2018勒索病毒白皮书(政企篇)

360终端安全实验室

2019年2月

摘 要

* 2018年，勒索病毒攻击整体态势以服务器定向攻击为主，辅以撒网式无差别攻击手段。
* 2018年共有430余万台（只包括国内且不含WannaCry数据）计算机遭受勒索病毒攻击；GandCrab、GlobeImposter、CrySis这三大家族勒索病毒的受害者最多，合计占比高达80.2%；勒索病毒最常使用的攻击手段是远程桌面弱口令暴力破解攻击。
* 勒索病毒对政企单位的攻击以单点试探为主，79.8%仅尝试攻击一台终端；政府行业的单位最容易遭到勒索病毒攻击，占被攻击单位总数的21.0%；金融行业的终端最容易遭到勒索病毒攻击，占被攻击终端总数的31.8%。
* 5月是政企单位感染勒索病毒的最高峰，其数值是最低谷（2月）的5.3倍；政府单位是感染勒索病毒的重灾区，被感染数量占被感染单位总数的24.1%；GlobeImposter最难防范，34.0%的受害政企单位感染了该勒索病毒；各大勒索病毒都爱感染政府行业。
* 政企单位可以通过业务系统无法访问、电脑桌面被篡改、文件后缀被篡改等方式判断是否感染了勒索病毒。如果已经感染了勒索病毒，建议通过隔离中招主机、排查业务系统、联系专业人员进行自救等多种方式，在等待专业人员救助之前有效止损。
* 政企单位防范勒索病毒建议从七个方面着手，即及时更新最新的补丁库、杜绝弱口令、重要资料定期隔离备份、提高网络安全基线、保持软件使用的可信、选择正确的反病毒软件、建立高级威胁深度分析与对抗能力。

目 录

[第一章，勒索病毒整体攻击态势 1](#_Toc1403014)

[一、 整体态势 1](#_Toc1403015)

[二、 活跃家族 1](#_Toc1403016)

[三、 传播特点 2](#_Toc1403017)

[第二章，政企遭遇勒索攻击分析 5](#_Toc1403018)

[一、 攻击力度 5](#_Toc1403019)

[二、 感染分析 6](#_Toc1403020)

[第三章，勒索病毒发展趋势预测 9](#_Toc1403021)

[一、 紧跟漏洞发展步伐 9](#_Toc1403022)

[二、 更多的传播方式 9](#_Toc1403023)

[三、 攻击面和目标扩大化 9](#_Toc1403024)

[四、 被攻击的设备种类不断扩大 9](#_Toc1403025)

[第四章，勒索病毒应急响应指南 10](#_Toc1403026)

[一、 如何判断中毒 10](#_Toc1403027)

[二、 如何紧急自救 11](#_Toc1403028)

[三、 如何进行恢复 11](#_Toc1403029)

[四、 如何避免中毒 13](#_Toc1403030)

[附录1、2018热点勒索病毒事件 15](#_Toc1403031)

[附录2、关于360终端安全实验室 17](#_Toc1403032)

[附录3、关于360天擎新一代终端安全管理系统 17](#_Toc1403033)

[附录4、关于360天擎终端安全响应系统 18](#_Toc1403034)

# 第一章，勒索病毒整体攻击态势

2018年，勒索病毒攻击特点也发生了变化：2017年，勒索病毒由过去撒网式无差别攻击逐步转向以服务器定向攻击为主，而2018年，勒索病毒攻击则以服务器定向攻击为主，辅以撒网式无差别攻击手段。

## 整体态势

### 摘要：2018年共有430余万台计算机遭受勒索病毒攻击，12月攻击最盛。

根据360互联网安全中心的数据（包括360安全卫士和360杀毒的查杀数据），2018年共计430余万台计算机遭受勒索病毒攻击（只包括国内且不含WannaCry数据）。值得关注的是，在2018年11月和12月，由于GandCrab勒索病毒增加了蠕虫式（蠕虫下载器）攻击手段以及Satan勒索病毒加强了服务器攻击频次，导致攻击量有较大上升。



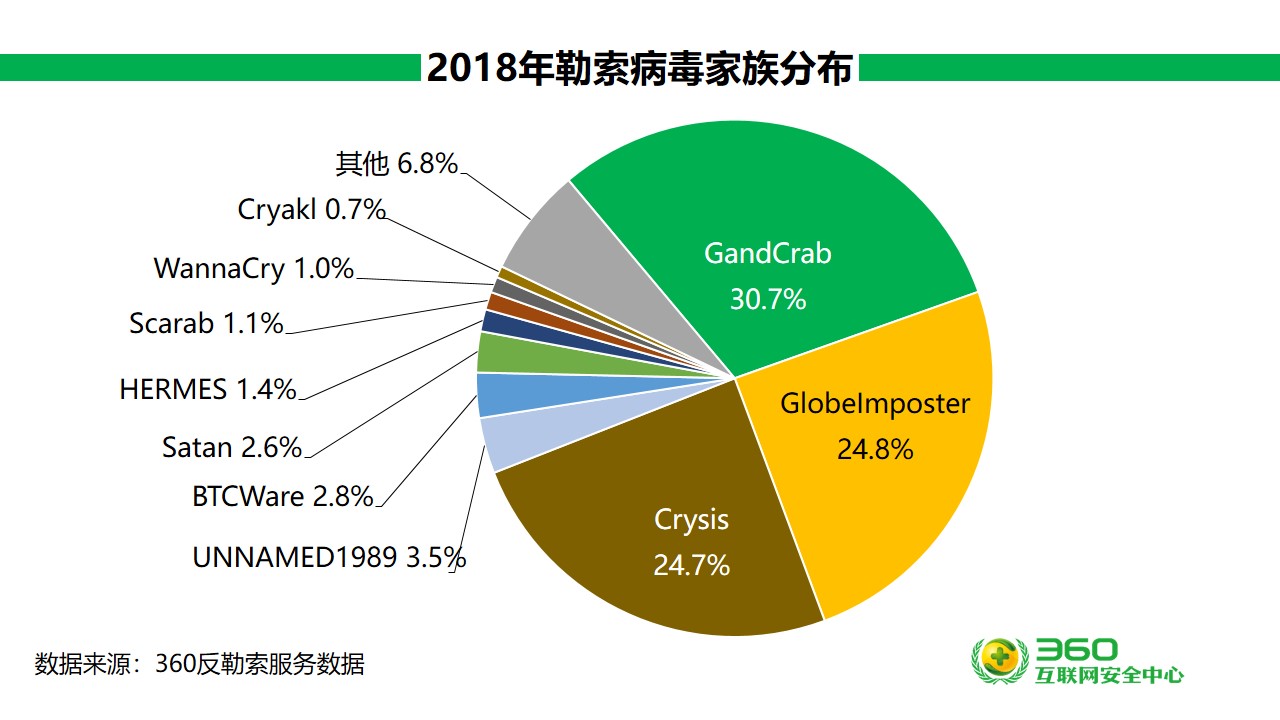
需要指出的是，以上趋势仅基于监控数据，实际许多用户是黑客通过服务器攻击渗透入侵内网后投放的勒索病毒，亦或用户终端不联网通过内网其他机器感染的勒索病毒，这些情形下是无法监控到数据的。

## 活跃家族

### 摘要：2018年GandCrab、GlobeImposter、CrySis这三大家族勒索病毒的受害者最多，合计占比高达80.2%。

根据360反勒索服务统计的数据，2018年GandCrab、GlobeImposter、CrySis这三大家族勒索病毒的受害者最多，合计占比约80.2%。本年度的活跃家族除了少数病毒，都有针对政企用户进行的攻击，因此企业用户仍然是勒索病毒最热衷的攻击对象。360终端安全实验室统计的用户反馈数据，大体和这个数据类似，后文将有详细分析。

以下是360反勒索服务统计数据得到的分析图：



## 传播特点

### 摘要：2018年度勒索病毒最常使用的攻击手段是远程桌面弱口令暴力破解攻击。

勒索病毒采用的传播手段和其他病毒类似，不过2018年度最为常用的攻击手段却是远程桌面弱口令暴力破解攻击，大量政企、个人用户反馈的勒索病毒都是基于此攻击方式。

下面根据病毒传播影响范围、危害大小列出最常用的几种攻击方式。

### 1.弱口令攻击

有多种系统或软件的弱口令遭受攻击，这里勒索病毒最常用的是远程桌面登录弱口令。除此外，勒索病毒弱口令攻击还包括针对数据库系统、Tomcat管理账户、VNC等弱口令的攻击。

### 2.U盘蠕虫

U盘蠕虫过去主要用于传播远控和挖矿病毒，但在2018年11月突然出现传播GandCrab勒索病毒的现象。360终端安全实验室曾对该类蠕虫做了详细分析，具体可参见：

https://mp.weixin.qq.com/s?\_\_biz=MzI2MDc2MDA4OA==&mid=2247485868&idx=1&sn=96ccb8bd5f34d2187173abc49bdad18e

这种传播方式的出现，导致2018年11月GandCrab勒索病毒突然成规模的爆发，令许多用户遭受攻击。

### 3.系统、软件漏洞

由于许多用户安全意识不足，导致许多NDay漏洞被黑客利用进行攻击。2018年，有多个勒索软件家族通过Windows系统漏洞或Web应用漏洞入侵Windows服务器。其中最具代表性的当属Satan勒索病毒，Satan勒索病毒最早于2018年3月在国内传播，其利用多个Web应用漏洞入侵服务器，如下表所示。

|  |
| --- |
| **简述\漏洞编号** |
| JBoss反序列化漏洞CVE-2017-12149 |
| JBoss默认配置漏洞CVE-2010-0738 |
| JBoss默认配置漏洞CVE-2015-7501 |
| WebLogic反序列化漏洞CVE-2017-10271 |
| Put任意上传文件漏洞 |
| “永恒之蓝”相关漏洞 CVE-2017-0146 |
| Struts远程代码执行漏洞S2-052（仅扫描）CVE-2017-9805 |
| WebLogic任意文件上传漏洞CVE-2018-2894 |
| Spring Data Commons远程代码执行漏洞CVE-2018-1273 |

### 4.其他攻击方式

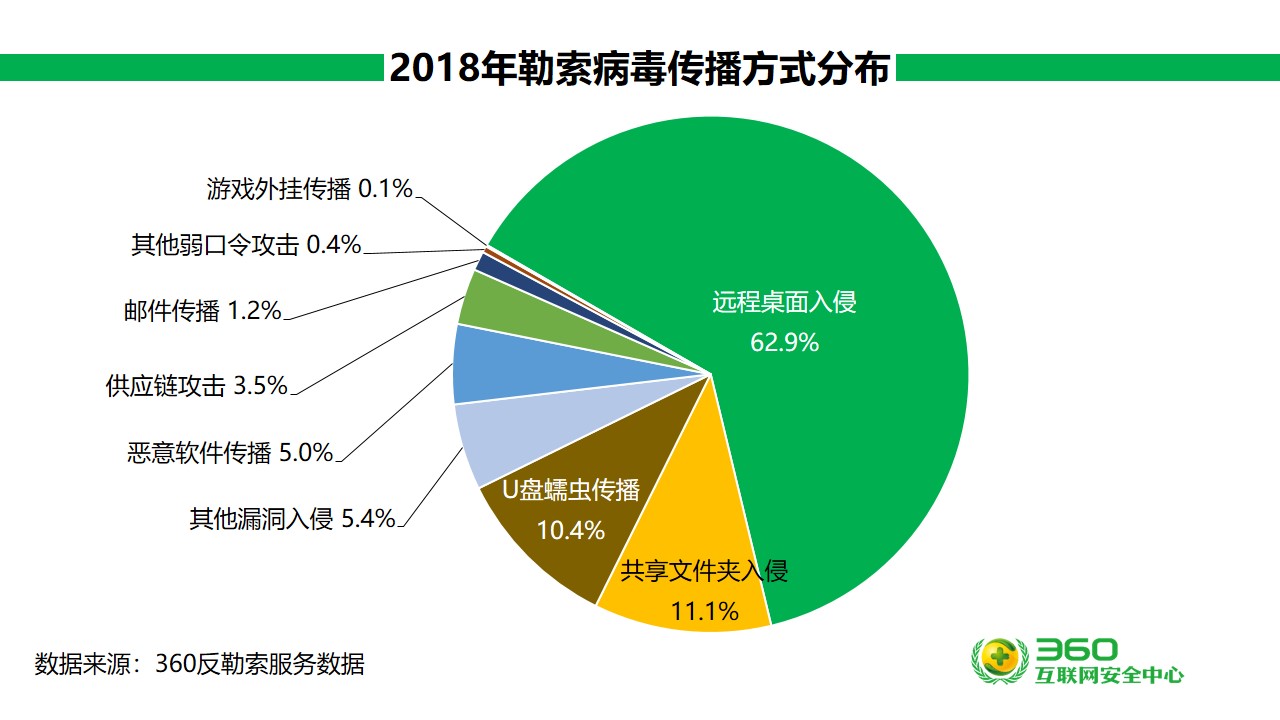
相比前面几种攻击方式，其他攻击方式的影响要小不少，这些方式主要包括：

（1）软件供应链攻击：以unnamed1989勒索病毒（“微信支付勒索病毒”）为代表，该勒索病毒主要是因为开发者下载了带有恶意代码的易语言第三方模块，导致调用该模块所开发出来的软件均被感染了恶意代码。根据统计，在此次事件中被感染的软件超过50余种。此外RushQL Oracle数据库勒索病毒也属于软件供应链攻击。

（2）无文件攻击方式：比如GandCrab勒索病毒就采用了“无文件攻击”进行传播，其技术原理主要通过Powershell将GandCrab编码加密后以内存载荷方式加载运行，实现全程无恶意代码落地，从而躲避安全软件的检测。

（3）邮件附件传播：这种方式通过邮件附件传播病毒下载器，诱使用户点击运行下载器下载勒索病毒后中毒。此方式在2016-2017年是勒索病毒最常见的传播方式，但在2018年已经很少被采用。

下图是360反勒索平台接收到的反馈案例统计，可以看到通过远程桌面弱口令攻击方式传播的案例占比最高，高达62.9%，其次是共享文件被加密，占比为11.1%，而通过U盘蠕虫进行传播的案例占比则为10.4%。



（以上数据直接引用360互联网安全中心的数据）

# 第二章，政企遭遇勒索攻击分析

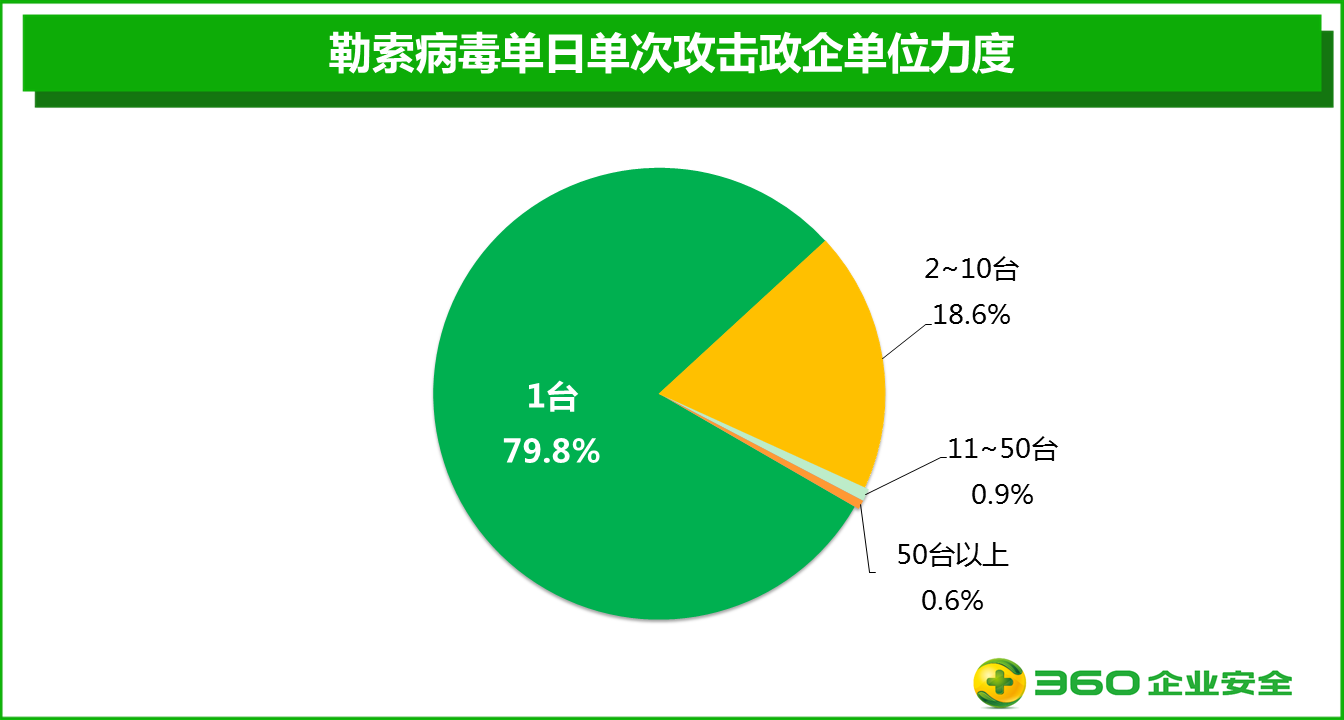
由于感染政企客户更有可能获得赎金，再加上勒索病毒本身也以服务器定向攻击为主，所以，2018年政企客户被勒索病毒攻击的势头尤其凶猛，各行各业都遭到了无差别攻击。

## 攻击力度

本节数据来自360企业安全公有云安全监测数据（只包括国内且不含WannaCry数据），以每日被攻击终端为基本研究单位，本地已经可以查杀的勒索病毒不在统计之列。

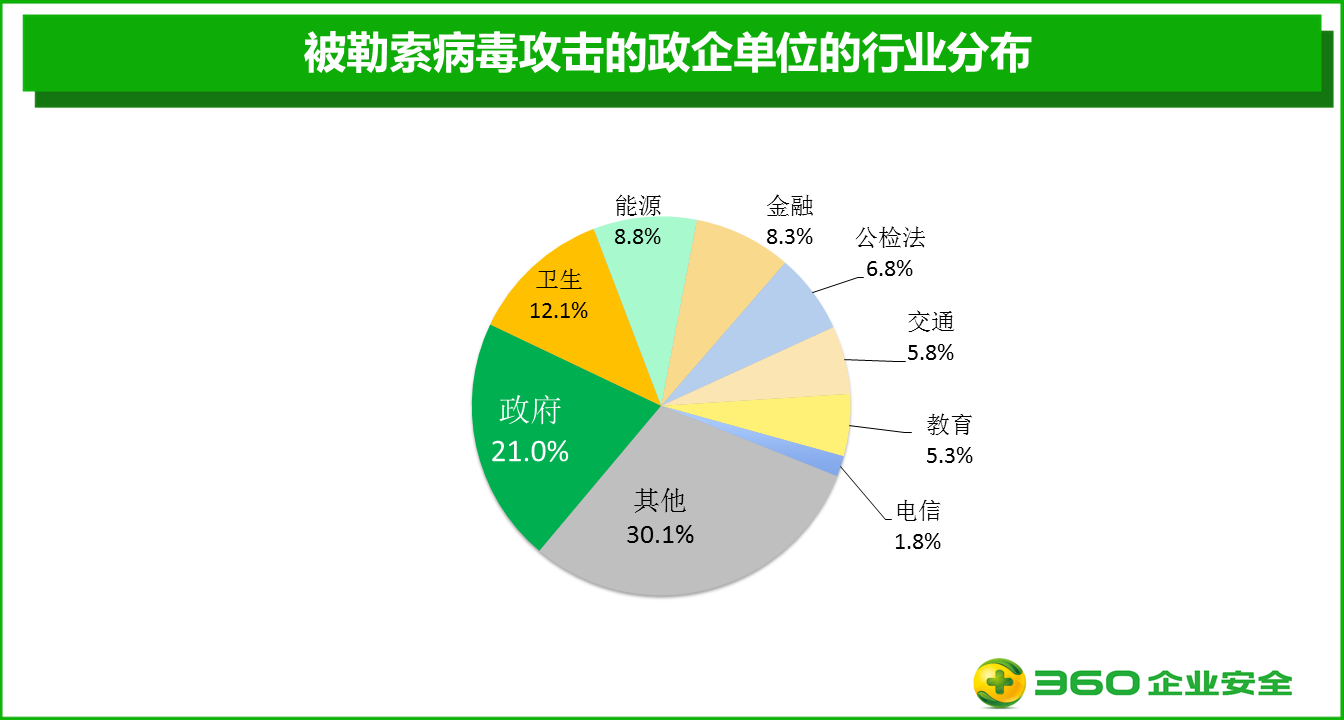
### 摘要：勒索病毒对政企单位的攻击以单点试探为主，79.8%仅尝试攻击一台终端。

在政企单位所遭遇的勒索病毒攻击事件中，单日单次攻击事件仅针对一台终端的比例占到攻击事件总量的79.8%，仅有0.6%的攻击事件针对的终端总数超过50台。



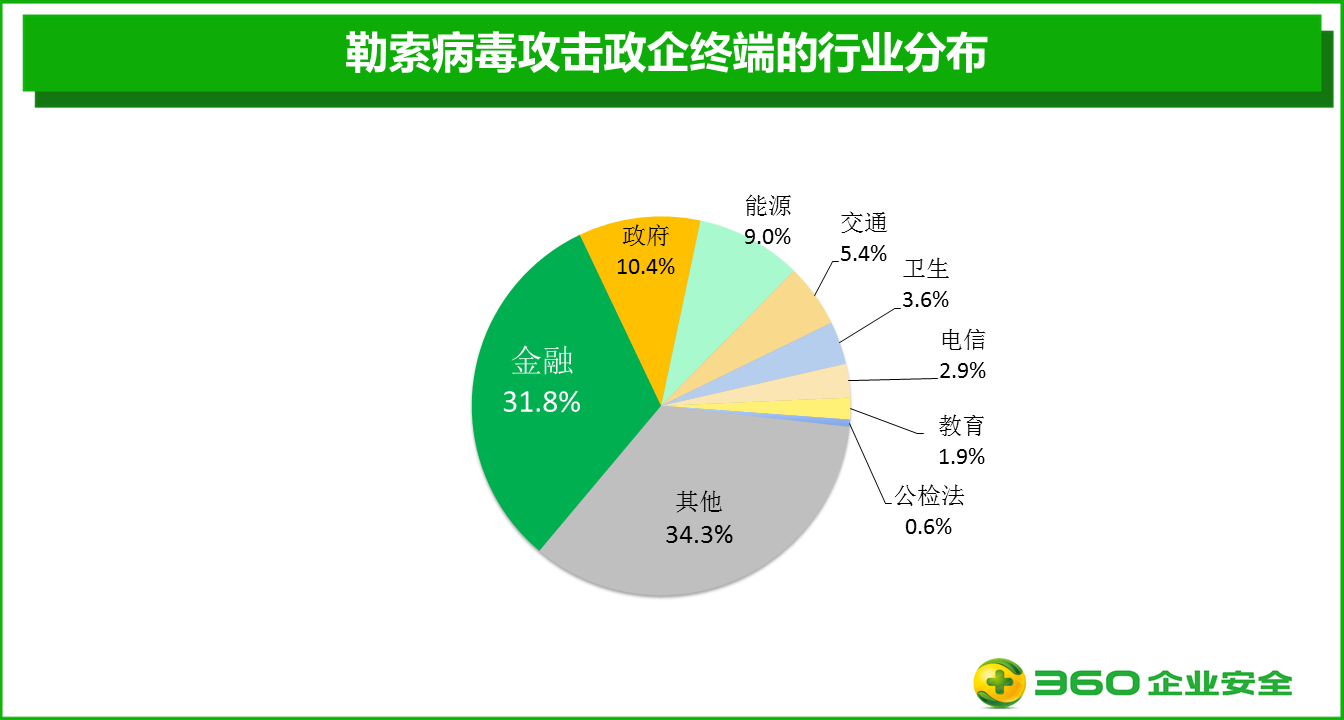
### 摘要：政府行业的单位最容易遭到勒索病毒攻击，占被攻击单位总数的21.0%。

在遭遇勒索病毒攻击的政企单位中，政府单位的数量最多，占到被攻击单位总数的21.0%；其次是卫生、能源单位，占比分别为12.1%、8.8%。



### 摘要：金融行业的终端最容易遭到勒索病毒攻击，占被攻击终端总数的31.8%。

在遭遇勒索病毒攻击的政企终端中，金融行业终端最多，占到总攻击终端数量的31.8%；其次是政府、能源终端，占比分别为10.4%、9.0%。



## 感染分析

本节数据来自360终端安全实验室接到的政企单位感染勒索病毒后的应急响应请求。总体政企用户感染范围达到历史新高，可以说是前所未有的影响。

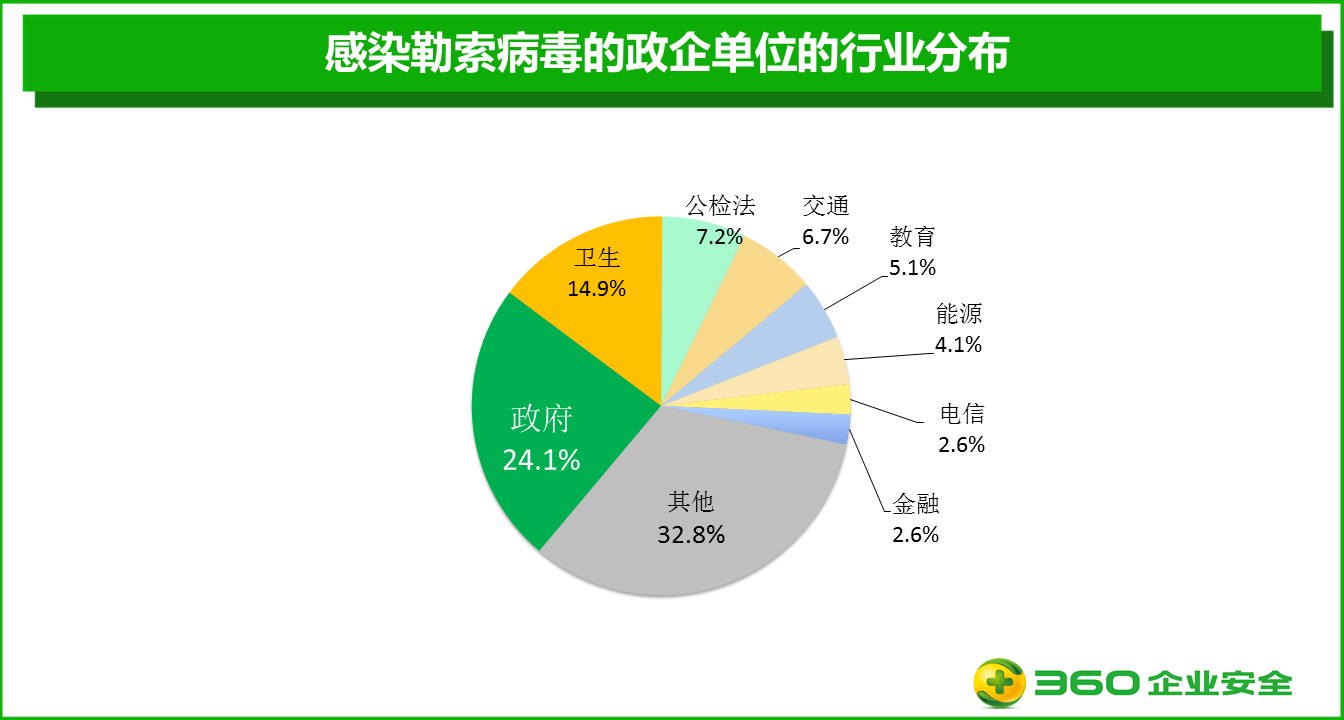
### 摘要：5月是政企单位感染勒索病毒的最高峰，其数值是最低谷时的5.3倍。

2018年，政企单位感染勒索病毒的最高峰出现在5月，最低谷出现在2月，最高峰月份感染勒索病毒的单位数量是最低谷时的5.3倍。



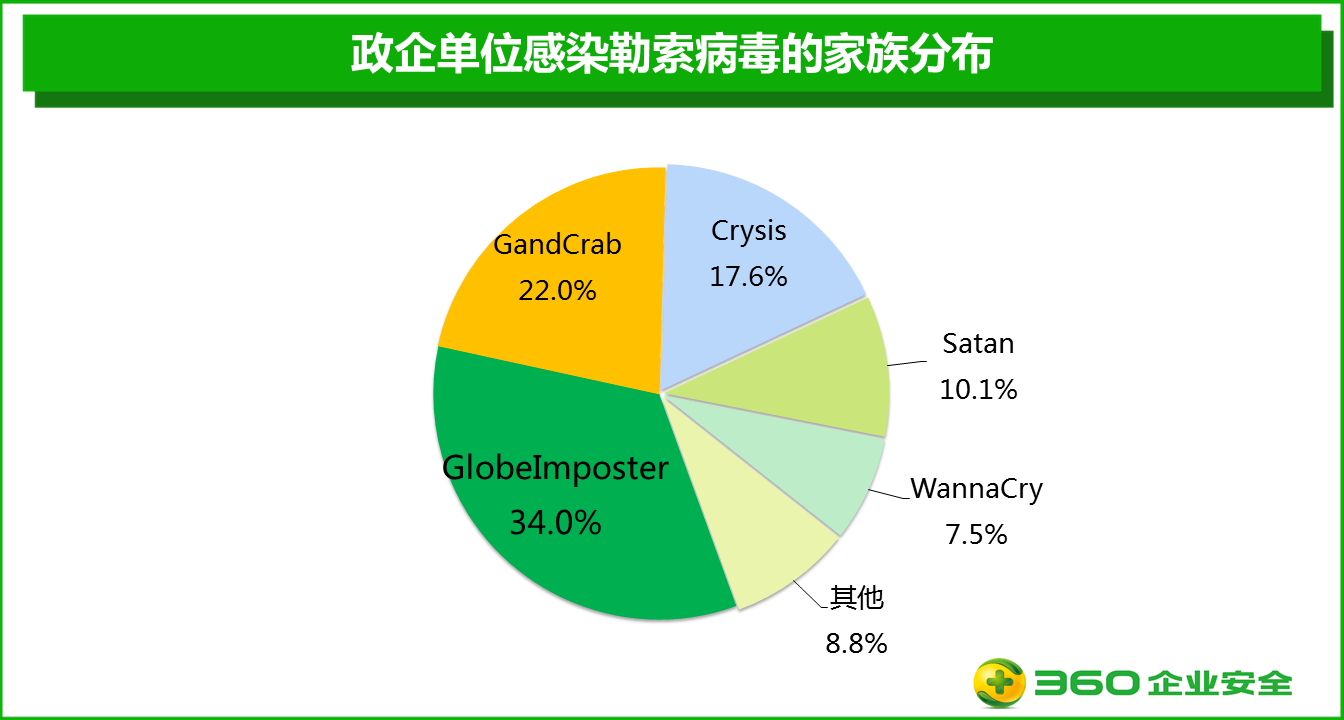
### 摘要：政府单位是感染勒索病毒的重灾区，数量是被感染政企单位总数的24.1%。

在被勒索病毒感染的政企单位中，政府单位的占比最高，占到被感染政企单位总数的24.1%；其次是卫生、公检法单位，占比分别是14.9%、7.2%。



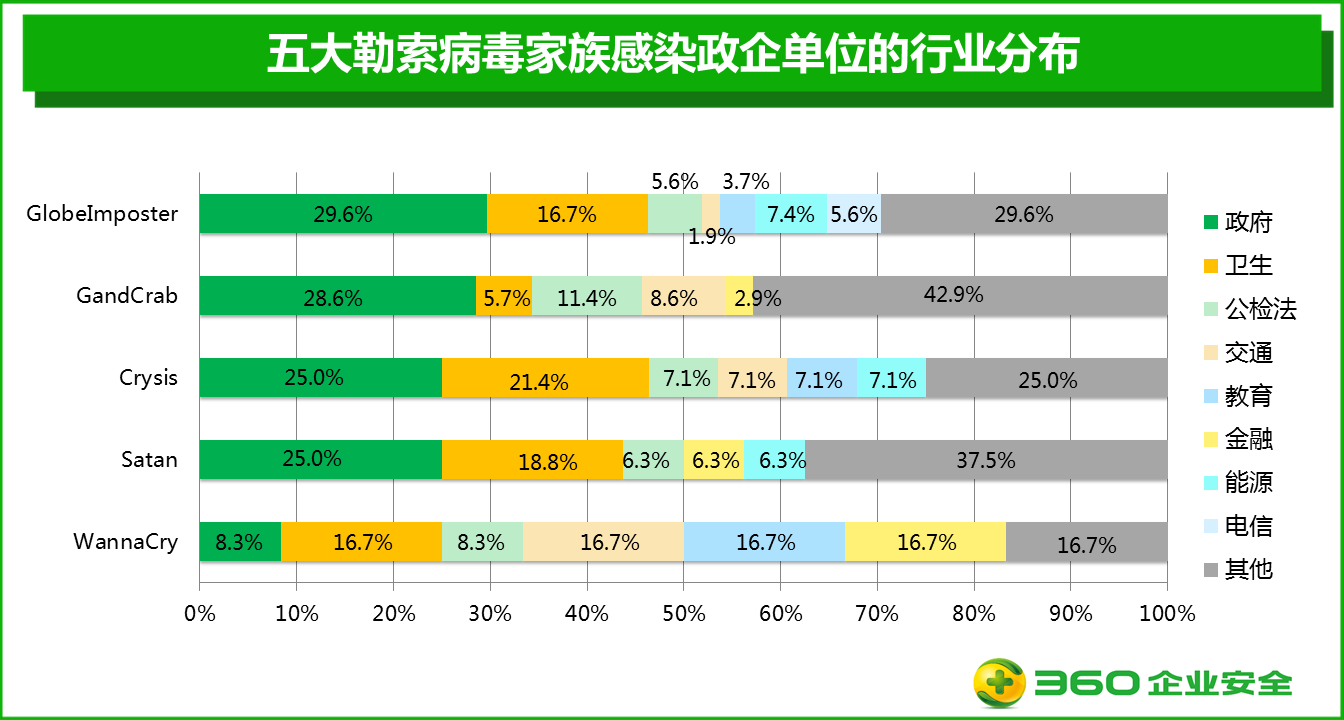
### 摘要：GlobeImposter最难防范，34.0%受害政企单位感染了该勒索病毒。

在感染勒索病毒的政企单位中，34.0%感染了GlobeImposter，22.0%感染了GandCrab，17.6%感染了Crysis，10.1%感染了Satan，仍然有7.5%单位感染WannaCry。



### 摘要：四大勒索病毒都爱感染政府行业，WannaCry的感染则相对平均。

GlobeImposter感染最多的是政府单位，占感染政企单位总数的29.6%；其次是卫生行业，占比为16.7%；GandCrab感染最多的是政府单位，占感染政企单位总数的28.6%；其次是公检法行业，占比为11.4%；Crysis感染最多的是政府单位，占感染政企单位总数的25.0%；其次是卫生行业，占比为21.4%；Satan感染最多的是政府单位，占感染政企单位总数的25.0%；其次是卫生行业，占比为18.8%；而WannaCry的感染则相对平均。



# 第三章，勒索病毒发展趋势预测

2018年勒索病毒攻击产生的影响和危害达到新的高度，特别是针对服务器的攻击，给广大政企用户带来了前所未有的影响。360终端安全实验室预计，2019年勒索病毒威胁仍将在病毒威胁排行榜上执牛耳领跑众毒。

以下是从不同的侧面对未来勒索病毒发展趋势的预测分析。

## 紧跟漏洞发展步伐

2018年除了Satan利用众多Web应用漏洞进行传播外，最有技术进取心的就要数GandCrab了，比如GandCrab在V5版本先后加入了对CVE-2018-8120、CVE-2018-8440、CVE-2018-0896等漏洞的利用技术。

## 更多的传播方式

2018年除了常规模式外，新出现了利用U盘蠕虫传播勒索病毒的手段，此外利用软件供应链传播也在本年得以实现，使得短时间内大量用户遭受攻击。我们预计2019年勒索病毒传播方式将继续扩展。

## 攻击面和目标扩大化

2016年出现的RushQL Oracle数据库勒索病毒在2018年得以死灰复燃，此种病毒和其他勒索病毒最大的不同点在于它只破坏数据库的结构，而不是加密磁盘文件，这属于典型的数据库攻击。我们预计2019年勒索病毒攻击目标将继续扩大，包括各种操作系统、应用程序都将成为勒索病毒攻击的目标。

## 被攻击的设备种类不断扩大

以往勒索病毒主要攻击PC和服务器以及部分移动设备，未来包括工控设备、嵌入式设备、IoT设备等都可能面临勒索病毒攻击的风险。

# 第四章，勒索病毒应急响应指南

政企单位如果已经感染勒索病毒，鉴于等待专业人员的救助往往需要一定的时间，所以，360终端安全实验室建议及时采取必要的自救措施，有效止损，将损失降到最低。

## 如何判断中毒

勒索病毒的主要目的是为了勒索，所以在植入病毒完成加密后，必然会提示受害者您的文件已经被加密了无法再打开，需要支付赎金才能恢复文件。

### 1.业务系统无法访问

2018年以来，勒索病毒的攻击不再局限于加密核心业务文件，转而对企业的服务器和业务系统进行攻击，感染企业的关键系统，破坏企业的日常运营，甚至还延伸至生产线——生产线不可避免地存在一些遗留系统和各种硬件难以升级打补丁等原因，一旦遭到勒索攻击的直接后果就是生产线停产。

当然，业务系统出现无法访问、生产线停产等现象时，并不能100%确定是服务器感染了勒索病毒，也有可能是遭到DDoS攻击或是中了其他病毒等原因所致，还需要结合以下特征来判断。

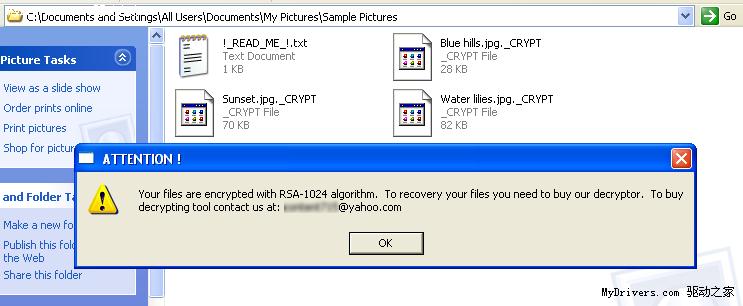
### 2.电脑桌面被篡改

服务器被感染勒索病毒后，最明显的特征是电脑桌面发生明显变化，即：桌面通常会出现新的文本文件或网页文件，这些文件用来说明如何解密的信息，同时桌面上显示勒索提示信息及解密联系方式，通常提示信息英文较多，中文提示信息较少。



### 3.文件后缀被篡改

服务器感染勒索病毒后，另外一个典型特征是：办公文档、照片、视频等文件的图标变为不可打开形式，或者文件后缀名被篡改。一般来说，文件后缀名会被改成勒索病毒家族的名称或其家族代表标志，如：GlobeImposter家族的后缀为.dream、.TRUE、.CHAK等；Satan家族的后缀.satan、sicck；Crysis家族的后缀有.ARROW、.arena等。



## 如何紧急自救

政企单位如果已经感染勒索病毒，鉴于等待专业人员的救助往往需要一定的时间，所以360终端安全实验室建议及时采取必要的自救措施，及时止损，将损失降到最低。

### 1.隔离中招主机

当确认服务器已经被感染勒索病毒后，应立即隔离被感染主机。隔离的目的，一方面是为了防止感染主机自动通过连接的网络继续感染其他服务器，另一方面是为了防止黑客通过感染主机继续操控其他服务器。

隔离主要包括物理隔离和访问控制两种：物理隔离常用的操作方法是断网和关机；访问控制常用的操作方法是加策略和修改登录密码。

### 2.排查业务系统

业务系统的受影响程度直接关系着事件的风险等级。评估风险，及时采取对应的处置措施，避免更大的危害。所以，在已经隔离被感染主机后，需要对局域网内的其他机器进行排查，检查核心业务系统是否受到影响，生产线是否受到影响，并检查备份系统是否被加密等，以确定感染的范围。

### 3.联系专业人员

在应急自救处置后，建议第一时间联系专业的技术人士或安全从业者，对事件的感染时间、传播方式，感染家族等问题进行排查。

请拨打360企业安全集团全国400应急热线：4008 136 360 转2 转4。

## 如何进行恢复

一般来说，可以通过历史备份、解密工具、重装系统来恢复被感染的系统，建议在专业人员指导下进行，避免造成其他不必要的损失。

### 1.历史备份还原

事先进行备份，既是最有效也是成本最低的恢复文件的方式。如果事前已经对文件进行了备份，就不会再担忧和烦恼，可以直接自行恢复被加密的文件。值得注意的是，在文件恢复之前，应确保系统中的病毒已被清除，已经对磁盘进行格式化或是重装系统，以免插上移动硬盘的瞬间，或是网盘下载文件到本地后，备份文件也被加密。

### 2.解密工具恢复

绝大多数勒索病毒使用的加密算法都是国际公认的标准算法，这种加密方式的特点是，只要加密密钥足够长，普通电脑可能需要数十万年才能够破解，破解成本是极高的。通常情况，如果不支付赎金是无法解密恢复文件的。

但是，对于以下三种情况，可以通过360提供的解密工具恢复感染文件。

1. 勒索病毒的设计编码存在漏洞或并未正确实现加密算法。
2. 勒索病毒的制造者主动发布了密钥或主密钥。
3. 执法机构查获带有密钥的服务器，并进行了分享。

可以通过网站（http://lesuobingdu.360.cn/）查询哪些勒索病毒可以解密。例如：今年下半年大规模流行的GandCrab家族勒索病毒，GandCrabV5.0.3及以前的版本可以通过360解密大师进行解密。



需要注意的是：使用解密工具之前，务必要备份加密的文件，防止解密不成功导致无法恢复数据。

### 3.重装操作系统

当文件无法解密，也觉得被加密的文件价值不大时，也可以采用重装系统的方法，恢复系统。但是，重装系统意味着文件再也无法被恢复。另外，重装系统后需更新系统补丁，并安装杀毒软件和更新杀毒软件的病毒库到最新版本，而且对于服务器也需要进行针对性的防黑加固。

当然，还有一种我们并不推荐的恢复方式，就是通过支付赎金来解密。勒索病毒的赎金一般为比特币或其他数字货币，数字货币的购买和支付对一般用户来说具有一定的难度和风险，所以即便选择支付赎金的解密方式，也不建议自行支付赎金，请联系专业的安全公司或数据恢复公司进行处理，以保证数据成功恢复。

## 如何避免中毒

360终端安全实验室提醒广大政企单位从以下角度入手进行勒索病毒防范：

### 1.及时更新最新的补丁库

病毒大规模爆发的原因都是因为补丁安装不及时所致，及时更新补丁是安全运维工作的重中之重。

如果由于业务特殊性，对打补丁有着要求非常严格的要求，建议选择专业的补丁管理产品。例如360终端安全产品就集成了先进的补丁管理功能，能够进行补丁编排，对补丁按照场景进行灰度发布，并且对微软更新的补丁进行二次运营，能够解决很多兼容性问题，更大程度解决补丁难打的问题。

### 2.重要资料定期隔离备份

尽量建立单独的文件服务器进行重要文件的存储备份，即使条件不允许，也应对重要的文件进行定期隔离备份。

### 3.提高网络安全基线

掌握日常的安全配置技巧，如对共享文件夹设置访问权限，尽量采用云协作或内部搭建的wiki系统实现资料共享；尽量关闭3389、445、139、135等不用的高危端口，禁用Office宏等。

### 4.保持软件使用的可信

平时要养成良好的安全习惯，不要点击陌生链接、来源不明的邮件附件，打开前使用安全扫描并确认安全性，尽量从官网等可信渠道下载软件，目前通过软件捆绑来传播的病毒也在逐渐增多，尤其是移动应用环境，被恶意程序二次打包的APP在普通的软件市场里非常常见。

### 5.选择正确的反病毒软件

随着威胁的发展，威胁开始了海量化和智能化趋势。对于海量化的威胁，就需要利用云计算的能力来对抗威胁海量化的趋势，因此在选择反病毒软件时，需要选择具备云查杀能力的反病毒软件。

### 6.建立高级威胁深度分析与对抗能力

很多智能威胁通过多种手段来躲避传统反病毒软件的查杀，这时就需要建立高级威胁深度分析和对抗能力，从终端、事件和时间等多维度综合分析，配合全流量威胁检测手段，可以更加有效的识别新兴威胁。

### 7.提升新兴威胁对抗能力

通过对抗式演习，从安全的技术、管理和运营等多个维度，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，持续提升企业对抗新兴威胁的能力。

# 附录1、2018热点勒索病毒事件

2018年，为了赚取更多的赎金，勒索病毒们练就了十八般武艺，充分利用各种缝隙和漏洞发起攻击，一时间，热点勒索病毒事件此起彼伏。

### 1.几度破解，GandCrab的2018有点传奇

GandCrab是360互联网安全中心在2月2日捕获的一款新型勒索病毒。该勒索病毒一出现便利用RaaS的分发模式迅速在全网范围内广泛传播。8月开始陆续采用RDP 暴力破解方式投放，11月利用U盘蠕虫大肆传播。不过该勒索病毒早期版本可解密。早在3月初，罗马尼亚安全公司BitDefender就放出了该勒索病毒的解密工具，为中招用户提供解密服务。

此后病毒进行了相应的升级来躲避解密。

而10月16日，一位叙利亚的父亲在twitter上求助说自己孩子的照片和视频均被该勒索病毒（v5.0.3）加密了，但付不起赎金。看到该求助后，GandCrab作者良心发现，放出了针对叙利亚地区受害者的解密工具。而很快，BitDefender则放出了v5.0.3（含）之前所有版本的解密工具。

### 2.以吃鸡外挂的名义，Xiaoba勒索病毒很张扬

2月6日，一款名为Xiaoba的勒索病毒以“吃鸡”外挂的名义，在贴吧、QQ群等社交平台中疯狂扩散。诱骗玩家关闭安全软件，并对全盘文件进行加密。此外，该勒索病毒作者还参与其他类型恶意软件或外挂程序的开发，并高调发布到各种论坛中，很是张扬。

### 3.专盯高价值服务器，GlobeImposter阴魂不散

GlobeImposter只加密服务器，危害巨大。其中有影响力的事件要数2月24国内某省级儿童医院被GlobeImposter攻击出现系统瘫痪状况。时值儿童流感高发季，医院大厅人满为患。事件起因是该院多台服务器感染GlobeImposter勒索病毒，其中包括数据库文件在内的多种重要文件被病毒加密。黑客要求院方在6小时内为每台中招机器支付1个比特币赎金（当时约合人民币66000余元）。具不完全统计，仅2018年一年期间，该病毒家族就出现了近100个新型变种在网络中传播。

### 4.三七分成，Saturn开启传销式扩散传播

3月5日，一款名为Saturn的勒索病毒开始发起攻击。该勒索病毒会要求受害者在7天内支付300美元等价的比特币，逾期则会赎金翻倍。但与以往勒索病毒不同，该病毒还采用了一种新的传播模式——病毒作者会为二次传播者按照三七的比例进行分成，鼓励和诱导他人帮助其进行病毒的扩散和分发。

### 5.勒索or挖矿，Rakhni看配置决定如何赚更多钱

7月10日， Rakhni勒索病毒家族的最新变种发起了新一波的攻击。该勒索病毒使用“鱼叉式钓鱼邮件”进行传播，诱导受害者打开邮件附件中的Word文档，一旦用户根据诱导点击了文档中的图标，则会启动附带的恶意程序。与以往不同的是，该程序会根据受害用户的计算机环境以及配置，自动判断对受害机器投放勒索病毒和挖矿木马哪个能为作者赚取更多的利润。

### 6.死灰复燃，RushQL只为勒索Oracle数据库

11月，360终端安全实验室陆续接到数起用户反馈，中了Oracle数据库勒索病毒。经确认，该病毒是由“SQL RUSH Team”组织发起的RushQL数据库勒索病毒，是因为用户下载使用了破解版PL/SQL导致的。该病毒最早出现在2016年11月，期间沉寂了1年多，直到最近突然呈现出死灰复燃之势。

### 7.数万人中招，“微信支付”勒索病毒短暂的一生

12月1日，国内首次出现了要求微信支付赎金的勒索病毒。该勒索病毒入侵电脑运行后会加密用户文件，并在桌面释放一个“你的电脑文件已被加密，点此解密”的快捷方式，随后弹出解密教程和收款二维码，最后强迫受害用户通过手机转账缴付解密酬金，而且该勒索病毒没有修改文件后缀名。

在接到报案后，东莞网警24小时内火速侦破“12.05”特大新型勒索病毒破坏计算机信息系统案，抓获病毒研发制作者。

# 附录2、关于360终端安全实验室

360终端安全实验室由多名经验丰富的恶意代码研究专家组成，着力于常见病毒、木马、蠕虫、勒索软件等恶意代码的原理分析和研究，致力为中国政企客户提供快速的恶意代码预警和处置服务，在曾经流行的WannaCry、Petya、Bad Rabbit的恶意代码处置过程中表现优异，受到政企客户的广泛好评。

360终端安全实验室以360天擎新一代终端安全管理系统为依托，为政企客户提供简单有效的终端安全管理理念、完整的终端解决方案和定制化的安全服务，帮助客户解决内网安全与管理问题，保障政企终端安全。

# 附录3、关于360天擎新一代终端安全管理系统

360天擎新一代终端安全管理系统是360企业安全集团为解决政企机构终端安全问题而推出的一体化解决方案，是中国政企客户3300万终端的信赖之选。系统以功能一体化、平台一体化、数据一体化为设计理念，以安全防护为核心，以运维管控为重点，以可视化管理为支撑，以可靠服务为保障，能够帮助政企客户构建终端防病毒、入侵防御、安全管理、软件分发、补丁管理、安全U盘、服务器加固、安全准入、非法外联、运维管控、主机审计、移动设备管理、资产发现、身份认证、数据加密、数据防泄露等十六大基础安全能力，帮助政企客户构建终端威胁检测、终端威胁响应、终端威胁鉴定等高级威胁对抗能力，为政企客户提供安全规划、战略分析和安全决策等终端安全治理能力。

特别的是，360企业安全还面向所有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，帮政企客户免除后顾之忧。



# 附录4、关于360天擎终端安全响应系统

360天擎终端安全响应系统（EDR）以行为引擎为核心，基于人工智能和大数据分析技术，对主机、网络、文件和用户等信息，进行深层次挖掘和多维度分析，结合云端优质威胁情报，将威胁进行可视化，并通过场景化和全局性的威胁追捕，对事件进行深度剖析，识别黑客/威胁意图，追踪威胁的扩散轨迹，评估威胁影响面，从而协同EPP、SOC、防火墙等安全产品，进行快速自动化的联动响应，将单次响应转化为安全策略，控制威胁蔓延，进行持续遏制，全面提升企业安全防护能力。