勒索软件简史

安天安全研究与应急处理中心（安天 CERT）

勒索软件已经成为当今网络安全的主流威胁之一。如果说前几年我们对勒索软件这一名词还略感陌生，那么现在则不得不重新对其进行认识与审视。安天最早从 2014 年开始全面跟踪勒索软件专题的恶意程序， 2014 年 4 月 30 日，安天接到用户称其专门攻击 wps 办公系统的恶意邮件附件，确认攻击者为 CTB–Locker（敲诈者），并发布《“攻击 WPS”样本实为敲诈者》，2015 年发布系统全面地介绍勒索软件的报告《揭开勒索软件的真面目》。之后的 2016 年是勒索软件大规模爆发的一年，随着勒索软件攻击趋向本地化、多语言化的发展，我国也从一个过去很少受到勒索软件感染的国家变成如今受感染最严重的国家之一。

自 1989 年勒索软件出现至今，已有近三十年的历史，漫长的岁月不但没有使其逐渐消亡，反而愈演愈烈。从最初的伪装反病毒软件到勒索比特币，再到开始感染不同平台，不断进行开发与更新，如今勒索软件已然呈爆发性增长，成为不可小觑的威胁。因此，我们必须要重视这一威胁，并提早部署有效的防御措施，安天等很多网络安全厂商也都在其安全防护产品中添加了针对勒索软件的防护模块。本文我们将回顾以往关于勒索软件的内容，并结合 2016 年至今勒索软件发生的新变化，更加系统和深入地带领读者认识勒索软件。

一、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。

暗网又称深网、不可见网、隐藏网，即指那些存储在网络数据库里，但不能通过网页跳转的访问方式，而需要通过动态网页技术访问的资源集合，不属于那些可以被标准搜索引擎索引的表面网络。

随着互联网的迅速发展，一些非法分子利用网络匿名的特性，通过比特币的交易形式开始了一些不为人知的非法交易。匿名支付的网络特性在一定程度上为不法分子通过比特币进行的交易给予了很大的支撑。比特币是一种通过密码编码，在复杂算法的大量计算下产生的电子货币。暗网具有一定的隐秘性，在保护隐私的同时，也为犯罪分子提供了安全的窝巢。那么，比特币和暗网一旦结合，则使整个勒索过程变得密不透风。在有些攻击者给出的勒索信上，甚至还“贴心”地介绍了进入暗网的方法，比特币的购买方法和支付方法。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

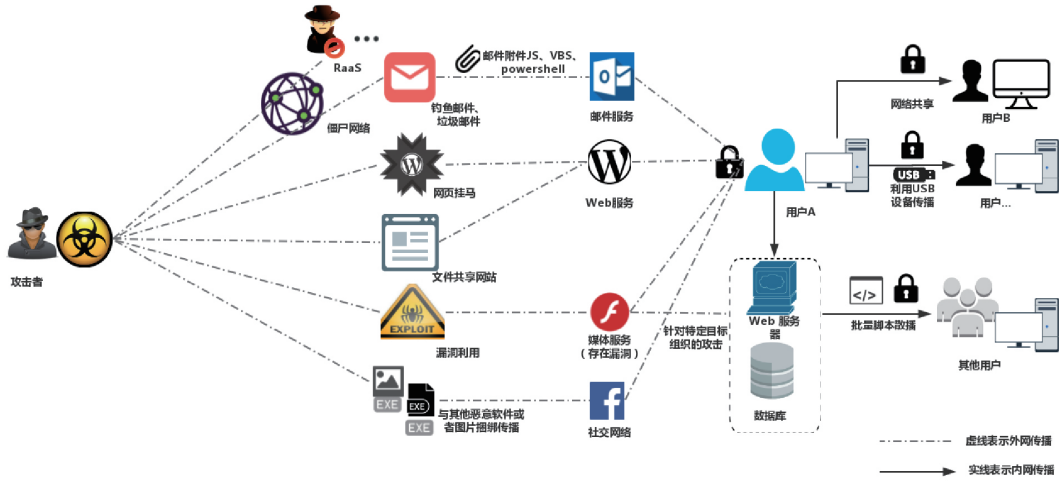


图 1

二、主要传播手段

勒索软件的传播手段主要以成本较低的邮件传播为主。同时也有针对医院类特定组织的攻击，通过入侵组织内部的服务器，使用批量脚本及其勒索软件负载的简单组合，通过半自动化的方式向网络中散播勒索软件。随着人们对勒索软件的警惕性提高，勒索者也增加了其他的传播渠道，具体的传播方式如下：

● 邮件传播：攻击者以广撒网的方式大量传播垃圾邮件、钓鱼邮件，一旦收件人打开邮件附件或者点击邮件中的链接地址，勒索软件会以用户看不见的形式在后台静默安装，实施勒索；

● 漏洞传播：当用户正常访问网站时，攻击者利用页面上的恶意广告验证用户的浏览器是否有可利用的漏洞。如果存在，则利用漏洞将勒索软件下载到用户的主机；

● 捆绑传播：与其他恶意软件捆绑传播；

● 僵尸网络传播：一方面僵尸网络可以发送大量的垃圾邮件，另一方面僵尸网络为勒索软件即服务 (RaaS) 的发展起到了支撑作用；

● 可移动存储介质、本地和远程的驱动器（如 C 盘和挂载的磁盘）传播：恶意软件会自我复制到所有本地驱动器的根目录中，并成为具有隐藏属性和系统属性的可执行文件；

● 文件共享网站传播：勒索软件存储在一些小众的文件共享网站，等待用户点击链接下载文件；

● 网页挂马传播：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；

● 社交网络传播：勒索软件以社交网络中的 .JPG 图片或者其他恶意文件载体传播（见图 1）。

三、勒索软件的演进（见图 2）

1. 最早的勒索软件

已知最早的勒索软件出现于 1989 年，是由哈佛大学毕业的 Joseph Popp 创建。该勒索软件发作后，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，称其非法所得费用用于艾滋病研究。该木马采取的方式为对称加密，解密工具很快可恢复文件名称，但该恶意代码开启了近 30 年的勒索软件攻击。

2. 加密用户文件的勒索软件

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下生成，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。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

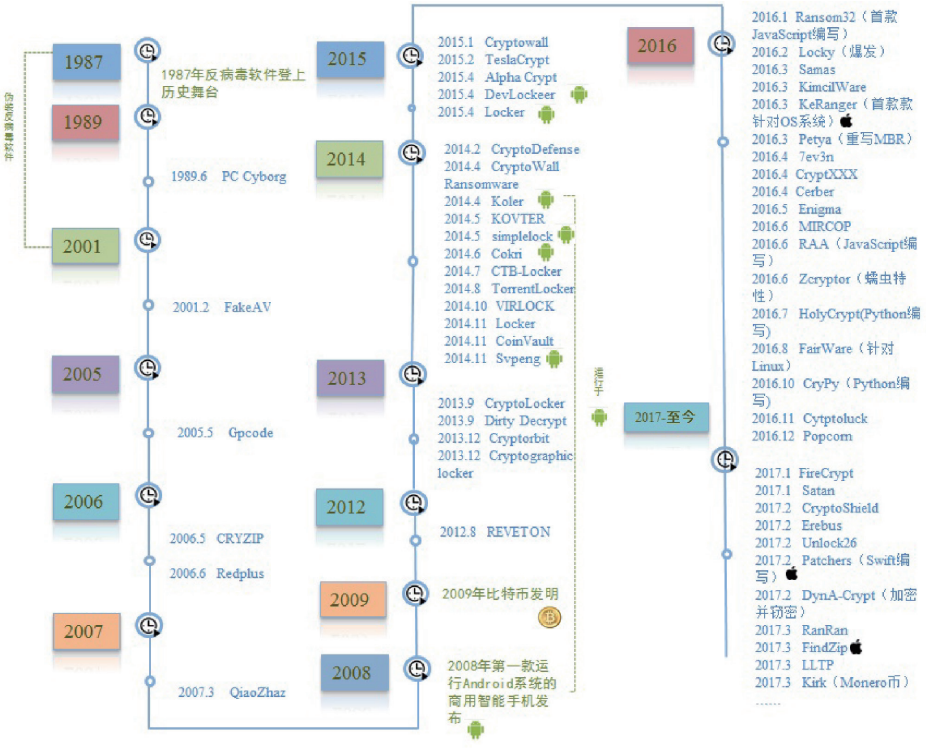


图 2　勒索软件发展史

3. 首次使用 RSA 加密的勒索软件

Archievus 是在 2006 年出现的勒索软件，勒索软件发作后，会对系统中“我的文档”目录中所有内容进行加密，并要求用户从特定网站购买来获取密码解密文件。它在勒索软件的历史舞台上首次使用 RSA 加密算法。RSA 是一种非对称加密算法，让加密的文档更加难以恢复。

4. 国内首个勒索软件

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。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。

5. 最早出现的 Android 平台勒索软件家族

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，而较早出现的为 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。

6. 首例 Linux 平台勒索软件

俄罗斯杀毒软件公司 Doctor Web 的研究人员发现了一种新的勒索软件，命名为 Linux.Encoder.1，该勒索软件是针对 Linux 系统的恶意软件。这个 Linux 恶意软件使用 C 语言编写，它启动后作为一个守护进程来加密数据，以及从系统中删除原始文件，使用 AES-CBC-128 对文件加密之后，会在文件尾部加上“.encrypted”扩展名。

7. 首例具有中文提示的勒索软件

安天在 2016 年 2 月发现一款新的勒索软件家族，

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

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提示勒索文件。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。“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。

四、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。

1. 主攻 Windows 的 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，如图 3 所示：

完成加密操作弹出付款窗口，需要用户使用

图 3 CryptoLocker 的勒索界面

moneypak 或比特币，在 72 小时或 4 天内付款 300 美元或欧元，方可对加密的文件进行解密。

2. 匿名交易 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。

3. 勒索软件即服务模式 Cerber

自 2016 年开始，采用勒索软件即服务（Ransomware-as-a-Service）模式，名为 Cerber 的勒索软件开始爆发。攻击者在 2016 年下半年开始了频率极高的版本升级，仅在 8 月份就发现了 Cerber2 和 Cerber3 两个版本，而在 10 月及 11 月，Cerber4 和 Cerber5 相继推出。

勒索软件即服务（RaaS）是一整套体系，指从勒索到解锁的服务。勒索软件作者开发出恶意代码，通过在暗网中出售、出租或以其他方式提供给有需求的攻击者作为下线，下线实施攻击并获取部分分成，原始开发者获得大部分利益，在只承担最小风险的前提下扩大了犯罪规模。而采用这种服务模式的勒索软件越来越多地将目标放在了企业上，对于很多企业来说，他们不希望失去重要的数据资料，因此更愿意去支付赎金。

Cerber 通过垃圾邮件和漏洞利用工具 Rig-V Exploit EK 传播，自 Cerber4 开始，它不再使用 Cerber 作为加密文件的后缀，而是使用 4 个随机字符。Cerber 采用 RSA2048 加密文件，拥有文件夹及语言地区的黑名单，而在黑名单中的文件夹及语言地区均不能加密。

4. 中文提示勒索软件 Locky

安天 CERT 在 2016 年 2 月份发现了一款新的勒索软件家族，名为“Locky”。它通过 RSA-2048 和

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

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。

Locky 恶意代码样本运行后，显示中文的提示信息，如图所示。

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；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。

5. “传销”解密的 PopcornTime

自 2016 年末开始，一种名为 PopcornTime 的新型勒索软件逐渐活跃。该勒索软件正在不断地被进行新版本的开发，研究人员还在暗网中发现了该勒索软件的源代码。该勒索软件有一个与众不同的特点：除了支付 1 个比特币解密文件之外，还可以将恶意代码链接发送给其他人，如果两名以上的受害者支付了赎金，最初的受害者就可以获得免费的解密密钥。受害者很有可能为了解密文件而将勒索软件传播出去，这种方式也许会成为勒索软件发展的新趋势。

PopcornTime 在后台加密特定目录、特定后缀名的用户文件。特定目录包括：我的文档、图片、音乐和桌面共四个文件夹，特定后缀名共 500 余种。解密方式除了正常的支付比特币，增加了“传销”解密的方式，即只要发展两个下线（让其他两个人中招且支付赎金），就可以获取解密密钥。

6. 典型勒索软件家族对比

安天 CERT 对以上五个典型勒索软件家族特点进行了总结，如表 1 所示。

表 1

	Cryptolocker	CTB-Locker	Cerber	Locky	PopcornTime
发现时间	2013 年 9 月	2015 年初	2016 年初	2016 年 2 月	2016 年末
传播途径	邮件附件	邮件附件	邮件附件 漏洞利用	邮件附件	邮件附件 受害人为解密文件而向外传播
付款方式	Monepak/Ukash/cashU/Bitcoin	Bitcoin	Bitcoin	Bitcoin	Bitcoin
赎金数量	300 美元 / 欧元	8 比特币	1 比特币	0.5 比特币	1 比特币
被加密文件后缀名	.crypt	7 位随机字符	.cerber-->4 位随机字符	.locky	.filock
加密文件格式数量	71	114	400 左右	140 左右	500 左右

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

7. 可感染工控设备的 LogicLocker

在 2017 年旧金山 RSA 大会上，乔治亚理工学院（GIT）的研究员向人们展示了一种可以感染工控设施，向中水投毒的勒索软件，名为 LogicLocker。它可以改变可编程逻辑控制器（PLCs），也就是控制关键工业控制系统（ICS）和监控及数据采集（SCADA）的基础设施，例如发电厂或水处理设施。通过 LogicLocker，他们可以关闭阀门，控制水中氯的含量并在机器面板上显示错误的读数。

LogicLocker 针对三种已经暴露在互联网上的 PLC，感染后修改密码，锁定合法用户并要求赎金。如果用户付钱，他们可以找回他们的 PLC。但是如果没有，攻击者可以使水厂设备发生故障，或者向水中投入大量威胁生命的氯元素。

该勒索软件攻击生命周期包括对 PLC 的攻击、侦察并感染更多的 PLC、获取设备密码和控制列表等资源、窃取并加密 PLC 程序及通过邮件进行勒索这几个节点。如图所示：

针对工业控制系统的攻击并不新鲜，Stuxnet、Flame 和 Duqu 已经给我们以震惊。但是对于勒索软件的攻击却是头一次，以金钱为目标的攻击者可能很快就会瞄准关键的基础设施，而在这些攻击的背后，很可能是拥有国家背景的攻击者们。

8. 移动平台勒索软件开始愈演愈烈

2014 年 4 月，随着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，并且有愈演愈烈的趋势。目前国内外出现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。

下图所示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。

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

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

充值、转账等方式后，仍不能获得解锁密码，甚至会被勒索软件作者将受害用户加入黑名单。

五、防御：我该做什么

1. 解密方法

就目前而言，勒索软件多采用非对称加密方式，除使用攻击者提供的密钥外，破解密码的可能性几乎为零。现有的勒索软件解密工具主要是通过以下几个方式获得密钥，恢复被加密的文件：

- 研究人员通过逆向分析，发现勒索软件执行上的逻辑漏洞，根据漏洞获得加密密钥或者跳过密钥直接解密文档。
- 有些勒索软件保存解密密钥的服务器被当地警方发现，警方在服务器中找到了大量密钥。这些密钥是由感染勒索软件的计算机生成，后上传到此服务器中保存的。它们在感染者交付赎金后被用作加密文档的解密密钥。警方与一些技术公司合作，根据从服务器中取出的解密密钥制作了相应的解密工具。
- 勒索软件保存密钥的服务器被安全厂商反制，在取得服务器权限后，将服务器内的密钥导出制作成相应勒索软件的解密工具。
- 解密密钥被其他竞争对手泄露或是勒索软件作者主动将密钥交出。
- 一些勒索软件加密算法复杂程度较低，加密过程照搬其他现有的加密算法或者只做小部分修改，使得研究人员可以编写程序暴力破解，计算出对应的解密密钥。
- 密钥在上传的过程中没有使用加密的通讯协议，被技术人员截获解密密钥。

2. 预防勒索软件的部分安全建议

为了避免受到勒索软件的威胁，安天针对不同用户给出如下建议：

- PC 用户

及时备份重要文件，且文件备份应与主机隔离；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；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；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；定期用反病毒软件扫描系统，如杀毒软件有启发式扫描功能，可使用该功能扫描计算机。

- Android 平台的移动终端用户

安装手机杀毒软件（比如 LBE 安全大师、安天 AVL Pro 等）；由可靠的安卓市场下载手机应用程序；尽量少或者不访问博彩、色情等潜在危险程度较大的网站。

3. 针对个人用户的勒索软件解决方案

- PC 用户

高强度加密方式绑架用户数据的勒索软件一旦感染主机，将对用户的数据安全构成严重威胁，所以，良好的安全意识和预防工作就显得非常重要。如果个人用户不慎感染勒索软件，且没有做好数据备份，则可根据勒索软件特性，如勒索界面、加密文件名等特征在网络中查找是否有相应解密工具。如安天持续关注勒索软件动态，对新发布的勒索软件解密工具做了收集，可方便用户快速查找解密工具。

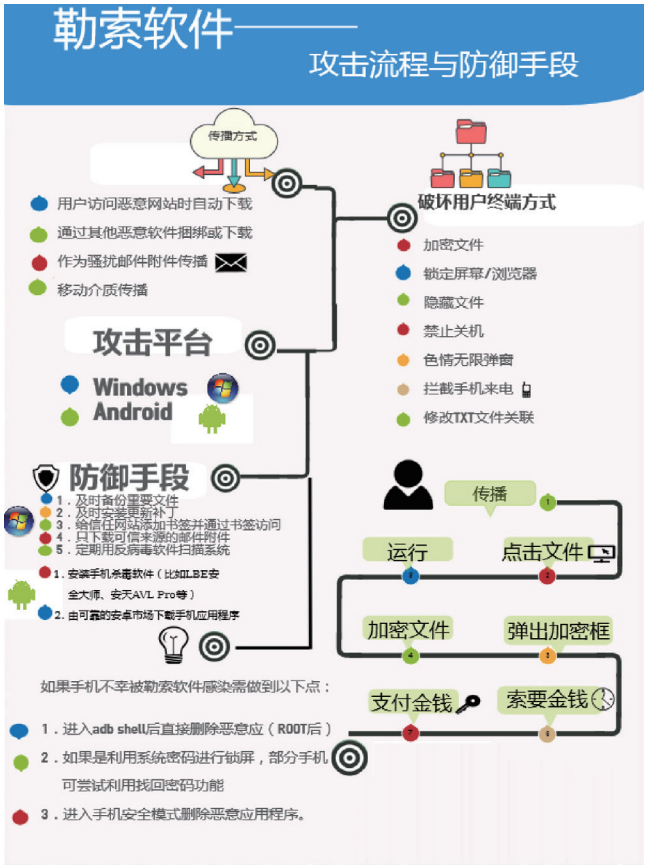
- 已经受到勒索软件感染的移动终端用户

对于感染勒索软件的移动终端用户来说，可采取以下方法删除恶意程序：如果手机已 root 并开启 USB 调度模式，可进入 adb shell 后直接删除恶意应用；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；可进入手机安全模式删除恶意应用程序。

4. 企业用户的全方位勒索软件解决方案

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。以安天企业安全产品“智甲”为例，即是从这几方面入手进行防御和处理的，在病毒查杀的基础上，结合勒索软件的行为特性，采用了“边界防御 + 主动防御 + 文档安全工具”的三重防御模式，可以有效阻止已知勒索软件和未知的勒索软件的进入、启动和破坏等行为，并且具有不依赖病毒特征的检测防护能力，从而保护用户数据和文件的安全。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net



六、总结

从 2016 年勒索软件爆发式的增长趋势来看，勒索软件目前已泛滥成灾，呈现爆发趋势，仅在下半年内就出现了数以千计的勒索软件变种，攻击对象已由传统办公终端扩展到了服务器终端，一旦感染将成为个人与企业用户的噩梦。而且，新型勒索软件的出现表现出了攻击者正在不断地更新传播方式、开发大量变种以及将勒索软件作为一种商业模式来开展，除了加密用户的数据文件勒索钱财外，极有可能发起更具有针对性的攻击。

据专家推测，在未来一段时间内，勒索软件攻击事件将会持续增长。造成这种情况的原因主要包括：勒索软件能让攻击者短时间内就获得丰厚利润，在利益驱动下，将会有越来越多攻击者加入其中；攻击者通过匿名支付和匿名网络实现赎金的交易，犯罪隐藏性高，难以捕获；研发勒索软件的技术水平相对较低，现在甚至有了制作平台，很多没有技术能力的人员也可以加入到这条黑产链条当中。在未来，勒索软件会进一步复合化，与目前的黑产合流，走向更多的系统平台，攻击范围会越来越大。针对勒索软件的防御将会成为安全产品面临的巨大挑战。

在勒索软件防御方面，现有防御措施已暴露出许多不足之处，首先很多勒索软件攻击者采用社工攻击手段，通过钓鱼邮件、网站挂马的方式实现攻击，防火墙等网络防御手段不能完全地阻拦勒索软件进入网络；其次由于每天都有大量新型勒索软件问世，传统的基于文件特征的方式很难准确检测出这些病毒。

但是，无论现今勒索软件采用何种攻击手段，其最终都需要在终端上才能完成攻击行为，因此加强终端的反病毒能力才是防勒索的核心。并且杀毒产品的检测手段，不能只依赖于传统的病毒特征，要提供更有效更准确的检测方式。

链接 欧盟“拒绝勒索软件”计划迈向全球化

2016 年 7 月 25 日，荷兰国家警察署、欧洲刑警组织、英特尔计算机安全公司（Intel Security）和卡巴斯基实验室共同启动“拒绝勒索软件计划”（No More Ransom），这是执法机关和私营领域共同合作对抗勒索软件的行动。这一项目得到了欧洲司法合作组织（Eurojust）和欧盟委员会（European Commission）的支持。同年 12 月，又有 30 家最新的来自公共领域以及私营领域的合作伙伴加入“拒绝勒索软件项目”。新的合作伙伴带来更多的解密工具，为勒索软件受害者找回自己的数据提供更多机会。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net