# 2016 敲诈者病毒威胁形势分析报告

# （年报）

360互联网安全中心

2016 年 12 月 15 日

360互联网安全中心

# 摘　　要


- 360 互联网安全中心的监测显示，2016 年 1 月 1 日至 11 月 29 日，共截获电脑端新增敲诈者病毒变种 113 种，涉及样本 16.7 万个，全国至少有 497 多万台用户电脑遭到了敲诈者病毒攻击。在 9 月底至 10 月中旬出现敲诈者病毒攻击的高峰。
- Cerber、Locky、XTBL 是目前最主流的三大敲诈者病毒家族。网页挂马传播、邮件附件传播、服务器入侵传播是目前最主流的三大传播方式。
- 遭遇敲诈者病毒攻击的国内电脑用户遍布全国所有省份。其中，广东占比最高，为 13.2%，江苏 9.4%，山东 5.8%，排名前十省份占国内所有被攻击总量的 60.6%。
- 在敲诈者病毒攻击的国内目标人群中，18.9%为企业用户，81.1%为普通个人用户。受害者主动寻求帮助的人群中，62.4%为企业用户，37.6%为个人用户。
- IT/互联网行业是最容易受到敲诈者病毒攻击的行业，占比为 25.7%；其次为制造业占比 18.8%，政府或事业单位占比为 14.4%。
- 普通职员是遭遇敲诈者病毒攻击次数最多的受害者，占比高达 51.1%，其次是经理、高级经理，占比为 39.4%，企业中、高管理层，占比为 6.6%，CEO、董事长、总裁等企业的掌舵者被敲诈者病毒攻击的比例也达到了 2.9%。
- 42.6%的受害者不知道自己是如何感染的敲诈者病毒，21.8%是通过浏览陌生网页感染病毒，11.9%是通过下载软件感染病毒，8.9%是主动点击查看邮件的附件感染病毒，5.0%是通过 U 盘传播感染，3.5%是通过开启 3389 端口，遭到黑客远程攻击。
- 94.6%的受害者电脑上办公文档被感染，88.1%的受害者认为办公文档是造成损失最大的文件类型。
- 11.9%的受害者会为了恢复文件而支付赎金，其中，58.4%是通过淘宝平台，33.3%是按照病毒提示付款的，8.3%的受害者是通过请朋友帮助操作付款的。
- 不愿意支付赎金的用户中，有 39.9%的受害者是因为不相信支付赎金后会给自己的文件解密，24.7 %的受害者是因为不想继续纵容黑客进而选择拒绝支付赎金，10.7%的受害者是相信会有恢复工具能够修复加密的文件。
- 调研显示，16.8%的受害者恢复了文件。其中，26.5%是通过使用解密工具，17.6%是通过历史网络备份数据。
- 在感染敲诈者病毒后，48.4%的受害者通过重装系统清除了病毒，18.3%的受害者通过安装安全软件查杀掉病毒，11.8%的受害者直接删除中毒文件。但仍有 21.5%的受害者未进行任何处理。



**关键词：**敲诈者病毒、比特币、支付赎金

360互联网安全中心

# 目　　录

# 第一章　敲诈者病毒的大规模攻击

敲诈者病毒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。敲诈者病毒已有十多年的历史，之前的敲诈方式是加密或隐藏文件后要求转账或者购买指定商品，传播量和影响力并不高。

目前，流行的比特币敲诈者病毒，在 2014 年时已经开始在国外流行了，到 2015 年开始大量流入国内。在国内大量传播的主流敲诈者家族有 TeslaCrypt、Locky、Cerber、CryptXXX、XTBL 等多个家族，每个家族在传播对抗过程中又产生多个分支版本。目前捕获的敲诈者病毒和敲诈者病毒变种超过 200 个版本，传播量和影响力都非常大。

近期大规模流行的敲诈者病毒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，使受害者几乎不可能在不支付赎金的情况下自行解密被加密的文件。此类敲诈者病毒，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 互联网安全中心监测到大量针对普通网民的敲诈者病毒攻击，并且在 9 月底至 10 月中旬达到敲诈者病毒攻击的高峰，成为对网民直接威胁最大的一类木马病毒。

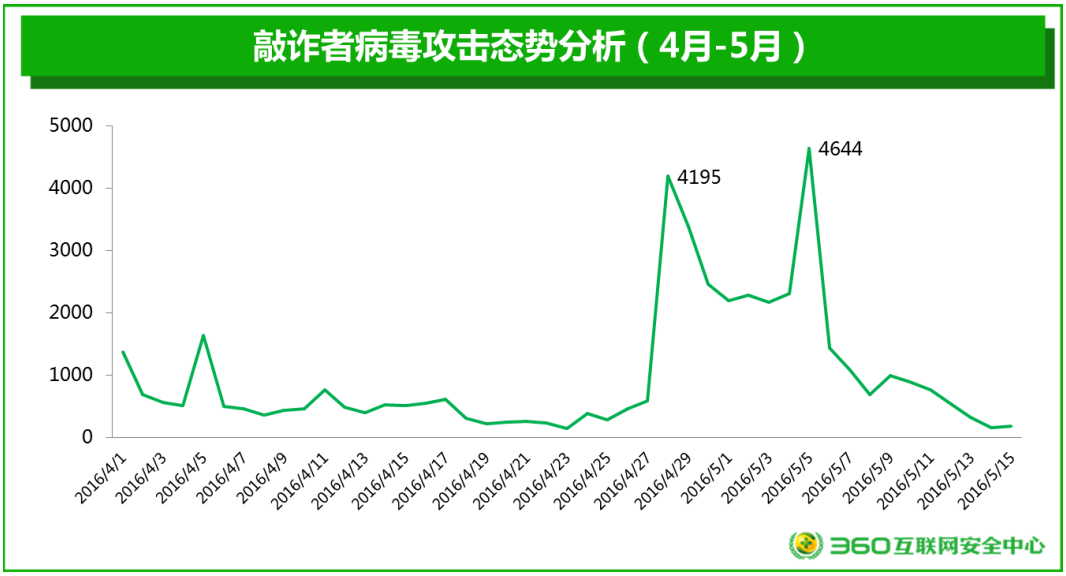
本次报告重点分析个人电脑端的敲诈者病毒威胁形势。关于手机端的敲诈者病毒威胁形势，请参见 360 互联网安全中心早前发布的专题研究报告《Android 勒索软件研究报告》，参考链接：http://zt.360.cn/1101061855.php?dtid=1101061451&did=1101724388

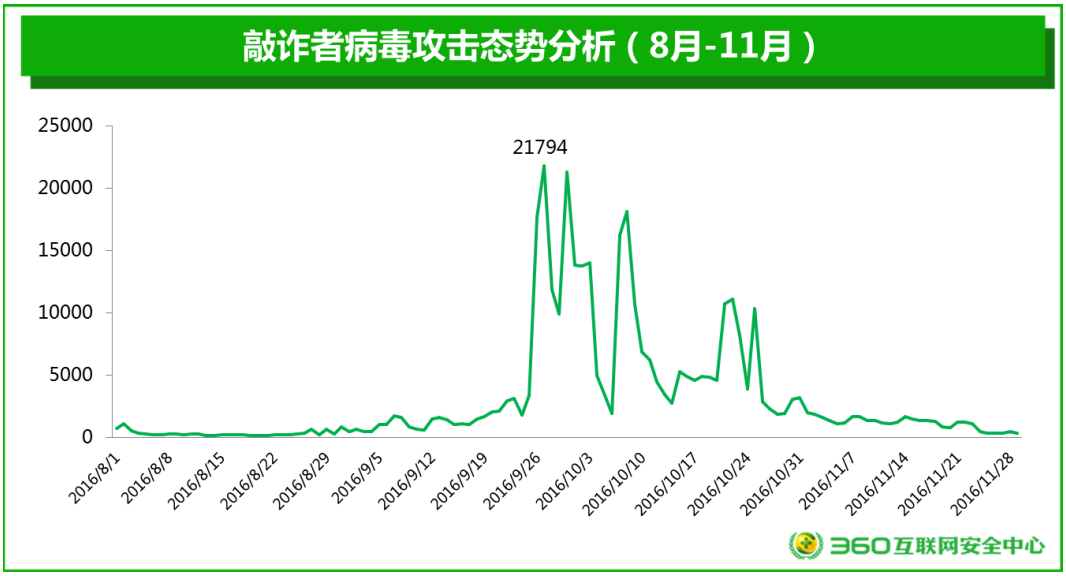
本章内容主要针对，2016 年 1 月-11 月期间，360 互联网安全中心监测到的敲诈者病毒攻击的相关数据。

## 一、　敲诈者病毒的攻击量

360 互联网安全中心的监测显示，2016 年共截获电脑端新增敲诈者病毒变种 113 种，涉及样本 16.7 万个，全国至少有 497 多万台用户电脑遭到了敲诈者病毒攻击 。

根据监测显示，2016 年上、下半年共发生过两次大规模的敲诈者病毒攻击，一次发生在 4 月底至 5 月初，另一次发生在 9 月底至 10 月初。但是，上半年攻击高峰时一天之内被攻击的电脑最多可达到 4644 台，下半年攻击高峰时单日拦截敲诈者病毒超过 2 万余次的情况。下面两张图分别给出了 2016 年 4 月至 5 月，8 月至 11 月期间，敲诈者病毒攻击的态势分析图形。

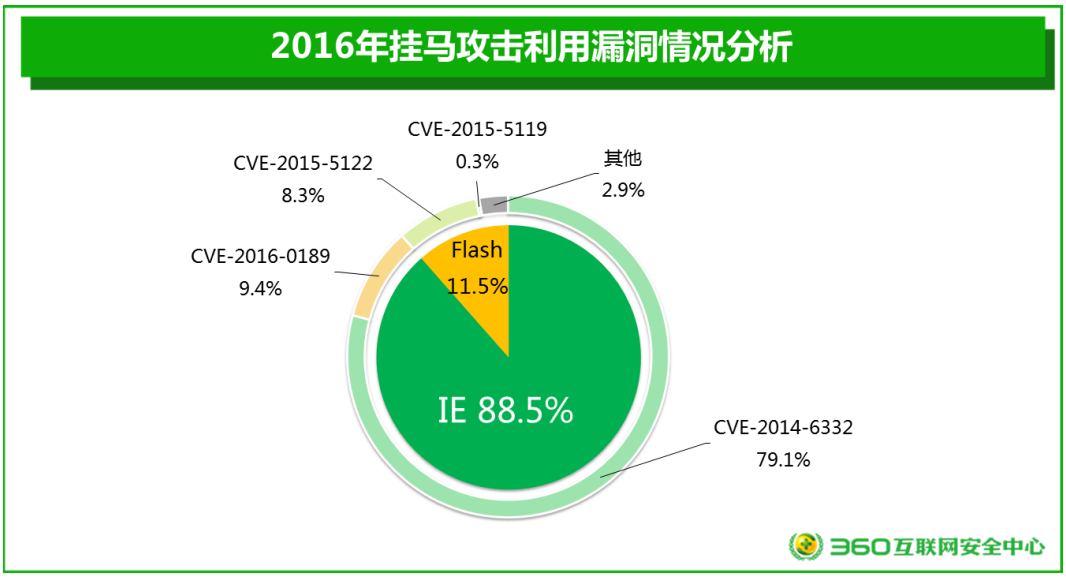



2016 年上半年发生的大规模敲诈者病毒攻击，主要是因为国外某些色情网站被黑客挂马攻击所致，而下半年发生的大规模敲诈者病毒攻击，主要是因为国内某大型金融服务平台网站被黑客挂马攻击所致。挂马攻击是指攻击者在网页中嵌入恶意代码，当用户访问该网页时，嵌入的恶意代码利用浏览器本身的漏洞，在用户不知情的情况下下载并执行恶意木马。

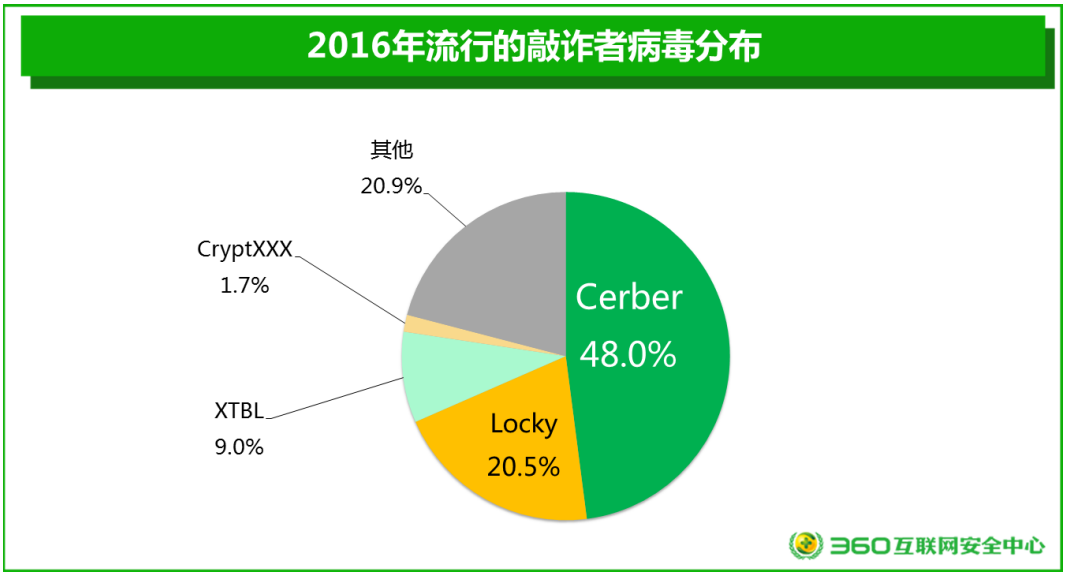
360 互联网安全中心的监测显示，2016 年以来，挂马攻击主要是利用了 IE 漏洞和 Flash 漏洞，其中，IE 漏洞占比为 88.5%，Flash 漏洞占比为 11.5%。被利用最多的四个漏洞分别是 CVE-2014-6332（IE 漏洞）、CVE-2016-0189（IE 漏洞）、CVE-2015-5122（Flash 漏洞）、CVE-2015-5119（Flash 漏洞）。

从下图可以看出，除了 CVE-2016-0189 漏洞是在 2016 年 5 月披露的，其余三个漏洞被利用最多的类型均是在 2014 年或 2015 年就已经被披露过，并且微软和 Adobe 早已发布过相应的补丁来修复这些漏洞，所以说如果用户及时给系统打补丁修复漏洞，完全可以避免绝大多数的网页挂马攻击，避免敲诈者病毒的感染。




## 二、 敲诈者病毒的家族

360 互联网安全中心监测显示， Cerber、Locky、XTBL 是目前最主流的三大敲诈者病毒家族。其中，Cerber 占比为 48.0%，Locky 占比为 20.5%，XTBL 占比为 9.0%。



目前，全球主流的敲诈者病毒家族（类型）有 75 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 | XTBL |
| CryptoHitman | KEYHolder | Protected Ransomware | |

## 三、 敲诈者病毒的传播方式

360 互联网安全中心监测显示，近期的敲诈者病毒主要采用以下三种传播方式：

1) 网页挂马传播

利用浏览器或 Flash 等应用程序漏洞，在网页内嵌入恶意脚本。一旦用户使用未打补丁的程序访问网站，便会触发恶意脚本。脚本会自动执行敲诈者病毒，进而加密用户文件。这类敲诈者病毒属于撒网抓鱼式的传播，并没有特定的针对性，一般中招的受害者多数为裸奔用户，未安装任何杀毒软件。

2) 邮件附件传播

通过伪装成产品订单详情或图纸等重要文档类的钓鱼邮件，在附件中夹带含有恶意代码的脚本文件。一旦用户打开邮件附件，便会执行里面的脚本，释放敲诈者病毒。这类传播方式的针对性较强，主要瞄准公司企业、各类单位和院校，他们最大的特点是电脑中的文档往往不是个人文档，而是公司文档。

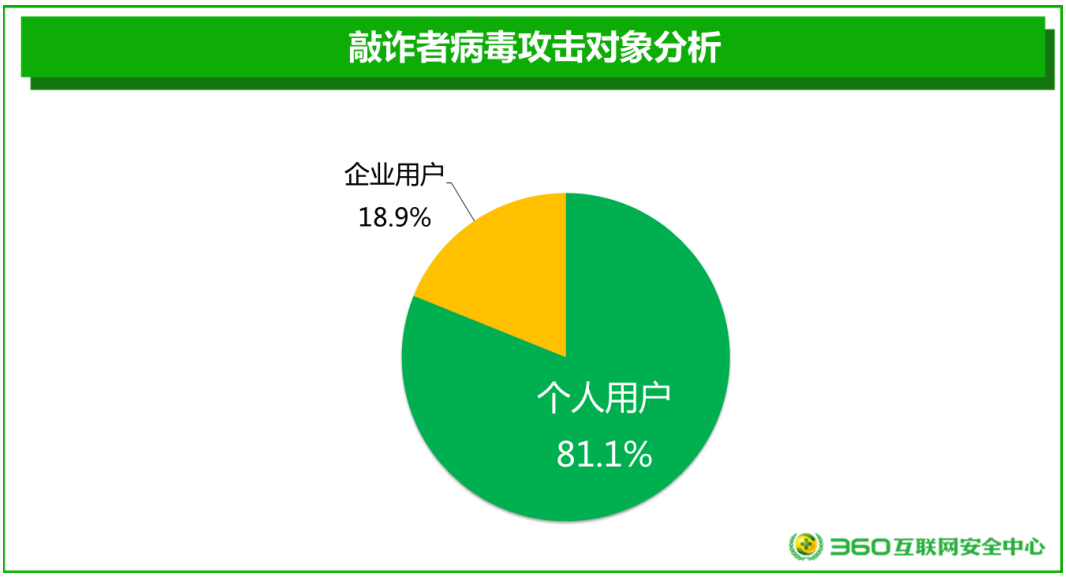
3) 服务器入侵传播

最近以 XTBL 家族为代表的敲诈者病毒主要采用此类攻击方式。黑客通过弱口令、服务器漏洞等方式攻击服务器，并尝试以高权限登录。一旦登录成功，黑客就可以在服务器上为所欲为，例如：卸载服务器上的安全软件并手动运行敲诈者病毒。最后，黑客会留下支付赎金的方式，进而实施敲诈勒索。这类传播途径针对的情况与邮件传播类似，最终目的都是给公司业务的运转制造破坏，迫使公司为了止损而不得不交付赎金。

## 四、 敲诈者病毒的攻击对象

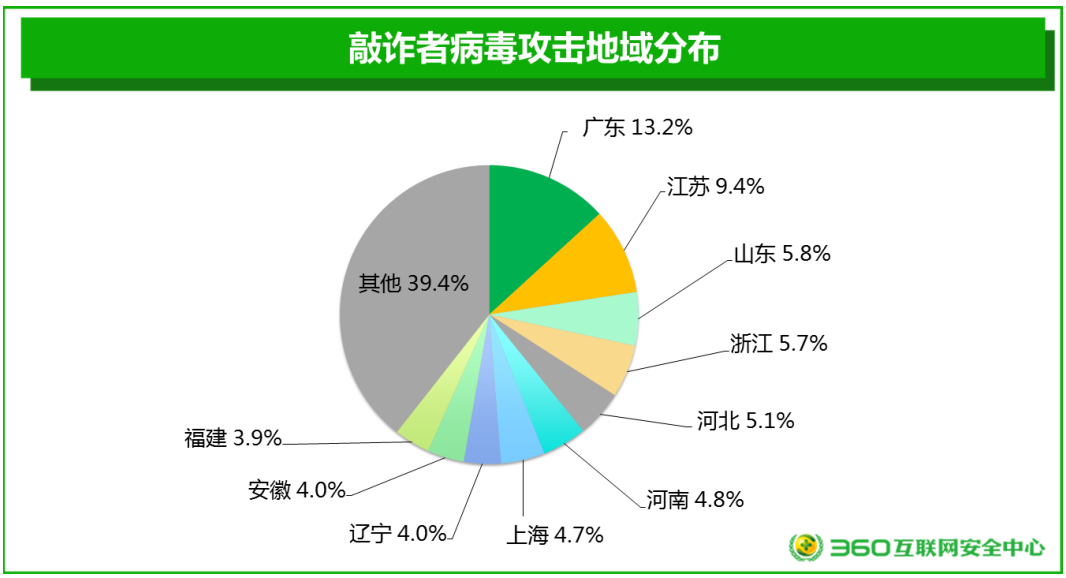
360 互联网安全中心的监测显示，在敲诈者病毒攻击的国内目标人群中，有 18.9%为企业用户，而另外 81.1%为个人用户。

相比于个人用户，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；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。




## 五、 敲诈者病毒攻击的地域分布

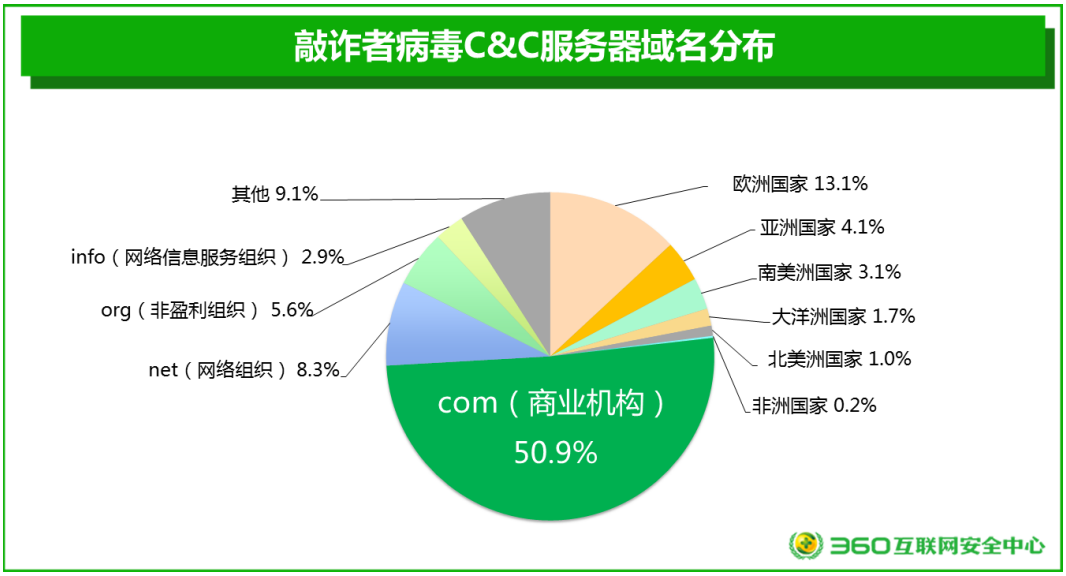
360 互联网安全中心监测显示，遭遇敲诈者病毒攻击的国内电脑用户遍布全国所有省份。其中，广东占比最高，为 13.2%，其次是江苏 9.4%，山东 5.8%，浙江 5.7%，河北 5.1%，河南 4.8%，上海 4.7%，辽宁 4.0%，安徽 4.0%，福建 3.9%。排名前十省份占国内所有被攻击总量的 60.6%。



## 六、 敲诈者病毒的服务器分布

敲诈者病毒通常会使用 C&C 服务器，用于向木马发布加密公钥或记录感染者信息。统计显示，仅自 2016 年 1 月敲诈者病毒开始大规模爆发至 2016 年 11 月底，360 互联网安全中心已经累计监测到各类敲诈者病毒 C&C 服务器 14775 个。

针对最为活跃的部分敲诈者病毒的 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 50.9%，net 和 org 占比分别为 8.3%和 5.6%。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 23.2%左右，其中，属于欧洲国家的域名最多，占 13.1%，其次是亚洲国家 4.1%，南美洲国家 3.1%，大洋洲国家 1.7%，北美洲国家 1.0%，非洲国家 0.2%。



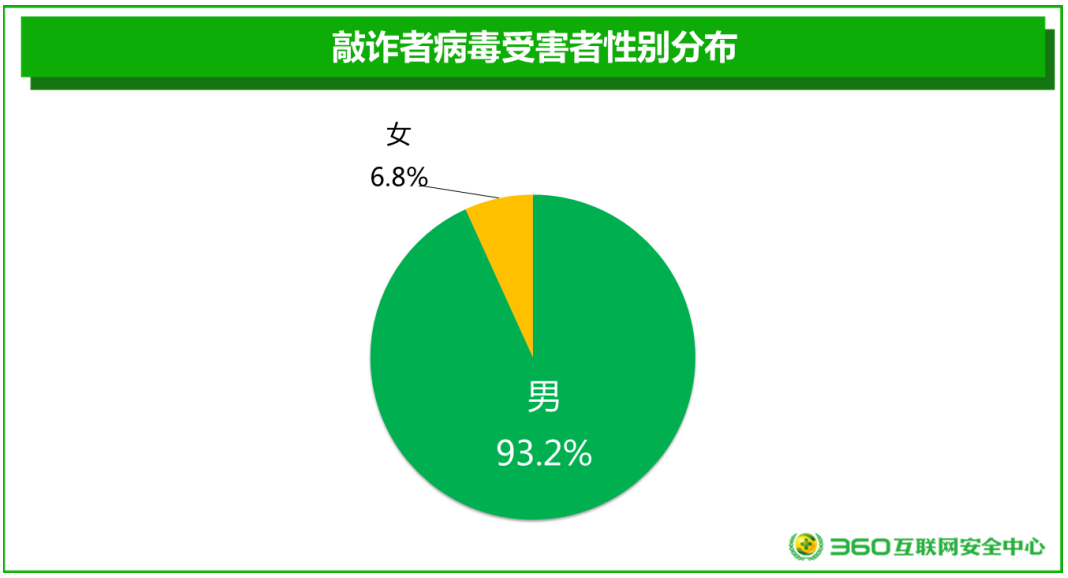
# 第二章　受害者感染途径和文件类型

截至 2016 年 11 月 30 日，360 反勒索服务共接到了 1000 余位遭遇敲诈者病毒攻击的受害者求助。目前绝大多数（94.8%）求助用户并不是在安装了 360 安全卫士，并开启了反勒索服务的情况下感染的敲诈者病毒。特别值得注意的是，还有相当数量的受害者在感染敲诈者病毒时，电脑上没有安装任何安全软件。

为了更好的了解敲诈者病毒的感染原因及受害者特点，以帮助更多的用户提高安全意识，免遭敲诈者病毒侵害，本次报告特别对这 1000 余位求助的受害者进行了抽样调研分析。本报告的第二、三章内容中的各项数据统计，均是来源于本次抽样调研的统计结果。

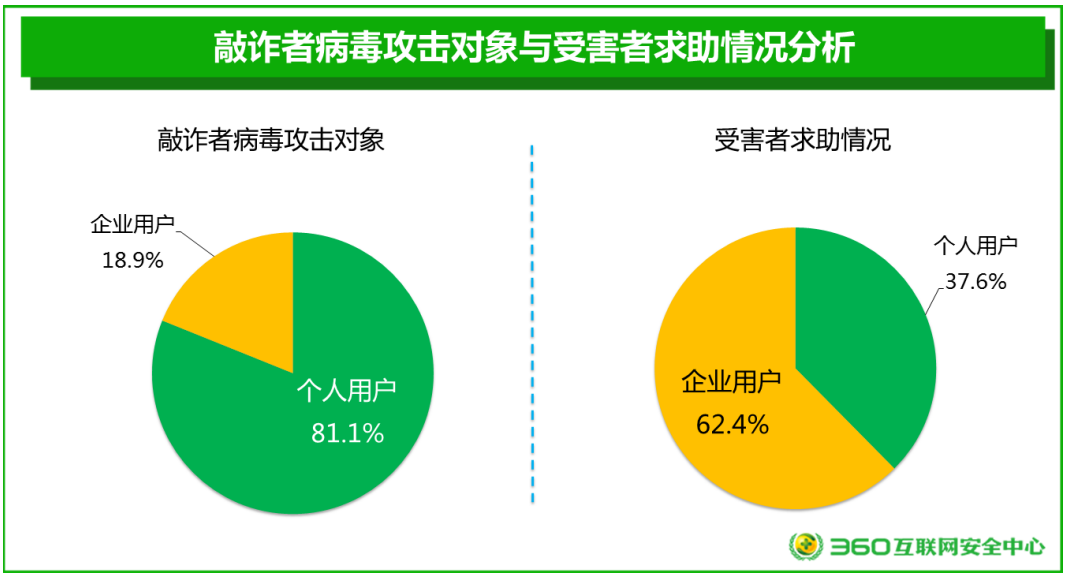
## 一、受害者的基本属性

根据调研数据显示，男性是最容易受到敲诈者病毒攻击的对象，占比高达 93.2%，而女性占比仅为 6.8%。同时调查还显示，男性受害者感染敲诈者病毒的主要原因是通过浏览陌生网页。

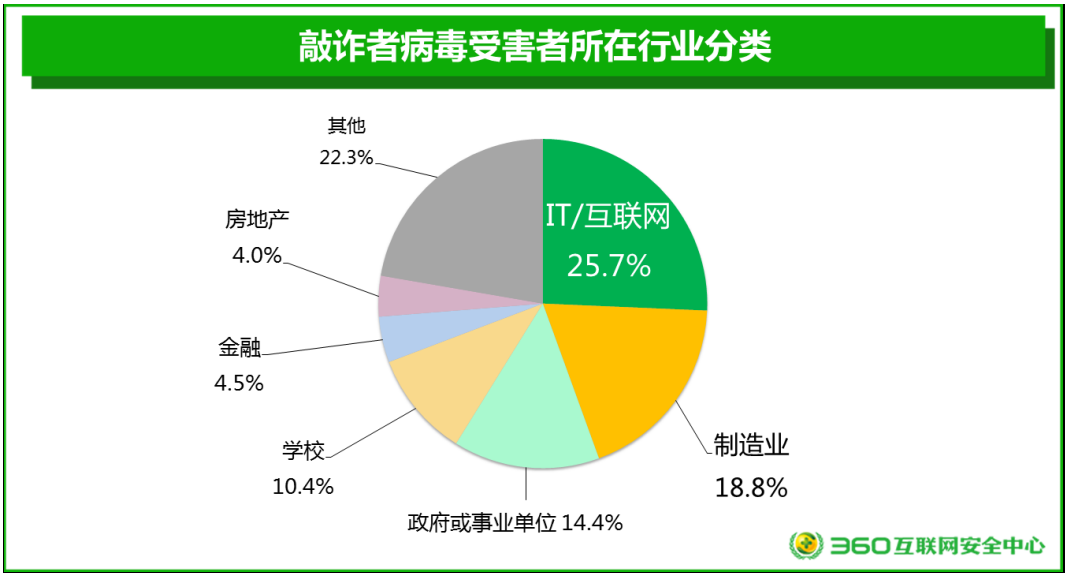


在 360 互联网安全中心接到的受害者主动寻求帮助的人群中，62.4%为企业用户，37.6%为个人用户。这与我们前面分析的敲诈者病毒攻击对象的构成形成了鲜明的对比。在前面的分析中我们看到，在敲诈者病毒的攻击对象中，仅 18.9%为企业用户，81.1%为普通个人用户。

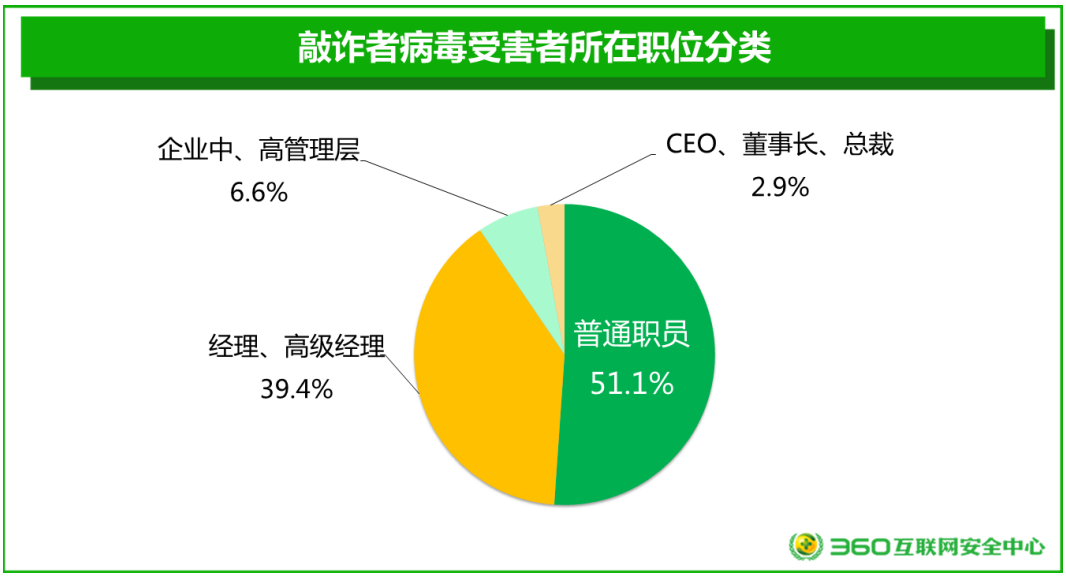
为什么敲诈者病毒的攻击对象与受害者求助人群的构成差异如此之大呢？通过对受害者的调研分析发现，除了国内几次网页挂马传播外，攻击者还会针对企业用户采取邮件传播、服务器入侵等方式传播敲诈者病毒，虽然攻击量不大，但造成的危害比较高。企业用户电脑中毒以后，由于被加密的多是相对更加重要的公司办公和业务文件，因此，企业用户往往会更加积极寻求解决办法，特别是更加积极向专业安全厂商寻求帮助。




从求助的受害者所在的行业分类中可以看出，IT/互联网行业是最容易受到敲诈者病毒攻击的行业，占比为 25.7%；其次，制造业占比为 18.8%，政府或事业单位占比为 14.4%，学校占比为 10.4%，金融类占比为 4.5%，房地产占比为 4.0%。

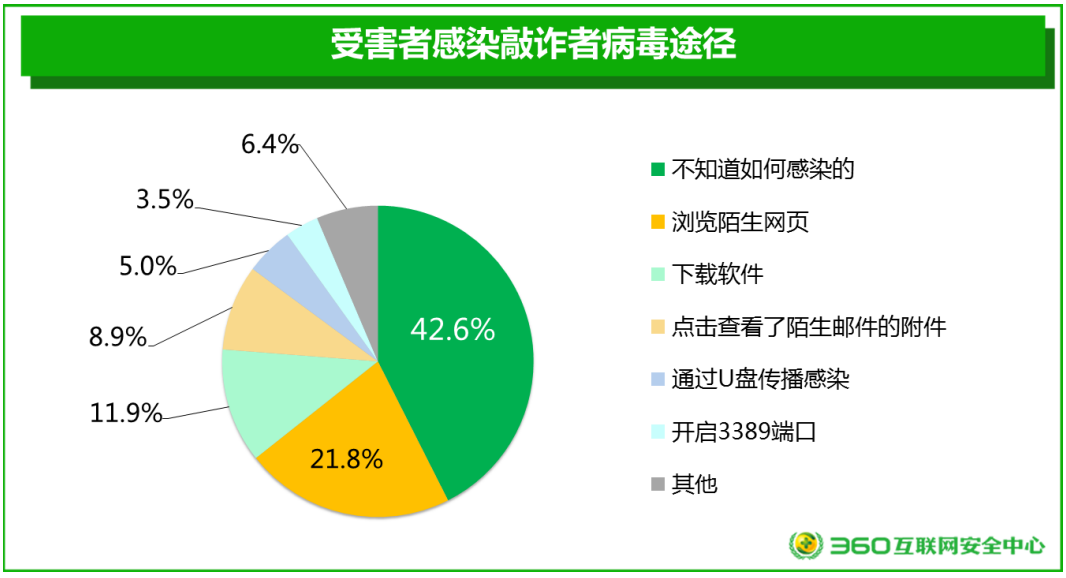


从求助的受害者所在的职位分类中可以看出，普通职员是遭遇敲诈者病毒攻击次数最多的受害者，超过受害者总数的一半以上，占比为 51.1%，其次是经理、高级经理，占比为 39.4%，企业中、高管理层，占比为 6.6%，CEO、董事长、总裁等企业的掌舵者被敲诈者病毒攻击的比例也达到了 2.9%。



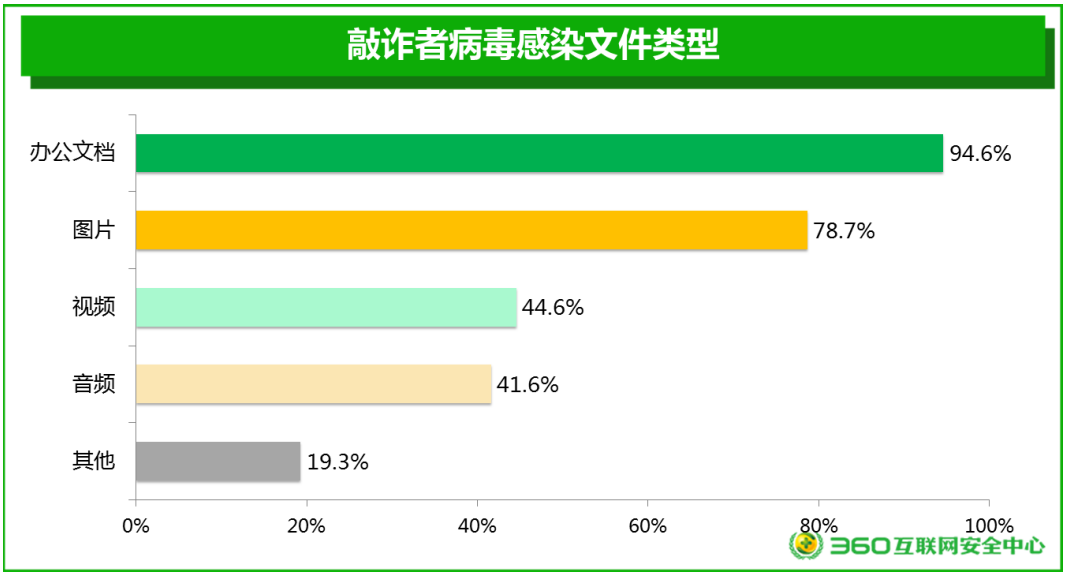

## 二、受害者的感染途径

从求助的受害者感染敲诈者病毒的途径可以看出，42.6%的受害者不知道自己是如何感染的敲诈者病毒，可见该病毒在感染、执行过程中具有极强的隐蔽性，让受害者难以察觉。21.8%的受害者是在浏览陌生网页时感染病毒，11.9%的受害者是下载软件时感染病毒，8.9%的受害者是主动点击查看了陌生邮件的附件感染病毒，5.0%的受害者是通过 U 盘传播感染病毒，3.5%的受害者是开启 3389 端口（Windows 系统自带的远程控制端口），黑客通过远程控制用户的电脑，进而让其感染敲诈者病毒。



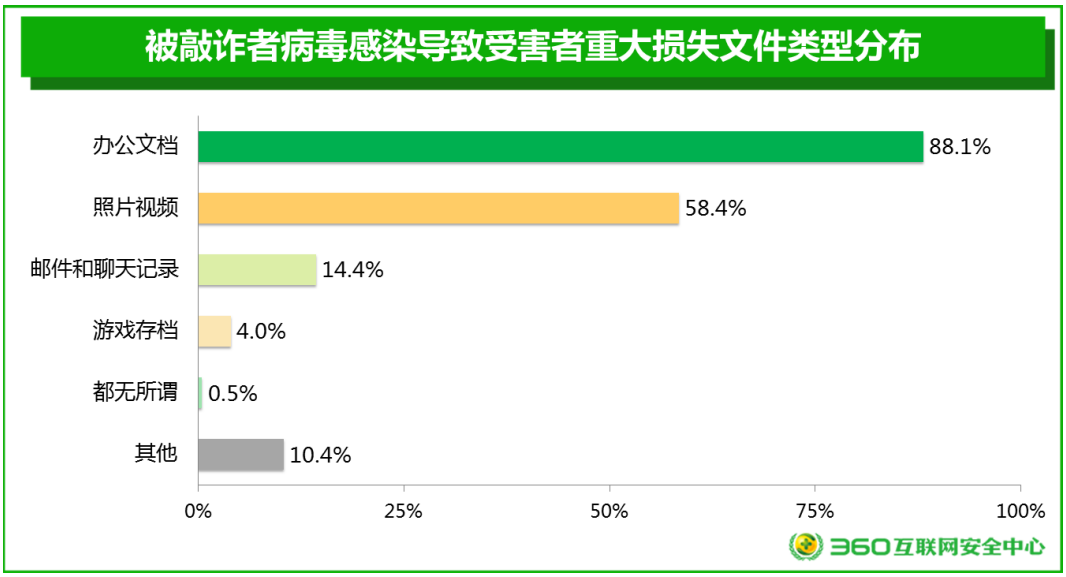
## 三、受害者的感染文件类型

从求助的受害者文件感染类型可以看出，94.6%是受害者电脑上的办公文档被感染，其次，78.7%的图片文件被感染，44.6%的视频文件被感染，41.6%的音频文件被感染。




## 四、导致重大损失的文件类型

在被询问到哪种被病毒加密的文件类型造成损失更加重大的问题时，88.1%的受害者认为办公文档被加密造成的损失破坏最大；其次是认为照片视频文件造成的损失严重，占比为58.4%，邮件和聊天记录，占比为 14.4%，游戏存档，占比为 4.0%。




我们发现，在主动寻求帮助的受害者中，办公文档是感染数量最多，同时也是导致受害者损失最大的文件类型。因为办公文档中往往含有我们工作中用到的重要资料，更加被我们重视和关注。

# 第三章　敲诈者病毒攻击后处理情况

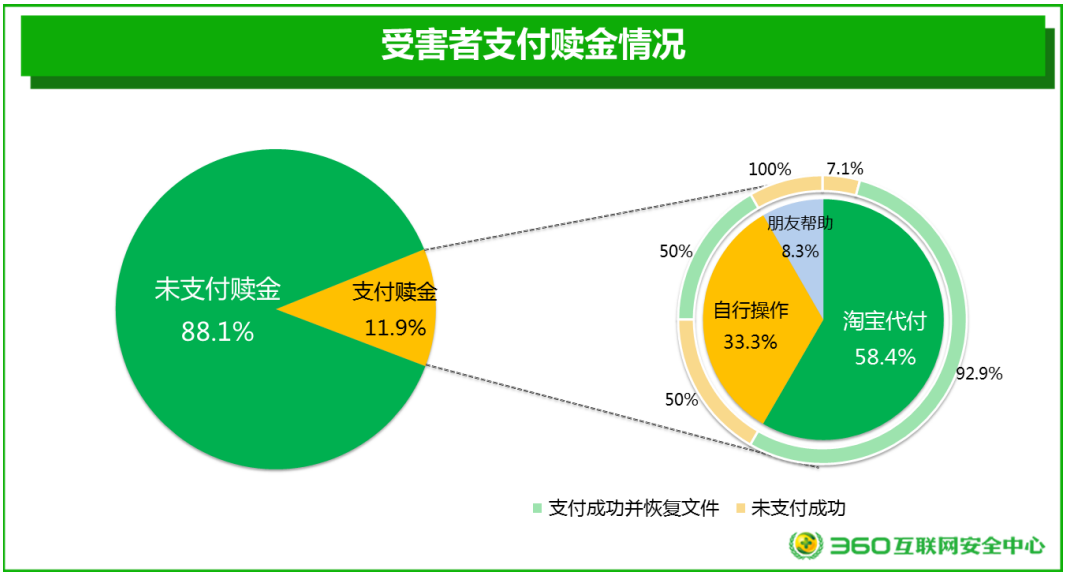
## 一、赎金的支付与支付方式

根据 360 反勒索服务平台对受到敲诈者病毒攻击用户的统计数据显示，目前，绝大多数的敲诈者病毒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 11 月底，1 个比特币价格约为 5223 元。据此计算，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 10446-15669 元人民币。

在 360 反勒索服务目前接到的所有用户求助中，绝大多数（94.8%）求助用户并不是在安装了 360 安全卫士，并开启了反勒索服务的情况下感染的敲诈者病毒，因此无法获得 360 代为支付赎金的帮助。抽样调查显示，在这些求助的受害者中，已有 11.9%的受害者为了恢复文件而支付赎金，另外 88.1%的受害者选择了拒绝为恢复文件而支付赎金。

进一步调查显示，在支付赎金的受害者中，58.4%的受害者是通过在淘宝平台找付款赎金服务付款的，33.3%的受害者是自己按照病毒提示兑换比特币的方式付款的，8.3%的受害者是通过请朋友帮助操作付款的。

另外，我们发现用户通过不同方式支付赎金的成功率有很大的不同。比如，在使用淘宝支付，即在淘宝平台找敲诈者病毒代付赎金服务的用户中，92.9%的受害者最终成功支付了赎金，并恢复了文件；而在自行操作，即自己按照敲诈者病毒提示去兑换比特币付款的用户中，仅有 50.0%的受害者成功支付赎金，并恢复了文件；而最不靠谱的其实是朋友，接受调研的受害者中，所有向朋友求助帮忙支付赎金的用户，均未能支付成功。总体计算下来，仅有 70.8%的受害者最终成功支付了赎金。这一情况说明：支付比特币，对于普通个人用户来说还是有一定难度的，未必都能支付成功。

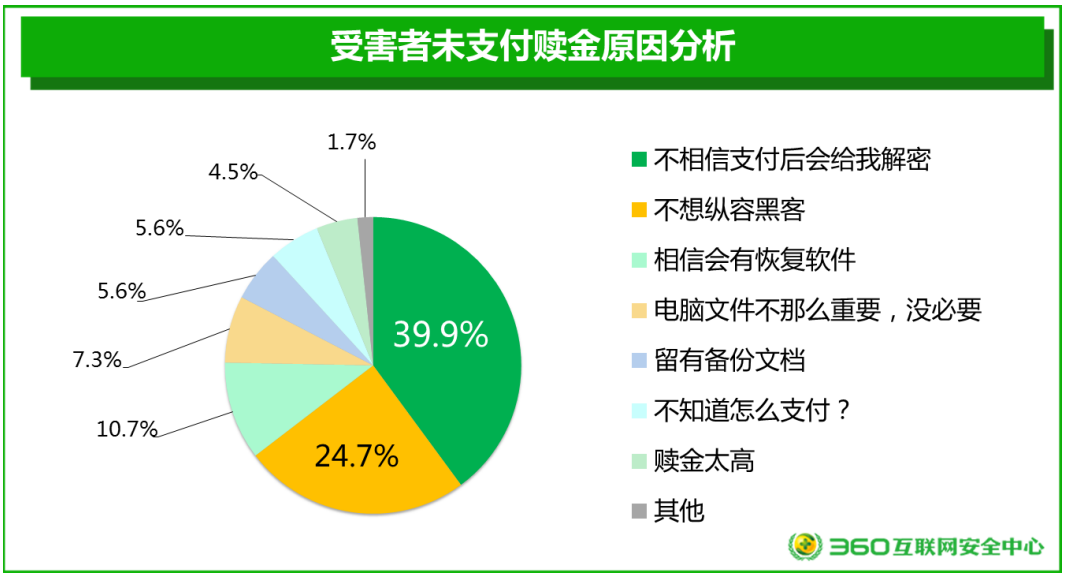



支付赎金但是文档未被解密，主要有几下原因：未按照规定时间支付赎金；未按照规定金额支付赎金；未按照规定时间的规定金额支付赎金；支付操作流程不正确。

## 二、拒绝支付赎金的原因

如前所述，绝大多数，即 88.1%的受害者选择了拒绝为恢复文件而支付赎金。本次报告也特别对这些受害者为什么会拒绝支付赎金的问题进行了调研。

调研结果显示：39.9%的受害者是因为不相信支付赎金后会给自己的文件解密，24.7 %的受害者是因为不想继续纵容黑客进而选择拒绝支付赎金，10.7%的受害者是因为相信会有恢复工具能够修复加密的文件，7.3%的受害者是因为自己的电脑文件中没有重要到需要支付赎金的程度，5.6%的受害者是因为存有备份文件可自行恢复，5.6%的受害者是因为不知道如何支付赎金，4.5%的受害者是因为赎金太高。



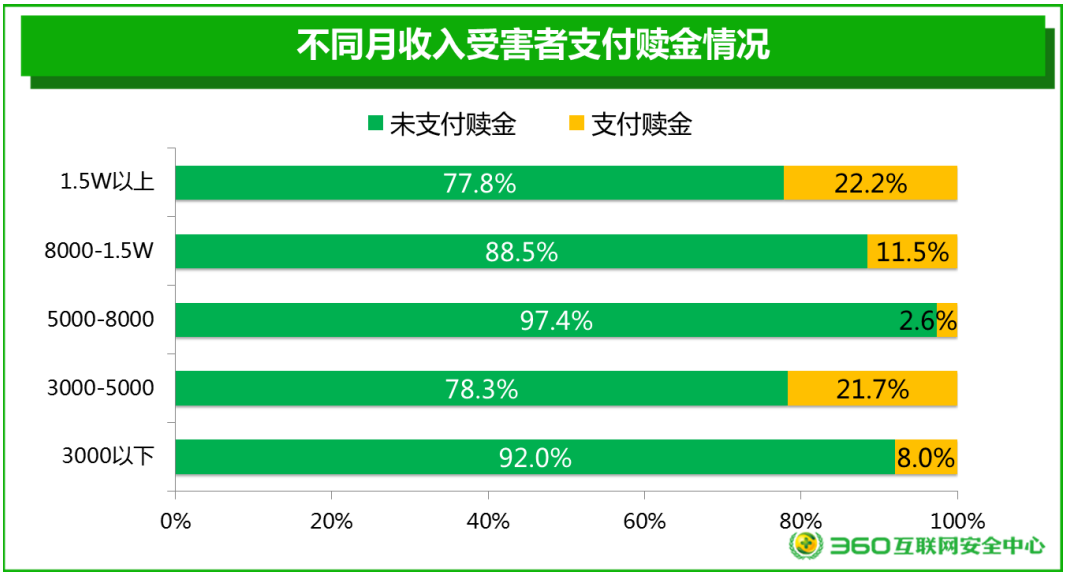

## 三、影响赎金支付的因素

用户调研显示，影响支付赎金的最重要、最根本的因素是被感染文档本身的重要性。不过，除了文件本身的重要性之外，究竟还有哪些因素会影响用户赎金支付意愿呢？本次报告从三个方面对用户进行了调研，分别是受害者的：月收入、工作职位和所在行业。

从受害者的收入方面来看，月收入在 1.5W 以上的受害者最愿意支付赎金，他们选择支付赎金的人占比为 22.2%。对于高收入群来说，电脑中的文件尤其是办公文档非常重要，而且他们支付能力更强，所以他们往往更愿意支付赎金。

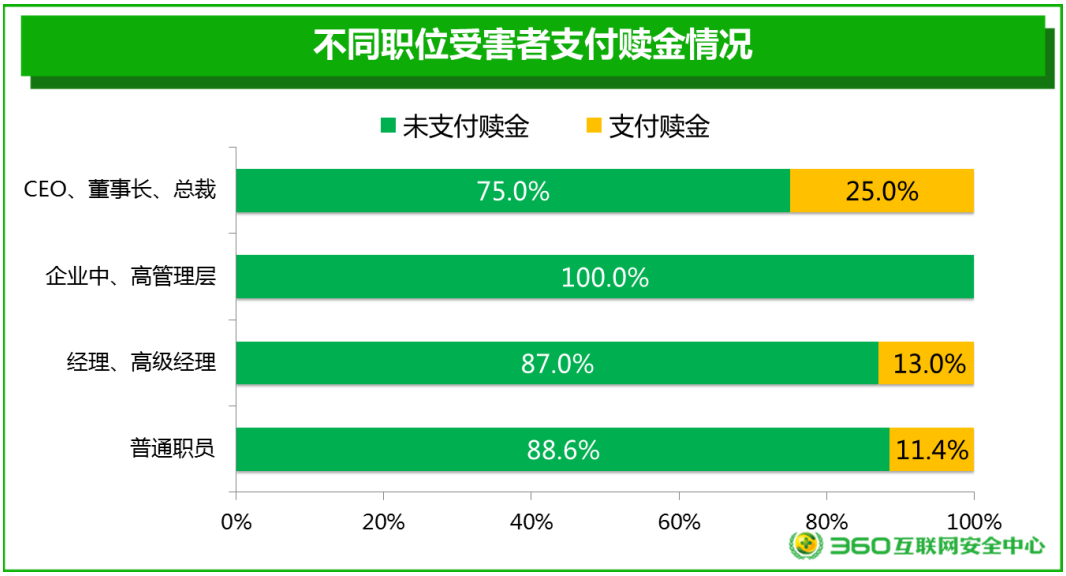
其次是月收入在 3000-5000 元的受害者，这一人群支付赎金的比例为 21.7%。分析认为，这一收入层次的人群绝大多数为企业打工者，作为一线工作人员，他们的很多办公资料也是非常重要，并十分有必要恢复的。

相比之下，其他收入水平的受害者支付赎金的比例均在 10%左右或 10%以下。下图给出了具体情况分析。



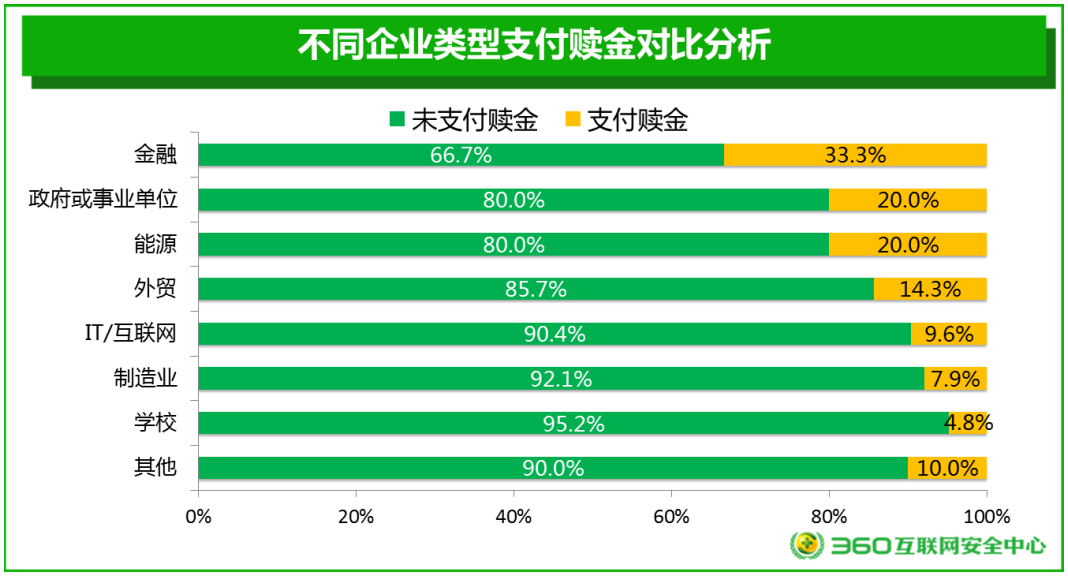

从受害者的工作职位来看：CEO、董事长、总裁等企业核心领导是最愿意支付赎金的，占比为 25.0%，这与前面一项基于收入的分析结论基本一致。由于他们的电脑中往往含有公司最核心的资料，且不一定有其他的备份文档，所以他们也更愿意通过支付赎金来恢复文件。

在我们的调研反馈中，企业中、高管理层没有任何人支付赎金，这主要是由于他们电脑中的资料在下属那里往往存有备份。




从受害者所在的行业来看：金融行业受害者最愿意支付赎金，占比为 33.3%，其次，20.0%为政府或事业单位，20.0%为能源行业，14.3%为外贸行业，9.6%为 IT/互联网，7.9%为制造业，4.8%为学校。

金融行业的支付赎金占比最高，主要是由于金融行业含有大量的投资、风险、客户等金融投资的核心资料。

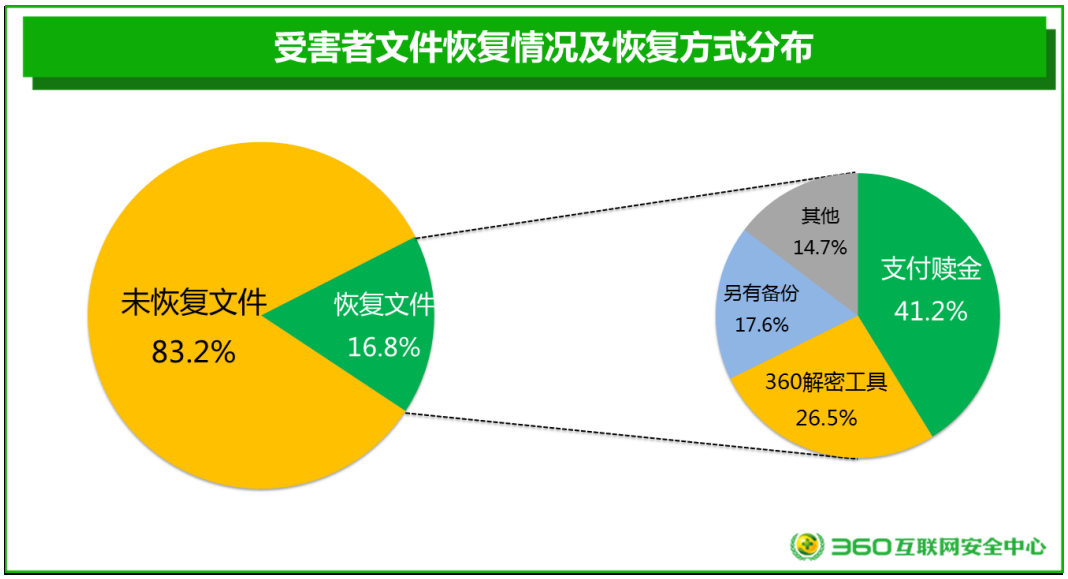



综合收入、职位和行业这三方面因素来看，受害者所属的行业是对支付意愿影响最大的因素。

## 四、恢复感染文件的方法

感染敲诈者病毒后，对于用户来说，最重要的是能否恢复被加密的文件。目前来看，成功支付赎金的受害者都成功的恢复了被加密的文件。此外，由于目前仍有相当一部分的敲诈者病毒并未规范使用加密算法，对文件进行加密，所以，对于感染了此类敲诈者病毒的用户来说，即便不支付赎金，也可以通过专业安全机构，如 360 等安全厂商提供的一些解密工具对文件进行解密。还有一些用户提前对重要文件进行了备份，所以也最终成功恢复了文件。

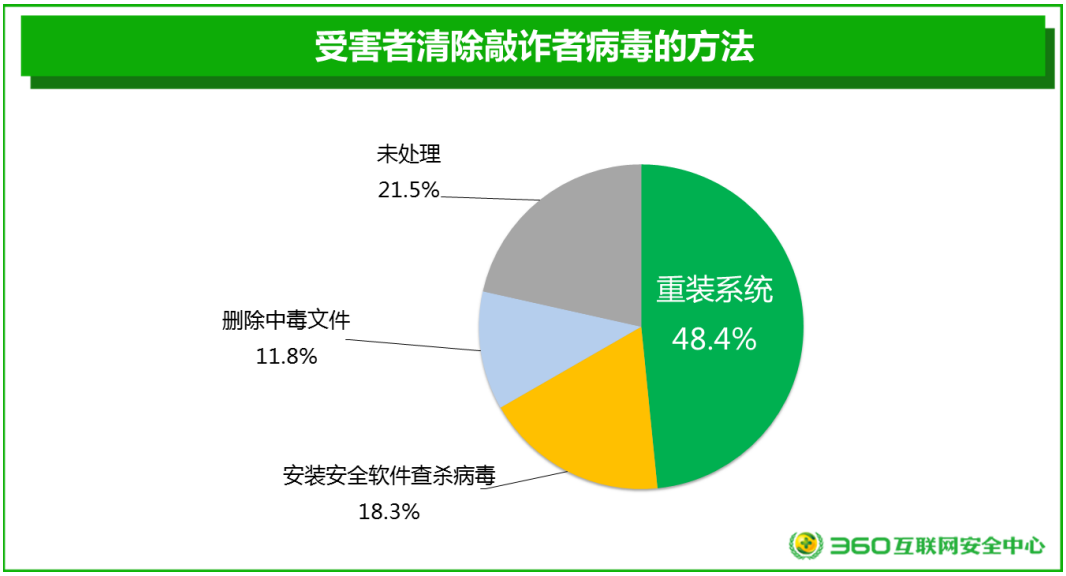
总体来看，在接受调研的受害者中，有 16.8%的受害者最终成功恢复了文件，另外 83.2%的受害者没有恢复文件。在受害者恢复文件的方式中，41.2%的受害者是通过支付赎金恢复的文件，26.5%的受害者是通过 360 提供的解密工具恢复的文件，17.6%的受害者是通过历史备份（如云盘、移动硬盘等）恢复的文件。



## 五、敲诈者病毒清除方法

用户电脑感染敲诈者病毒后，需要进行及时的清除。但不同的人也会选择不同的方法进行清除。抽样调查结果显示：48.4%的受害者通过重装系统清除了病毒，18.3%的受害者通过安装安全软件查杀掉病毒，11.8%的受害者直接删除中毒文件。而且我们还发现，用户选择采用何种方式清除病毒，与用户是否支付了赎金没有关系。

特别值得注意的是，我们发现有 21.5%的受害者在知道自己电脑已经感染敲诈者病毒后，没有采取任何措施清除病毒。这是十分危险的，因为尽管目前已知的绝大多数敲诈者病毒的攻击都是“一次性”的，但也有一部分病毒会带有诸如“下载者”这样的病毒成分，不及时处理，电脑就有可能会持续不断的遭到更多的木马病毒的侵害。




还有一点特别值得注意。在我们协助受害者进行电脑检测时发现，有相当数量的受害者在感染敲诈者病毒时，并未安装任何安全软件。

调查中还发现，对于没有安装安全软件的受害者，在中敲诈者病毒后会首先下载并安装安全软件进行病毒查杀，但是，这种操作是存在一定的风险性的。如果受害者自行清除病毒，可能会同时删除掉被加密的文件和本地保留的密钥文件，造成文档无法解密。

我们特别提醒广大受害者，如果要想恢复文件，切不可直接用安全软件查杀病毒，应该在文件恢复后再安装安全软件进行病毒查杀。另外，要想恢复文件，要在黑客规定的时间内按照标准流程以规定的金额完成付款。

# 第四章　敲诈者病毒的应对措施

## 一、 敲诈者病毒的危害

对于每个人来说，计算机中的文档数据价值各有不同。以实际收到的用户反馈案例看，我们接到的一些个人用户受到的损失如下：

曾经有一位老教授，编写了多年的文稿，大量的资料都被加密，那是他十几年的心血。而当时敲诈者留下的联系方式已经失效，想支付赎金解密都没有办法。最后还好在另外一台计算机中有几个月前的一部分备份，才减小了一部分损失。

还有一个案例是有个大四学生，而被加密的文档包括他辛辛苦苦完成的论文——如果无法解密甚至可能影响到该学生的毕业。

对于企业，影响可能就更大了，曾经有过一个影楼的摄影师电脑中毒了，有很多客户的照片还没有交付照片都被加密了，无法解密的话直接损失就有数万元之多，还有可能是影楼信誉扫地，以及自己丢了工作。

还有一家律师事务所，因为一位员工的计算机中招，除了这位员工计算机文件被加密外，还将数台文件共享服务器中文档加密，直接造成公司业务停摆。

很多时候这个损失已经无法用钱来衡量了，我们之前接到一位用户，敲诈者将其计算机中大量照片加密，用户不愿意给攻击者支付赎金，不愿意助长这类行为，但自己多年来拍摄的照片全部损坏，甚是心痛。

## 二、 敲诈者病毒的不可解

采用了不对称加密算法的敲诈者病毒，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病毒进行有效的防护，一旦电脑感染木马，一旦木马对电脑系统中的文件的加密过程完成，理论上来说，除非向攻击者支付赎金获取解密密码，否则目前技术手段下将无法恢复文件。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。

造成敲诈者病毒“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，敲诈者病毒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已经被公认为是安全有效的，只有拿到密钥才能够进行解密，其算法依据是一些数学难题，密钥在数学上是无法破解的。

所以，一旦电脑感染了敲诈者病毒（不包括锁屏木马或采用对称加密技术等简单的敲诈者病毒），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。

## 三、 360 反勒索服务

对于敲诈者病毒，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。由于敲诈者病毒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病毒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，已经可以对敲诈者病毒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者病毒，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病毒，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。

## 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病毒的攻击：

**养成良好的安全习惯：**

1） 电脑应当安装具有云防护和主动防御功能的安全软件，不随意退出安全软件、关闭防护功能，对安全软件提示的各类风险行为不要轻易放行。

2） 使用安全软件的第三方打补丁功能对系统进行漏洞管理，第一时间给操作系统和 IE、Flash 等常用软件应及时打好补丁，以免病毒利用漏洞自动入侵电脑。

3） 尽量使用安全浏览器，减少遭遇挂马攻击的风险。

4） 重要文档数据应经常做备份，一旦文件损坏或丢失，也可以及时找回。

**减少危险的上网操作：**

5） 不要浏览来路不明的色情、赌博等不良信息网站，这些网站经常被用于发动挂马、钓鱼攻击。

6） 不要轻易打开陌生人发来的邮件附件或邮件正文中的网址链接。

7） 不要轻易打开后缀名为 js 、vbs、wsf、bat 等脚本文件和 exe、scr 等可执行程序，对于陌生人发来的压缩文件包，更应提高警惕，应先扫毒后打开。

8） 电脑连接移动存储设备，如 U 盘、移动硬盘等，应首先使用安全软件检测其安全性。

9） 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。

**采取及时的补救措施：**

10） 安装 360 安全卫士并开启反勒索服务，一旦电脑被敲诈者病毒感染，可以通过 360 反勒索服务支付赎金，以尽可能的减小自身经济损失。

# 附录 1 2016 年敲诈者病毒重大攻击事件

## 一、 印度三家银行被敲诈，面临百万美元损失

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 1 比特币赎金。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。

## 二、 好莱坞长老教会遭敲诈，支付 40 比特币赎金

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 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。

## 三、 美国多所学校遭敲诈，支付 20 比特币赎金

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 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。

## 四、 带毒邮件传播 Locky，某央企一周三次中招

2016 年 2 月中旬，一种名为“Locky”新型病毒开始伪装成电子邮件附件的形式，在全世界各地迅速传播，并很快成为最流行敲诈者病毒之一。一旦电脑用户点击携带病毒的附件，则计算机上的办公文档、照片、视频等文件就会被恶意加密。用户要想重新解开数据的密码，就必须向这款病毒的发布者缴纳一定数量的赎金。其中，国内某央企一周内连续三次中招，给该机构造成不可逆的严重损失。

## 五、 美国国会为阻敲诈者病毒封杀谷歌、雅虎部分服务

2016 年 5 月，据外媒报道，美国国会众议院议员开始受到敲诈者病毒的攻击，为了阻止该病毒的扩散，美国国会先后封杀了 Google 的 Appspot.com 域名和雅虎电邮服务 Yahoo Mail，并警告议员注意网络安全。

## 六、 外国机构研究显示 35%的大型企业过去一年曾被敲诈

2016 年 8 月，Malwarebytes 公布的 Osterman 全球研究报告显示，125 家接受调查的加拿大企业中，44 家在过去 1 年内公司网站被敲诈者病毒攻击过，不少企业甚至因此被迫停业。为找回公司文件和恢复被病毒感染的 IT 系统，33 家企业被迫向黑客支付赎金，金额均在在 1000 到 5 万加元之间。

## 七、 香港多家知名机构遭敲诈，被勒索赎金数万元

2016 年 10 月，中国香港地区电脑保安事故协调中心共接到 277 宗有关敲诈者病毒的报告，较去年同期激增 5.6 倍，受害者多为中小企业及非盈利机构。敲诈者病毒一般隐身于邮件附件内，伪装成账单、发票等诱使收件人点击，执行后加密所有本地文件及部分共享服务

器中的文件。香港海事处电脑系统中招后遭遇黑客数万元比特币的赎金勒索，四大会计师事务所之一的德勤也成为受害者。

## 八、 Locky 病毒借 Facebook 等知名网站攻击用户

2016 年 11 月，敲诈者病毒 Locky 攻击国外多款主流社交网站，Facebook、LinkedIn 等被植入含有恶意程序的图片，用户浏览时自动下载，点击查看时敲诈者病毒便运行起来。国外多家媒体纷纷对此发布预警，提醒网民慎重点击网络及本地中的可疑图片。

## 九、 旧金山公交系统被敲诈，市民免费乘坐公交车

2016 年 12 月，旧金山的公交售票系统也因敲诈者入侵而大面积瘫痪，市民得以免费乘坐公交车。负责当地公交运营的 SF Muni 公司电脑上出现了“你已被黑”的警告信息，想要恢复系统运行要缴纳 73 万美元的赎金。

# 附录 2 非常规敲诈者病毒样例

部分敲诈者病毒是针对特定国家的，比如，Cerber 会避开俄语国家，XTBL 主要针对中日韩。国内和国外的敲诈者病毒很多是使用相同的技术手段，只是在传播方式和渠道上有所不同。不过，出现过一些比较非常规的敲诈者病毒，这些病毒大多属于黑客新人练手的作品，可能会显得比较另类，有些甚至单个文件可单个解密，并且限时优惠，这些病毒很多并没有使用规范的加密方式，很大一部分可以通过技术手段破解。

## 一、 Voldemont 敲诈者病毒

一个伏地魔的照片突然出现在面前，着实有些吓人。Voldemont 敲诈者病毒没有勒索信，也不让你看到那一大堆被加密的文件，在你面前只有这么一张图。不过还有一个更吓人的，就是这款敲诈者病毒不勒索比特币，而是直接要你把信用卡发给他。

这是目前已知的可信度最低的敲诈者病毒攻击，受害者一旦主动告知黑客信用卡的卡号后，黑客可以无节制的盗刷信用卡。另一方面，对比比特币的敲诈者病毒攻击来说，此类敲诈者病毒攻击并不是不可解的，还是可以通过寻求安全厂商或是公安机关的帮助，在不支付赎金的情况下，成功恢复文件的。

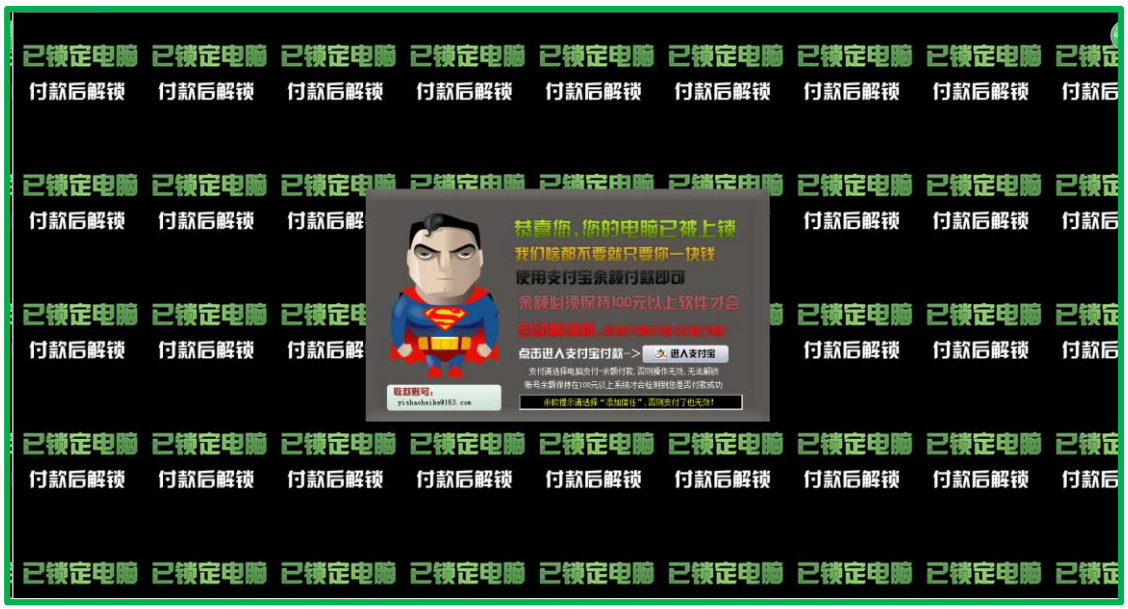
## 二、Cerber3 敲诈者病毒

分级加密方式，每一个文件中都存储有加密文件使用的密钥，攻击者对单个文件实施解密操作。在攻击者提供的付款页面中也提供了“免费解密单个文件”的功能。单个文档单个加密或是解密，并且还可以享受限时优惠。


## 三、一元钱敲诈者病毒

超人现身我们的电脑屏幕，并声称“我们啥都不要就只要你一块钱”，要求用支付宝余额付款，并且，只有余额在 100 元以上才会给解密。

黑客在受害者支付赎金的过程中可能会盗刷支付宝余额。在此提醒广大受害者，支付赎金时，尽量保证余额在 101 元，不要存入大量的现金，并且暂时关闭小额免密支付，同时要注意支付工具提供的支付金额提醒，尽可能的减少财产损失，避免二次被骗。



## 四、Popcorn Time 敲诈者病毒

Popcorn Time 敲诈者病毒不仅可以让受害人通过支付赎金来恢复他们的文件，还可以通过让受害人去感染两个新用户，并让他们支付赎金的方式，去获得一个免费的解密密钥。


更严重的是，在未完成的敲诈者病毒代码中还发现，如果用户输入错误的解密密钥 4 次以上，敲诈者病毒有可能会将文件删除。

# 附录 3 360 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病毒，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，如果用户遇敲诈者病毒攻击，点击下图中的“申请服务”按钮即可申请理赔。

# 附录 4 360 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“敲诈者病毒防护功能”：

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“启用敲诈者病毒防护功能”，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。

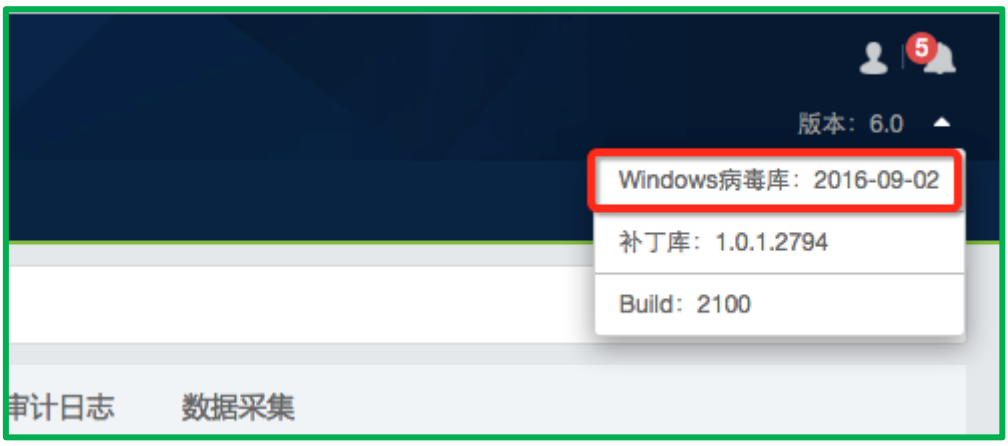
5、终端升级模式设定为自动升级：

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”。