勒索病毒威胁形势分析报告

360互联网安全中心

2016 年 8 月 31 日

360互联网安全中心

摘　　要

- 敲诈者木马是一类特殊形态的木马，它们通过给用户电脑或手机中的系统、屏幕或文件加密的方式，向目标用户进行敲诈勒索。
- 根据 360 互联网安全中心的监测，仅 2016 年上半年，共截获电脑端新增敲诈者病毒变种 74 种，涉及 PE 样本 40000 多个，涉及非 PE 文件 10000 多个，全国至少有 580000 多台用户电脑遭到了敲诈者病毒攻击，且有多达 50000 多台电脑最终感染敲诈者病毒，平均每天有约 300 台国内电脑感染敲诈者木马。
- 监测显示，近期的敲诈者木马主要采用以下三种传播方式：邮件钓鱼、下载器挂马（JS 挂马）、执行器挂马（DLL 挂马）。
- 通过对敲诈者木马的受害者的调研分析，在敲诈者木马攻击的国内目标人群中，有 19.7%的人为企业用户，而另外 80.3%左右的国内被攻击者为普通个人用户。
- 感染敲诈者木马的国内电脑用户遍布全国所有省份，其中，广东占比最高，为 14.4%，其次是浙江 8.2%，北京 7.0%。排名前十的省份的感染者总量占国内所有感染者的 62.2%。
- 用户反馈显示，目前绝大多数的敲诈者木马均以比特币为赎金支付方式，从而使资金流向和攻击者本人都无法被追踪。赎金的金额一般为 2-3 个比特币。2016 年 4 月底-5 月初，1 个比特币价格约为 2900 元，而到了 2016 年 6 月，1 个比特币的价格一度高涨到了最高 5100 元。据此计算，2016 年 4 至今，如果有用户按照攻击者限定的时间支付赎金，赎金额度应在 5800 -15300 元人民币。
- 统计显示，仅自 2015 年 4 月敲诈者木马开始大规模爆发至 2016 年 5 月 15 日，360 互联网安全中心就已经累计监测到各类敲诈者木马 C&C 服务器 8000 余个。其中，com 域名被使用的最多，超过了总量的一半，为 51.4%，org 和 net 占比分别为 8.0%和 7.8%。此外，欧洲国家的域名占比为 17.5%，在各大洲中占比最高。
- 在国内曾有过不同规模爆发的 PC 端敲诈者木马家族主要是以下几个：CTB-Locker、CryptoLocker、Cryptowall、Locky、Teslacrypt、VirLocker。
- 一旦电脑感染了敲诈者木马（不包括锁屏木马或采用对称加密技术等简单的敲诈者木马），期望通过其他技术手段恢复系统文件的愿望通常来说都是无法实现的。

关键词：敲诈、比特币、赎金

360互联网安全中心

目　　录

第一章　敲诈者木马的大规模攻击

敲诈者木马是一类特殊形态的木马，它们通过给用户电脑或手机中的系统、屏幕或文件加密的方式，向目标用户进行敲诈勒索。早期比较简单的敲诈者木马会采用修改锁屏密码或开机密码的方式来锁定目标设备，但对于专业技术人员而言，要解锁此类木马通常并不太困难。此类木马目前在 PC 端已经非常少见，但在手机端仍然比较常见。

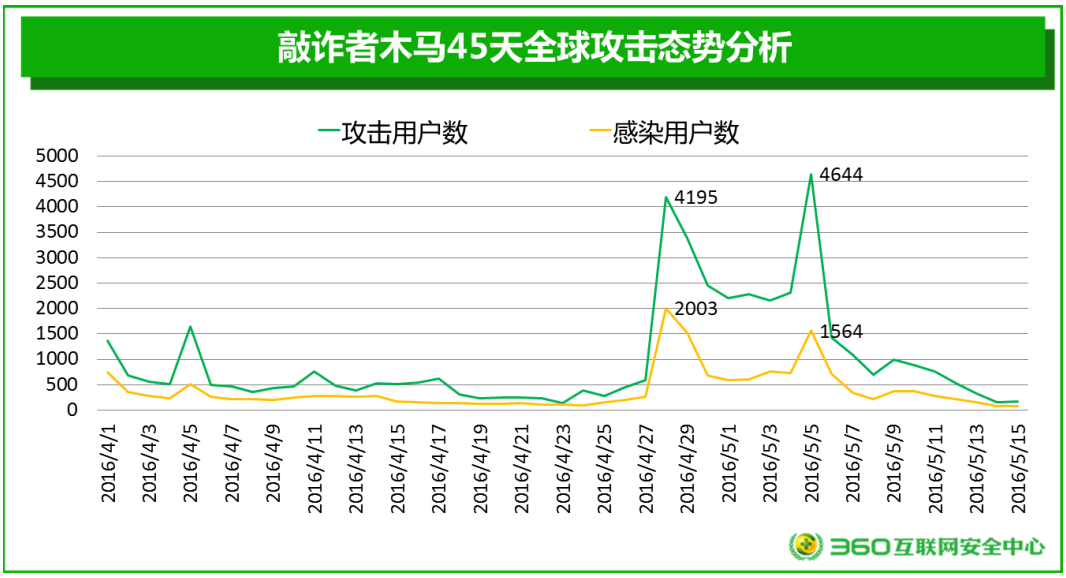
而近期大规模流行的敲诈者木马则主要采用不对称加密的方式对系统中的特定文件，如文档、图片、视频等进行高强度加密，使受害者完全不可能在不支付赎金的情况下自行解密被加密的文件。此类敲诈者木马，对于存储了大量机密或敏感文件的企业用户来说，威胁尤其严重，以往也主要被用于攻击企业或机构用户。但是，2016 年以来，360 互联网安全中心检测到大量针对普通网民的敲诈者木马攻击，并且在 4 月底至 5 月初达到攻击高峰，成为 4-5 月间，对网民直接威胁最大的一类木马病毒。

本次报告重点分析个人电脑端的敲诈者木马威胁形势。关于手机端的敲诈者木马威胁形势，请参见 360 互联网安全中心早前发布的专题研究报告《Android 勒索软件研究报告》，参考链接：http://zt.360.cn/1101061855.php?dtid=1101061451&did=1101724388

一、　敲诈者木马的感染量

根据 360 互联网安全中心的监测，根据 360 互联网安全中心的监测，仅 2016 年上半年，共截获电脑端新增敲诈者病毒变种 74 种，涉及 PE 样本 40000 多个，涉及非 PE 文件 10000 多个，全国至少有 580000 多台用户电脑遭到了敲诈者病毒攻击，且有多达 50000 多台电脑最终感染敲诈者病毒，平均每天有约 300 台国内电脑感染敲诈者木马。

下图给出了敲诈者木马 4 月 1 日至 5 月 15 日期间每日攻击用户数和最终感染用户数的对比情况。从图中可见，在 4 月底至 5 月初的攻击高峰期，一天之内被攻击的电脑最多可达 4644 台，感染敲诈者木马的电脑最多可卡 2003 台。



造成攻击成功率如此之高的主要原因有以下两个方面：一是电脑感染木马前用户未使用安全软件，或所使用安全软件不具备充分的主动防御能力，不能准确识别此类木马或此类木

马的攻击行为；二是在木马的表面诱惑下，很多用户无视安全软件的风险提示，手动放行了木马程序。

二、 敲诈者木马的传播方式

监测显示，近期的敲诈者木马主要采用以下三种传播方式：

1） 钓鱼邮件

这是一种比较经典的木马传播方式，主要手法是将恶意程序以邮件附件的形式发送给攻击目标。一旦被攻击者打开或运行邮件的附件，恶意程序就会被执行。

就敲诈者木马而言，最常见恶意附件形式主要有三种：JS 脚本、可执行文件和 Office 宏病毒文件等。而从近期的监测来看，敲诈者木马的钓鱼邮件中，已经很少使用 PE 文件或 Office 宏病毒文件这两种形式，主要攻击方法就是恶意的 JS 脚本附件。

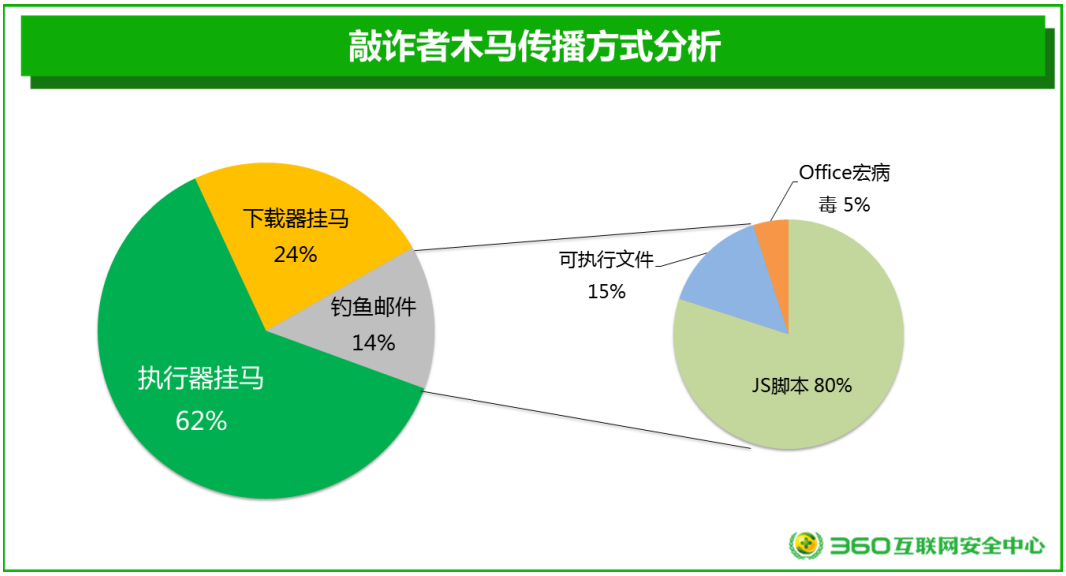
2） 下载器挂马（JS 挂马）

这是一种比较传统的网页挂马攻击方式，主要方法是在页面中嵌入恶意的 JS 脚本，一旦用户使用有漏洞的，且不具备主动防御能力的浏览器或其他客户端软件访问该挂马网页时，恶意的 JS 脚本就会被运行。

3） 执行器挂马（DLL 挂马）

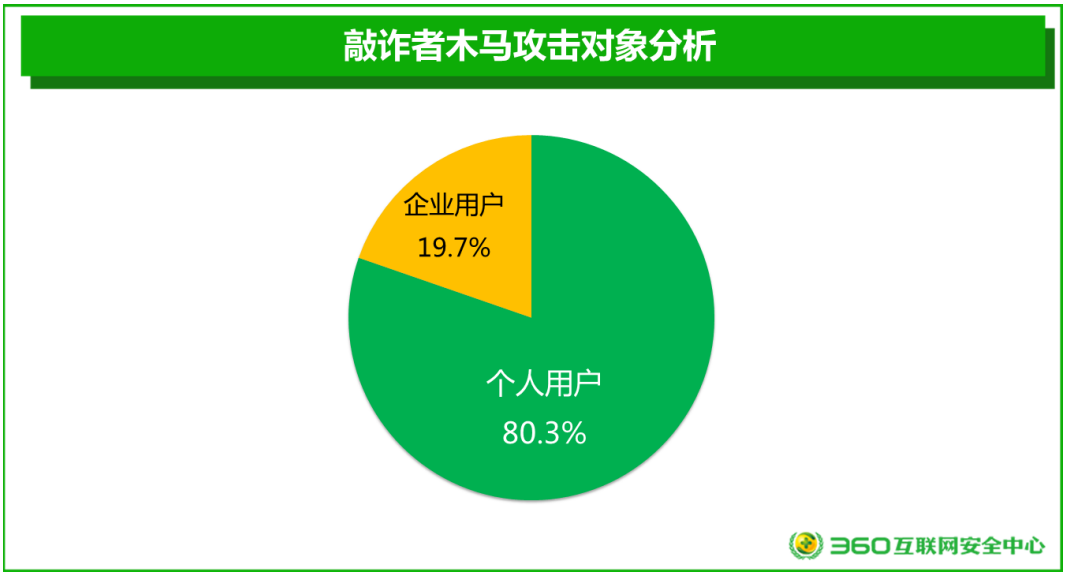
这是最近新出现的一种网页挂马传播方式，而且已经成为了最主流的传播方式。其主要攻击方式是通过页面挂马程序注入浏览器，启动并执行一个 dll 类的木马程序。

下图给出了敲诈者木马的三类主要传播方式，以及钓鱼邮件恶意附件的主要类型。可以看到，尽管传统的钓鱼邮件攻击仍然存在，但占比已经仅为 14%。而执行器挂马攻击则已经成为最主要的攻击方式，占比超过了 60%，下载器挂马排第二，占比为 24%。由于微软早前已经停止了对 IE 浏览器的更新,预计国内 IE 用户遭遇敲诈者木马的挂马攻击的风险还会继续加大。



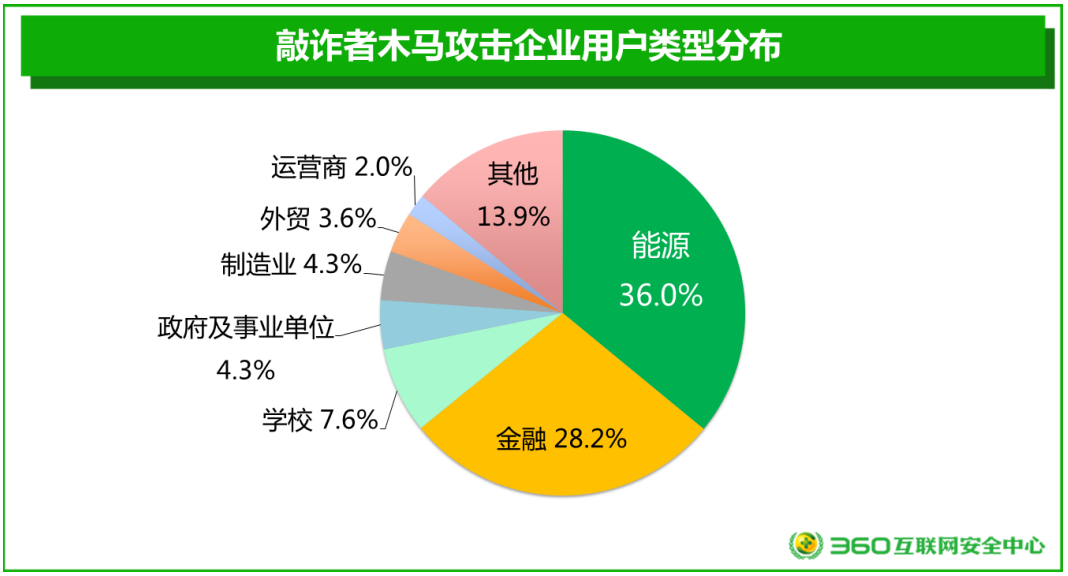
三、 敲诈者木马的攻击对象

通过对敲诈者木马的受害者的调研分析，在敲诈者木马攻击的国内目标人群中，有 19.7%的人为企业用户，而另外 80.3%左右的国内被攻击者为普通个人用户。



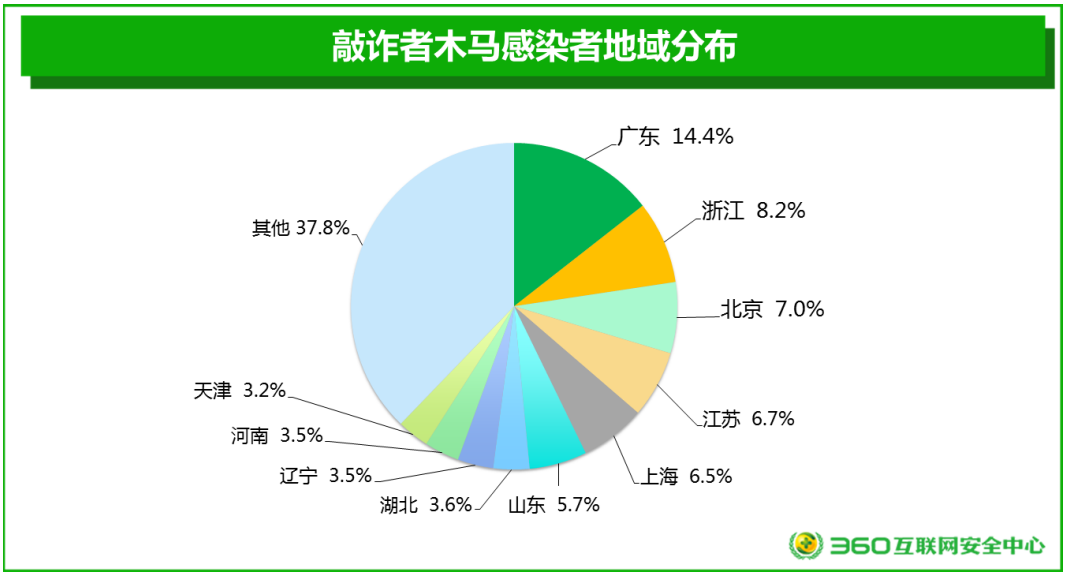
相比于普通个人用户，企业用户的攻击价值往往要高得多，因为企业用户电脑中所存储的数据往往更具机密性和不可复制性，因此企业用户为恢复文件而支付赎金的意愿也要比普通个人用户强得多。但从另一个角度来看，普通个人用户在上网安全意识和防护技术水平等方面都比较欠缺，因此也更容易被攻击并中招，攻击者一旦将普通用户设定为攻击目标，其对整个互联网的危害也将更加严重。

下图给出了被攻击的企业用户的行业分布情况。统计显示，能源行业是敲诈者木马排在首位的重灾区，占受害企业用户总量的 36.0%，其次是金融业，占 28.2%。学校 7.6%，政府及事业单位 4.3%和制造业 4.3%分列其后。

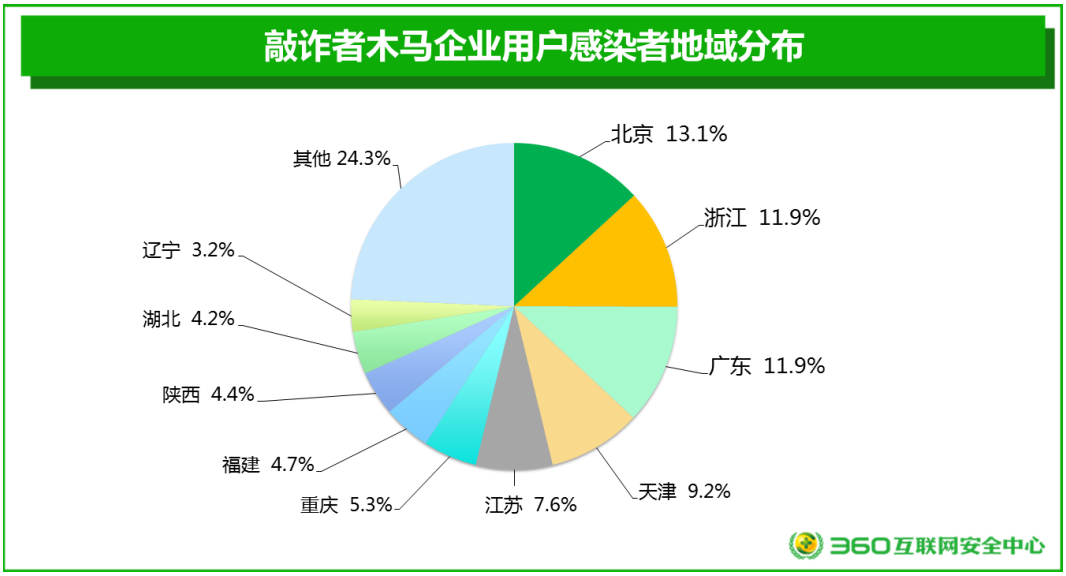


四、 受害者的地域分布

根据 360 互联网安全中心的监测，在 2016 年 4 月 1 日至 5 月 15 日期间感染敲诈者木马的国内电脑用户遍布全国所有省份，其中，广东占比最高，为 14.4%，其次是浙江 8.2%，北京 7.0%。排名前十的省份的感染者总量占国内所有感染者的 62.2%。



而就感染敲诈者木马的企业用户而言，北京地区最多，占比为 13.1%，浙江、广东各占 11.9%，排在第二、第三位。相比于普通个人电脑用户，企业用户的感染者更为集中，排名前十的省份的感染者总量占国内所有感染者的 75.7%。



五、 受害者的经济损失

用户反馈显示，目前绝大多数的敲诈者木马均以比特币为赎金支付方式，从而使资金流向和攻击者本人都无法被追踪。赎金的金额一般为 2-3 个比特币。2016 年 4 月底-5 月初，1 个比特币价格约为 2900 元，而到了 2016 年 6 月，1 个比特币的价格一度高涨到了最高 5100

元。据此计算，2016 年 4 至今，如果有用户按照攻击者限定的时间支付赎金，赎金额度应在 5800-15300 元人民币。

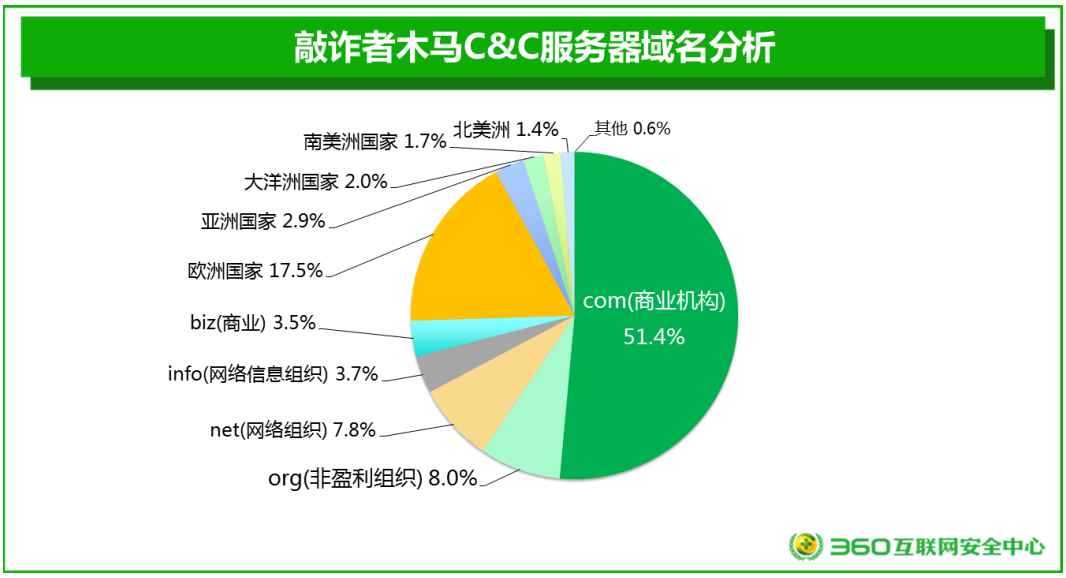
按照前述分析，每天有约 300 台国内电脑感染敲诈者木马，并假设所有受害者均支付了赎金，则：2016 年 4 月-7 月间，攻击者每天可以从国内受害者手中获得约 174 万-459 万元人民币的赎金。

而如果按照前述分析中给出的 2016 年 4 月底出现的单日感染量高峰 2003 台计算机计算，如果所有受害者均支付赎金，则攻击者们在这一天可以获得高达 1162 万-1743 万元人民币的赎金。

第二章　敲诈者木马的服务器分布

敲诈者木马通常会使用 C&C 服务器，用于向木马发布加密公钥或记录感染者信息。这些服务器往往在攻击成功后立即消失，平均生命周期在 1-2 个小时，而在对抗最激烈的时期，某些木马的 C&C 服务器会每 10-20 分钟就变化一次。统计显示，仅自 2015 年 4 月敲诈者木马开始大规模爆发至 2016 年 5 月 15 日，360 互联网安全中心就已经累计监测到各类敲诈者木马 C&C 服务器 8000 余个。其中，绝大多数 C&C 服务器使用指定域名与木马联络，仅有不足 1%的 C&C 服务器使用固定 IP。

我们针对近期最为活跃的部分敲诈者木马的 C&C 服务器域名进行了分析，结果显示：com 域名被使用的最多，超过了总量的一半，为 51.4%，org 和 net 占比分别为 8.0%和 7.8%。此外，具有明显国家归属的域名，如 uk（英国）、ru（俄罗斯）、au（澳大利亚）等，也占到了总量的 25.5%左右，其中，属于欧洲国家的域名最多，占 17.5%，其次是亚洲国家 2.9%，大洋洲国家 2.0%。



下表给出了 360 互联网安全中心在 4 月 1 日至 5 月 15 日期间监测到的敲诈者木马使用的 C&C 服务器域名中，最常见的 20 个域名后缀及其出现的次数情况。

排名	域名后缀	出现次数	排名	域名后缀	出现次数
1	com(商业机构)	569	11	de(德国)	13
2	org(非盈利组织)	89	12	ca(加拿大)	12
3	net(网络组织)	86	13	jp(日本)	12
4	uk(英国)	54	14	nl(荷兰)	12
5	ru(俄罗斯)	47	15	ro(罗马尼亚)	7
6	info(网络信息组织)	41	16	fr(法国)	6
7	biz(商业)	39	17	it(意大利)	6
8	au(澳大利亚)	19	18	at(奥地利)	5
9	br(巴西)	14	19	hu(匈牙利)	5
10	pl(波兰)	14	20	ar(阿根廷)	4

表 1 敲诈者木马 C&C 服务器域名后缀 TOP20（2016 年 4 月 1 日-5 月 15 日）

第三章　敲诈者木马的家族与发展

目前全球主流的敲诈者木马家族（类型）有 74 种之多，详见下表（按字母排序）。

7ev3n	CryptoJoker	KimcilWare	Radamant
8lock8	CryptoMix	Kriptovo	RemindMe
Alpha	CryptoTorLocker	KryptoLocker	Rokku
AutoLocky	CryptoWall	LeChiffre	Samas
BitCryptor	CryptXXX	Locky	Sanction
BitMessage	CrySiS	Lortok	Shade
Booyah	CTB-Locker	Magic	Shujin
Brazilian Ransomware	DMA Locker	Maktub Locker	SNSLocker
BuyUnlockCode	ECLR Ransomware	MireWare	SuperCrypt
Cerber	EnCiPhErEd	Mischa	Surprise
Chimera	Enigma	Mobef	TeslaCrypt
CoinVault	GhostCrypt	NanoLocker	TrueCrypter
Coverton	GNL Locker	Nemucod	UmbreCrypt
Crypren	Hi Buddy!	Nemucod-7z	VaultCrypt
Crypt0L0cker	HydraCrypt	OMG! Ransomcrypt	Virlocker
CryptoDefense	Jigsaw	PadCrypt	WonderCrypter
CryptoFortress	JobCrypter	PClock	Xort
CryptoHasYou	KeRanger	PowerWare	
CryptoHitman	KEYHolder	Protected Ransomware	

表 2 敲诈者木马家族主流类型

其中，在国内曾有过不同规模爆发的 PC 端敲诈者木马家族主要是以下几个：CTB-Locker、CryptoLocker、Cryptowall、Locky、Teslacrypt、VirLocker。而这些主要家族中，只有 VirLocker 对被加密文档采用了对称加密算法，这也就导致了感染此木马的文档是可以被恢复的，所以很快绝迹。现如今，PC 端的敲诈者木马基本上都是采用了不对称的高强度加密算法对文件进行加密。

下面是敲诈者木马在国内发展历史的简介：

最先进入我国的是 CTB-Locker 敲诈者木马，相关分析参见：《首次现身中国的 CTB-Locker“比特币敲诈者”病毒分析》，参考链接：http://blogs.360.cn/blog/ctb-locker/

之后进入我们视野的是 VirLocker 木马，相关分析参见：《360 全球唯一可成功修复还原 VirLock 变种感染文件》，参考链接：http://weibo.com/p/1001603804790554493920。由于其算法可逆的特性，我们也对逆向恢复被加密的文件的方法做出了阐述。

接下来，CTB-Locker 进行了更新，同时国内的一些黑客个人或组织也开始使用 CTB-Locker 的模版为自己牟利。我们也对新一波的 CTB-Locker 木马进行了分析和查杀。相关分析参见：《CTB-LOCKER 分析报告》，参考链接：http://blogs.360.cn/360safe/2015/05/27/ctb-locker 分析报告/

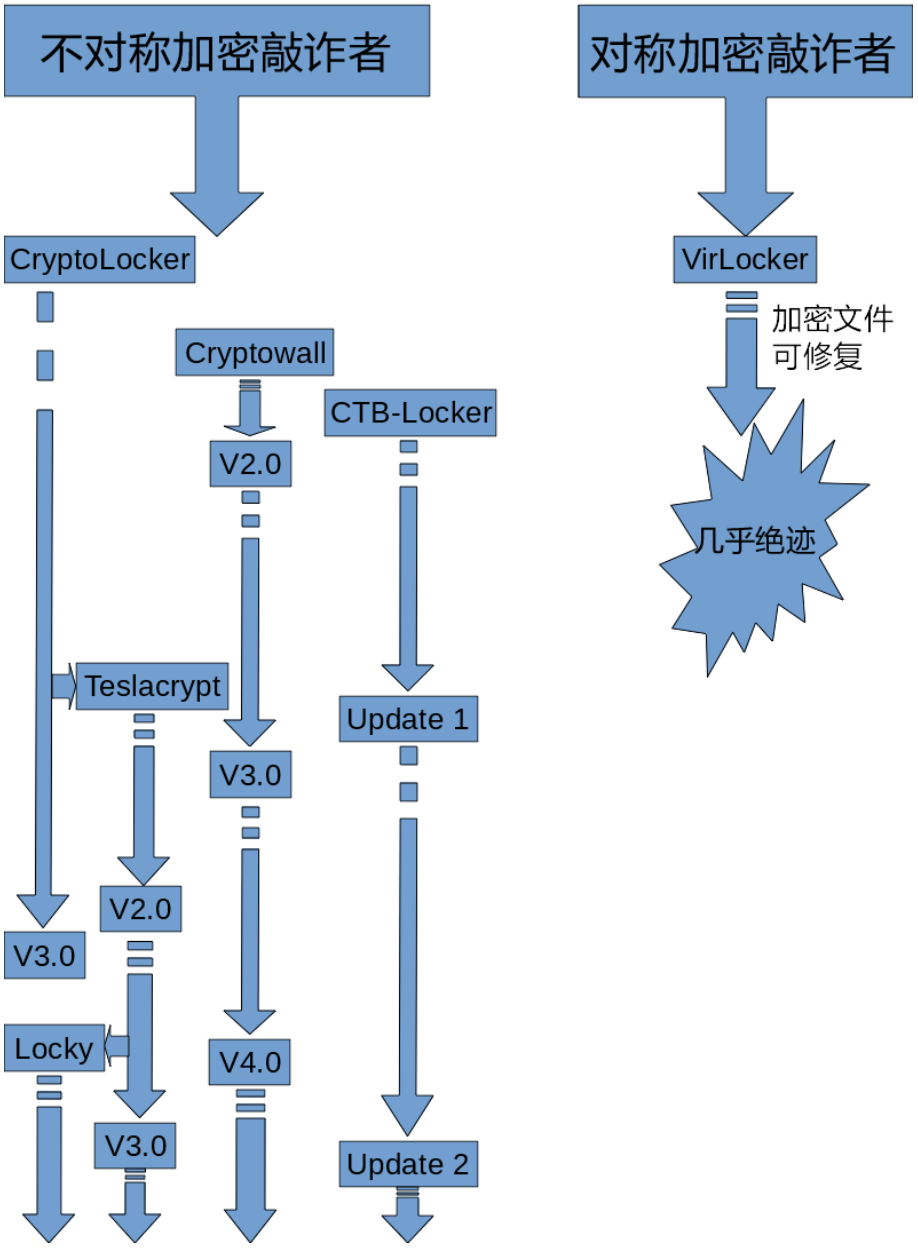
CryptoLocker 虽然出现较早，但进入国内相对较晚。但一进入国内就带有比较明显的“本

土化”气息，结合了论坛挂马、邮件蠕虫、宏病毒等多种途径传播。相关分析参见：《CryptoLocker 敲诈者病毒再出新变种》，参考链接：http://weibo.com/1645903643/CvslgbK0E?type=comment#_rnd1464163725986 和《警惕 CryptoLocker 敲诈者卷土重来！》，参考链接：http://weibo.com/ttarticle/p/show?id=2309403943915932749380

最近，基于 Teslacrypt 等木马变化而来的敲诈者木马又借助 Office 的宏代码进行大肆传播。相关分析参见：《勒索软件 Locky 最新传播载体分析——中文版 Office 危在旦夕》，参考链接：http://weibo.com/ttarticle/p/show?id=2309403973223459991970

近日又出现了名为 SNSLocker 的新木马，但据目前监控。该木马并尚未在国内大规模传播。

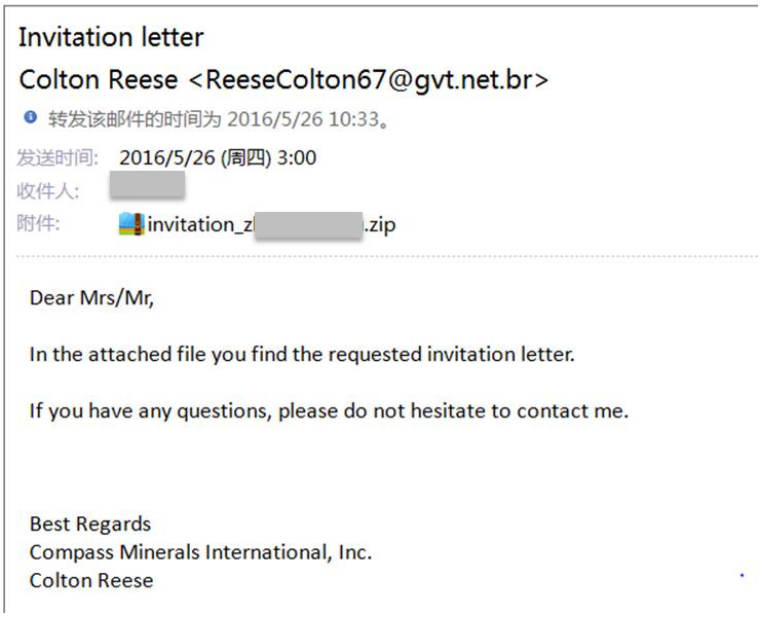
下面给出了部分 PC 端敲诈者木马在国内发展的基本过程。



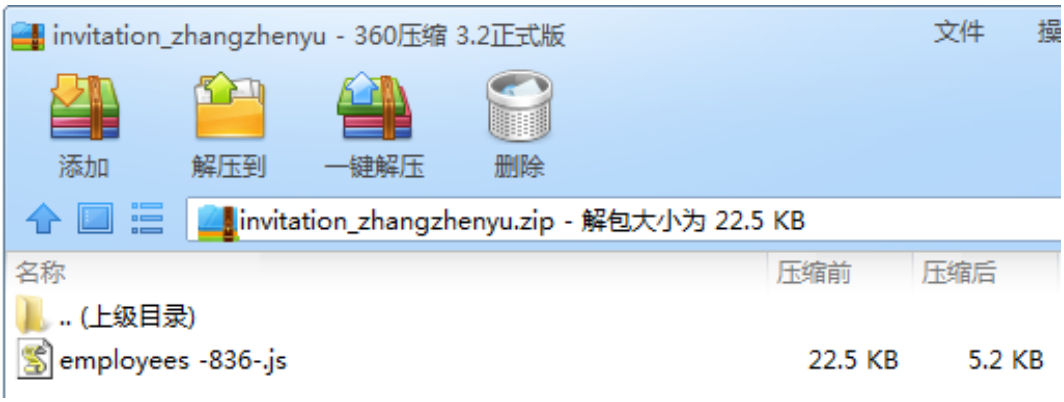
第四章 敲诈者木马的敲诈过程

下面，我们就以钓鱼邮件攻击为例，简要说明敲诈者木马的敲诈过程，以帮助读者了解敲诈者木马。

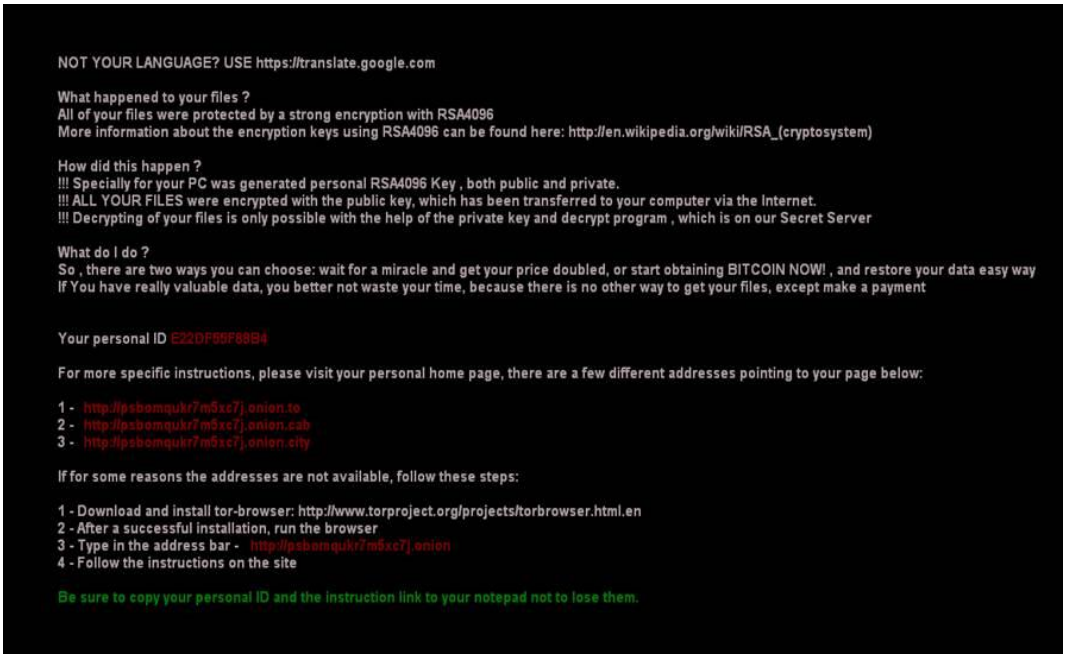
首先，用户会收到一封陌生人发来的携带了附件的钓鱼邮件。而邮件附件通常是携带了敲诈者木马的一个压缩文件包。下图是某位用户向我们举报一封敲诈者木马钓鱼邮件截图。可以看到，邮件名为“Invitation letter（邀请函）”，而邮件的附件名为“invitation_xxx.zip”。其中“xxx”是收件人的邮箱名（@之前的名称），而且，由于这位举报用户恰好为某个企业用户，其邮箱为办公邮箱，且邮箱名就是这位用户的真实姓名。所以，这封邮件乍一看上去，很像是一封真正的邀请函，而且对于习惯了英文办公的国内用户来说邮件更具有迷惑性。



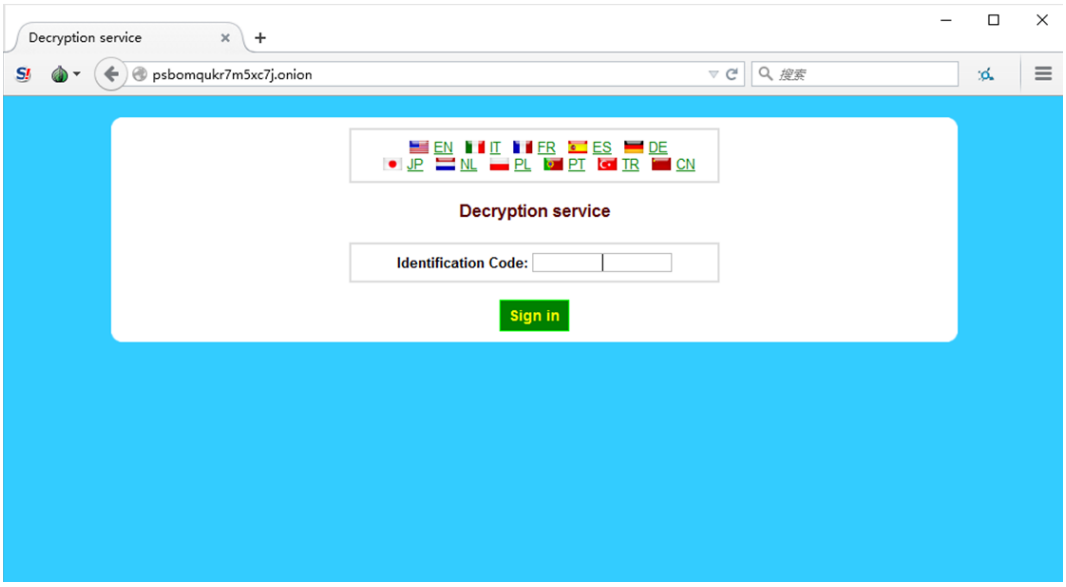
解压邮件附件，可以看到一个压缩包内有一个后缀名为 js 的文件。这就是用于攻击的恶意脚本文件了。用户一旦打开这个文件，电脑就会中招。



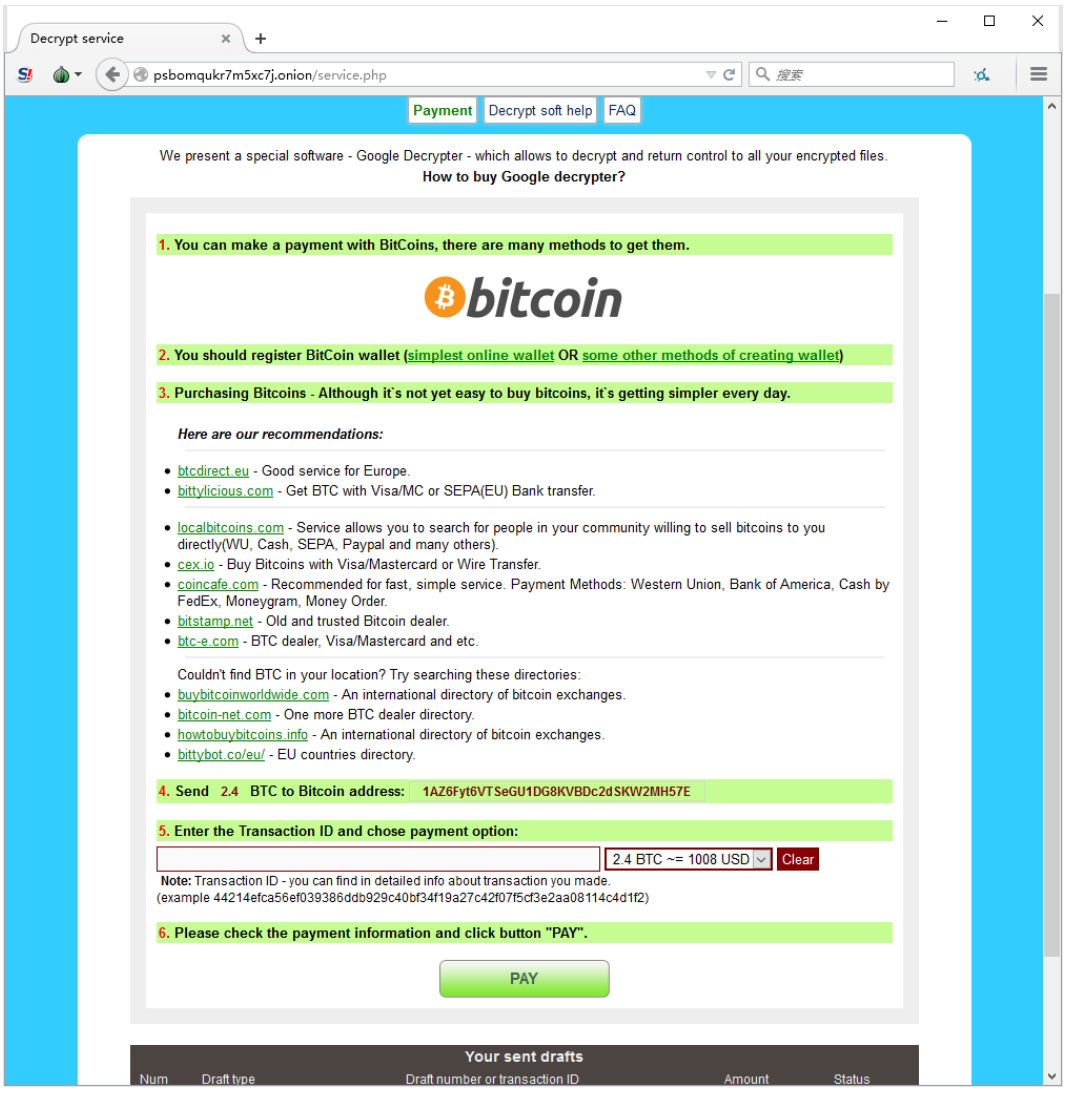
当受害者电脑已经感染该敲诈者木马后，木马会给出一个敲诈信息的页面，其中包含几个付赎金的网址和一个用户的“私人 ID”。



打开木马提供赎金支付页面后，页面会要求受害者输入“私人 ID”。



输入 ID 后，页面便会跳转到一个比特币的支付页面。本例中测试的这个木马样本索要的赎金为 2.4 个比特币，约合 1008 美元。



支付赎金后，木马就会从指定服务器上获取解密密码，输入解锁密码后，系统一般就可以恢复正常了。

不过，近期我们也监测到个别的流氓敲诈者，即受害者即使支付了赎金，攻击者也不向受害者提供解密密码。好在这种流氓攻击者目前数量还比较有限。绝大多数情况下，支付赎金以获取解密密码的方式还是有效的。

另外，目前我们监测到敲诈者木马钓鱼邮件及木马的交互界面，绝大多数都是英文的，很少能见到中文内容的邮件。这一方面可能是因为目前来自境外的攻击者仍占主流，而境外攻击者还普遍不熟悉中文。而另一方面，虽然我们已经监测到一些国内攻击者，但这些攻击者可能也愿意使用英文来隐藏自己的身份。

第五章　敲诈者木马的应对措施

一、敲诈者木马的不可解

采用了不对称加密算法的敲诈者木马，其核心特点是“可防不可治”。也就是说，一旦系统或安全软件未能对敲诈者木马进行有效的防护，一旦电脑感染木马，一旦木马对电脑系统中的文件的不对称加密过程完成，理论上来说，除非攻击者支付赎金获取解密密码，否则就没有任何技术手段可以将文件恢复。这与其他类型的木马攻击后，系统通常可以被修复的情况完全不同。

造成敲诈者木马“可防不可治”的主要原因是加密算法在数学上的不可逆。实际上，敲诈者木马通常来说也不会使用什么特殊的加密算法，而是使用国际通行各种标准加密算法对电脑文件进行加密。而这些标准的加密算法，原本的设计目的就是为了保证只有特定的人才能解密特定的加密文件，其数学算法本身是不可逆的，密码也是数学上不可破解的。

所以，一旦电脑感染了敲诈者木马（不包括锁屏木马或采用对称加密技术等简单的敲诈者木马），期望通过其他技术手段恢复系统文件的愿望通常来说都是无法实现的。

二、FBI 的撕票建议

支付赎金，就等于是向犯罪分子低头，而且理论上说，执法机构可能也永远无法抓捕到犯罪分子来为你伸张正义——起码对于使用比特币做赎金的犯罪分子确实如此。而不支付赎金，或者是没有在犯罪分子要挟的时间内（一般为 24 小时或 48 小时）支付赎金，则意味着电脑系统中的文件将永远也无法恢复。这就使得所有遭到敲诈者木马攻击受害者都感到非常的“窝囊”和不知所措。

对此，在 2016 年 5 月初，FBI 向公众发了“不要向敲诈者木马支付赎金”的建议，以此来打击敲诈者木马攻击者的嚣张气焰。

不过，FBI 的这一建议也被很多人批评为撕票建议，因为这等于是在人质被绑架后，一

口拒绝绑架犯的赎金要求，很有可能会导致绑架犯的撕票。而对于电脑中确实有重要文件资料的受害者来说，也不太可能拒绝支付赎金，除非受害者电脑中资料的价值低于敲诈者木马要求的赎金。

三、 360 反勒索服务

对于敲诈者木马，最为有效的应对手段是事前防护，即在木马的攻击过程中对其进行拦截和风险提示。由于敲诈者木马的程序特征与一般的木马完全不同，所以早前的很多敲诈者木马确实可以绕过绝大多数的安全防护软件，但现在，如 360 安全卫士等具有云防护和主动防御能力的安全软件，已经可以对敲诈者木马进行非常有效的发现与拦截。

但是，任何安全防护措施都不可能对木马病毒实现百分之百的有效防御，一旦用户电脑感染木马病毒，帮助用户挽回损失，才是安全企业应尽的责任。故此，针对危害日益严重的敲诈木马，360 互联网安全中心自 2016 年 8 月 15 日起开始实施“反勒索服务”：一旦使用 360 安全卫士的用户开启此项服务，在没有看到 360 安全产品的任何风险提示的情况下感染敲诈者木马，可以直接通过 360 反勒索服务申请赔付，360 公司将替受害者支付最高 3 个比特币的赎金。

关于赔付计划的详细内容，请参见本报告附录 1。

四、给用户的安全建议

对于普通用户，我们给出以下建议，以帮助用户免遭敲诈者木马的攻击：

1） 不要轻易打开陌生人发来的邮件附件或正文中的网址链接。

2） 不要轻易打开后缀名为 js 或 dll 的陌生文件。

3） 如果陌生人发来的邮件附件为压缩格式，请不要轻易点开，如果附件解压后有后缀名为 js 的文件，则千万不要打开。

4） 电脑应当安装具有云防护和主动防御功能的安全软件，以使电脑尽可能避免遭到敲诈者木马的攻击。

5） 尽量使用安全浏览器，以免电脑遭到挂马攻击。

6） 打开邮件附件或其他从网络上接受的文件（如聊天软件传输）前，应首先使用安全软件对其进行扫描检测。

7） 对于安全性不确定的文件，可以选择在安全软件的沙箱功能中打开运行，从而避免木马对实际系统的破坏。

8） 如果电脑已经被敲诈者木马感染，可以通过敲诈者木马赎金计划来减小自身的经济损失。

附录 1 360 反勒索服务

2016 年 8 月 15 日，360 安全卫士发布 11.0 beta 版。该版本的安全卫士首次推出了 360 反勒索服务。用户在主界面上点击“反勒索服务”按钮，就可以按照提示申请开通 360 反勒索服务。用户在完全开通此项服务后，如果在没有看到 360 安全卫士的任何风险提示的情况下感染敲诈者木马，360 公司将替受害者支付最高 3 个比特币的赎金。

想要获得最高额度的赔偿，用户在进入 360“反勒索服务”选项后，需要同时开启 360 文档保护和 360 反勒索服务。开启这两项服务后，如果用户遇敲诈者木马攻击，点击下图中的“申请服务”按钮即可申请理赔。

附录 1 360 天擎企业级百万敲诈先赔服务

2016 年 9 月 6 日，360 企业安全正式宣布，向所有 360 天擎政企用户免费推出敲诈先赔服务：如果用户在开启了 360 天擎敲诈先赔功能后，仍感染了敲诈者病毒，360 企业安全将负责赔付赎金，为政企用户提供百万先赔保障。

360 企业安全此次敢于向政企客户做出无忧先赔服务，其信心来自背后的强大技术实力和在用户中的成功实践检验。事实上，自敲诈者病毒诞生之日起，360 企业安全就对该病毒进行了深入的研究，并在百亿级别安全大数据分析的基础上，依托于免疫、QVM 机器学习引擎和行为识别等方式，以及独家推出的“文档防护功能”，对敲诈者病毒进行全面的防御和拦截，已经帮助政企用户抵挡住了敲诈者病毒的一轮又一轮攻击。国内使用 360 天擎的企业用户，只要开启了相关的防护功能，目前还没有出现终端感染敲诈者病毒的情况。

为了增强企业客户对抗敲诈者病毒的信心，并让更多人成为敲诈者病毒的监督者，360 天擎率先在企业市场独家推出敲诈先赔服务。服务关键内容摘要如下：

◆ 服务标准：当企业用户保持不间断开启 360 文档保护功能与 360 天擎敲诈先赔服务功能，并在其要求的环境下运行程序，仍遭受敲诈者病毒侵害，造成约定文件被加密勒索的，360 以尽力帮助企业用户还原文件为宗旨，将承担企业用户被勒索的现金损失，但不直接支付现金给企业用户，仅对企业用户单次所遭受的现金勒索进行解密服务，亦不对解密结果做绝对性的保证。

◆ 申请时效：政企用户遭受敲诈病毒勒索之日起的 72 小时内。

◆ 赔付金额：服务期间，如果政企用户感染了敲诈者病毒，每终端每次获赔上限为 1 万元人民币或 3 个比特币，每企业用户累计获赔上限为 100 万元人民币或者 200 个比特币。

◆ 补充说明：每位企业用户每年享受“360 天擎敲诈先赔”服务不限次数，但是针对同一企业用户，在 360 天擎为企业用户提供首次“360 天擎敲诈者先赔”服务后，企业用户需保证按照 360 天擎提交的安全整改方案进行安全改造，否则将不再享受“360 天擎敲诈先赔”服务。

细节条款见官网：http://b.360.cn/special/agreement/agreement.html

360 天擎敲诈先赔配置指南

1、开启安全防护中心的“立体防护”：

在“策略中心→分组策略→病毒查杀→安全防护中心”中，确保“立体防护已开启”。默认情况下是开启的，若显示未开启，点击“全部开启”，并点击“保存”按钮。

2、终端定制需要安装“安全防护中心”和“病毒查杀”模块：

在“策略中心→分组策略→基本设置→终端定制”中，将“终端功能定制”模块中的“安全防护中心”和“病毒查杀”两个模块勾选上。

3、开启“文件系统实时保护”功能和“敲诈者木马防护功能”：

在“策略中心→分组策略→病毒查杀→安全防护中心”中，在“实时防护”模块中勾选上“打开文件系统实时防护”和“启用敲诈者木马防护功能”，并点击“保存”按钮。

建议：不要将“未知文件防误杀”模块中的“启用未知文件防误杀功能”开启。

4、将云查杀设置的文件安全鉴定模式设置为“直接连接 360 云安全鉴定中心”：

在“策略中心→分组策略→病毒查杀→云查杀设置”中，在“云查询”模块中将文件安全鉴定模式选择为“直接连接 360 云安全鉴定中心”，不能勾选“关闭 QVM 人工智能云查询”。并在“未知样本鉴定”模块中将鉴定模式选择为“使用 360 云安全鉴定中心”。并点击“保存”按钮。

建议：目前已知敲诈者病毒多是针对连接外网的终端，因此建议企业 IT 运维人员将连接外网的终端单独设立分组，并针对该分组完成以上的设置。

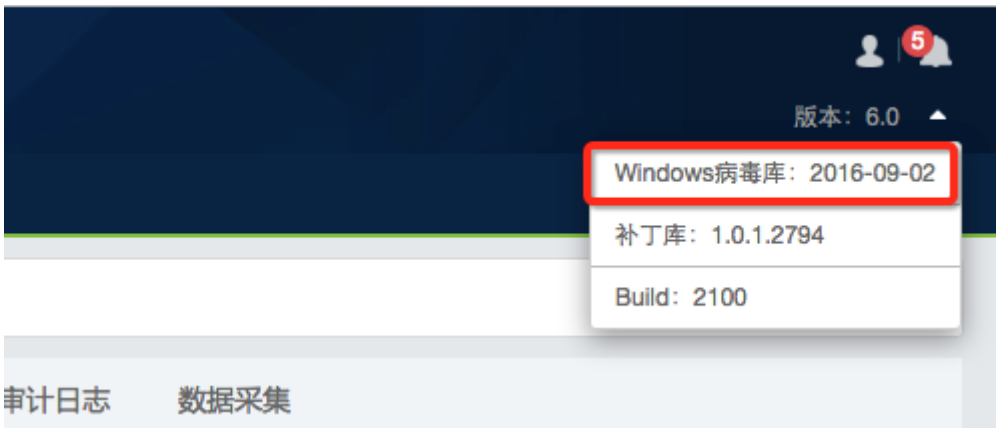
5、终端升级模式设定为自动升级：

在“策略中心→分组策略→基本设置→基本设置”中，在“升级设置”模块中选择“自动升级主程序和备用病毒库到最新版”，并点击“保存”按钮。

在“策略中心→分组策略→基本设置→通讯设置”中，在“通讯设置”模块中将终端与控制中心网络环境选择为“互联网优先”，并点击“保存”按钮。

6、防病毒引擎和特征库升级到最新版本：

确保天擎控制中心显示“Windows 病毒库”更新时间与当前时间相差小于 8 天。



若超过 8 天未更新病毒库，需要点击检测并升级病毒库。

建议：对于可以连接外网的控制中心，建议将“系统管理→系统设置→升级设置→服务器升级配置”中病毒库更新周期，设置为“每天”。

附录 2 敲诈者木马攻击事件

2016 年 1 月，三家印度银行和一家印度制药公司的计算机系统感染了敲诈者病毒，每台被感染的电脑索要 1BTC 赎金。攻击者渗透到计算机网络，然后利用未保护的远程桌面端口感染网络中的其它计算机。因为被感染的计算机很多，被勒索的印度公司面临数百万美元的损失。

2016 年 2 月 5 日，美国好莱坞长老教会纪念医学中心的电脑系统在遭受为期一星期的敲诈者病毒攻击后，该中心宣布决定支付给黑客 40 枚比特币(约 17000 美元)来修复这一问题。随后加拿大渥太华的一家医院和安大略省的一家医院也被敲诈者病毒攻击。

2016 年 2 月，美国南卡罗来纳州霍里县多所学校的电脑和服务器遭遇敲诈者病毒攻击，黑客控制了当地学校系统的网络和服务器，最终不得不支付价值 8500 美元的 20 个比特币给匿名黑客，以便让受到勒索影响的电脑、服务器和网络恢复正常。

2016 年 2 月至 3 月 5 日，中国香港地区电脑保安事故协调中心共接获 41 宗有关敲诈者病毒的报告，电脑受感染后文件会遭加密无法打开，黑客敲诈“比特币”以换取解密钥匙，受害者多是中小企及非牟利机构。

2016 年 2 月以来，360 互联网安全中心监测到一大波敲诈者病毒大规模爆发，国内单位组织陆续开始受到的冲击，公司对外的邮箱收到大量携带该木马的邮件。包括国家计算机病毒应急处理中心在内的国家机构也都发布了相应的计算机病毒疫情通报。自 3 月以来国内已有上万台电脑中招，淘宝上甚至已经出现了协助代付款解密的服务。其中国内某央企一周内连续三次中招，所安装的某国外安全软件无法防御，最终导致该企业部分终端用户中招，给该机构造成不可逆的严重损失。