

# 2019 年 勒索病毒疫情分析报告



**360 互联网安全中心**

核心安全反病毒部

2019 年 12 月

## 摘 要

- ✧ 2019 年前 11 个月，国内受勒索病毒攻击的计算机数量约 412.5 万台（排除 WannaCry 数据）。2 月和 3 月的攻击相对较高，全年整体攻击趋势平稳，总体攻击量仍然较高。
- ✧ 2019 年前 11 个月，360 反勒索服务平台一共接收并处理了超过 4600 例遭勒索病毒攻击求助。
- ✧ 2019 年前 11 个月，活跃的勒索病毒家族以 GlobeImposter、Crysis、phobos 为主，这三大勒索病毒家族的受害者占比约为 45.9%。
- ✧ 超过半数的勒索病毒依靠远程桌面入侵方式传播。而今年，利用破解软件或激活工具传播的勒索病毒数量也有显著提升，占到了总量的 12.0%。
- ✧ 勒索病毒所攻击的地区以数字经济发达和人口密集地区为主，全年受到攻击最多的省市前三为：广东、浙江、北京。
- ✧ 被勒索病毒感染的系统中 Windows 7 系统占比最高，占到总量的 40.1%。在系统分类中，服务器系统占比进一步提高，占到总量的 29.4%。
- ✧ 据统计，在 2019 年前 11 个月，受到勒索病毒攻击最多的行业前三分别为：批发零售、制造业、教育，占比分别为 16.8%、16.1%、12.4%。
- ✧ 根据反勒索服务的反馈数据统计，受感染计算机的使用者多为 80 后和 90 后，分别占到总数的 56.5%和 23.7%。男性受害者占到了 92.5%，女性受害者则仅为 7.5%。
- ✧ 根据反勒索服务的反馈数据统计，97.4%的受害者在遭到勒索病毒攻击后，选择不向黑客支付赎金。
- ✧ 2019 年前 11 个月，勒索病毒进一步加强对服务器系统的攻势。弱口令攻击依然是勒索病毒进入受害器的主要手段。此外，钓鱼邮件、漏洞入侵、网站挂马、利用破解或激活工具传播也是勒索病毒传播的常见手段。
- ✧ 2019 年，勒索病毒形势更加严峻，技术攻防更加激烈，传播形式更加多样，而对勒索病毒相关的服务也提出了更高的要求，标准化、专业化会是未来的一个趋势。
- ✧ 预计 2020 年，勒索病毒的制作与攻防解密相关产业会有进一步的发展。而与之对应的打击力度，也势必会增加。

# 目 录

<b>第一章 勒索病毒攻击形势</b>	<b>1</b>
一、 勒索病毒总体攻击态势	1
二、 反勒索服务处理情况	2
三、 勒索病毒家族分布	2
四、 传播方式	3
<b>第二章 勒索病毒受害者分析</b>	<b>4</b>
一、 受害者所在地域分布	4
二、 受攻击系统分布	5
三、 受害者所属行业分布	6
四、 受害者年龄层分布	7
五、 受害者性别分布	7
六、 受害者赎金支付情况	8
<b>第三章 勒索病毒攻击者分析</b>	<b>9</b>
一、 黑客登录受害计算机时间分布	9
二、 勒索联系邮箱的供应商分布	9
三、 攻击手段	10
(一) 弱口令攻击	10
(二) 钓鱼邮件	12
(三) 利用系统与软件漏洞攻击	12
(四) 网站挂马攻击	14
(五) 破解软件与激活工具	14
<b>第四章 勒索病毒发展趋势分析</b>	<b>16</b>
一、 勒索病毒攻防技术发展	16
(一) 勒索病毒攻击形势变化	16
(二) 勒索病毒防护技术发展	17
(三) 勒索病毒处置服务更趋专业化	18
二、 勒索病毒相关产业发展	18
(一) 病毒制作传播与解密相关产业	18
(二) 针对勒索病毒相关的犯罪打击	18
<b>第五章 安全建议</b>	<b>20</b>
一、 针对个人用户的安全建议	20
(一) 养成良好的安全习惯	20

(二) 减少危险的上网操作 .....	20
(三) 采取及时的补救措施 .....	20
二、 针对企业用户的安全建议 .....	20
<b>附录 1 2019 年勒索病毒大事件 .....</b>	<b>22</b>
一、 GANDCRAB 金盆洗手 .....	22
二、 GLOBELMPSTER 继续蔓延 .....	22
三、 美国城市遭勒索病毒攻击，政府已交赎金 .....	22
四、 易到用车遭勒索病毒攻击 .....	23
五、 勒索病毒瞄准 NAS 服务器 .....	23
六、 六千余台服务器感染 LILocked .....	24
七、 要么缴纳赎金要么泄露数据 .....	25
八、 197 万元勒索赎金坑苦受害公司 .....	26
<b>附录 2 360 安全卫士反勒索防护能力 .....</b>	<b>27</b>
一、 弱口令防护能力 .....	27
二、 漏洞防护防护能力 .....	27
三、 挂马网站防护能力 .....	29
四、 钓鱼邮件附件防护 .....	29
<b>附录 3 360 解密大师 .....</b>	<b>30</b>
<b>附录 4 360 勒索病毒搜索引擎 .....</b>	<b>31</b>

## 第一章 勒索病毒攻击形势

2019 年前 11 个月，360 互联网安全中心监测到大量针对普通网民和政企部门的勒索病毒攻击。根据 360 安全大脑统计，2019 年前 11 个月共监控到受勒索病毒攻击的计算机 412.5 万台，处理反勒索申诉案件近 4600 例。从攻击情况和危害程度上看，勒索病毒攻击依然是当前国内计算机面临的最大的安全威胁之一。在企业安全层面，勒索病毒威胁也已深入人心，成为企业管理者最为担忧的安全问题。本章将针对 2019 年前 11 个月，360 互联网安全中心监测到的勒索病毒相关数据进行分析。

### 一、勒索病毒总体攻击态势

截至 2019 年 11 月 30 日数据，360 互联网安全中心共监测到受勒索病毒攻击的计算机 412.5 万台，平均每天有约 1.2 万台国内计算机遭受勒索病毒的攻击。该攻击量较 2018 年相比基本持平，总体疫情态势依然严峻。

下图是 2019 年前 11 个月受勒索病毒攻击设备数情况。从图中可见，勒索病毒在上半年的高峰集中在 2 月份前后，主要是由于 GandCrab 家族的一次较大规模挂马疫情导致。而下半年则相对平稳，11 月出现了小幅的抬头趋势，但并未出现单个家族比较集中的勒索病毒攻击疫情。

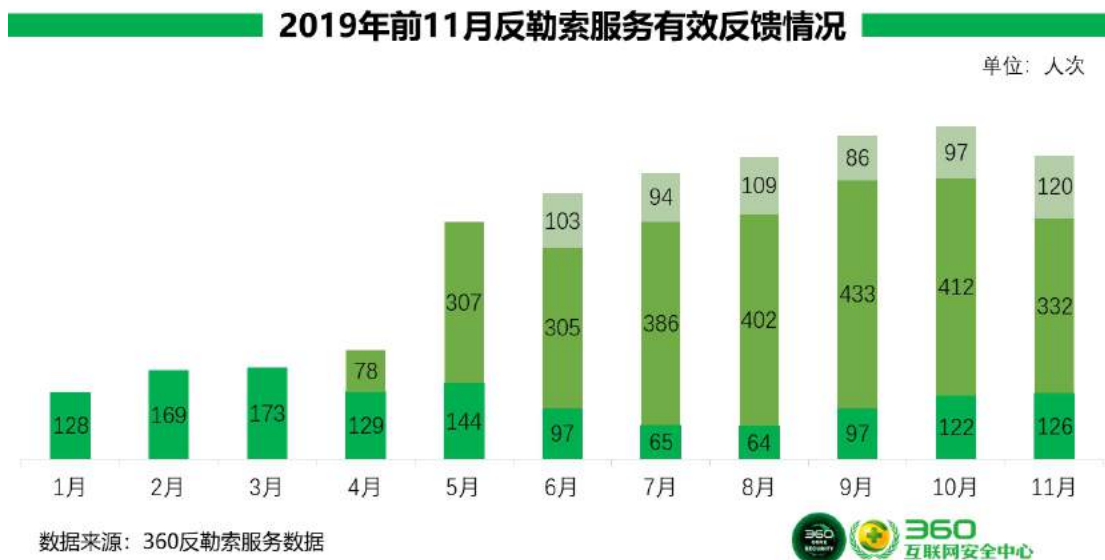


总体而言，2019 年勒索病毒的攻击态势依旧严峻。虽然 GandCrab 家族在 2 月发动了一波挂马攻击后便宣布不再更新，但其继任者 Sodinokibi（“锁蓝”勒索病毒）很快就接替了其传播渠道，继续危害社会。只要还存在着丰厚的利润，整个勒索病毒产业就不会因为某一款病毒或某一个家族的退出而就此退出历史舞台。

## 二、 反勒索服务处理情况

2019 年前 11 个月，以 360 反勒索服务平台、360 解密大师沟通群、360 论坛勒索病毒板块为主的几大渠道，一共接收并处理了近 4800 位遭受勒索病毒程序攻击的受害者求助，其中超 4600 位经核实确认为遭到了勒索病毒的攻击。通过以上反馈渠道，反勒索服务共帮助超过 485 位用户完成文件解密。

下图给出了在 2019 年上前 11 个月，每月通过 360 安全卫士反勒索服务、360 解密大师沟通群、360 论坛勒索病毒板块，提交申请并确认感染勒索病毒的有效申诉量情况。其峰值出现 9、10 月份，两月均有超过 600 位用户被确认感染勒索病毒。但由于解密大师沟通群反馈和论坛反馈两个渠道为下半年新加入的反馈渠道，所以与之前数据并无横向对比意义，而下半年三大渠道的合计反馈量则总体平稳，无较大波动。



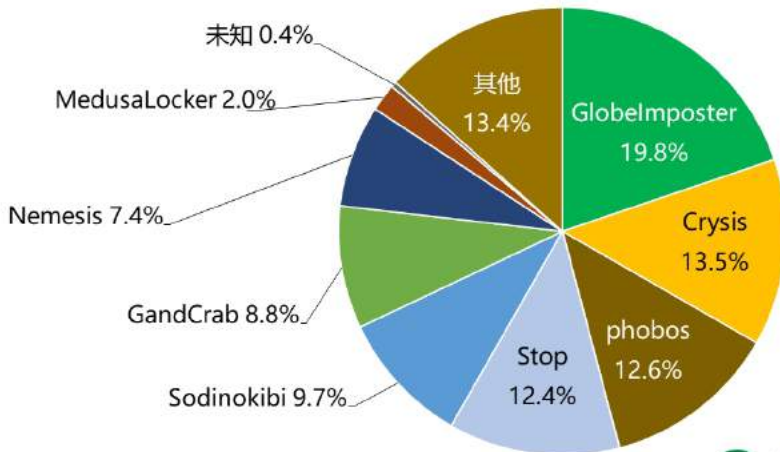
2019 年 1 月至 3 月期间，勒索病毒感染量涨幅较大，主要是受到 GandCrab、Paradise 以及 GlobeImposter 三个勒索病毒家族的影响。在 2 月到 3 月期间，由于 GandCrab 和 Paradise 勒索家族使用 Fallout Exploit Kit 漏洞工具进行挂马攻击导致不少用户中招。在 2019 年 4 月底一款新型勒索病毒 Sodinokibi 利用 WebLogic 漏洞传播，到导致 5 月份感染量上升。由于该勒索病毒“继承”了 GandCrab 的多个传播渠道、传播方式、传播人员等，该勒索病毒一直被视为 GandCrab 勒索病毒家族的“传承”。在 8 月份到 9 月份期间，Stop 勒索病毒开始疯狂利用激活工具/破解软件传播勒索病毒。9 月至 11 月份，通过暴力破解远程桌面进行传播的 GlobeImposter、Crysis 以及 phobos 有大幅度上升。同时出现多个其他勒索病毒：例如 GarrantyDecrypt、Hermes837、MedusaLocker 等勒索病毒。

## 三、 勒索病毒家族分布

下图给出的是根据 360 反勒索服务数据，所计算出的 2019 年前 11 个月勒索病毒家族流行度占比分布图，PC 端 Windows 系统下 GlobeImposter、Crysis、phobos 这三大勒索病毒家族的受害者占比最多，合计占到了 45.9%。由于 GandCrab 家族的退出，前 11 个月的数据

中，各家族的占比相较于上半年的数据会显得更为平均，前 7 名之间的差距都不是非常的悬殊。

2019年前11月勒索病毒家族分布

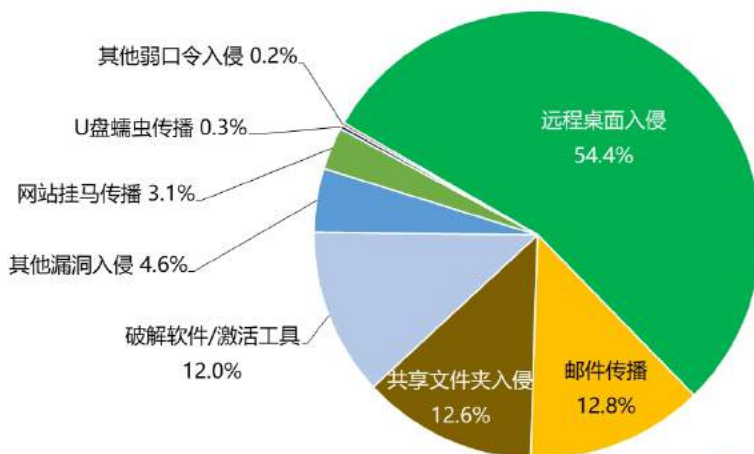


数据来源：360反勒索服务数据

#### 四、 传播方式

下图给出了攻击者投递勒索病毒的各种方式的占比情况，统计可以看出，远程桌面入侵仍然是用户计算机被感染的最主要方法。而邮件传播的方式则再次回暖，超越共享文件夹入侵方式成为占比第二的传播手段。此外，值得注意的是：破解软件/激活工具以 12% 的占比一跃成为占比第四的传播方式。这是以往从未出现过的。这也对经常使用此类软件的用户敲响了警钟，对于安全软件对此类程序的报毒，不要盲目的认为是对此类程序的“误报”。

2019年前11月勒索病毒传播方式分布



数据来源：360反勒索服务数据

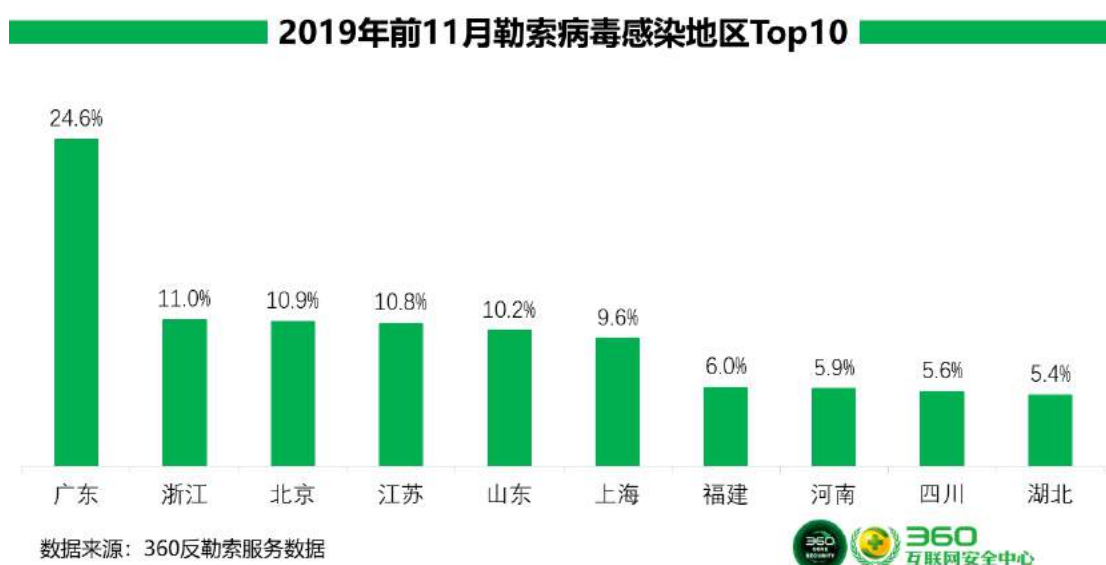
## 第二章 勒索病毒受害者分析



基于反勒索服务数据中申诉用户所提供的信息，我们对 2019 年前 11 个月遭受勒索病毒攻击的受害人群做了分析。在地域分布方面并没有显著变化，依旧以数字经济发达地区和人口密集地区为主。而受感染的操作系统、所属行业则受今年流行的勒索病毒家族影响，与以往有较为明显的变化。勒索病毒反馈者性别依旧以男性为主。

## 一、 受害者所在地域分布

360 互联网安全中心监测显示，2019 年前 11 个月反馈中招者排名前十的地区中广东地区占比高达 24.6%。其次是浙江省占比 11.0%，北京占 10.9%。Top10 地区与以往数据区别并不大，依然是传统的勒索病毒高发区域。下图给出了被感染勒索病毒最多的前十个地区的占比情况。





2019 年前 11 个月受害者地区占比分布图如下。其中信息产业发达地区和人口密集地区是被攻击的主要对象。

### 2019年前11月勒索病毒感染地区分布

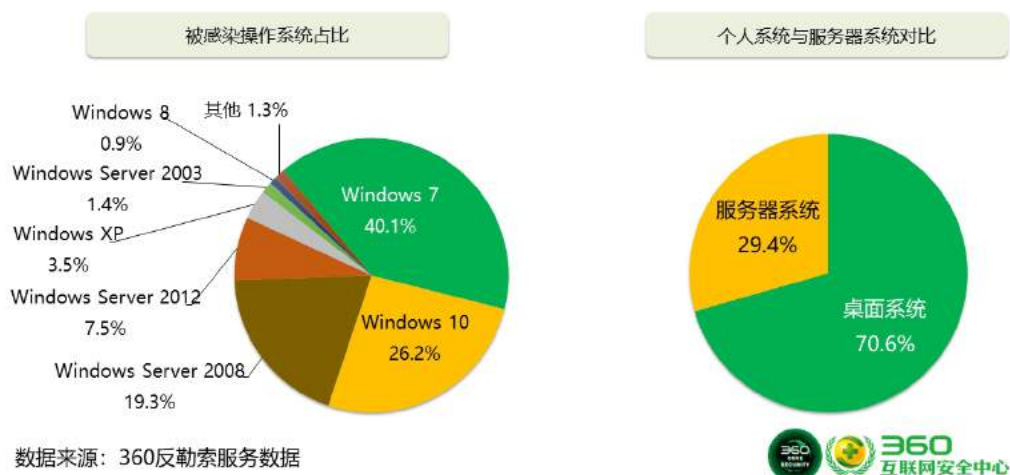


数据来源：360反勒索服务数据

## 二、 受攻击系统分布

基于反勒索服务数据统计，被勒索病毒感染的系统中 Windows 7 系统占比最高，占到总量的 40.1%。其主要原因是国内使用该系统的用户基数较大。而根据对系统类型进行统计发现，虽然个人用户的占比依然是绝对多数，但将前 11 个月的总体数据与 2019 年上半年数据相比，服务器感染勒索病毒的占比提升了超过 4 个百分点，更是比 2018 年度提升了 7% 左右的占比。由此可见，黑客对服务器系统的针对性是日渐提升的。

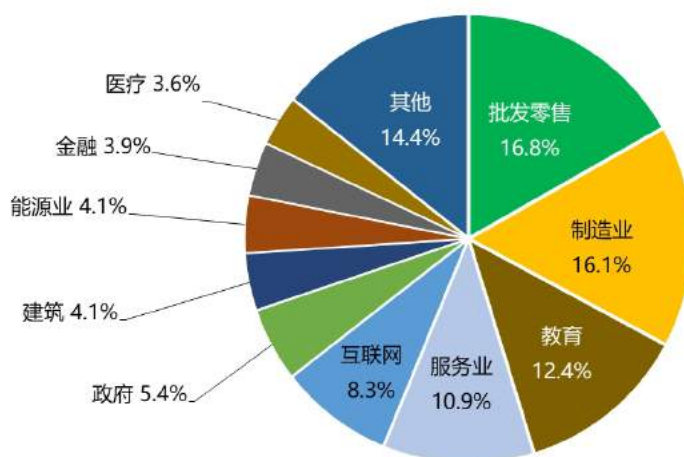
### 2019年前11月勒索病毒感染系统分布



### 三、 受害者所属行业分布

下图给出了受勒索病毒攻击的受害者所属行业分布情况。根据反馈数据的统计显示，2019 年前 11 个月最易受到勒索病毒攻击的行业前十分别为：批发零售、制造业、教育、服务业、互联网、政府机关、建筑、能源业、金融业、医疗。这一数据与上半年波动不大，全年所呈现的态势大体一致。

**2019年前11月最易受勒索病毒感染行业**

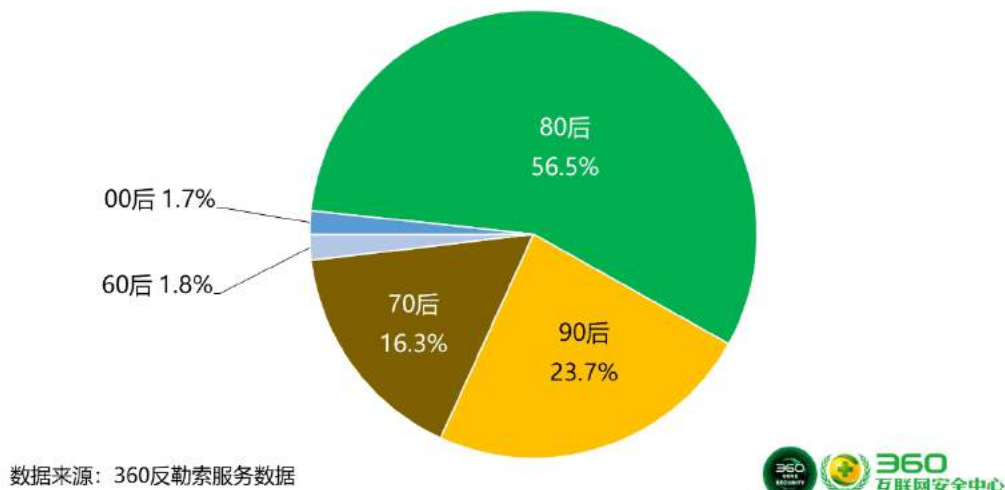


数据来源：360反勒索服务数据

#### 四、 受害者年龄层分布

下图给出了 360 反勒索服务的申诉者年龄层分布情况。其中 80 后站比高达 56.5%，超过半数，其次是 90 后。这主要是由于这两个年龄层用户是目前工作中使用计算机和系统运维人员的主要群体，其接触计算机的时间明显高于其他年龄层的用户，导致其受到勒索病毒攻击的概率也远高于其他年龄层用户。

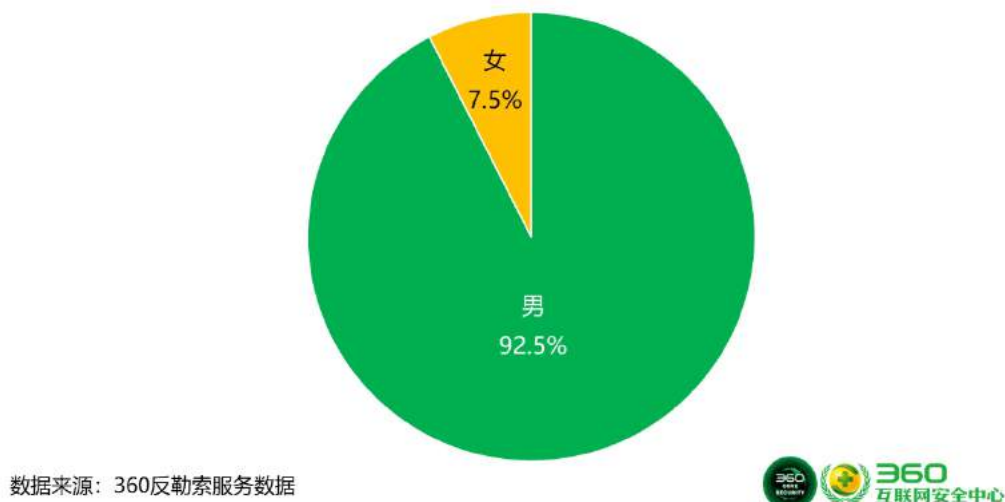
2019年前11月勒索病毒受害者年龄层分布



#### 五、 受害者性别分布

下图展示的是 360 反勒索服务平台申诉用户的性别分布情况。

2019年前11月勒索病毒受害者性别分布

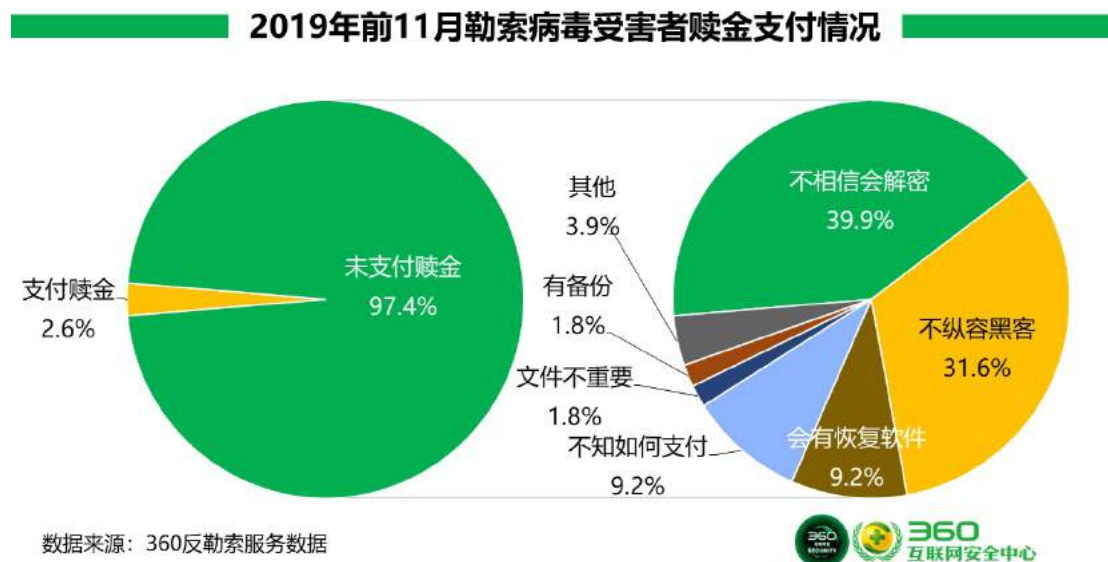


造成申诉者男女占比悬殊的原因主要有二点：其一、与计算机接触最为频繁的 IT 技术行业或 IT 运维类岗位的男性员工占比明显多于女性。其二、很多女性用户遇到病毒问题，

往往会优先选择寻求身边男性朋友的帮助。

## 六、 受害者赎金支付情况

下图为根据 360 反勒索服务申诉者的赎金支付情况做出的统计。



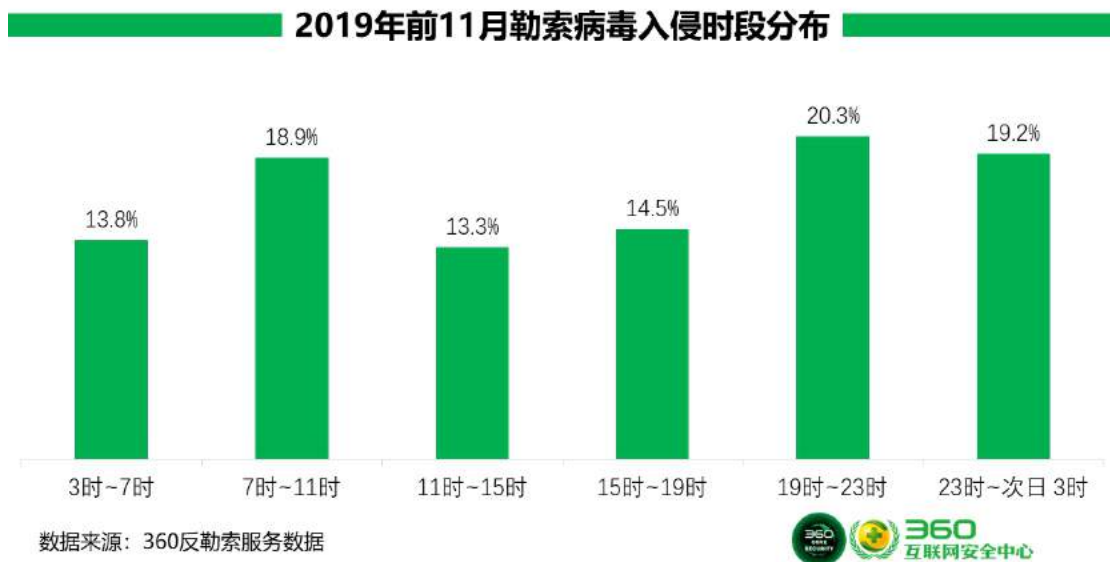
由图可见, 受害者中仅 2.6% 支付了赎金, 而 97.4% 的受害者并未支付赎金。而不选择支付赎金的理由, 则更多是对支付后黑客是否会信守承诺给予解密工具表示担忧。排在其次的, 则是由于不愿向黑客低头。

## 第三章 勒索病毒攻击者分析

2019 年的数据分析显示，勒索病毒整体上已经抛弃了 C&C 服务器的使用。取而代之的是内嵌密钥以及直接投毒的方式，在黑客的联系方式上，更多的使用了电子邮箱，而不再是之前单纯的洋葱网络上的聊天室。黑客将传播的主要手段转变为了对服务器的直接入侵，这其中远程桌面弱口令攻击是绝对的主力入侵方案。

### 一、 黑客登录受害计算机时间分布

下图给出了黑客成功攻陷计算机后的首次登录时间分布情况。针对被黑客攻击计算机（服务器系统居多）的相关数据进行分析发现分布并不平均，中午和下午时间段攻击量较低，攻击主要集中在 19 时至次日 3 时以及 7 时至 9 时两个时段。猜测这可能和攻击者与中国的时差有关。

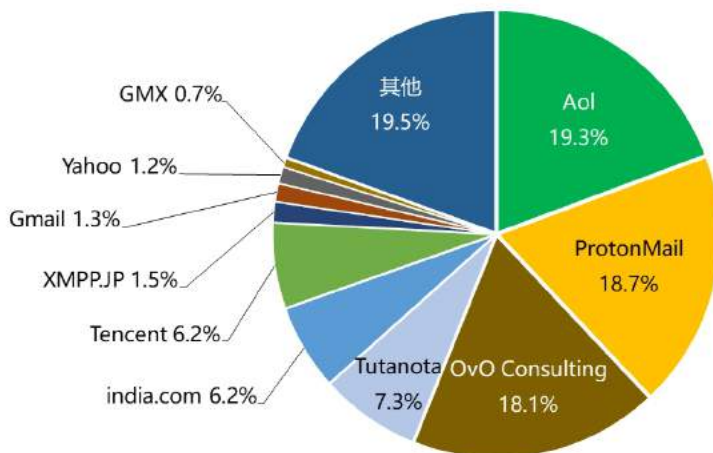


### 二、 勒索联系邮箱的供应商分布

虽然仍有一些勒索病毒在选择使用暗网等更加隐蔽的方式与受害者进行沟通，但越来越多的攻击者会在加密文件后留下邮箱地址，方便用户联系攻击者。

通过分析相关数据，我们发现勒索病毒作者更偏爱 Aol、ProtonMail、OvO Consulting 三家网站所提供的邮箱服务。我们推测这是病毒作者出于自身习惯、隐藏信息、注册便捷度等几方面综合考虑后导致的一个综合结果。其中 Aol 和 ProtonMail 是传统的流行免费邮箱，而 OvO Consulting 则更加注重匿名性——该邮箱供应商允许用户使用包括洋葱网络在内的各种暗网或代理服务注册邮箱，为病毒作者隐藏自身的目的提供了极大的便捷。

2019年前11月勒索邮箱供应商分布



数据来源：360反勒索服务数据



### 三、 攻击手段

#### （一） 弱口令攻击

口令暴力破解攻击依然是当前最为流行的攻击手段，使用过于简单的口令或者已经泄露的口令是造成设备被攻陷的最常见原因。计算机中涉及到口令爆破攻击的暴露面，主要包括远程桌面弱口令、SMB 弱口令、RPC 远程过程调用、数据库管理系统弱口令(例如 MySQL、SQL Server、Oracle 等)、Tomcat 弱口令、phpMyAdmin 弱口令、VNC 弱口令、FTP 弱口令等。因系统遭遇弱口令攻击而导致数据被加密的情况，也是所有被攻击情况的首位。而合理的安全设置，可以有效降低设备被弱口令攻击的风险。

弱口令攻击持续成为黑客热衷使用的手段，其原因有以下几点：

首先，虽然弱口令问题已经是一个老生常谈的安全问题了，但目前仍存在大量系统使用过于简单的口令或已经泄露的口令。究其原因，安全意识淡薄不在乎安全问题是一方面原因，还有一些是图省事、便于设备管理，而在多台设备中使用相同口令和简单口令，存在侥幸心理认为黑客不会攻击到自己的机器。另外还有一个重要原因是使用者不清楚自己的设备中存在弱口令问题。

其次，各种弱口令攻击工具比较完善，被公布在外的利用工具和教程众多，攻击难度低；

再次，各类软件与系统服务，本身对口令爆破攻击的防护能力较弱，市面上很多安全软件也不具备防护弱口令扫描攻击的能力，造成这类攻击横行。

而弱口令形成的原因，也不单单是因为使用了过于简单的口令。使用已经泄露的口令，也是一个重要原因。如部分软件系统，存在内置口令，这个口令早已被攻击者收集，另外多个服务和设备使用相同口令，也是造成口令泄露的一个常见因素。因此，有效的安全管理是防护弱口令攻击的重要手段。

通过对数据进行统计分析发现，远程桌面弱口令攻击已成为传播勒索病毒的最主要方式。根据 360 互联网安全中心对远程桌面弱口令爆破的监控，此类攻击的日均拦截量超过 220 万次。排名靠前的勒索病毒家族，如 GlobeImposter, GandCrab, Crysis 都在利用这一方法进行传播。



从我们日常处理勒索病毒攻击事件的总结来看，黑客常用的攻手法一般是：首先尝试攻击暴露于公网的服务器，在获得一台机器的权限后，会利用这台机器做中转，继续寻找内网内其他易受攻击的机器，在内网中进一步扩散。在掌握一定数量的设备之后，就会向这些设备植入挖矿木马和勒索病毒。有时，黑客还会利用这些被感染机器对其他公网机器发起攻击。因此，当用户感知到机器被攻击文件被加密时，通常是多台设备同时中招。

而在被弱口令攻击的设备中，也不局限于传统的 PC 设备，如今年 7 月份的 ech0Raix 勒索病毒：该勒索病毒主要攻击 NAS 服务器，通过我们对中招服务器日志分析发现，中招的设备上存在大量的远程桌面口令爆破记录和 SSH 口令爆破记录，并且在文件被加密前有通过远程桌面成功登录服务器记录。经进一步分析确认，该勒索病毒的传播是先通过爆破拿到远程桌面密码，登录到系统后再通过本地创建计划任务下载执行勒索病毒，实现加密用户本地文件。



优先级	日志	日期 & 时间	用户	事件
Information	系统	2019/07/19 08:38:13	admin	Scheduled Task [Synology scandisk] was removed.
Information	系统	2019/07/19 08:38:10	admin	Scheduled Task [Synology scandisk] was created.
Information	系统	2019/07/19 08:32:57	admin	Scheduled Task [Synology scandisk] was removed.
Information	系统	2019/07/19 08:32:53	admin	Scheduled Task [Synology scandisk] was created.



## （二）钓鱼邮件

“钓鱼邮件”攻击是最常见的一类攻击手段，在勒索病毒传播中也被大量采用。通过具有诱惑力的邮件标题、内容、附件名称等，诱骗用户打开木马站点或者带毒附件，从而攻击用户计算机。比如 Sodinokibi 勒索病毒，就大量使用钓鱼邮件进行传播。攻击者伪装成 DHL 向用户发送邮件，提示用户收货地址有误，需要用户查看邮件附件中的“文档”后进行联络。但实际该邮件中的“Download now”按钮跳转到勒索病毒下载地址。

日期：2019年9月25日周三 06:09  
主题：您包裹的运送问题



## （三）利用系统与软件漏洞攻击

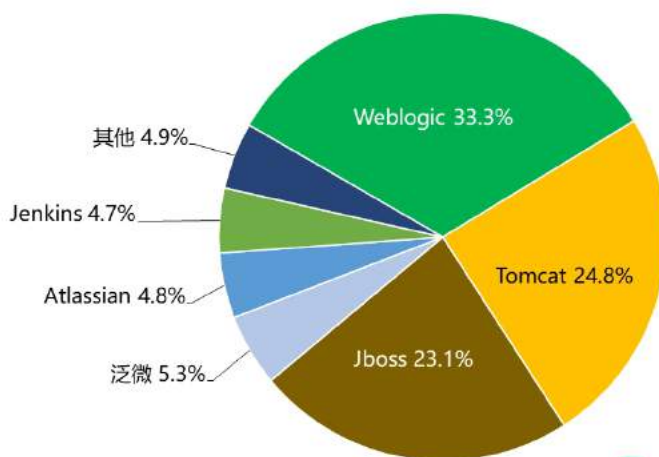
漏洞攻防一直是安全攻防的最前沿阵地，利用漏洞发起攻击也是最常见的安全问题之一。目前，黑客用来传播勒索病毒的系统漏洞、软件漏洞，大部分都是已被公开且厂商已经修补了的安全问题，但并非所有用户都会及时安装补丁或者升级软件，所以即使是被修复的漏洞（Nday 漏洞）仍深受黑客们的青睐。一旦有利用价值高的漏洞出现，都会很快被黑客加入到自己的攻击工具中。“永恒之蓝”工具就是其中的一个典型代表，其被用来传播 WannaCry 勒索病毒。

由于大部分服务器都会对外开放部分服务，这意味着一旦系统漏洞、第三方应用漏洞没有及时修补，攻击者就可能乘虚而入。比如年初的 alanwalker 勒索病毒，攻击 WebLogic、JBoss、Tomcat 等 Web 应用，之后通过 Web 应用入侵 Windows 服务器，下载执行勒索病毒。今年，常被用来实施攻击的漏洞包括（部分列举）：

Confluence RCE 漏洞 CVE-2019-3396
WebLogic 反序列化漏洞 CVE-2019-2725
Windows 内核提权漏洞 CVE-2018-8453
JBoss 反序列化漏洞 CVE-2017-12149
JBoss 默认配置漏洞 CVE-2010-0738
JBoss 默认配置漏洞 CVE-2015-7501
WebLogic 反序列化漏洞 CVE-2017-10271
“永恒之蓝”相关漏洞 CVE-2017-0146
Struts 远程代码执行漏洞 S2-052（仅扫描）CVE-2017-9805
WebLogic 任意文件上传漏洞 CVE-2018-2894
Spring Data Commons 远程代码执行漏洞 CVE-2018-1273
“双脉冲星”系列漏洞 CVE-2017-0143、CVE-2017-0145
泛微 OA E-cology 远程代码执行漏洞 CNVD-2019-32204
WinRAR 远程代码执行漏洞 CVE-2018-20250
windows 提权漏洞 CVE-2018-8120

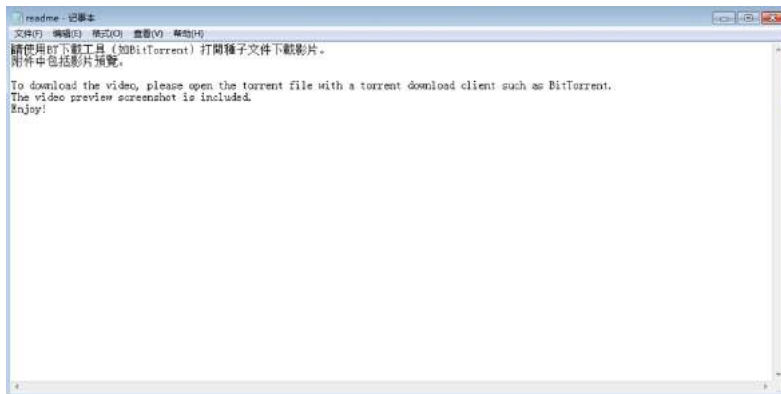
又如今年 4 月底，360 安全大脑就监控到有黑客在利用各类 Web 组件漏洞攻击用户服务器，并植入“锁蓝”勒索病毒。攻击者主要使用的是一个 4 月底被披露的 WebLogic 远程代码执行漏洞，因为许多用户还没来得及打补丁，“锁蓝”才会屡屡得手。

## 2019年前11月易受勒索病毒攻击Web应用分布



数据来源：360互联网安全中心查杀数据

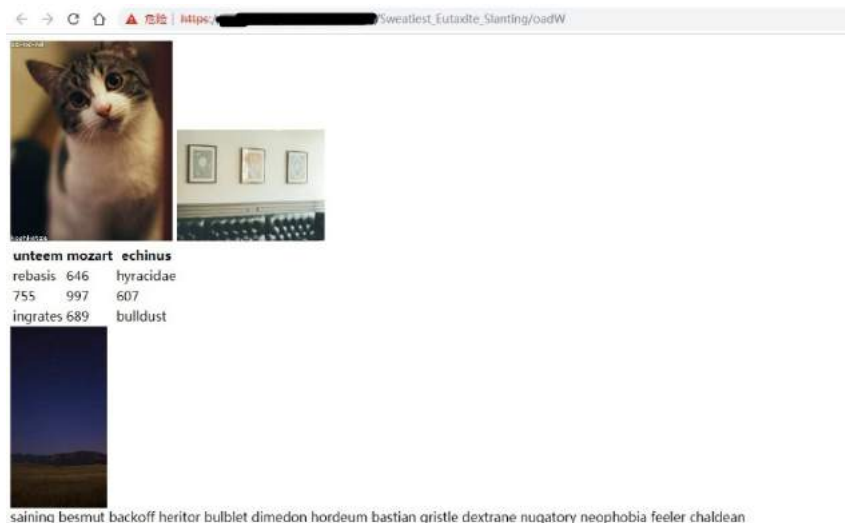
如今年 3 月底，360 安全大脑就监测到，有黑客通过虚假种子资源传播“CRYPTED!”勒索病毒。在攻击中，黑客利用公布不久的 WinRAR 远程代码执行漏洞 CVE-2018-20250 下发勒索病毒，并攻击了数百台国内的计算机。



#### （四） 网站挂马攻击

挂马攻击一直以来是黑客们热衷的一种攻击方式，常见的有通过攻击正常站点，插入恶意代码实施挂马，也有自己搭建恶意站点诱骗用户访问的。如果访问者的机器存在漏洞，那么在访问这些被挂马站点时，就极有可能感染木马病毒。如今年 3 月份再次活跃的 Paradise 勒索病毒，就是通过网站挂马的方式进行传播的。攻击者使用了在暗网上公开售卖的 Fallout Exploit Kit 漏洞利用工具进行攻击，该漏洞利用工具之前还被用来传播 GandCrab 和一些其它恶意软件。

在使用的漏洞方面，Windows 自身漏洞和 flash 漏洞是网页挂马中，最常被使用到的漏洞。比如 CVE-2018-4878 flash 漏洞和 CVE-2018-8174 Windows VBScript 引擎远程代码执行漏洞就被用来传播 GandCrab。下图展示的就是一个传播 GandCrab 的挂马网站。



#### （五） 破解软件与激活工具

破解软件与激活工具通常都涉及到知识产权侵权问题，一般是由个人开发者开发与发布，缺少有效的管理，其中鱼龙混杂，也是夹带木马病毒的重灾区。如国内流行的一些系统激活工具中，多次被发现携带有下载器，rootkit 木马，远控木马等。STOP 勒索病毒便是其中一


类，从去年年底开始活跃的 STOP 勒索病毒，通过捆绑在一些破解软件和激活工具中，当用户下载使用这些软件是，病毒便被激活，感染用户计算机，加密计算机中的文件。下图即为一款携带了勒索病毒的破解软件。

## Bandicut 3.1.5.511 Crack All Serial Key Full Torrent Free Download

By xproductkey | June 24, 2019 0 Comment

Download Crack + Setup

### Bandicut Video Cutter 3.1.5 Crack Latest Version Plus Key



**Bandicut 3.1.5.511 Crack** is super-fast video cutting/joining software with an easy-to-use interface. It allows users to trim parts of video quickly while keeping the original video quality. Users can also extract audio from video to MP3, join multiple video files, remove one or more parts from the video, or split the

## 第四章 勒索病毒发展趋势分析

2019 年，勒索病毒毫无疑问的再次领跑了最热门安全话题，成为政府、企业、个人最为关注的安全风险之一。随着勒索病毒的发展蔓延，整个行业也发生了一些变化，我们将从技术和产业两个方面进行分析。

### 一、勒索病毒攻防技术发展

#### （一）勒索病毒攻击形势变化

**攻防加剧，攻击针对性加强。**随着勒索病毒发展，其技术攻防也在进一步加剧。勒索病毒在制作传播上，也使用了更多样的漏洞，以往勒索病毒的漏洞利用往往集中在传播阶段，利用各式漏洞来加强其传播与感染能力，最典型的如 WannaCry 集成“永恒之蓝”漏洞利用工具，得以大范围传播。而今年勒索病毒开始在更多阶段利用漏洞发起攻击，如“锁蓝”勒索病毒就集成了 CVE-2018-8453 Windows 内核提权漏洞，使病毒能够运行在较高权限，威力进一步加强。对漏洞的利用也不局限于此，更多新披露漏洞会很快被用来发起攻击，每当有新漏洞被披露，就会有新一波攻击发起。还出现了利用供应链发起攻击的勒索病毒攻击事件。与过去“广撒网”无差别攻击形势相比，部分攻击团伙开始将目标锁定在一些具有较高支付价值的行业中，而攻击成功后的要价也动辄数百万元，在今年公开的新闻报道中，此类攻击已有数十次之多，要价最高的有上千万元，造成的损失更是以亿衡量。

**传播渠道更加丰富，攻击目标更加丰富。**今年，勒索病毒的传播渠道进一步得到扩展，传统的“灰黑”产传播渠道均见到了勒索病毒的身影，如以往携带常规病毒木马的重灾区“破解软件”中，今年就大量出现勒索病毒的身影，影响了很多普通用户的数据安全。在攻击的目标方面，勒索病毒制作团伙也在尝试更多样的攻击目标，以往主要出现在 Windows 平台的勒索病毒，目前在 Android, MacOS, Linux 上均有出现。而被打击的目标，也不再只局限于计算机，数据库、各种嵌入式设备、专用设备上也被曝出受到勒索病毒攻击影响。年中针对 NAS 平台的攻击，造成部分群辉(Synology)和威联通(QNAP)的用户数据被加密，而攻击者使用的勒索病毒程序，就是从一个 Linux 勒索病毒变种而来。

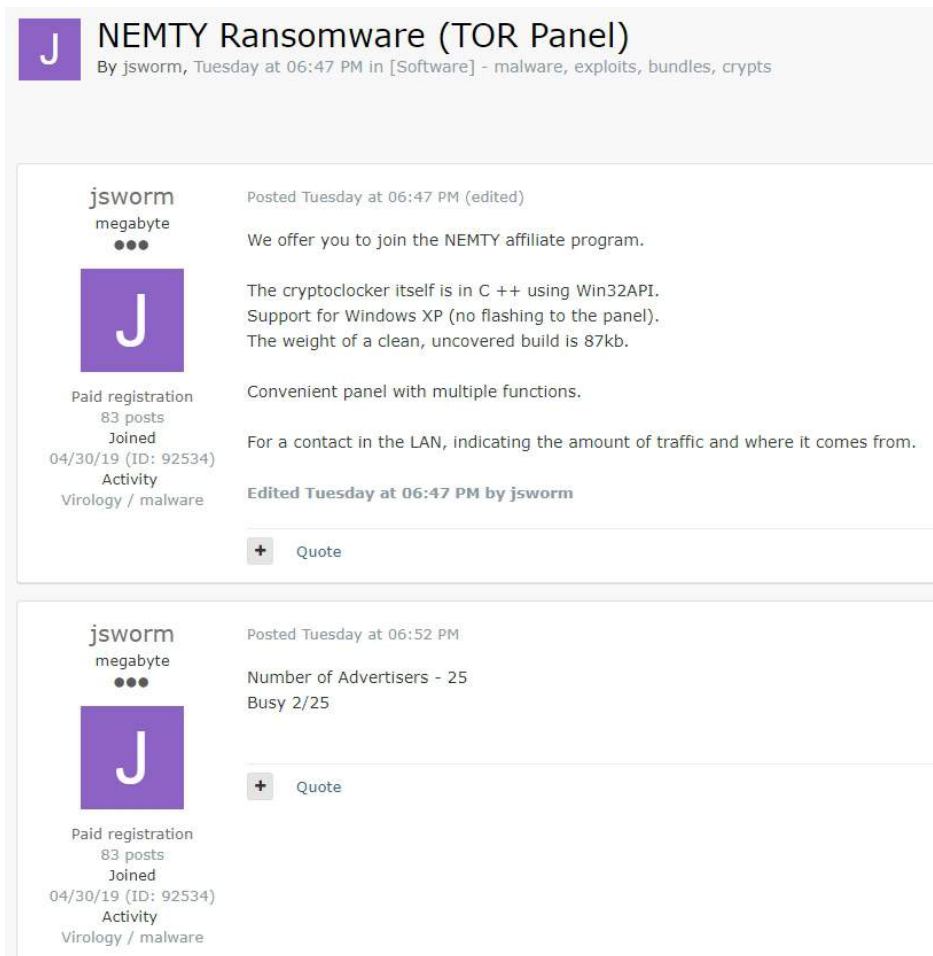
**勒索病毒正成为网络犯罪的一种新变现方式。**勒索病毒为传统病毒木马与网络攻击提供了一种新的快速变现方式，相比传统的变现方式，如抓“肉鸡”、建设僵尸网络、数据窃取倒卖、虚拟财产窃取、流量倒卖都需要一定规模，并根据设备数字资产情况来进行多环节的操作，勒索病毒的变现方式更为粗暴直接，正被越来越多的网络“灰黑”产采用。

**对现实生活的影响进一步加大，**回顾过去一年的新闻，勒索病毒攻击了多家美国市政网络，造成市政服务停摆，给民众造成不便，还迫使多个美国州政府支付赎金解决。而国内的情况也不容乐观，企业、医院、政府部门因勒索病毒原因停工、停产、业务无法正常办理的情况也有发生。勒索病毒不再只是一个安全行业的词汇，也更多的被普通大众所了解。

**勒索软件即服务（RaaS）被广泛使用，被用做破坏工具。**不论是 2019 年新增的勒索病毒，还是之前勒索病毒的变种，越来越多的勒索病毒作者开始尝试通过 RaaS 的方式来分发其病毒程序，而这一趋势不仅给勒索病毒制作者之间增加了一些竞争，也让黑产人员在勒索



病毒的获取更加方便，进一步加剧了勒索病毒的传播。



在一些针对地区基础设施的攻击中，也出现了勒索病毒的身影，这一现象的背后，很可能是针对特定地区的破坏行为，而不单单是商业上的勒索。勒索病毒在攻击中扮演了破坏工具的角色，同时还起到了转移视线的作用。

## (二) 勒索病毒防护技术发展

2019 年，勒索病毒的防御重点，已经由对病毒的识别、查杀、拦截，转为了对病毒传播渠道的封堵，对主机的安全加固和对被加密文件的解密探索上来。

依托多年来的技术积累，360 安全卫士在勒索病毒的识别、查杀、拦截方面均有良好表现，病毒作者通过免杀来绕过杀软的查杀和防御已经非常困难。目前勒索病毒在投递之前，通常会诱使用户退出安全软件或者攻击者主动关闭杀毒软件来避免病毒被查杀。因此在对抗勒索病毒攻击方面，对用户的安全科普是一方面，对病毒传播渠道的封锁拦截也是重要的一项内容。例如 STOP 勒索病毒会捆绑在一些激活工具中进行传播，在获取用户信任之后，依靠用户手动放行来实施攻击。杀毒软件如果能先于攻击者，在其传播渠道上进行拦截提示，能够取得更好的效果。

前 11 个月，针对服务器的攻击占整体勒索病毒攻击的 29.4% 以上，服务器由于无人值守，长期暴露于公网之上等原因，造成其被攻击的攻击面相对较大。而服务器被攻击的常见原因包括口令爆破攻击和系统或软件服务漏洞攻击，针对这一系列问题，360 安全卫士增加了“远程桌面爆破防护”、RPC 爆破防护、SMB 协议爆破防护、SQL Server 爆破防护、VNC 爆破防护、Tomcat 爆破防护等一系列防护，同时还增加了对金万维、瑞友的防护支持。在

漏洞保护方面，增加有 WebLogic、JBoss、Tomcat 等多种服务器常见软件的漏洞防护，以及大量系统漏洞的防护能力。如果无法保证服务器本身的安全，那么勒索病毒的防护能力也会大打折扣，因此针对服务器的安全加固也是勒索病毒防护的重要防护目标。

对被勒索病毒加密文件的破解，一直以来都是勒索病毒受害者最关注的问题，因此对勒索病毒进行破解也是安全公司能力体现的重要方面。目前流行的勒索病毒也并非都无法破解，常见的破解原理包括：

1. 利用泄露的私钥破解，通过各种渠道获取到病毒作者的私钥实现破解，如知名的 GandCrab 勒索病毒的私钥就被警方获取并公开，安全公司因此可以制作解密工具来进行解密。
2. 利用加密流程漏洞进行破解，有部分勒索病毒本身编写不规范，错误使用加密算法或随机数生成算法等，造成加密密钥或关键数据能够被计算获取，从而解密。
3. 名密文碰撞解密，这类解密常用于使用流式加密生成一个固定长度的密钥串，之后加密文件的勒索病毒。通过明密文对比计算从而得到使用的加密密钥，如 STOP 勒索病毒就是使用类似方法进行的破解。
4. 爆破解密，这类解密也是由于病毒作者对密钥处理的不规范，造成密钥空间不足，为爆破解密提供了可能。常见的如使用时间做种子产生随机数做密钥的情况。

### （三）勒索病毒处置服务更趋专业化

以往的勒索病毒处置，多属于被攻击公司和安全公司应急响应的一部分，由安全运维团队兼职处理。随着勒索病毒感染事件的常态化，在勒索病毒处置方面，也出现了更多的专职处置团队。市面上也开始出现专项代理处置勒索病毒解密业务的解密公司。安全公司的处置业务也由之前的查杀病毒，协助解密，逐步扩展为：帮助企业恢复生产，查清原因，以及后续的安全加固服务，服务更趋专业化。安全产品对勒索病毒的防护能力，也成为企业和个人选择安全软件的一个重要关注点。

## 二、勒索病毒相关产业发展

### （一）病毒制作传播与解密相关产业

勒索病毒经过多年发展，其制作传播链条也逐步分工细化，包括制作、销售、传播、支付、解密等多个环节组成，参与人员更多，团队数量也在增加。

勒索病毒在赎金索要方面，也出现分化。部分团伙不在局限于比特币，门罗币等“数字货币”，开始接受一些支付工具直接转账的请求。而另外一些团伙则开始要求用户使用匿名性更高的一些“数字货币”——如“达世币”进行支付。在赎金要求方面，也有分化趋势，部分勒索病毒的赎金要求降低到了 300 美元左右，而有一些则要求数十万美元不等。

在勒索病毒解密方面，目前网上有记录的国内解密公司就有将近 100 余家，提供代缴赎金，数据解密恢复，数据库恢复等业务，因为其解密方式多是通过像黑客支付赎金来完成，也存在一些被人诟病的问题。

### （二）针对勒索病毒相关的犯罪打击

各国政府对勒索病毒问题的重视程度也在加大，对勒索病毒的打击力度加强。如我国



内，主管单位也发起过“勒索病毒的专项治理工作”，以加强机关单位对勒索病毒的重视程度与防护能力。

近年来对勒索病毒犯罪的打击也取得了一些进展，如前不久 FBI、欧洲刑警组织、罗马尼亚警察局、DIICOT、NCA 等多家执法机构合作，拿到了 GandCrab 勒索病毒的私钥，帮助用户解密文件。

在国内，去年年底名噪一时的“扫码支付勒索病毒”，也很快被侦破，就在前不久作者被提起公诉，绳之以法。

在今年 6 月，国内一家知名“解密公司”控制人被武汉警方抓获，该公司联合黑客攻击国内多家公司的电脑，以解密为由索利，先后获利 700 余万元。

## 第五章 安全建议

面对严峻的勒索病毒威胁态势，我们分别为个人用户和企业用户给出有针对性的安全建议。希望能够帮助尽可能多的用户全方位的保护计算机安全，免受勒索病毒感染。

### 一、 针对个人用户的安全建议

对于普通用户，我们给出以下建议，以帮助用户免遭勒索病毒攻击。

#### (一) 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或关闭防护功能，对安全软件提示的各类风险行为不要轻易采取放行操作。
- 2) 可使用安全软件的漏洞修复功能，第一时间为操作系统和浏览器、Flash 等常用软件打好补丁，以免病毒利用漏洞入侵电脑。
- 3) 尽量使用安全浏览器，减少遭遇挂马攻击、钓鱼网站的风险。
- 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。
- 5) 电脑设置的口令要足够复杂，包括数字、大小写字母、符号且长度至少应该有 8 位，不使用弱口令，以防攻击者破解。

#### (二) 减少危险的上网操作

- 6) 不要浏览来路不明的色情、赌博等不良信息网站，此类网站经常被用于发起挂马、钓鱼攻击。
- 7) 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。也不要轻易打开扩展名为 js、vbs、wsf、bat、cmd、ps1 等脚本文件和 exe、scr、com 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，先使用安全软件进行检查后再打开。
- 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。

#### (三) 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，一旦电脑被勒索软件感染，可以通过 360 反勒索服务申请赔付和寻求帮助，以尽可能的减小自身损失。

### 二、 针对企业用户的安全建议

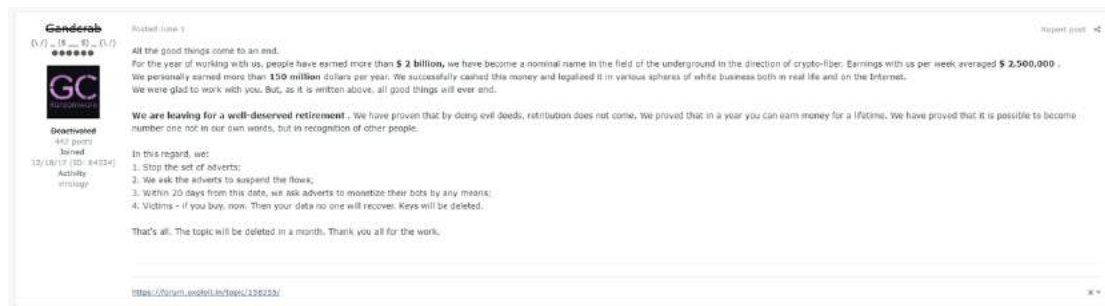
- 1) 及时给办公终端和服务端打补丁修复漏洞，包括操作系统以及第三方应用的补丁，尤其是对外提供服务的各种第三方应用，这些应用的安全更新容易被管理员忽视。

- 2) 如果没有使用的必要，应尽量关闭不必要的服务与对应端口，比如：135、139、445、3389 等，不对外提供服务的设备不要暴露于公网之上。对外提供服务的系统，应保持在较低权限。
- 3) 企业用户应采用具有足够复杂的登录口令，来登录办公系统或服务器，并定期更换口令。对于各类系统和软件中的默认账户，应该及时修改默认密码，同时清理不再使用的账户，多台设备使用不同口令。
- 4) 提高安全运维人员职业素养，除工作电脑需要定期进行木马病毒查杀外，远程办公使用到的其它计算机也应定期查杀木马病毒。

## 附录 1 2019 年勒索病毒大事件

### 一、 GandCrab 金盆洗手

GandCrab 勒索病毒最早出现于 2018 年 2 月，通过 RaaS 服务广泛传播。但在 2019 年 6 月 1 日，这款曾一度成为 2018 年传播量榜首的勒索病毒突然宣布不再更新。



据该声明自称，GandCrab 的制作团队已经通过该勒索病毒获得了超过 20 亿美元的巨额收益。值得庆幸的是，虽然该团队表示将销毁用于解密的密钥，但最终 FBI 公布了解密密钥，360 也在第一时间完成了解密大师工具的更新。目前，该病毒的受害者可以通过解密工具直接解密被其加密的文件。

### 二、 GlobeImposter 继续蔓延

继 2018 年初，国内一省级儿童医院感染 GlobeImposter 勒索病毒，不久 9 月山东十市不动产系统遭其入侵之后，2019 年 3 月 10 日，360 安全大脑监测发现 GlobeImposter 勒索病毒家族进一步蔓延，此次医疗行业中多家大型医院受到不同程度的感染。

GlobeImposter 是目前国内最流行的勒索病毒之一，根据 360 安全大脑的监测发现，GlobeImposter 最初的爆发轨迹可追溯到 2017 年。通过对比 2017 年至 2019 年的勒索病毒家族占比数据，就能明显看出 GlobeImposter 流行度的变化，在所有流行勒索病毒中的占比中，该家族由 2017 年的 3.2% 快速跃升至 2018 年的 24.8%，而 2019 年上半年更是进一步提升到了 26.6% 的占比，虽然下半年 Stop、phobos 和 Sodinokibi 三家勒索病毒的传播量大幅度上涨导致最终 GlobeImposter 在 2019 年前 11 个月的总占比数下降至 19.8%，但已经是坐稳了年度传播量最大勒索病毒的宝座。

### 三、 美国城市遭勒索病毒攻击，政府已交赎金

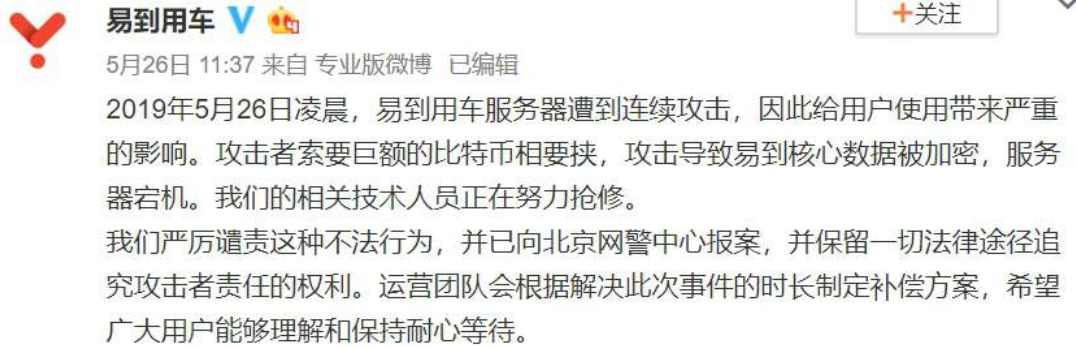
2019 年 5 月底，美国佛罗里达州里维埃拉政府部门遭到勒索病毒攻击导致市政服务瘫痪，初步估计造成损失在 1800 万美元以上。当地政府已向黑客支付 65 比特币的赎金，按当时汇率核算，折合美元约 60 万美元。

据报道，此次事件是由于一名警局雇员打开了一封病毒邮件引起的。最终病毒感染了整个市政网络并传播勒索病毒，导致除 911 相关服务外，几乎所有市政服务设施全面瘫痪。除准备向黑客支付的赎金外，当地政府还计划花费 94 万美元用于购买的新的设备以重建其

IT 基础设施。

#### 四、 易到用车遭勒索病毒攻击

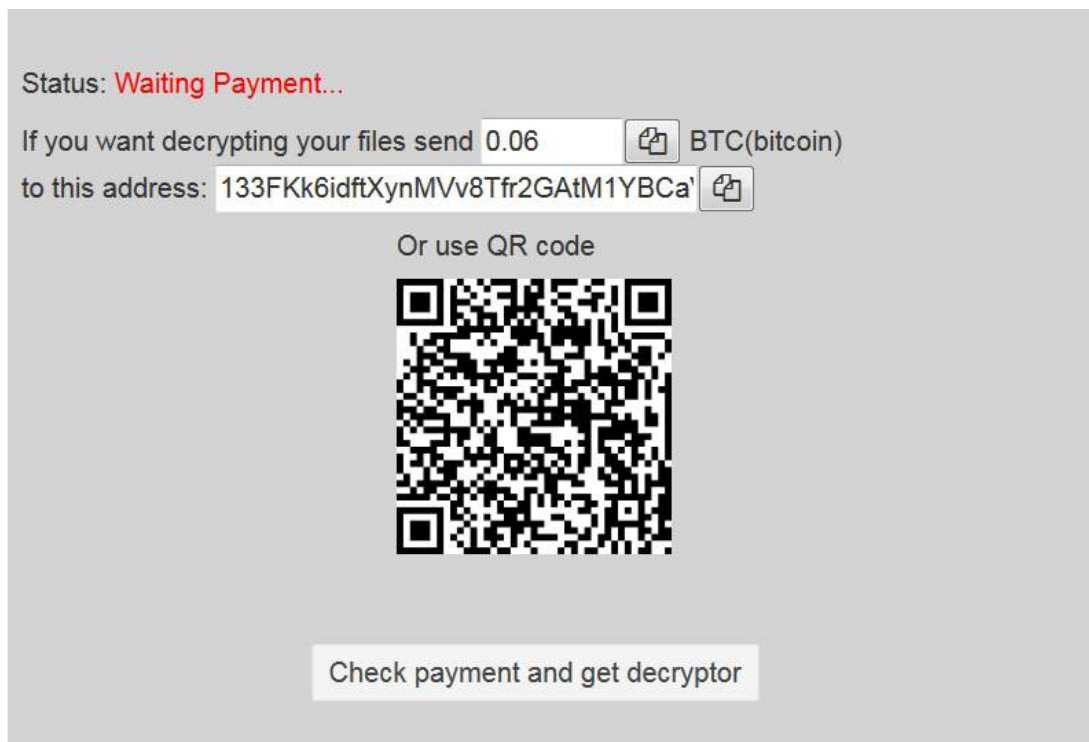
2019 年 5 月 26 日，知名公司“易到用车”服务器遭到勒索病毒攻击。致使其 APP 完全瘫痪。



据易到用车官方微博称，此次攻击导致其核心数据被加密且服务器宕机。攻击者向易到索要巨额比特币作为要挟。

#### 五、 勒索病毒瞄准 NAS 服务器

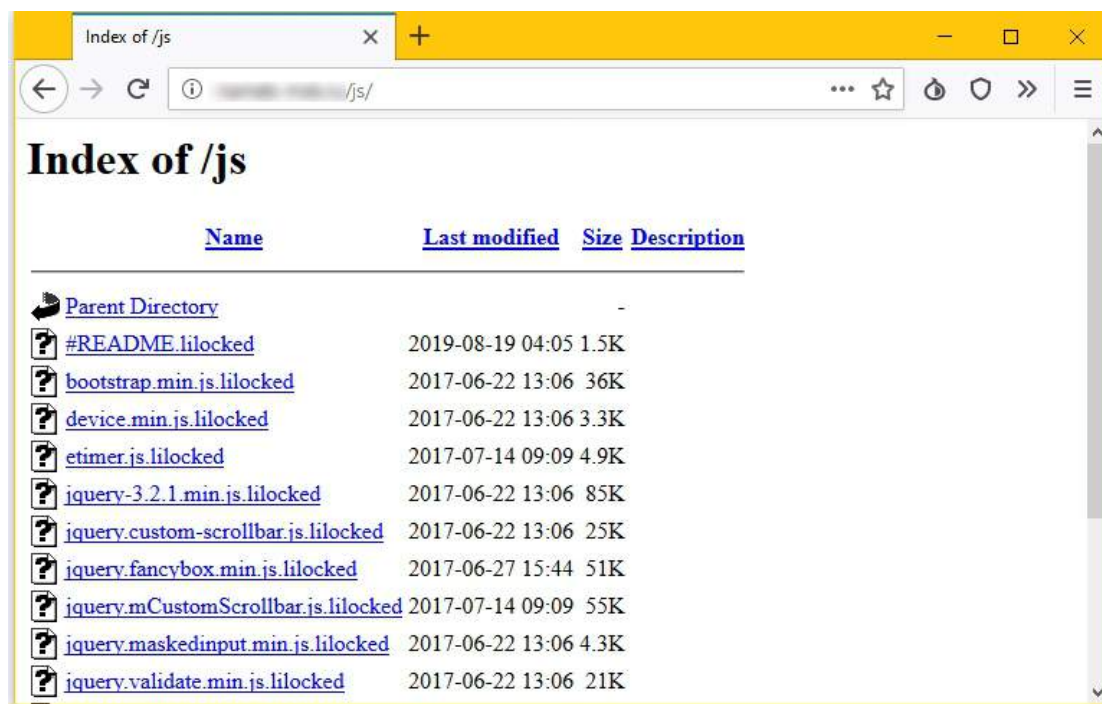
2019 年 7 月，国内主流的 NAS 服务设备群晖(Synology)和威联通(QNAP)受到勒索病毒攻击。勒索病毒将文件扩展名修改为.encrypt，并向受害用户索要 0.06 个比特币（当时约合人民币 4300 元）作为解密文件的赎金。



经分析，发现该勒索病毒主要通过弱口令爆破的方法对 NAS 服务器进行入侵。虽然从勒索金额总量上来讲，此次事件导致的直接经济损失并不巨大，但这意味着勒索病毒作者已在积极的寻找勒索病毒的传统攻击目标意外的新平台和新系统。

## 六、 六千余台服务器感染 Lilocked

2019 年 7 月至 9 月期间，约有 6700 余台服务器受到了来自 Lilocked 勒索病毒的攻击。分析人员猜测，该勒索病毒瞄准了服务器中运行的一款名为 Exim 的电子邮件服务软件，也正因如此，勒索病毒并未获取到服务器的管理员权限，而仅加密了一些 Web 服务相关的文件。

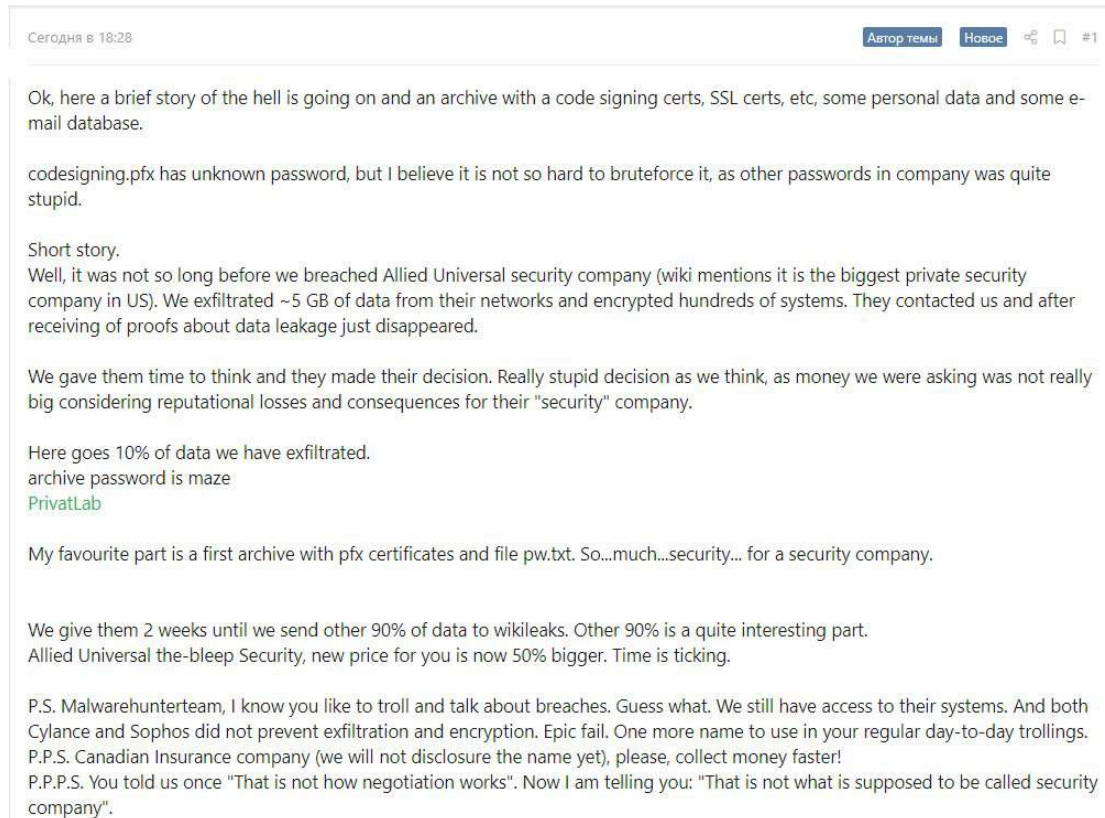


该病毒向受害者勒索 0.03 比特币（在当时约合人民币 2300 元）的赎金。



## 七、 要么缴纳赎金要么泄露数据

2019 年 11 月，由于在规定时间内未收到 Allied Universal 公司交付的赎金，勒索病毒 Maze 的作者对外发布了近 700MB 的机密数据。并宣称发布的数据不到他们窃取到的数据总量的 10%，并要求受害公司尽快交付赎金，否则会进一步公布其余的数据。



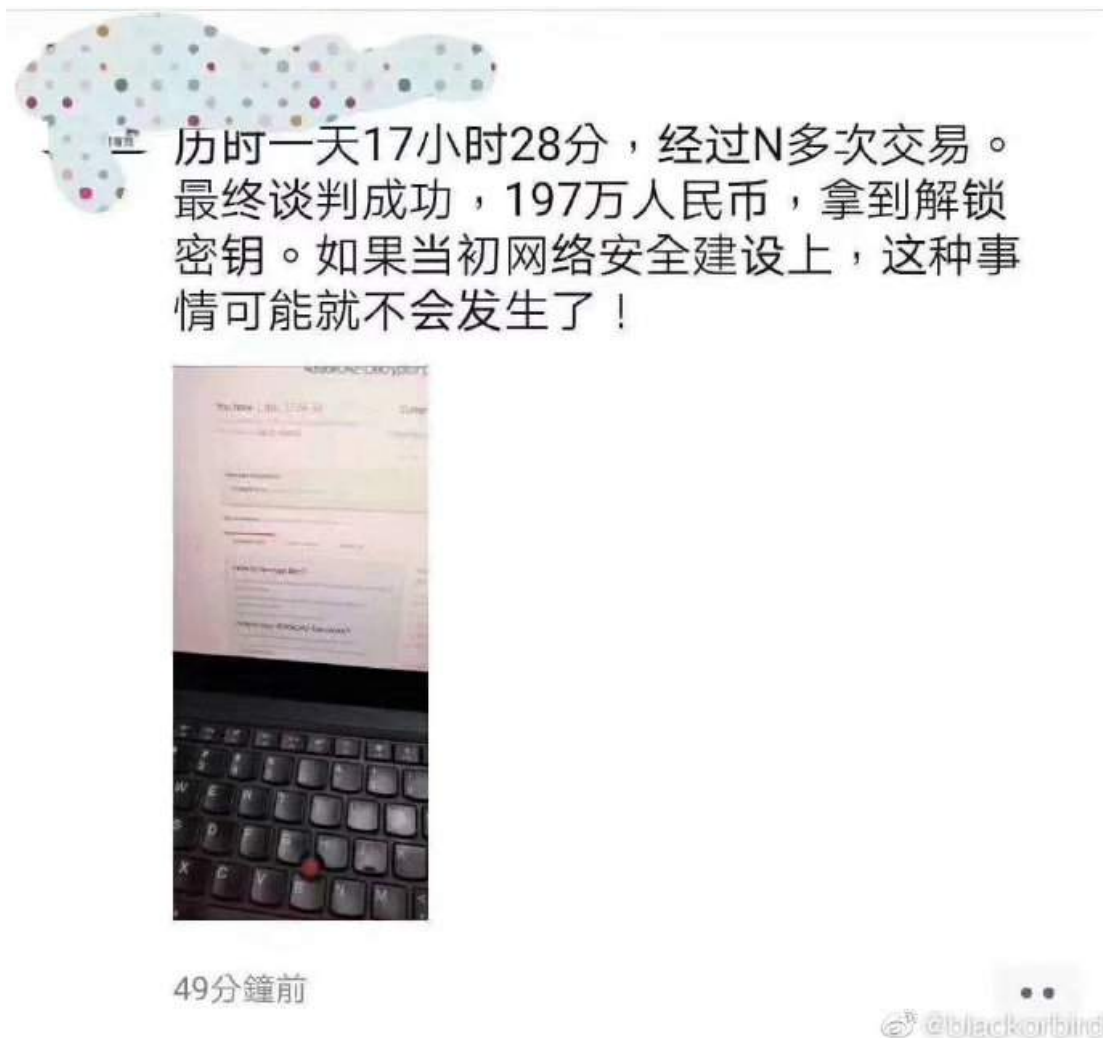
在公布了数据之后，黑客将勒索金额从此前的 300 比特币（当时约合 230 万美元）提高到了 450 比特币（当时约合 380 万美元）。而受害公司则表示最多支付 5 万美元的赎金。双方还在进一步的沟通谈判。

这一事件也意味着单纯通过加密文件对受害人实施敲诈勒索已经不能再满足黑客的胃口了，他们正在尝试新的勒索方法。



## 八、 197 万元勒索赎金坑苦受害公司

2019 年 12 月，一条微博引起广泛关注：一家公司遭受勒索病毒攻击，在经过了数日多轮的谈判后，最终以 197 万人民币的价格购得解密密钥。发布者自己也表示对未能在对网络安全建设给予更多的重视而感到后悔。



## 附录 2 360 安全卫士反勒索防护能力

### 一、 弱口令防护能力

2017 年至今，针对服务器进行攻击的勒索病毒一直是勒索病毒攻击的一个重要方向，其中弱口令爆破被许多勒索病毒家族传播者所青睐。针对这一问题，360 安全卫士推出了系统安全防护功能，完善了“口令爆破”防护能力。

- 2017 年-2018 年：新增对远程桌面弱口令防护支持。
- 2018 年-2019 年：新增 SQL Server 爆破、VNC 爆破、Tomcat 爆破的防护支持。
- 2019 年：新增 RPC 协议弱口令爆破防护、SMB 协议爆破拦截优化版正式上线、新增对金万维、瑞友管理软件的支持。

同时，对 MYSQL、SQL Server、Tomcat 等服务器常用软件也加入了多方位的拦截防护。

安全操作中心

防护记录

下载记录

拦截记录

上报记录

优化记录

权限记录

可恢复区

已阻止区

已信任区

补丁管理

拦截时间

2019-07-11 18:24:59

2019-07-04 14:09:31

2019-07-04 09:40:11

2019-07-04 09:40:01

2019-07-03 16:37:23

2019-07-03 16:36:42

2019-07-03 16:36:29

详情描述

拦截说明

[已拦截] RPC登录密码暴力破解

[已拦截] 远程桌面弱口令攻击

[启动] 卫士启动

[退出] 卫士退出

[已拦截] 远程桌面弱口令攻击

[启动] 卫士启动

[退出] 卫士退出

次数

防护 1 次

防护 1 次

防护 2 次

☐

显示全部

清空所有日志

复制选中的日志

复制全部日志

刷新

360 安全卫士拦截 RPC 登录密码暴力破解

### 二、 漏洞防护能力

新增漏洞拦截能力（部分列举）：

- 新增对 Outlook 远程代码执行漏洞拦截(CVE-2017-11774，它允许攻击者逃离 Outlook 沙箱并在底层操作系统上运行恶意代码)。
- 新增对致远 OA 系统远程任意文件上传漏洞拦截支持(该漏洞会造成攻击者恶意上

传恶意代码到用户系统)。

- 新增对破坏力堪比“永恒之蓝”的高危远程桌面漏洞(CVE-2019-0708)的拦截支持。
- 新增对 Windows 10 下多个本地提权的 0day 漏洞拦截支持。
- 新增对 IE11 处理 MHT 文件方式时可绕过 IE10 浏览器保护漏洞拦截支持。(该漏洞能在用户不知情的情况下，被黑客用来发起钓鱼网络攻击，窃取本地文件)。
- 新增对 WinRAR 远程代码执行漏洞拦截支持(CVE-2018-20250, unacev2.dll 任意代码执行漏洞)。
- 新增对泛微 OA E-cology 远程代码执行漏洞拦截支持(该漏洞能在用户系统中执行任意恶意代码)
- 新增对 PHPStudy 后门拦截与修复(该后门能使攻击者在用户系统中执行任意恶意代码)



360 安全卫士拦截漏洞攻击

### 三、 挂马网站防护能力

针对勒索病毒的防护，更高效可靠的防护时间点应该是其攻击传播阶段。2019 年 GandCrab、Paradise 两个家族都利用到了网站挂马来传播勒索病毒，针对这一情况，360 安全大脑能第一时间监控并识别该网站的恶意行为并做出拦截。



360 安全卫士对挂马网站进行拦截

### 四、 钓鱼邮件附件防护

钓鱼邮件一直以来都是勒索病毒传播的重要渠道，2019 年有更多团伙开始使用钓鱼邮件来传播其代理的勒索病毒。冒充国际快递，国际警方等诱惑用户下载运行邮件附件的案例数不胜数。针对这一情况，360 安全大脑精准识别邮件附件中潜藏的病毒木马，替用户快速检测附件中是否存在问题。



360 安全卫士对藏有病毒的邮件附件进行拦截

## 附录 3 360 解密大师

360 解密大师是 360 安全卫士提供的勒索病毒解密工具，是目前全球范围内支持解密类型最多的一款解密工具。

2019 年前 11 个月 360 解密大师共计更新版本 42 次，累计支持解密勒索病毒超过 320 种，前 11 个月服务用户超 26000 台次，解密文件近 8500 万次，挽回损失超 5.47 亿元（按照单笔赎金 3000 美元估算）。

下图给出了 360 解密大师在 2019 年前 11 个月，成功解密被勒索病毒感染的文件和机器数量的 Top10。其中，GandCrab 由于本身感染基数大且全部版本均已有可靠的解密方案，所以占比最多。



## 附录 4 360 勒索病毒搜索引擎

该数据来源 lesuobingdu.360.cn 的使用统计。（由于 WannaCry、AllCry、TeslaCrypt、Satan 以及 kraken 几个家族在过去曾出现过大规模爆发，之前的搜索量较高，长期停留在推荐栏里，对结果有一定影响，故在统计中去除了这几个家族的数据。）



通过对 2019 年前 11 个月勒索病毒搜索引擎热词进行分析发现，除了由于用户各种原因滞留的热词外，搜索量排前十的关键词情况如下：

- GandCrab: “GandCrab”成为关键词主要由于黑客留下的文档中都会包含该“GandCrab”关键词以及版本号。该勒索病毒的传播渠道众多，导致该勒索病毒的受害者在 2019 年上半年占比也是最高的，该勒索病毒传播者在 2019 年 6 月 1 日宣布正式停播。
- Help989: “help989”成为关键词主要由于被加密文件后缀会被统一修改为“help989”，该关键词属于 GlobeImposter 勒索病毒家族。该勒索病毒家族，后缀更新非常频繁，从 2017 年开始传播至今，其后缀上百种。“help989”后缀为 GlobeImposter 家族在 2019 年感染用户最多的变种之一。该勒索病毒家族目前主要通过爆破远程桌面口令，手动投毒。其主要受害者为企业用户。
- Wecanhelp: “wecanhelp”成为关键词主要由于被加密文件后缀会被统一修改为“wecanhelp”，该关键词属于 Nemesis 勒索病毒家族。该勒索病毒最早在 2017 年 2 月份出现，早期的 Nemesis 勒索病毒被称作为 CryptON 勒索病毒/X3m 勒索病毒，同时早期该勒索病毒存在算法漏洞，能通过碰撞解密出文件。所以该团队在复出时正式更名为 Nemesis 勒索病毒。
- Actin: “Actin”成为关键词主要由于被加密文件后缀，会被统一修改为“ACTIN”，该关键词属于 phobos 勒索病毒家族。该勒索病毒是 2019 年新增的一个勒索病毒家族，该家族从传播渠道到勒索提示信息，全部都在刻意模仿 Crysis 勒索病毒家族。
- Supportthehelpgood:同“help989”。
- Adage:同“actin”。
- ETH: “ETH”成为关键词，主要由于被加密文件后缀会被统一修改为“ETH”，该关键词



词属于 Crysis 勒索病毒家族。该勒索病毒是当前传播史最长的一个家族，该勒索病毒家族从 2016 年开始传播至今，通常是由爆破远程桌面口令后手动投毒传播。

- Scaletto: 同 “help989”
- Adobe: 同 “ETH”。
- Harma: 同 “ETH”

