赤豹安全实验室通过对勒索病毒的长期监测与跟踪分析，针对全球2018年全年勒索病毒感染现状与趋势进行分析、研究，涵盖了勒索软件的起源、特征、现状、技术趋势和防御方案等多个方面。

本报告由北京江民新科技术有限公司赤豹安全实验室，综合了江民大数据威胁情报平台、江民终端反病毒监测网国内外研究数据、以及权威媒体公开报道，通过对勒索病毒的长期监测与跟踪分析，针对全球2018年全年勒索病毒感染现状与趋势进行分析、研究，涵盖了勒索软件的起源、特征、现状、技术趋势和防御方案等多个方面。

一 勒索软件简介

1.1 什么是勒索病毒?

勒索病毒，是一种流行的木马，通过骚扰、恐吓甚至采用绑架用户文件等方式，使用户数据资产或计算资源无法

常使用，并以此为条件向用户勒索钱财。主要以漏洞利用、RDP弱口令暴力破解、钓鱼邮件、网页挂马等形式进
传播。这种病毒利用各种加密算法对文件进行加密后，向文件所有者索要赎金。如果感染者拒付赎金，就无法获
加密的私钥，无法恢复文件。
这种病毒其实只是传统安全技术的一个小小的应用创新，以前加密技术一直用于防，现在却用于攻，从防到攻，
然发现原来加密技术可以这么玩。在数字世界里，勒索这门生意，这几年却正蓬勃兴起。勒索软件的概念可以追
到1989 年，那时人们通过人工投递的软盘，将 PC 锁定恶意代码发送给受害者，但自2014年以来，随着比特币
加密数字货币在全球的广泛使用，这类业务有了令人侧目的增长。

1.2 勒索病毒为什么愈演愈烈?

一方面，利用勒索病毒的成本非常低。在黑市上只要几千元就可以购买一个未知病毒，勒索成功一次就可以获利
万元甚至几十万元，十几倍到上百倍的利润，着实让人疯狂。
另一方面，勒索病毒防护非常麻烦。因为它简单粗暴，直接对文件加密，管杀不管埋，只要加密成功，就等着收
金，传统的安全防护措施对这种不讲道理的攻击手段束手无策。
第三方面，虚拟货币缺乏监管。现实中一个勒索案最难解决的问题是如何收赎金，而由于虚拟货币监管缺位，恰
解决了这个赎金问题。
所以，门槛低、启动成本低、高收益、风险低，这些因素组合在一起，勒索病毒愈演愈烈!

1.3 勒索病毒发展简史

1、原始阶段:

最早的勒索软件出现于1989年，名为“艾滋病信息木马”。该木马通过替换系统文件，在开机时计数，一旦系统
启动达到90次时，该木马将隐藏磁盘的多个目录，C盘的全部文件名也会被加密，从而导致系统无法启动。此时
屏幕显示信息声称用户的软件许可已过期，要求邮寄189美元以解锁系统。

2006年出现的Redplus勒索木马是国内首款勒索软件。该木马会隐藏用户文档，然后弹出窗口勒索赎金，金额从
70元至200元不等。据我国计算机病毒应急处理中心统计，全国各地的该病毒及其变种的感染报告有580多例。
实际上用户的文件并未丢失，只是被移动到一个具有隐藏属性的文件夹中。

2、新发展期，比特币赎金阶段:
从2013年的CryptoLocker开始，勒索软件进入了新的发展期，比特币进入了黑客的视野。CryptoLocker可以感
大部分Windows操作系统，通常通过邮件附件传播，附件执行后会对特定类型的文件进行加密，之后弹出付款窗
口，也就是从这款软件开始，黑客开始要求机构使用比特币的支付赎金，而就是这款软件为黑客组织带来了近
41000枚比特币的收入，按照比特币最新的市价这些比特币的价值有近10亿美元之巨。

3、勒索软件平台化及开源化趋势:

同为2015年一款名为Tox的勒索软件开发包在年中发布，通过注册服务，任何人都可创建勒索软件，管理面板会
示感染数量、支付赎金人数以及总体收益，Tox的创始人收取赎金的20%。

2015年下半年，土耳其安全专家发布了一款名为Hidden Tear的开源勒索软件。它仅有12KB，虽然体量较小，
是麻雀虽小五脏俱全，这款软件在传播模块，破坏模块等方面的设计都非常出色。尽管来自土耳其的黑客一再强

此软件是为了让人们更多地了解勒索软件的工作原理，可它作为勒索软件的开源化，还是引发了诸多争议，在阅了这款勒索软件的源代码后，笔者也是突然醒悟原来编程的思路与方法真的是别有洞天，破坏性思维和建设性思的确是完全不同的风格。

4、与窃取大众隐私信息结合的趋势

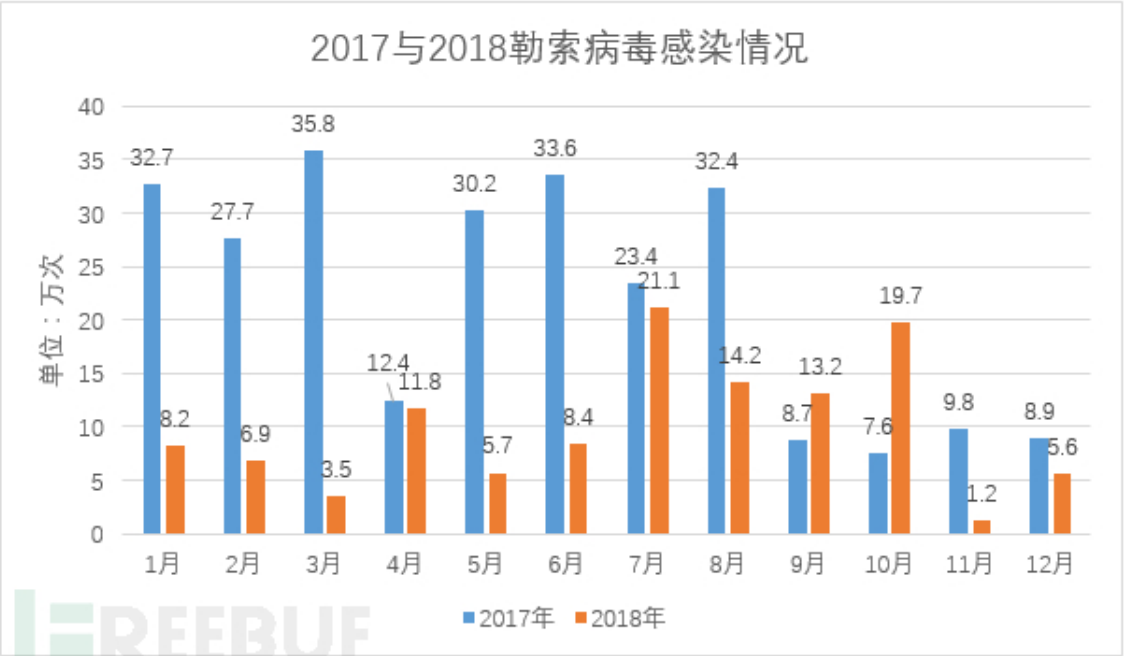
近年来，针对某些快捷酒店住宿系统及私营医院HIS系统的入侵、脱库(脱库指黑客入侵到系统后进行信息窃取行事件频发，而16年之前黑客一般只会将信息悄然盗出后在黑市上待价而沽，但目前黑客更是要在出售掉隐私信息前还要对医院及酒店进行勒索。去年底美国好莱坞某医疗中心就被黑客攻陷，并勒索340万美元的赎金，虽然经一番讨价还价医院最终支付了1.7万美元后运营恢复，但是该院的就诊记录不久就出现在了的数据黑市上。

而且最近的勒索病毒明显加强了“用户体验”的建设，会给用户很强的心理暗示，比如某些最新的勒索软件将U计成无法退出的界面，而且赎金随时间涨价，还会以倒计时强化紧迫感。

二 2018年勒索病毒感染情况

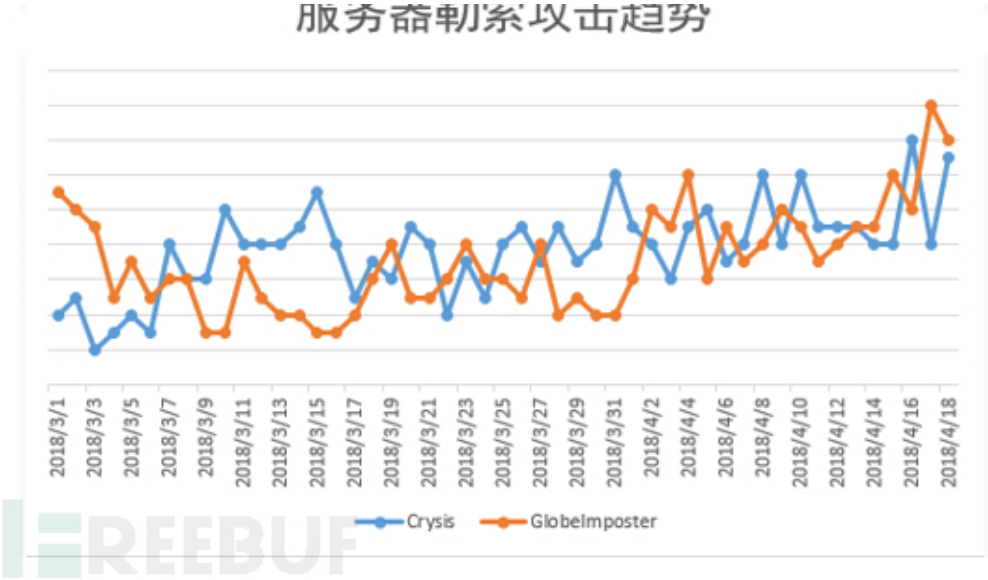
2.1 2018年勒索病毒感染情况

根据江民病毒监测中心对勒索病毒监测到的数据统计发现，2017年1月到8月，和2018年7到10月是勒索病毒感高发期，2017年勒索病毒感染事件共计为263.2万次，2018年为119.5万次，较去年下降了54.6%。



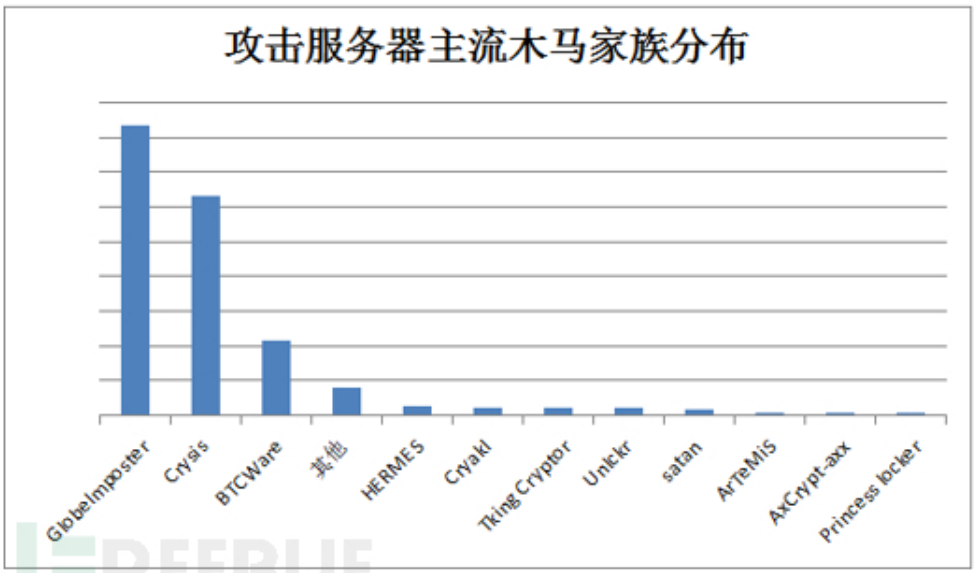
2.2 服务器攻击趋势及攻击者家族

近一个多月以来，每周都有企业Windows服务器遭受勒索病毒攻击，针对服务器的勒索病毒攻击呈现走高趋势，今年以来，两大针对服务器攻击的勒索病毒家族（GlobeImposter和Crysis家族）均出现爆发传播的迹象。



GlobeImposter,Crysis,BTCWare三款勒索病毒，是近来针对服务器攻击的主流，占比超过90%。这三款勒索病毒，都属于全球爆发类的勒索病毒，其中GlobeImposter更是多次攻击国内医疗和公共服务机构，国内外安全机构多次发布过该家族的预警。

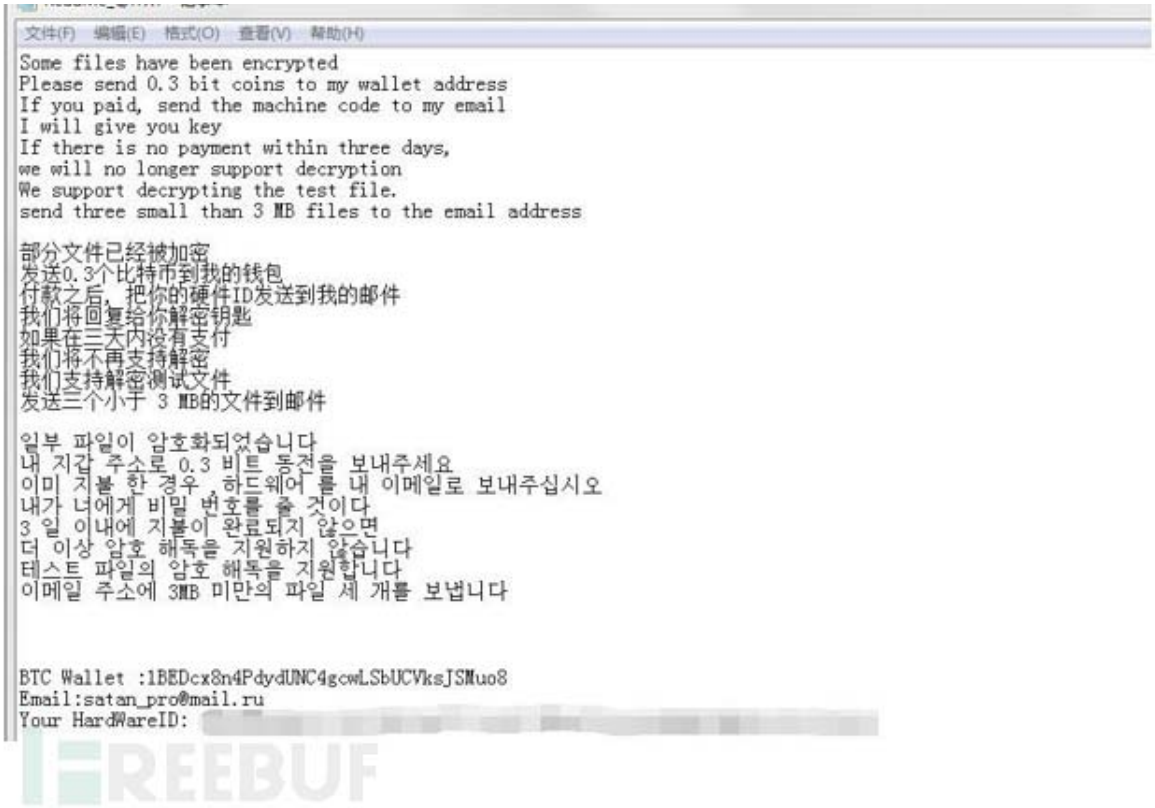
三 主要勒索事件汇总



3.1 近两年勒索事件

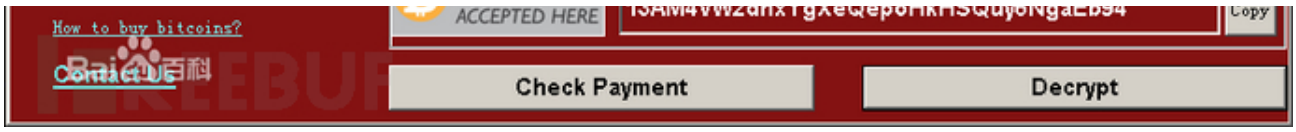
1、2017年1月份，撒旦(Satan)恶意勒索程序首次出现。

Satan病毒的开发者通过网站允许用户生成自己的Satan变种，并且提供CHM和带宏脚本Word文档的下载器生成脚本进行传播。Satan勒索病毒主要用于针对服务器的数据库文件进行加密，非常具有针对性加密完成后，会用英韩三国语言索取0.3个比特币作为赎金，并威胁三天内不支付不予解密。



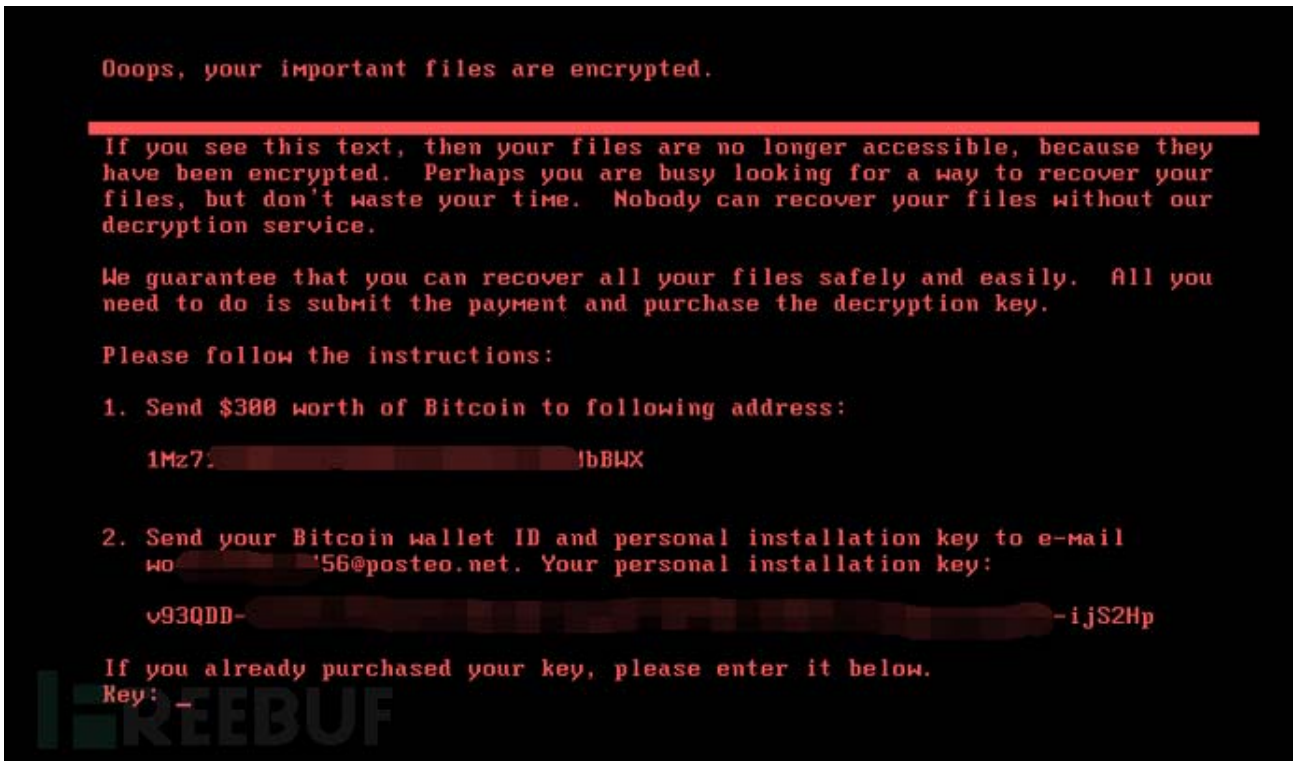
2、2017年5月12日，一种名为“想哭”的勒索病毒袭击全球

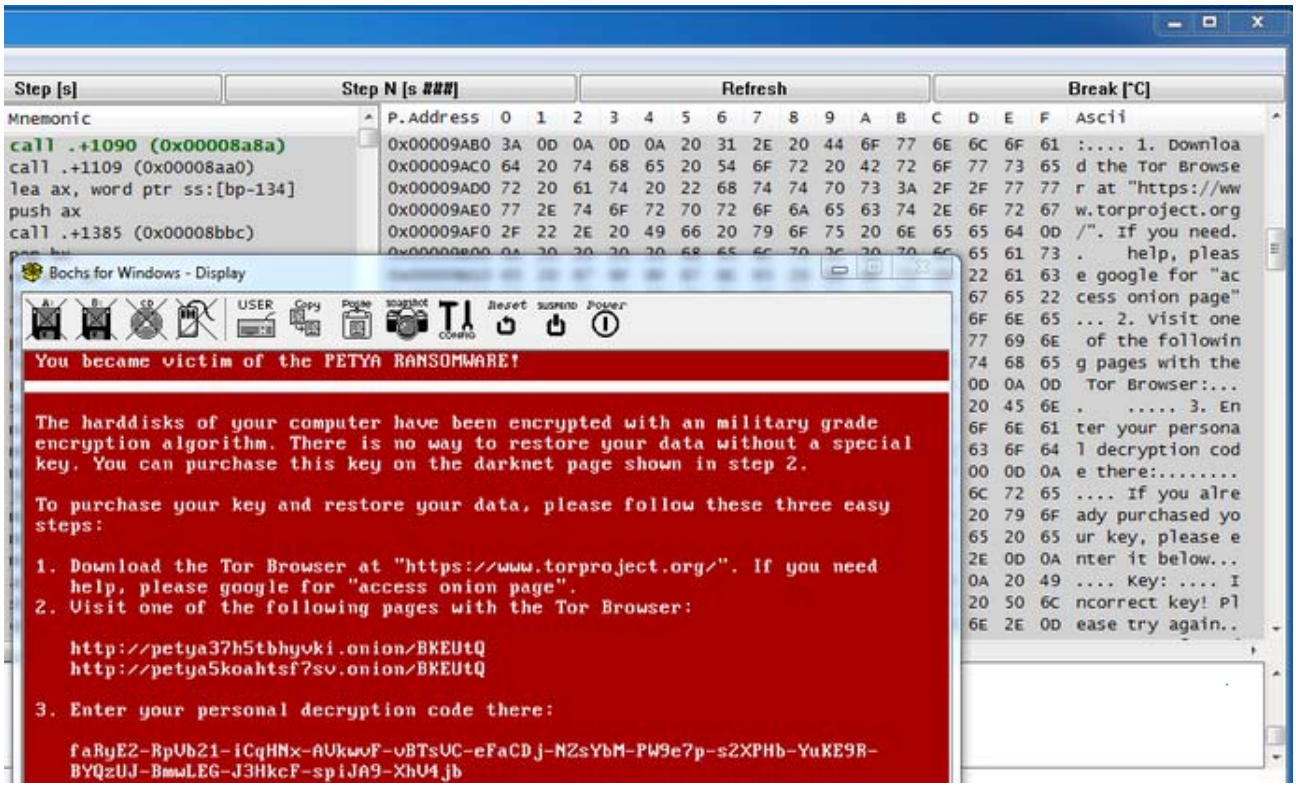
超过150多个国家和地区，影响领域包括政府部门、医疗服务、公共交通、邮政、通信和汽车制造业。不法分子用NSA（National Security Agency，美国国家安全局）泄露的危险漏洞“EternalBlue”（永恒之蓝）进行传播。勒索病毒肆虐，俨然是一场全球性互联网灾难，给广大电脑用户造成了巨大损失。最新统计数据显示，150个国家和地区超过10万台电脑遭到了勒索病毒攻击、感染。

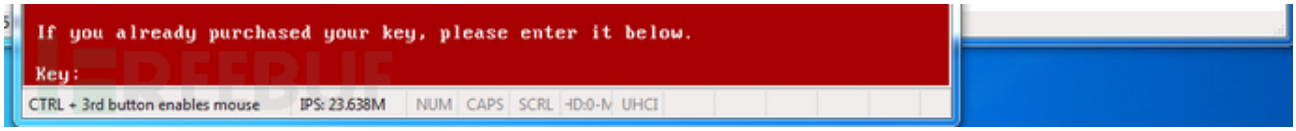


3、2017年6月27日晚，Petya勒索病毒爆发

欧洲多个国家被大规模攻击，尤其是乌克兰，政府机构、银行、企业等均遭大规模攻击，其中乌克兰副总理的电
也遭受攻击。病毒作者要求受害者支付价值300美元的比特币之后，才会回复解密密钥。

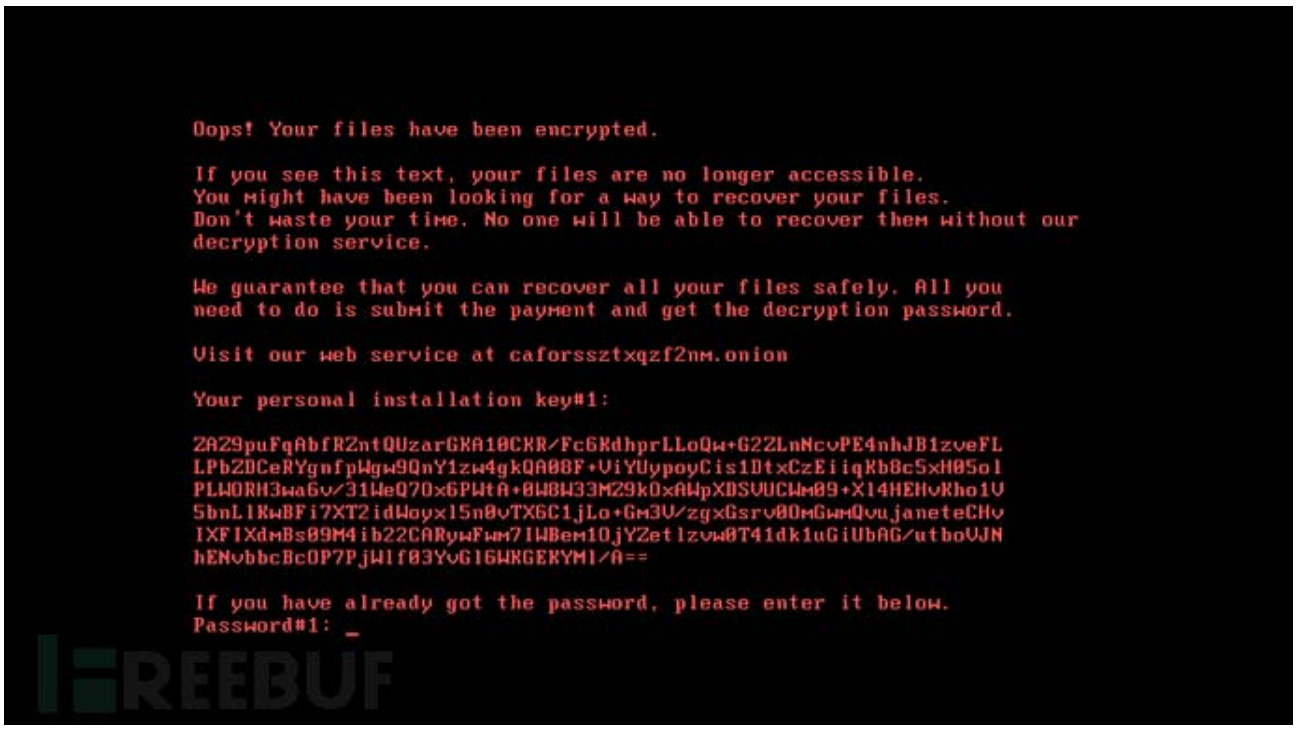






4、2017年10月24日，俄罗斯、乌克兰等国遭到勒索病毒BadRabbit攻击

乌克兰敖德萨国际机场、首都基辅的地铁支付系统及俄罗斯三家媒体中招，德国、土耳其等国随后也发现此病毒。

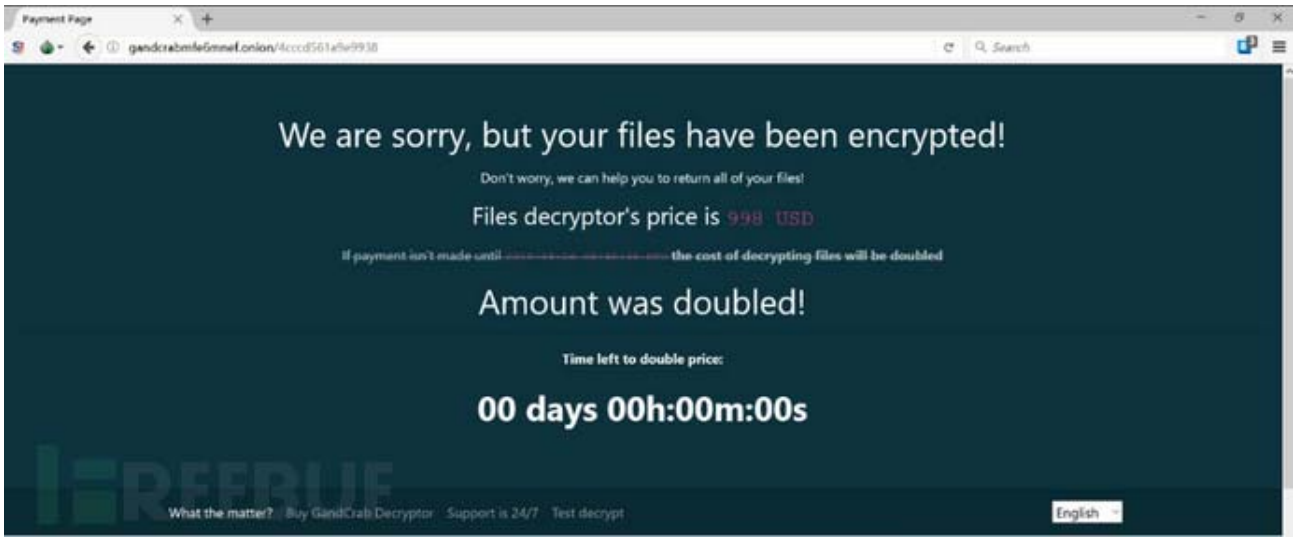


5、xiaoba勒索病毒

10月20日，发现一例国产勒索病毒Xiaoba。该病毒加密后文件以.xiaoba[数字]结尾，不同文件类型其结尾数字不相同，其赎金可以通过微信、支付宝支付，目前暂未发现该勒索病毒有大范围传播。倒计时200秒还不缴赎金被加密的文件就会被全部销毁。

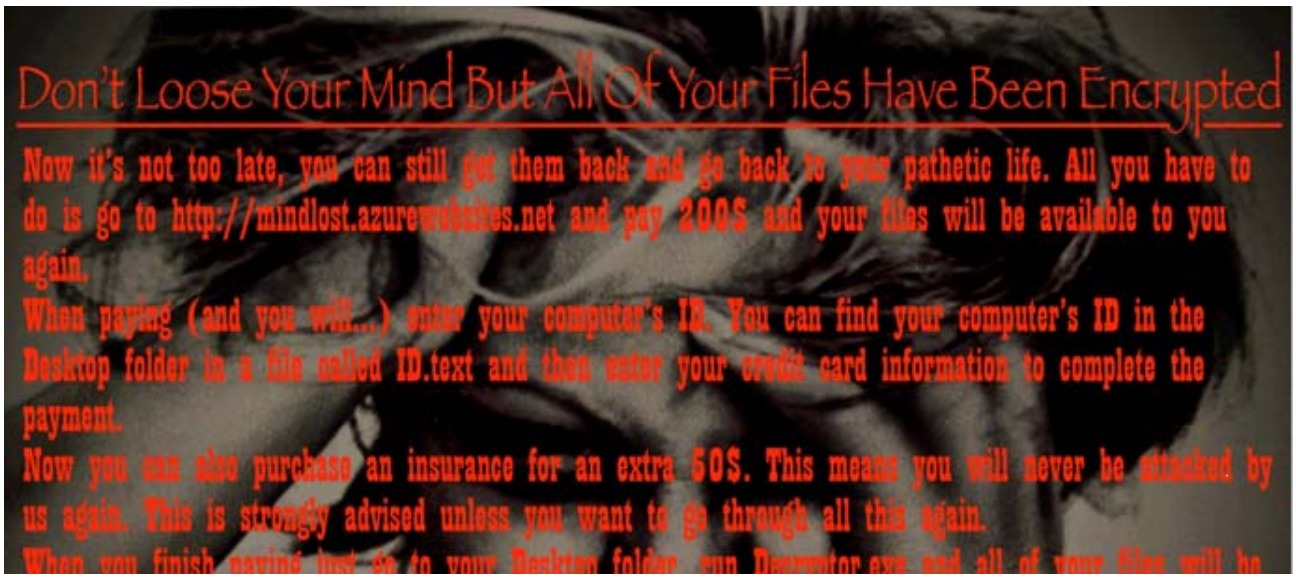
6、2018年1月，GandGrab勒索家族首次出现

应该算是勒索病毒家族中的最年轻，但是最流行的一个勒索病毒家族，短短几个月的时候内，就出现了多个此勒
病毒家族的变种，而且此勒索病毒使用的感染方式也不断发生变化，使用的技术也不断在更新，此勒索病毒主要
过邮件进行传播，采用RSA+ASE加密的方式进行加密，文件无法还原。



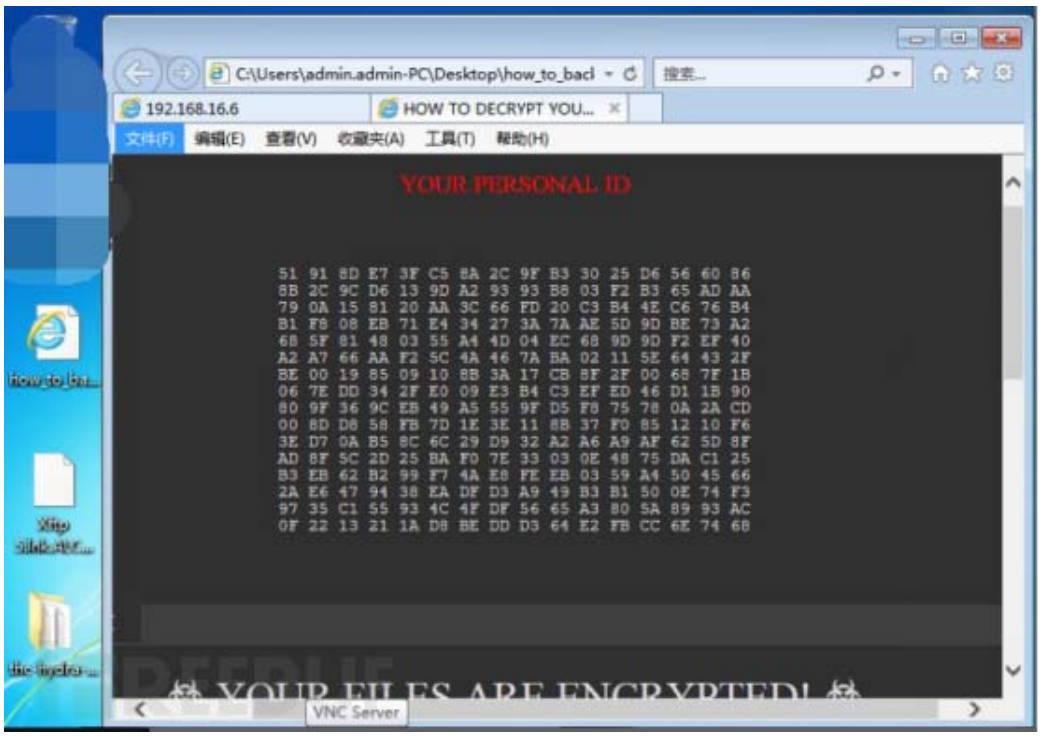
7、2018年2月，多家互联网安全企业截获了Mind Lost勒索病毒

该勒索软件采用C#语言开发，其主要功能是采用AES加密方式加密本地文件，之后引导受害者至指定的网页要求
费解密文件，与以往勒索软件不同的是，此次勒索软件并没有要求受害者支付比特币等数字货币进行付费解密操
作，而是直接要求用户使用信用卡或借记卡支付赎金，以此来套取银行卡信息，进而将此信息出售给不法分子从
牟取更大利益。加密样本账户的电脑的Users目录下的文件，如果后缀
为”.txt”,”.jpg”,”.png”,”.pdf”,”.mp4”,”.mp3”,”.c”,”.py”的文件就直接加密，且解密赎金达到20
美元。其加密完成后显示的提示图片如下：



8、GlobeImposter勒索病毒家族

GlobeImposter勒索病毒家族是从2017年5月开始出现，并在2017年11月和2018年3月有两次较大范围的疫情发，在2017年11月前的GlobeImposter勒索病毒大部分被称为GlobeImposter1.0，此时的病毒样本加密后缀名“.CHAK”较为常见，在2018年3月时出现了GlobeImposter2.0，此时的病毒样本加密后缀名以“.TRUE”，“.doc”较为常见，GlobeImposter也增加了很多新型的技术进行免杀等操作。



9、“麒麟2.1”的勒索病毒

2018年3月1日，监测到了“麒麟2.1”的勒索病毒。通过QQ等聊天工具传文件方式传播，一旦中招就会锁定电文件，登录后会转走支付宝所有余额。中招后，它会锁定电脑文件，表面上要求扫码用支付宝付款3元，但实际扫码是登录支付宝，登录后会转走支付宝所有余额。

10、2018年3月，CrySiS勒索病毒爆发

服务器文件被加密为.java后缀的文件，采用RSA+AES加密算法，主要运用了Mimikatz、IP扫描等黑客工具，进RDP爆破，利用统一密码特性，使用相同密码对全网业务进行集中攻击，通过RDP爆破的方式植入，同时此勒索毒在最近也不断出现它的新的变种，其加密后缀也不断变化之中。

11、2018年12月1日，一个以微信为支付手段的勒索病毒在国内爆发

几日内，该勒索病毒至少感染了10万台电脑，通过加密受害者文件的手段，已达到勒索赎金的目的，而受害者必通过微信扫一扫支付110元赎金才能解密。

2018年6月，罗某某自主研发出病毒“cheat”，用于盗取他人支付宝的账号密码，进而以转账方式盗取资金。

同时制作内含“cheat”木马病毒代码的某开发软件模块，在互联网上发布，任何通过该开发软件编写的应用软均包含木马病毒代码，代码在后台自动运行，记录用户淘宝、支付宝等账号密码，以及键盘操作，上传至服务器此外，嫌疑人通过执行命令对感染病毒的计算机除系统文件、执行类文件以外的所有文件进行加密，随后弹出包解密字样和预置微信收款二维码的勒索界面，解密程序标题显示“你的电脑已被加密，请执行以下操作，扫一扫维码，你需要支付110进行解密”。

四 常见传播方式

勒索病毒的传播方式有很多,比如服务器入侵传播、利用漏洞传播、邮件附件传播、通过软件供应链传播和挂马传播等，我们这里总结了几种最常见传播方式。

4.1 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

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。

如Locky病毒,该病毒一般是通过邮件方式进行传播,黑客对目标对象发送带有附件的恶意邮件,员工或者领导一旦
开附件后,电脑、手机上的各种重要文件,包括软件源代码、Word、PPT、PDF、图片等都会被加密,无法正常使用

4.2 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
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
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
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。

4.3 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
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，以及2018年12月被
光的国产“cheat”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
毒通过税务软件M.E.Doc的升级包投递到内网中进行传播。

4.4 漏洞传播

漏洞传播存在多种类型。

1、通过服务器弱口令传播

如Rapid勒索病毒,根据部分网友在部分论坛中的反馈发现,该病毒通过服务器弱口令方式传播。

2、永恒之蓝系列

①Wannacry及其变种可谓该系列病毒中最为臭名昭著的一类了,爆发以来造成的损失不计其数,包括安全狗在内的
多厂商均针对该系列病毒推出过解决方案。

②Petya勒索病毒的变种。使用的传播攻击形式和WannaCry类似,但该病毒除了使用了永恒之蓝(MS17-010)漏洞
还罕见的使用了黑客的横向渗透攻击技术,利用WMIC/PsExec/mimikatz等

③Satan勒索病毒。通过永恒之蓝漏洞攻击工具在局域网内横向传播,主动入侵未安装补丁的服务器

3、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
软件。

4、复合传播方式

I、GandCrab家族勒索病毒

传播渠道相对其他家族丰富很多,包括挂马攻击、水坑攻击、漏洞攻击和钓鱼邮件攻击,其中水坑攻击令人防不胜
防。水坑攻击传播通过入侵网站后台,将网页内容篡改为乱码,并且提示需要更新字体,诱导用户下载运行“字体更
程序”,实际上用户下载到的是GandCrab2勒索病毒。GandCrab3勒索病毒还通过Bondat蠕虫下载传播。

II、Crysis勒索软件

Crysis这个勒索软件主要通过垃圾邮件、钓鱼邮件、游戏修补程序、注册机、捆绑破解软件等方式传播;有的厂商
认为主要传播方式是利用服务器弱口令漏洞,爆破远程登录用户名和密码,进而通过RDP(远程桌面协议)远程登录目
服务器运行勒索病毒,黑客远程登录服务器后手动操作。

III、GlobeImposter勒索者病毒

GlobeImposter勒索者病毒可以利用电子邮件、文件传输等方式进行扩散,更主要的特点是利用系统的漏洞发起主
态攻击。针对企业服务器的攻击以弱口令爆破服务器后远程登录的方式最为常见。黑客使用自动化攻击脚本,暴力
解服务器管理员账号密码,入侵后可秘密控制服务器,卸载服务器上的杀毒软件并植入勒索病毒。

5 小结

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
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。

五 针对企业服务器勒索攻击

5.1 以企业服务器为攻击目标已成勒索病毒新趋势

从去年下半年开始，勒索病毒在国内的攻击重点开始转向了各类服务器，尤其以windows服务器为甚。黑客利用
口令和各类系统漏洞，软件漏洞向服务器远程渗透投毒，经常出现一个服务集群多台主机被感染的情况，造成的
响轻则服务中断，有严重的更影响到整个公司的运营，已经成为影响企业安全的一大问题。

企业服务器上的数据文件一旦被加密，将严重威胁到公司的正常运转，企业也更倾向于向不法黑客交付赎金。服
器或将成为不法黑客传播勒索病毒的重点攻击目标。

2018开年以来，针对Windows服务器的勒索病毒攻击此起彼伏，尤其是最近国内数家机构服务器同时被
GlobeImposter勒索病毒攻击，黑客在突破企业防护边界后释放并运行勒索病毒，最终导致系统被破坏，日常业
大面积瘫痪，服务器安全问题开始备受关注。

六 勒索攻击发展趋势

1、远程访问弱口令攻击成为主流

许多企业工作中需要进行远程维护，所以许多机器都启用了远程访问。如果密码过于简单，它将很容易被攻击者用。到了2018年，通过弱口令爆破远程登录服务器、再植入勒索病毒的攻击方式最为常见。几个影响力最大的勒索病毒几乎全都采用这种方式进行传播，感染用户数量最多。

2、勒索病毒变种更新迭代更快

勒索病毒每隔一段时间就会出现一个新变种，有的修改加密算法，增加了加密速度，有的为了对抗查杀，使用了杀、反逆向、反沙箱等手段。此外有的勒索病毒新版本开始使用随机后缀，从而增加了受害者查找所中勒索病毒型的难度。

3、国产勒索病毒开始活跃

最近针对国内用户的勒索病毒流行，此类通常会使用全中文的勒索提示界面，个别会要求直接通过微信、支付宝维码的形式来索取赎金。鉴于国内移动支付操作简单，与其它语言版本的勒索病毒相比，索取的赎金数值不高且付操作简单，因此受害者支付赎金的可能性更高。

4、勒索门槛越来越低

随着各种编程语言编写的勒索病毒的出现，勒索软件的开发门槛越来越低。而且我们发现继使用PHP、Python等语言之后，另一种更简单易用的脚本语言——AutoIt语言也被发现用于编写勒索病毒，加上网上迅速传播的一些索病毒的技术细节，导致了勒索病毒从制作到传播的技术门槛不断降低。

5、内网安全重视程度亟需加强

Wannacry集中爆发在企业和高校等组织的内网，核心原因还是内网安全重视程度不够，MS17-010漏洞迟迟未到修复，很多内网主机445文件共享端口未被禁用是主要原因。

如果内网提前做安全加固，比如及时修复MS17-010 SMB服务远程代码执行漏洞，针对Windows系统不安全项核查修复（比如禁用SMB服务），定期异地备份系统数据等亦可避免感染这次的Wannacry勒索蠕虫或降低勒索虫感染带来的损失。无论是内网还是外网，定期的防黑加固甚至一套完整的纵深防御体系建设应该被重视并予以行。

七 如何防范勒索病毒?

7.1 对勒索病毒的方法

第一，已知病毒。对于已知病毒的防范，技术手段比较多，首先是把相关补丁打上，然后将杀毒软件、IPS、W等安全设备的事件库升级到最新版本，基本就能有效防范已知的勒索病毒。

第二，未知病毒。对于未知病毒的防范一直以来都是个难点，基本上所有中招的单位中的都是未知勒索病毒。针

这种病毒的防范，只能采用主动防护的措施，从系统底层采用白名单技术，严格控制对系统中文件的操作权限，止非信任程序对文件的加密操作，可以有效的防止新勒索病毒的攻击。对勒索病毒的防护还是应该采用主动防护措施，事先部署防勒索系统，将重要文件保护起来。

勒索病毒以防为主，目前大部分勒索病毒加密后的文件都无法解密，注意日常防范措施：

1、.数据备份和恢复：可靠的数据备份可以将勒索软件带来的损失最小化，但同时也要对这些数据备份进行安全防护，避免被感染和损坏。

2、小心使用不明来源的文件，陌生邮件及附件也需谨慎打开

3、安装安全防护软件并保持防护开启状态

4、及时安装Windows漏洞补丁！

5、同时，也请确保一些常用的软件保持最新版本，特别是Java，Flash和Adobe Reader等程序，其旧版本经常包含可被恶意软件作者或传播者利用的安全漏洞。

6、为电脑设置较强的密码——尤其是开启远程桌面的电脑。并且不要在多个站点重复使用相同的密码。

7、安全意识培训：对员工和广大计算机用户进行持续的安全教育培训是十分必要的，应当让用户了解勒索软件的传播方式，如社交媒体、社会工程学、不可信网站、不可信下载源、垃圾邮件和钓鱼邮件等。通过案例教育使用户具备一定的风险识别能力和意识。

目前，勒索软件仍然是一项顶级的流行性安全威胁。为了攻击大型企业和组织，勒索软件不断研究新型变体，企机密文件和数据的安全风险与日俱增。结合了基于信任的行为分析和其他反勒索软件功能（如白名单和应用程序制，行为分析，网络监控，漏洞屏蔽和高仿真机器学习）的跨代技术方式的安全解决方案可以更好地保护企业，时最大限度地减少对其计算机内部资源的影响。

浏览... 未选择文件。