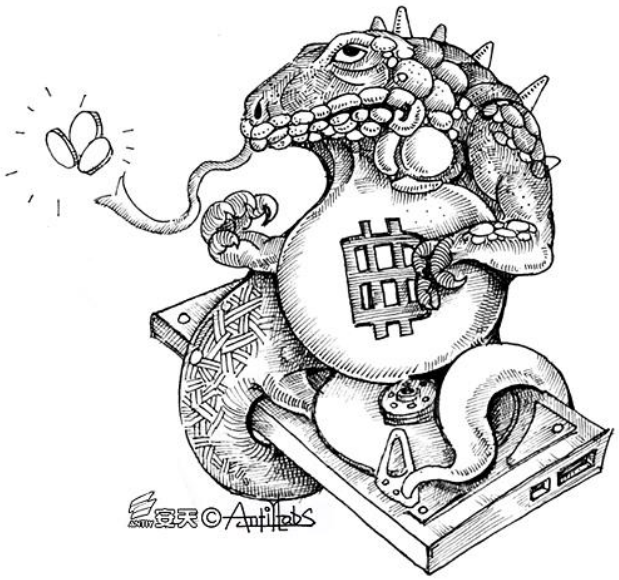
揭开勒索软件的真面目

——安天安全研究与应急处理中心



目 录

1 前言

2013 年 9 月，戴尔公司的 SecureWorks 威胁应对部门（CTU）发现了一种名为“CryptoLocker”的勒索软件，它以邮件附件形式分发，感染计算机并加密近百种格式文件（包括电子表格、数据库、图片等），向用户勒索 300 美元或 300 欧元。据统计，仅在最初的 100 天时间内，该勒索软件就感染了 20 万至 25 万个系统[1]。

2014 年 8 月，《纽约时报》报道了这样一则消息：一种名为“ScarePackage”的勒索软件在一个月的时间内感染了约 90 万部 Android 手机，该软件不仅会访问手机的摄像头、电话功能，还会在手机屏幕弹出消息，指责手机用户传播色情内容，手机用户只有支付了几百美元的“赎金”才能正常使用手机[2]。

2014 年 12 月，安全公司 Sophos 和 ESET 的研究人员发现了一种可以自我复制的勒索软件（VirLock，又称 VirRansom），该软件不仅会加密受害主机的文档、图片、音频、视频和压缩文件，同时还会使计算机“锁屏”，以侵犯著作权为由，向计算机用户索要 0.652 个比特币[3]（根据本文撰写时的比特币兑换价格，约合 1027 元人民币）。

对于传统的感染式病毒，未安装反病毒软件的用户会因中毒而导致系统程序和应用程序被感染，不过一般可以通过重新安装操作系统和应用程序解决问题；对于远程控制类木马，用户可以采用临时断开网络的办法，暂时摆脱攻击者的远程控制。但是，如果计算机上的照片被勒索软件加密，用户很可能会彻底失去一段美好的回忆；如果被加密的是急需使用而又没有备份的毕业论文、重要资料，恐怕用户也只好向犯罪分子屈服，乖乖地支付赎金。勒索软件为何如此猖狂？它是如何向用户进行勒索的？我们又该如何检测与预防这类威胁？本文将全面介绍勒索软件的传播手段、攻击流程及防御方法，彻底揭开勒索软件的真面目。

1.1 何谓勒索软件

勒索软件（ransomware）是一种流行的木马，通过骚扰、恐吓甚至采用绑架用户文件等方式，使用户数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财。这类用户数据资产包括文档、邮件、数据库、源代码、图片、压缩文件等多种文件。赎金形式包括真实货币、比特币或其它虚拟货币。一般来说，勒索软件作者还会设定一个支付时限，有时赎金数目也会随着时间的推移而上涨。有时，即使用户支付了赎金，最终也还是无法正常使用系统，无法还原被加密的文件。

1.2 主要传播手段

勒索软件的传播手段与常见的木马非常相似，主要有以下几种：

1. 借助网页木马传播，当用户不小心访问恶意网站时，勒索软件会被浏览器自动下载并在后台运行
2. 与其他恶意软件捆绑发布
3. 作为电子邮件附件传播
4. 借助可移动存储介质传播

1.3 主要表现形式

一旦用户受到勒索软件的感染，通常会有如下表现形式，包括：

1. 锁定计算机或移动终端屏幕
2. 借杀毒软件之名，假称在用户系统发现了安全威胁，令用户感到恐慌，从而购买所谓的“杀毒软件”

3. 计算机屏幕弹出类似下图的提示消息，称用户文件被加密，要求支付赎金

图 1 勒索软件弹出的提示消息

2 勒索软件的分类

根据勒索软件所使用的勒索方式，主要分为以下三类：

1. 影响用户系统的正常使用。比如 PC Cyborg、QiaoZhaz（Trojan/Win32.QiaoZhaz）等，会采用锁定系统屏幕等方式，迫使系统用户付款，以换取对系统的正常使用。
2. 恐吓用户。比如 FakeAV（Trojan[Ransom]/Win32.FakeAV）等，会伪装成反病毒软件，谎称在用户的系统中发现病毒，诱骗用户付款购买其“反病毒软件”。又如 Reveton（Trojan[Ransom]/Win32.Foreign），会根据用户所处地域不同而伪装成用户所在地的执法机构，声称用户触犯法律，迫使用户支付赎金。
3. 绑架用户数据。这是近期比较常见的一种勒索方式，最典型的是 CTB-Locker 家族（Trojan[Ransom]/Win32.CTBLocker），采用高强度的加密算法，加密用户文档，只有在用户支付赎金后，才提供解密文档的方法。

根据上述分类方法，结合具体行为、运行平台，可将勒索软件整理如下表：

方式	具体行为	平台	典型家族命名	其它名称
影响使用	锁定系统屏幕	Windows	Trojan/Win32.QiaoZhaz	**QiaoZhaz**
		Android	Trojan[rog,sys,fra]/Android.DevLockeer	**DevLockeer**
			Trojan[rog,sys,fra]/Android.Koler	**Koler**
			Trojan[rog,sys,pay]/Android.Locker	**Locker**
	修改文件关联	Windows	Trojan/Win32.QiaoZhaz	**QiaoZhaz**
	拦截手机来电	Android	Trojan[rog,fra,sys]/Android.Cokri	**Cokri**
	色情无限弹窗	Android	Trojan[rog,sys,fra]/Android.Koler	**Koler**
	伪装色情应用	Android	Trojan[rog,sys]/Android.simplelock	**simplelock**
恐吓用户	伪装杀毒软件	Windows	Trojan[Ransom]/Win32.FakeAV	**FakeAV**
		Android	Trojan[rog,sys]/Android.Svpeng	**Svpeng**
			Trojan[rog,sys]/Android.simplelock	**simplelock**
	伪装当地执法机构	Windows	Trojan[Ransom]/Win32.Foreign	**Reveton**

方式	具体行为	平台	典型家族命名	其它名称
绑架数据	隐藏用户文件	DOS	Trojan/DOS.AidsInfo	**PC Cyborg**
		Windows	Trojan/Win32.Pluder	**Redplus**
	删除用户文件	Windows	Trojan/Win32.QiaoZhaz	**QiaoZhaz**
		Android	Trojan[rog,sys,fra]/Android.Koler	**Koler**
	加密用户文档数据	Windows	Trojan[Ransom]/Win32.CTBLocker	**CTB-Locker**
			Trojan[Ransom]/Win32.Blocker Trojan[Ransom]/Win32.Bitman	**CrytoLocker**
			Trojan[Ransom]/Win32.Locker	**Locker**
		Android	Trojan[rog,sys]/Android.simplelock	**simplelock**
		Android	Trojan[rog,sys,fra]/Android.Koler	**Koler**
	加密通讯录	Android	Trojan[rog,fra,sys]/Android.Cokri	**Cokri**

3 勒索软件的演进史

3.1 几种典型勒索软件家族的出现

已知最早的勒索软件出现于 1989 年，名为“艾滋病信息木马”（Trojan/DOS.AidsInfo，亦称“PC Cyborg 木马”），其作者为 Joseph Popp。该木马程序以“艾滋病信息引导盘”的形式进入系统，采用替换 AUTOEXEC.BAT（DOS 系统文件，位于启动盘根目录，文件为文件格式，用于描述系统启动时自动加载执行的命令）文件的方式，实现在开机时记数。一旦系统启动次数达到 90 次时，该木马将隐藏磁盘的多个目录，C 盘的全部文件名也会被加密（从而导致系统无法启动）。此时，屏幕将显示信息，声称用户的软件许可已经过期，要求用户向“PC Cyborg”公司位于巴拿马的邮箱寄去 189 美元，以解锁系统。作者在被起诉时曾为自己辩解，称其非法所得用于艾滋病研究。

2001 年，专门仿冒反病毒软件的恶意代码家族（Trojan[Ransom]/Win32.FakeAV）出现，2008 年左右开始在国外流行。该恶意代码家族的界面内容为英文，又因为当时国内部分反病毒厂商已经开始采用免费的价格策略，所以该恶意代码家族在国内不容易得逞，对国内影响相对较小。FakeAV 在伪装成反病毒软件欺骗用户的过程中，所使用的窗体标题极具迷惑性。据安天 CERT 统计，其标题有数百种之多，常用标题如下表所示：

窗体标题	中文翻译
AntiSpyWare2008	反间谍软件 2008
AntiVirus2013	反病毒软件 2013
Security Defender	安全卫士
ScannRepair	扫描修复工具
Virus Doctor	病毒医生
Spyware Cleaner	间谍软件清除者/终结者
System Care Antivirus	系统护理杀毒
Data Recovery	数据恢复
AVDefender 2014	反病毒卫士 2014
AVSecurity 2015	反病毒安全 2015

Adware Checker	广告软件清除者/终结者

2005 年出现了一种加密用户文件的木马（Trojan/Win32.GPcode）。该木马在被加密文件的目录生成具有警告性质的 txt 文件，要求用户购买解密程序。所加密的文件类型包括：.doc、.html、.jpg、.xls、.zip 及.rar。

2006 年出现的 Redplus 勒索木马（Trojan/Win32.Pluder），是国内首个勒索软件。该木马会隐藏用户文档和包裹文件，然后弹出窗口要求用户将赎金汇入指定银行账号。据国家计算机病毒应急处理中心统计，来自全国各地的该病毒及其变种的感染报告有 581 例。在 2007 年，出现了另一个国产勒索软件 QiaoZhaz，该木马运行后会弹出“发现您硬盘内曾使用过盗版了的我公司软件，所以将您部分文件移动到锁定了的扇区，若要解锁将文件释放，请电邮 liugongs19670519@yahoo.com.cn 购买相应软件”的对话框。

3.2 赎金支付方式的变化

早期的勒索软件采用传统的邮寄方式接收赎金（比如 Trojan/DOS.AidsInfo），会要求受害者向指定的邮箱邮寄一定数量的赎金。我们也发现了要求受害者向指定银行账号汇款（比如 Trojan/Win32.Pluder）和向指定号码发送可以产生高额费用的短信（比如 Trojan[rog,sys,fra]/Android.Koler）的勒索软件。直到比特币（比特币是一种 P2P 形式的数字货币，可以兑换成大多数国家的货币）这种虚拟货币支付形式出现后，由于它可以为勒索软件提供更为隐蔽的赎金获取方式，2013 年以来，勒索软件逐渐采用了比特币为代表的虚拟货币的支付方式。可以说，虚拟货币的出现，加速了勒索软件的泛滥。

3.3 移动终端的勒索软件

2014 年 4 月下旬，勒索软件陆续出现在以 Android 系统为代表的移动终端。较早出现的为 Koler 家族（Trojan[rog,sys,fra]/Android.Koler）。该家族主要行为是：在用户解锁屏及运行其它应用时，会以手机用户非法浏览色情信息为由，反复弹出警告信息，提示用户需缴罚款，从而向用户勒索高额赎金。近两年的移动平台勒索软件家族样本中，东欧和俄罗斯所占比例最多，达到 59%，其次是英、美和中国。从下图可以看到安天从各国捕获的移动终端勒索软件家族的比例，其中 simplelock.a 类所占比例接近总数的一半。

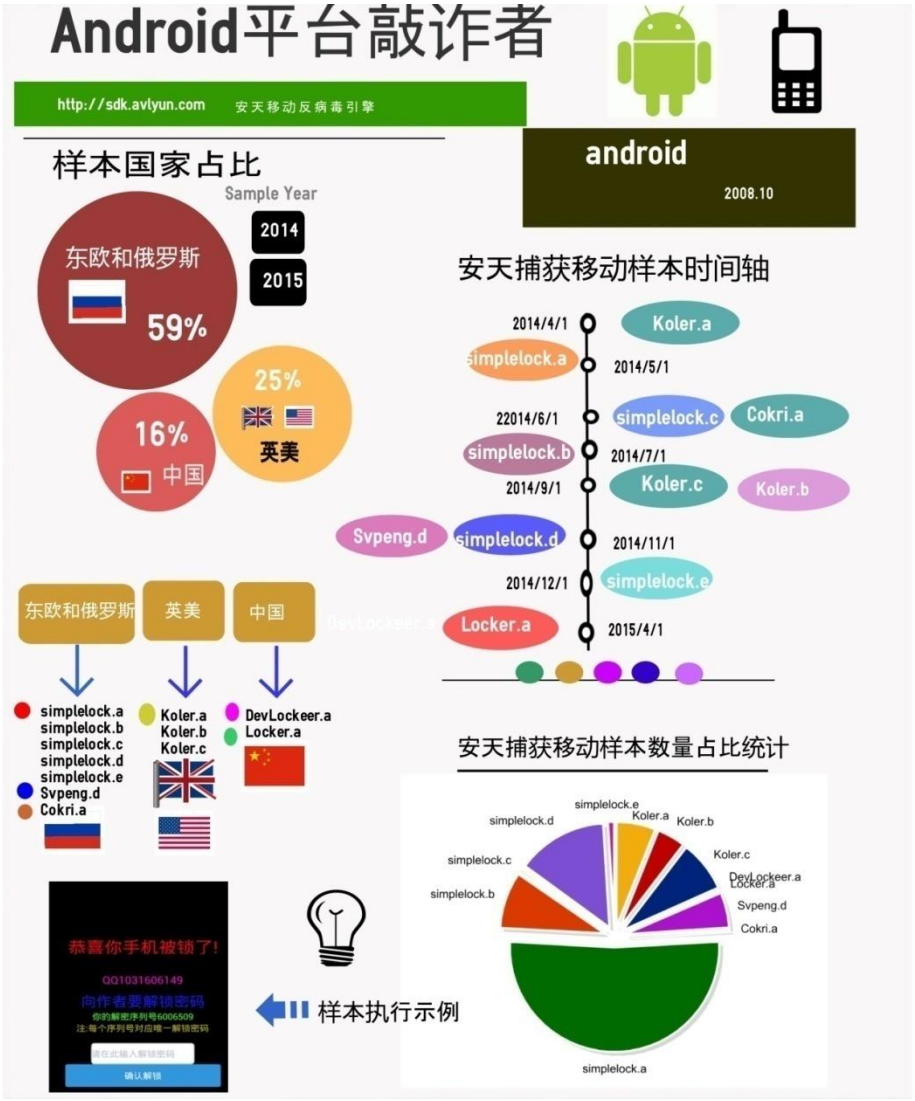


图 2 移动终端的勒索软件

典型的移动终端勒索软件家族如下表所示：

移动终端的典型勒索软件家族		
国内	DevLockeer.a	给用户手机设置锁屏密码进行勒索付费解锁。
	Locker.a	置顶勒索界面，勒索用户付费解锁。
国外	simplelock.a（东欧，俄罗斯）	置顶显示向用户勒索解锁界面，同时将用户 SD 卡上的文件进行加密。
	simplelock.b（东欧，俄罗斯）	伪装成杀毒应用，安装时要求用户激活设备管理器，运行时，强制将自身程序解锁的界面置顶，勒索用户付费解锁。
	simplelock.c（东欧，俄罗斯）	勒索用户付费解锁，将用户 SD 卡上的文件进行加密。
	simplelock.d（东欧，俄罗斯）	伪装成色情应用，强制将自身程序解锁的界面置顶，勒索用户付费解锁。
	simplelock.e（东欧，俄罗斯）	激活设备管理器，界面置顶。
	Svpeng.d（东欧，俄罗斯）	伪装杀毒界面，弹出伪装 FBI 的勒索界面，拍照显示当事人面貌，上传设备信息，强制将自身程序解锁的界面置顶，勒索用户付费解锁。
	Koler.a（英美）	解锁屏及运行其它应用会以非法浏览色情网站内容为由不断弹出警告信息，提示用户需缴罚款后才能解除。

	Koler.b（英美）	无限弹窗，清除系统数据，删除 SD 卡所有文件，强制锁屏设置新密码，勒索付费。
	Koler.c（英美）	以非法浏览色情网站内容为由不断弹出警告信息，勒索用户付费。
	Cokri.a（东欧，俄罗斯）	伪装成热门应用，运行后拦截所有来电并设置铃声静音，同时加密用户通讯录号码，然后无限弹出界面进行敲诈勒索。

3.4 新的威胁趋势

2015 年 1 月，Cryptowall 家族新变种（3.0）被发现使用 I2P 匿名网络通信，在一天内感染 288 个用户，该变种在加密受害者的文件后，向其勒索比特币，同时还有直接窃取用户比特币的行为。2 月和 4 月新出现的勒索软件家族 TeslaCrypt 和 Alpha Crypt，被发现利用了 Adobe 新近修复的 Flash 安全漏洞。同样利用这些漏洞还有 CTB-Locker、CryptoWall、TorrentLocker、BandarChor、Angler 等家族。其中最为值得关注的是 CTB-Locker，它使用了高级逃逸技术，可以躲避某些安全软件的检测。

2015 年 4 月 30 日，安天 CERT 曾接到用户提供的含有 CTB-Locker 的邮件附件，用户称已将该附件提交至第三方开放沙箱，怀疑其具有专门攻击国产办公系统的行为。经安天 CERT 分析确认，在该样本中并未发现针对国产办公环境的攻击能力。但随着勒索软件的持续泛滥和攻击手段的花样翻新，不能排除未来会出现专门针对我国办公环境的勒索软件。从目前获取的勒索软件新家族看，多数仍是采用社工手段群发邮件，但这些邮件往往紧随潮流趋势，令人防不胜防。比如：据 threatpost 报导，CTB_Locker 家族已经开始采用包含“Windows 10 免费升级”（Upgrade to Windows 10 for free）标题的社工邮件传播。

3.5 小结

从最早的“艾滋病信息木马”到最近出现的 Locker 勒索软件，二十几年的时间里，虽然勒索软件的新家族层出不穷，但主要的勒索方式仍以绑架用户数据为主。下图展示了 1989 年到 2015 年间勒索软件的演进史，在图片左侧标明了几个重要的时间点，从图中可以看出随着 Android 平台的日益普及，面向移动终端的勒索软件也日渐增多；随着比特币的广泛应用，以比特币代为赎金支付形式的勒索软件也逐渐多了起来。

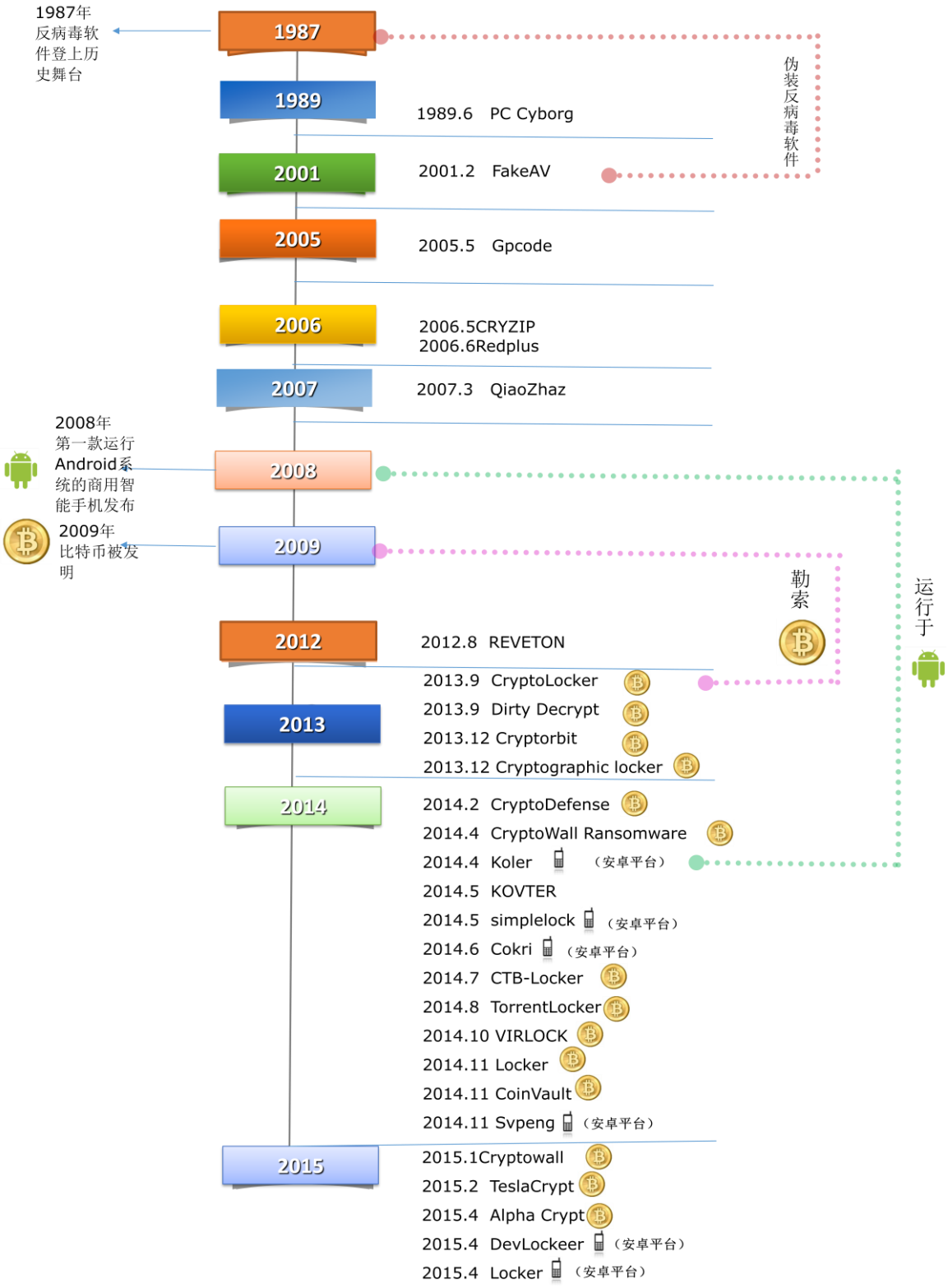


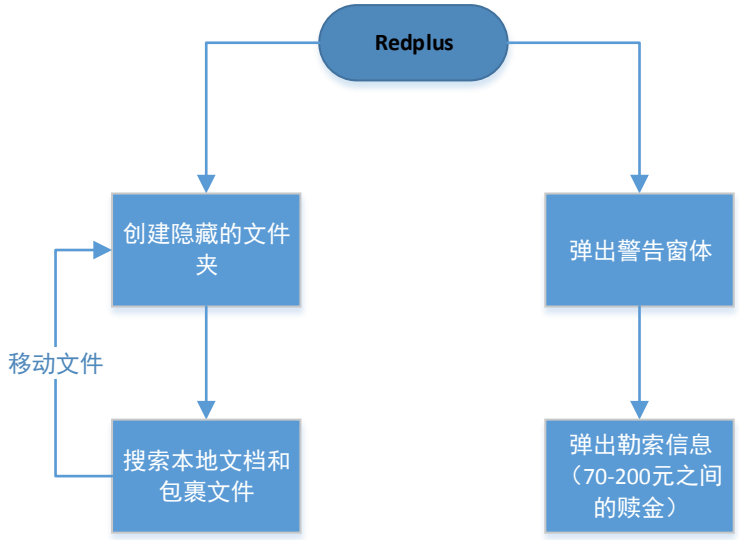
图 3 勒索软件的演进史

4 典型勒索软件家族分析

勒索软件的本质是木马，下面以几个典型勒索软件家族为例，详细地介绍其勒索过程，力求揭开勒索软件的真面目。

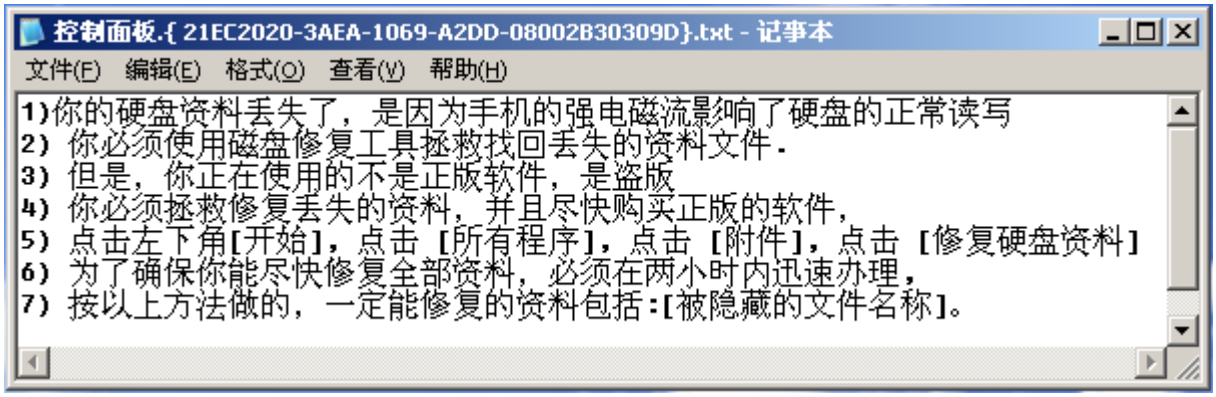
4.1 Redplus

安天在 2006 年 6 月 9 日捕获了国内最早出现的 Redplus 敲诈者木马，该木马会隐藏用户的文档文件，向用户勒索 70 元至 200 元不等的赎金。Redplus 木马运行后首先弹出虚假正版软件的对话框，点击 OK 后，会弹出勒索窗口。其主要行为流程如下：



Redplus 木马勒索 70 元至 200 元之间的一个赎金数目，并将赎金数编辑到需要发送的短信中，如（赎金数=70，需要发送的短信内容为=00000012020901100006101O#70）。

Redplus 木马为达到目的，生成的文本文件内容如下：

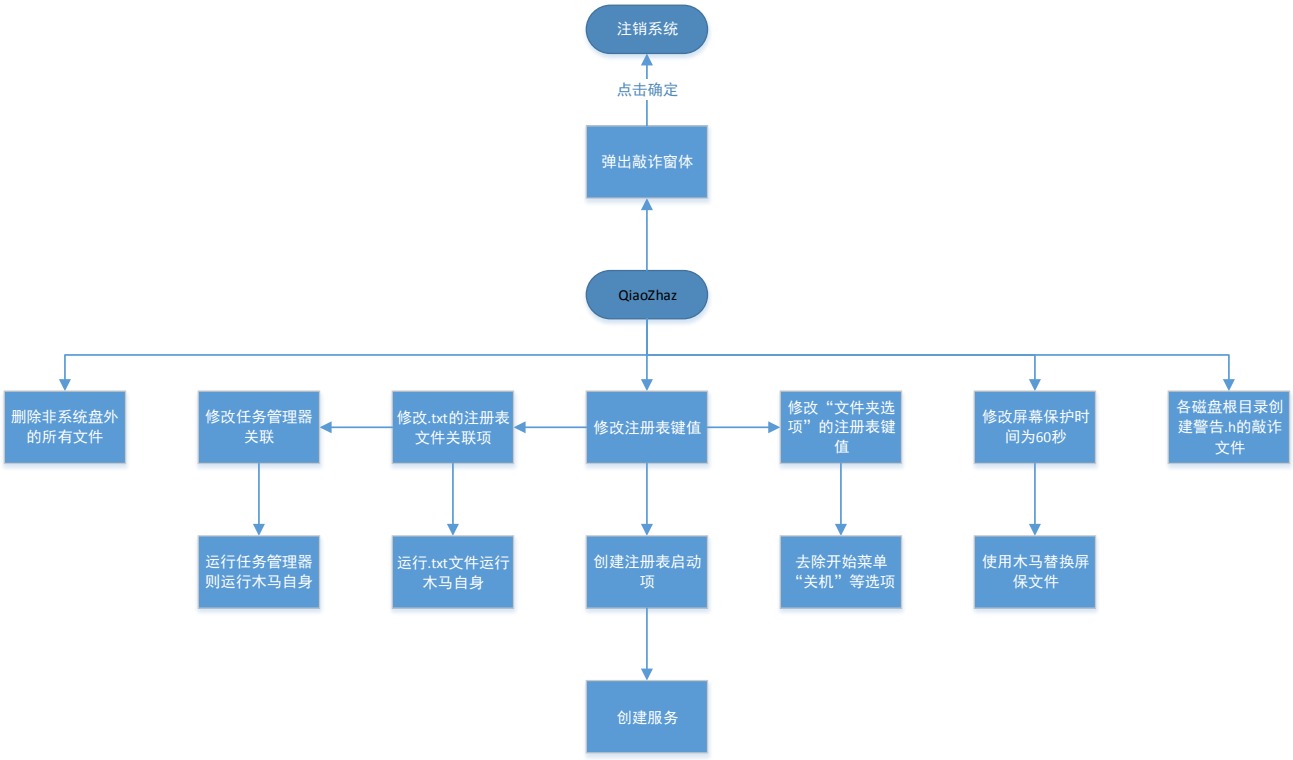


Redplus 木马在本地磁盘根目录下建立一个属性为系统、隐藏和只读的备份文件夹，名为“控制面板.{21EC2020-3AEA-1069-A2DD-08002B30309D}”，同时搜索本地磁盘上的用户文档和包裹文件（包括.xls、.doc、.mdb、.ppt、.wps、.zip、.rar），把搜索到的文件移动到上述备份文件夹中，造成用户常用文档丢失的假象，趁机勒索钱财。

Redplus 木马的作者欧阳某某于 2007 年在广州落网，共借助 Redplus 木马勒索款项 95 笔，合计人民币 7061.05 元。法院考虑到其自首情节，最终判其有期徒刑 4 年。

4.2 QiaoZhaz

2007 年 3 月 1 日至 2 日，安天分别捕获了两个敲诈者病毒，分别命名为 QiaoZhaz.c 和 QiaoZhaz.d。当用户中了 QiaoZhaz 后，弹出“发现您硬盘内曾使用过盗版了的我公司软件，所以将您部分文件移动到锁定了的扇区，若要解锁将文件释放，请电邮 liugongs19670519@yahoo.com.cn 购买相应软件”的对话框，当用户点击“确定”按钮后，系统会自动注销，全屏黑屏。QiaoZhaz 的行为流程图如下：



由于木马添加了注册表启动项和服务，导致每次开机后点击确定后木马就注销系统。去除“文件夹选项”，使用户无法选择“显示所有隐藏文件”并无法去掉“隐藏受保护的系统文件”“隐藏已知文件类型的扩展名”。去除开始菜单中的“搜索”、“运行”项和“关机”项，使用户不能使用搜索、command 命令和关机、注销。修改 txt 文件关联，当用户试图运行 txt 文件时，则会激活木马，使用同样的方法修改任务管理器关联，当用户打开任务管理器时就会激活木马。木马把屏保时间修改为 60 秒，在%system32%文件夹下生成木马屏保文件，当用户 60 秒不操作计算机时，系统会自动运行木马。该木马利用多种方法保护自身，结束指定的反病毒软件或反病毒工具。

QiaoZhaz.d 的行为更加恶劣，它除上述与 QiaoZhaz.c 相似的行为外，还删除非系统盘外的所有文件，使用户必须使用数据恢复软件才能找回原来的数据。同时在每个磁盘根目录下建立一个名为“警告.h”的文件，以此向用户进行敲诈勒索。

安天在 2007 年 3 月 6 日发布了“敲诈者病毒变种专用注册表修复工具”，是专门针对 QiaoZhaz 的注册表修复工具。

4.3 CryptoLocker

CryptoLocker 在 2013 年 9 月被首次发现，它可以感染大部分的 Windows 操作系统，包括：Windows XP、Windows Vista、Windows 7、Windows 8。CryptoLocker 通常以邮件附件的方式进行传播，附件执行之后会使用 RSA&AES 对特定类型的文件进行加密。并弹出勒索窗体，如下图所示：

图 4CryptoLocker 的勒索界面

完成加密操作弹出付款窗口，需要用户使用 moneypak 或比特币，在 72 小时或 4 天内付款 100 或 300 美元，方可对加密的文件进行解密。

加密的文件类型：

*.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.eps, *.ai, *.indd, *.cdr, ????????.jpg, ????????.jpe, img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c

安天 CERT 分析人员测试了一个已知的 CryptoLocker 样本，由于服务器已经无法正常返回，导致网络数据包通信不完整，如下图所示：

```
POST /home/ HTTP/1.1
Accept: */*
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
Host: otjsqhyceuwmr.info
Content-Length: 192
Cache-Control: no-cache
Pragma: no-cache

......'.Tf.....D`!X=.J.g..8....L.%
..,.t*U..|g..b....t.{.3D...RY....m;..&.........U.......!vZ;....L..
\............|.PO..gl.....,.*...w..?d{..H.j.......t....n.ep...On}...
....HTTP/1.1 405 Not Allowed
Server: nginx
Date: Thu, 11 Jun 2015 03:00:28 GMT
Content-Type: text/html
Content-Length: 568
Connection: close

<html>
<head><title>405 Not Allowed</title></head>
<body bgcolor="white">
<center><h1>405 Not Allowed</h1></center>
<hr><center>nginx</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

图 5CryptoLocker 的网络通信

ESET 在 2013 年 12 月发表了一篇文章，对新出现的 Cryptolocker 2.0 与 Cryptolocker 进行了相关技术的对比，如下表[4]：

	Cryptolocker	Cryptolocker 2.0
ESET 检测的病毒名	Win32/Filecoder.BQ	MSIL/Filecoder.D, MSIL/Filecoder.E
编写语言	C++	C#
付款方式	Monepak,Ukash,cashU,Bitcoin	Bitcoin
对称加密方式	RSA-2048	RSA-4096
C&C 通信加密方式	RSA	AES
C&C 地址	硬编码，动态生成的随机域名	硬编码

由于 Cryptolocker 所使用的技术在 CTB-Locker 中基本都包含，并未对该类勒索软件进行深入分析，具体细节请看下面 CTB-Locker 的分析。

4.4 CTB-Locker

CTB-Locker 是 Curve-Tor-Bitcoin Locker 的缩写，是当前全球影响较大的勒索软件家族，主要通过邮件附件传播，使用高强度的加密算法，加密用户系统中的文档、图片、数据库等重要资料。加密完成后，CTB-Locker 会采用弹出窗体和修改桌面背景等方式，提示用户支付赎金，并要求用户在 96 小时内支付 8 比特币（约合人民币 1 万元）赎金，否则将销毁用户文件。该家族在国外一直很活跃，国内也陆续出现受害者。该家族的另一个特点是使用洋葱路由（Tor），通过完全匿名的比特币交易方式获取赎金，这使得该勒索软件的作者难以追踪。

典型攻击流程如下图所示：

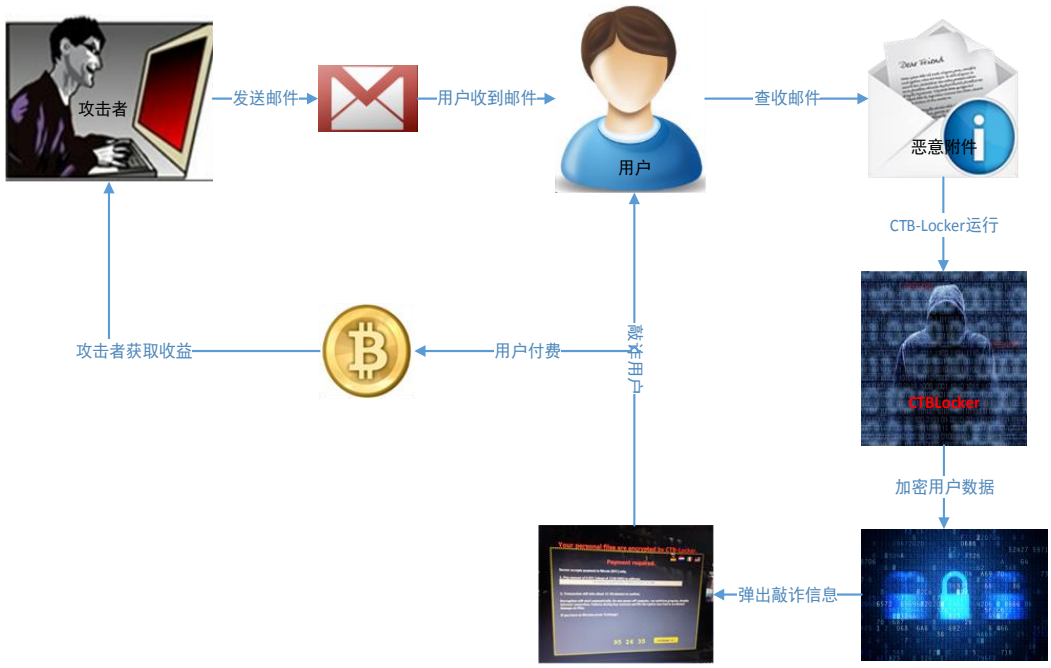


图 6CTB-Locker 的攻击流程

安天 CERT 分析人员随机提取了一个样本，该样本执行后，会弹出窗体要求用户向其支付赎金。

图 7CTB-Locker 的勒索界面

同时，还会修改桌面背景，告诉用户如何下载安装 Tor 浏览器，以及如何通过 Tor 浏览器访问其赎金支付页面。

图 8CTB-Locker 要求用户安装 Tor 浏览器

通过分析该样本，可以了解 CTB-Locker 的一般执行过程，如下图所示。

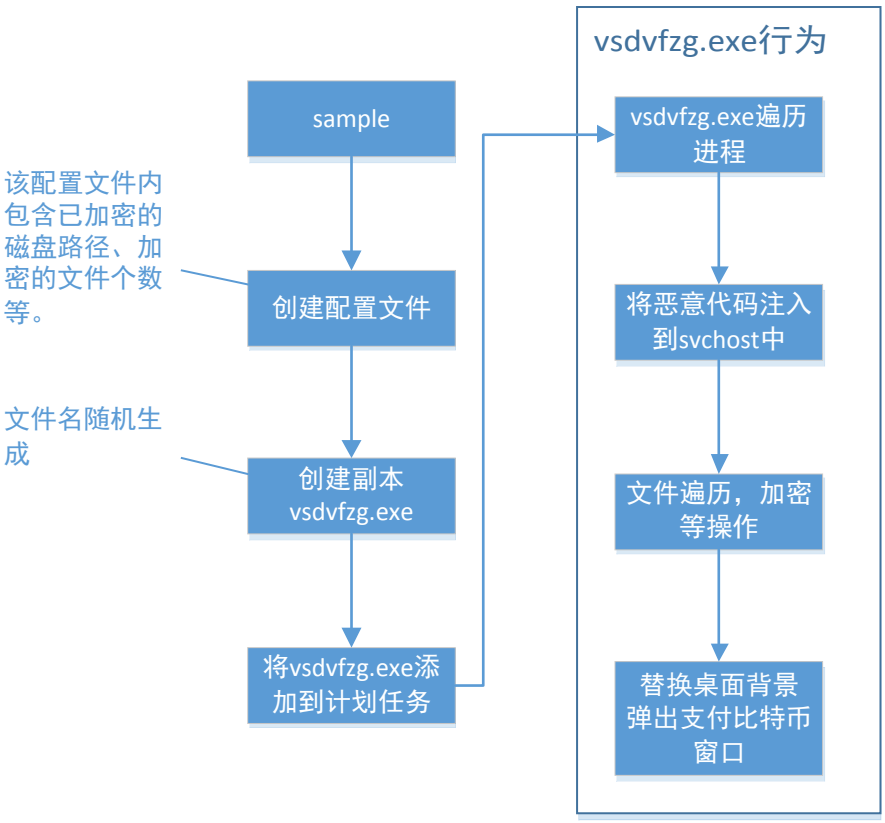


图 9CTB-Locker 样本一般执行过程

该样本在文件遍历过程中，一旦发现具有以下后缀的文件时，将对其进行加密操作。

图 10 解密后的 CTB-Locker 文件扩展名数据

加密部分是比较关键的一部分，在这里重点说明一下。

首先样本会将要加密的文件以后缀名为.tmp 的形式调用函数 MoveFileEx 移动到临时目录下面。接着根据文件的时间和和当前系统运行的时间等信息，填充一个缓冲区。然后对这个缓冲区计算 SHA256。根据计算的 SHA256 值作为会话私钥(session private key)使用 Elliptic curve Diffie-Hellman（ECDH）算法产生一个会话公钥（sessIonpublickey)。再与配置文件中的一个主公钥（master public key）使用 ECDH 算法产生一个会话共享密钥(session shared secret)，对会话共享密钥计算 SHA256 并将这个值作为 AES 加密的 KEY。相关代码如下：

```
lea     eax, [ebp+50h+var_104]
push    eax
lea     eax, [ebp+50h+var_124]
push    eax
lea     eax, [ebp+50h+var_B4] ; 产生会话公钥
push    eax
call    sub_25F63FF
push    offset najzljf_data
lea     eax, [ebp+50h+var_124]
push    eax
lea     eax, [ebp+50h+var_164] ; 会话共享密钥(session shared secret)
push    eax
call    sub_25F63FF
lea     eax, [ebp+50h+var_144]
push    eax
lea     eax, [ebp+50h+var_164]
push    20h ; ' '
push    eax
call    Sha256          ; 计算sha256
mov     edi, [ebp+50h+arg_1C] ; 加密后的密钥
```

需要说明的是，这个 AES 密钥是要保存到该函数的一个参数中给调用者的，但是调用者只是保存了 5 个 AES 密钥，这也就是为什么离线模式下 CTB-Locker 仍然能够解密 5 个文件的原因。把文件读取出来，然后使用 ZLIB 压缩后使用 AES 加密。加密的数据从一个临时文件的头部偏移 0x30 位置开始写入。文件加密完后会向临时文件的头部写入 0x30 的数据，其中开头的 0x20 字节就是会话公钥。文件加密后五个 AES 加密的密钥，加密文件个数，加密的磁盘等信息会保存在配置文件中。

4.5 移动平台勒索软件

2014 年 4 月，国外开始出现移动平台勒索软件，国内也很快出现了类似软件，并且有愈演愈烈地趋势。目前国内外出现的移动平台的赎金方式有人民币、Q 币、美元、卢布等，勒索方式有锁屏、加密文件、加密通讯录等方式。据了解该类软件爆发后国内已经有上千人的手机受到感染。这类勒索软件的发展将对用户手机及资料形成严重威胁。

国内出现的勒索软件通常伪装游戏外挂或付费破解软件，用户点击即会锁定屏幕，需加手机界面留下

的 QQ 号为好友去支付赎金才能解锁。

下面是该类勒索软件的一个真实案例。受害用户手机被锁定，勒索软件作者在手机界面给出 QQ 号码，要求受害用户加 QQ 好友并支付一定赎金才能解锁。

用户加该 QQ 后会提示回答验证问题。在该案例中，可以看到勒索者的相关资料，在用户个人信息中可以看到勒索者的相关身份信息，但无法确保其真实性。

图 11 勒索过程示意图

在受害用户加好友以后，勒索软件作者与其聊天，勒索人民币 20 元，并要求用户转账到指定支付宝账户才给出解锁密码。据了解，该勒索软件作者同时也对其他 Android 手机用户进行勒索行为，并且在受害用户支付赎金后，未能提供解锁密码。甚至还在勒索软件中加入短信拦截木马功能，盗取用户支付宝和财富通账户。有时，受害用户在多次进行充值、转账等方式后，仍不能获得解锁密，甚至会被勒索软件作者将受害用户加入黑名单。

5 防御：我该做什么

5.1 安全建议与部分解决办法

为了避免受到勒索软件的威胁，对于 PC 用户，安天 CERT 安全工程师给出如下建议：

1. 及时备份重要文件
2. 及时安装更新补丁，避免一些勒索软件利用漏洞感染计算机
3. 给信任网站添加书签并通过书签访问
4. 对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接
5. 定期用反病毒软件扫描系统

对于 Android 平台的移动终端用户，建议如下：

1. 安装手机杀毒软件（比如 LBE 安全大师、安天 AVL Pro 等）
2. 由可靠的安卓市场下载手机应用程序

对于已经受到勒索软件感染的移动终端用户，可以尝试使用以下方式：

1．如果手机 root 并开启 USB 调度模式，可进入 adb shell 后直接删除恶意应用

2．如果是利用系统密码进行锁屏，部分手机可尝试利用找回密码功能

3．进入手机安全模式删除恶意应用程序。主流安卓手机进入安全模式的方式是，按住【电源键】开机，直到屏幕上出现品牌 LOGO 或运营商画面后，按住【音量减少】键不放。如果进入安全模式成功，锁屏界面的左下角会显示“安全模式”字样。此时可对恶意应用进行正常的卸载处理。

5.2 普通用户的防御方法

通过前面的分析可以看出，采用高强度加密方式绑架用户数据的勒索软件，将对用户的数据安全构成严重威胁，做好安全防御显得极为重要。普通用户可下载专门的防御产品如 CryptoMonitor（该程序可以根据行为检测结果，在勒索软件试图加密用户数据时将其阻止[5]）。

5.3 企业用户的防御方法

对于企业用户来说，针对勒索软件类的安全威胁防护可从预警、防御、保护、处置和审计几个步骤来进行有效防御和处理，保护系统免受攻击。首先，将企业用户接触到的未知应用程序自动提交到企业内部的云平台，通过特征检测、虚拟化执行等方式集中鉴定，及时发现恶意程序。其次，企业 IT 管理人员可将具有重要价值的文件资源的主机设置为重要计算机或受限计算机，一旦勒索软件或其它可疑程序运行时，可以通过可信应用基线（白名单）检测的方式及时将其发现，并予以阻止。再次，可采用安全文档措施保护具有重要价值的文件。最后，通过云端追溯功能来对恶意样本进行全网追查，便于事后审计和定损。

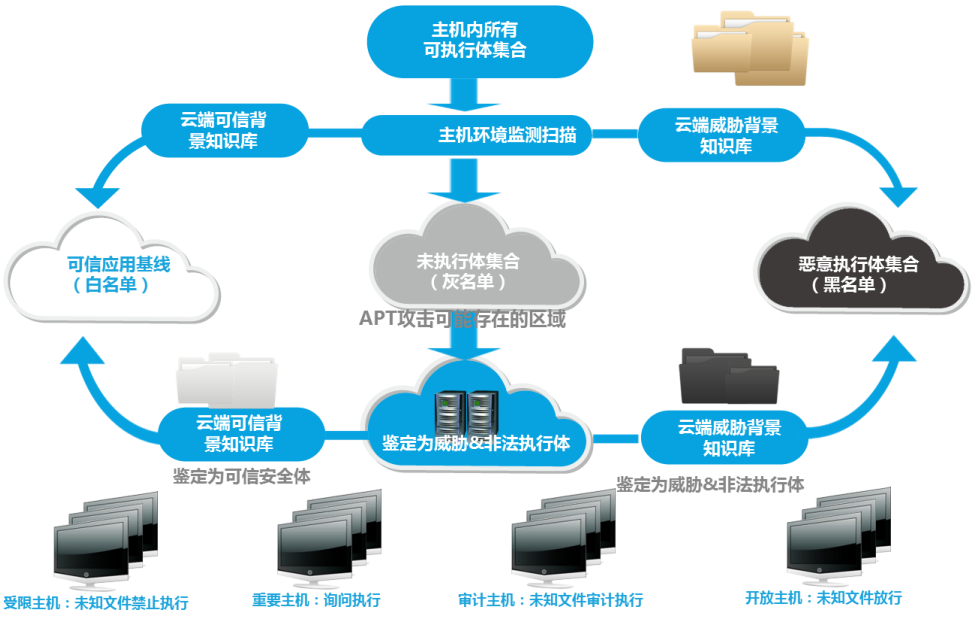


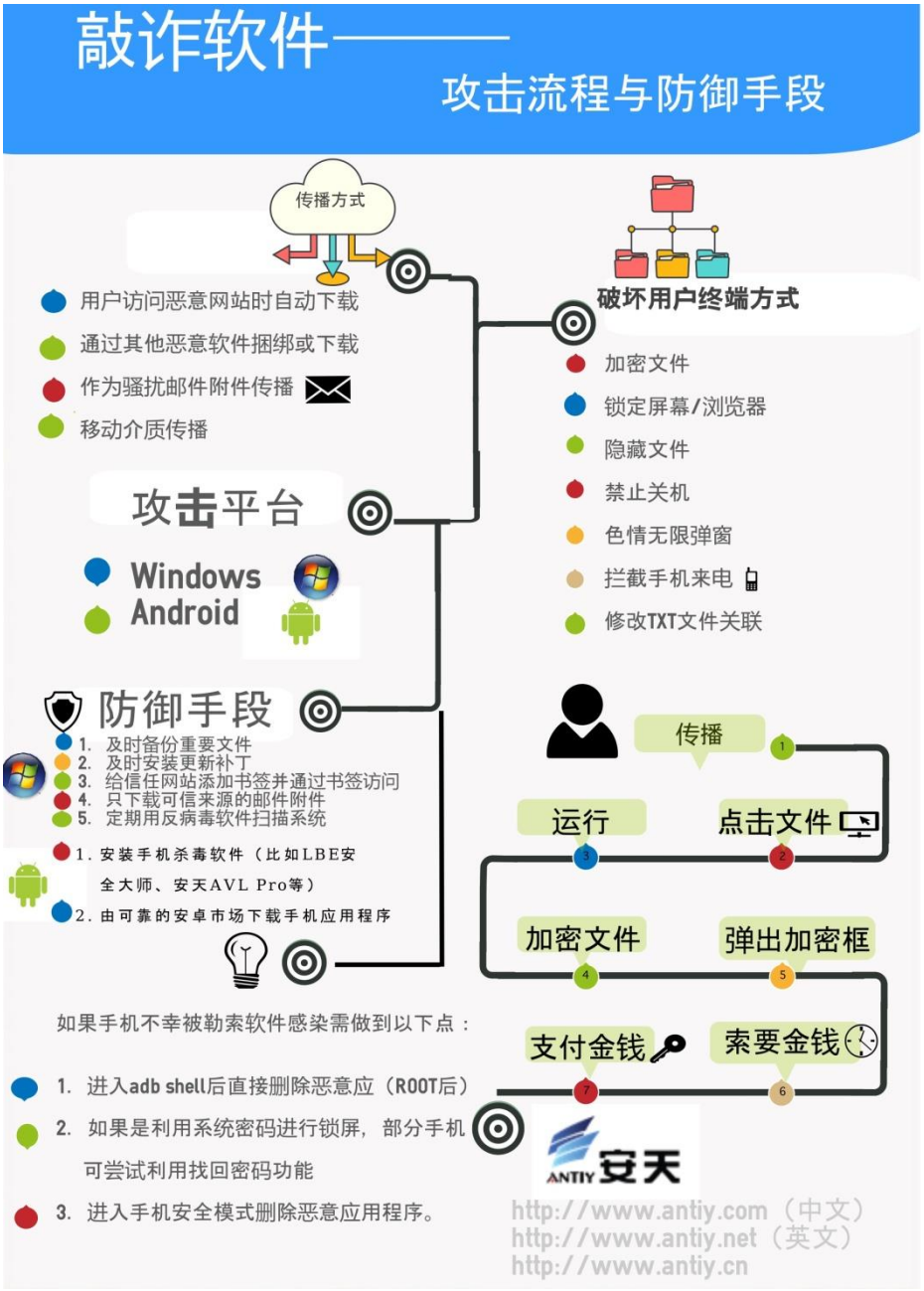
图 12 安天企业安全产品工作流程

6 总结

勒索软件的技术含量虽然不高，却可以对用户的数据安全造成严重危害，其威胁不可小觑。

2015 年 5 月底，勒索软件 Locker 的作者公布了其使用的勒索数据库并公开表达了歉意，随后还提供了自动解密程序供受害者使用。据统计，该数据库中共包含 62,703 条勒索记录。按该软件显示的勒索金额 0.1 比特币（约合 175 元人民币）计算，如果这些受害者都支付赎金，作者获得的非法收入可达一千万元。在巨额非法收入的诱惑下，很可能会有越来越多的恶意代码作者开始从事勒索软件的开发，借助比特币等难于追踪的支付方式的保护，勒索软件的作者也会越来越有恃无恐。

希腊战士跳出木马，杀死睡梦中的守军，打开城门。城外隐藏的军队如潮水般涌入特洛伊城，将城市烧成一片灰烬。此时的特洛伊人懊悔没有听从拉奥孔的劝告，但为时已晚……对于一般的感染式病毒或木马，即使用户在遭受安全威胁之后再安装反病毒软件，依然可以亡羊补牢，让系统重新处于安全状态。但对于绑架用户数据的勒索软件而言，没有可靠的事前防御和检测能力，面对已经被勒索软件加密的用户数据，侧重于保护系统安全的反病毒软件也无能为力。只有安装侧重于保护数据安全的工具或部署针对企业安全特点的安全产品，才能尽量避免给勒索软件以可乘之机。



附录一：参考资料

[1] 来源：CryptoLocker Ransomware

http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/

[2] 来源：恶意勒索软件 ScarePackage 肆虐美国 Android 用户需小心提防

http://www.cnbeta.com/articles/322803.htm

[3] 来源：新型恶意勒索软件 VirLock

http://netsecurity.51cto.com/art/201412/462202.htm

[4] 来源：Cryptolocker 2.0 – new version, or copycat?

http://www.welivesecurity.com/2013/12/19/cryptolocker-2-0-new-version-or-copycat/

[5] 来源：EasySync CryptoMonitor

https://easysyncsolutions.com/CryptoMonitorDetails

[6] 来源：CryptoLocker Ransomware Information

http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

[7] 来源：ransomware would you pay up？

https://nakedsecurity.sophos.com/2012/09/25/ransomware-would-you-pay-up/

[8] 来源：Ransomware

http://www.trendmicro.com/vinfo/us/security/definition/ransomware

[9] 来源：cryptowall ransomeware-removal

http://translate.google.com.hk/translate?langpair=auto%7Czh-CN&u=http://www.enigmasoftware.com/cryptowallransomware-removal/

[10] 来源：Crytplocker_Update_RevD

https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25203/en_US/Cryptolocker_Update_RevD.pdf

[11] 来源：ransomware internal publication

https://sites.google.com/site/alonjb/ransomwareinternalpublication

[12] 来源：ransomware-kovter-infections-on-the-rise

http://www.csoonline.com/article/2156408/malware-cybercrime/ransomware-kovter-infections-on-the-rise.html

[13] 来源：reveton-ransomware-upgraded-with-powerful-password-stealer

http://www.pcworld.com/article/2466980/reveton-ransomware-upgraded-with-powerful-password-stealer.html

[14] 来源：inside-a-reveton-ransomware-operation

http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

[15] 来源：“攻击 WPS 样本”实为敲诈者

http://www.antiy.com/response/CTB-Locker.html

[16] 来源：部分利用社工技巧的群发邮件样本关联分析

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

[17] 来源：勒索软件 CTB-Locker 核心原理的一些疑问和分析

http://www.freebuf.com/articles/system/57918.html

[18] 来源：Windows 10 Upgrade Spam Carries CTB-Locker Ransomware

https://threatpost.com/windows-10-upgrade-spam-carries-ctb-locker-ransomware/114114

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