WannaCry 一周年

勒索软件威胁形势分析报告

360 互联网安全中心

2018 年 5 月 11 日

主要观点

- 2017 年 5 月 WannaCry（永恒之蓝勒索蠕虫）大规模爆发以来，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。
- Crysis、Cerber、GlobeImposter 和 WannaCry 是勒索软件的四大家族，这四大家族的受害者数量占到所有受害者总数的 66.0%。
- 针对中国用户的勒索软件攻击，九成以上来自境外，其中四成来自美国。统计显示：在针对中国电脑用户的勒索软件攻击中，93.5%的攻击来自境外；其中，来自美国的攻击最多，占比高达 42.2%；其次是俄罗斯，占比为 11.3%；来自中国本土的攻击量排第三，占比为 6.5%；荷兰、乌克兰分别排在第四和第五。
- 在向 360 互联网安全中心求助的勒索软件受害者中，75.2%的被感染电脑使用的是 Windows Server 操作系统，受害者多为中小企业。这再次表明了勒索软件攻击者已经将主要攻击目标从高价值个人转向了企业服务器。造成这种情况的主要原因可能是企业为服务器支付赎金的意愿相对更高。
- WannaCry 之所以能够穿透内网，攻击被隔离的网络设备，主要是因为以下六种原因：一机双网缺乏有效管理、缺陷设备被带出办公区、协同办公网络未完全隔离、防火墙未关闭 445 端口、办公网与生活网未隔离、外网设备分散无人管理。
- 2017 年以来，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。
- 未来一年，勒索软件的质量和数量还将持续不断攀升，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。
- 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。

摘　要

- 2017 年全年，国内共有约有 505.7 万台电脑遭到勒索软件攻击。如果从 WannaCry 大规模爆发的 5 月开始计算，2017 年 5 月到 2018 年 4 月，全国共有约 463.5 万台电脑遭到了勒索软件攻击。2017 年 11 月是勒索软件攻击的最高峰。

- Crysis、Cerber、GlobeImposter 和 WannaCry 这四大勒索软件家族的受害者最多，共占到总量的 66.0%。其中，Crysis 占比为 23.6%，Cerber 占比为 15.4%，GlobeImposter 占比为 14.3%，WannaCry 占比为 12.8%。

- 统计显示，2018 年 1-4 月，在向 360 互联网安全中心求助的勒索软件受害者中，制造业是遭受攻击最多的行业，占比约为 23.1%；其次是互联网企业，占比约为 15.7%；外贸行业排第三，占比约为 10.6%。

- 通过对受害者电脑的远程取证，360 互联网安全中心对 2018 年 1-4 月间，勒索软件攻击者的 IP 信息进行了深入分析。统计显示：在针对中国电脑用户的勒索软件攻击中，93.5%的攻击来自境外；其中，来自美国的攻击最多，占比高达 42.2%；其次是俄罗斯，占比为 11.3%；来自中国本土的攻击量排第三，占比为 6.5%；荷兰、乌克兰分别排在第四和第五。

- 在向 360 互联网安全中心求助的勒索软件受害者中，广东省受害者最多，约占全国总量的 23.5%，其次是浙江省和江苏省，约占全国受害者求助总数的 7.4%，排名第四的是北京，约占 5.6%，山东排名第五，约占 5.3%。

- 在向 360 互联网安全中心求助的勒索软件受害者中，75.2%的被感染的电脑使用的是 Windows Server 操作系统。具体来看，Server2008/2008 R2 占比最高，达 55.3%，其次是 Server2012/2012 R2，占比约为 18.9%，Win7/Win7 SP1 排第三，占比约为 15.5%。

- 2017 年 5 月-2018 年 4 月，国内至少有约有 368.5 万台电脑遭到了 WannaCry 的攻击，其中，2017 年 9 月是攻击最高峰，2018 年 2 月大幅减少后，在随后的 3 月又开始反弹。

- WannaCry 之所以能够穿透内网，攻击被隔离的网络设备，主要是因为以下六种原因：一机双网缺乏有效管理、缺陷设备被带出办公区、协同办公网络未全隔离、防火墙未关闭 445 端口、办公网与生活网未隔离、外网设备分散无人管理。

- 2017 年以来，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。

- 未来一年，勒索软件的质量和数量还将持续不断攀升，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。

- 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

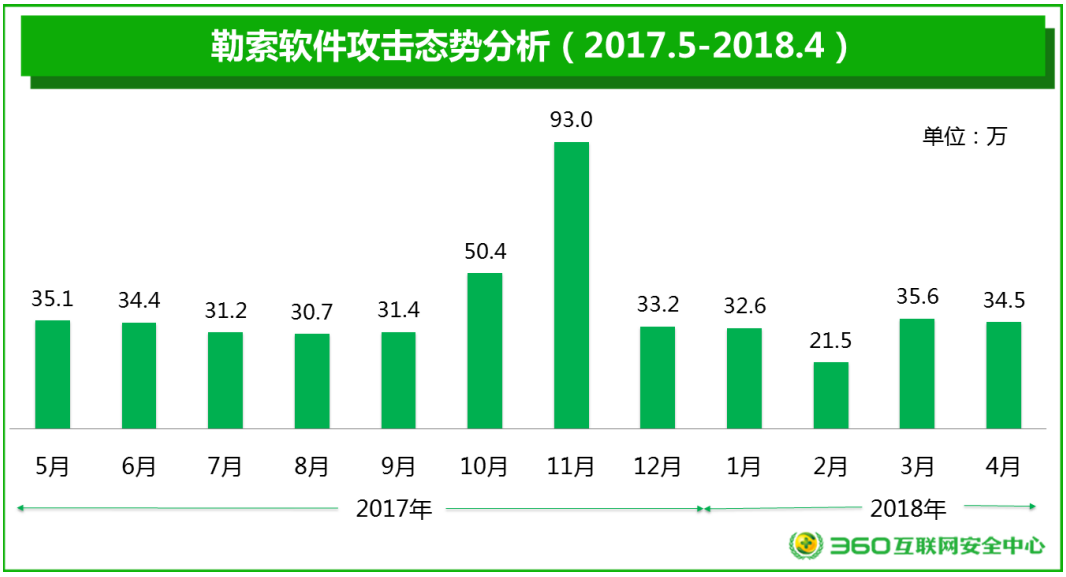
第一章　勒索软件的大规模攻击

2017 年 5 月 WannaCry（永恒之蓝勒索蠕虫）大规模爆发以来，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 5 月-2018 年 4 月期间，360 互联网安全中心监测到的勒索软件活动情况进行分析。

一、　勒索软件的攻击量

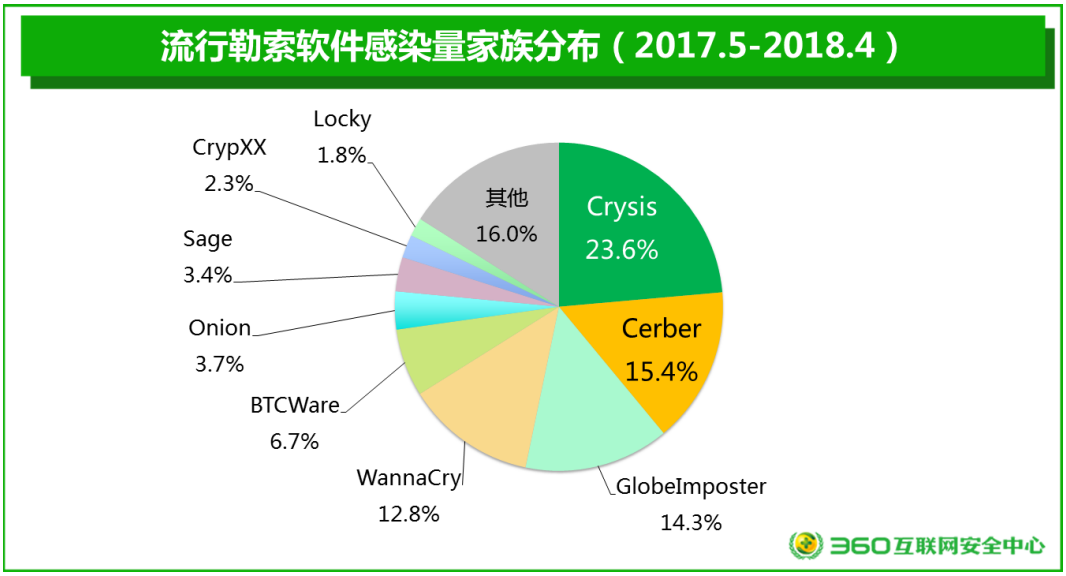
根据 360 互联网安全中心的监测数据显示，2017 年全年，国内共有约 505.7 万台电脑遭到勒索软件攻击。如果从 WannaCry 大规模爆发的 5 月开始计算，2017 年 5 月到 2018 年 4 月，全国共有约 463.5 万台电脑遭到了勒索软件攻击。

下图给出了在 2017 年 5 月-2018 年 4 月期间，勒索软件每月攻击用户数量的情况。其中 11 月是攻击最高峰，一天之内被攻击的电脑平均可达 3.1 万台。特别说明，此部分攻击态势分析数据不包含 WannaCry 勒索蠕虫的相关数据。



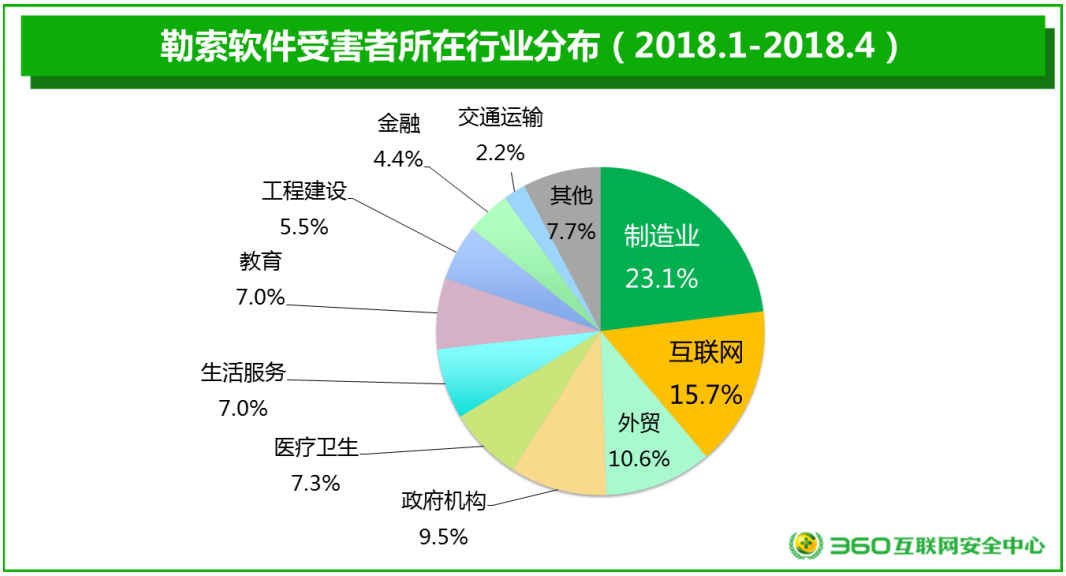
二、　勒索软件家族分布

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，Crysis、Cerber、GlobeImposter 和 WannaCry 这四大勒索软件家族的受害者最多，共占到总量的 66.0%。其中，Crysis 占比为 23.6%，Cerber 占比为 15.4%，GlobeImposter 占比为 14.3%，WannaCry 占比为 12.8%。各勒索软件家族分布具体如下图所示。



三、 勒索软件受害者行业分布

统计显示，2018 年 1-4 月，在向 360 互联网安全中心求助的勒索软件受害者中，制造业是遭受攻击最多的行业，占比约为 23.1%；其次是互联网企业，占比约为 15.7%；外贸行业排第三，占比约为 10.6%。勒索软件受害者的具体行业分布如下图所示。

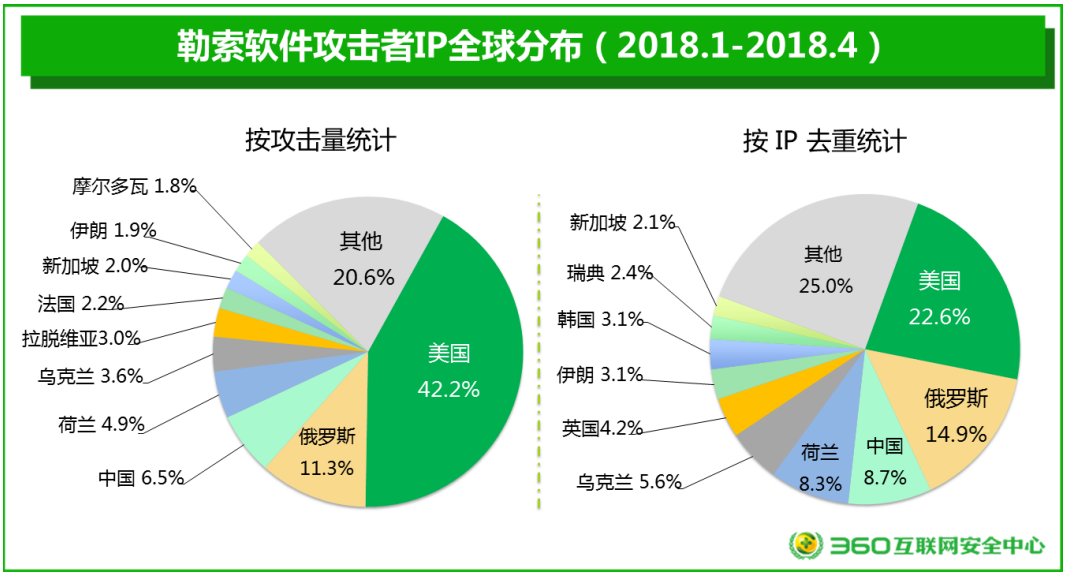


而在 2017 年的统计中，能源行业是遭受攻击最多的行业，占比为 42.1%，其次为医疗行业为 22.8%，金融行业为 17.8%。

四、 勒索软件攻击者地域分布

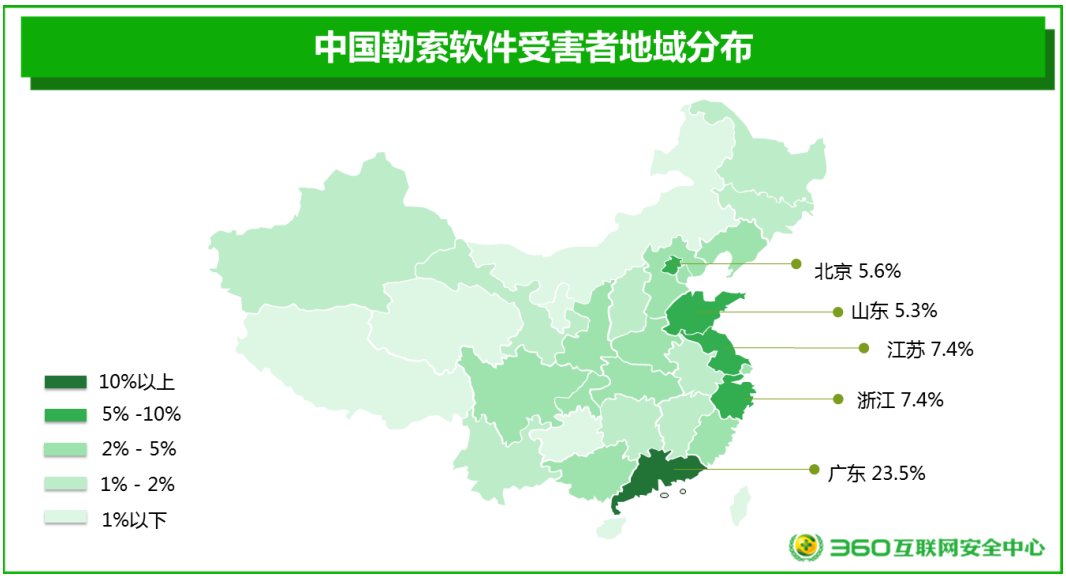
通过对受害者电脑的远程取证，360 互联网安全中心对 2018 年 1-4 月期间，勒索软件攻击者的 IP 信息进行了深入分析。统计显示：在针对中国电脑用户的勒索软件攻击中，93.5%的攻击来自境外；其中，来自美国的攻击最多，占比高达 42.2%；其次是俄罗斯，占比为 11.3%；来自中国本土的攻击量排第三，占比为 6.5%；荷兰、乌克兰分别排在第四和第五。

而如果对攻击者 IP 进行去重统计，则美国、俄罗斯、中国、荷兰和乌克兰仍然是针对中国境内用户发动勒索软件攻击排名前五的国家。其中，美国攻击者 IP 数量的占比为 22.6%；俄罗斯为 14.9%，而来自中国的攻击者 IP 数量占比为 8.7%。



五、 勒索软件受害者地域分布

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，广东省受害者最多，约占全国总量的 23.5%，其次是浙江省和江苏省，约占全国受害者求助总数的 7.4%，排名第四的是北京，约占 5.6%，山东排名第五，约占 5.3%。

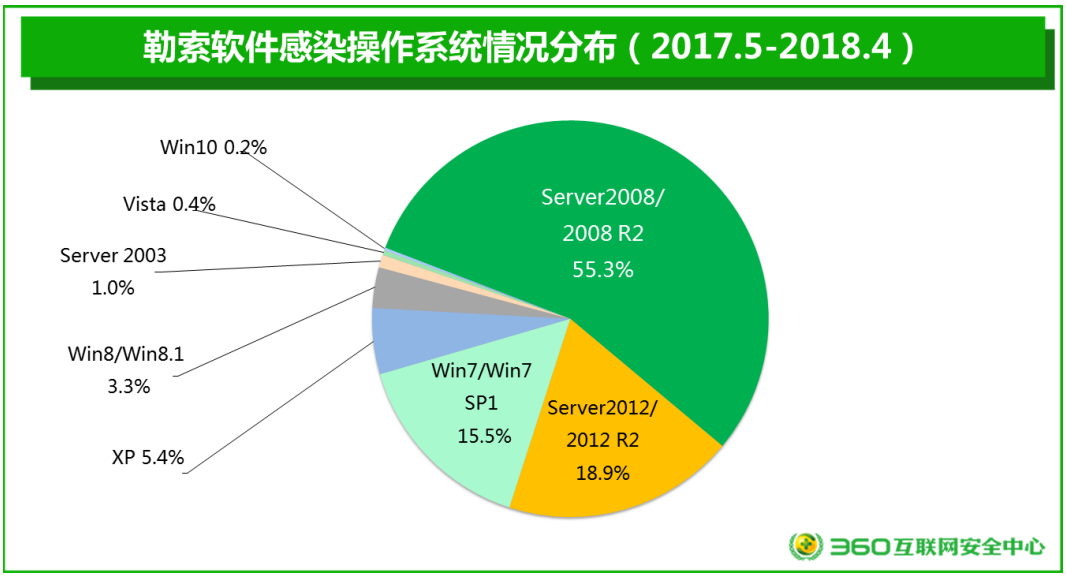


六、 勒索软件感染操作系统分布

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，75.2%的被感染电脑使用的是 Windows Server 操作系统，受害者多为中小企业。这再次表明了勒索软件攻击者已经将主要攻击目标从高价值个人转向了企业服务器。造成这种情况的主要原因可能是企业为

服务器支付赎金的意愿相对更高。

从求助的受害者被感染电脑所使用的具体操作系统来看，Server2008/2008 R2 占比最高，达 55.3%，其次是 Server2012/2012 R2，占比约为 18.9%，Win7/Win7 SP1 排第三，占比约为 15.5%。



第二章　WannaCry 攻击分析

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。

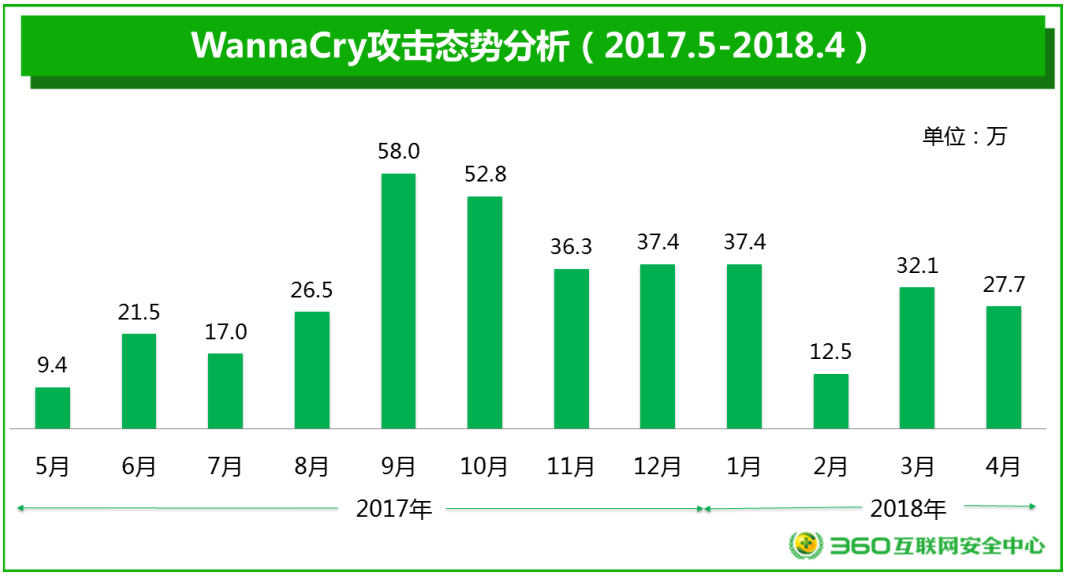
一、 勒索蠕虫的空前影响

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。

监测数据显示，2017 年 5 月-2018 年 4 月，国内至少有约有 368.5 万台电脑遭到了 WannaCry 的攻击，其中，2017 年 9 月是攻击最高峰，2018 年 2 月大幅减少后，在随后的 3 月又开始反弹。不过，2017 年 5 月以后，WannaCry 的攻击虽然仍然持续存在，但实际发作并锁死用户电脑的事情已经微乎其微。



二、 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。

三、 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 1 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。

第三章　勒索软件的攻击特点

2017 年以来，勒索软件的攻击主要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 年以来，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

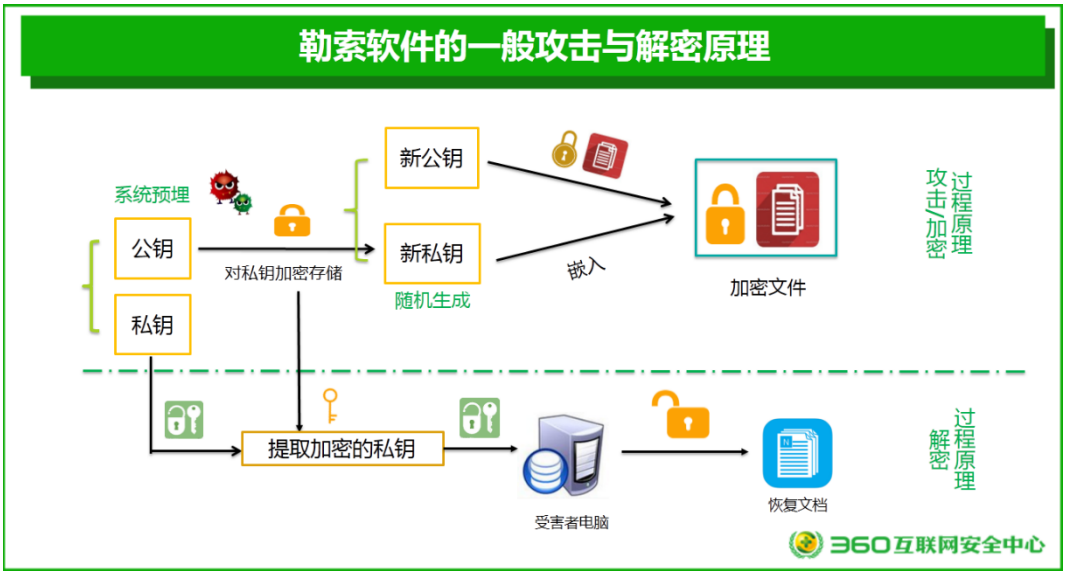
3）　把新生成的私钥采用黑客预埋的公钥进行加密保存在一个 ID 文件或嵌入在加密文件里

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 年以来，勒索软件的攻击进一步聚焦在高利润目标上，特别是针对中小企业网络服务器的攻击急剧增长。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。而到了 2018 年 1-4 月，被勒索软件感染的电脑中，75.2%为 Windows Server 服务器，受害者多为中小企业。可见，勒索软件攻击者将主要攻击目标从高价值个人转向了企业服务器的趋势更加明显，而且目标转移的速度非常之快。

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

传统的勒索软件攻击，大多是以高价值个人为攻击目标。而 2017 年以来，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 年以来，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。

第四章　勒索软件趋势预测

2017 年以来，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。本章将给出我们对未来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 2017 年 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”。

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 2　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。

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。

第五章　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。