27d4c68a36f861eb f91958f038fbed0d85fab44f7601efc3 080a068b66ca6ae71e00b4a3d1c25dfc e201bc299739910b821db298fb632a63 cf51b223cc146e5ca36cd4c46fa486d6 5f599cf7a3e749694e438e89b969a2a6 25c941a3345850562bb76b8bf4cad42d

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