2017

勒索软件威胁形势分析报告

360 互联网安全中心

2017 年 12 月 20 日

摘　要

- 2017 年 1-11 月，360 互联网安全中心共截获电脑端新增勒索软件变种 183 种，新增控制域名 238 个。全国至少有 472.5 多万台用户电脑遭到了勒索软件攻击，平均每天约有 1.4 万台国内电脑遭到勒索软件攻击。
- 在向 360 互联网安全中心求助的勒索软件受害者中，Cerber、Crysis、WannaCry 这三大勒索软件家族的受害者最多，共占到总量的 58.4%。其中，Cerber 占比为 21.0%，Crysis 占比为 19.9%，WannaCry 占比为 17.5%。
- 2017 年，勒索软件的传播方式主要有以下五种：服务器入侵传播、利用漏洞自动传播、邮件附件传播、通过软件供应链进行传播和利用挂马网页传播。
- 遭遇勒索软件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 14.9%，其次是浙江 8.2%，江苏 7.7%。排名前十省份占国内所有被攻击总量的 64.1%。
- 抽样调研显示，在遭到勒索软件攻击的政企机构中，能源行业是遭受勒索软件攻击最多的行业，占比为 42.1%，其次是医疗行业为 22.8%，金融行业为 17.8%。
- 2017 年，勒索软件的攻击主要呈现以下特点：无 C2 服务器加密技术流行、攻击目标转向政企机构、攻击目的开始多样化、勒索软件平台化运营、境外攻击者多于境内攻击者。
- 2017 年，约 15%的勒索软件攻击是针对中小企业服务器发起的定向攻击，尤以 Crysis、xtbl、wallet、arena、Cobra 等家族为代表。
- 2017 年 1 月至 11 月，360 反勒索服务共接到了 2325 位遭遇勒索软件攻击的受害者求助。调研数据显示，男性是最容易受到勒索软件攻击的对象，占比高达 90.5%，而女性占比仅为 9.5%。
- 在向 360 互联网安全中心求助的所有勒索软件受害者中，IT/互联网行业的受害者最多，占比为 27.0%；其次是制造业，占比为 18.6%；教育行业占比为 14.8%。
- 从求助的受害者工作职位来看，普通职员超过受害者总数的一半以上，占 51.8%，其次是经理、高级经理，占 33.0%，企业中、中高管理层，占 13.4%，CEO、董事长、总裁等占比为 1.8%。
- 从求助的受害者文件感染类型可以看出，87.6%是受害者电脑上的办公文档被感染，其次，77.4%的图片文件被感染，54.0%的视频文件被感染，48.7%的音频文件被感染，8.2%的数据库文件被感染。
- 在求助的受害者中，已有 5.8%的受害者为了恢复文件而支付赎金，另外 94.2%的受害者选择了拒绝为恢复文件而支付赎金。
- 2017 年 5 月，影响全球的勒索软件永恒之蓝勒索蠕虫（WannaCry）大规模爆发。它利用了据称是窃取自美国国家安全局的黑客工具 EternalBlue（永恒之蓝）实现了全球范围内的快速传播，在短时间内造成了巨大损失。
- 不同行业遭受永恒之蓝勒索蠕虫攻击的情况也有所不同，工程建设行业是遭受攻击最多的行业，占比为 20.5%，其次制造业为 17.3%，能源行业为 15.3%。

- 本次报告还总结了勒索软件攻击与应急响应的十大典型案例，其中五个为永恒之蓝攻击与响应典型案例，另五个为服务器入侵攻击与响应典型案例。
- 2018 年勒索软件攻击趋势预测：从整体态势来看，勒索软件的质量和数量将不断攀升，并且会越来越多的使用免杀技术；从攻击特点来看，勒索软件的自我传播能力将越来越强，静默期也会不断延长；从攻击目标来看，勒索软件攻击的操作系统类型将越来越多，同时定向攻击能力也将更加突出；此外，勒索软件造成的经济损失会越来越大，受害者支付赎金的数量也会越来越多，但由于各种原因，通过支付赎金恢复文件的成功率将大幅下降。
- 在反勒索软件方面，以下技术最有可能成为主流趋势：文档自动备份隔离保护技术、智能诱捕技术、行为追踪技术、智能文件格式分析技术和数据流分析技术等。对于企业级用户来说，云端免疫技术、密码保护技术等也将起到至关重要的作用。

目　　录

研究背景

勒索软件是近两年来影响最大，也最受关注的网络安全威胁形式之一。攻击者通过电子邮件、网络渗透、蠕虫病毒等多种形式，向受害者的电脑终端或服务器发起攻击，加密系统文件并勒索赎金。

2016 年，包括 IBM、Symantec、360 等国内外多家知名安全机构已经开始高度关注勒索软件攻击。2016 年 12 月，360 互联网安全中心发布了《2016 敲诈者病毒威胁形势分析报告（年报）》。报告指出，2016 年，全国至少有 497 万多台用户电脑遭到了勒索软件攻击，成为对网民直接威胁最大的一类木马病毒。

2017 年，勒索软件继续呈现出全球性蔓延态势，攻击手法和病毒变种也进一步多样化。特别是 2017 年 5 月全球爆发的永恒之蓝勒索蠕虫（WannaCry，也有译作“想哭”病毒）和随后在乌克兰等地流行的类 Petya 病毒，使人们对于勒索软件的关注达到了空前的高度。在全球范围内，政府、教育、医院、能源、通信、制造业等众多关键信息基础设施领域都遭受到了前所未有的重大损失。

与 WannaCry 无差别的显性攻击相比，针对中小企业网络服务器的精准攻击则是隐性的，不为多数公众所知，但却也已成为 2017 年勒索软件攻击的另一个重要特点。统计显示，在 2017 年的国内勒索软件的攻击目标中，至少有 15%是明确针对政企机构的，其中由以中小企业为主要目标。相比于一般的个人电脑终端或办公终端，服务器数据的珍贵程度和不可恢复性更强（针对服务器的渗透式勒索攻击一般不会留下死角或备份），因此被勒索者支付赎金的意愿也相对更强。

为进一步深入研究勒索软件的攻击特点和技术手段，帮助个人电脑用户和广大政企机构做好网络安全防范措施，360 互联网安全中心对 2017 年的勒索软件攻击形势展开了全面的研究，分别从攻击规模、攻击特点、受害者特征、典型案例、趋势预测等几个方面进行深入分析。

第一章　勒索软件的大规模攻击

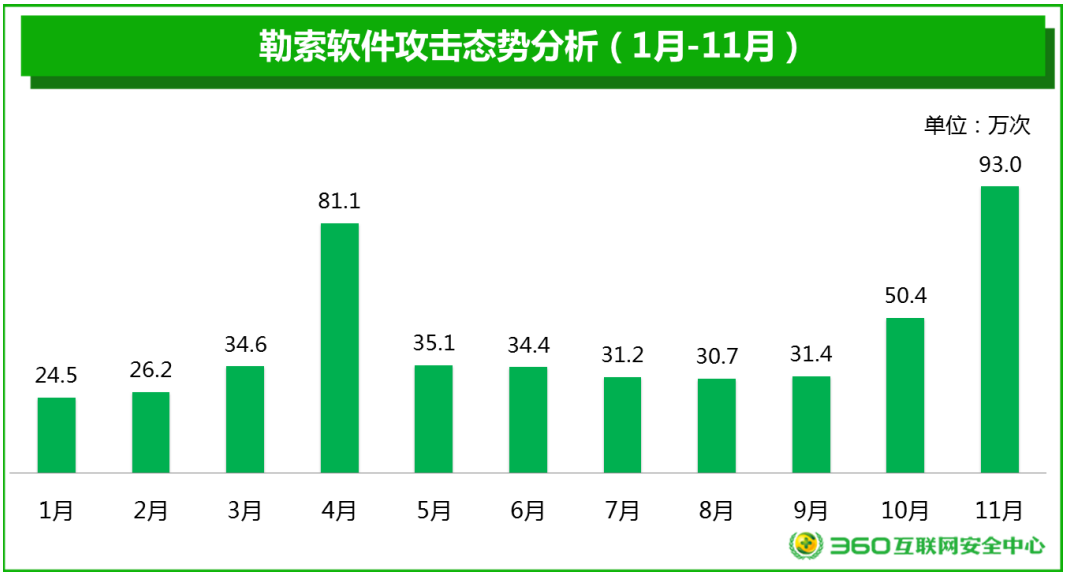
2017 年以来，360 互联网安全中心监测到大量针对普通网民和政企机构的勒索软件攻击。勒索软件已成为对网民直接威胁最大的一类木马病毒。本章内容主要针对，2017 年 1 月-11 月期间，360 互联网安全中心监测到的勒索软件的相关数据进行分析。

一、　勒索软件的攻击量

2017 年 1-11 月，360 互联网安全中心共截获电脑端新增勒索软件变种 183 种，新增控制域名 238 个。全国至少有 472.5 多万台用户电脑遭到了勒索软件攻击，平均每天约有 1.4 万台国内电脑遭到勒索软件攻击。

特别说明，2017 年截获的某些勒索病毒，如 Cerber 病毒，会向某个 IP 地址段进行群呼，以寻找可能响应的控制服务器。病毒这样做的目的可能是为了避免其服务器被拦截。如果没有服务器响应群呼消息，病毒则会按照其他既定流程执行代码。2017 年，360 互联网安全中心共截获新增此类 IP 地址段 51 个。

下图给出了勒索软件 1 月至 11 月期间每月攻击用户数的情况。从图中可见，4 月攻击高峰期时的攻击量为 81.1 万，一天之内被攻击的电脑平均可达 2.7 万台。11 月是第二个攻击小高峰，一天之内被攻击的电脑平均可达 3.1 万台。下图分别给出了 2017 年 1 月至 11 月勒索软件每月攻击的态势分析图形。注意，此部分攻击态势分析数据不包含 WannaCry 勒索蠕虫的相关数据。



2017 年四月份发生的大规模勒索软件攻击，主要是因为 Shadow Brokers（影子经纪人）组织公开了披露美国国家安全局发现的漏洞“永恒之蓝”，虽然“WannaCry”是在五月份爆发的，但此漏洞一直都有被别的勒索软件利用进行攻击。

10 月至 11 月发生的大规模勒索软件攻击，主要是因为在 10 月份时出现了一种以.arena 为后缀的勒索软件，11 月份时出现了一种以.java 为后缀的勒索软件。这两款勒索软件主要是由攻击者通过娴熟的手法入侵服务器后释放勒索病毒的。以.arena 和.java 为后缀的勒索软

件在 10 月至 11 月流行的主要原因有三：

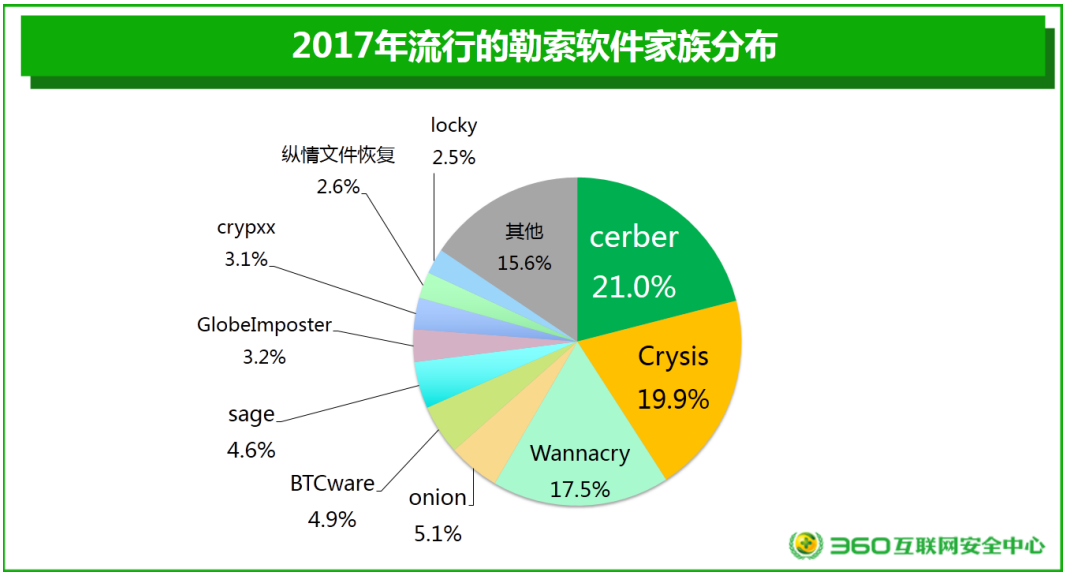
1） 攻击者入侵手段升级导致成功率大幅提高；

2） 这两款勒索软件成功入侵了大量企业的服务器；

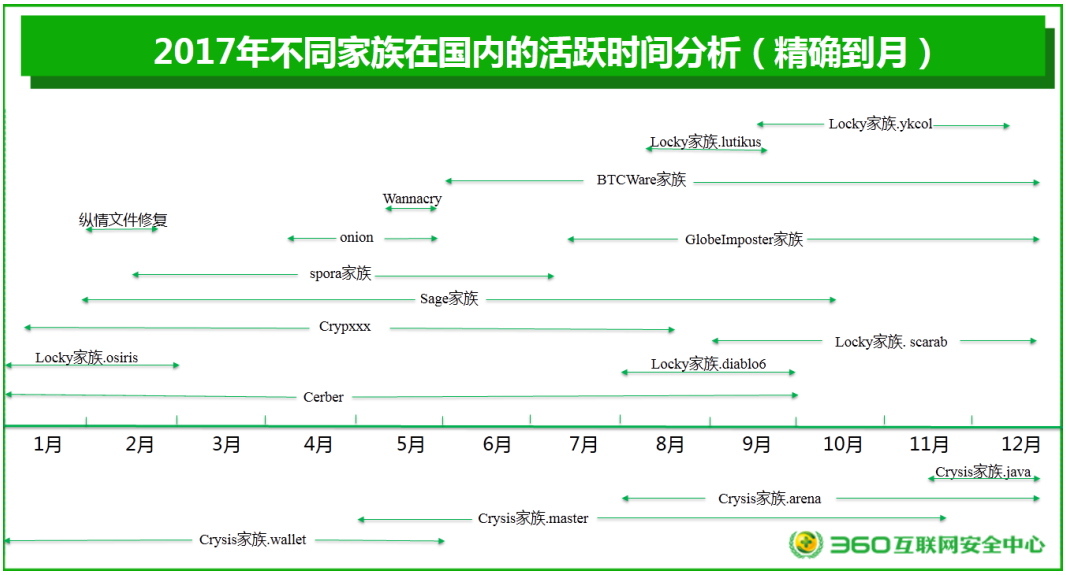
3） 以.arena 和.java 为后缀的这两款勒索软件都属于 Crysis 家族，这个家族每次更换新的私钥都会换一个后缀（10 月份是.arena 后缀，11 月份是.Java 后缀）。新出现的.arena 和.java 替代了.wallet 开始流行。

二、 勒索软件的家族分布

统计显示，在向 360 互联网安全中心求助的勒索软件受害者中，Cerber、Crysis、WannaCry 这三大勒索软件家族的受害者最多，共占到总量的 58.4%。其中，Cerber 占比为 21.0%，Crysis 占比为 19.9%，WannaCry 占比为 17.5%，具体分布如下图所示。



结合 360 互联网安全中心的大数据监测分析，下图给出了 2017 年不同勒索软件家族在国内的活跃时间分析。特别需要说明的是：“类 Petya”勒索病毒（该病毒说明请参考第四章的第二节介绍），虽然在国外发动了大规模的攻击行为，产生了及其重要影响，但是在国内基本就没有传播，所以在下图中没有体现这两个家族。



三、 勒索软件的传播方式

360 互联网安全中心监测显示，黑客为了提高勒索软件的传播效率，也在不断更新攻击方式，钓鱼邮件传播依然是黑客常用的传播手段，服务器入侵的手法更加娴熟运用，同时也开始利用系统自身的漏洞进行传播。今年勒索软件主要采用以下五种传播方式：

1） 服务器入侵传播

以 Crysis 家族为代表的勒索软件主要采用此类攻击方式。黑客首先通过弱口令、系统或软件漏洞等方式获取用户名和密码，再通过 RDP（远程桌面协议）远程登录服务器，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勒索软件。所以，在这种攻击方式中 ，一旦 服务器被入侵，安全软件一般是不起作用的。

服务器能够被成功入侵的主要原因还是管理员的帐号密码被破解。而造成服务器帐号密码被破解的主要原因有以下几种：为数众多的系统管理员使用弱密码，被黑客暴力破解；还有一部分是黑客利用病毒或木马潜伏在用户电脑中，窃取密码；除此之外还有就是黑客从其他渠道直接购买账号和密码。黑客得到系统管理员的用户名和密码后，再通过远程登录服务器，对其进行相应操作。

2） 利用漏洞自动传播

今年，通过系统自身漏洞进行传播扩散成为勒索软件的一个新的特点。上半年震动世界的 WannaCry 勒索病毒就是利用微软的永恒之蓝（EternalBlue）漏洞进行传播。黑客往往抓住很多人认为打补丁没用还会拖慢系统的错误认识，从而利用刚修复不久或大家重视程度不高的漏洞进行传播。如果用户未及时更新系统或安装补丁，那么即便用户未进行任何不当操作，也有可能在完全没有预兆的情况下中毒。此类勒索软件在破坏功能上与传统勒索软件无异，都是加密用户文件勒索赎金。但因为传播方式不同，导致更加难以防范，需要用户自身提高安全意识，尽快更新有漏洞的软件或安装对应的安全补丁。

3） 软件供应链攻击传播

软件供应链攻击是指利用软件供应商与最终用户之间的信任关系，在合法软件正常传播和升级过程中，利用软件供应商的各种疏忽或漏洞，对合法软件进行劫持或篡改，从而绕过

传统安全产品检查达到非法目的的攻击类型。

2017 年爆发的 Fireball、暗云 III、类 Petya、异鬼 II、Kuzzle、XShellGhost、CCleaner 等后门事件均属于软件供应链攻击。而在乌克兰爆发的类 Petya 勒索软件事件也是其中之一，该病毒通过税务软件 M.E.Doc 的升级包投递到内网中进行传播。

4） 邮件附件传播

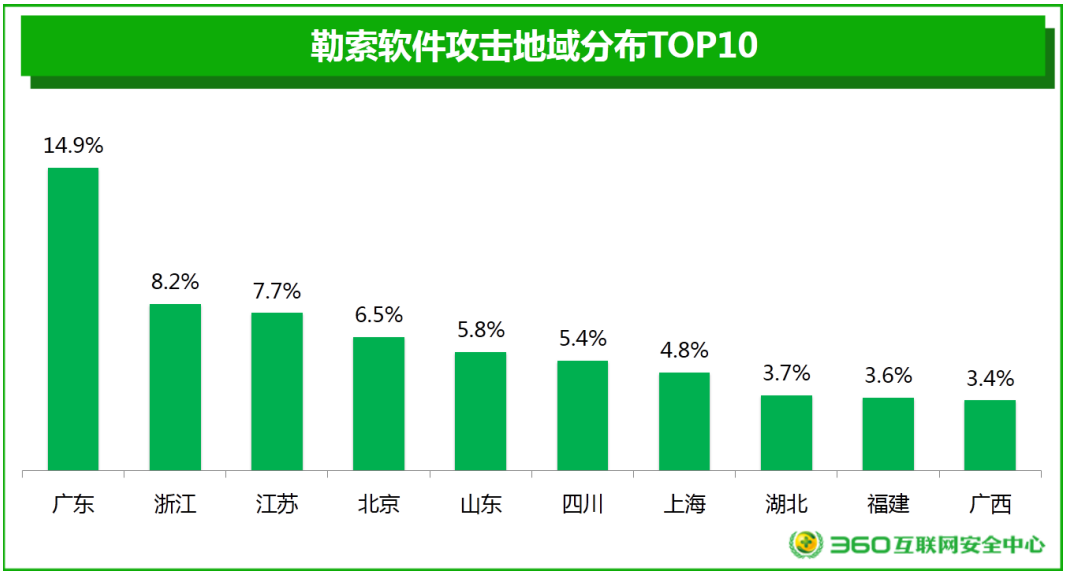
通过伪装成产品订单详情或图纸等重要文档类的钓鱼邮件，在附件中夹带含有恶意代码的脚本文件。一旦用户打开邮件附件，便会执行里面的脚本，释放勒索病毒。这类传播方式的针对性较强，主要瞄准公司企业、各类单位和院校，他们最大的特点是电脑中的文档往往不是个人文档，而是公司文档。最终目的是给公司业务的运转制造破坏，迫使公司为了止损而不得不交付赎金。

5） 利用挂马网页传播

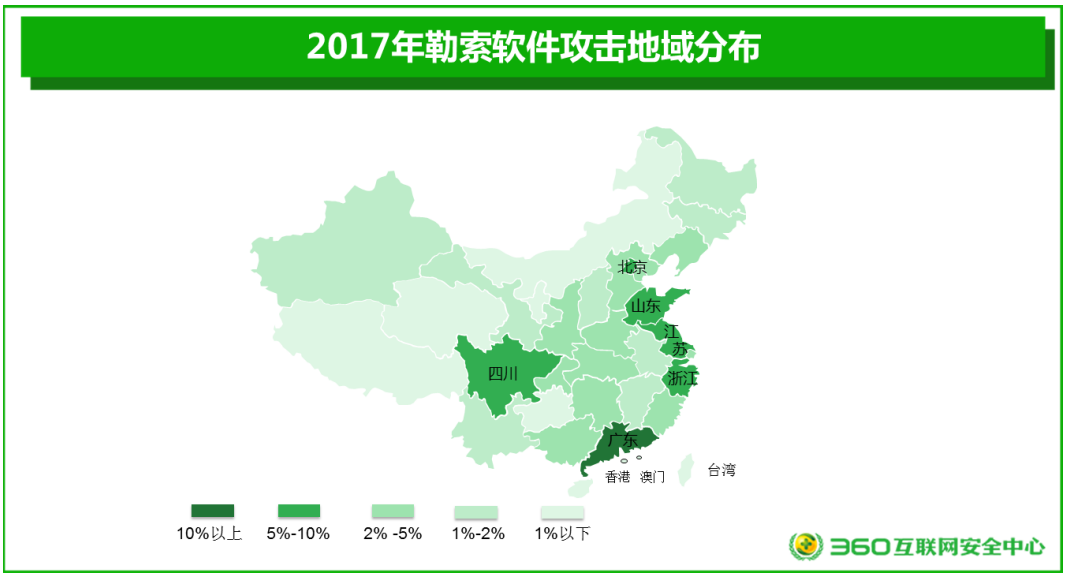
通过入侵主流网站的服务器，在正常网页中植入木马，让访问者在浏览网页时利用 IE 或 Flash 等软件漏洞进行攻击。这类勒索软件属于撒网抓鱼式的传播，并没有特定的针对性，一般中招的受害者多数为裸奔用户，未安装任何杀毒软件。

四、 勒索软件攻击的地域

360 互联网安全中心监测显示，遭遇勒索软件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 14.9%，其次是浙江 8.2%，江苏 7.7%。排名前十省份占国内所有被攻击总量的 64.1%。



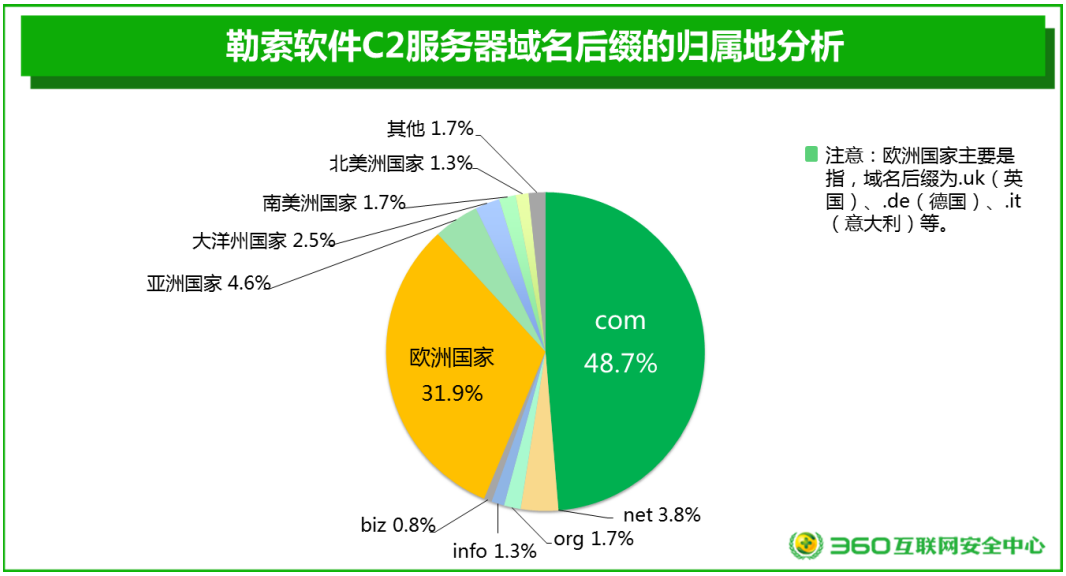
2017 年勒索软件攻击地域分布如下图所示。



五、 勒索软件服务器分布

360 互联网安全中心针对最为活跃的部分勒索软件的 C2 服务器域名后缀的归属地进行了分析，结果显示：.com 域名被使用的最多，约为总量的一半，为 48.7%，.net 和.org 占比分别为 3.8%和 1.7%。此外，属于欧洲国家的域名最多，占 31.9%，其次是亚洲国家 4.6%，南美洲国家 1.7%，大洋洲国家 1.7%，北美洲国家 1.3%。

特别值得注意的是，主流的大勒索家族都不再使用 C2 服务器加密技术了，但还是有很多小众勒索家族在使用 C2 服务器的加密技术。

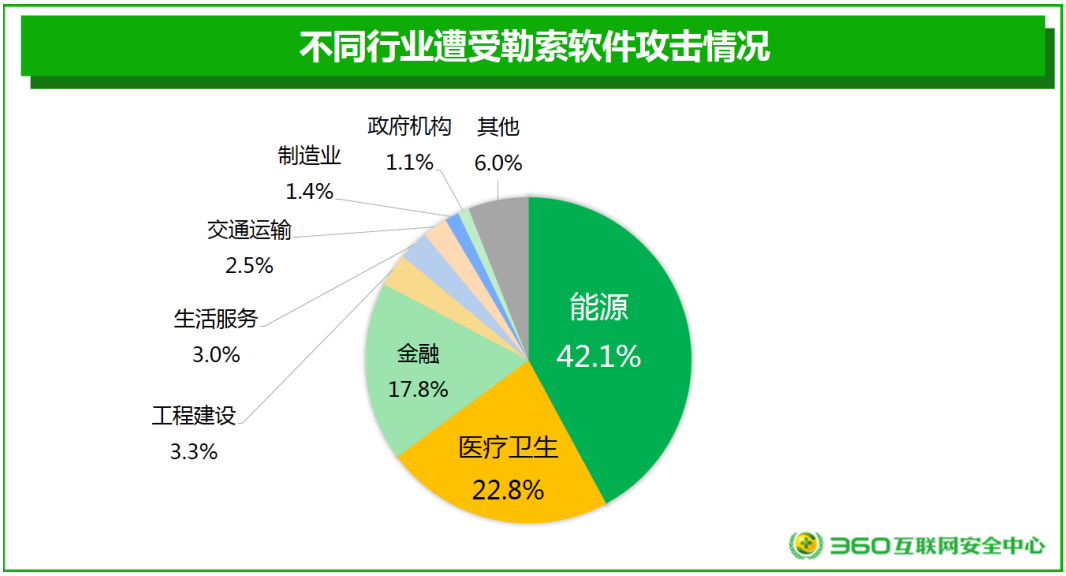


六、 勒索软件攻击的行业

为更加深入的了解各行业勒索软件遭到攻击的情况，360 威胁情报中心 联合全国一百余家政府机构、事业单位和大中型企业的 IT 管理人员，对各企业遭勒索软件攻击情况展开

了深入的调查分析。并希望此项研究能够对更多机构的网络管理者提供有价值的参考信息。

不同行业政企机构遭受勒索软件攻击的情况分析显示，能源行业是遭受攻击最多的行业，占比为 42.1%，其次为医疗行业为 22.8%，金融行业为 17.8%，具体分布如下图所示。需要说明的是，遭到攻击多不代表被感染的设备多。攻击量是通过企业级终端安全软件的监测获得的。



从上图中，我们知道能源、医疗卫生、金融是遭受勒索软件攻击最多的三个行业，那么究竟是哪些家族对这三个行业发动的攻击呢？下表分别给出了每个行业遭受勒索软件攻击最多的前五个家族，具体如下表所示。可以看出，针对不同行业，攻击者者所使用的勒索软件类型是有很大区别的。

能源		医疗卫生		金融	
家族 TOP5	占比	家族 TOP5	占比	家族 TOP5	占比
locky	29.5%	cerber	43.7%	cerber	61.6%
cerber	24.9%	spora	18.1%	类 petya	17.7%
cryptomix	9.5%	crysis	8.2%	locky	10.5%
globeimposter	7.4%	sage	5.4%	shade	1.8%
btcware	7.2%	locky	4.5%	spora	1.8%

表 1　能源、医疗卫生、金融行业遭受勒索攻击的家族 TOP5

七、　勒索软件的攻击特点

如果说，挂马攻击是 2016 年勒索软件攻击的一大特点，那么 2017 年，勒索软件的攻击则呈现出以下六个明显的特点：无 C2 服务器加密技术流行、攻击目标转向政企机构、攻击目的开始多样化、勒索软件平台化运营、影响大的家族赎金相对少、境外攻击者多于境内攻击者。

（一）　无 C2 服务器加密技术流行

2017 年，我们发现黑客在对文件加密的过程中，一般不再使用 C2 服务器了，也就是说现在的勒索软件加密过程中不需要回传私钥了。

这种技术的加密过程大致如下：

1） 在加密前随机生成新的加密密钥对（非对称公、私钥）

2） 使用该新生成新的公钥对文件进行加密

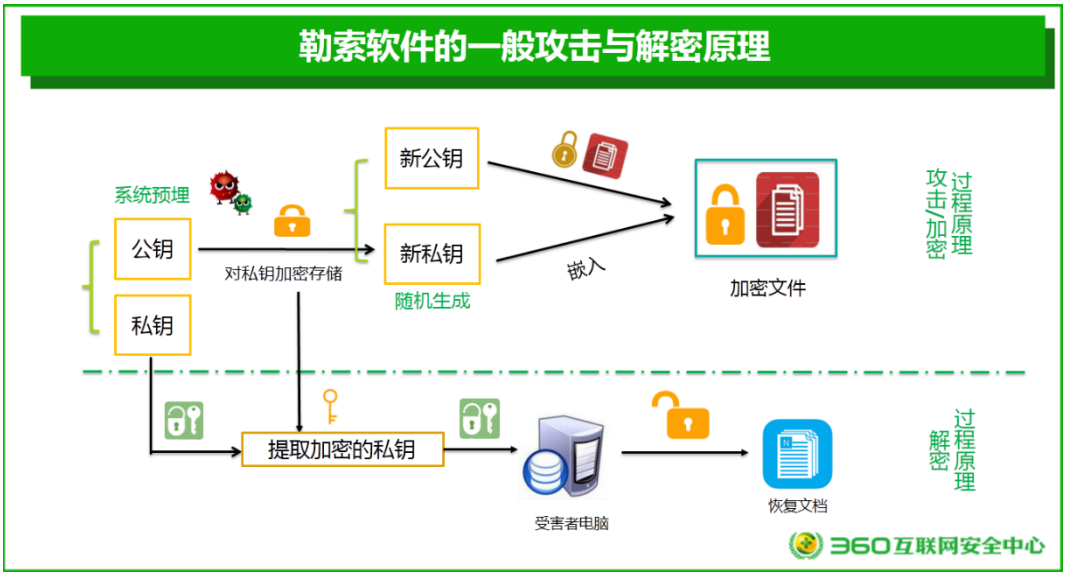
3） 把新生成的私钥采用黑客预埋的公钥进行加密保存在一个 ID 文件或嵌入在加密文件里

解密过程大致如下：

1） 通过邮件或在线提交的方式，提交 ID 串或加密文件里的加密私钥（该私钥一般黑客会提供工具提取）；

2） 黑客使用保留的预埋公钥对应的私钥解密受害者提交过来的私钥；

3） 把解密私钥或解密工具交付给受害者进行解密。



通过以上过程可以实现每个受害者的解密私钥都不相同，同时可以避免联网回传私钥。这也就意味着不需要联网，勒索病毒也可以对终端完成加密，甚至是在隔离网环境下，依然可以对文件和数据进行加密。显然 ，这种技术是针对采用了各种隔离措施的政企机构所设计的。

（二） 攻击目标转向政企机构

2017 年，勒索软件的攻击进一步聚焦在高利润目标上，其中包括高净值个人、连接设备和企业服务器。特别是针对中小企业网络服务器的攻击急剧增长，已经成为 2017 年勒索软件攻击的一大鲜明特征。据不完全统计，2017 年，约 15%的勒索软件攻击是针对中小企业服务器发起的定向攻击，尤以 Crysis、xtbl、wallet、arena、Cobra 等家族为代表。

客观的说，中小企业往往安全架构单一，相对容易被攻破。同时，勒索软件以企业服务器为攻击目标，往往也更容易获得高额赎金。例如：针对 Linux 服务器的勒索软件 Rrebus，虽然名气不大，却轻松从韩国 Web 托管公司 Nayana 收取了 100 万美元赎金，是震惊全球的永恒之蓝全部收入的 7 倍之多。Nayana 所以屈服，是因为超 150 台服务器受到攻击，上面托管着 3400 多家中小企业客户的站点。这款勒索病毒的覆盖面有限，韩国几乎是唯一的重

灾区。

（三） 针对关键信息基础设施的攻击

以 WannaCry、类 Petya 为代表的勒索软件，则是将关键信息基础设施作为了主要攻击目标，这在以往是从未出现过的严峻情况。关键基础设施为社会生产和居民生活提供公共服务，保证国家或地区社会经济活动正常进行，其一旦被攻击将严重影响人们的日常生活，危害巨大。

（四） 攻击目的开始多样化

顾名思义，勒索软件自然就是要勒索钱财。但这种传统认知已经在 2017 年被打破。以网络破坏、组织破坏为目的的勒索软件已经出现并开始流行。其中最为典型的代表就是类 Petya。与大多数勒索软件攻击不同，类 Petya 的代码不是为了向受害者勒索金钱，而是要摧毁一切。类 Petya 病毒的主要攻击目的就是为了破坏数据而不是获得金钱。此外，以 Spora 为代表的窃密型勒索软件在加密用户文档时，还会窃取用户账号密码和键盘输入等信息，属于功能复合型勒索软件。

这些不仅以“勒索”为目的的“勒索软件”，实际上只是结合了传统勒索软件对文件进行加密的技术方法来实现其数据破坏、信息窃取等其他攻击目的。相比于勒索金钱，这种攻击将给对手带来更大的破坏和更大的威胁。这不仅会引发网络犯罪“商业模式”的新变种，而且会反过来刺激网络保险市场的进一步扩张。

（五） 勒索软件平台化运营

2017 年，勒索软件已经不再是黑客单打独斗的产物，而是做成平台化的上市服务，形成了一个完整的产业链条。在勒索软件服务平台上，勒索软件的核心技术已经直接打包封装好了，小黑客直接购买调用其服务，即可得到一个完整的勒索软件。这种勒索软件的生成模式我们称其为 RaaS 服务，而黑市中一般用“Satan Ransomware（撒旦勒索软件）”来指代由 RaaS 服务生成的勒索软件。

RaaS 服务允许任何犯罪者注册一个帐户，并创建自己定制版本的撒旦勒索软件。一旦勒索软件被创建，那么犯罪分子将决定如何分发勒索软件，而 RaaS 服务平台将处理赎金支付和增加新功能。对于这项服务，RaaS 服务平台的开发者将收取受害者所支付赎金的 30％，购买 RaaS 服务者将获取剩余 70％的赎金。

（六） 境外攻击者多于境内攻击者

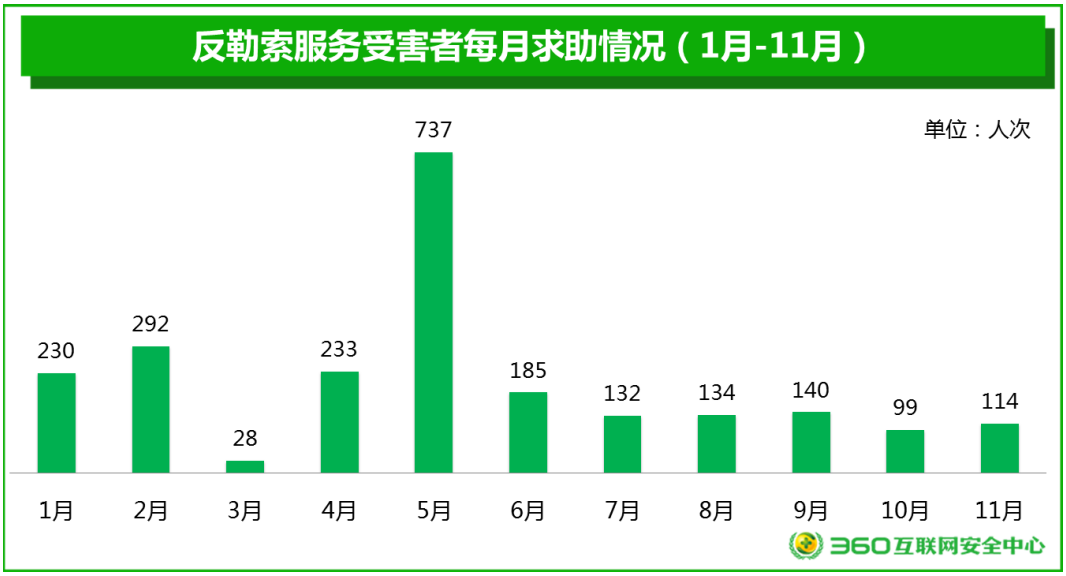
2017 年，勒索软件的攻击源头以境外为主。绝大多数的勒索软件攻击者基本都是境外攻击者，国内攻击者较少，而且国内攻击者技术水平也相对较低，制作水平也不高。有些国内攻击者编写的勒索软件程序甚至存在很多漏洞，因此也比较容易被破解。比如：MCR 勒索病毒，我们可以直接获取到密钥从而恢复文件。

第二章　勒索软件受害者特征分析

2017 年 1 月至 11 月，360 反勒索服务共接到了 2325 位遭遇勒索软件攻击的受害者求助。为了更好的了解勒索软件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，免遭勒索软件侵害，本次报告特别对这两千多位求助受害者进行了随机抽样调研，并从中选取了有效的 452 份调研问卷进行分析。本报告的第二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、受害者的求助情况

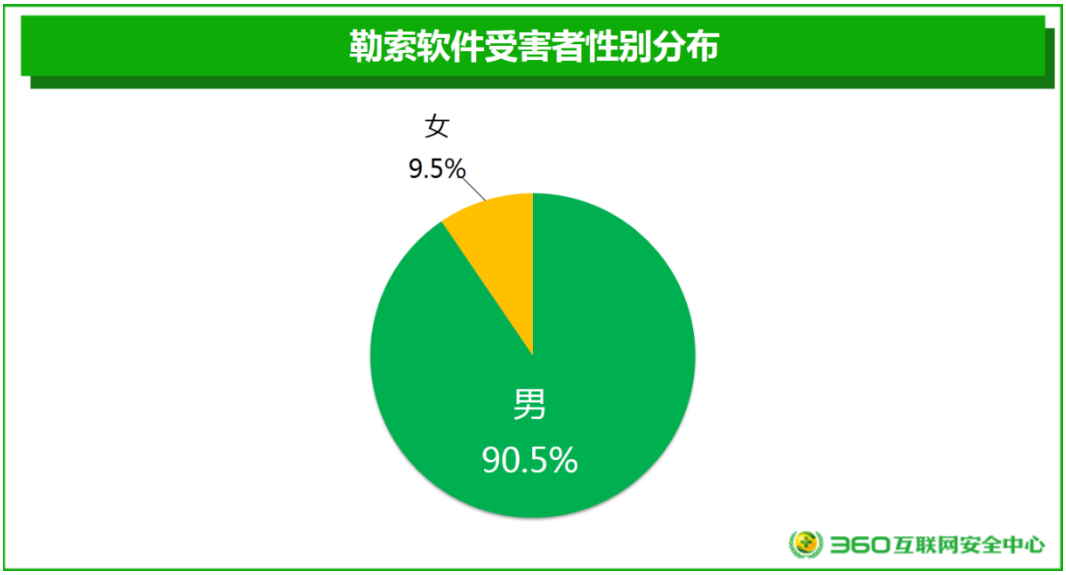
2017 年 1 月至 11 月，360 反勒索服务共接到了 2325 位遭遇勒索软件攻击的受害者求助。从数据统计中可以看到，5 月份是受害者求助的高峰期，主要是因为 WannaCry 勒索蠕虫的爆发。受害者每月求助情况具体如下图所示。



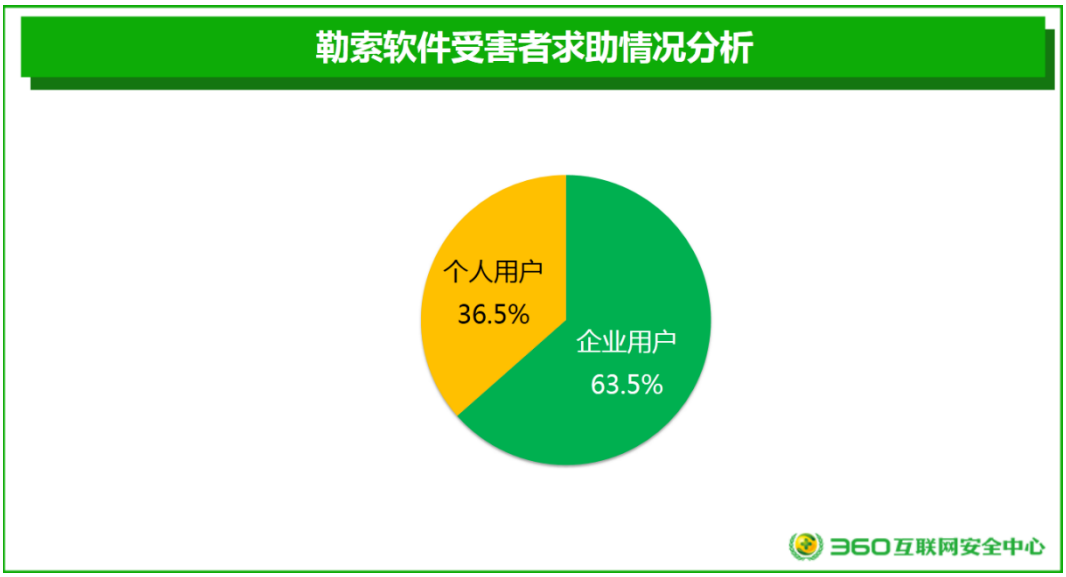
调研发现，目前绝大多数求助用户并不是在安装了 360 安全卫士，并开启了反勒索服务的情况下感染的勒索软件。特别值得注意的是，还有相当数量的受害者在感染勒索软件时，电脑上没有安装任何安全软件。

二、受害者的基本特征

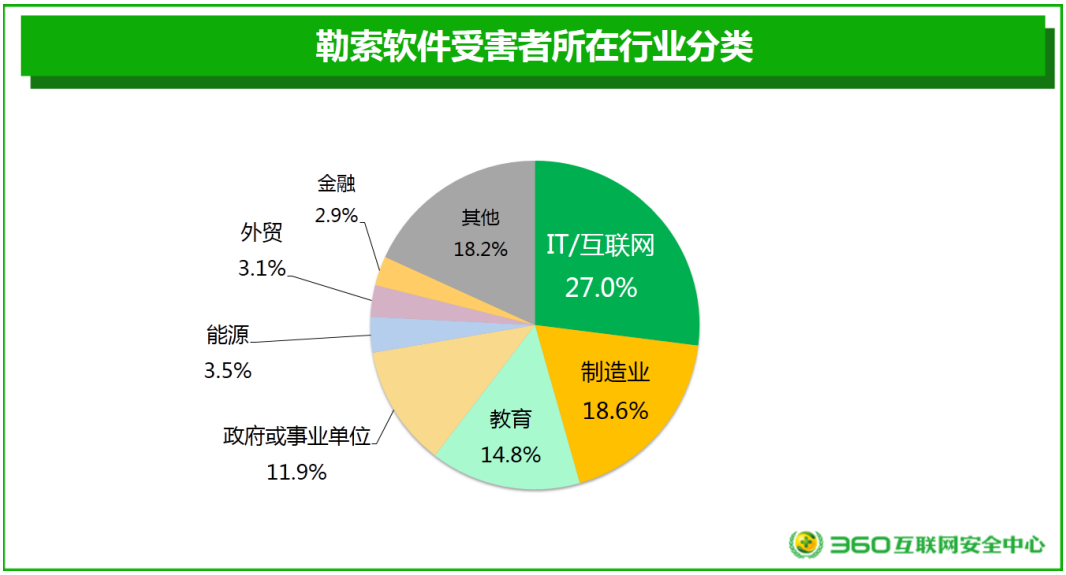
调研数据显示，男性是最容易受到勒索软件攻击的对象，占比高达 90.5%，而女性占比仅为 9.5%。



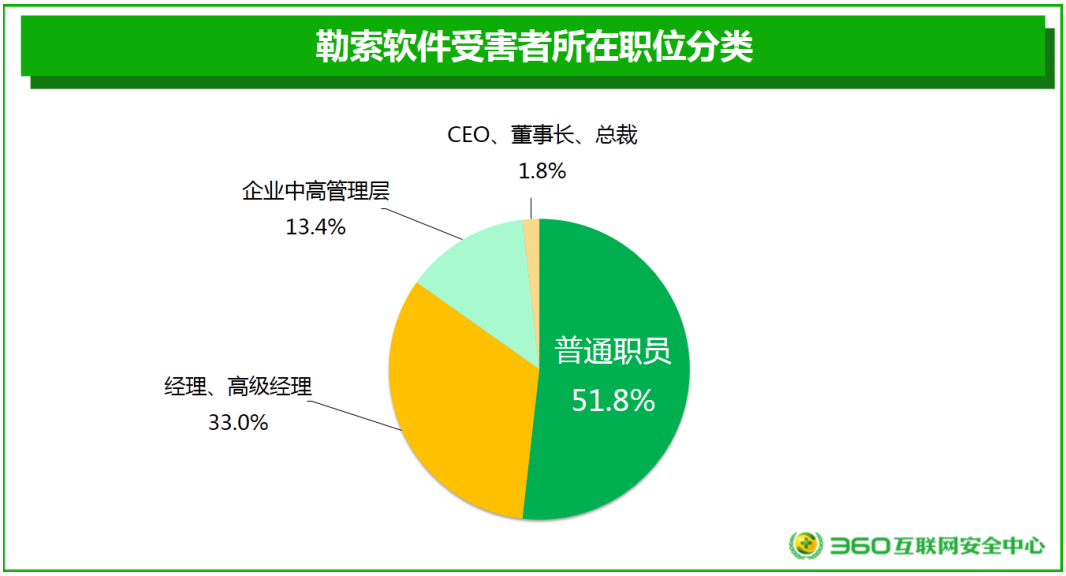
在 360 互联网安全中心接到的受害者主动寻求帮助的人群中，63.5%为企业用户，36.5%为个人用户。通过对受害者的调研分析发现，攻击者会针对企业用户采取服务器入侵、邮件传播等方式传播勒索软件，造成的危害比较高。企业用户电脑中毒以后，由于被加密的多是相对更加重要的公司办公和业务文件，因此，企业用户往往会更加积极寻求解决办法，特别是更加积极向专业安全厂商寻求帮助。



从求助的受害者所在的行业分类（注：此处与上一章中根据攻击量监测进行的行业分析统计方法有所不同）中可以看出，IT/互联网行业的受害者最多，占比为 27.0%；其次是制造业，占比为 18.6%；教育行业占比为 14.8%。具体分布如下图所示。

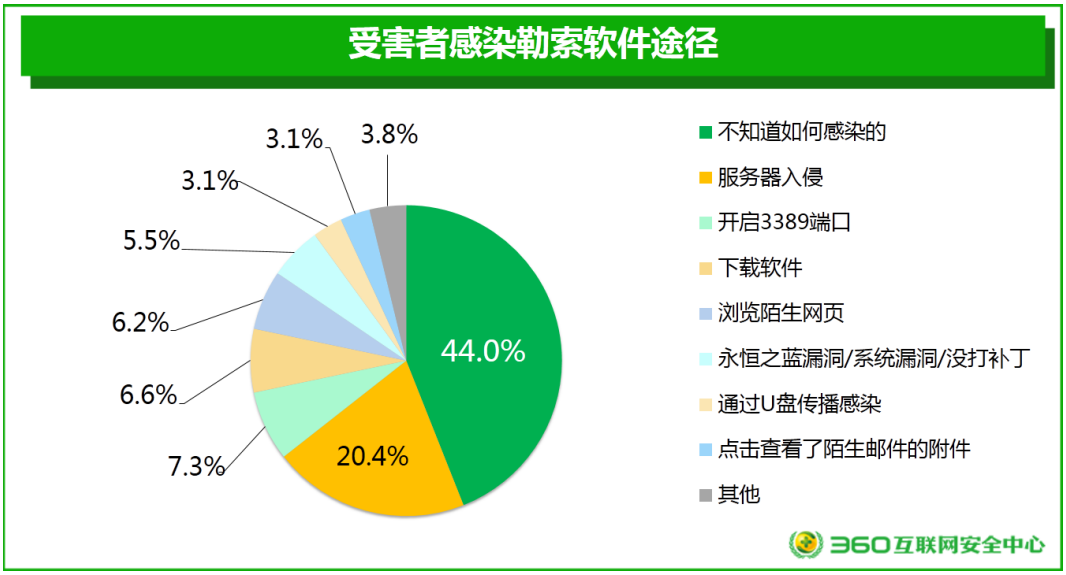


从求助的受害者所在的职位分类中可以看出，普通职员是遭遇勒索软件攻击次数最多的受害者，超过受害者总数的一半以上，占比为 51.8%，其次是经理、高级经理，占比为 33.0%，企业中、中高管理层，占比为 13.4%，CEO、董事长、总裁等企业的掌舵者被勒索软件攻击的比例也达到 1.8%。

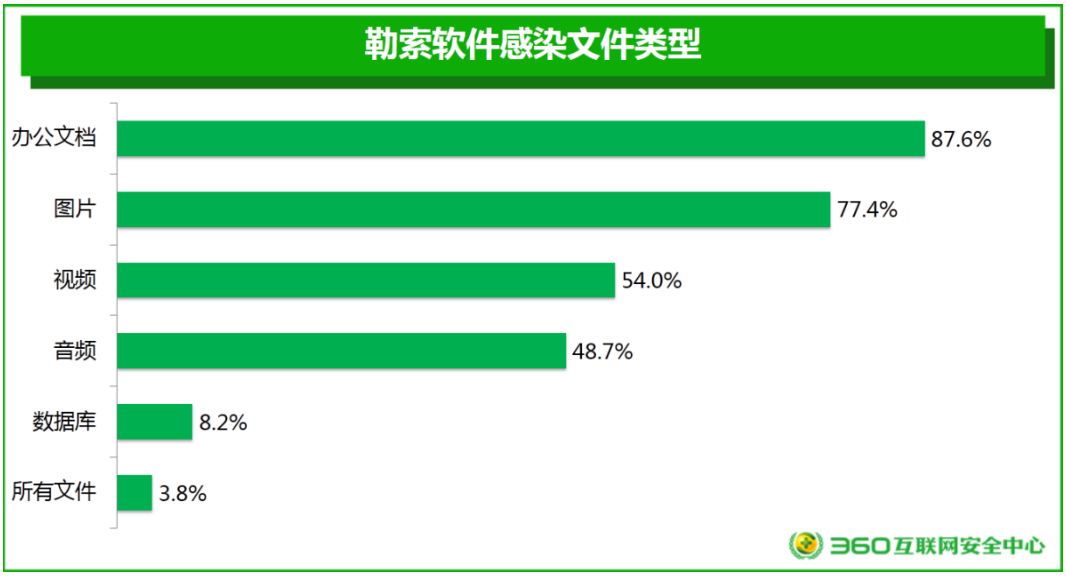


三、受害者的感染情况

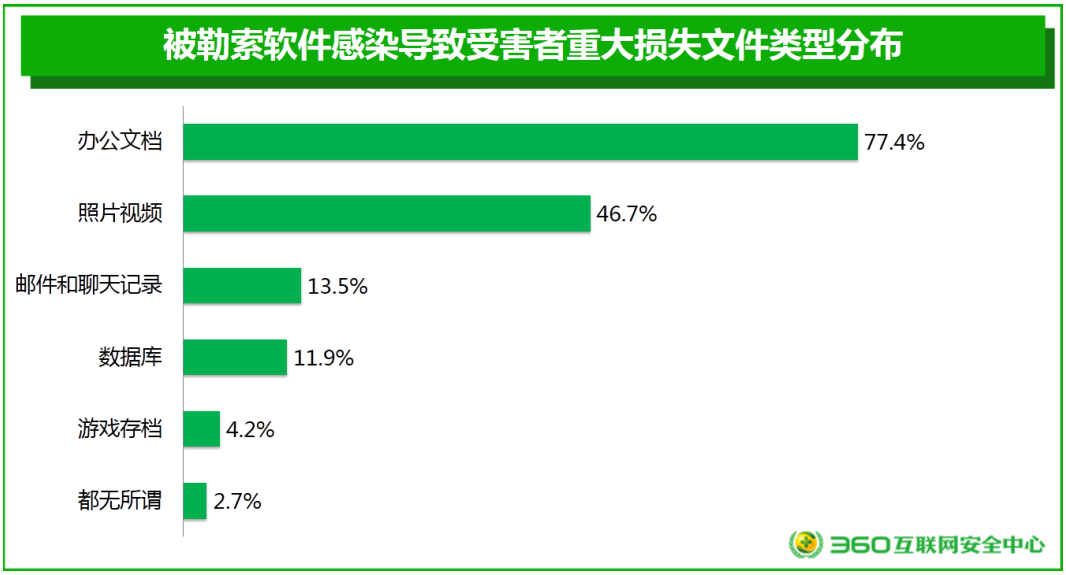
从求助的受害者感染勒索软件的途径可以看出，44.0%的受害者不知道自己是如何感染的勒索软件，可见该病毒在感染、执行过程中具有极强的隐蔽性，让受害者难以察觉。20.4%的受害者是因为服务器被入侵而感染的勒索软件，7.3%的受害者是因为开启 3389 端口（Windows 系统自带的远程控制端口），黑客通过远程控制用户的电脑，进而让其感染勒索软件。具体如下图所示。可见，2017 年，带毒电子邮件已经不是再是勒索软件传播的主要途径。



从求助的受害者文件感染类型可以看出，87.6%是受害者电脑上的办公文档被感染，其次，77.4%的图片文件被感染，54.0%的视频文件被感染，48.7%的音频文件被感染，8.2%的数据库文件被感染。数据库文件被加密主要是由于今年发现了大量针对服务器的攻击，尤其是针对网络安全措施相对较弱的中小企业，从而导致数据库被加密的现象时有发生。



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，77.4%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46.7%；邮件和聊天记录占比为 13.5%；数据库类文件占比为 11.9%；游戏存档类文件占比为 4.2%。



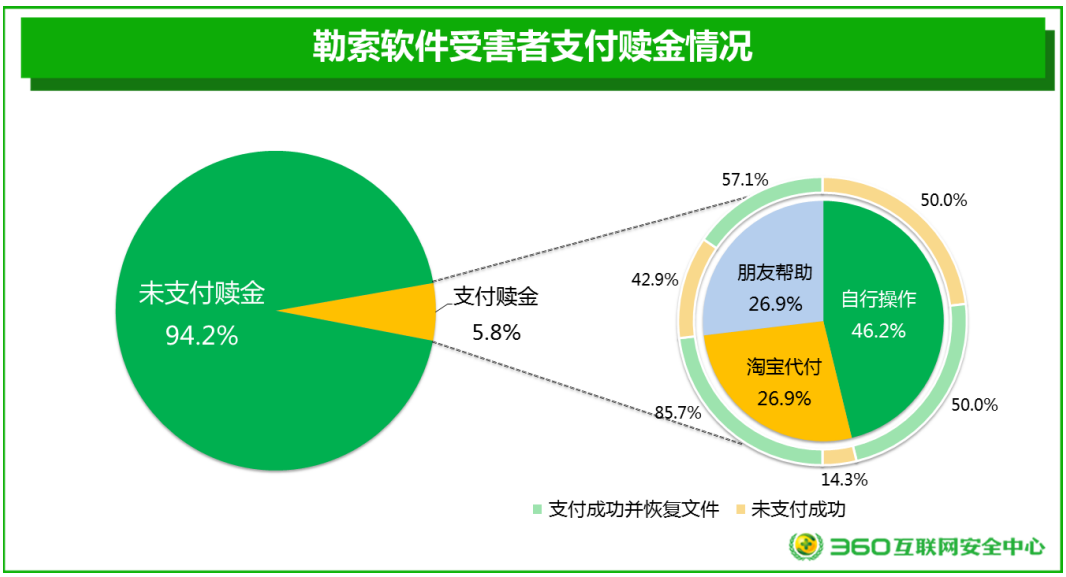
我们发现，在主动寻求帮助的受害者中，办公文档是感染数量最多，同时也是导致受害者损失最大的文件类型。因为办公文档中往往含有我们工作中用到的重要资料，更加被我们重视和关注。

四、赎金支付与支付方式

根据 360 反勒索服务平台对受到勒索软件攻击用户的统计数据显示，绝大多数的勒索软件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。但是，9 月底时比特币在中国已经全面停止交易了，导致受害者文件被勒索病毒感染后更加难以恢复。

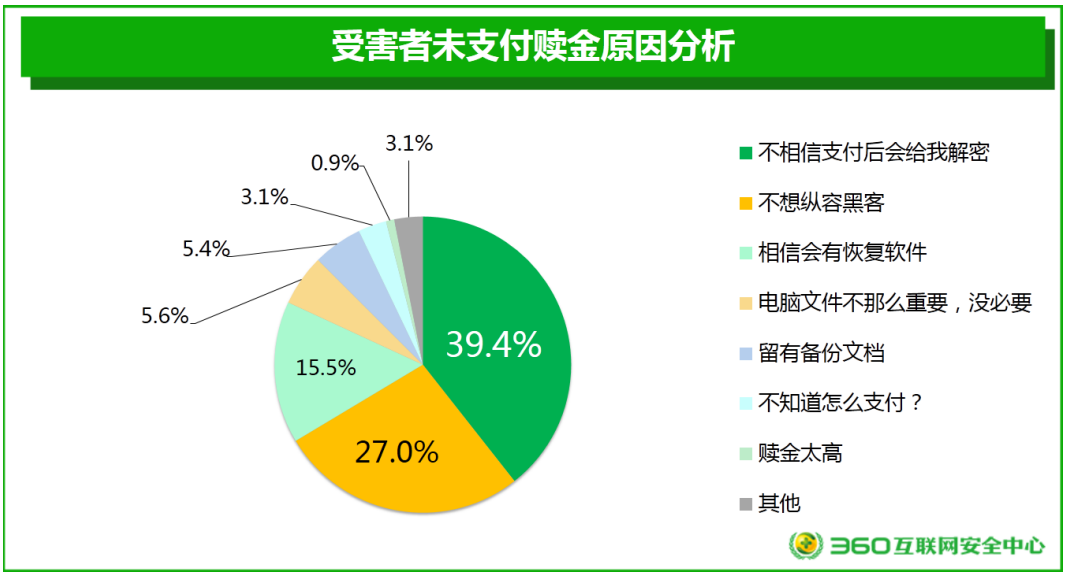
抽样调查显示，在这些求助的受害者中，已有 5.8%的受害者为了恢复文件而支付赎金，另外 94.2%的受害者选择了拒绝为恢复文件而支付赎金。

进一步调查显示，在支付赎金的受害者中，46.2%的受害者是自己按照病毒提示兑换比特币的方式付款的，26.9%的受害者是通过在淘宝平台找代付赎金服务付款的，26.9%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，在淘宝平台找勒索软件代付赎金服务的用户中，85.7%的受害者最终成功支付了赎金，并恢复了文件；朋友帮忙付款的，57.1%的受害者成功支付了赎金，并恢复了文件；而自己按照勒索软件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。

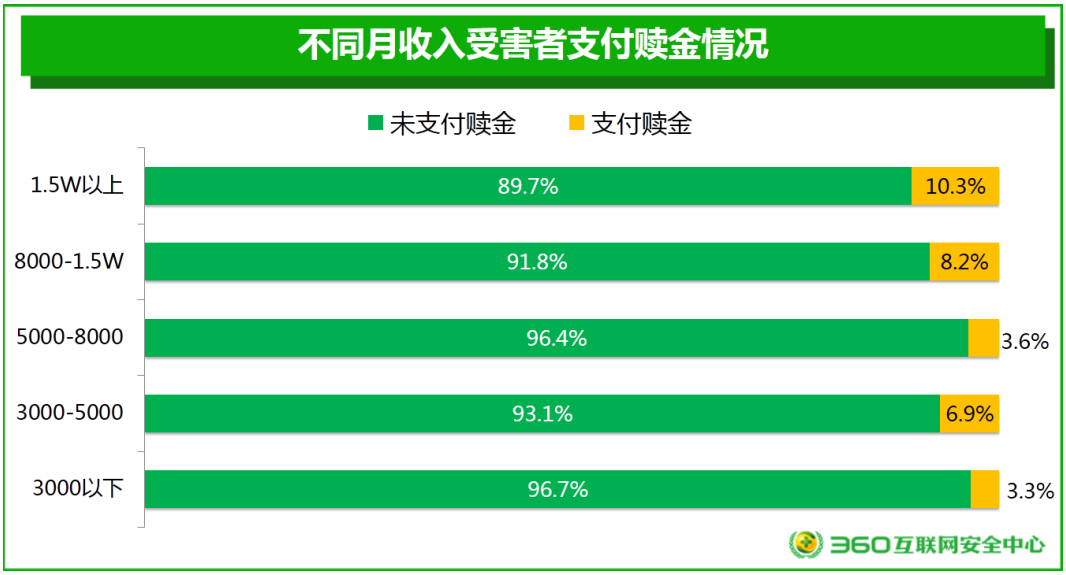
如前所述，绝大多数，即 94.2%的受害者选择了拒绝为恢复文件而支付赎金。本次报告也特别对这些受害者为什么会拒绝支付赎金的问题进行了调研。结果显示：39.4%的受害者是因为不相信支付赎金后会给自己的文件解密，27.0%的受害者是因为不想继续纵容黑客进而选择拒绝支付赎金，15.5%的受害者是因为相信会有恢复工具能够修复加密的文件，具体如下图所示。



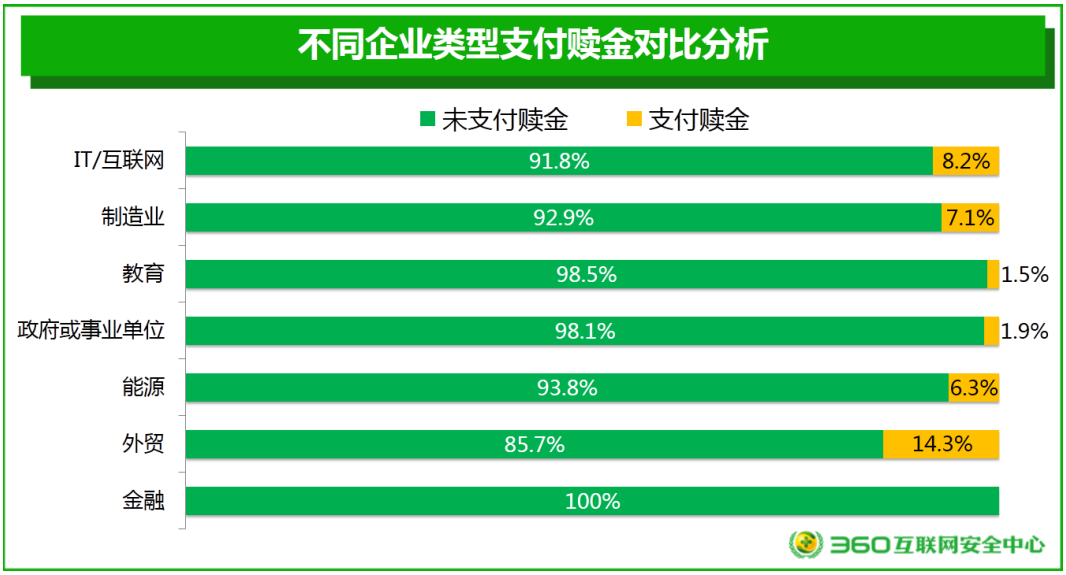
五、影响赎金支付的因素

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？本次报告从受害者的月收入和所在行业这两个方面对用户进行了调研。

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 10.3%。对于高收入人群来说，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。下图给出了具体情况分析。



下图给出了求助的不同行业受害者支付赎金的比例对比。统计显示，金融行业中招的受害者竟无一人支付赎金，这与 2016 年的情况大相径庭。在 2016 年的调研统计中，金融行业受害者支付赎金的比例最高，达 33.3%。此外，2017 年，求助的金融行业受害者仅占求助者总数的 2.9%，相比去年 4.5%有一定的下降趋势。进一步的调研分析发现，造成这种明显变化的主要原因是：金融机构在 2017 年普遍加强了网络安全建设和灾备恢复能力，虽然也有感染情况发生，但抗灾容灾能力明显增强。



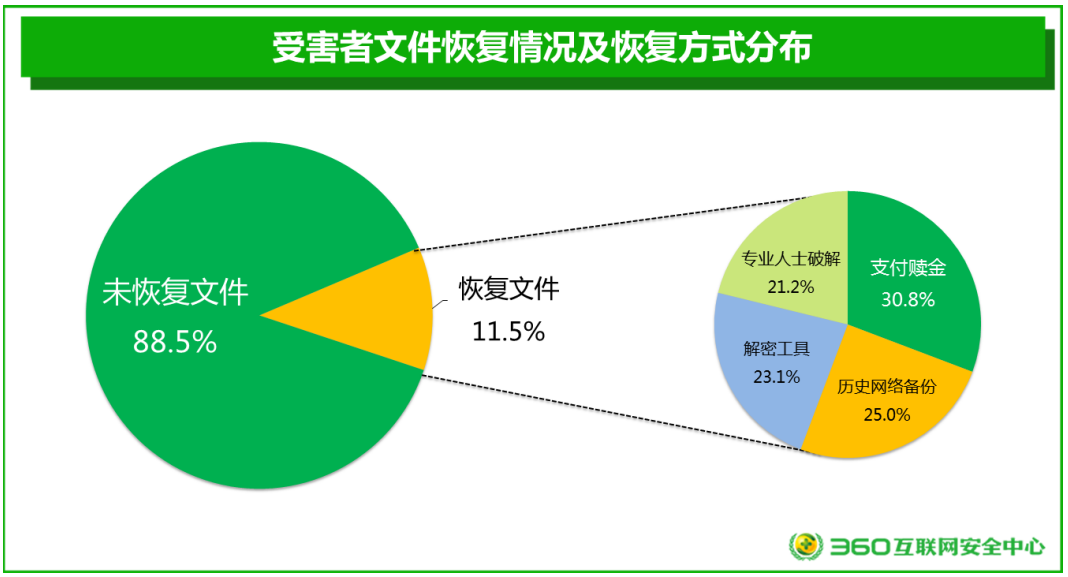
综合收入、职位和行业这三方面因素来看，受害者所属的行业是对支付意愿影响最大的因素。

六、恢复感染文件的方法

感染勒索软件后，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。可见，目前勒索软件攻击者的“信用”还是不错的。此外，由于目前仍有相当一部分的勒索软件并未规范使用加密算法，对文件进行加密，所以，对于感染了此类勒索软件的用户来说，即便不支付赎金，也可以通过专业安全机

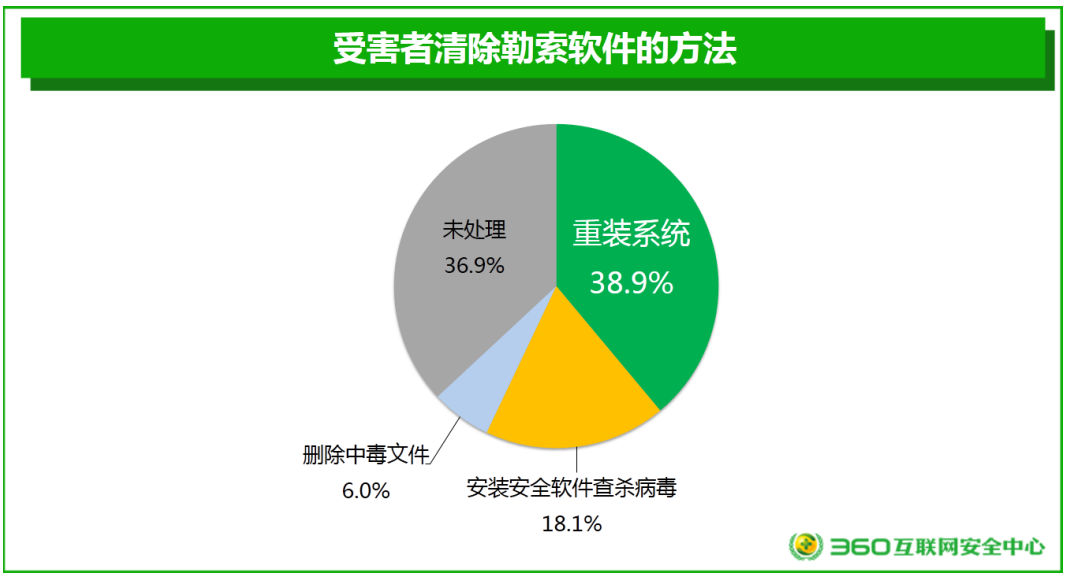
构，如 360 等安全厂商提供的一些解密工具对文件进行解密。还有一些用户提前对重要文件进行了备份，所以也最终成功恢复了文件。

总体来看，在接受调研的受害者中，有 11.5%的受害者最终成功恢复了文件，另外 88.5%的受害者没有恢复文件。在受害者恢复文件的方式中，30.8%的受害者是通过支付赎金恢复的文件，25.0%的受害者是通过历史备份（如云盘、移动硬盘等）恢复的文件，23.1%的受害者是通过解密工具恢复文件的，21.2%的受害者是通过专业人士破解恢复文件的。



用户电脑感染勒索软件后，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：38.9%的受害者通过重装系统清除了病毒，18.1%的受害者通过安装安全软件查杀掉病毒，6.0%的受害者直接删除中毒文件。

特别值得注意的是，我们发现有 36.9%的受害者在知道自己电脑已经感染勒索软件后，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勒索软件的攻击都是“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。



另外，研究发现，受害者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。

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勒索软件时，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，在感染勒索软件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。

第三章　WannaCry 勒索软件的大规模攻击

2017 年 5 月，影响全球的勒索软件永恒之蓝勒索蠕虫（WannaCry）大规模爆发，它利用了据称是窃取自美国国家安全局的黑客工具 EternalBlue（永恒之蓝）实现了全球范围内的快速传播，在短时间内造成了巨大损失。本章主要针对永恒之蓝勒索蠕虫事件进行分析。关于 WannaCry 的深入技术分析，详见本报告“附录 2 WannaCry 攻击技术详解”。

一、 勒索蠕虫的空前影响

永恒之蓝勒索蠕虫(WannaCry)可能是自冲击波病毒以来，影响范围最广，破坏程度最大的一款全球性病毒。特别是在该病毒的攻击过程中，大量“不联网”的、一向被认为是相对比较安全的企业和机构的内网设备也被感染，这给全球所有企业和机构都敲响了警钟：没有绝对的隔离，也没有绝对的安全，不联网的不一定比联网的更加安全。

作为一款“破坏性”病毒，WannaCry 的传播速度和影响都是十分惊人的。360 互联网安全中心于 2017 年 5 月 12 日中午 13 点 44 分，截获了 WannaCry 的首个攻击样本，是世界上最早截获该病毒的公司。而在随后的短短几个小时内，就有包括中国、英国、美国、德国、日本、土耳其、西班牙、意大利、葡萄牙、俄罗斯和乌克兰等国家被报告遭到了 WannaCry 的攻击，大量机构设备陷入瘫痪。

根据 360 互联网安全中心的数据统计，仅仅 30 多个小时，截至 2017 年 5 月 13 日 20:00 时，360 互联网安全中心便已截获遭 WannaCry 病毒攻击的我国政企机构 IP 地址 29372 个。而从后续国内外媒体披露的情况来看，在全球范围内遭受此次 WannaCry 病毒攻击的国家已超过了 100 个。

WannaCry 感染电脑设备后，会将电脑中的办公文档、照片、视频等文件加密，并向用户勒索比特币。

2017 年 5 月 12 日下午 14 时许，距发现 WannaCry 病毒仅仅十几分钟，360 安全监测与响应中心就启动了针对 WannaCry 的黄色应急响应程序，并于当日下午 14:26，通过 360 安全卫士微博发出全面预警通告。与此同时，CNCert、各地网信办、公安机关等部门也都先后启动了全国范围内的大规模应急响应预警和处置工作。经过全国安全工作者大约 72 小时的连续奋战，截至 2017 年 5 月 15 日下午，WannaCry 的快速传播得到了有效的抑制，到 5 月 16 日，新增感染者数量已经非常有限。

二、 WannaCry 攻击态势分布

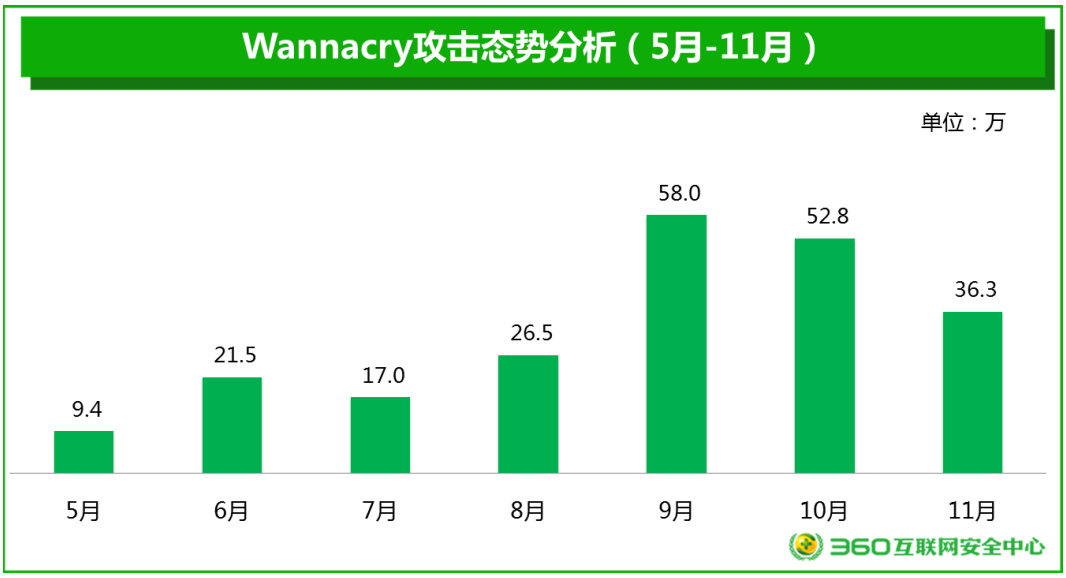
360 互联网安全中心监测显示，WannaCry 自被发现以来，相关网络攻击一直存在，而且攻击范围越来越广。

WannaCry 病毒入侵到用户的电脑后，首先会先访问一个特定的，原本并不存在的网站：

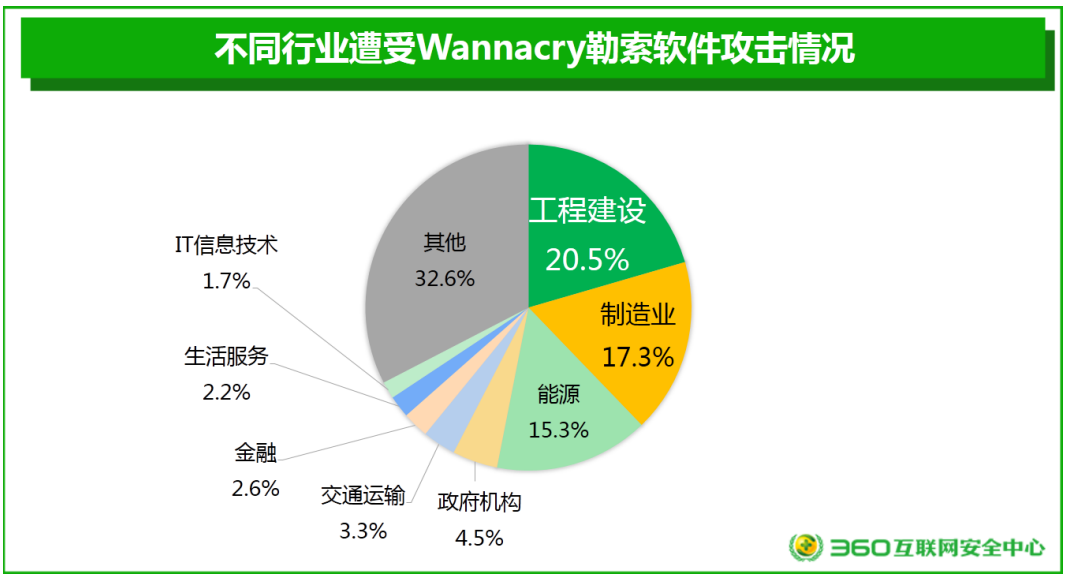
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

如果连接成功则退出程序，连接失败则继续攻击（相当于是个开关）。但在 WannaCry 大爆发第二天（2017 年 5 月 13 日晚），英国的一个分析人员对这个域名进行了注册，病毒再访问这个网站就发现能访问了，即不再加密用户数据。所以 5 月份之后，遭到 WannaCry 攻

击的联网电脑中的文件不会被实质性加密。也就是说虽然该病毒还在传播，但已经没有实际危害了。2017 年 5 月-11 月，永恒之蓝勒索蠕虫 WannaCry 攻击态势分析如下图所示。



360 威胁情报中心及 360 天擎的监测信息显示，不同行业遭受永恒之蓝勒索蠕虫攻击的情况也有所不同，工程建设行业是遭受攻击最多的行业，占比为 20.5%，其次制造业为 17.3%，能源行业为 15.3%，具体分布如下图所示。需要说明的是，该数据是根据 2017 年 5-11 月的总体情况进行分析和统计的，与 5 月份永恒之蓝勒索蠕虫刚刚爆发时相关数据统计有一定的区别。



三、 三位一体的新型病毒

从事后分析来看，WannaCry 的大规模传播绝非偶然。除了政企机构普遍存在的电脑更新不及时，系统防护能力弱等客观原因外，WannaCry 所独有的一些新型特点也是其得以成功传播的关键。WannaCry 最主要的特点是：勒索软件+蠕虫病毒+永恒之蓝。也正是由于这一特点，360 互联网安全中心将该病毒的中文名称译为：永恒之蓝勒索蠕虫。

首先，WannaCry 是首次被发现的勒索软件与蠕虫病毒的组合体。

勒索软件是最近一两年开始流行起来的一种趋利明显的恶意程序，它会使用非对称加密算法加密受害者电脑内的重要文件并以此来向受害者索要赎金，除非受害者支付赎金，否则被加密的文件无法被恢复。而以往的勒索软件，大多是通过挂马、邮件以及其他一些社工手段进行点对点的传播，从未出现过众多用户被自动攻击的情况。

而蠕虫病毒的历史则比较久远，最早可以追溯到 1988 年著名的莫里斯蠕虫。这类病毒主要是利用系统漏洞，对联网设备进行扫描，并发起自动攻击。早些年也曾出现过类似“冲击波”这样破坏性明显的蠕虫病毒，但近年来，蠕虫病毒则主要被用于制造僵尸网络，用以发动诸如垃圾邮件攻击和 DDoS 攻击等，少量蠕虫会进行盗窃数字资产等活动。

但 WannaCry 则是首次将“勒索”与“蠕虫”相结合，从而使勒索软件获得了一种超低成本的攻击方式，并在现实攻击中得以猖獗。从结果来看，WannaCry 破坏了海量的数据，不仅导致了信息的损毁，还直接导致依赖文件进行工作的电脑和设备失去服务能力，引发业务的中断，影响从线上波及线下，甚至使很多政府机构对外办事机构都停了工。

第二，WannaCry 是军用武器民用化的产物。

蠕虫病毒的攻击其实每天都在发生。但如果只是一般的蠕虫病毒，也不至于传播得如此广泛。而 WannaCry 的一个重要特点，就是整合了 Shadow Brokers（影子经纪人，黑客组织）所公布的，据称是 NSA 数字武器库中最好用的武器：ETERNALBLUE（永恒之蓝） SMB 漏洞利用工具。尽管在 WannaCry 爆发时，永恒之蓝所利用的系统漏洞已经被微软的官方补丁修护，但由于该漏洞补丁仅推出一个月，很多政企机构还未能及时给自己的内网设备全面更新，加之永恒之蓝是一款军用级网络攻击武器，未打补丁的设备很难有效防护，所以使得 WannaCry 的攻击异常顺利。

事实上，早在 2015 年 Hacking Team 武器库泄漏事件后，军用网络武器的民用化趋势就已经呈现了出来，WannaCry 的出现，使这种趋势成为了噩梦。

四、 自杀开关的成败得失

WannaCry 在逻辑设计上，有一个非常不可思议的特点，就是该病毒启动时，会首先访问一个原本并不存在的网址 URL：http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com。之后，WannaCry 会根据对该 URL 的访问结果来决定是否再继续执行下去：如果访问成功，程序会直接退出；如果访问失败，程序才会继续攻击下去。

下图是逆向的程序启动逻辑的 C 语言伪代码。

```
qmemcpy(&szUrl, aHttpWww_ifferf, 0x39u);
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);
if ( v5 )
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
else
{
  InternetCloseHandle(v4);
  InternetCloseHandle(0);
  sub_408090();
  result = 0;
}
return result;
```

```
aHttpWww_ifferf db 'http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com',0
                                        ; DATA XREF: WinMain(x,x,x,x)+A7o
```

这的确是一个非常罕见的病毒设计逻辑。起初我们猜测这个启动逻辑可能是蠕虫作者为了控制蠕虫活跃度而设计的一个云开关，而蠕虫作者最终可能是因为害怕被追踪而放弃了注册这个域名。但在分析该病毒的其他部分代码时，我们发现 WannaCry 的作者应该是一名对病毒检测对抗拥有丰富经验的人，所以我们又猜测作者可能是出于对抗检测的目的而设计了这个开关。

具体来说，目前的病毒检测分为在线检测和离线检测两种。离线检测能保证病毒检测系统以安全高效的方式工作。但要做“离线病毒分析”，就需要对病毒检测系统做很多特殊处理，比如检测系统需要欺骗病毒程序使其认为自己是运行在连线的网络环境中。这就需要使用到 Fake Responses（欺骗响应）技术：即病毒的所有网络请求都会被病毒检测系统模拟响应。所以，病毒作者可能是想使用这个启动逻辑来识别病毒检测系统是否有网络欺骗行为，以保护病毒在传播初期不被杀毒厂商快速检测封杀，从而错过控制蠕虫病毒大范围感染传播的最佳时机。而一旦病毒感染的设备达到一定的规模，就会呈现几何基数的快速增长，进而变得不可控。

但从实战情况来看，也恰恰这个被特殊设计的自杀开关，成为了安全人员追踪和反制 WannaCry 传播的重要方法。首先，由于英国的一组安全研究人员快速注册了这个本不存在 URL，从而直接避免了大量联网设备感染 WannaCry 后被锁；第二，我们可以通过 WannaCry 对该 URL 的访问请求量或 DNS 解析量进行分析，来实现对 WannaCry 感染疫情的总体监控。360 互联网安全中心也正是基于 DNS 解析量的分析，快速实现了对 WannaCry 感染疫情态势感知。

在 WannaCry 后期的各类变种中，有的修改了自杀开关的 URL 地址，有的则是直接删除了该自杀开关。

五、 WannaCry 整体攻击流程

WannaCry 整体攻击流程大致如下：

1） 利用永恒之蓝工具，通过 MS17-010 漏洞，入侵用户电脑；

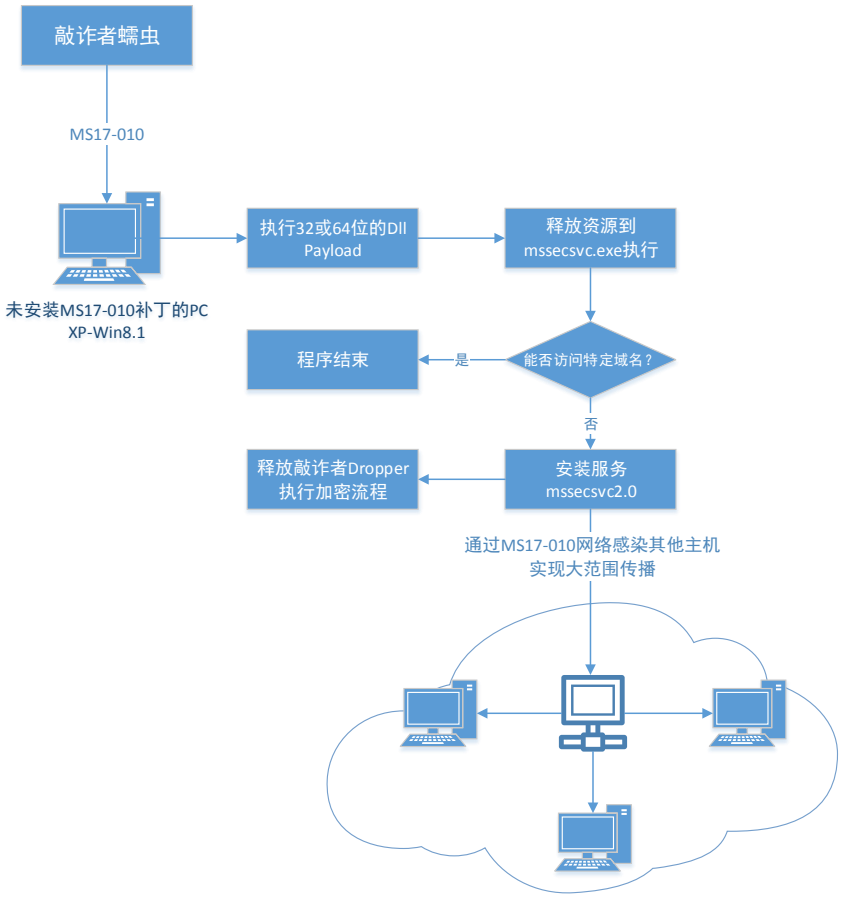
2） 执行一个 dll 文件，释放可执行模块 mssecsvc.exe；

3） 访问指定 URL，即自杀开关；

4） 若指定 URL 连接不上，则释放 mssecsvc2.0；

5） 释放 Dropper，对电脑中的文件进行加密及发送勒索消息；

6） 感染其他电脑。



六、 WannaCry 穿透内网原因

2017 年 5 月，影响全球的永恒之蓝勒索蠕虫（Wannacry）大规模爆发后，有两个重要问题一直让很多我国政企机构管理者和安全从业者感到困惑：一个是内网穿透问题，一个是同业差距问题。

1） 内网穿透问题

WannaCry 传播和攻击的一个明显的特点，就是内网设备遭感染的情况要比互联网设备

遭感染的情况严重得多。虽然说，未打补丁是内网设备中招的根本原因，但 WannaCry 究竟是如何穿透的企业网络隔离环境，特别是如何穿透了物理隔离的网络环境，一直是令业界困惑的问题。

2） 同业差距问题

WannaCry 传播和攻击的另外一个重要特点，就是有些机构大面中招，而有些机构则几乎无一中招。而且，即便是在同行业、同规模、同级别，甚至是安全措施都差不太多的大型政企机构中，也是有的机构全面沦陷，有的机构却安然无事。究竟是什么原因导致这种天差地别的结果呢？

为能深入研究上述两个问题，寻找国内政企机构安全问题的症结所在及有效的解决途径，360 威胁情报中心联合 360 安全监测与响应中心，对 5 月 12 日-5 月 16 日间，国内 1700 余家大中型政企机构的网络安全应急响应情况进行了抽样调研。并对上述问题得出了一些初步结论。

此次调研显示，在大量感染 WannaCry 的机构案例中，病毒能够成功入侵政企机构内部网络，主要原因有以下几类：

1） 一机双网缺乏有效管理

一机双网或一机多网问题，是此次 WannaCry 能够成功入侵物理隔离网络的首要原因。一机双网问题是指一台电脑设备既连接在物理隔离的网络中，同时又直接与互联网或其他网络相连。病毒首先通过互联网感染某台设备，随后再通过这台染毒设备攻击内网系统中的其他设备。

2） 缺陷设备被带出办公区

将未打补丁或有安全缺陷的设备带出办公场所，并与互联网相连，是此次 WannaCry 感染内网设备的第二大主要原因。WannaCry 爆发初期，时逢“一带一路”大会前夕。很多机构在此期间进行了联合集中办公，其中就不乏有机构将内部办公网上电脑设备被搬到了集中办公地点使用。这些电脑日常缺乏有效维护，未打补丁，结果不慎与互联网相连时就感染了 WannaCry。而这些被带出办公区的缺欠电脑，又由于工作需要，持续的，或不时的会通过 VPN、专线等方式与机构内网相连，于是又将 WannaCry 感染到了机构的内网设备中。

3） 协同办公网络未全隔离

这是一类比较特殊的问题，但在某些政企机构中比较突出。即，某些机构在其办公系统或生产系统中，同时使用了多个功能相互独立，但又需要协同运作的网络系统；而这些协同工作的网络系统中至少有一个是可以与互联网相连的，从而导致其他那些被“物理隔离”的网络，在协同工作过程中，因网络通信而被病毒感染。

4） 防火墙未关闭 445 端口

这一问题主要发生在政企机构内部的不同子网之间。大型政企机构，或存在跨地域管理的政企机构之中，发生此类问题的较多。一般来说，企业使用的防火墙设备，大多会对互联网访问关闭 445 端口。但很多企业在内部多个子网系统之间的防火墙（内部防火墙）上，却没有关闭 445 端口。从而导致这些政企机构内部的某个子网中一旦有一台设备感染了 WannaCry（可能是前述任何一种原因），病毒就会穿透不同子网之间防火墙，直接对其他子

网系统中的设备发动攻击，最终导致那些看起来相互隔离的多个子网系统全部沦陷，甚至有个别企业的共享服务器被感染后，直接导致其在各地分支机构的网络设备全部中招。

5） 办公网与生活网未隔离

这一问题在某些超大型政企机构中比较突出。受到历史、地理等复杂因素的影响，这些机构大多自行建设了规模非常庞大的内部网络，而且这些网络本身并未进行非常有效的功能隔离。特别是这些企业在办公区附近自建的家属楼、饭店、网吧，及其他一些娱乐场所，其网络也往往是直接接入了企业的内部网络，而没有与办公区的网络进行有效隔离。这也就进一步加剧了不同功能区电脑设备之间的交叉感染情况。

6） 外网设备分散无人管理

这也是一类比较特殊，但在某些政企机构中比较突出的问题。产生这一问题的主要原因是：某些政企机构，出于管辖、服务等目的，需要将自己的电脑设备放在关联第三方的办公环境中使用；但这些关联第三方可能是多家其他的政企机构，办公网点也可能分散在全国各地，甚至是一个城市中的多处不同地点；由此就导致了这些设备虽然被经常使用，但却长期无人进行安全管理和维护，电脑系统长期不打补丁，也不杀毒的情况，所以也有相当数量的电脑中招。

七、 其他暴露出来的问题简析

(一) 意识问题

员工甚至 IT 管理者的安全意识差，轻视安全问题，不能对突发安全事件做出正确的判断，是本次永恒之蓝勒索蠕虫在某些机构中未能做到第一时间有效处理的重要原因。具体表现在以下几个主要方面：

1） 病毒预警不在乎：很多企业员工或管理者根本不相信会有严重的病毒爆发，即便是看到国家有关部门的预警公告后，也毫不在意。这种倾向在越低层的员工中越明显。

2） 管理规定不遵守：政企机构中普遍存在上班时间上网购物，上色情网站的情况；还有很多私自搭建 WiFi 热点，造成了机构内网暴露。而这些行为，在绝大多数机构中都是明文禁止的。

3） 应急方案不执行：看到企业紧急下发的安全须知、应急办法和开机操作规范等材料，很多机构员工仍然我行我素，不按要求操作。

4） 风险提示不满意：有很多员工看到安全软件进行风险提示，仍然选择放行相关程序或网页；甚至有人反馈要求安全厂商不要对某些恶意软件或恶意网站进行风险提示。

(二) 管理问题

从永恒之蓝勒索蠕虫事件来看，凡是出现较大问题的政企机构，其内部的安全管理也普遍存在非常明显的问题。具体也表现在以下几个方面：

1） 业务优先忽视安全：很多政企机构非常强调业务优先，并要求任何安全措施的部署都不得影响或减缓业务工作的开展；甚至有个别机构在明知自身网络系统及电脑设备存在重大安全漏洞或已大量感染病毒的情况，仍然要求业务系统带毒运行，拒绝安全排查和治理。更有个别机构为保证信息传达的及时，上级部门领导即便收到了带毒邮件，看到了安全软件

的风险提示后，仍然会坚持向下级部门进行转发。

2） 安全监管地位较低：政企机构中的安全监管机构，安全监管领导的行政级别较低，缺乏话语权和推动力，难以推动落实网络安全规范，无法及时有效应对实时威胁，也是大规模中招企业普遍存在的一个典型特征。

3） 管理措施无法落实：由于安全监管部门在机构内的地位较低，日常的安全教育和培训又十分缺乏，从而导致了很多政企机构内部的安全管理措施无法落实。

(三) 技术问题

客观的说，通过员工教育来提高整体安全意识，在实践中往往是难以实现的。采用必要的技术手段还是十分必须的。从永恒之蓝勒索蠕虫的应急过程来看，政企机构内网设备遭大规模感染的主要技术原因有以下几个方面：

1） 物理隔离网络缺乏外联检测控制：很多采用物理隔离网络的机构，仅仅是在网络建设方面搭建了一张与互联网物理隔离的网络，而对联网设备本身是否真的会连接到互联网上，则没有采取任何实际有效的技术检测或管理方法。

2） 逻辑隔离网络缺乏内网分隔管理：采取逻辑隔离的网络，很多都存在内部子网之间边界不清的问题。这一方面表现为很多不同功能的网络设备完全没有任何隔离措施——如前述的某些大型政企机构自建的家属区、饭店、网吧等的网络与办公网没有隔离；另一方面则表现为尽管子网之间有相互隔离，但由于配置不当导致措施不够有效。

3） 隔离网内电脑不打补丁情况严重：电脑不打补丁，是永恒之蓝勒索蠕虫能够大范围攻击内网设备的根本原因。而政企单位内部隔离网络中的设备不打补丁的情况实际上非常普遍，但原因却是多种多样的。

我们不妨先来看看永恒之蓝相关的几个关键时间点：

时间点	事项
2017.3.14	微软发布安全补丁 MS17-010
2017.4.14	NSA“永恒之蓝”黑客工具泄漏
2017.5.12	永恒之蓝勒索蠕虫爆发

表 2 永恒之蓝关键事件对应的时间点

也就是说，永恒之蓝勒索蠕虫在爆发之前，我们是有 58 天的时间可以布防的，但因为很多政企单位在意识、管理、技术方面存在一些问题，导致平时的安全运营工作没有做到位，才会在永恒之蓝来临之际手忙脚乱。

对于为何有大量的政企机构不给内网电脑打补丁这个具体问题，我们也一并在这里进行一个归纳总结。具体如下：

1） 认为隔离措施足够安全

很多机构管理者想当然的认为隔离的网络是安全的，特别是物理隔离可以 100%的保证内网设备安全，因此不必增加打补丁、安全管控和病毒查杀等配置。

2） 认为每月打补丁太麻烦

在那些缺乏补丁集中管理措施的机构，业务系统过于复杂的机构，或者是打补丁后很容易出现异常的机构中，此类观点非常普遍。

3） 打补丁影响业务占带宽

很多带宽资源紧张或是内网设备数量众多的机构都持这一观点。有些机构即便是采用了内网统一下发补丁的方式，仍然会由于内网带宽有限、防火墙速率过低，或补丁服务器性能不足等原因，导致内部网络拥塞，进而影响正常业务。

4） 打补丁影响系统兼容性

因为很多机构内部的办公系统或业务系统都是自行研发或多年前研发的，很多系统早已多年无人维护升级，如果给内网电脑全面打补丁，就有可能导致某些办公系统无法再正常使用。

5） 打补丁可能致电脑蓝屏

这主要是因为某些机构内部电脑的软硬件环境复杂，容易出现系统冲突。如主板型号过老，长期未更新的软件或企业自用软件可能与微软补丁冲突等，都有可能导致电脑打补丁后出现蓝屏等异常情况。

综上所述，很多政企机构不给隔离网环境下的电脑打补丁，也并不都是因为缺乏安全意识或怕麻烦，也确实有很多现实的技术困难。但从更深的层次来看，绝大多数政企机构在给电脑打补丁过程中所遇到的问题，本质上来说都是信息化建设与业务发展不相称造成的，进而导致了必要的安全措施无法实施的问题。所以，企业在不断加强网络安全建设的同时，也必须不断提高信息化建设的整体水平，逐步淘汰老旧设备，老旧系统，老旧软件。否则，再好的安全技术与安全系统，也未必能发挥出最好的，甚至是必要的作用。

第四章　勒索软件攻击与响应典型案例

一、 永恒之蓝攻击与响应典型案例

永恒之蓝来势汹汹，在最为关键的 72 小时内，所有政企单位都在争分夺秒：已经感染的要控制风险扩散，尚未感染的要加固防线避免感染。

（一） 某大型能源机构的应急响应处置方案

场景回顾

2017 年 5 月 12 日 14:26，360 互联网安全中心发现安全态势异常，启动黄色应急响应程序，安全卫士在其官方微博上发布永恒之蓝紧急预警。5 月 13 日凌晨 1:23’，360 安全监测与响应中心接到某大型能源企业的求助，反映其内部生产设备发现大规模病毒感染迹象，部分生产系统已被迫停产。360 安全监测与响应中心的安全服务人员在接到求助信息后，立即赶往该单位总部了解实际感染情况。

疫情分析

初步诊断认为：WannaCry 病毒已在该机构全国范围内的生产系统中大面积传播和感染，短时间内病毒已在全国各地内迅速扩散，但仍处于病毒传播初期；其办公网环境、各地业务终端（专网环境）都未能幸免，系统面临崩溃，业务无法开展，事态非常严重。

进一步研究发现，该机构大规模感染 WannaCry 的原因与该机构业务系统架构存在一定的关联；用户系统虽然处于隔离网，但是存在隔离不彻底的问题；且存在某些设备、系统的协同机制通过 445 端口来完成的情况。

处置方案

安服人员第一时间建议全网断开 445 端口，迅速对中招电脑与全网机器进行隔离，形成初步处置措施。随后，针对该企业实际情况，制定了应急处置措施，提供企业级免疫工具并开始布防。该企业在全国范围内针对该病毒发送紧急通知，发布内部应急处理和避免感染病毒的终端扩大传播的公告。

5 月 16 日，病毒蔓延得到有效控制，染毒终端数量未继续增长，基本完成控制及防御工作。整个过程中，该企业和安全厂商全力协作配合，监控现场染毒情况、病毒查杀情况，最终使病毒得到有效控制。

（二） 某全国联网机构的应急响应处置方案

场景回顾

5 月 13 日上午 9:00 许，某大型政府机构接到安全厂商（360）工作人员打来的安全预警电话。在全面了解“永恒之蓝”病毒的爆发态势后，总局领导高度重视，立刻提高病毒应对等级。随机，安全公司在该机构的驻厂人员立即对该政府机构进行现场勘测。

疫情分析

检测结果显示：该机构在各地都布置了防火墙设备，并且 445 端口处于关闭状态，而且统一在全国各地布置了终端安全软件，但是仍有终端电脑存在未及时打补丁情况。尽管该机构尚未出现中毒电脑，但是系统仍然存在安全隐患、有重大潜在风险。

处置方案

应急指挥小组与安全公司驻厂工作人员协同明确应对方案：首先，优先升级总局一级控制中心病毒库、补丁库，确保补丁、病毒库最新；随后，开始手动升级省级二级控制中心，确保升级到最新病毒库和补丁库;对于不能级联升级的采用远程升级或者通知相关管理员手动更新；进一步对系统内各终端开展打补丁、升级病毒库、封闭端口工作。

最终，在病毒爆发 72 小时之内，该机构未出现一起感染事件。

（三） 某市视频监控系统应急响应处置方案

场景回顾

5 月 13 日凌晨 3:00 许，360 安全监测与响应中心接到某单位（市级）电话求助，称其在全市范围内的的视频监控系统突然中断了服务，大量监控设备断开，系统基本瘫痪。安服人员第一时间进行了远程协助，初步判断：猜测可能是监控系统的服务器遭到攻击感染了勒索病毒，进而感染了终端电脑，建议立即逐台关闭 Server 服务，并运行免疫工具，同时提取病毒样本进行分析。

疫情分析

安服人员现场实地勘察后发现：确实是该视频监控系统的服务器中招了，罪魁祸首正是 WannaCry，并且由于服务器中招已经使部分办公终端中招。溯源分析显示，“永恒之蓝”先在一台视频网络服务器上发作，然后迅速扩散，导致该市局视频专网终端及部分服务器（大约 20 多台）设备被病毒感染，数据均被加密，导致大量监控摄像头断开连接。断网将对当地的生产生活产生重要影响。

处置方案

安服人员首先在交换机上配置 445 端口阻塞策略；其次，分发勒索病毒免疫工具，在未被感染的终端和服务器上运行，防止病毒进一步扩散；另外，对于在线终端，第一时间推送病毒库更新和漏洞补丁库；由于部分被加密的服务器在被感染之前对重要数据已经做了备份，因此对这些服务器进行系统还原，并及时采取封端口、打补丁等措施，避免再次感染。

至 5 月 16 日，该机构的视频监控系统已经完全恢复正常运行，13 日凌晨被感染的终端及服务器以外，没有出现新的被感染主机。

（四） 某大企业提前预警紧急处置避免感染

场景回顾

5 月 13 日，某单位信息化部门工作人员看到了媒体报道的永恒之蓝勒索蠕虫事件。虽然该单位内部尚未发现感染案例，但考虑到自身没有全面部署企业级安全管理软件，所以对自身安全非常担忧。5 月 14 日上午 8:00，该单位紧急打电话向 360 安全监测与响应中心求助。

疫情分析

安服人员现场实际勘测后发现：该机构实际上已经部署了防火墙、上网行为管理等网关设备，但是内部没有使用企业级安全软件，使用的是个人版安全软件。所以难以在很短的时间内摸清内部感染情况。

处置方案

在安服人员协助下，该单位开始进行全面的排查，并采取必要的防护措施。在 NGFW 设备上开启控制策略，针对此次重点防护端口 445、135、137、138、139 进行阻断；同时，将威胁特征库、应用协议库立即同步至最新状态；在上网行为管理设备中更新应用协议库状态，部署相应控制策略，对“永恒之蓝勒索蠕虫”进行全网阻塞。

在病毒爆发 72 小时之内，该机构未出现一起感染事件。但是，在第一时间该机构无法准确判断自己的实际感染情况，造成恐慌。经过此次事件，该机构已经充分认识到企业级终端安全管理的重要性。

（五） 某新能源汽车厂商的工业控制系统被勒索

场景回顾

2017 年 6 月 9 日，某新能源汽车制造商的工业控制系统开始出现异常。当日晚上 19 时，该机构生产流水线的一个核心部分：动力电池生产系统瘫痪。这也就意味着所有电动车的电力电机都出不了货，对该企业的生产产生了极其重大的影响。该机构紧急向 360 安全监测与响应中心进行了求助。

实际上，这是永恒之蓝勒索蠕虫的二次突袭，而该企业的整个生产系统已经幸运的躲过了 5 月份的第一轮攻击，却没有躲过第二次。监测显示，这种第二轮攻击才被感染情况大量存在，并不是偶然的。

疫情分析

安服人员现场实际勘测发现：该机构的工业控制系统已经被 WannaCry 感染，而其办公终端系统基本无恙，这是因其办公终端系统上安装了比较完善的企业级终端安全软件。但在该企业的工业控制系统上，尚未部署任何安全措施。感染原因主要是由于其系统存在公开暴露在互联网上的接口。后经综合检测分析显示，该企业生产系统中感染 WannaCry 的终端数量竟然占到了整个生产系统电脑终端数量的 20%。

事实上，该企业此前早已制定了工业控制系统的安全升级计划，但由于其生产线上的设备环境复杂，操作系统五花八门（WinCE 终端、WinXP 终端及其他各种各样的终端都会碰到），硬件设备也新老不齐（事后测试发现，其流水线上最老的电脑设备有 10 年以上历史），所以部署安全措施将面临巨大的兼容性考验，所以整个工控系统的安全措施迟迟没有部署。

处置方案

因该厂商的生产系统中没有企业级终端安全软件，于是只能逐一对其电脑进行排查。一天之后也仅仅是把动力电池的生产系统救活。此后，从 6 月 9 日开始一直到 7 月底差不多用了两个月时间，该企业生产网里中的带毒终端才被全部清理干净。经过此次事件，该机构对工业控制系统安全性更加重视，目前已经部署了工控安全防护措施。经过测试和验证，兼容性问题也最终得到了很好的解决。

二、 混入升级通道的类 Petya 勒索病毒

病毒简介

类 Petya 病毒是 2017 年全球流行并造成严重破坏的一类勒索软件。具体包括 Petya 病毒，NotPetya 病毒和 BadRabbit 病毒（坏兔子）三种。从纯粹的技术角度看，类 Petya 病毒的三个子类并不属于同一木马家族，但由于其攻击行为具有很多相似之处，因此有很多安全工作者将其归并为一类勒索软件，即类 Petya 病毒。

Petya 病毒主要通过诱导用户下载的方式进行传播。病毒会修改中招机器的 MBR（主引导记录，Master Boot Record）并重启设备。重启后，被感染电脑中 MBR 区的恶意代码会删除磁盘文件索引（相当于删除所有文件） ，导致系统崩溃和文件丢失。

NotPetya 主要通过永恒之蓝漏洞进行初次传播。破坏方式同 Petya 相同（具体实现上的技术细节略有不同）。其后期版本还会通过局域网弱口令或漏洞进行二次传播。2017 年 6 月底爆发在乌克兰、俄罗斯多个国家的勒索软件攻击事件，实际上就是 NotPetya 的攻击活动。由于其行为与 Petya 及其类似，因此一开始被很对人误认为是 Petya 病毒攻击。由于 NotPetya 存在破坏性删除文件的行为，因此，即便支付了赎金，数据恢复的可能性也不大。关于 NotPetya 的真实攻击目的，目前业界也还有很多不同的看法。

BadRabbit 主要通过诱导用户下载进行初次传播。会通过一般的勒索软件常用的不对称加密算法加密用户文件，并修改 MBR 导致用户无法进入系统。同时，还会通过局域网弱口令或漏洞进行二次传播。

场景回顾

2017 年 6 月 27 日晚，乌克兰、俄罗斯、印度、西班牙、法国、英国以及欧洲多国遭受大规模“类 Petya”勒索病毒袭击，该病毒远程锁定设备，然后索要赎金。其中，乌克兰地区受灾最为严重，政府、银行、电力系统、通讯系统、企业以及机场都不同程度的受到了影响，包括首都基辅的鲍里斯波尔国际机场（Boryspil International Airport）、乌克兰国家储蓄银行（Oschadbank）、船舶公司（AP Moller-Maersk）、俄罗斯石油公司（Rosneft）和乌克兰一些商业银行以及部分私人公司、零售企业和政府系统都遭到了攻击。

疫情分析

根据事后的分析，此次事件在短时间内肆虐欧洲大陆，在于其利用了在乌克兰流行的会计软件 M.E.Doc 进行传播。这款软件是乌克兰政府要求企业安装的，覆盖率接近 50%。更为严重的是，根据安全机构的研究，M.E.Doc 公司的升级服务器在问题爆发前接近三个月就已经被控制。也就是说，攻击者已经控制了乌克兰 50%的公司的办公软件升级达三个月之久。类 Petya 攻击只是这个为期三个月的控制的最后终结，目的就是尽可能多的破坏掉，避免取证。至于在之前的三个月当中已经进行了什么活动，已无法得知了。

三、 服务器入侵攻击与响应典型案例

（一） 某关键基础设施的公共服务器被加密

病毒简介

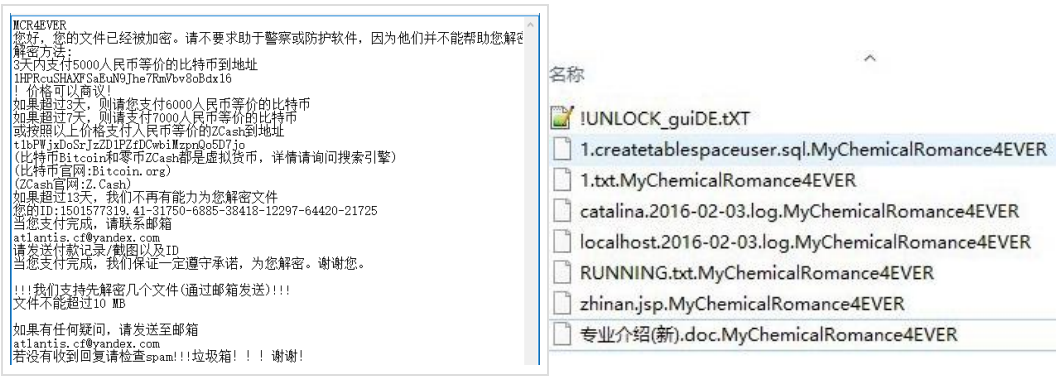
勒索病毒是个舶来品，无论是英文版的勒索信息，还是比特币这一赎金交付方式，都透漏着浓浓的国际化味道。而最近，360 威胁情报中心却发现一款国产化的勒索病毒。该病毒为国内黑客制造，并第一次以乐队名字 MCR 命名，即称该病毒为 MCR 勒索病毒。该病毒在 2017 年 7 月底首次出现，采用 python 语言编写。

该病毒加密文件后，文件扩展名会变为“.MyChemicalRomance4EVER”。而扩展名中的“My Chemical Romance”，其实是源自一支美国新泽西州的同名朋克乐队。该乐队成立于 2002 年，十一年后的 2013 年宣告解散。朋克这种充满了叛逆与不羁的音乐风格向来深受年轻人的喜爱。

该勒索软件的特点是：在加密的文件类型列表中，除了大量的文档类型外，还包括有比特币钱包文件和一些较重要的数据库文件。而另一个更大的特点则是，该木马不同于以往的勒索软件使用不对称加密算法，而是采用了 AES 对称加密算法，并且用于加/解密的密钥则是硬编码在脚本中的：“MyChemicalRomance4EVER_tkfy_lMCR”中。因为使用对称加密算法，并且密钥可以从脚本中获得。所以在不支付赎金的情况，被加密的文件资料也可以比较容易的被解密恢复。

场景回顾

2017 年 8 月 5 日，某公共服务系统单位的工作人员在对服务器进行操作时，发现服务器上的 Oracle 数据库后缀名都变为了“.MyChemicalRomance4EVER”，所有文件都无法打开。该 IT 人员怀疑自己的服务器被勒索软件进行了加密，因此向 360 安全监测与响应中心进行求助。



疫情分析

安全人员现场勘测发现，该公共服务系统感染的是 MCR 勒索病毒。该病毒名字起的很“朋克”,但传播方式却颇为老套,即伪装成一些对广大网民比较有吸引力的软件对外发布，诱导受害者下载并执行。比如我们现场截获并拿来分析的这个样本，就自称是一款叫做“VortexVPN”的 VPN 软件。除此之外，还有类似于 PornDownload、ChaosSet、BitSearch 等，基本都是广大网友都懂得的各种工具软件。

而与众不同的是，这款病毒竟然是用 Python 语言编写了木马脚本，然后再打包成一

个.exe 的可执行程序。首先，木马会判断自身进程名是否为 systern.exe。如果不是，则将自身复制为 C:\Users\Public\systern.exe 并执行。之后，木马释放 s.bat 批处理脚本，关闭各种数据库和 Web 服务及进程。接下来，就是遍历系统中所有文件并加密且留下勒索信息了。当然，为了避开敏感的系统文件，代码有意避开了“C:\Documents and Settings”和“C:\Windows”两个目录。最终木马会调用系统的 wevtutil 命令，对系统日志中的“系统”、“安全”和“应用程序”三部分日志内容进行清理，并删除自身，以求不留痕迹。

处置方案

安服人员发现该勒索软件程序写的有漏洞，可直接利用 360 解密工具恢复数据。因此，在未向黑客支付一分钱的前提下，360 帮助该单位成功的恢复了所有被加密的文件。建议该企业员工：不要从不明来源下载程序；安装杀毒软件并开启监控；更不要相信所谓外挂、XX 工具、XX 下载器一类的程序宣称的杀软误报论。

（二） 某云平台服务上托管的服务器被加密

病毒简介

2016 年 2 月，在国外最先发现的一款能够通过 Java Applet 传播的跨平台（Windows、MacOS）恶意软件 Crysis 开始加入勒索功能，并于 8 月份被发现用于攻击澳大利亚和新西兰的企业。Crysis 恶意软件甚至能够感染 VMware 虚拟机，还能够全面收集受害者的系统用户名密码，键盘记录，系统信息，屏幕截屏，聊天信息，控制麦克风和摄像头，现在又加入了勒索功能，其威胁性大有取代 TeslaCrypt 和对手 Locky 勒索软件的趋势。

Crysis 勒索软件的可怕之处在于其使用暴力攻击手段，任何一个技能娴熟的黑客都可以使用多种特权升级技术来获取系统的管理权限，寻找到更多的服务器和加密数据来索取赎金。主要攻击目标包括 Windows 服务器（通过远程爆破 RDP 账户密码入侵）、MAC、个人 PC 电脑等。该勒索软件最大特点是除了加密文档外，可执行文件也加密，只保留系统启动运行关键文件，破坏性极大。

场景回顾

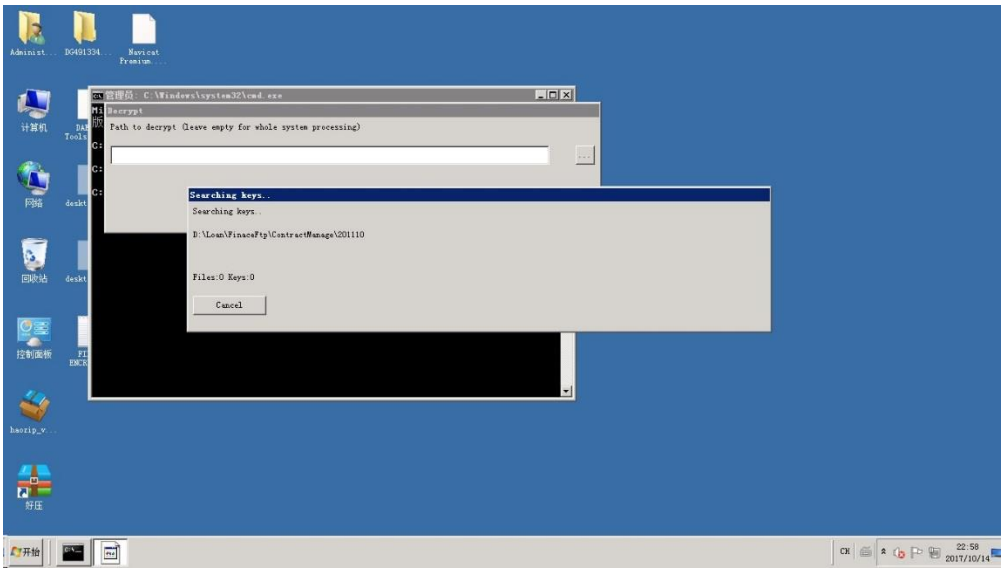
2017 年 10 月 15 日，某云平台服务商，发现托管在自己机房的用户服务器上的数据均被加密，其中包含大量合同文件、财务报表等文件都无法打开。该 IT 人员怀疑自己的服务器被勒索软件进行了加密，因此向 360 安全监测与响应中心进行求助。

疫情分析

安服人员现场实际勘测发现：该机构的公共服务器被暴露在公网环境中，并且使用的是弱密码；黑客通过暴力破解，获取到该服务器的密码，并使用远程登录的方式，成功的登录到该服务器上。黑客在登陆服务器后，手动释放了 Crysis 病毒。

处置方案

因其服务器上存储着大量重要信息，其对企业发展产生至关重要的作用，所以该机构选择支付赎金，成功恢复所有被加密的文档。下图为该机构支付赎金的解密过程示意图。



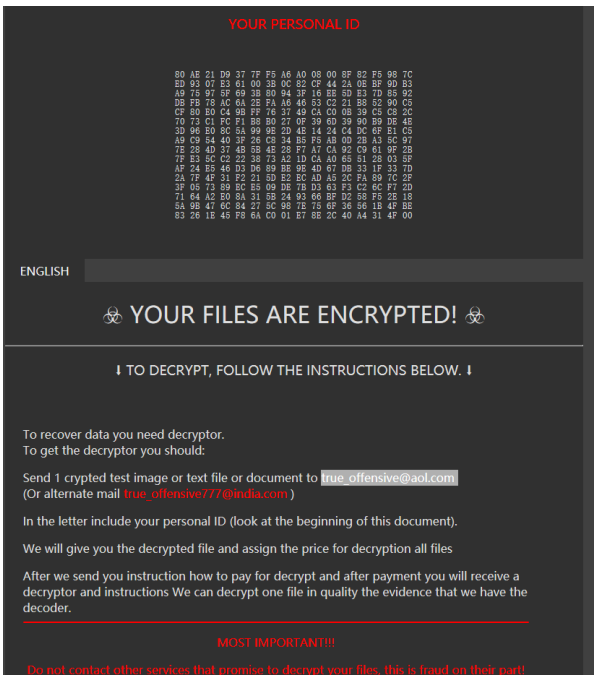
（三） 江苏某大型房地产企业服务器被加密

病毒简介

GlobeImposter 病毒最早出现是在 2016 年 12 月份左右，第一个版本存在漏洞，可解密，但后期版本只能支付赎金解密。2017 年 5 月份出现新变种，7、8 月初进入活跃期。该病毒从勒索文档的内容看跟 Globe 家族有一定的相似性。

场景回顾

2017 年 7 月 12 日，某大型房地产企业发现自己的服务器上数据库被加密，该企业的 IT 技术人员担心受到责罚，隐瞒实际情况未上报。10 月 18 日，该企业领导在查询数据时，发现服务器上的数据均已经被加密，且长达数月之久，意识到自己内部员工无法解决此问题，于是向 360 安全监测与响应中心进行求助。



疫情分析

安全厂商人员实际勘测发现：攻击者主要是使用带有恶意附件的邮件进行钓鱼攻击。受害者在点击了附件中的 VBS 脚本文件，即 GlobeImposter 病毒后，VBS 脚本文件负责从网络上下载勒索软件，通过 rundll32.exe 并带指定启动参数进行加载。样本执行后在内存中解密执行，解密后才是真正的功能代码。该勒索软件会对系统中的文件进行扫描，对磁盘上指定类型的文件进行加密，被样本加密后的文件后缀为.thor。样本加密文件所使用的密钥为随机生成，加密算法为 AES-CBC-256，用样本内置的 RSA 公钥，通过 RSA-1024 算法对随机生成的 AES 加密密钥进行加密处理。

处置方案

由于距离加密时间太久，黑客密钥已经过期，被加密的数据和文件无法恢复，给该企业造成了大量的财产损失。

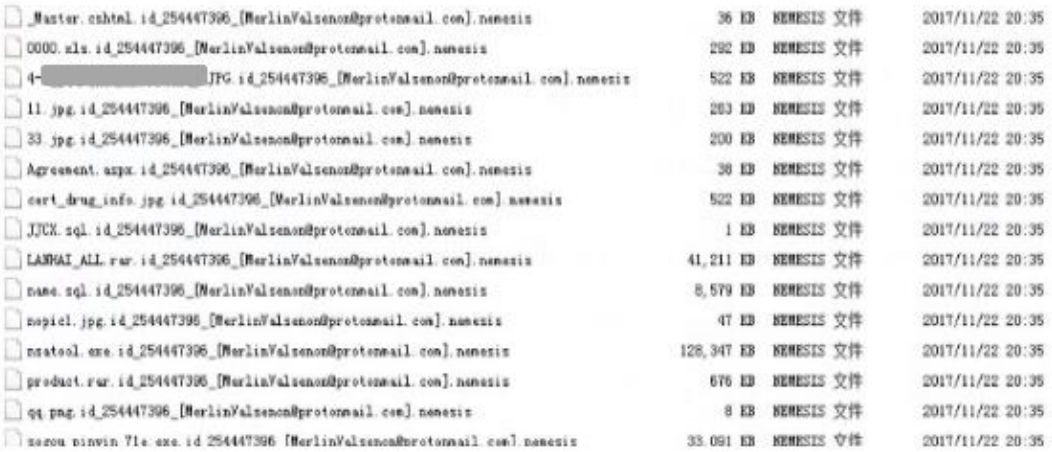
（四） 某市政务系统的服务器被加密

病毒简介

CryptON 病毒最早出现在 2016 年 12 月，该病毒是一系列 Cry9，Cry36，Cry128，Nemsis 等勒索病毒的统称，早期版本可通过对比加密和未加密的文件来暴力运算破解获取解密密钥，后期版本无法解密。

场景回顾

2017 年 11 月 26 日，某市政务系统被发现其服务器上的数据库、业务系统不能使用，文件内容无法存储，所有文件都打不开了。该机构紧急向 360 安全监测与响应中心进行求助。



疫情分析

安服人员现场勘测发现：该系统感染的勒索软件为 CryptON 病毒。攻击者首先使该机构的 IT 运维人员的电脑感染木马程序，之后在 IT 人员登录服务器时窃取了账号和密码，再通过窃得的帐号密码远程登录到服务器上，最后释放勒索软件。

处置方案

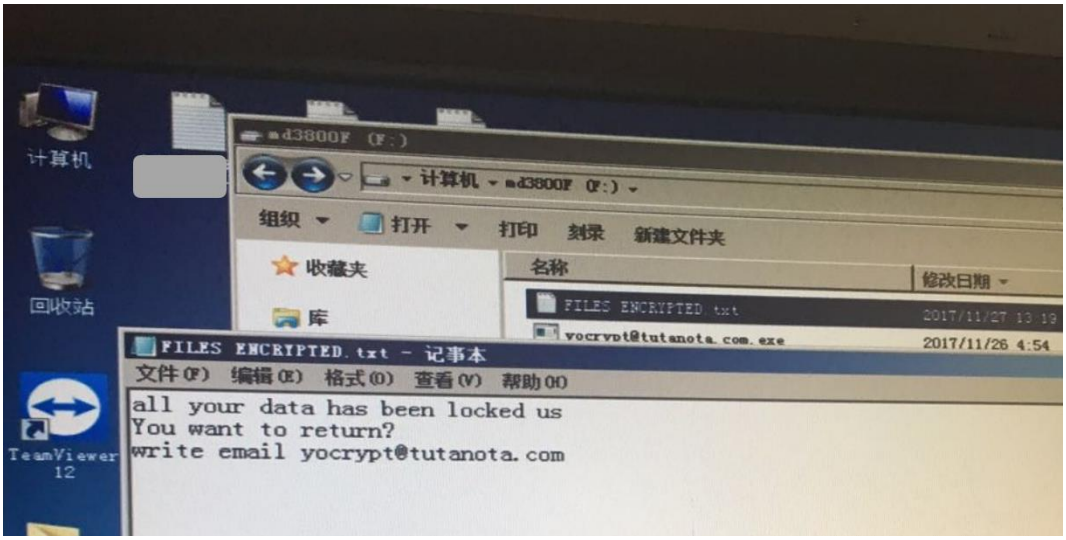
由于 CryptON 病毒的不可解性，要想恢复数据文件，只能支付赎金。该机构在得知只有支付赎金才能解密的情况下，放弃了数据恢复，直接重装了系统，并加强了对运维人员电脑的监控与管理。

（五） 某知名咨询公司的两台服务器被加密

场景回顾

2017 年 11 月，某知名咨询公司发现其服务器上所有文件被加密，怀疑自己感染了勒索病毒，紧急向 360 安全监测与响应中心进行求助。

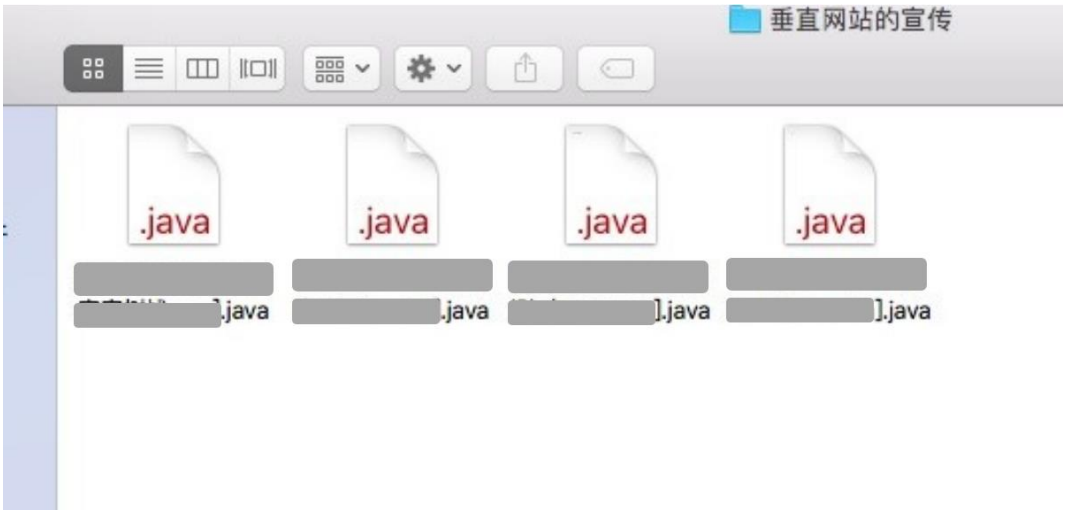
根据该企业 IT 人员介绍：被锁定的服务器一共有两台，一台是主服务器，存储了大量该咨询公司为国内外多家大型企业提供咨询服务的历史资料，十分珍贵；而另一台是备份服务器，主要是出于安全考虑，用于备份主服务器资料。两台设备同时被锁，意味着备份数据已不存在；同时，目前只要将 U 盘插入服务器，U 盘数据也会被立即加密。在发现服务器中毒后，他们已经对当日与服务器连接过的所有办公终端进行了排查，未发现有任何电脑的中毒迹象。



疫情分析

安服人员现场勘测发现：该企业未曾部署过任何企业级安全软件或设备，其服务器上安装的是某品牌免费的个人版安全软件，所有 200 余台办公电脑安装的也都是个人版安全软件，且未进行过统一要求。中招服务器升级了 5 月份的漏洞补丁，后续月份的补丁都没有升级过；同时，其内部办公终端与服务器之间也没有进一步的安全防护措施，仅仅靠用户名和密码来进行验证。

经确认，该公司两台服务器感染的勒索软件为 Crysis 的变种，文件被加密后的后缀名为为.java，目前这个勒索软件无解。这个家族有一个特点就是针对的都是服务器，攻击的方式都是通过远程桌面进去，爆破方式植入。而之所以会发生 U 盘插入后数据全部被加密的情况，是因为服务器上的勒索软件一直没有停止运行。



处置方案

在安服人员的远程指导下，该企业 IT 人员首先断开了服务器的网络链接；随后卸载了服务器上已经安装的安全软件。这一步的处置措施还是十分必要的，因为一旦安全软件发挥作用杀掉了勒索软件，那么对于已经感染勒索软件的电脑来说，有可能导致勒索软件被破坏，被加密的数据无法恢复。

因被加密的两台服务器上存储着该企业及其重要的资料，且无其他备份。所以该企业在得知无法解密的情况下，选择向攻击者支付赎金，进而文件恢复。

特别的是，攻击者显然是对该企业的网络服务系统进行了长期、细致的研究，同时攻击主服务器和备份服务器是经过精心设计和周密考虑的。

第五章　2018 年勒索软件趋势预测

2017 年，勒索软件的攻击形式和攻击目标都已经发生了很大的变化。本章将给出我们对 2018 年勒索软件攻击趋势的预测。

一、 整体态势

（一） 勒索软件的质量和数量将不断攀升

2017 年勒索软件在暗网上获得规模性增长，相关产品销售额高达 623 万美元，是 2016 年的 25 倍，而一款 DIY 勒索软件售价从 50 美分到 3000 美元不等，中间价格一般在 10.5 美元左右。2017 年 7 月，根据谷歌、加州大学圣地亚哥分校和纽约大学坦登工程学院的研究人员联合发布的一份报告显示，在过去两年，勒索软件已迫使全球受害者累计支付了超过 2500 万美元的赎金。

无论对制作者还是使用者而言，影响广泛、物美价廉、门槛低获利快的勒索软件都是当前比较“靠谱”的获利方式，因此，制作者会不断采用新的技术来提升勒索软件的质量，使用者则会通过使用更多数量的勒索软件来广开财路。

（二） 勒索软件会越来越多的使用免杀技术

成功进驻系统并运行是敲诈勒索的前提。因此，为了获得更大的经济利益，在勒索软件的制作、传播过程中，首先要做的就是“自我保护”，即躲避杀毒软件的查杀。以 Petrwrap 为例，它在 6 月底在欧洲引发大面积感染，俄罗斯、乌克兰、波兰、法国、意大利、英国及德国也被其感染。但根据《黑客新闻》6 月 27 日报道，最近的 VirusTotal 扫描显示，61 款杀毒软件当中只有 16 款能够成功检测到该病毒。

在各界充分认识到勒索软件引发的可怕后果的前提下，攻击者必然会在 2018 年趁热打铁，充分利用这种担心和恐慌获取更多的赎金，不断使用更新的技术和更多的变种来突破杀毒软件的防线将成为必然。

二、 攻击特点

（一） 勒索软件的传播手段将更加多样化

相比于个人受害者，组织机构更有可能支付大额赎金，而感染更多设备从而给组织机构造成更大的损失是提升赎金支付可能性的重要手段。因此，除了通过更多的漏洞、更隐蔽的通道进行原始传播，勒索软件的自我传播能力也将会被无限的利用起来，类似 WannaCry、类 Petya、坏兔子等以感染的设备为跳板，然后利用漏洞进行横向移动，攻击局域网内的其他电脑，形成“一台中招，一片遭殃”的情况将会在 2018 年愈演愈烈。针对各企业对于软件供应链的管理弱点，通过软件供应链通道进行原始传播在未来一年有很大概率被再次利用。

（二） 勒索软件的静默期会不断延长

震惊全球的 WannaCry 的大规模爆发开始于 5 月 12 日（星期五）下午，周末正好是组织机构使用电脑的低峰期，这给安全厂商和组织机构应急处置以免蠕虫快速扩散提供了足够

的缓冲时间，也让攻击者失去了获得更多赎金的可能。

为了避免“亏本”，获得更多的赎金，未来的勒索软件会在获得更多“勒索筹码”之前尽可能隐蔽自己，一边延长自己的生命周期，一边选择合适的时间发作，让安全厂商合组织机构“措手不及”。

事实上，“永恒之石”病毒就是很好的佐证，它采用了 7 个被影子经纪人黑客团伙放出的据称是 NSA 开发的漏洞利用工具，被称为可突然袭击的“世界末日”级蠕虫。一旦进入系统，它会下载 Tor 的私有浏览器，发送信号到其隐藏服务器，然后进入等待状态，24 小时内没有任何动作，之后服务器便会响应，开始下载和自我复制动作。目前为止，“永恒之石”依然静静地传播和感染更多计算机中，有鉴于其隐秘本质，有多少台电脑已经被“永恒之石”感染尚未可知，它会被武器化成什么样子也还不明朗。

三、 攻击目标

（一） 勒索软件攻击的操作系统类型将越来越多

目前，绝大多数勒索软件攻击的都是 Windows 操作系统，但针对 MacOS 的勒索软件 MacRansom 已经出现在暗网中；针对 Linux 服务器的勒索软件 Rrebus 也已经造成了巨大的损失；针对安卓系统的勒索软件也在国内网络中出现。但这也许只是开始，越自认为“安全”、越小众的系统，防护能力可能越弱，一旦被攻破，支付赎金的可能性也就越大，因此，勒索软件不会放过任何一个系统。

（二） 勒索软件定向攻击能力将更加突出

2017 年影响面最大的两个勒索软件，WannaCry（永恒之蓝）攻击者收到的赎金可能不足 15 万美元，类 Petya 的攻击者更是只拿到可怜的 11181 美元赎金，但针对 Linux 服务器的勒索软件 Rrebus 看似名不见经传，却轻松从韩国 Web 托管公司 Nayana 收取 100 万美元赎金，仅此一家缴纳的赎金就是永恒之蓝从全球获得赎金的 7 倍之多。

由此可见，针对特定行业、关键业务系统的敲诈勒索更容易成功，更容易获得高额赎金，这将让以敲诈勒索为核心目的的攻击者逐渐舍弃华而不实的广撒网式攻击，将重心转移到发动更有针对性的定向攻击。

四、 造成损失

（一） 经济损失与赎金支付都将持续升高

安全意识培训公司 KnowBe4 曾估测：WannaCry 的大规模爆发，在其前 4 天里，就已经造成了 10 亿美元的经济损失。而随着勒索软件技术的进一步成熟和平台化，勒索软件的攻击也将会更加频繁，攻击范围更加广泛，造成的经济损失也会不断攀升。

美国网络安全机构 Cybersecurity Ventures 在 2017 年 5 月发布的报告中预测，2017 年勒索软件攻击在全球造成的实际损失成本将达到 50 亿美元，预计 2019 年的攻击损失可能升至 115 亿美元。而相关数据还显示，勒索软件在 2015 年给全球造成的实际损失仅为 3.25 亿美元。

以类 Petya 勒索病毒为例，根据全球各地媒体的相关报道，仅仅是它给 4 家全球知名公司造成的经济损失就已经远超 10 亿美金，如下表所示。

公司名称	造成损失	影响范围
默克集团 （美国医药巨头）	3.1 亿美元	全球营销、研发以及销售持续一周受到影响，邮件处于瘫痪状态，7 万名员工被禁用电脑。
Maersk 集团 （全球最大航运公司）	3 亿美元	集团下属航运公司、集装箱码头公司和德高货运受到严重影响。
FedEx 公司 （全球最大快递运输公司之一）	3 亿美元	TNT 配送网络系统遭受重创。
利洁时集团 （全球最大家用清洁用品公司）	1 亿英镑	破坏公司多个市场的产品生产与发售，世界各地工厂的订单、支付和货运受到影响。

表格 3　知名企业遭到的重大损失情况

经济损失的不断提高也将促使更多的政企机构向攻击者支付赎金。预计到 2018 年，攻击者在不断提升勒索软件自身能力的同时，也将进一步锁定风险承受能力较差的攻击目标实施攻击，并在加密数据基础上使用更多的威胁方式，例如不支付赎金就将关键信息公开在互联网上等，迫使组织机构不得不缴纳高额的赎金。

鉴于很多组织机构即便承受巨额损失也没有交纳赎金，将来攻击者还可能会开展“针对性服务”，让感染者支付其“能力范围内”的赎金。例如攻击者就与 Nayana 进行了漫长的谈判，将赎金从最初的 440 万美元降至 100 万美元，才出现了 2017 年的单笔最高赎金事件。

所以，未来迫不得已支付赎金的政企机构中招者会越来越多，也会出现更多类似韩国 Web 托管公司 Nayana 支付 100 万美元赎金的大户，攻击者获得的赎金总额必将持续升高。

（二）　通过支付赎金恢复文件的成功率将大幅下降

对于中招的组织机构而言，在尝试各种方式解密被勒索软件加密的数据无果后，即便想要通过支付赎金的方式来解决问题，其成功率也将大幅下降。其主要原因倒不是勒索者的信用会快速下降，而是很多现实的网络因素可能会大大限制你支付赎金恢复文件的成功率。

首先，你可能“没钱可付”，绝大多数的勒索软件均以比特币为赎金支付方式，但 9 月底比特币在中国已经全面停止交易了。

其次，你也可能“来不及付”，交纳赎金一般是有时间限制的，一般为 1-2 天，但国产勒索病毒 Xiaoba 只给了 200 秒的反应时间。

第三，你即便通过各种方式支付了赎金，也可能“无法提供付款证明”给攻击者，因为很多勒索软件要求受害者向特定邮箱发送支付证明，黑客才会为其解锁，但越来越多的邮件供应方无法忍受攻击者通过其平台非法获利，而会第一时间将其邮箱关停。

第六章　勒索软件防御技术新趋势

一、 个人终端防御技术

（一） 文档自动备份隔离保护

文档自动备份隔离技术是 360 独创的一种勒索软件防护技术。这一技术在未来一两年内可能会成为安全软件反勒索技术的标配。

鉴于勒索软件一旦攻击成功往往难以修复，而且具有变种多，更新快，大量采用免杀技术等特点，因此，单纯防范勒索软件感染并不是“万全之策”。但是，无论勒索软件采用何种具体技术，无论是哪一家族的哪一变种，一个基本的共同特点就是会对文档进行篡改。而文档篡改行为具有很多明显的技术特征，通过监测系统中是否存在文档篡改行为，并对可能被篡改的文档加以必要的保护，就可以在相当程度上帮助用户挽回勒索软件攻击的损失。

文档自动备份隔离技术就是在这一技术思想的具体实现，360 将其应用于 360 文档卫士功能模块当中。只要电脑里的文档出现被篡改的情况，它会第一时间把文档自动备份在隔离区保护起来，用户可以随时恢复文件。无论病毒如何变化，只要它有篡改用户文档的行为，就会触发文档自动备份隔离，从而使用户可以免遭勒索，不用支付赎金也能恢复文件。

360 文档卫士的自动备份触发条件主要包括亮点：一、开机后第一次修改文档；二、有可疑程序篡改文档。当出现上述两种情况时，文档卫士会默认备份包括 Word、Excel、PowerPoint、PDF 等格式在内的文件，并在备份成功后出现提示信息。用户还可以在设置中选择添加更多需要备份的文件格式。比如电脑里的照片非常重要，就可以把 jpg 等图片格式加入保护范围。

此外，360 文档卫士还集合了“文件解密”功能，360 安全专家通过对一些勒索软件家族进行逆向分析，成功实现了多种类型的文件解密，如 2017 年出现的“纵情文件修复敲诈者病毒”等。如有网友电脑已不慎中招，可以尝试通过“文档解密”一键扫描并恢复被病毒加密的文件。

（二） 综合性反勒索软件技术

与一般的病毒和木马相比，勒索软件的代码特征和攻击行为都有很大的不同。采用任何单一防范技术都是不可靠的。综合运用各种新型安全技术来防范勒索软件攻击，已经成为一种主流的技术趋势。

下面就以 360 安全卫士的相关创新功能来分析综合性反勒索软件技术。相关技术主要包括：智能诱捕、行为追踪、智能文件格式分析、数据流分析等，具体如下。

智能诱捕技术是捕获勒索软件的利器，其具体方法是：防护软件在电脑系统的各处设置陷阱文件；当有病毒试图加密文件时，就会首先命中设置的陷阱，从而暴露其攻击行为。这样，安全软件就可以快速无损的发现各类试图加密或破坏文件的恶意程序。

行为追踪技术是云安全与大数据综合运用的一种安全技术。基于 360 的云安全主动防御体系，通过对程序行为的多维度智能分析，安全软件可以对可疑的文件操作进行备份或内容检测，一旦发现恶意修改则立即阻断并恢复文件内容。该技术主要用于拦截各类文件加密

和破坏性攻击，能够主动防御最新出现的勒索病毒。

智能文件格式分析技术是一种防护加速技术，目的是尽可能的降低反勒索功能对用户体验的影响。实际上，几乎所有的反勒索技术都会或多或少的增加安全软件和电脑系统的负担，相关技术能否实用的关键就在于如何尽可能的降低其对系统性能的影响，提升用户体验。360 研发的智能文件格式分析技术，可以快速识别数十种常用文档格式，精准识别对文件内容的破坏性操作，而基本不会影响正常文件操作，在确保数据安全的同时又不影响用户体验。

数据流分析技术，是一种将人工智能技术与安全防护技术相结合的新型文档安全保护技术。首先，基于机器学习的方法，我们可以在电脑内部的数据流层面，分析出勒索软件对文档的读写操作与正常使用文档情况下的读写操作的区别；而这些区别可以用于识别勒索软件攻击行为；从而可以在“第一现场”捕获和过滤勒索软件，避免勒索软件的读写操作实际作用于相关文档，从而实现文档的有效保护。

二、 企业级终端防御技术

（一） 云端免疫技术

如本报告第三章相关分析所述，在国内，甚至全球范围内的政企机构中，系统未打补丁或补丁更新不及时的情况都普遍存在。这并非是简单的安全意识问题，而是多种客观因素限制了政企机构对系统设备的补丁管理。因此，对无补丁系统，或补丁更新较慢的系统的安全防护需求，就成为一种“强需求”。而云端免疫技术，就是解决此类问题的有效方法之一。这种技术已经被应用于 360 的终端安全解决方案之中。

所谓云端免疫，实际上就是通过终端安全管理系统，由云端直接下发免疫策略或补丁，帮助用户电脑做防护或打补丁；对于无法打补丁的电脑终端，免疫工具下发的免疫策略本身也具有较强的定向防护能力，可以阻止特定病毒的入侵；除此之外，云端还可以直接升级本地的免疫库或免疫工具，保护用户的电脑安全。

需要说明的事，云端免疫技术只是一种折中的解决方案，并不是万能的或一劳永逸的，未打补丁系统的安全性仍然比打了补丁的系统的安全性有一定差距。但就当前国内众多政企机构的实际网络环境而诺言，云端免疫不失为一种有效的解决方案。

（二） 密码保护技术

针对中小企业网络服务器的攻击，是 2017 年勒索软件攻击的一大特点。而攻击者之所以能够渗透进入企业服务器，绝大多数情况都是因为管理员设置的管理密码为弱密码或帐号密码被盗。因此，加强登陆密码的安全管理，也是一种必要的反勒索技术。

具体来看，加强密码保住主要应从三个方面入手：一是采用弱密码检验技术，强制网络管理员使用复杂密码；二是采用反暴力破解技术，对于陌生 IP 的登陆位置和登陆次数进行严格控制；三是采用 VPN 或双因子认证技术，从而使攻击者即便盗取了管理员帐号和密码，也无法轻易的登陆企业服务器。

第七章　给用户的安全建议

一、 个人用户安全建议

对于普通用户，我们给出以下建议，以帮助用户免遭勒索软件的攻击：

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，一旦电脑被勒索软件感染，可以通过 360 反勒索服务申请赎金赔付，以尽可能的减小自身经济损失。

二、 企业用户安全建议

1） 提升新兴威胁对抗能力

传统基于合规的防御体系对于勒索软件等新兴威胁的发现、检测和处理已经呈现出力不从心的状态。而通过对抗式演习，从安全的技术、管理和运营等多个维度出发，对企业的互联网边界、防御体系及安全运营制度等多方面进行仿真检验，可以持续提升企业对抗新兴威胁的能力。

2） 及时给办公终端和服务器打补丁修复漏洞，包括操作系统以及第三方应用的补丁。

3） 如果没有使用的必要，应尽量关闭不必要的常见网络端口，比如：445、3389 等。

4） 企业用户应采用足够复杂的登录密码登陆办公系统或服务器，并定期更换密码。

5） 对重要数据和文件及时进行备份。

6） 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，如有远程家中办公电脑也需要定期进行病毒木马查杀。

附录 1　2017 年勒索软件重大攻击事件

一、 MongoDB 数据库被窃取

2017 年 1 月，GDI 基金会的联合创始人 Victor Gevers 警告说，MongoDB（分布式文档存储数据库）在野外安装的安全性很差。这位安全专家发现了 196 个 MongoDB 实例，这些实例可能被骗子们窃取并被勒索赎金。据悉，有多个黑客组织参与了此次攻击，他们劫持服务器后，用勒索程序替换了其中的正常内容。外媒称，大多数被攻破的数据库都在使用测试系统，其中一部分可能包含重要生产数据。部分公司最终只得支付赎金，结果发现攻击者其实根本没有掌握他们的数据，又被摆了一道。

二、 知名搜索引擎 Elasticsearch 被勒索敲诈

2017 年 1 月，数百台存在安全缺陷的 Elasticsearch 服务器在几个小时之内遭到了勒索攻击，并被擦除了服务器中的全部数据。安全研究专家 Niall Merrigan 估计，目前已经有超过 2711 台 Elasticsearch 服务器遭到了攻击。

此次攻击活动与之前的勒索攻击一样，攻击者入侵了 Elasticsearch 服务器之后会将主机中保存的数据全部删除，当服务器所有者向攻击者支付了赎金之后他们才可以拿回自己的数据。因此，安全研究专家建议广大 Elasticsearch 服务器的管理员们在官方发布了相应修复补丁之前暂时先将自己的网站服务下线，以避免遭到攻击者的勒索攻击。

三、 港珠澳桥资料遭黑客加密勒索

2017 年 5 月，港珠澳大桥一地盘办公室，其电脑伺服器遭黑客的勒索软件攻击，而且被加密勒索。据星岛日报消息，香港路政署表示，今年 3 月 2 日，接到驻工地工程人员通知，指驻工地工程人员写字楼内的伺服器遭勒索软件(Ransomware)攻击，伺服器内的部份档案遭加密勒索。经调查后发现，驻工地工程人员已即时切断有关伺服器的网络连线，并向警方求助。香港路政署已要求驻工地工程人员及承建商，更新其写字楼内所有电脑的网络保安软件，以加强网络保安。有关事件并没有影响该合约的工程进度。据悉，受害公司为奥雅纳工程顾问公司，有传黑客要求付钱才将档案还原。

四、 WannaCry 在全球大规模爆发

2017 年 5 月，WannaCry 在全球大规模爆发。该恶意软件会扫描电脑上的 TCP 445 端口(Server Message Block/SMB)，以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，然后要求以比特币的形式支付赎金。2017 年 5 月 12 日，WannaCry 勒索病毒已经攻击了近 100 个国家，其中包括英国、美国、中国、俄罗斯、西班牙和意大利等。2017 年 5 月 14 日，WannaCry 勒索病毒出现了变种：WannaCry 2.0，取消 Kill Switch 传播速度或更快。截止 2017 年 5 月 15 日，WannaCry 已造成至少有 150 个国家受到网络攻击，已经影响到金融，能源，医疗等行业，造成严重的危机管理问题。中国部分 Window 操作系统用户也遭受感染，校园网用户首当其冲，受害严重，大量实验室数据和毕业设计被锁定加密。

360 互联网安全中心于 2017 年 5 月 12 日中午 13 点 44 分，截获了 WannaCry 的首个攻击样本，是世界上最早截获该病毒的公司。而在随后的短短几个小时内，就有包括中国、英国、美国、德国、日本、土耳其、西班牙、意大利、葡萄牙、俄罗斯和乌克兰等国家被报告遭到了 WannaCry 的攻击，大量机构设备陷入瘫痪。

截至 2017 年 5 月 13 日 20:00 时，360 互联网安全中心便已截获遭 WannaCry 病毒攻击的我国政企机构 IP 地址 29372 个。而从后续国内外媒体披露的情况来看，在全球范围内遭受此次 WannaCry 病毒攻击的国家已超过了 100 个。

五、 欧洲大规模爆发类 Petya 病毒

2017 年 6 月，俄罗斯最大石油企业 Rosneft 等超过 80 家俄罗斯和乌克兰公司遭到网络袭击，黑客向能源和交通等行业企业、银行业和国家机构等植入病毒并封锁电脑，相关用户被要求支付 300 美元的加密式数字货币以解锁电脑。攻击者通过感染乌克兰流行会计软件（M.E.Doc） 更新服务器，向用户推送包含病毒的软件更新。用户更新软件就会感染病毒，给企业系统和数据造成惨重损失。

乌克兰受到的攻击最为严重，乌克兰政府官员报告称，乌克兰电网、银行和政府部门的网络系统遭到严重入侵。乌克兰副总理 Pavlo Rozenko 在其推特上发布了一张黑暗的电脑屏幕的照片，并称政府总部的电脑系统因受到攻击已经关闭。此外病毒攻击已经波及到英国、俄罗斯等欧洲多国的机场、银行和大型企业的网络系统。法国建筑巨头圣戈班、俄罗斯石油公司(Rosneft)、丹麦货运公司马士基(Maersk)、西班牙食品巨头 Mondelez 随后相继自曝受网络袭击。此外，挪威国家安全机构、西班牙的企业都惨遭上述黑客攻击。

六、 多国正在遭遇彼佳勒索病毒袭击

2017 年 6 月，乌克兰，俄罗斯，印度，西班牙，法国，以及英国欧洲多国正在遭遇彼佳勒索病毒袭击；政府，银行，电力系统，通讯系统，企业以及机场都不同程度的受到了影响。此次黑客使用的是彼佳勒索病毒的变种 Petwarp，使用的攻击方式和 WannaCry 相同。彼佳和传统的勒索软件不同，不会对电脑中的每个文件都进行加密，而是通过加密硬盘驱动器主文件表（MFT），使主引导记录（MBR）不可操作，通过占用物理磁盘上的文件名，大小和位置的信息来限制对完整系统的访问，从而让电脑无法启动。如果想要恢复，需要支付价值相当于 300 美元的比特币。

七、 韩国网络托管公司 Nayana 再遭勒索

2017 年 6 月，韩国 IDC 旗下的一家网络托管公司 Nayana 遭遇了勒索软件攻击，其 153 台 Linux 服务器被攻陷。最终，该公司同意向攻击者支付价值 100 万美元（约合 683 万人民币）的比特币才获得了“救赎”。

不过，Nayana 似乎并没有在付出高额经济代价之后吸取教训。没有修补漏洞或使用弱密码的 Linux 服务器再次成为了勒索软件的攻击目标。Nayana 在本月 8 日宣布，9 台托管于 Nayana 的服务器受到了勒索软件的攻击。攻击者并没有注明详细的赎金数额，但留下了联系方式。这和 6 月份的攻击很相似，攻击者似乎给了 Nayana 一个“讨价还价”的余地。

八、 Spora 窃取凭据并记录您输入的内容

2017 年 8 月，勒索恶意软件已经升级，使其能够窃取浏览信息并记录受感染 PC 的击键。Spora 勒索软件是文件锁定恶意软件最常见的家族之一，它似乎紧随着 Cerber 的脚步，获得了从比特币钱包中窃取密码和货币的能力。通过窃取受害者的证件，罪犯确保了双重发薪日，因为他们不仅可以通过勒索赎金赚钱，还可以在地下论坛上向其他犯罪分子出售被盗的信息。

从本质上讲，Spora 在获得窃取数据的能力之前已经是一个强大的勒索软件。Deep Instinct 的安全研究人员发现了这个新的变种。这个 Spora 版本是在 8 月 20 日开始的 48 小时内发布的，它是通过一个网络钓鱼攻击传播的，目标是一个 Word 文档，声称是发票。为了查看文件的内容，要求用户启用一个 Windows 脚本文件，它允许文档放弃其恶意负载。这是 Spora 第一次嵌入到文档中，而不是从 Web 服务器中提取。

九、 勒索病毒坏兔子来袭俄乌等国中招

2017 年 10 月 24 日，一种名叫“坏兔子（Bad Rabbit）”的新型勒索病毒从俄罗斯和乌克兰最先开始发动攻击，并且在东欧国家蔓延。俄罗斯最大的新闻通讯社之一国际文传通讯社、《丰坦卡报》网站及另一家媒体 24 日也遭“坏兔子”病毒攻击，国际文传通讯社发稿受到影响。乌克兰敖德萨国际机场一些航班被推迟。

乌克兰国家机构和基础设施是此次攻击的主要目标，奥德萨机场、基辅地铁和乌克兰基础设施部门都受到了此次大规模网络攻击的影响。俄罗斯网络安全厂商卡巴斯基实验室 10 月 25 日报告，“坏兔子”已经攻击了位于俄罗斯、乌克兰、土耳其和德国境内的约 200 家公司的计算机网络。其中，大部分目标位于俄罗斯境内。

十、 通用汽车制造中心遭勒索软件攻击

斯普林希尔（Spring Hill），是美国田纳西州下辖的 95 个县之一，也是重要的汽车制作中心，通用汽车的土星汽车制造工厂所在地。2017 年 11 月 3 日晚些时候，这座城市遭遇了勒索软件的攻击。Spring Hill 的发言人杰米 佩奇（Jamie Page）表示，当时一名政府雇员打开了一封不明来源的电子邮件，这一举措导致 Spring Hill 城市管理系统的服务器被劫持、服务器文件被加密。一份赎金票据显示在计算机屏幕上，攻击者的赎金需求为 25 万美元。Spring Hill 政府方面并没有向攻击者支付赎金，而是下令其 IT 部门使用备份文件来重建数据库。攻击导致众多城市服务被迫中断，比如在线支付功能，包括水电气费、交通罚款费以及证书办理，包括营业执照、食品安全许可证等。

附录 2　WannaCry 攻击技术详解

一、WannaCry 的蠕虫攻击

（一） 针对 445 端口的扫描

作为一款蠕虫病毒，WannaCry 在感染某台电脑后，便会对周边联网的其他电脑设备发起自动攻击。具体的攻击步骤是：

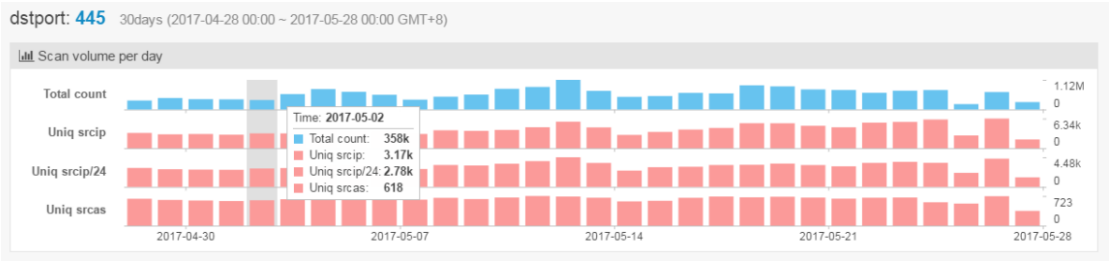
1） 根据被感染电脑的 IP 地址等信息，判断被感染电脑所处的环境是内网还是互联网；

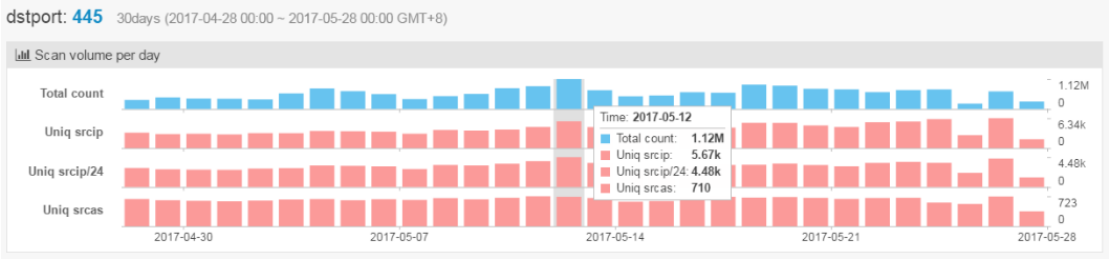
2） 如果被感染的电脑处于内网中，则对整个内网网段进行扫描；

3） 如果被感染的电脑处于外网或互联网上，则同时启动 128 个线程，循环扫描随机生成的 IP 地址。

4） 扫描时，首先探测目标 IP 的 445 端口是否开启，如果开启，则使用永恒之蓝工具发起远程攻击，向目标 IP 发送 SMB 协议的漏洞利用代码。

根据 360 互联网安全中心研发的全网扫描器实时监测系统(http://scan.netlab.360.com/#/dashboard)显示，在平日，针对 445 端口进行扫描的扫描源 IP 数约为 3100 个左右；而在 5 月 12 日 WannaCry 爆发当日，针对 445 端口进行扫描的扫描源 IP 数大幅上升到 5600 余个，见图 3。

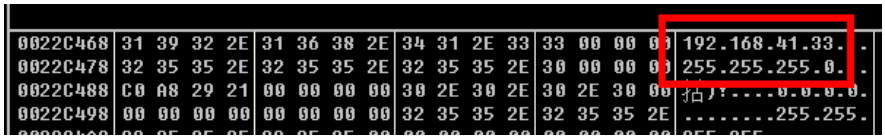




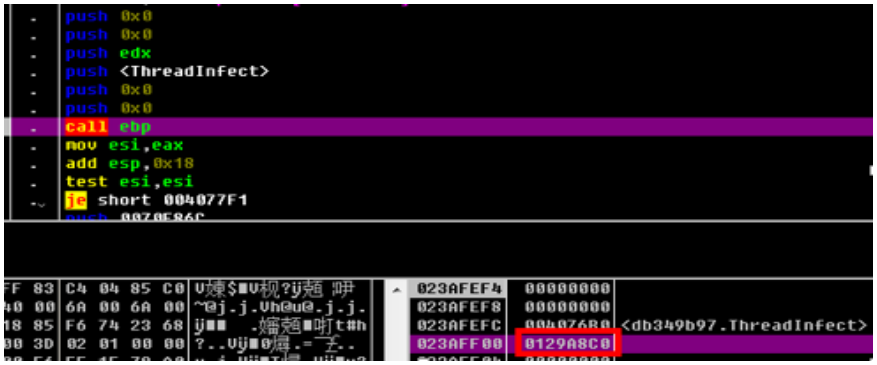
（二） 针对内网设备的攻击

针对内网设备的攻击过程分为两步：

1） 获取本机 IP 和子网掩码



2） 根据子网掩码生成局域网内其他所有电脑的 IP 列表，并将它们都列为攻击目标



(三) 针对互联网设备的攻击

由于外网，或互联网上的 IP 地址空间要远远大于内网或局域网，因此，WannaCry 的攻击方法要稍微复杂一些。具体来说，WannaCry 会以 2 秒时间为间隔循环启动 1 个攻击线程，直到保持 128 个并发攻击，每个线程会循环生成随机的合法 IP 地址进行攻击，这种攻击方式会在被感染的电脑上持续进行 24 小时。

特别的，该病毒在选择攻击目标 IP 地址时，也采用了一些特别的处理：

1） IP 地址的第一段会排除 127 和大于等于 224 的情况；

2） 每隔 40 分钟，病毒会对 IP 地址中的第一段进行一次随机分配

3） 每隔 20 分钟，病毒会对 IP 地址中的第二段进行一次随机分配

4） 如果攻击的 IP 地址 445 端口是开放的，会持续对这个 IP 地址的 C 段子网（x.x.x.1-x.x.x.254）发起 254 次攻击

其具体攻击代码：

```
mov     edi, 1
push    445             ; hostshort
mov     word ptr [esp+12Ch+name.sa_data+0Ch], ax
mov     [esp+12Ch+argp], edi
mov     dword ptr [esp+12Ch+name.sa_data+2], ecx
mov     [esp+12Ch+name.sa_family], 2
call    htons
push    IPPROTO_TCP     ; protocol
push    edi             ; type
push    AF_INET         ; af
mov     word ptr [esp+134h+name.sa_data], ax
call    socket
```

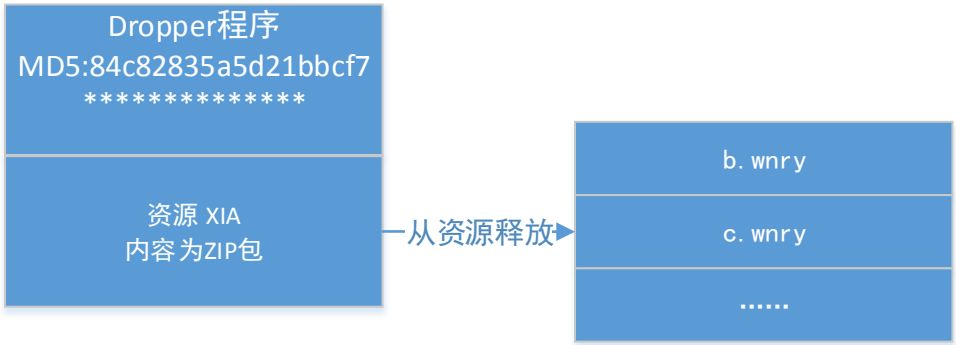
```
if ( q_Connect_445(a1) > 0 )
{
  v1 = (void *)beginthreadex(0, 0, q_MS17_010, a1, 0, 0);
  v2 = v1;
  if ( v1 )
  {
    if ( WaitForSingleObject(v1, 600000u) == WAIT_TIMEOUT )
      TerminateThread(v2, 0);
    CloseHandle(v2);
  }
}
InterlockedDecrement((volatile LONG *)&FileName[268]);
endthreadex(0);
return 0;
```

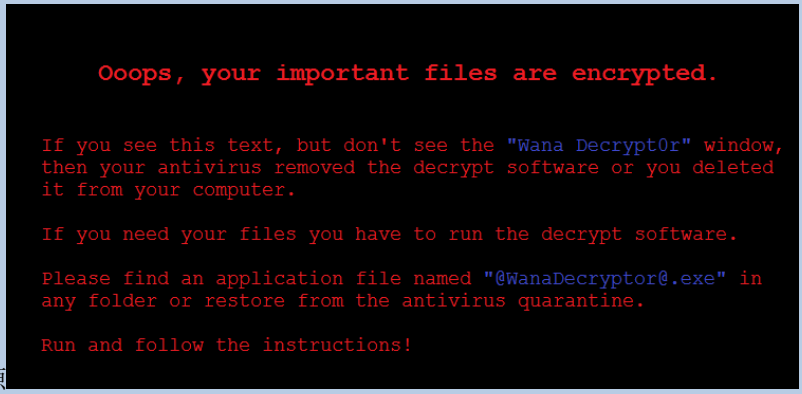
二、 WannaCry 的勒索攻击

作为一款勒索软件，WannaCry 的勒索攻击也很有自己的特点。特别是对不同类型文件的分类分级加密，以及某些反病毒技术的使用，让人印象深刻。

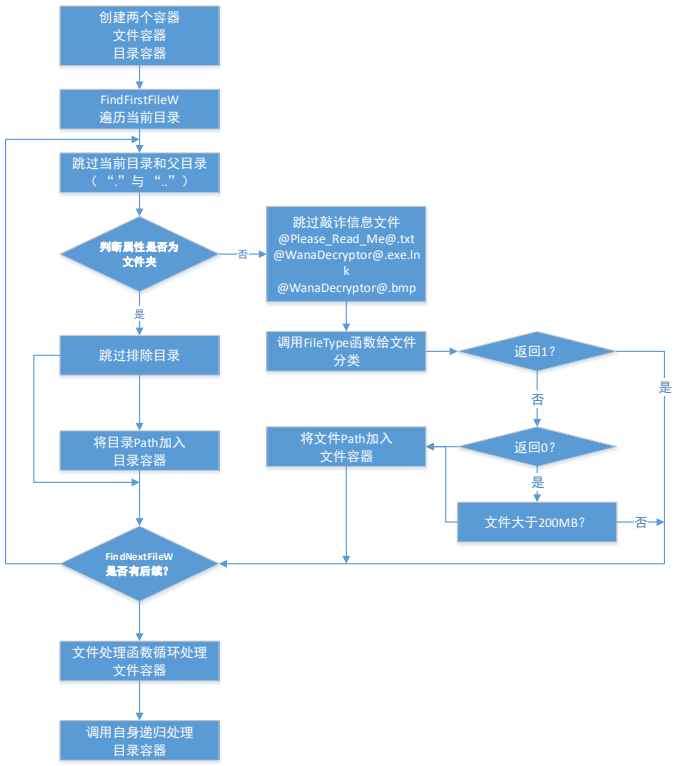
（一）WannaCry 的文件扫描

对文件进行加密，是勒索软件最基本的攻击方式。WannaCry 也不例外。WannaCry 在感染电脑后，会首先从程序资源中的 zip 压缩包中解压释放一个敲诈勒索功能相关的程序。见图：



名称	作用
b.wnry	 敲诈图片资源
c.wnry	配置文件，包含钱包信息，tor 地址
r.wnry	Q&A
s.wnry	压缩包，包含 TOR 网络组件
t.wnry	加密的 PAYLOAD，用于加密文件
u.wnry	解密程序（@WanaDecryptor@.exe）
taskdl.exe	删除临时文件
taskse.exe	在任意的远程桌面的 session 中运行指定的程序
taskhsvc.exe	网络通讯组件

WannaCry 的加密程序会首先按字母顺序遍历查找硬盘，从 Z 盘倒序遍历盘符直到 C 盘，其中会跳过无法加密的光驱盘，还会特别注意移动硬盘设备，我们将 WannaCry 程序的文件递归函数抽象成了下图的信息图，以方便大家理解。



（二） WannaCry 的分级加密

WannaCry 会根据要加密文件的大小和类型等信息，对文件进行详细的分类和分级，并使用不同的规则对不同类型的文件进行加密，目的是以最快的速度加密用户最有价值的文件。

exe、dll	1
type 列表 1 中	2
type 列表 2 中	3
wncryt	4
wncyr	5
wncry	6
均不符合以上规则	0

type 列表 1：

".doc",".docx",".xls",".xlsx",".ppt",".pptx",".pst",".ost",".msg",".eml",".vsd",".vsdx",".txt",".csv",".rtf",".123",".wks",".wk1",".pdf",".dwg",".onetoc2",".snt",".jpeg",".jpg"

type 列表 2：

".docb",".docm",".dot",".dotm",".dotx",".xlsm",".xlsb",".xlw",".xlt",".xlm",".xlc",".xltx",".xltm",".pptm",".pot",".pps",".ppsm",".ppsx",".ppam",".potx",".potm",".edb",".hwp",".602",".sxi",".sti",".sldx",".sldm",".sldm",".vdi",".vmdk",".vmx",".gpg",".aes",".ARC",".PAQ",".bz2",".tbk",".bak",".tar",".tgz",".gz",".7z",".rar",".zip",".backup",".iso",".vcd",".bmp",".png",".gif",".raw",".cgm",".tif",".tiff",".nef",".psd",".ai",".svg",".djvu",".m4u",".m3u",".mid",".wma",".flv",".3g2",".mkv",".3gp",".mp4",".mov",".avi",".asf",".mpeg",".vob",".mpg",".wmv",".fla",".swf",".wav",".mp3",".sh",".class",".jar",".java",".rb",".asp",".php",".jsp",".brd",".sch",".dch",".dip",".pl",".vb",".vbs",".ps1",".bat",".cmd",".js",".asm",".h",".pas",".cpp",".c",".cs",".suo",".sln",".ldf",".mdf",".ibd",".myi",".myd",".frm",".odb",".dbf",".db",".mdb",".accdb",".sql",".sqlitedb",".sqlite3",".asc",".lay6",".lay",".mml",".sxm",".otg",".odg",".uop",".std",".sxd",".otp",".odp",".wb2",".slk",".dif",".stc",".sxc",".ots",".ods",".3dm",".max",".3ds",".uot",".stw",".sxw",".ott",".odt",".pem",".p12",".csr",".crt",".key",".pfx",".der"

程序为了能尽快的加密其认为重要的用户文件，设计了一套复杂的优先级队列:

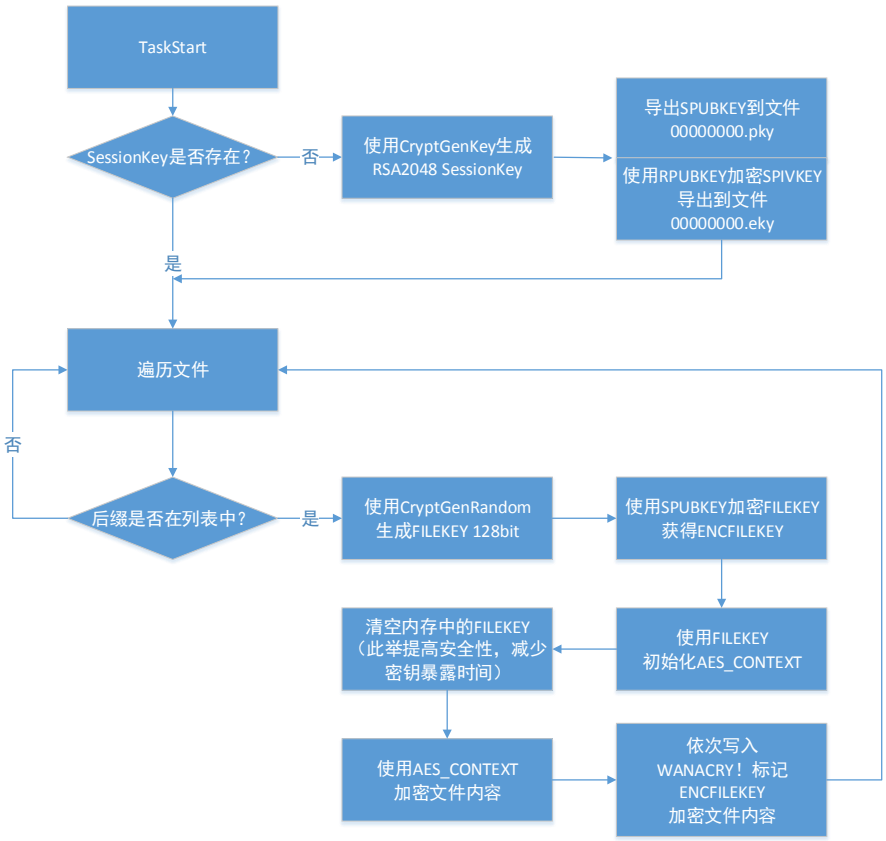
1） 对 type2（满足后缀列表 1）进行加密（小于 0x400 的文件会降低优先级）。

2） 对 type3（满足后缀列表 2）进行加密（小于 0x400 的文件会降低优先级）。

3） 处理剩下的文件（小于 0x400 的文件），或者其他一些文件。

（三） WannaCry 的加密算法

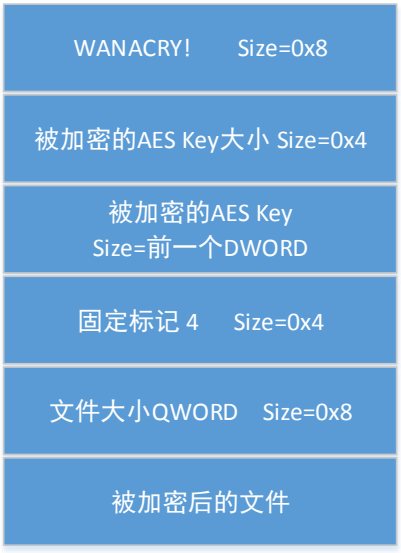
在完成了需要加密文件的编辑处理后，程序就开始了最为关键的文件加密流程，整个加密过程使用了标准的 RSA 和 AES 加密算法，其中 RSA 加密功能使用了微软的 CryptoAPI 函数实现，加密流程如图所示：



程序加密文件的关键密钥说明：

密钥	简介
RPUBKEY	RSA 2048 Root Public Key，硬编码于程序中
RPIVKEY	RSA 2048 Root Private Key，作者持有，目前未公开
SPUBKEY	RSA 2048 Session Public Key，每个受害用户唯一的会话密钥（公钥），用于加密 AES KEY，导出到文件 00000000.pky
SPIVKEY	RSA 2048 Session Private Key，每个受害用户唯一的会话密钥（私钥），用于解密 AES KEY，Encrypt（RPUBKEY，SPIVKEY），即用 RPUBKEY 加密后导出到文件 00000000.eky
FILEKEY	AES 128Bit KEY，每一个文件生成一个，通过 CryptGenRandom 生成
ENCFILEKEY	被 SPUBKEY 加密的 FILEKEY，存在于被加密的文件当中

被加密后的文件格式如下图：



值得注意的是，在加密过程中，程序会随机选取一部分文件使用内置的 RSA 公钥来进行加密，其目的是为解密程序提供的免费解密部分文件功能。相关的 C 语言伪代码见图 10：

```
62 LABEL_29:
63   if ( a4 == 4 && FileSize.HighPart <= 0 && FileSize.LowPart < 0xC800000 )
64   {
65     if ( *((_DWORD *)v4 + 582) )
66     {
67       if ( !((unsigned int)rand() % *((_DWORD *)v4 + 582)) )
68       {
69         v10 = *((_DWORD *)v4 + 584);
70         if ( v10 < *((_DWORD *)v4 + 583) )
71         {
72           v62 = 1;
73           v64 = v4 + 44;
74           *((_DWORD *)v4 + 584) = v10 + 1;
75         }
76       }
77     }
78   }
79   v52 = 512;
80   if ( !q_init_key((int)v64, &pbBuffer, 0x10u, (int)&v49, (int)&v52) )
81     goto LABEL_62;
```

而能免费解密的文件路径则在文件 f.wnry 中

```
1 C:\Reverse\Ollydbg52\Plugin\shourtcuts.txt.WNCRY
2 C:\Reverse\Ollydbg52\脱壳脚本\Acprotect\ULTRAPROTECT 1.x - ACPROTECT 1.22 VB.txt.WNCRY
3 C:\Reverse\Ollydbg52\脱壳脚本\Armadillo\Armadillo 5.xx OEP Finder (Standard Protection + Debug
4 C:\Reverse\Ollydbg52\脱壳脚本\ASProtect\ASProtect 1.2x - 1(1).3x (Registered) OEP Finder.txt.WN
5 C:\Reverse\Ollydbg52\脱壳脚本\SecuROM\SECUROM OEP SCRIPT 1.1 [MAIN EXE].txt.WNCRY
6 C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\Default Pi
7 C:\Python27\include\longintrepr.h.WNCRY
8 C:\Python27\include\methodobject.h.WNCRY
9 C:\Reverse\AndroidNP\lib\smali.jar.WNCRY
```

在完成加密之后，WanaCrypt0r 会对其认为重要的文件进行随机数填充，然后将文件移动到指定的临时文件夹目录然后删除。此举用于对抗文件恢复类软件，同时兼顾加密文件的速度。

被随机数填充的文件需要满足以下几点（见下图）：

1） 文件在特殊目录中（桌面，我的文档，用户文件夹）。

2） 文件小于 200M。

3） 文件后缀在 type 列表 1。

具体填充的逻辑如下：

1） 如果文件小于 0x400,直接覆盖对应长度的随机数。

2） 如果文件大于 0x400,对文件距离末尾 0x400 处进行覆盖。

3） 再次重定位文件指针到文件头，以 0x40000 大小的缓冲区为单位向写随机数直到文件末尾。

```
.text:100030D6                          ; ---------------------------------------------------------------------------
.text:100030D6
.text:100030D6                          loc_100030D6:                           ; CODE XREF: sub_10003010+B5↑j
.text:100030D6                                                                  ; sub_10003010+BE↑j
.text:100030D6 40024 B8 00 00 04 00             mov     eax, 40000h
.text:100030DB 40024 89 74 24 20                mov     [esp+40024h+var_40004], esi
.text:100030DF
.text:100030DF                          loc_100030DF:                           ; CODE XREF: sub_10003010+C4↑j
.text:100030DF 40024 8D 54 24 24                lea     edx, [esp+40024h+pbBuffer]
.text:100030E3 40024 50                         push    eax             ; dwLen
.text:100030E4 40028 52                         push    edx             ; pbBuffer
.text:100030E5 4002C E8 36 13 00 00             call    CryptGenRandomWrapper
.text:100030EA 40024 8B 54 24 14                mov     edx, dword ptr [esp+40024h+FileSize+4]
.text:100030EE 40024 8B 5C 24 10                mov     ebx, dword ptr [esp+40024h+FileSize]
.text:100030F2 40024 EB 3A                      jmp     short loc_1000312E
.text:100030F4                          ; ---------------------------------------------------------------------------
```

```
.text:10003161                          ; ---------------------------------------------------------------------------
.text:10003161
.text:10003161                          loc_10003161:                           ; CODE XREF: sub_10003010+126↑j
.text:10003161                                                                  ; sub_10003010+130↑j
.text:10003161 40024 8D 54 24 18                lea     edx, [esp+40024h+var_4000C]
.text:10003165 40024 6A 00                      push    0               ; _DWORD
.text:10003167 40028 52                         push    edx             ; _DWORD
.text:10003168 4002C 8D 44 24 2C                lea     eax, [esp+4002Ch+pbBuffer]
.text:1000316C 4002C 53                         push    ebx             ; _DWORD
.text:1000316D 40030 50                         push    eax             ; _DWORD
.text:1000316E
.text:1000316E                          loc_1000316E:                           ; CODE XREF: sub_10003010+14F↑j
.text:1000316E 40034 55                         push    ebp             ; _DWORD
.text:1000316F 40038 FF 15 20 D9 00 10          call    qWriteFile
.text:10003175 40020 55                         push    ebp             ; hFile
.text:10003176 40024 FF 15 78 70 00 10          call    ds:FlushFileBuffers
.text:1000317C 40020 6A 00                      push    0               ; dwMoveMethod
.text:1000317E 40024 6A 00                      push    0               ; lpDistanceToMoveHigh
.text:10003180 40028 6A 00                      push    0               ; lDistanceToMove
.text:10003182 4002C 55                         push    ebp             ; hFile
.text:10003183 40030 FF D7                      call    edi ; SetFilePointer
.text:10003185 40020 8B 44 24 14                mov     eax, [esp+40020h+var_4000C]
.text:10003189 40020 8B 54 24 10                mov     edx, dword ptr [esp+40020h+FileSize+4]
.text:1000318D 40020 33 F6                      xor     esi, esi
.text:1000318F 40020 33 FF                      xor     edi, edi
.text:10003191 40020 85 C0                      test    eax, eax
.text:10003193 40020 7C 54                      jl      short loc_100031E9
.text:10003195 40020 7F 0A                      jg      short loc_100031A1
.text:10003197 40020 85 D2                      test    edx, edx
.text:10003199 40020 76 4E                      jbe     short loc_100031E9
.text:1000319B 40020 EB 04                      jmp     short loc_100031A1
.text:1000319D                          ; ---------------------------------------------------------------------------
```

（四） WannaCry 的文件删除

为了加快加密速度，WannaCry 并没有在文件原文上进行加密处理，而是采用了先加密，后删除的处理方法。但分析发现，在进行文件删除操作时，病毒作者的处理逻辑不够严谨，因此也就为数据的恢复提供了可能性。

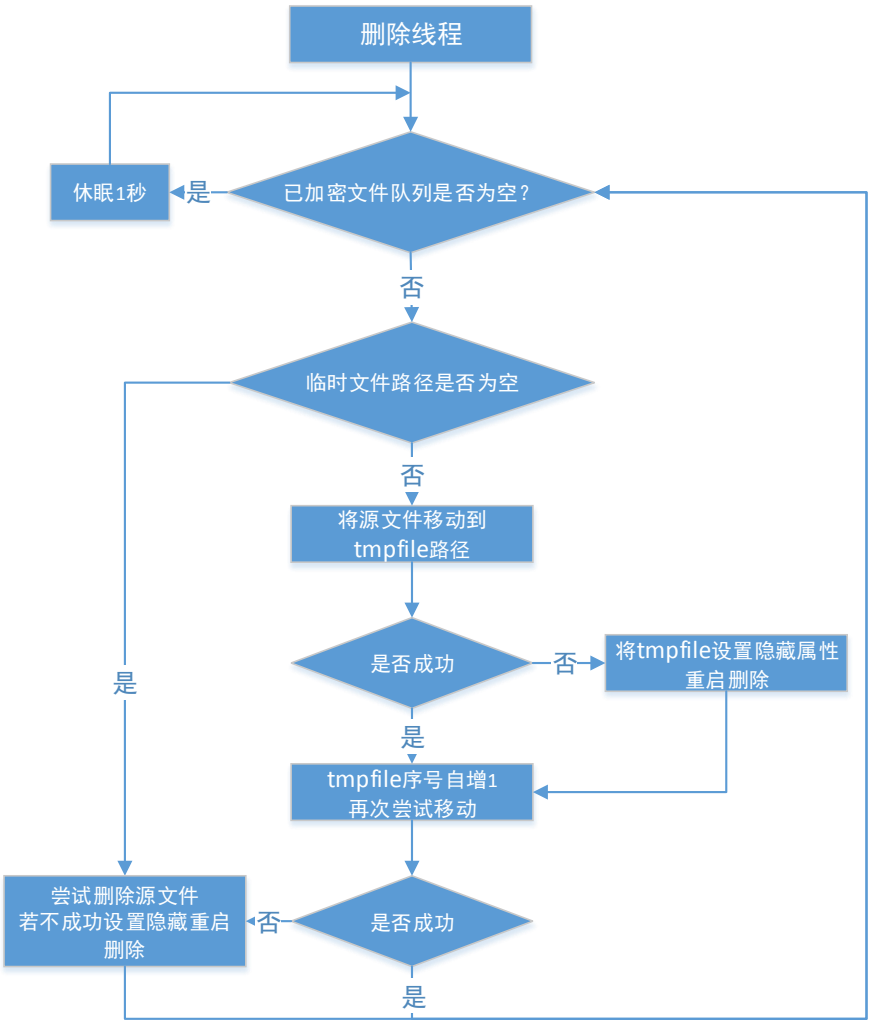
WannaCry 删除文件的操作大致过程：首先尝试将文件移动到临时文件夹，生成一个临时文件，然后再尝试多种方法删除文件。

1） 当采用遍历磁盘的方式加密文件的时候，会在当前盘符生成“$RECYCLE”+ 全局自增量+”.WNCYRT”(eg： "D:\\$RECYCLE\\1.WNCRYT")路径的临时文件。

2） 当盘符为系统盘(eg：C)时，使用的系统临时目录(%temp%)。

3） 之后程序以固定时间间隔，来删除临时文件夹下的文件。

详细的删除文件流程信息图见图 12：



（五） 文件的解密流程

首先，解密程序通过释放的 taskhsvc.exe 向服务器查询付款信息，若用户已经支付过，则将 eky 文件发送给作者，作者解密后获得 dky 文件，这就是解密之后的 Key。

解密流程与加密流程相反，解密程序将从服务器获取的 dky 文件中导入 Key。

```
push    offset a08x_dky ; "%08X.dky"
push    ecx             ; Dest
call    edi ; __imp_sprintf
```

```
v2 = this;
if ( !q_CryptAcquireContext() )
{
  q_DestroyKey(v2);
  return 0;
}
if ( lpFileName )
{
  if ( !q_ImportKeyFromFile(*((_DWORD *)v2 + 1), (int)((char *)v2 + 8), lpFileName) )
  {
    q_DestroyKey(v2);
    return 0;
  }
}
else if ( !g_CryptImportKey(*((_DWORD *)v2 + 1), &g_InsideKey, 1172, 0, 0, (char *)v2 + 8) )
{
  q_DestroyKey(v2);
  return 0;
}
return 1;
```

可以看到，当不存在 dky 文件名的时候，使用的是内置的 Key，此时是用来解密免费的解密文件使用的。

```
85C0          test eax,eax
75 0D         jnz X@WanaDec.00404709
8BCE          mov ecx,esi
E8 6D000000   call @WanaDec.00404770
33C0          xor eax,eax
5E            pop esi
C2 0400       retn 0x4
8B4424 08     mov eax,dword ptr ss:[esp+0x8]
85C0          test eax,eax
75 2D         jnz X@WanaDec.0040473E
8B4E 04       mov ecx,dword ptr ds:[esi+0x4]
8D46 08       lea eax,dword ptr ds:[esi+0x8]
50            push eax
6A 00         push 0x0
6A 00         push 0x0
68 94040000   push 0x494
68 94074200   push @WanaDec.00420794
51            push ecx
FF15 C4174200 call dword ptr ds:[0x4217C4]   advapi32.CryptImportKey
```

```
mov     esi, [esp+0Ch+arg_0]
mov     ecx, [ebx+8]
lea     eax, [esp+0Ch+arg_4]
push    eax
push    esi
push    0
push    1
push    0
push    ecx
call    q_CryptDecrypt
```

之后解密程序从文件头读取加密的数据，使用导入的 Key 调用函数 CryptDecrypt 进行解密，解密出的数据作为 AES 的 Key 再次进行解密，得到原文件。

```
    v24 -= (unsigned int)v25;
    q_AES_Decrypt(*((_DWORD *)v10 + 306), *((_DWORD *)v10 + 307), v25, 1);
    if ( !g_WriteFile(v5, *((_DWORD *)v10 + 307), v25, &v26, 0) || v26 != v25 )
      goto LABEL_33;
  }
  SetFilePointerEx(v5, liDistanceToMove, 0, 0);
```

（六） WannaCry 的对抗技术

从 WannaCry 的代码来看，病毒作者具有一定反检测对矿能力。这里举两个例子。

1） 静态文件特征查杀的技巧

WannaCry 敲诈程序在启动时使用了一个躲避杀毒软件的静态文件特征查杀的技巧。它会释放一个 DLL 模块到内存中，直接在内存中加载运行该 DLL 模块，DLL 模块中的函数 TaskStart 用于启动整个加密的流程，动态获取文件系统和加密功能相关的 API 函数，用内存中的动态行为来和杀毒软件的文件静态扫描特征对抗。相关的逆向代码如下：

```
10004466 push    edi
10004467 mov     edi, ds:GetProcAddress
1000446D push    offset aCryptacquireco ; "CryptAcquireContextA"
10004472 push    esi             ; hModule
10004473 call    edi ; GetProcAddress
10004475 push    offset aCryptimportkey ; "CryptImportKey"
1000447A push    esi             ; hModule
1000447B mov     g_CryptAcquireContextA, eax
10004480 call    edi ; GetProcAddress
10004482 push    offset aCryptdestroyke ; "CryptDestroyKey"
10004487 push    esi             ; hModule
10004488 mov     g_CryptImportKey, eax
1000448D call    edi ; GetProcAddress
1000448F push    offset aCryptencrypt ; "CryptEncrypt"
10004494 push    esi             ; hModule
10004495 mov     g_CryptDestroyKey, eax
1000449A call    edi ; GetProcAddress
1000449C push    offset aCryptdecrypt ; "CryptDecrypt"
100044A1 push    esi             ; hModule
100044A2 mov     g_CryptEncrypt, eax
100044A7 call    edi ; GetProcAddress
100044A9 push    offset aCryptgenkey ; "CryptGenKey"
100044AE push    esi             ; hModule
100044AF mov     g_CryptDecrypt, eax
100044B4 call    edi ; GetProcAddress
100044B6 mov     ecx, g_CryptAcquireContextA
100044BC mov     g_CryptGenKey, eax
100044C1 test    ecx, ecx
```

2） 特定目录躲避

WannaCry 在文件遍历的过程中会排除和比较一些路径或者文件夹名称，其中有一个很有意思的目录名“ This folder protects against ransomware. Modifying it will reduce protection”。我们发现这个目标是国外的一款名为 ransomfree 的勒索防御软件创建的防御目录，勒索软件如果触碰这个目录下的文件，就会被 ransomfree 查杀。所以，当 WannaCry 遇到这个目录时，就会自动跳过去。这说明病毒作者有非常强的杀毒攻防对抗经验。

（七） 数据恢复的可行性

通过对 WannaCry 文件加密流程分析，我们会发现程序在加密线程中会对满足条件的文件用随机数或 0x55 进行覆写，从而彻底破坏文件的结构并防止数据被恢复。但是覆写操作只限定于特定的文件夹和特定的后缀名。也就是说，程序只对满足条件的文件进行了覆写操作，受害者机器上仍然有很多的文件未被覆写，这就为数据恢复提供了可能。

而在删除线程中，我们发现程序是先将源文件通过 Windows 系统的 MoveFileEx 函数移

动到其创建的临时文件夹下，最后统一进行删除。在这个过程中源文件的文件名会发生改变，常规数据恢复软件不知道这个文件操作逻辑，导致大部分文件无法恢复，如果我们针对改变的文件名调整文件恢复策略，就可能恢复大部分文件。

另一方面，因为删除操作和加密操作在不同的线程中，受用户环境的影响，线程间的条件竞争可能存在问题，从而导致移动源文件的操作失败，使得文件在当前位置被直接删除，在这种情况下被加密的文件有很大概率可以进行直接恢复，但是满足这种情形的文件是少数。

根据以上分析，我们发现了除了系统盘外的文件外，用我们精细化处理的方法进行数据恢复，被加密的文件有很大概率是可以完全恢复的。据此 360 公司开发了专门的恢复工具 2.0 版，以期帮助在此次攻击中广大的受害者恢复加密数据。

三、 WannaCry 与永恒之蓝

WannaCry 的攻击力极强，最主要的原因就是使用了 NSA 泄密的网络武器永恒之蓝。本章主要分析一下 WannaCry 与永恒之蓝的具体关系。

（一） 永恒之蓝的泄漏历程

2016 年 8 月 13 日，黑客组织 Shadow Brokers 声称攻破了为 NSA 开发网络武器的美国黑客团队 Equation Group，并表示，如果得到 100 万比特币（现价约合 5.68 亿美元），将公开这些工具。后来的事实证明，该组织从 2016 年 8 月 1 日开始，就已经在为披露包括永恒之蓝在内的一系列的 NSA 网络攻击武器做准备。在这期间的 13 天里，该组织在 Reddit，GitHub，Twitter，Imgur 等多个平台建立了相关的披露账号，并且于 13 日开始将相关文档在以上平台进行披露。被泄露的工具包为一个 256MB 左右的压缩文件，其中包含未加密的压缩包 eqgrp-free-file.tar.xz.gpg，及被用于拍卖的压缩包 eqgrp-auction-file.tar.xz.gpg。

2017 年 1 月 8 日，Shadow Brokers 再度开卖窃取方程式组织的 Windows 系统漏洞利用工具，此次拍卖的工具要价 750 比特币（当时折合人民币 4650000 元左右）。从公开的工具截图来看此次的工具包括 Windows 的 IIS、RPC、RDP 和 SMB 等服务的远程代码执行，还有一些后门、Shellcode 以及一些其他的小工具。

2017 年 2 月 10 日，一个疑似早期版本的 WannaCry 加解密模块程序被上传到的 VirusTotal，代码的编译时间是 2 月 9 日。在 WannaCry 爆发以后，通过代码相似度比较，我们有相当大的把握认为这个版本与后来肆虐网络的版本同源。

2017 年 4 月 14 日，Shadow Brokers 公布了之前泄露文档中出现的 Windows 相关部分的文件，该泄露资料中包含了一套针对 Windows 系统相关的远程代码利用框架及漏洞利用工具（涉及的网络服务范围包括 SMB、RDP、IIS 及各种第三方的邮件服务器）。这批数据和工具是 Shadow Brokers 在 2016 年以来数次公布的数据中最有价值也同时最具攻击力的一部分，其中涉及 SMB 服务的影响面最广而且最稳定的 ETERNALBLUE 漏洞利用工具直接催生了 WannaCry 勒索蠕虫。

同日，微软也发布了相应的通告，Shadow Brokers 公布的大部分之前未知的漏洞，在 2017 年 3 月 14 日的例行补丁包中已经被修复，只要打好补丁，就可以免于攻击。至于 Shadow Brokers 为何是要等到微软已经给系统打了补丁之后披露相关网络武器，我们不得而知。

2017 年 5 月 12 日，北京时间下午 3 点多前后，WannaCry 勒索蠕虫开始爆发。

2017 年 5 月 12 日，北京时间晚上 11 点多，英国安全研究人员@MalwareTechBlog 得到并分析了 WannaCry 蠕虫样本，发现样本关联了一个域名并将其注册，在当时他并不非常清楚此域名的作用。事实上由于恶意代码本身的逻辑，此域名如果获得有效的解析蠕虫就会退出不再执行后续破坏性的加密操作，所以此域名的注册极大地抑制了勒索蠕虫的破坏作用。之后该 Twitter 作者写了文章成，“How to Accidentally Stop a Global Cyber Attacks”描述了他是如何第一时间注意到这次攻击事件，并迅速做出应对的过程。

2017 年 5 月 12 日下午，360 启动应急响应机制。同时，CNCert、网信、公安等也在全国范围内展开了积极的应急响应，并与包括 360 在内的专业安全厂商进行了积极的合作与联动。

2017 年 5 月 16 日，经历过两天的工作日，最终确认，WannaCry 的感染量不再增加，没有出现不可控发展趋势，针对 WannaCry 的应急响应告一段落。

（二） WannaCry 模块对比

通过对 WannaCry 程序代码和实际发送的攻击数据包进行分析，我们发现程序使用的漏洞攻击代码和开源黑客工具所利用的永恒之蓝漏洞攻击近乎一致。

图 14 是程序攻击数据包的对比分析：左图为病毒程序的逆向代码，右图为黑客工具 metasploit 的开源代码，可以看到攻击代码的内容几乎一致。

```
; char make_smb1_anonymous_login_packet[
make_smb1_anonymous_login_packet db     0

                db     0
                db     0
                db  88h ;
                db 0FFh
                db  53h ; S
                db  4Dh ; M
                db  42h ; B
                db  73h ; s
                db     0
                db     0
                db     0
                db     0
                db  18h
                db     7
                db 0C0h ;
                db     0
                db     0
                db     0
                db     0
                db     0
                db     0
                db     0
                db     0
                db     0
                db     0
                db     0
                db     0
                db     0
                db     0
                db     0
                db 0FFh
```

```
485   def make_smb1_anonymous_login_packet
486     # Neither Rex nor RubySMB appear to support Anon login?
487     pkt = ""
488     pkt << "\x00"                  # Session message
489     pkt << "\x00\x00\x88"          # length
490     pkt << "\xffSMB"               # SMB1
491     pkt << "\x73"                  # Session Setup AndX
492     pkt << "\x00\x00\x00\x00"      # NT SUCCESS
493     pkt << "\x18"                  # Flags
494     pkt << "\x07\xc0"              # Flags2
495     pkt << "\x00\x00"              # PID High
496     pkt << "\x00\x00\x00\x00"      # Signature1
497     pkt << "\x00\x00\x00\x00"      # Signature2
498     pkt << "\x00\x00"              # TreeID
499     pkt << "\xff\xfe"              # PID
500     pkt << "\x00\x00"              # Reserved
501     pkt << "\x00\x00"              # UserID
502     pkt << "\x40\x00"              # MultiplexID
503
504     pkt << "\xff"                  # No further commands
505     pkt << "\x00"                  # Reserved
506     pkt << "\x0d"                  # Word Count
507     pkt << "\x88\x00"              # AndXOffset
508     pkt << "\x04\x11"              # Max Buffer
509     pkt << "\x0a\x00"              # Max Mpx Count
510     pkt << "\x00\x00"              # VC Number
511     pkt << "\x00\x00\x00\x00"      # Session key
512     pkt << "\x01\x00"              # ANSI pw length
513     pkt << "\x00\x00"              # Unicode pw length
514     pkt << "\x00\x00\x00\x00"      # Reserved
515     pkt << "\xd4\x00\x00\x00"      # Capabilities
516     pkt << "\x4b\x00"              # Byte count
517     pkt << "\x00"                  # ANSI pw
518     pkt << "\x00\x00"              # Account name
519     pkt << "\x00\x00"              # Domain name
```

```
                db     0
                db     0
                db     0
                db     0
                db     0
                db     0
aWindows20002195:
                unicode 0, <Windows 2000 2195>,0
aWindows20005_0:
                unicode 0, <Windows 2000 5.0>,0
; char byte 42E65C[3]
```

```
518     pkt << "\x00\x00"              # Account name
519     pkt << "\x00\x00"              # Domain name
520
521   # Windows 2000 2195
522   pkt << "\x57\x00\x69\x00\x6e\x00\x64\x00\x6f\x00\x77\x00\x73\x00\x20\x00\x32"
523   pkt << "\x00\x30\x00\x30\x00\x30\x00\x20\x00\x32\x00\x31\x00\x39\x00\x35\x00"
524   pkt << "\x00\x00"
525
526   # Windows 2000 5.0
527   pkt << "\x57\x00\x69\x00\x6e\x00\x64\x00\x6f\x00\x77\x00\x73\x00\x20\x00\x32"
528   pkt << "\x00\x30\x00\x30\x00\x30\x00\x20\x00\x35\x00\x2e\x00\x30\x00\x00\x00"
```

我们再将抓取到的，程序的真实攻击网络数据包进行分析对比，发现攻击的关键数据包也完全一致。

（三） 军用武器的民用化

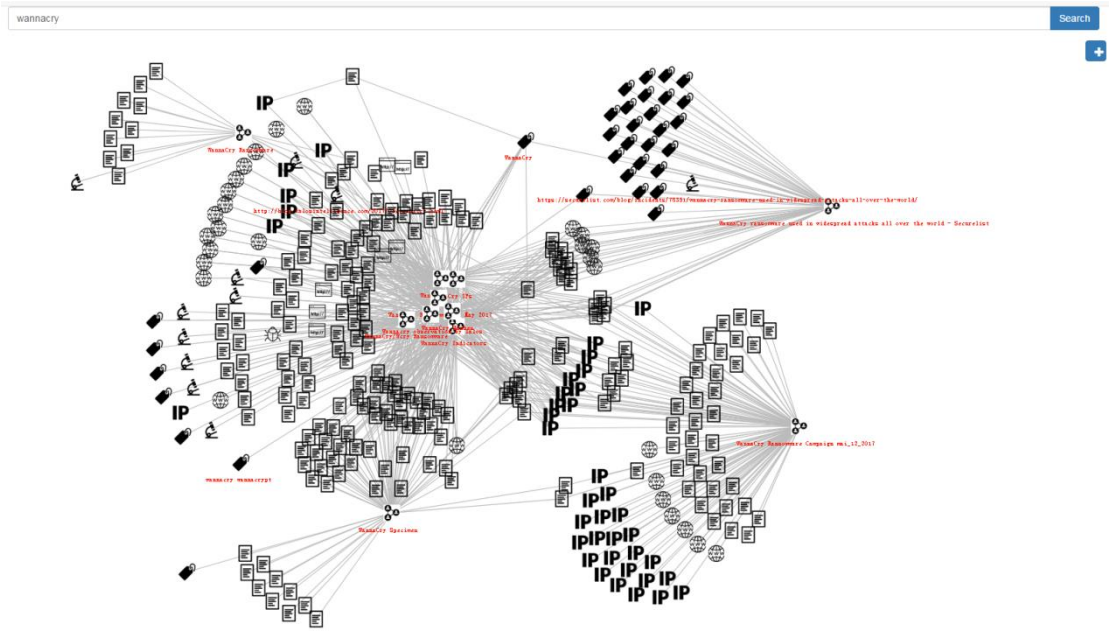
诸如永恒之蓝这类军用网络攻击武器被用于民用网络攻击领域的现象令人不安，这也暗示着基于 NSA 工具的 SMB 服务漏洞正在积极地被蠕虫式利用传播。在 WannaCry 勒索蠕虫肆虐期间就出现了很多个去除掉自杀开关的修改版本，之后还发现了几乎捆绑 NSA 所有可用 SMB 漏洞攻击工具进行传播的 EternalRocks（永恒之石）家族，这些派生的和其他恶意代码家族理论上具备更强的传播力，甚至会逐渐取代 WannaCry 蠕虫的主流地位。

WannaCry 蠕虫的加密勒索行为会促使中招用户尽快进行处置，重装系统、安装补丁，以减少后续的感染源。但是，如果其他利用 SMB 漏洞进行传播的蠕虫只是秘密地潜伏控制，不做更多引起用户注意的事情，则可能持续地保持活跃状态。2003 年的 SQL Slammer 蠕虫，就一个 400 多字节的 UDP Payload，只存在于内存中，理论上只要为数不多的受感染的系统同时重启一次，蠕虫就会被消灭，可是就这样一个蠕虫存活了至少十年（也许现在还活着）。2008 年爆发的 Conficker 蠕虫到现在都还处于活跃状态，从监测到的已感染的源 IP 数量来看，完全有可能再活跃 10 十年。

此外，Shadow Brokers 还宣称，将会在未来一段时间里，披露更多的 NSA 利用 0day 漏洞进行攻击的网络武器。如果此言成真，很可能引起网络安全更大的灾难。

四、 WannaCry 的变种分析

就在 WannaCry 原始版本的蠕虫泛滥成灾之时，360 互联网安全中心又监测到了大量基于原始版本进行修改的变种，总量达到数百个，在情报中心的图关联搜索中可以很直观地看到部分关联。见图。

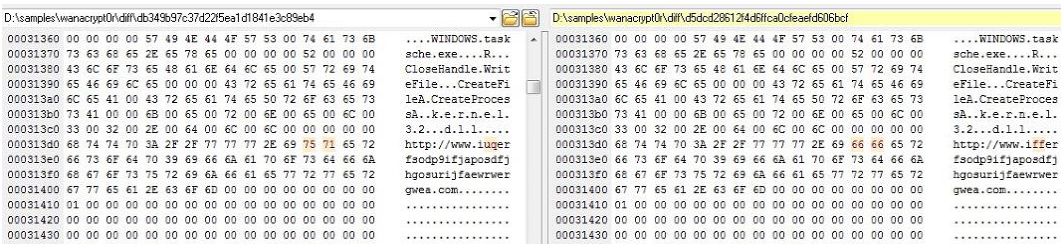


从图中可以看到：

1） MD5 值：d5dcd28612f4d6ffca0cfeaefd606bcf

此变种和原始版本蠕虫只有细微的差别，只是通过二进制 Patch 的方法修改了自杀开关，病毒链接的 URL 的地址被改为 http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com。

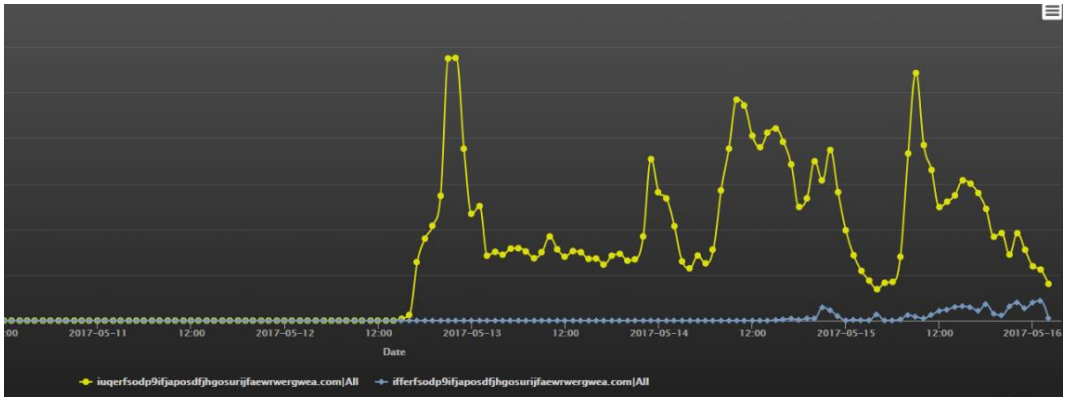
以后发现的多个类似变种也都采用了这种通过简单二进制 Patch 的方式修改开关域名的方法，与原始版本相关，整个恶意代码只有域名部分的字节被进行了修改。见图 16。



WannaCry 部分变种样本及对应开关域名如下表：

样本	自杀开关
550ea639584fbf13a54eccdaa359d398	http://www.udhridhfowhgibe9vheiviehfiehbfvieheifheih.com
c2559b51cfd37bdbd5fdb978061c6c16	http://www.iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com
0156edf6d8d35def2bf71f4d91a7dd22	http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
61f75bb0c76fe332bccfb3383e5e0178	http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
4287e15af6191f5cab1c92ff7be8dcc3	http://www.ayylmaotjhsstasdfasdfasdfasdfasdfasdf.com
dd7216f5cb34dcf9bd42879bd528eaf4	http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.cum

图是原始版本 WannaCry 的开关域名与其中一个修改后域名的解析量对比。其中从对 DNS 访问量的监测来看，此类样本对整体感染面影响基本可以忽略不计。



从图中还可以看出，开关域名对蠕虫的传播影响非常大，在域名被安全研究者注册，形成有效解析和访问以后，初始的指数级感染趋势很快被抑制，之后再也没有超过最早快速上升阶段所形成的高峰。

至于那些通过简单 Patch 得到的蠕虫为什么无法流行开来，我们猜测的原因倒并不是越来越多的系统被及时打上了补丁（这无法解释为什么非 WannaCry 蠕虫但同样利用 NSA SMB 系列漏洞的其他恶意代码感染量持续上升的趋势），而是因为主机上的防病毒工具所起的作用。这些简单 Patch 过的恶意代码与原始版本太像了，基于特征码的病毒查杀引擎就能非常

有效地识别并做自动化的处理，如果这类派生蠕虫不像 WannaCry 那样在活动的早期感染量以链式反应一样迅速突破一个临界值就很难再流行开来。

2）MD5 值：d724d8cc6420f06e8a48752f0da11c66

该变种样本在原版样本的基础上，从二进制 Patch 直接去除了检查开关域名以停止加密的功能，可以直接进入感染流程。图 18 为修改前后的比较。

但是，该样本在勒索模块的部分可能是由于作者疏忽，样本里硬编码的用于解压 zip 的密码还是 WNcry@2ol7, 这个密码并不能解压成功，导致勒索流程被废掉了。接来下的变种可能会修复这个“Bug”，而使攻击的威胁程度大增。事实上，后来也确实出现了完全去除自杀开关并且可工作的版本。

综上，这些基于原始蠕虫简单修改的恶意代码已经构不成严重威胁，更麻烦的在于那些潜伏下来让人无感知的恶意代码家族，这些才是真正值得担心的东西。

附录 3　从 DNS 和 sinkhole 视角看 WannaCry 蠕虫

域名系统(Domain Name System, DNS)数据作为全网流量数据的一种采样方式，可以在大网尺度对域名做有效的度量和分析。我们利用 DNS 数据，在过去数年里对多个安全事件，包括 Mirai 等僵尸网络、DGA 等恶意域名，以及黑色产业链条进行跟踪和分析。对于最近爆发的 WannaCry 蠕虫病毒，利用 DNS 数据进行分析，也是很有意义的。

众所周知，WannaCry 蠕虫病毒有一个开关域名。在蠕虫感染过程中，有效载荷通过 445 端口上的 MS17-010 漏洞投递并成功启动后，会尝试访问特定域名的网页。如果成功访问网页，则随即退出，蠕虫会被压制，不会进一步发作；如果访问网页失败，蠕虫会开始破坏动作，并随后弹框勒索赎金。本文首先从我们手头的 DNS 数据视角，就开关域名和其他域名的访问情况，描绘本次 WannaCry 蠕虫病毒在国内的感染和防御情况。

尽管在注册开关域名时，Kryptos Logic Vantage 的研究人员并没有意识到这个域名的重要作用，但实际上，正是这个开关域名成功防止了 WannaCry 蠕虫的蔓延，研究人员因此自嘲说“意外地拯救了世界”。得益于 Kryptos Logic Vantage 对我们的信任，我们获得了关键域名 sinkhole 的部分日志数据。本文的第二部分，将基于 sinkhole 日志的统计信息，分析 WannaCry 的感染情况。

从 DNS 视角看 WannaCry 在国内的感染和防御情况

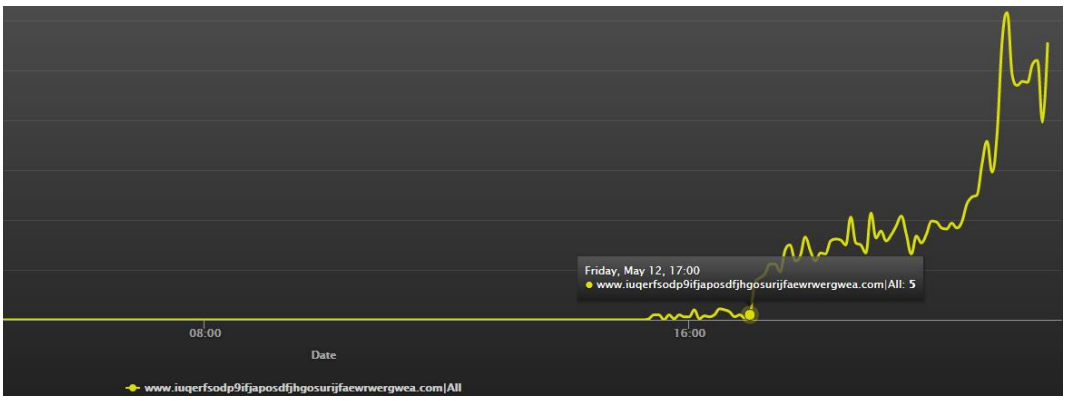
这里，有必要先介绍一下我们在 DNS 方面“看见”的能力，从而向读者确认我们所见的数据能够代表中国地区。我们及合作伙伴的 DNS 数据源每日高峰期处理超过 100 万次/秒的 DNS 请求和响应，客户来源覆盖国内各地理区域、行业、运营商等不同领域。

在这次 WannaCry 事件中，我们估算能够看到全国大约 10%的相关 DNS 流量。如果将整个国内互联网视为一个复杂系统，DNSPAI 则是对 DNS 流量的一个采样，而全部的 DNS 流量是对整个复杂系统在协议维度的一个采样。在这个尺度上，即使只有 1%的采样比也是非常惊人的。通过合理设定数据处理管道和充分运用大数据分析技术，我们能够对中国大陆地区的网络安全情况有一个较为全面的了解。

一、 WannaCry 在国内的感染趋势

（一） 早期感染阶段

5 月 12 日（周五）15:20（北京时间，下同），我们看到了首个访问该域名的 DNS 请求。此时的域名解析是不成功的，自然无法访问到目标网页，机器一旦感染蠕虫，就会发作。这个阶段的 DNS 访问曲线如图所示。



这段时间又可以划分为如下若干更小的时间片。

1）15:00～17:00 之间，每个小时的感染数量分别是 9，25 和 202，每个小时扩大约一个数量级，这是极早期快速感染阶段；

2）17:00～22:00 之间，每小时新增感染达到了一个较高水平，最高达到 2800/小时，这是第一次高峰阶段；

3）22:00～23:00 之间，感染速度逐渐下降，这应该是夜间更多机器关机导致，可以归纳为夜间自然下降阶段；

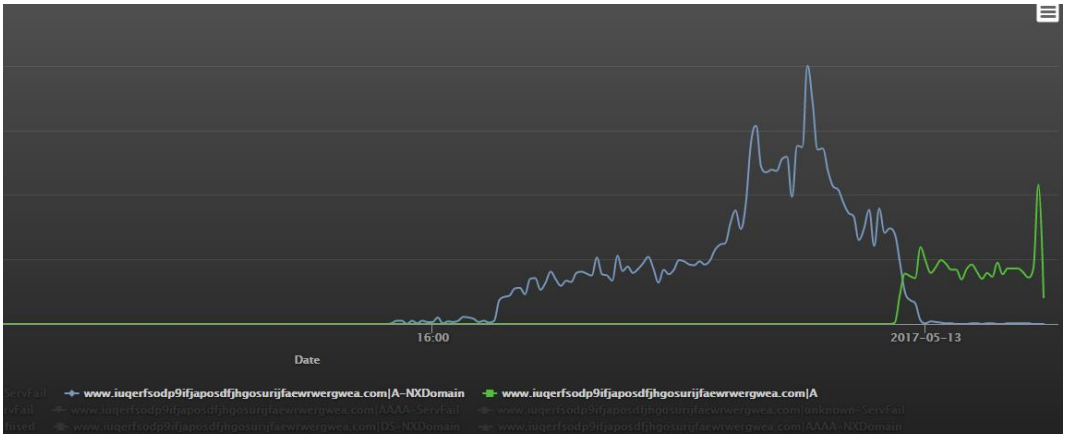
仔细观察这段时间的感染情况，可以得出以下结论：1)我们有理由认为 15:00 附近就是国内蠕虫最初感染发作的时间，尽管我们看到的仅是国内 DNS 数据的采样而非全部。这是因为最初的感染速度非常小，为个位数，并且在随后的每个小时内扩充约 1 个数量级，如果我们把时间向前追溯，就可以得到这个结论。2)压制域名的上线有重大意义：在整个早期感染阶段，蠕虫扩张的速度非常快，如果不是压制域名争取了时间，所有后续的防御行动都会困难很多。事实上，周五这天晚上 22:00 附近就是 WannaCry 感染速度的历史最高水平，即使是后来的周一早上上班大开机的时刻也没能超过这个水平。

（二） 域名压制阶段

开关域名于周五 23:30 左右上线，开始了对 WannaCry 的压制。这段时间也可以继续细分为如下若干时间片段。

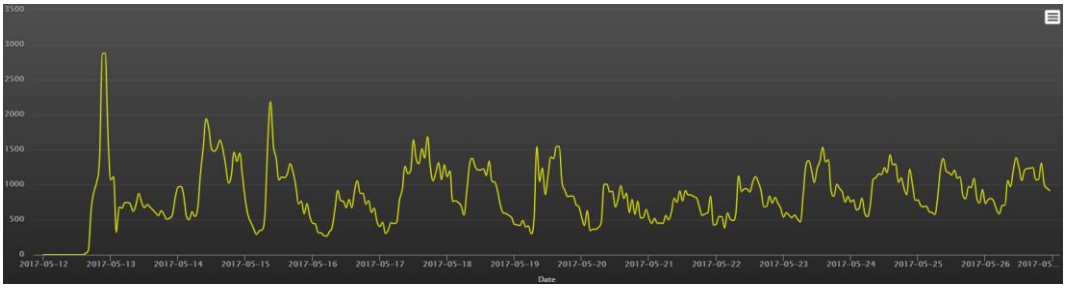
压制域名同步到全网阶段

由于 DNS 本身的缓存，压制域名虽然最早于 23:30 左右上线，但是这个案例中还需要大约 30 分钟才能让全网所有节点都能感知到。在这 30 分钟里，全网范围内 DNS 应答中，NXDOMAIN（域名不存在）和 A（回应 IP 地址）两种类型同时存在。前者在回落，后者在上升。域名上线后大约 5～10 分钟时，两条曲线出现十字交叉，域名上线 30 分钟后，NXDOMAIN 被压制到地板附近。



平稳控制阶段

NXDOMAIN 被压制以后，过度到了平稳控制阶段。在这个阶段，一方面，微软补丁更新和安全社区的共同努力减少了感染机器的数量；另一方面，总有机器因为各种原因被新增感染。总体而言，总感染量处于动态平衡状态，并且会随着时间推移最终平稳下降。从既往其他类似情况看，下降过程也许会耗费数年，并且往往会出现以周为单位的规律性波动



在这个阶段，有以下情况值得一提。

在 5 月 17 日以后，DNS 数据中信噪比逐渐下降，逐渐变得不再适合用来做分析和度量。这主要是由于开关域名被媒体和公众大量关注，越来越多的针对开关域名的访问是来自浏览器而非 WannaCry。

尽管如此，每天的 DNS 访问曲线仍然是不多的风向标之一。在感染的早期，每个人都无法预测 WannaCry 的后续发展趋向，只能严密监视域名访问情况。白天相对夜晚有个波峰，这是正常现象；周日的波峰比周六更高一些，没人知道这是个什么样的兆头；直到周一早晨 9:00 的波峰开始回落，确认周一读数小于周五，我们才能基本认为感染情况大体得到控制；随后，在周三和周四感染情况有所反弹，每个人的心又提到嗓子眼；直到再下一周数据整体回落，我们才能最终确认局势受控，从应急状态回到平稳的工作状态。

二、WannaCry 不同变种感染情况对比

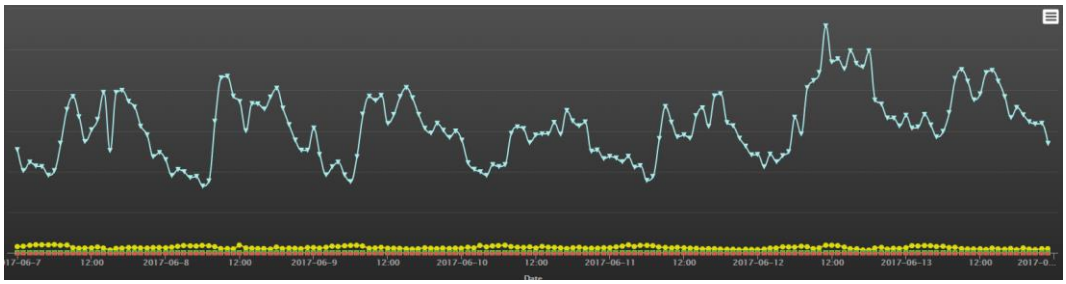
随着时间推移，不断有 WannaCry 的不同变种被曝光，有的样本去掉了对开关域名的检测（但是幸运的是该样本被改坏了，无法正常启动），有的样本使用了不同的开关域名，但是从 DNS 数据层面来看，除了原始版本，其他版本并没有得到广泛传播。

我们至少捕获到以下 WannaCry 变种样本：

- hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- hxxp://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- hxxp://www.udhridhfowhgibe9vheiviehfiehbfvieheifheih.com
- hxxp://www.iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- hxxp://www.ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com

对应域名的 DNS 访问曲线如图所示。

- 传播的主体，是 iuqerf 的原始版本；
- ifferf 版本有少量传播，比原始版本小了一个数量级；
- 其他版本只有零星访问或者干脆没有访问。



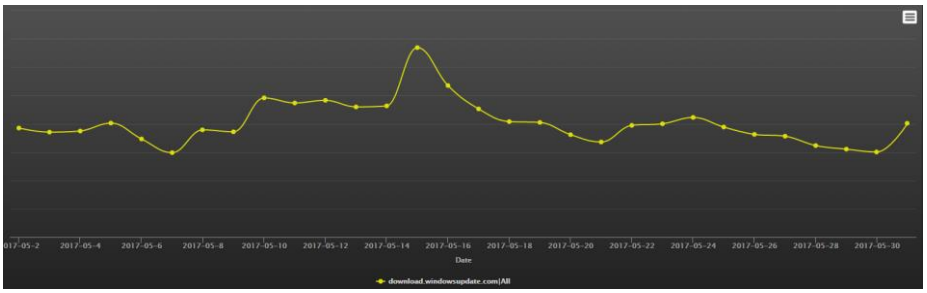
变种版本的感染范围远小于原始版本，也许可以归为补丁防御工作开始启动。无论如何，可以预期后续变种如果仅仅修改了开源域名，并不会比 ifferf 版本带来更大影响。总体而言，在这个案例中，非原始版本的 WannaCry 的感染情况不值得引起安全社区的密切关注。

三、微软 WSUS 补丁更新服务的访问情况

微软补丁是本次 WannaCry 防御体系的关键，理应获得比 WannaCry 变种更多的关注。查询微软 WSUS 服务的官网可知，WSUS 服务与下列域名访问有关：

- hxxp://windowsupdate.microsoft.com
- hxxp://download.windowsupdate.com
- hxxp://download.microsoft.com
- hxxp://test.stats.update.microsoft.com
- hxxp://ntservicepack.microsoft.com

简单查询可知，download.windowsupdate.com 的访问量最大，我们选用这个域名的 DNS 访问情况来代表补丁更新情况，如图所示。



通常而言，补丁更新分发的高峰是在“星期二补丁日”的第二天。按照惯例，微软是在每个月第二周的星期二发补丁，第二天（周三）是中国区用户更新的高峰时间。但是这一次，5 月 15 日（周一）当天出现了一个波峰。这种情况可以理解为系统网络管理员、个人在经过周六和周日的宣传后，大量用户在周一更新了微软补丁。

从这个意义上来说，这一次整个安全社区在周六、周日紧急行动起来，向社会和公众说明情况，提供防御手段和解决方案，是非常必要的。如果错过了周六和周日宣传准备的时间窗口，周一早上的开机时刻也许就是灾难时刻。

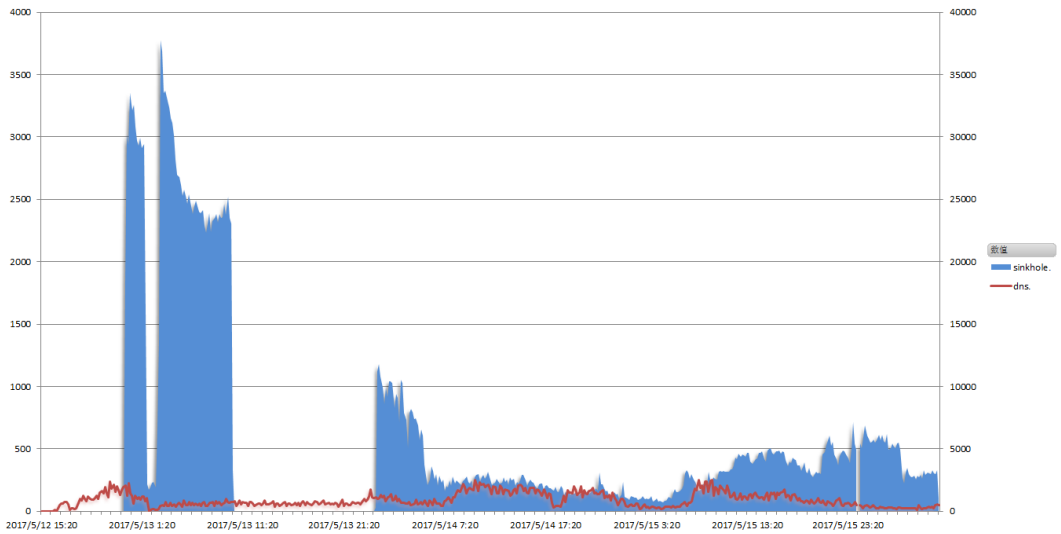
四、 从 sinkhole 视角看 WannaCry 的感染情况

如前所述，得益于 Kryptos Logic Vantage 对我们的信任，我们获得了域名 sinkhole 的关键日志。这段数据覆盖了全球，是 WannaCry 事件中全球视角的唯一权威数据。Kryptos Logic Vantage 授权我们展示部分统计信息。

我们得到的 sinkhole 数据，发生在北京时间 5 月 12 日 23:40～5 月 16 日 8:10，缺失了 5 约 13 日 10:30～5 月 14 日 00:20 之间的数据。这段数据显示，开关域名共计被访问了 266 万次，涉及 16 万个独立来源 IP。

五、 Sinkhole 与 DNS 数据对比分析

将 sinkhole 数据与 DNS 数据放在一起对比，可以清晰地进行分析。如图所示，蓝色部分为 sinkhole 数据，红色部分为 DNS 数据。DNS 数据在纵轴上缩放了 10 倍，以便清晰地展示数据的趋势。



按时间顺序解读图，可以得知：

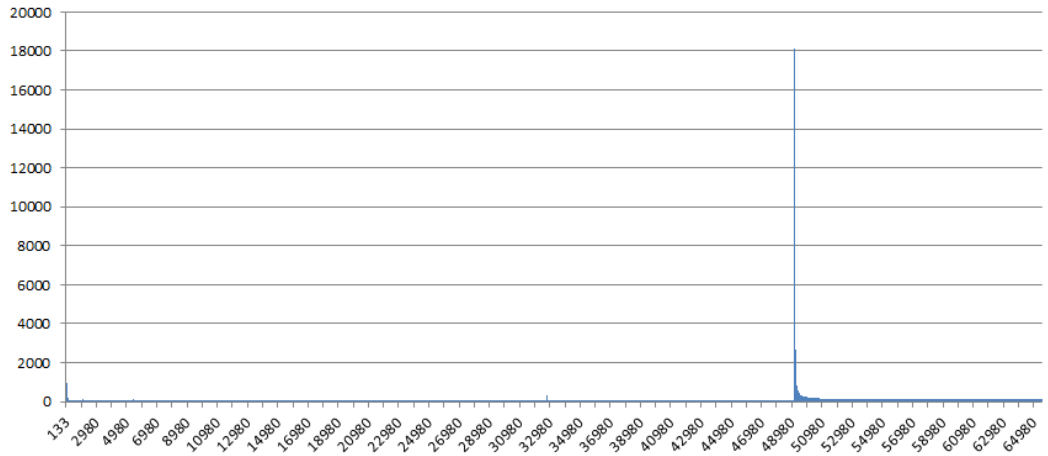
1）域名刚刚上线后的 5 个小时之内是 sinkhole 访问的历史高峰，每分钟约 3500 次；

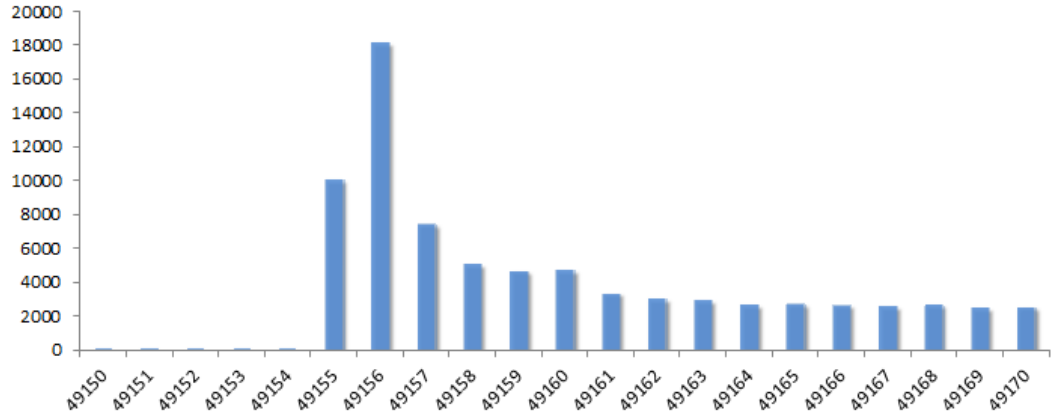
2）上线 6 小时后 sinkhole 访问数量开始持续回落，到北京时间 5 月 14 日 6 时许降低到高峰时段的十分之一，到 15 日 3 时为最低点，约为历史高峰水平的三十分之一。可以认为，域名上线，有效压制了蠕虫的发展；

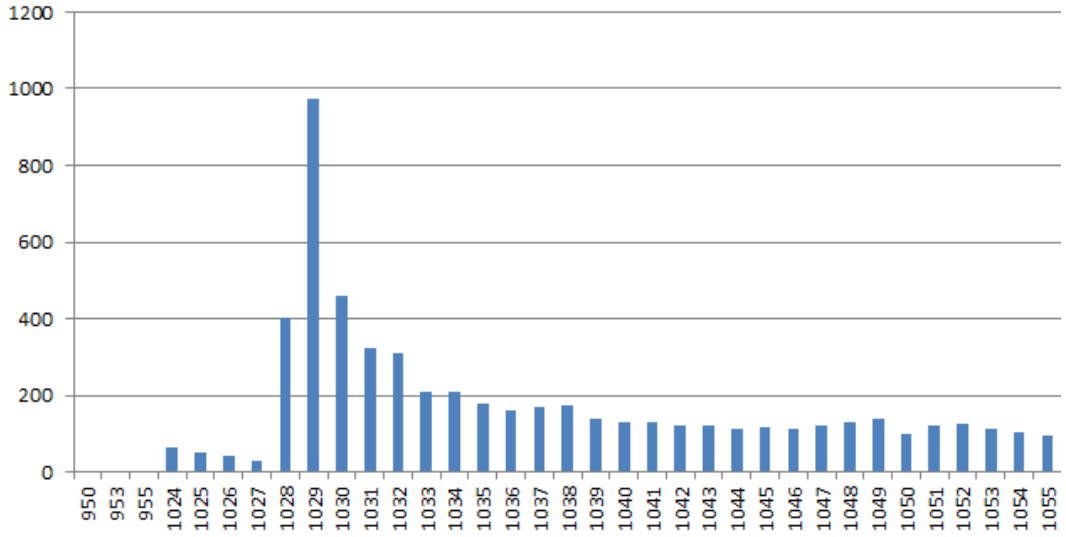
以上观察结果与之前 DNS 数据观察结果一致。我们猜测，缺失的 14 个小时的数据，趋势也是一直在下降。

六、来源端口和 Windows 动态端口范围设定

除了时序方面，来源端口方面的数据分布也引起了我们的注意。端口 49150 前后的来源访问次数差别非常大，端口 1024 前后也有一个局部的暴涨。下图分别是全端口分布、端口 49150 附近数据缩放以及端口 1024 附近数据缩放。







我们查到，Windows 操作系统对动态端口范围有如表所示的设定。

Windows Version	Dynamic Port Range	Source
Windows XP	1024～65535	non-official
Windows 2000 Professional	1024～65535	non-official
Windows Server 2003	1024～65535	non-official
Windows Vista	49152～65535	official
Windows7	49152～65535	official
Windows Server 2008	49152～65535	official

基于以上事实，我们有如下推测。

1）相当比例机器被感染的时机，发生在 Windows 刚刚启动完成的阶段，这时动态端口几乎都没有被使用，操作系统按照预设范围由低到高，给请求分配了范围下限附近的端口；

2）处在下限边缘但很少被使用到的端口，例如，49152/49153/49154 和 1024/1025/1026/1027，也许是被操作系统自身在启动过程中用掉；

3）绝大部分被感染版本是 Windows Vista/Windows 7/WindowsServer2008 及以后版本，之前版本感染的不多。

附录 4　360 安全卫士反勒索服务

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 5　360 天擎敲诈先赔服务

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，仍感染了勒索软件，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，自勒索软件出现之日起起，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”，对勒索软件进行全面的防御和拦截，已经帮助政企用户抵挡住了勒索软件的一轮又一轮攻击。

360 敲诈先赔细节条款见官网：http://360.net/special/agreement/agreement.html

截至本报告发布之日，正确使用 360 天擎并开启敲诈先赔功能的政企客户中，感染勒索软件的数量为“0”。

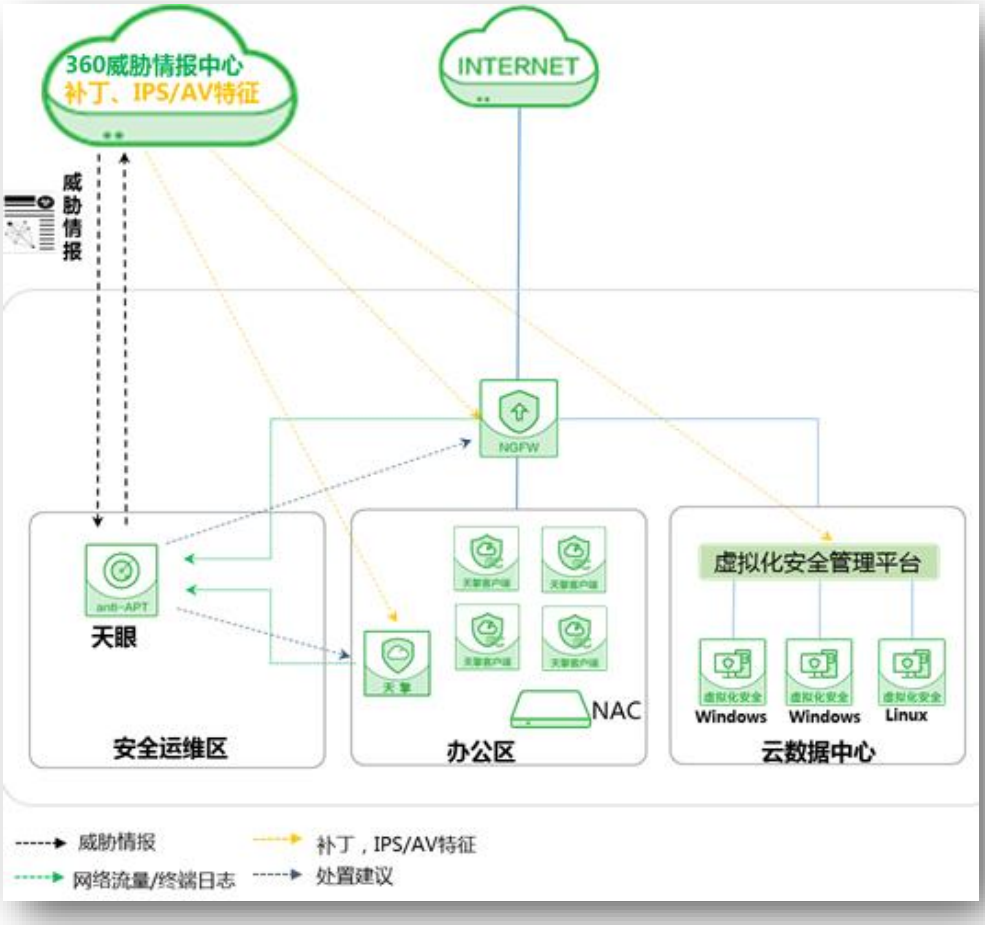
附录 6　360 勒索软件协同防御解决方案

360 勒索软件协同防御解决方案是 360 企业安全为了帮助政企单位规避勒索软件等新兴安全威胁而推出的整体解决方案，全面兼顾事前、事中、事后不同阶段的不同安全需求，通过安全运营提升安全管理水平和响应处置能力，通过威胁情报提前洞悉风险隐患，通过协同防御响应处置威胁，通过百万敲诈先赔免除后顾之忧，让政企单位能够更加从容的面对日益猖獗的勒索软件等安全威胁。

方案构成

大数据分析是安全可见的基础，而威胁情报则是能否发现威胁的关键。传统的安全防御措施缺乏大数据存储与分析挖掘能力，也没有丰富的威胁情报作为支撑，产品之间更是各自为政，因此很难及时发现并层层阻断高级威胁。

基于安全协同的理念，360 勒索软件协同防御解决方案为客户构建了威胁情报驱动的，终端安全、边界安全、大数据分析等安全设备联动的纵深防御体系，将威胁情报与数据分析能力贯穿于监测与防御体系，通过对云端威胁情报、边界网络流量与本地终端数据的汇总分析与协同响应，以及持续高效的安全运营，让政企客户能够对勒索软件等新兴安全威胁“看得见、防得住、查得清、搞得定”。



方案特点

1） 基于威胁情报的预警服务

2） 边界+终端+威胁情报多层次智慧防御体系

3） 特征+威胁情报多维检测精准告警

4） 大数据驱动的自动化+人工有效响应机制

5） 百万敲诈先赔保障

应用价值

构建完整防御架构。防御手段必须完善才能不给勒索软件可乘之机。这就需要充分考虑到每一个可能突破的薄弱环节，例如安全主机加固、安全域划分、终端准入机制、安全运维体系。

提供增强持续监测能力。攻击随时都在发生，安全系统应该也要适应动态的安全环境，因此要充分考虑对安全状态持续的监测及对突发安全威胁及时遏制的能力。

建立及时响应处置机制。防御系统随时可能被攻破，为减少攻击造成的损失，需要建立正确的应急响应流程，减少处理中流程错误情况；能够自动化的响应处置，加快处理速度；具有溯源取证能力，以便了解攻击来源途径。

建立安全预警规范。建立与安全厂商实时联动的安全预警中心，实时获取最新的安全动态，更新自身的安全系统。在下一次攻击发生之前与安全厂商共同完成对内的预警动作。

增强云虚拟化场景下的主机防护能力。近年来，云计算已经广泛应用，运行 Windows Server 及 Linux 的 VM 也会面临蠕虫勒索病毒的威胁。因此，云平台的安全隐患也需要给予高度重视。