奇安信

新一代网络安全领军者

勒索病毒应急响应

自救手册

编写说明

勒索病毒，是伴随数字货币兴起的一种新型病毒木马，通常以垃圾邮件、服务器入侵、网页挂马、捆绑软件等多种形式进行传播。机器一旦遭受勒索病毒攻击，将会使绝大多数文件被加密算法修改，并添加一个特殊的后缀，且用户无法读取原本正常的文件，对用户造成无法估量的损失。勒索病毒通常利用非对称加密算法和对称加密算法组合的形式来加密文件，绝大多数勒索软件均无法通过技术手段解密，必须拿到对应的解密私钥才有可能无损还原被加密文件。黑客正是通过这样的行为向受害用户勒索高昂的赎金，这些赎金必须通过数字货币支付，一般无法溯源，因此危害巨大。

自2017年5月WannaCry（永恒之蓝勒索蠕虫）大规模爆发以来，勒索病毒已成为对政企机构和网民直接威胁最大的一类木马病毒。近期爆发的GlobeImposter、GandCrab、Crysis等勒索病毒，攻击者更是将攻击的矛头对准企业服务器，并形成产业化；而且勒索病毒的质量和数量的不断攀升，已经成为政企机构面临的最大的网络威胁之一。

为帮助更多的政企机构，在遭遇网络安全事件时，能够正确处置突发的勒索病毒，及时采取必要的自救措施，阻止损失扩大，为等待专业救援争取时间。奇安信集团安服团队结合1000余次客户现场救援的实践经验，整理了《勒索病毒应急响应自救手册》，希望能对广大政企客户有所帮助。

目录

第一章 常见勒索病毒种类介绍

自2017年“永恒之蓝”勒索事件之后，勒索病毒愈演愈烈，不同类型的变种勒索病毒层出不穷。

勒索病毒传播素以传播方式快，目标性强著称，传播方式多见于利用“永恒之蓝”漏洞、爆破、钓鱼邮件等方式传播。同时勒索病毒文件一旦被用户点击打开，进入本地，就会自动运行，同时删除勒索软件样本，以躲避查杀和分析。所以，加强对常见勒索病毒认知至关重要。如果在日常工作中，发现存在以下特征的文件，需务必谨慎。由于勒索病毒种类多至上百种，因此特整理了近期流行的勒索病毒种类、特征及常见传播方式，供大家参考了解：

一、WannaCry勒索

2017年5月12日，WannaCry勒索病毒全球大爆发，至少150个国家、30万名用户中招，造成损失达80亿美元。WannaCry蠕虫通过MS17-010漏洞在全球范围大爆发，感染了大量的计算机，该蠕虫感染计算机后会向计算机中植入敲诈者病毒，导致电脑大量文件被加密。受害者电脑被黑客锁定后，病毒会提示需要支付相应赎金方可解密。

1）常见后缀：wncry

2）传播方式：永恒之蓝漏洞

3）特征： 启动时会连接一个不存在url

创建系统服务mssecsvc2.0

释放路径为Windows目录

二、GlobeImposter勒索

2017年出现，2018年8月21日起，多地发生GlobeImposter勒索病毒事件，攻击目标主要是开始远程桌面服务的服务器，攻击者通过暴力破解服务器密码，对内网服务器发起扫描并人工投放勒索病毒，导致文件被加密多个版本更新，并常通过爆破RDP后手工投毒传播，暂无法解密。

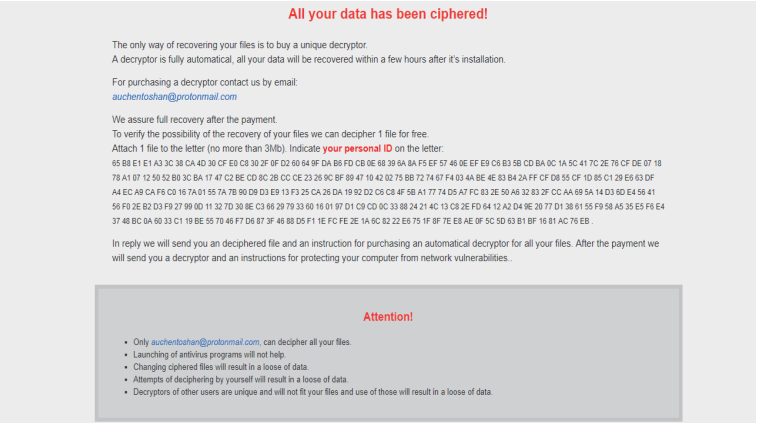
1）常见后缀：auchentoshan、动物名+4444

2）传播方式：RDP爆破

垃圾邮件

捆绑软件

3）特征：释放在%appdata%或%localappdata%



三、Crysis/Dharma勒索

最早出现在2016年，在2017年5月万能密钥被公布之后，消失了一段时间，但在2017年6月后开始继续更新。攻击方法同样是通过远程RDP爆力破解的方式，植入到用户的服务器进行攻击，其加密后的文件的后缀名为.java，由于CrySiS采用AES+RSA的加密方式，最新版本无法解密。

1）常见后缀：【id】+勒索邮箱+特定后缀

2）传播方式：RDP爆破

3）特征：勒索信位置在startup目录

样本位置在%windir%\System32

Startup目录

%appdata%目录

四、GandCrab勒索

2018年年初面世，作者长时间多个大版本更新，仅仅半年的时候，就连续出现了V1.0,V2.0,V2.1,V3.0,V4.0等变种，病毒采用Salsa20和RSA-2048算法对文件进行加密，并修改文件后缀为.GDCB、.GRAB、.KRAB或5-10位随机字母，并将感染主机桌面背景替换为勒索信息图片。GandCrab5.1之前版本可解密，最新GandCrab5.2无法解密。

1）常见后缀：随机生成

2）传播方式：RDP爆破

钓鱼邮件

捆绑软件

僵尸网络

漏洞传播

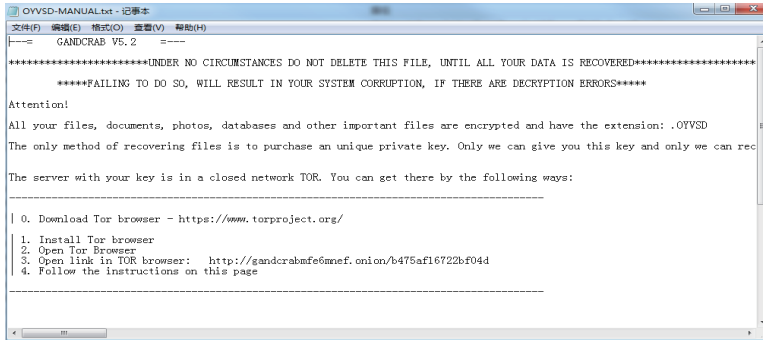
……

3）特征：勒索信位置在startup目录

样本位置在%windir%\System32

Startup目录

%appdata%目录



五、Satan勒索

撒旦（Satan）勒索病毒首次出现2017年1月份。该勒索进行Windows&Linux双平台攻击，最新版本攻击成功后，会加密文件并修改文件后缀为“evopro”。除了通过RDP爆破外，一般还通过多个漏洞传播。

1）常见后缀：evopro

sick

…

2）传播方式：永恒之蓝漏洞

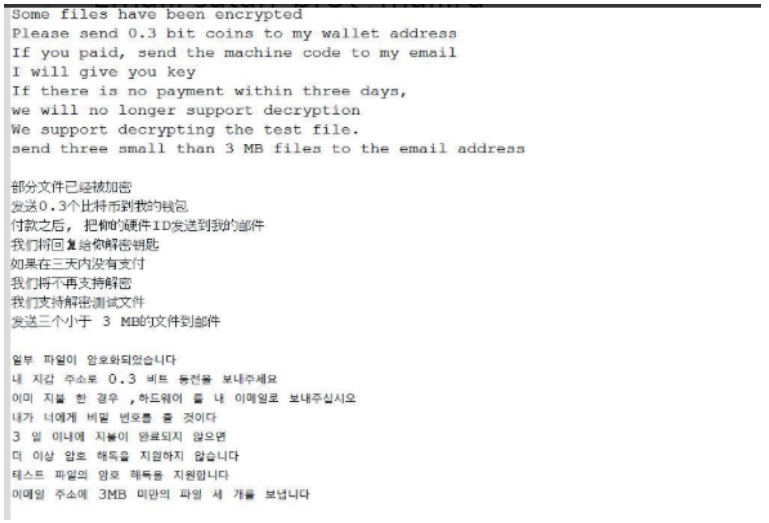
RDP爆破

JBOSS系列漏洞

Tomcat系列漏洞

Weblogic组件漏洞

3）特征：最新变种evopro暂时无法解密，老的变种可解密



六、Sacrab勒索

Scarab（圣甲虫）恶意软件于2017年6月首次发现。此后，有多个版本的变种陆续产生并被发现。最流行的一个版本是通过Necurs僵尸网络进行分发，使用Visual C语言编写而成，又见于垃圾邮件和RDP爆破等方式。在针对多个变种进行脱壳之后，我们发现有一个2017年12月首次发现的变种Scarabey，其分发方式与其他变种不同，并且它的有效载荷代码也并不相同。

1）常见后缀：.krab

.Sacrab

.bomber

.Crash

……

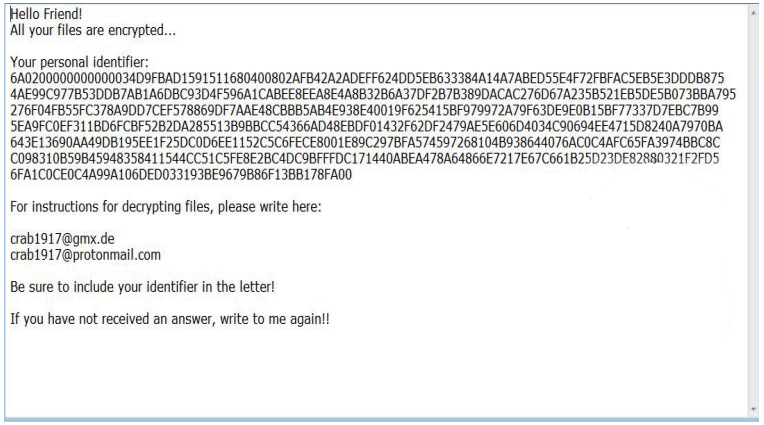
2）传播方式：传播方式：Necurs僵尸网络

RDP爆破

垃圾邮件

……

3）特征：样本释放%appdata%\Roaming



七、Matrix勒索

目前为止变种较多的一种勒索，该勒索病毒主要通过入侵远程桌面进行感染安装，黑客通过暴力枚举直接连入公网的远程桌面服务从而入侵服务器，获取权限后便会上传该勒索病毒进行感染，勒索病毒启动后会显示感染进度等信息，在过滤部分系统可执行文件类型和系统关键目录后，对其余文件进行加密，加密后的文件会被修改后缀名为其邮箱。

1）常见后缀：.GRHAN

.PRCP

.SPCT

.PEDANT

…

2）传播方式：RDP爆破

八、STOP勒索

同Matrix勒索类似，Stop勒索病毒也是一个多变种的勒索木马，一般通过垃圾邮件、捆绑软件和RDP爆破进行传播，在某些特殊变种还会释放远控木马。

1）常见后缀：.TRO

.djvu

.puma

.pumas

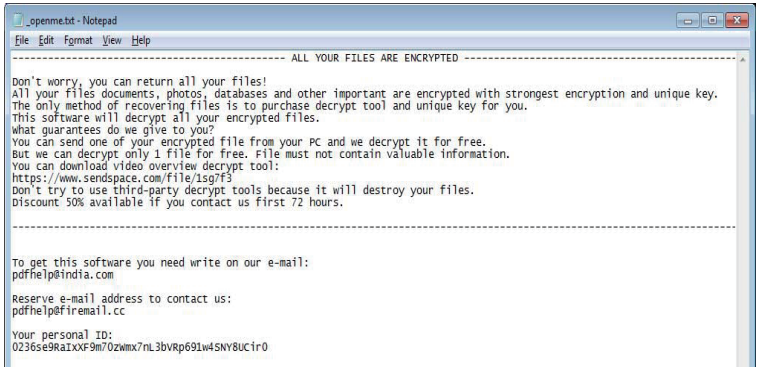
.pumax

.djvuq

...

2）特征：样本释放在%appdata%\local\<随机名称>

可能会执行计划任务

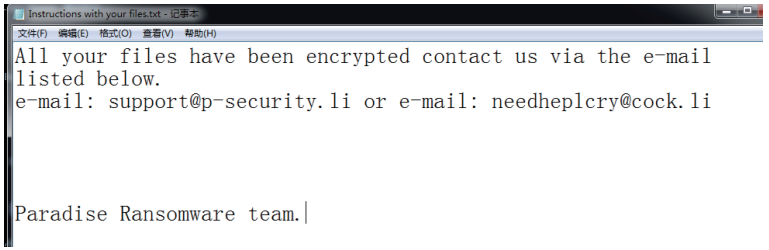


九、Paradise勒索

Paradise勒索最早出现在2018年7月下旬，最初版本会附加一个超长后缀如：（_V.0.0.0.1{yourencrypter@protonmail.ch}.dp）到原文件名末尾，在每个包含加密文件的文件夹都会生成一个勒索信如下：

而后续活跃及变种版本，采用了Crysis/Dharma勒索信样式图弹窗如：

勒索信如下样式



1）加密文件后缀：文件名_%ID字符串%_{勒索邮箱}.特定后缀

2）特征：将勒索弹窗和自身释放到Startup启动目录

第二章 如何判断病情

如何判断服务器中了勒索病毒呢？勒索病毒区别于其他病毒的明显特征：加密受害者主机的文档和数据，然后对受害者实施勒索，从中非法谋取私利。勒索病毒的收益极高，所以大家才称之为“勒索病毒”。

勒索病毒的主要目的既然是为了勒索，那么黑客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。所以，勒索病毒有明显区别于一般病毒的典型特征。如果服务器出现了以下特征，即表明已经中了勒索病毒。

一、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。

比如：2018年2月，某三甲医院遭遇勒索病毒，全院所有的医疗系统均无法正常使用，正常就医秩序受到严重影响；同年8月，台积电在台湾北、中、南三处重要生产基地，均因勒索病毒入侵导致生产停摆。

但是，当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，所以，还需要结合以下特征来判断。

二、电脑桌面被篡改

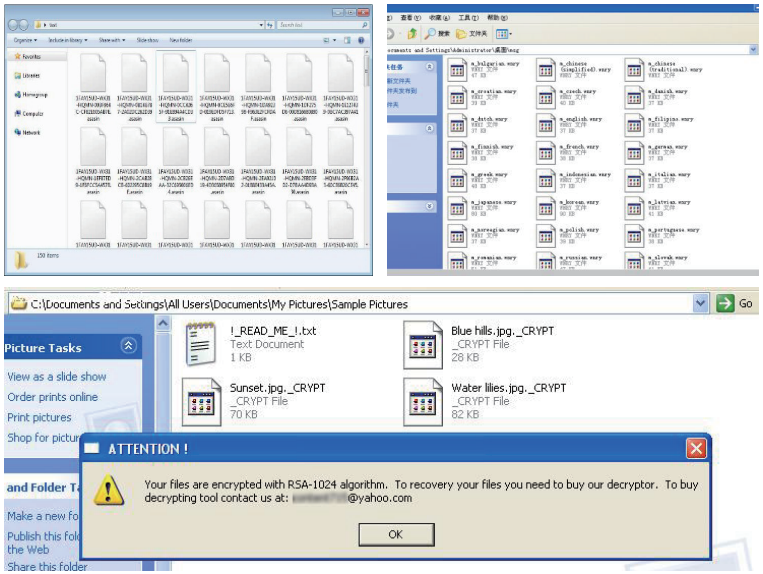
服务器被感染勒索病毒后，最明显的特征是电脑桌面发生明显变化，即：桌面通常会出现新的文本文件或网页文件，这些文件用来说明如何解密的信息，同时桌面上显示勒索提示信息及解密联系方式，通常提示信息英文较多，中文提示信息较少。

下面为电脑感染勒索病毒后，几种典型的桌面发生变化的示意图。

三、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。

下面为电脑感染勒索病毒后，几种典型的文件后缀名被篡改或文件图标变为不可打开的示意图。



当我们看到上述三个现象的时候，说明服务器已经遭到勒索病毒的攻击，此时，如果我们仓促的进行不正确的处置，反而可能会进一步扩大自己的损失。

所以，请保持冷静不要惊慌失措，现在我们需要做的是如何最大化的减少损失，并阻止黑客继续去攻击其他服务器。具体操作步骤请见下一章。

第三章 如何进行自救

当我们已经确认感染勒索病毒后，应当及时采取必要的自救措施。之所以要进行自救，主要是因为：等待专业人员的救助往往需要一定的时间，采取必要的自救措施，可以减少等待过程中，损失的进一步扩大。例如：与被感染主机相连的其他服务器也存在漏洞或是有缺陷，将有可能也被感染。所以，采取自救措施的目的是为了及时止损，将损失降到最低。

一、正确处置方法

（一）隔离中招主机

处置方法

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，隔离主要包括物理隔离和访问控制两种手段，物理隔离主要为断网或断电；访问控制主要是指对访问网络资源的权限进行严格的认证和控制。

1）物理隔离

常用的操作方法是断网和关机。

断网主要操作步骤包括：拔掉网线、禁用网卡，如果是笔记本电脑还需关闭无线网络。

2）访问控制

访问控制常用的操作方法是加策略和修改登录密码。

加策略主要操作步骤为：在网络侧使用安全设备进行进一步隔离，如

防火墙或终端安全监测系统；避免将远程桌面服务（RDP，默认端口为3389）暴露在公网上（如为了远程运维方便确有必要开启，则可通过VPN登录后才能访问），并关闭445、139、135等不必要的端口。

修改登录密码的主要操作为：立刻修改被感染服务器的登录密码；其次，修改同一局域网下的其他服务器密码；第三，修改最高级系统管理员账号的登录密码。修改的密码应为高强度的复杂密码，一般要求：采用大小写字母、数字、特殊符号混合的组合结构，口令位数足够长（15位、两种组合以上）。

处置原理

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。

有一类勒索病毒会通过系统漏洞或弱密码向其他主机进行传播，如WannaCry勒索病毒，一旦有一台主机感染，会迅速感染与其在同一网络的其他电脑，且每台电脑的感染时间约为1–2分钟左右。所以，如果不及时进行隔离，可能会导致整个局域网主机的瘫痪。

另外，近期也发现有黑客会以暴露在公网上的主机为跳板，再顺藤摸瓜找到核心业务服务器进行勒索病毒攻击，造成更大规模的破坏。

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，防止病毒继续感染其他服务器，造成无法估计的损失。

（二）排查业务系统

处置方法

在已经隔离被感染主机后，应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。

处置原理

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。

另外，备份系统如果是安全的，就可以避免支付赎金，顺利的恢复文件。

所以，当确认服务器已经被感染勒索病毒后，并确认已经隔离被感染主机的情况下，应立即对核心业务系统和备份系统进行排查。

（三）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。

政企机构中招客户可以联系：奇安信集团，全国400应急热线：95015 。

二、错误处置方法

（一）使用移动存储设备

错误操作

当确认服务器已经被感染勒索病毒后，在中毒电脑上使用U盘、移动硬盘等移动存储设备。

错误原理

勒索病毒通常会对感染电脑上的所有文件进行加密，所以当插上U 盘或移动硬盘时，也会立即对其存储的内容进行加密，从而造成损失扩大。从一般性原则来看，当电脑感染病毒时，病毒也可能通过U盘等移动存储介质进行传播。

所以，当确认服务器已经被感染勒索病毒后，切勿在中毒电脑上使用U盘、移动硬盘等设备。

（二）读写中招主机上的磁盘文件

错误操作

当确认服务器已经被感染勒索病毒后，轻信网上的各种解密方法或工具，自行操作。反复读取磁盘上的文件后反而降低数据正确恢复的概率。

错误原理

很多流行勒索病毒的基本加密过程为：

1）首先，将保存在磁盘上的文件读取到内存中；

2）其次，在内存中对文件进行加密；

3）最后，将修改后的文件重新写到磁盘中，并将原始文件删除。

也就是说，很多勒索病毒在生成加密文件的同时，会对原始文件采取删除操作。理论上说，使用某些专用的数据恢复软件，还是有可能部分或全部恢复被加密文件的。

而此时，如果用户对电脑磁盘进行反复的读写操作，有可能破坏磁盘空间上的原始文件，最终导致原本还有希望恢复的文件彻底无法恢复。

第四章 如何恢复系统

感染勒索病毒后，对于政企机构来说，最重要的就是怎么恢复被加密的文件了。一般来说，可以通过历史备份、解密工具或支付赎金来恢复被感染的系统。但是这三种操作都有一定的难度，因此，建议受害者不要自行操作。如果您想恢复系统，请联系专业的技术人员或安全厂商，确保赎金的支付和解密过程正确进行，避免其他不必要的损失。

政企机构中招客户可以联系：奇安信集团，全国400应急热线：95015 。

一、历史备份还原

（一）隔离中招主机

如果事前已经对文件进行了备份，那么我们将不会再担忧和烦恼。可以直接从云盘、硬盘或其他灾备系统中，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。

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。

二、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，可以通过互联网上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。

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。

三、专业人员代付

如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。具体主要体现在：

1）统计显示，95%以上的勒索病毒攻击者来自境外，由于语言不通，容易在沟通中产生误解，影响文件的解密。

2）数字货币交付需要在特定的交易平台下进行，不熟悉数字货币交易时，容易人才两空。

所以，即使支付赎金可以解密，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，以保证数据能成功恢复。

四、重装系统

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。

第五章 如何加强防护

一、终端用户安全建议

对于普通终端用户，我们给出以下建议，以帮助用户免遭勒索病毒的攻击：

养成良好的安全习惯

当确认服务器已经被感染勒索病毒后，轻信网上的各种解密方法或工具，自行操作。反复读取磁盘上的文件后反而降低数据正确恢复的概率。

1）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。

2）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。

3）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。

4）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。

5）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

1）安装奇安信集团旗下的“天擎”并开启“先赔服务”，一旦电脑被勒

索病毒感染，可以通过先赔服务申请赎金赔付，以尽可能的减小自身经济损失。

二、政企用户安全建议

1）如用户处存在虚拟化环境，建议用户安装虚拟化安全管理系统，进一步提升防恶意软件、防暴力破解等安全防护能力。

2）安装天擎等终端安全软件，及时给办公终端打补丁修复漏洞，包括操作系统以及第三方应用的补丁。

3）针对政企用户的业务服务器，除了安装杀毒软件还需要部署安全加固软件，阻断黑客攻击。

4）企业用户应采用足够复杂的登录密码登录办公系统或服务器，并定期更换密码，严格避免多台服务器共用同一个密码。

5）限制内网主机可进行访问的网络、主机范围。有效加强访问控制ACL策略，细化策略粒度，按区域按业务严格限制各个网络区域以及服务器之间的访问，采用白名单机制只允许开放特定的业务必要端口，其他端口一律禁止访问，仅管理员IP可对管理端口进行访问，如FTP、数据库服务、远程桌面等管理端口。

6）对重要数据和核心文件及时进行备份，并且备份系统与原系统隔离，分别保存。

7）部署天眼等安全设备，增加全流量威胁检测手段，实时监测威胁、事件。

8）如果没有使用的必要，尽量关闭3389、445、139、135等不用的高危端口，建议内网部署堡垒机类似的设备，并只允许堡垒机IP访问服务器的远程管理端口（445、3389、22）。

9）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。

10）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，持续提升企业对抗新兴威胁的能力。

附录1：勒索病毒已知被利用漏洞合集

已知被利用漏洞
RDP 协议弱口令爆破
Windows SMB 远程代码执行漏洞 MS17-010
Win32k 提权漏洞 CVE-2018-8120
Windows ALPC 提权漏洞 CVE-2018-8440
Windows 内核信息泄露 CVE-2018-0896
Weblogic 反序列化漏洞 CVE-2017-3248
WeblogicWLS 组件漏洞 CVE-2017-10271
Apache Struts2 远程代码执行漏洞 S2-057
Apache Struts2 远程代码执行漏洞 S2-045
Jboss 默认配置漏洞(CVE-2010-0738)
Jboss 反序列化漏洞(CVE-2013-4810)
JBOSS 反序列化漏洞(CVE-2017-12149)
Tomcat web 管理后台弱口令爆破
Spring Data Commons 远程命令执行漏洞(CVE-2018-1273)
WINRAR 代码执行漏洞(CVE-2018-20250)
Nexus Repository Manager 3 远程代码执行漏洞(CVE-2019-7238)

附录2：奇安信集团安服团队

奇安信是北京2022年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商，作为中国领先的网络安全品牌，奇安信多次承担国家级的重大活动网络安全保障工作，创建了稳定可靠的网络安全服务体系——全维度管控、全网络防护、全天候运行、全领域覆盖、全兵种协同、全线索闭环。

奇安信安全服务以攻防技术为核心，聚焦威胁检测和响应，通过提供咨询规划、威胁检测、攻防演习、持续响应、预警通告、安全运营等一系列实战化的服务，在云端安全大数据的支撑下，为客户提供全周期的安全保障服务。

应急响应服务致力于成为“网络安全120”。自2016年以来，奇安信已积累了丰富的应急响应实践经验，应急响应业务覆盖了全国31个省（自治区、直辖市），2个特别行政区，处置政企机构网络安全应急响应事件超过三千起，累计投入工时37000多个小时，为全国超过两千家政企机构解决网络安全问题。

奇安信还推出了应急响应训练营服务，将一线积累的丰富应急响应实践经验面向广大政企机构进行网络安全培训和赋能，帮助政企机构的安全管理者、安全运营人员、工程师等不同层级的人群提高网络安全应急响应的能力和技术水平。奇安信正在用专业的技术能力保障着企业用户的网络安全，最大程度地减少了网络安全事件所带来的经济损失，并降低了网络安全事件造成的社会负面影响。

应急响应7×24小时热线电话：95015。