安天防勒索解决方案

ANTIY 安天 | 智者安天下

目录

1 勒索攻击来势汹汹

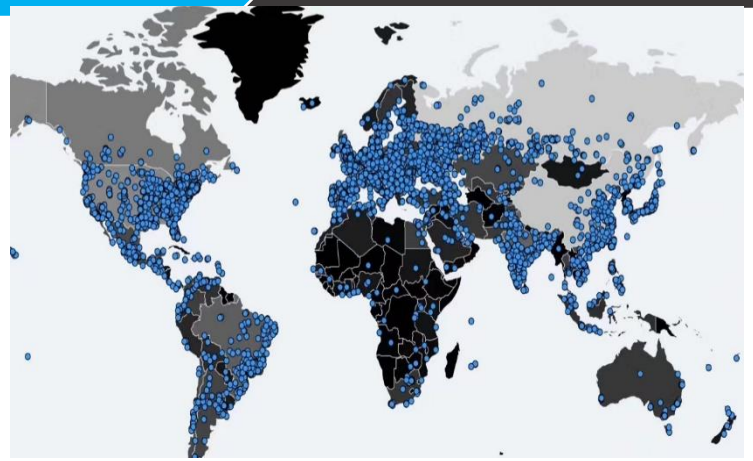
2 勒索软件肆虐的原因与机理

3 安天针对勒索软件提出全套防护解决方案

4 WannaCry勒索蠕虫的专项处置

5 WannaCry勒索蠕虫全球肆略的思考

勒索攻击来势汹汹



北京时间2017年5月12日20时左右，全球爆发大规模勒索软件感染事件，我国大量行业企业内网大规模感染，教育网受损严重，攻击造成了教学系统瘫痪，甚至包括校园一卡通系统。截止到5月13日23时，病毒影响范围进一步扩大，包括企业、医疗、电力、能源、银行、交通等多个行业均遭受不同程序的影响，只有缴纳高额赎金（有的要比特币）才能解密资料和数据。

勒索攻击来势汹汹—何谓勒索软件

软件定义：勒索软件（RansomWare）是一种流行的木马程序，通过骚扰、恐吓甚至采用绑架用户电子资产等方式，使用户数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财。勒索产业已成长为一个数十亿美元的市场。

传播手段：1、借助网页木马传播，当用户不小心访问恶意网站时，勒索软件会被浏览器自动下载并在后台运行；2、作为电子邮件附件传播；3、借助可移动存储介质传播；4、通过即时通讯软件传播；5、通过蠕虫攻击传播。

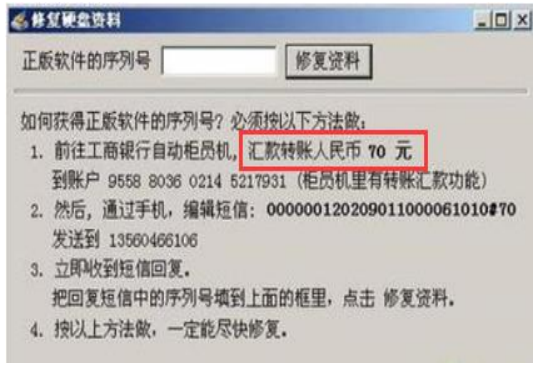
攻击对象：勒索病毒以前主要针对特定行业部门，现在攻击对象不在局限，已由定向攻击转为泛化攻击。

攻击呈现：勒索病毒文件一旦被用户点击打开，会利用连接至黑客的C&C服务器，进而上传本机信息并下载加密公钥和私钥。然后，将加密公钥私钥写入到注册表中，遍历本地所 有磁盘中的Office 文档、图片等文件，对这些文件进行格式篡改和加密。加密完成后，还会在桌面等明显位置生成勒索提示文件，指导用户去缴纳赎金。

攻击影响：该类型病毒可以导致重要文件无法读取，关键数据被损坏，给正常工作带来了极为严重的影响。

勒索攻击来势汹汹—何谓勒索软件

这类用户数据资产包括文档、邮件、数据库、源代码、图片、压缩文件等多种文件。赎金形式包括真实货币、比特币或其它虚拟货币。一般来说，勒索软件作者还会设定一个支付时限，有时赎金数目也会随着时间的推移而上涨。有时，即使用户支付了赎金，最终也还是无法正常使用系统，无法还原被加密的文件。



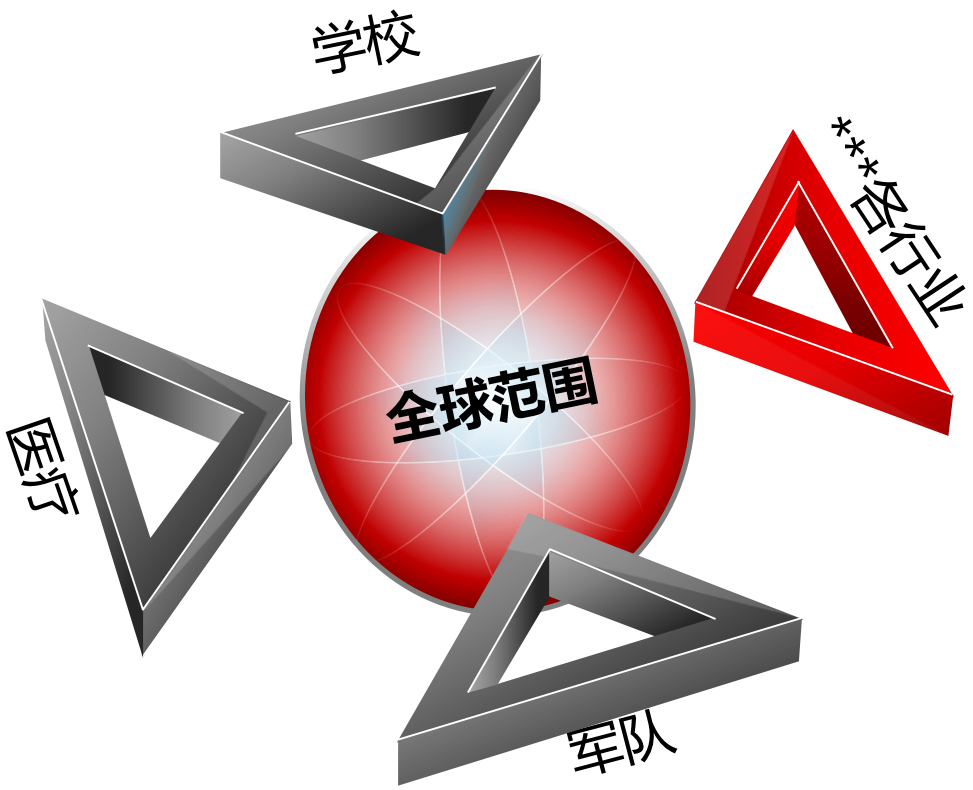
关键字：

骚扰、恐吓、绑架

关键字：

勒索钱财：邮寄现金、汇款转账、短信支付、Q币、**Bitcoin**…

勒索攻击来势汹汹—勒索事件影响范围



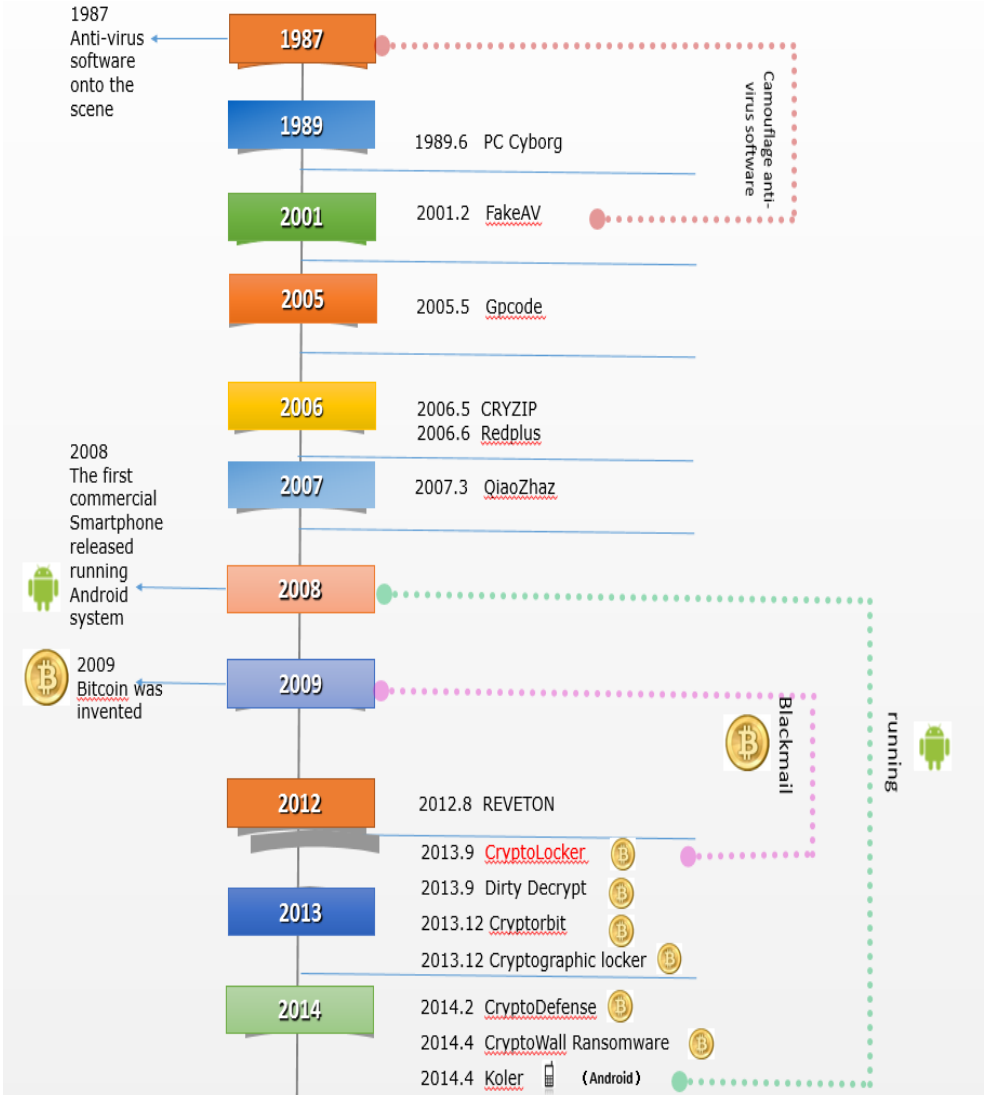
学校：
学生论文、档案管理、考试系统等业务系统文件被锁定-----

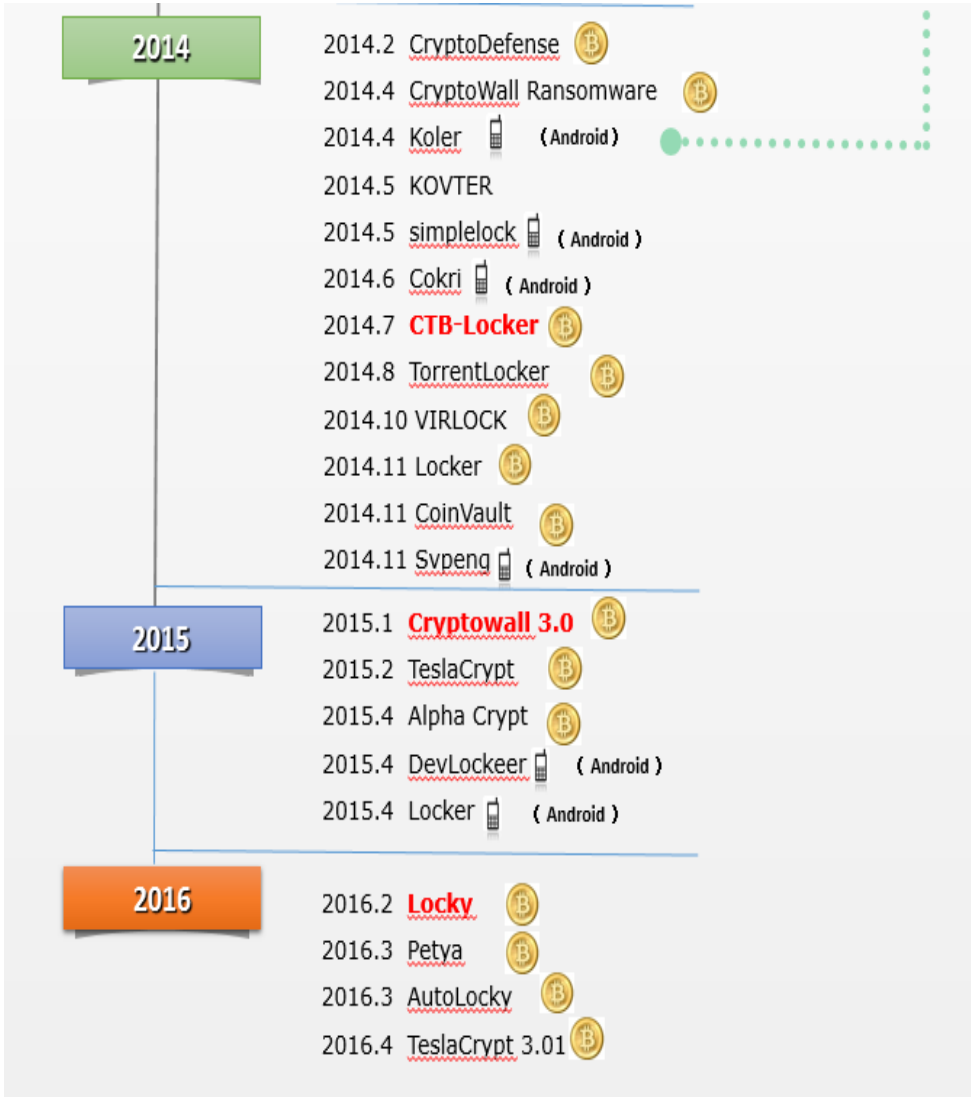
交通：
加油站无法加油，收费站无法收费，交通指挥系统被影响-----

医疗：
无法正常手术，挂号系统、取药系统等业务系统无法运行-----

重要系统文件与数据库被锁定，无法进行文件拷贝，系统蓝屏-----

勒索攻击来势汹汹—勒索软件的发展历程





2017年5月Wannacry勒索事件

此次勒索病毒是由ＮＳＡ泄漏的“永恒之蓝”黑客武器传播的。“永恒之蓝”可远程攻击微软视窗系统的４４５端口（支持文件共享），如果系统未安装今年３月的微软补丁，那么只要开机上网，无需任何操作，“永恒之蓝”就能在电脑里执行任意代码，植入勒索病毒等恶意程序。

勒索攻击来势汹汹—安全新挑战

勒索软件给文档与系统安全带来的新挑战

病毒库更新不及时，无法有效及时检测出新型勒索软件

常规检测手段无法发现并阻止勒索行为

数据一旦被加密，将无法进行破解

勒索软件肆虐的原因与机理

经济利益驱动

互联网黑色产业与灰色产业相互交织，产业规模保守估计过千亿元，产业暴利。

门槛日益降低

随着勒索软件制作门槛的日益降低，越来越多不法分子投身 其中，甚至出现了勒索软件制作平台，让0技术能力的人也有了制作能力。

军用工具泄露

组织级、国家级网络工具的泄露，使得从业人员得到了更多更专业更先进行攻击方法与工具，破坏性更强。

安全意识淡薄

用户侧从上至上部分人员安全意识淡薄，存在使用弱口令密码、乱用U盘介质、访问不安全网站、点击邮件恶意链接等不安全操作。

防护措施不足

只观注病毒、漏洞防护，边界访问控制防护，对勒索软件的防护意识不足，没有专业的防勒索检测与防护措施。

勒索软件肆虐的原因与机理

提升级勒索能力：NSA军用网络攻击工程的泄露，为黑客提供了国家战略级网络武器，大大加强了恶意黑客组织的攻击能力，使黑客组织的攻击水平从组织级提升到了国家级。

工具攻击对象重定向： NSA工具集是美国针对其它国家使用的攻击武器，被黑产利用后，工具的攻击对象从国家变成了社会单位，对象扩散化，而国家与社会各单位之间的防护能力是完成不同的，但攻击对象的属性变化后，攻击的影响力、破坏力、持续力，被防御力产生了极大的变大，进而使勒索软件在全球范围内肆无忌惮的横形。

▲「影子經紀人」在網上公布的NSA文件　網上圖片

攻击能力

攻击影响力

勒索软件肆虐的原因与机理

防勒索的核心—终端反病毒能力

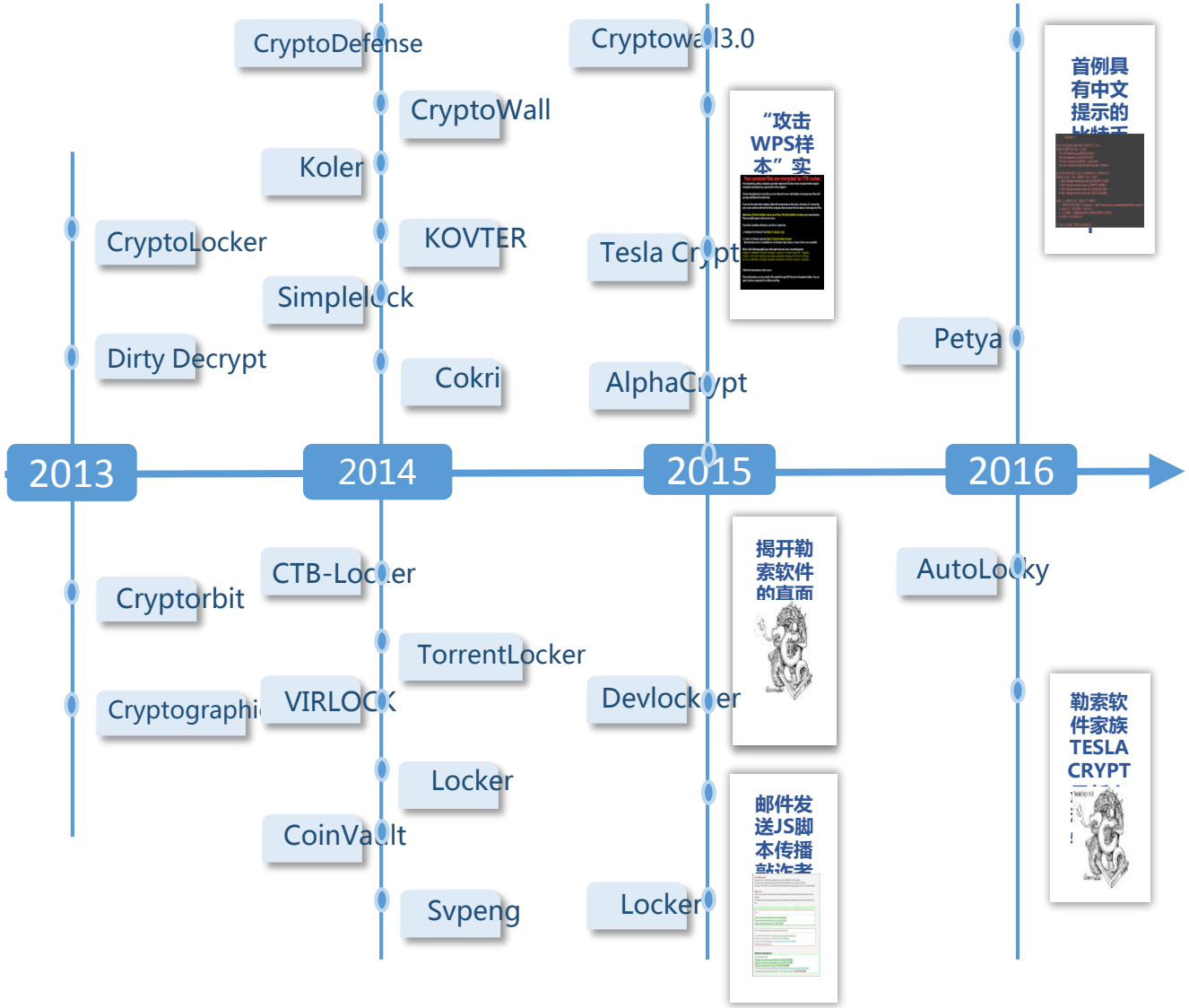
防火墙、流量监测、主机加固能够在一定程度上防御勒索软件，但很多方式治标不治本。

防勒索软件的核心：

- 病毒特征的识别
- 勒索行为的捕获和阻隔
- 文档访问的合法性判断

文档防护挑战	关键需求	传统方式	安天解决方案
难阻隔	有效阻隔已知、未知勒索软件	○	✓
难管控	有效阻止已知、未知勒索软件运行	○	✓
损失大	相关的补救措施	✗	✓

安天全套防护解决方案—防勒索软件能力



安天多年来一直致力于防勒索全套解决方案的研究，输出了多篇研究报告。

《揭开勒索软件的真面目》

http://www.antiy.com/response/ransomware.html

《"攻击WPS样本"实为敲诈者》

http://www.antiy.com/response/CTB-Locker.html

《邮件发送js脚本传播敲诈者木马的分析报告》

http://www.antiy.com/response/TeslaCrypt2.html

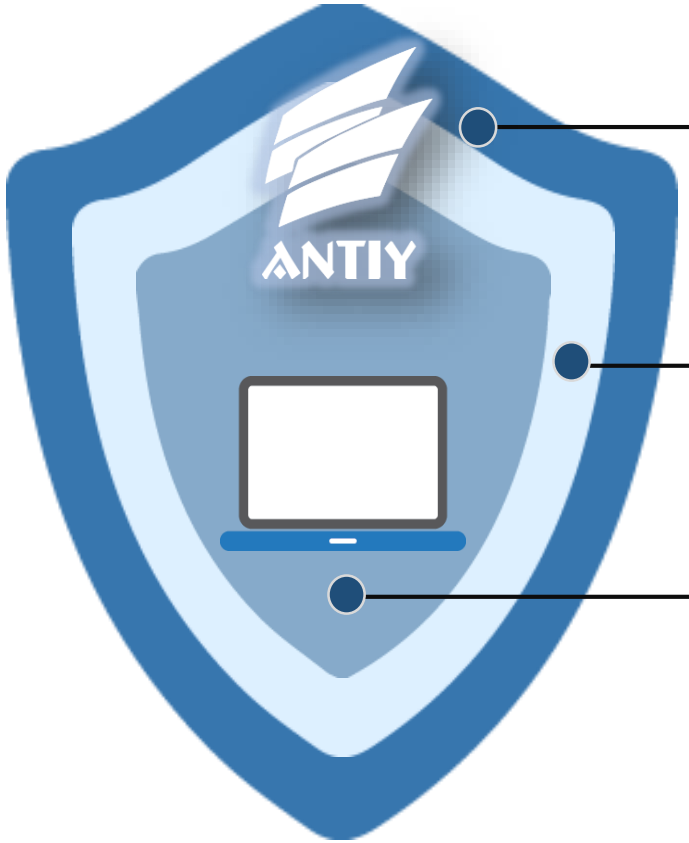
《首例具有中文提示的比特币勒索软件"LOCKY》

http://www.antiy.com/response/locky/locky.html

《勒索软件家族TeslaCrypt最新变种技术特点分析》

http://www.antiy.com/response/TeslaCrypt%204/TeslaCrypt%204.html

安天全套防护解决方案—三重防护体系



边界防御

主动防御

文档保护
针对勒索软件

三层防护—层层阻断

第一重——边界防御：及时阻隔已知病毒及未知病毒，使病毒不能通过边界（U盘拷贝、即时通讯软件传输、下载、邮件）进入终端【进不来】

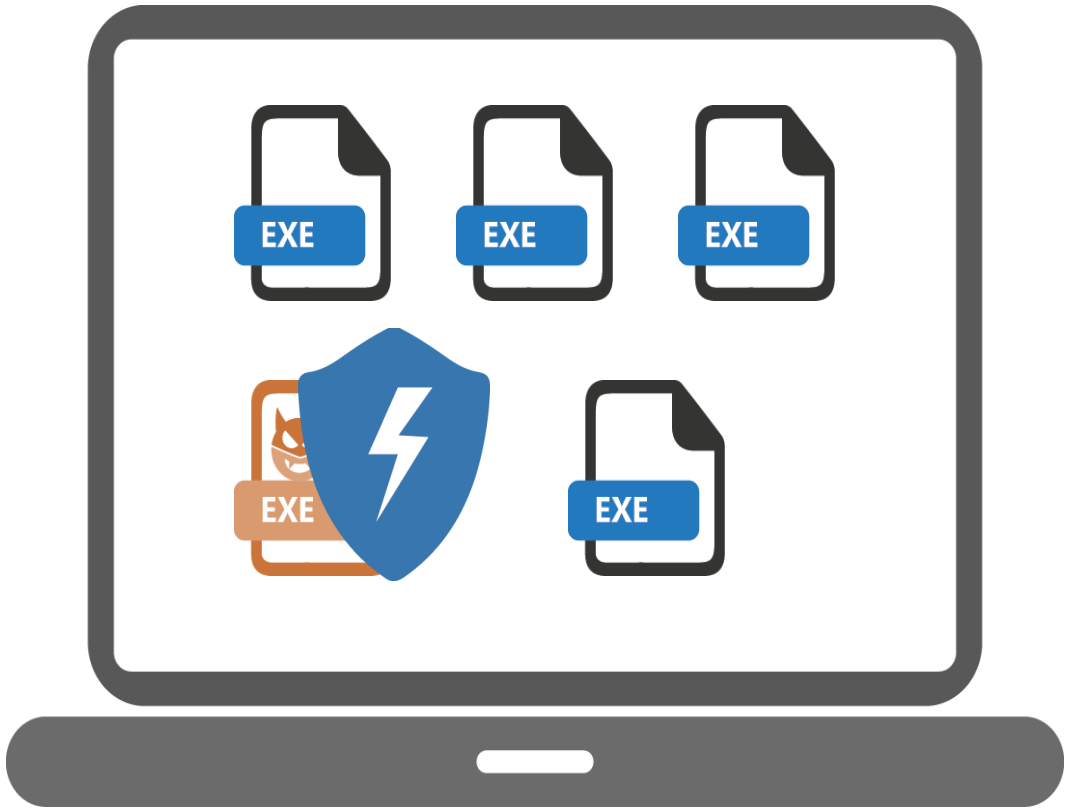
第二重——主动防御：及时阻止已知/未知病毒的运行【起不来】

第三重——文档安全工具：专门针对勒索软件的工具，并在加密文档之前及时阻断勒索进程，保护用户终端文档不被加密【改不了】

安天全套防护解决方案—边界防御

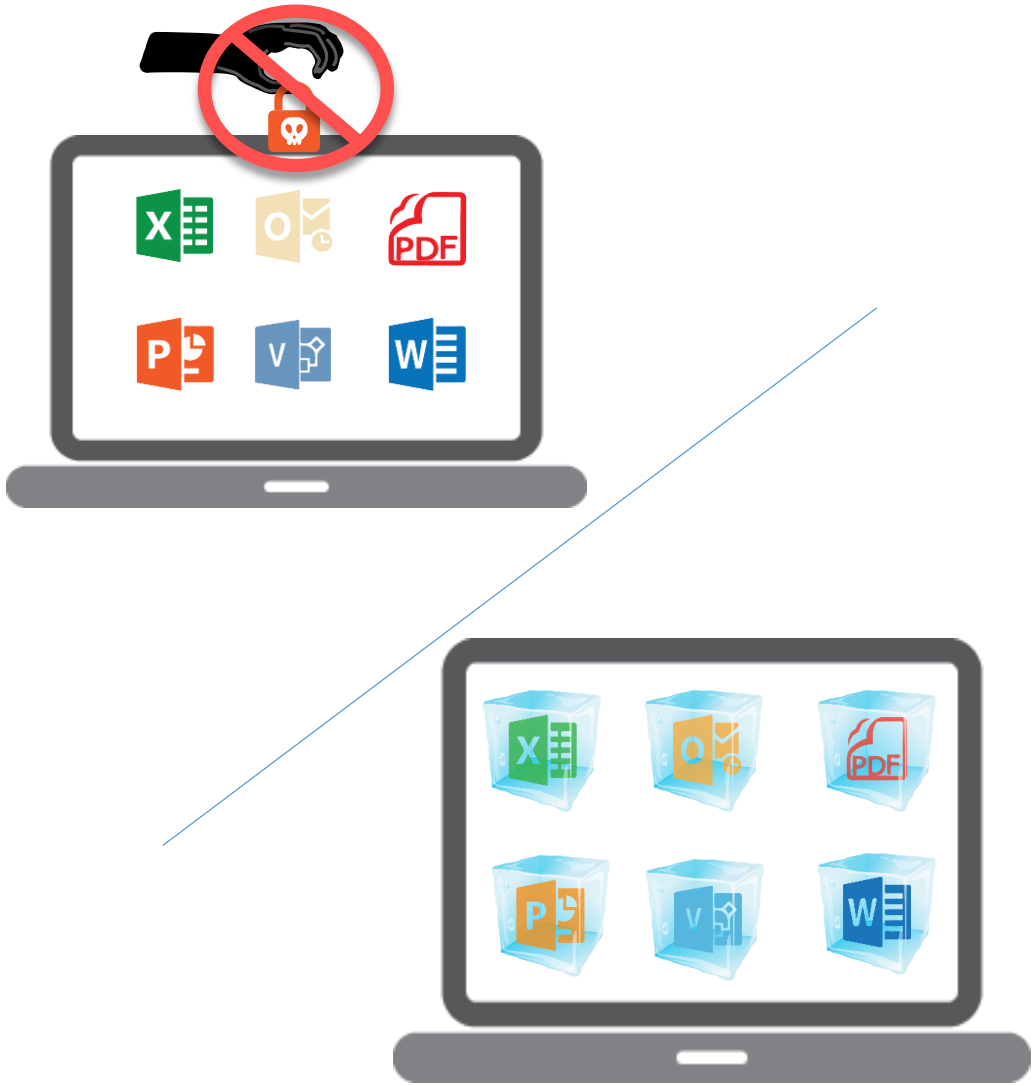
- 基于私有云架构，在云端存储海量病毒特征，当文件进入系统时，通过云查杀功能自动检测文件安全属性，精准阻隔已知勒索软件

安天全套防护解决方案—主动防御



- 通过文件行为监控、诱饵文档等多种防护手段，有效阻断可疑和高危行为，以应对未知和新型勒索软件。

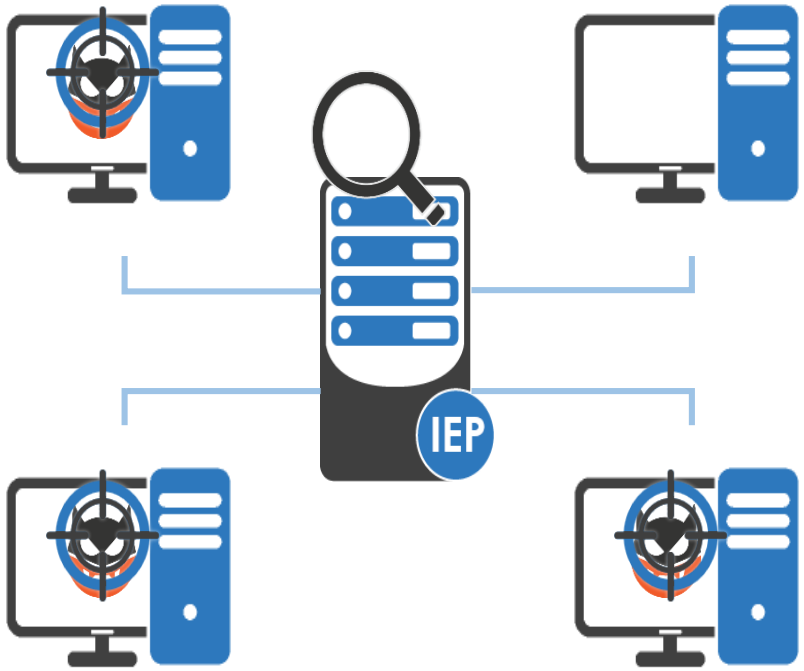
安天全套防护解决方案—文档安全防护（防勒索）



- 文档安全工具是安天针对勒索软件专门推出的防护功能，用户可以设置受保护的目录或者进行全盘锁定，进程访问受保护文档时，产品会校验进程合法性，针对非授权进程的访问及时阻断，通过文档安全工具，可以有效保障重要文档免受勒索软件破坏。

安天全套防护解决方案—全网追溯+定点查杀

突发安全事件快速响应



在全网范围内迅速定位感染文件、评估感染范围，远程一键式清除所有威胁。同时可以检查威胁残留，确认是否成功清除，防止顽固威胁。

一台终端发现威胁 -> 15分钟内全网追溯 -> 远程一键清除

安天全套防护解决方案—终端的威胁可视化

采用了网络拓扑的形式，通过3D化效果，展示终端层面的威胁情况，使管理人员直观快速掌握全网安全情况。

中观和微观可视化

智甲采用了网络拓扑的形式，通过3D化效果，展示终端层面的威胁情况。通过管理平台，可直接查看可视化界面，并且展示终端安全的实时情况。并可通过可视化页面，对终端下发操作指令，进行扫描，升级等各种操作。

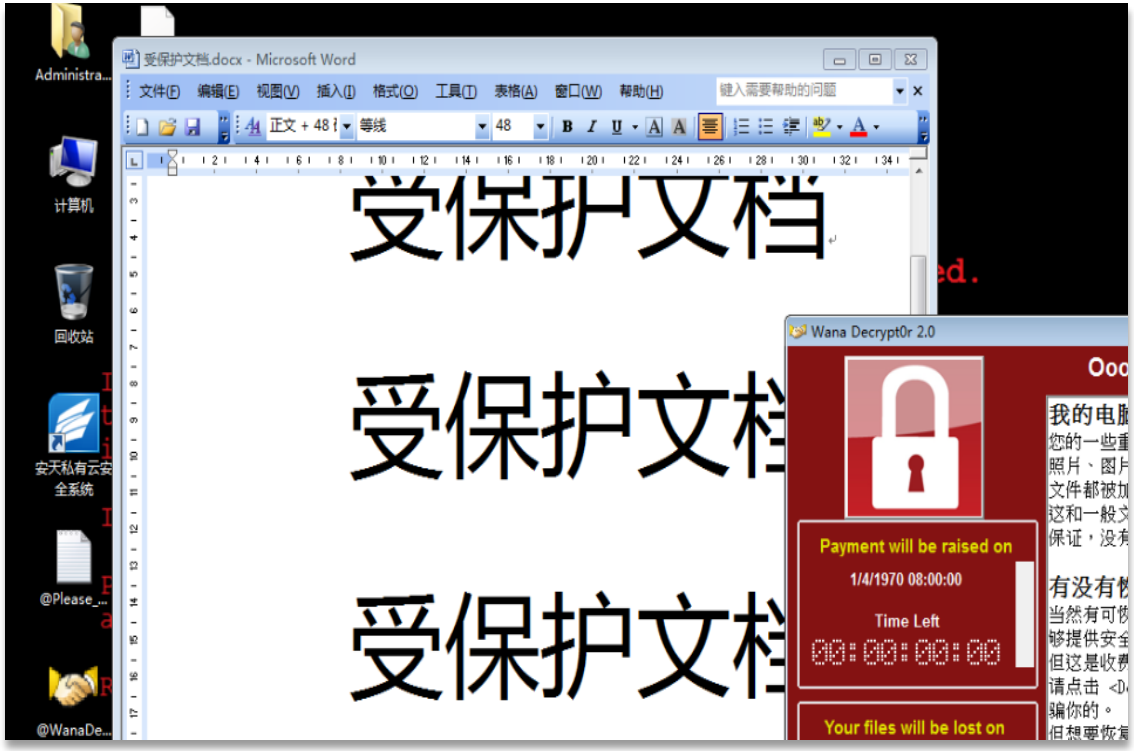
安天全套防护解决方案—产品&能力优势

- 较早就开始了针对防勒索持续投入，具有深厚的实战经验
- 多重防护机制，层层阻隔，有效拦截，为终端提供强大的防勒索能力
- 具有不仅仅依赖病毒特征码的防勒索能力

根据用户实际反馈，在wannacry爆发时，
智甲有效阻止了wannacry的勒索行为，保证了用户的数据安全

安天全套防护解决方案—wannacry解决方案展示

启动wannacry后，智甲通过行为监控，发现了wannacry的勒索行为，及时进行了告警并阻止了破坏行为



放行wannacry后，即使病毒正常启动，文档安全工具保护的文档依然未被加密，可正常访问。

针对勒索软件提出全套防护解决方案—案例一

某投资集团777勒索软件事件

-5月30日 进场了解情况，获取基础数据 ；

- 6月1日 进场采集样本及攻击线索；

- 6月2日 交付取证分析结果，了解需求，提供解决方案；

- 6月3-5日 与用户沟通方案细节，找到了解密工具并解密了文件，为解决实际问题。

针对勒索软件提出全套防护解决方案—案例二

黑龙江省某投资集团防御勒索软件解决方案

项目背景

黑龙江省某投资集团，其核心数据的安全性关乎全省经济发展大局。2016年5月末，集团OA系统和财务系统受到勒索软件攻击，约20万个关键文件被加密，断网8日，对工作运行产生严重影响并造成一定经济损失。

安天方案

安天智甲终端防御系统拥有专门的针对勒索软件的文档保护功能。该功能通过勒索行为感知、传输文件深度检测与管控、文档访问控制的方式，对勒索软件进行层层阻断，让勒索软件无机可乘。

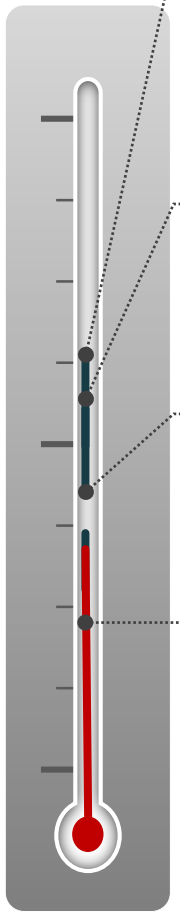
客户价值

帮助用户加固系统，防御恶意代码入侵，实时保护用户核心资产安全，持续保障用户业务顺畅，为用户构建相对安全的办公环境，降低用户风险，增强用户的安全自信。

WannaCry勒索蠕虫的专项处置

2017年05月13日	安天应急内容
6：00	安天紧急应对新型“蠕虫”式勒索软件“wannacry”全球爆发分析 http://www.antiy.com/response/wannacry.htm
9：45	更新《安天紧急应对新型“蠕虫”式勒索软件“wannacry”全球爆发分析 http://www.antiy.com/response/wannacry.htm
17：25	发布安天应对勒索软件“wannacry”防护手册 http://www.antiy.com/response/Antiy_Wannacry_Protection_Manual/Antiy_Wannacry_Protection_Manual.html
17：45	发布安天应对勒索者蠕虫病毒WannaCry FAQ http://www.antiy.com/response/Antiy_Wannacry_FAQ.html
19：03	发布蠕虫病毒WannaCry免疫工具和扫描工具 下载地址为：http://www.antiy.com/tools.html
…	持续更新

WannaCry勒索蠕虫全球肆略的思考—问题显像



我是局域网，我网络隔离了，为什么还被勒索了？

局域网与大量所谓隔离内网也都无法保证真正网络隔离，或者说纯粹隔离情况下几乎是无法有效工作的，维护设备带入，供应链带入，不受控的入口都有可能提供勒索软件的入口。

我有防火墙，配了防火墙，为什么还被勒索了？

防火墙是做访问规则控制的设备或软件，我们常会开放常用的22、80、139、445、3389等端口，而勒索软件会利用开放的常用端口进行入侵。

我装了杀毒软件，为什么还被勒索了？

杀毒软件是基于黑白名单匹配方式检测病毒，阻止非正常行为操作，而勒索软件的加密是一种用户正常操作行为。杀毒软件不具备发现专业的勒索软件能力。

我打了漏洞补丁，为什么还被勒索了？

更新补丁的不及时，也会给勒索软件的入侵留下时间机会。

思考

怎样才能避免发现wncy勒索软件事件？

怎样加强防勒索软件的能力？

用什么才能在事前、事中就发现阻止勒索事件？

WannaCry勒索蠕虫全球肆略的思考—防护思路

从**管理**与**技术**维度提升防勒索能力，做到**事前检测**　**事中阻断**、从而防止勒索事件的发生。

管理能力提升

加强安全意识宣贯，提升全员安全意识水平。

完善安全管理制度，提升安全管理水平。

进行安全培训，加强人员安全水平，避免乱点邮件链接、访问不安全网站、乱用U盘等安全现象。

完善内网纵深防御体系和能力

针对勒索软件的防护，采用回溯判定、分级防护的策略，通过安天追影威胁分析系统自动化判定勒索软件，并提供检出规则和特征分发到其他安全产品中，探海威胁检测系统对进入企业的勒索软件进行威胁感知，镇关威胁阻断系统对勒索软件进行传播阻断，智甲终端防御系统进行主机侧的检出、阻断与阻止勒索软件加密磁盘文件。

终端防御的有效回归

部署具有文档访问的进程白名单、批量文件篡改行为监控、诱饵文件和快速文件锁定的智甲安全防护产品，有效的在终端侧提升针对勒索软件的事前检测、事中阻断防护能力。解决隔离内网不及时补丁，不策略加固，安全软件不升级，只要打入一个节点，横扫全网的问题。