勒索病毒应急与响应手册

V1.0

杭州安恒信息技术股份有限公司

二〇一九年三月

前言

勒索病毒主要以邮件、程序木马、网页挂马的形式进行传播，利用各种非对称加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。勒索病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。

勒索病毒文件一旦进入本地，就会自动运行。接下来，勒索病毒利用本地的互联网访问权限连接至黑客的 C&C 服务器，进而上传本机信息并下载加密公钥，利用加密公钥对文件进行加密。除了拥有解密私钥的攻击者本人，其他人是几乎不可能解密。加密完成后，通常还会修改壁纸，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。勒索病毒变种类型非常快，对常规的杀毒软件都具有免疫性。攻击的样本以 exe、js、wsf、vbe 等类型为主，对常规依靠特征检测的安全产品是一个极大的挑战。勒索过程如下：

本手册第 1 章详述如何判断是否已感染勒索病毒，是否已被加密；第 2 章详述当主机处于不同的中毒阶段时，从基础措施和高级措施方向上，分别应如何进行应急响应；第 3 章介绍对于已加密系统的五种处理方式，重要文件需要恢复应分别尝试备份还原、解密、数据恢复、支付解密，价值较低的文件可直接重装系统，并进行主机加固；第 4 章详述如何进行勒索病毒的防治建议，包括五个基础措施和应用终端检测与响应（EDR）产品。

通过应用本手册，在不同阶段及时做出响应，尽可能避免或降低损失。

目录

第一章　判断当前状态

一 感染未加密

从攻击者渗透进入内部网络的某一台主机到执行加密行为往往有一段时间，如果在这段时间能够做出响应，完全可以避免勒索事件的发生。如果有以下情况，可能是处于感染未加密状态：

1　监测设备告警

如果使用了监测系统进行流量分析、威胁监测，系统产生大量告警日志，例如“SMB 远程溢出攻击”、“弱口令爆破”等，可能是病毒在尝试扩散。

2　资源占用异常

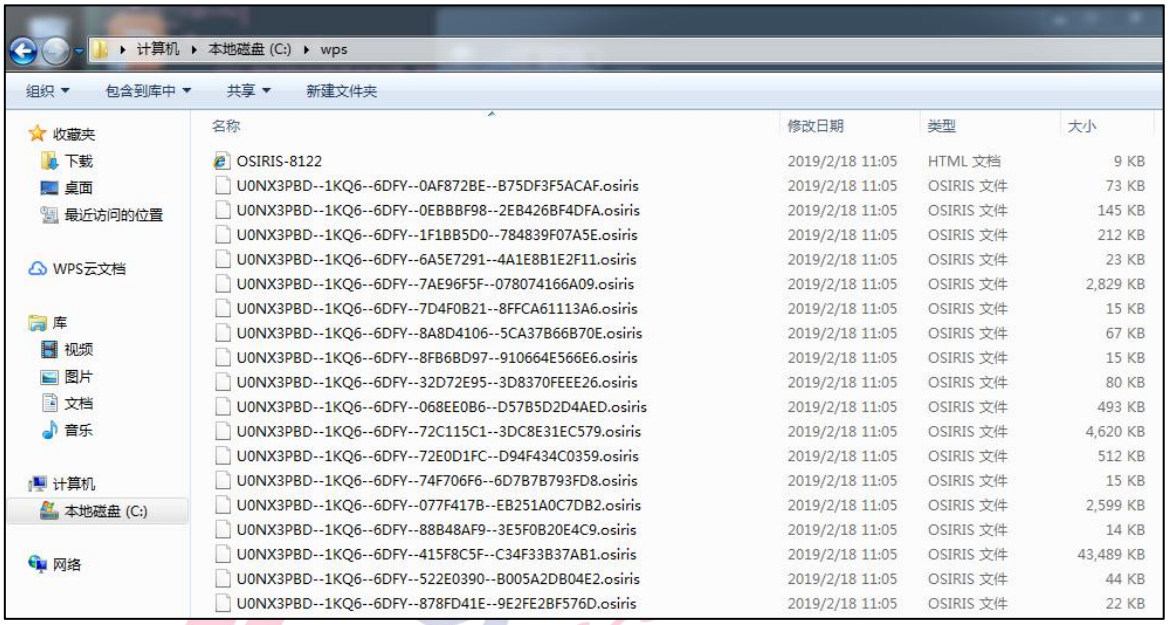
病毒会伪装成系统程序，释放攻击包、扫描局域网络 445 端口等占用大量系统资源，当发现某个疑似系统进程的进程在长期占用 CPU 或内存，有可能是感染病毒。

二 感染已加密

勒索病毒的目的是索要赎金，所以会加密文件并在明显位置留下勒索信，通过这两点可以判断系统是否已经被加密。

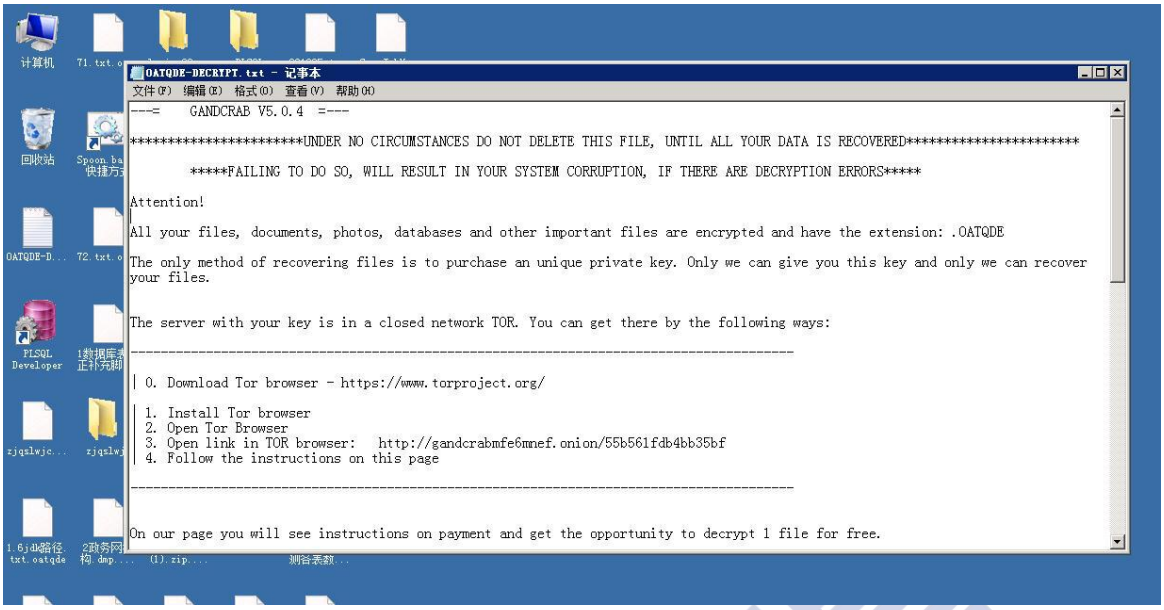
1 统一的异常后缀

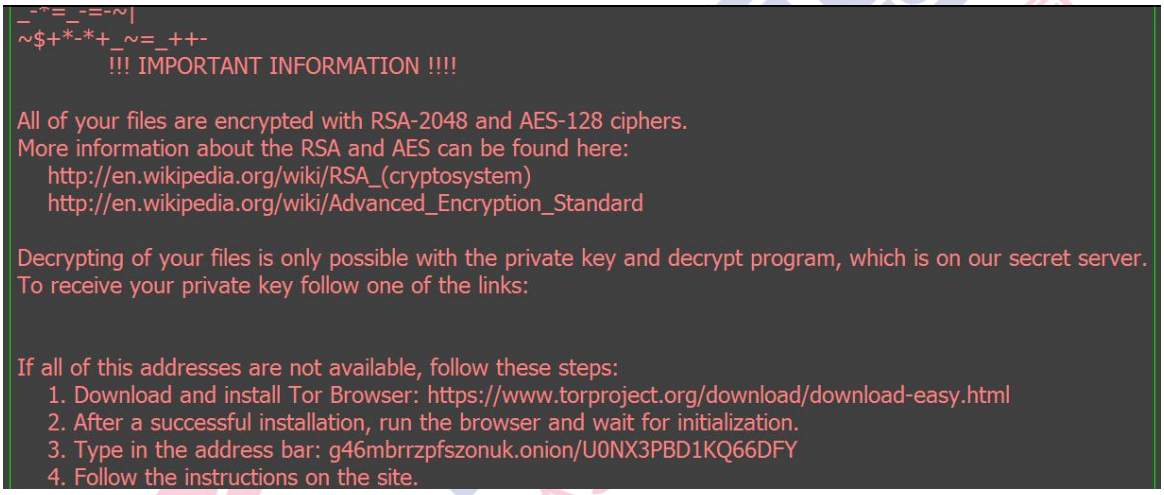
勒索病毒执行加密程序后会加密特定类型的文件，不同的勒索病毒会加密几十到几百种类型的文件，基本都会包括常见的文档、图片、数据库文件。当文件夹下文件变成如下统一异常不可用后缀，就是已经被加密了。



2 勒索信或桌面被篡改

勒索病毒加密文件的最终目的是索要赎金，所以会在系统明显位置如桌面上留下文件提示，或将勒索图片更改为桌面。勒索信绝大多数为英文，引导被勒索的用户交赎金。


OATQDE-DECRIPT.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
---= GANDCRAB V5.0.4 =---
**********UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED**********
*****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****
Attention!
All your files, documents, photos, databases and other important files are encrypted and have the extension: .OATQDE
The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.
The server with your key is in a closed network TOR. You can get there by the following ways:
| 0. Download Tor browser - https://www.torproject.org/
| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser: http://gandcrabmfe6mnef.onion/55b561fdb4bb35bf
| 4. Follow the instructions on this page
On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.


!!! IMPORTANT INFORMATION !!!!
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: g46mbrrzpfszonuk.onion/U0NX3PBD1KQ66DFY
4. Follow the instructions on the site.

第二章　响应当前状态

一 基础响应措施

某台主机在感染勒索病毒后，除了自身会被加密，勒索病毒往往还会利用这台主机去攻击同一局域网内的其他主机，所以当发现一台主机已被感染，应尽快采取响应措施，以下基础措施即使不是专业的人员也可以进行操作，以尽可能减少损失。

1 隔离中毒主机

（1）物理隔离

断网，拔掉网线或禁用网卡，笔记本也要禁用无线网络。

（2）逻辑隔离

访问控制、关闭端口、修改密码。访问控制可以由防火墙等设备来设置，禁止已感染主机与其他主机相互访问；视情况关闭 135、139、445、3389 等端口，避免漏洞被或 RDP（远程桌面服务）被利用；尽快修改被感染主机与同一局域网内的其他主机的密码，尤其是管理员（Windows 下的 Administrator，Linux 下的 root）密码，密码长度不少于 8 个字符，至少包含以下四类字符中的三类：大小写字母、数字、特殊符号，不能是人名、计算机名、用户名等。

2 排查其他主机

隔离已感染主机后，应尽快排查业务系统与备份系统是否受到影响，确定病毒影响范围，准备事后恢复。如果存在备份系统且备份系统是安全的，就可以将损失降到最低，也可以最快的恢复业务。

3 主机加固

主机感染病毒一般都是由未修复的系统漏洞、未修复的应用漏洞或者弱口令导致，所以在已知局域网内已有主机感染并将之隔离后，应检测其他主机是否有上述的问题存在。

(1) 系统漏洞可以使用免费的安全软件检测并打补丁。

(2) 应用漏洞可以使用免费的漏扫产品（AWVS、APPScan 等）检测并升级或采用其他方式修复。

(3) 弱口令应立即修改，密码长度不少于 8 个字符，至少包含以下四类字符中的三类：大小写字母、数字、特殊符号，不能是人名、计算机名、用户名等。

二 高级响应措施

基础措施可以一定程度上响应勒索事件，但当病毒情况严重、感染主机较多或面对未知类型勒索变种，基础措施的效果就十分有限。当有数百台甚至更多主机的场景感染勒索病毒，是无法逐一去采取基础响应措施，需要借助专业的安全产品进行监测、防护和专业的安全团队的技术支持。

1 监测：APT 警平台

安恒信息 APT 产品，对网络中传输的已知和未知恶意文件样本结合病毒引擎、静态分析和动态分析，对勒索病毒及其变种传播及时告警，对传播类型、传播途径、恶意代码传播、回连域名、漏洞利用等行为进行深度解析，准确定位感染源和感染主机。

通过 APT 内置沙箱虚拟执行环境，对流量中勒索病毒动态行为分析，捕获其动态行为、网络行为、进程行为、文件行为、注册表行为等关键信息，识别其中可疑的勒索病毒特点，快速对网络中传输的勒索病毒样本进行预警。

通过 APT 云端情报共享，依托于云端海量数据、高级的机器学习和大数据分析能力，及时共享最新的安全威胁情报，发现已知和未知威胁恶意样本传播行为，对勒索病毒更精确的定位分析。

2 查杀与防护：EDR 主机安全及管理系统

安恒主机卫士 EDR 通过“平台+端”分布式部署，“进程阻断+诱饵引擎”双引擎防御已知及未知类型勒索病毒。部署监控端后，通过平台统一下发安全策略。具备诱饵捕获引擎、内核级流量隔离等行业领先技术。对于**已知勒索病毒**，通过“进程启动防护引擎”零误报零漏报查杀；对于**未知勒索病毒**，采用“专利级诱饵引擎”进行捕获，阻断其加密行为；通过内核级的流量隔离技术，自动阻止勒索病毒在内网扩散或者接收远程控制端指令。

3 技术支持：安恒信息安全服务

(1) 勒索病毒应急响应服务

在勒索病毒已经加密系统文件后，既要遵循常规的应急响应实施过程也要针对勒索病毒的特点进行相对应的处理工作。

在高级响应措施中，安恒信息安全服务将基于第一现场收集到的各类应急处置信息，例如病毒感染文件的最初时间，结合操作系统日志、业务系统日志、网络设备日志等设备日志综合判断和构建这一时段信息系统各组件所执行的操作，并通过内

存取证，硬盘镜像等电子证物取证技术手段开展恶意样本取证分析操作，从以上应急响应业务操作中构建事件发展的时间线、证据链从而推测判断事件发生的准确原因以及病毒传播的源头，并进一步根据所发现的各类电子证物追踪背后攻击者，在各项应急处置过程进展顺利的情况下找出源头设备以及对应的攻击者。

在完成现场取证操作后，将对事件情况出具专业完整的应急响应报告，专业的应急响应报告不但需要对事件的描述和判断，也会针对此类勒索病毒事件给出专业的安全加固建议以及常用的应急处置办法，从而在本次应急处置过后不会在完成系统恢复之后再次被感染，从而造成更严重的影响。

(2) 开展应急响应的常规操作过程

过程	主要内容
初步信息收集	● 事发单位的网络拓扑情况 ● 单位信息系统人员情况 ● 针对事发系统的使用习惯 ● 事发信息系统的运维情况
上机操作	● 操作系统日志提取 ● 业务系统访问、操作、登录等日志提取 ● 病毒样本提取 ● 操作系统网络状态获取 ● 文件加密状态情况 ● 勒索内容表现形式
溯源操作	● 日志分析结果 ● 病毒分析结果 ● 主机安全漏洞排查情况 ● 病毒植入方式分析 ● 病毒影响范围与网络拓扑综合判断 ● 病毒扩散的方向-有外网入侵或内网系统相互传播 ● 初步给出入侵时间线、可疑 IP、其他可疑判断攻击者的数据
其他情况的处理	● 主机故障，例如系统无法开机，系统已经重启过多次等情况。 ● 日志缺失情况下的分析 ● 在未取证完毕的情况下受感染服务器重装系统 ● 现场要求数据恢复

	● 现场要求解密的可能性判断 ● 给出安全加固建议

第三章　已加密系统的处理办法

一 备份还原

备份可以是本机、异机或异地（云端）备份，通常勒索病毒会遍历所有磁盘并加密文件，同时删除 Windows 的阴影卷，删除备份历史快照，所以**本机备份**恢复的可能性很低。**异机备份**如果是通过本地磁盘到共享磁盘进行文件或者数据拷贝的方式实现，勒索病毒同样有可能加密了备份文件。与感染病毒的主机不在同一局域网内的**异地备份**系统最能在此时发挥作用。

进行备份还原前，要确保原主机上病毒已彻底清除，应进行磁盘格式化并重装系统。日常进行合理的数据备份，是最有效的灾难恢复方法。

二 解密工具

大部分勒索病毒使用 128 位密钥的 AES（对称加密算法）加密文件，再将 AES 的密钥使用 2048 位密钥的 RSA（非对称加密算法）加密，通过暴力破解来解密是不科学的，所以通常的解密工具是通过已公开的密钥来解密。而**密钥来源**有三种途径：

- 一是破解勒索程序得到，前提是勒索程序本身存在漏洞，但此概率极低。
- 二是勒索者对受害人感到愧疚、同情等极端情况而公开密钥。
- 三是执法机构获得勒索者的服务器，同时服务器上存储着密钥且执法机构选择公开。

除了付费解密的工具，还可尝试国际刑警组织反勒索病毒网站（https://www.nomoreransom.org/zh/index.html）提供的解密工具。

三 数据恢复

一部分勒索病毒加密文件的时候直接加密原文件，还有一部分勒索病毒是加密原文件副本再删除原文件，而原文件有些会用随机数覆盖，有些并没有。原文件没有被覆盖的情况就可以通过数据恢复的方式进行恢复。

除了收费的专业数据恢复可以尝试使用 DiskGenius 等工具扫描磁盘进行数据恢复。

四 支付解密

在早期勒索病毒基本都是勒索不同数额的比特币，但是随时虚拟货币市场的发展，勒索病毒勒索的内容也不单单围绕比特币。例如 2018 年 1 月首次出现的 Gandcrab 家族勒索的就是更能隐藏用户信息达世币。

注意：由于勒索病毒已呈现产业化，同时在大量的实例表明，现阶段存在大量的

变种病毒，支付赎金后，并不提供真实有效的密钥，实际解密成功率极低。同时，存在人为投毒后，冒以专家身份主动联系代付解密的情况，故不建议直接支付解密。但当数据十分重要且上述其他方法都无法恢复，最终经过综合评判，确定需要支付赎金以尝试解密时，也建议听取安全专家或警方人员的建议以及综合判断，谨慎处置。

五 重装系统

当使用上述方法恢复数据后或不需要解密文件，原本的中毒主机都需要重装系统后再使用。确保主机上没有可用数据后进行格式化并重装系统，格式化是保证不会有残余的病毒文件，当格式化之后将无法再进行数据恢复。重装系统后要打好补丁，软件应确保使用最新版本或打好补丁，避免漏洞被利用。口令也应符合上文中提到过的强口令要求。如何做好勒索病毒的事前防护会在第 4 章会详述。

第四章　勒索病毒的防治建议

由于勒索病毒的变种较多，同时具有病毒、蠕虫、人为投毒等多种形式，当勒索病毒成功运行后，解密较为困难，所以勒索病毒的防治主要预防为主，加强整体网络安全管理，以及有效的技术治理手段，如强化勒索病毒防护的 EDR 产品，监测传播途径的 APT 产品等。

一 基础防护措施及建议

很多勒索病毒的落地并不一定经过长时间复杂的攻击过程，可能就是源于一封垃圾邮件，所以一定不能忽略很多基础措施。

1　增强安全意识

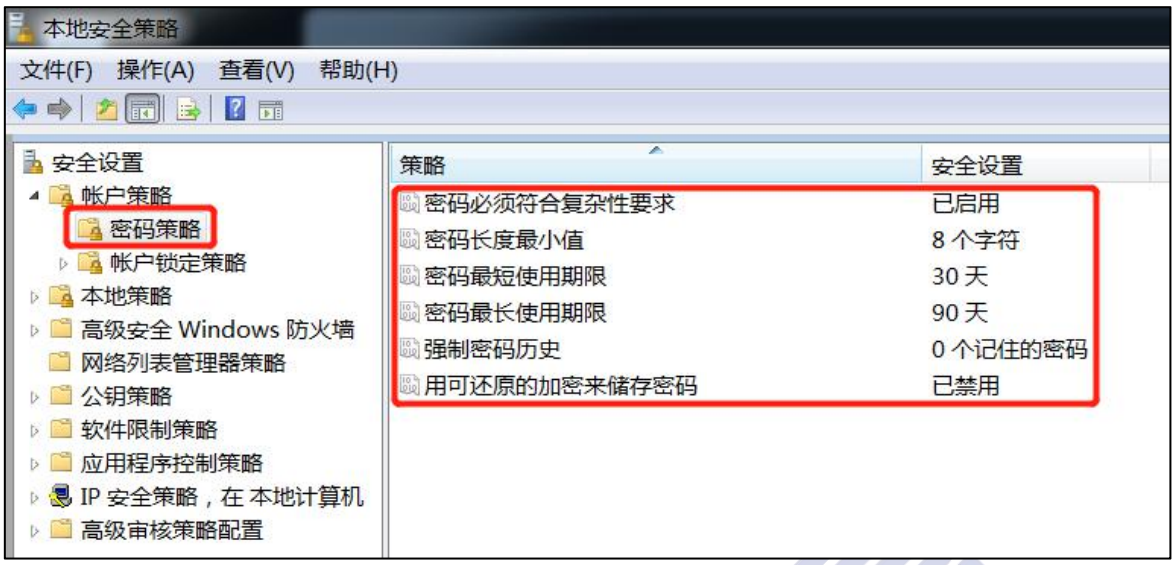
除了漏洞利用与暴力破解外，最多的感染勒索病毒的原因就是利用网页挂马、垃圾电子邮件与捆绑恶意程序，所以日常使用网络时要有以下安全意识：

- 不访问色情、博彩等等不良信息网站，这些网站通常会引导访客下载病毒文件或发动钓鱼、挂马攻击。
- 不轻易下载陌生人发来的邮件附件，不点击陌生邮件中的链接。
- 不随意使用陌生 U 盘、移动硬盘等外设，使用时切勿关闭防护软件比如 Windows 自带的 Windows defender，避免拷入恶意文件。
- 不轻易运行 bat、vbs、vbe、js、jse、wsh、wsf 等后缀的脚本文件和 exe 可执行程序，不轻易解压不明压缩文件。陌生文件下载运行前可使用文件威胁分析平台进行检测（http://ti.dbappsecurity.com.cn:8080/），避免感染病毒。
- 定期查杀病毒，清理可疑文件，备份数据。

2　增加口令强度

勒索病毒最常用的攻击方式是利用永恒之蓝漏洞和爆破 RDP（远程桌面协议）等服务弱口令，为应对后者应立即修改系统和各应用（MySQL、SQLServer 等）的弱口令、空口令、多台服务器共用的重复口令。强密码长度不少于 8 个字符，至少包含以下四类字符中的三类：大小写字母、数字、特殊符号，不能是人名、计算机名、用户名、邮箱名等。

在企业中可以通过密码策略让电脑使用者必须设置一个复杂密码，Windows 操作系统可以通过配置密码策略来实现。



3 修复系统漏洞

在微软发布高危漏洞公告后应尽快修复系统存在的漏洞，避免被恶意利用。微软安全响应中心：https://docs.microsoft.com/zh-cn/security-updates/。在企业中或个人如果不能及时关注响应这些漏洞信息，应借助安全软件完成漏洞修复。尤其当企业有庞大数量的主机需要管理时，应选择合适的安全管理系统完成修复漏洞的工作，这点在下一节详述。

4 修复应用漏洞

勒索病毒利用的漏洞工具除了广为人知的永恒之蓝系列，新型的勒索病毒一般还携带许多 Web 应用漏洞利用工具，比如 JBoss 反序列化漏洞(CVE-2013-4810)、Tomcat 任意文件上传漏洞（CVE-2017-12615）、Tomcat web 管理后台弱口令爆破、Apache Struts2 远程代码执行漏洞 S2-045 等。所以应定期检测并修复漏洞，最好是能够及时更新版本。

5 端口管理

除了必要的业务需求应关闭 135、139、445、3389 等端口，及时需要对部分机器开放，也应做出配置仅限部分机器可访问。通过防火墙配置、安全软件隔离或准入管理。

二 边界网络检测建议

1 传统安全设备边界防护弱点

利用电子邮件、应用程序漏洞（例如 web 应用漏洞）、0day 漏洞（零日漏洞）、Nday 漏洞（已知漏洞）、社会工程学等找到进入目标网络的大门获取权限后，进行勒索病毒植入。

由于传统防御体系是建立在已知知识、规则的基础上，缺乏对未知威胁的感知能

力，难以有效发现勒索病毒及其变种。

（1）网络防火墙

防火墙核心功能是网络层逻辑隔离和规则控制，应用层检测能力较弱，一般需要管理员手工添加规则防护，新一代防火墙通常集成了病毒、web 和内容检测，但都局限于特征明显的攻击检测，对于隐藏在合法数据包内的攻击难以防范。

（2）入侵检测系统（IDS）

IDS 基于单规则和特征库分析，仅限于对已知漏洞进行检测，易被绕过，误报率和漏报率较高，尤其在隐蔽性较强的攻击行为和 0day 面前无能为力。

（3）防病毒网关

防毒墙主要通过对 HTTP、FTP、SMTP、IMAP 等协议的数据进行病毒扫描，检测进出的数据，但所有的检测基本都基于文件类型，并且只能根据特征匹配已知的病毒木马攻击，难以检测利用 0day 进行的病毒传播行为。

2 安恒 APT 对边界流量深度检测

（1）勒索病毒突破网络边界防御传播途径

攻击方式	描述
水坑攻击	利用目标网站的防护弱点，植入恶意代码，当用户访问目标网站时执行恶意代码，一旦中招，将造成严重损失。
邮件恶意附件	勒索病毒利用用户防范意识薄弱的情况，将恶意程序伪装成看似正常的文件，通过邮件附件方式发送给用户，诱骗用户下载执行。
系统漏洞利用	此种方式的传播通常具有横向扩散的特点，病毒、蠕虫通过利用 ODAY、NDAY 漏洞感染无防护的站点、主机等。 锁定目标入侵弱点探测、渗透入侵、获取权限、命令控制、数据盗取的五大攻击阶段都经过精心策划，传统的防护设备对黑客势在必行的攻击力不从心，须加强应对 APT 高级威胁的安全防护手段。
软件下载、文件共享式攻击	勒索病毒以插件等形式被植入软件安装程序里，通过文件共享等形式传播，具有极强的隐蔽性，一旦执行，可能造成严重的数据、财产的损失。

（2）安恒 APT 对勒索病毒边界传播检测

检测方法	描述
恶意文件深度分析	结合先进的沙箱检测技术，通过病毒引擎检测、静态分析、动态分析等维度对协议文件进行深度分析，发现勒索病毒及其变种传播行为。

漏洞利用行为检测	对 ODAY/NDAY 漏洞利用行为检测，结合动态沙箱分析技术，发现网站漏洞、文件漏洞、系统漏洞等可能被勒索软件利用以及传播的行为。
DNS 异常流量检测	采用 DGA 域名检测算法，及时发现受控端和远控端之间的异常通讯，精确定位被勒索病毒感染主机。
社工攻击检测	对社工类攻击准确预测，比如通过邮箱域名信誉分析、收件人账号检测发现基于邮件钓鱼的勒索行为攻击；结合文件检测技术对邮件恶意附件隐藏的恶意代码深度分析，及时检出勒索病毒的传播行为。
云端高级威胁分析	通过云端提供的深层次威胁分析服务、安全预警服务和情报共享服务，对勒索病毒行为准确预判，防患未然。

三 终端防护建议：终端检测与响应（EDR）

1 传统杀毒软件在应对勒索时的困境

（1）单点能力无法应对勒索的分布式扩散

勒索病毒在局域网内大量扩散，对主机上安装的杀毒软件无法及时全部配置检测任务。

（2）杀毒软件无法处理未知的勒索病毒变种

勒索病毒变种繁多，杀毒软件依赖规则库，面对新型勒索病毒无法识别，只能任由其完成加密行为

2 安恒主机卫士 EDR 的优势

（1）防御已知和未知类型勒索病毒

面对使传统杀毒软件束手无策的未知类型勒索病毒，安恒主机卫士 EDR 采用诱饵引擎，在未知类型勒索病毒试图加密时发现并阻断其加密行为，有效守护主机安全。

（2）管控全局终端安全态势

服务器、PC 和虚拟机等终端安装了客户端软件后，上传病毒木马、违规外联、安全配置等威胁信息到管理控制中心。用户在管理控制中心可以看到所有安装了客户端软件的主机，包括服务器、PC 和虚拟机的安全态势，并进行统一任务下发，策略配置。

（3）全方位的主机防护体系

安恒主机卫士 EDR 包含传统杀毒软件的病毒查杀、漏洞管理、性能监控功能，在系统防护方面还可做到系统登录防护、系统进程防护、文件监控，还支持网络防护、Web 应用防护、勒索挖矿防御、外设管理等多个功能点。

（4）流量可视化，安全可见

安恒主机卫士 EDR 通过流量画像的流量全景图，展示内网所有流量和主机间通信关系，梳理通信逻辑，上帝视角对策略进行规划，便于用户第一时间发现威胁，一键清除威胁。

（5）简单配置，离线升级，补丁管理

安恒主机卫士 EDR 可将人类语言转化为具体安全配置，明确、有效的进行主机防护。主程序、病毒库、漏洞库、补丁库、Web 后门库、违规外联黑名单库全部支持离线导入升级包、一键自动升级，可在专网使用。

四 技术支持：安恒信息安全服务

1 渗透测试服务

信息系统的安全防护是每一个网络运营者在日常工作中不可获取的内容，但是攻击者的数量却依旧逐年增加并且攻击事件频发，我司总结多年的安全服务经验并结合海内外成熟的渗透测试攻防理念引导客户从攻击者的角度出发来认识自己的信息系统安全防护能力，使用攻击者的攻击思路与工具来验证自身的防护机制有效性、完整性和保密性从而真实的判断当前所处的网络安全形势。

2 安全加固建议

(1) 安装终端管理杀毒软件 EDR。

(2) 增强服务器补丁安装意识；

(3) 在网络层面部署流量分析设备 APT 以及大型内网中架设态势感知威胁预警平台。

(4) 对各类业务系统涉及到的服务器采用堡垒机进行安全管控。

(5) 对重要业务系统开展等级保护测评工作。

(6) 定期的安全评估工作，通过定期的安全评估和渗透工作，寻自身系统和应用的薄弱项，例如弱口令问题，主机基线配置问题；

(7) 增加日常网络安全培训计划，从人员意识到管理员安全技术能力培养，从而正确有效的面对各类安全事件并能快速处置。

(8) 定期开展应急演练工作，部署实际演练场景，时长练兵才能在安全事件发生时正确有效快速的处置。

(9) 重要数据异地安全备份是在安全事件发生后的有效恢复手段，也需要在演练中尝试已经备份的数据，从而保证备份数据有效性。

(10) 数据库的安全也是 WEB 应用安全的重要一环，应该坚持以下几个原则：

- 定时备份数据；
- 对外公开的 WEB 应用所使用的数据库帐号只赋予 SELECT 等极少数的权限，尤其 DROP TABLE 这样的权限要取消；
- 大部分数据库帐号仅仅使用 DB_OWER 即可，不需要高权限的 DBA(sa)帐号；

- 用户帐号密码等敏感数据，应该对密码列进行加密后存储，比如将密码串 MD5 加密，而不是将明文字符串存放在数据库中；
- 删除多余的危险数据库存储过程；
- 数据库所在的服务器严格控制网络访问，不但仅允许极少数主机访问它，还需要设置仅允许它访问极少数主机，双向都要控制。

3 安全培训

通过不同内容的安全培训加强企事业单位人员的安全技能和安全意识，从而做好安全建设和运营工作。

培训的形式较为丰富，可以是常见的安全意识宣讲活动、内部圆桌讨论形式、安全试验参与形式、应急演练模拟攻击试验，再到后期的安全认证体系培养。

- CISP 认证简介

  “注册信息安全专业人员”（英文为 Certified Information Security Professional，简称 CISP）系经中国信息安全测评中心认定的国家信息安全专业人员，具备保障信息系统安全的专业资质。

- 工业控制系统安全工程师 （CISP-ICSSE）认证培训简介

  工业控制系统（如数据采集与监控（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）等）广泛用于能源、交通、水利、冶金、石油化工、核能等工业生产领域，以及航空、铁路等公共服务领域，是国家关键基础设施的重要组成部分，其安全性事关经济发展、社会稳定和国家的战略安全。

- 云安全工程师（CISP-CSE）认证培训简介

  对云计算技术的充分理解以及云计算安全问题的深入分析成为各行业的迫切需求。云计算安全保障离不开专业人才的作用，培养一批精通云计算技术原理，掌握云计算安全理论和实践的专业人才对我国信息安全事业的发展有着重要意义。

- 大数据安全分析师 （CISP-BDSA）认证培训简介

  CISP-BDSA 是对我国大数据安全分析人员进行资质评定的重要形式之一。持证人员掌握涵盖大数据概述和分析过程、数据分析算法原理和示例、大数据系统工程实现、大数据安全分析常见案例、大数据系统安全法律法规等知识内容，具备大数据安全分析理论基础和实践能力，可从事大数据安全分析、安全管理等工作的高级应用型人才。

储备专业人才，培养网络安全意识是加强企事业单位安全防御力量的一项重要工作内容，只有人员的素质真正提升，才能让安全事件、勒索病毒远离我们的各类信息资产。

五 工控环境的适用性

1 勒索病毒对工业生产的危害

(1) 生产中断

一旦感染病毒会迅速扩散到该安全域内的每一台主机，HMI 主机的沦陷直接导致生产的不可视。尤其流程行业的生产是连续的、相互关联的，某个安全域的停车将导致整个企业的生产中断。

(2) 窃取机密

生产工艺是生产企业的核心竞争力，如果勒索病毒回传工业主机上的生产数据，企业将面临生产工艺的泄漏以及生产数据的泄漏。这足可以导致一个企业的覆灭。

(3) 恶意操作

勒索病毒可以利用操作站的系统漏洞、HMI 漏洞或弱口令等脆弱性问题，获得 HMI 软件的操作权限，对现场工业设备进行恶意操作，直接破坏设备安全或制造人员伤害。如果操作者了解流程行业知识，可直接操纵安全事故的发生。

(4) 劫持设备

很多 PLC、DCS 存在漏洞，自动化厂商已经将这些漏洞公布在其官网上供用户下载更新。但是工业企业追求生产的稳定性，一般不会对其进行更新。勒索病毒可以利用这些公布的漏洞，实现对工控系统的底层控制，获取设备的控制权而不被操作人员发现。

2 工控系统的勒索病毒防护

由于工控系统是生产控制的大脑，且赎金相对停产损失微不足道，勒索病毒的目标，盯上了工业领域。国内多个工业企业遭受了勒索病毒的攻击，工业主机被锁、蓝屏，不断重启，严重影响正常生产或导致直接停产。我们建议从以下几点做好工控系统的勒索病毒事前防护工作。

(1) 安全培训

在工控系统的特殊环境下，对运营管理人员的要求更高于普通 IT 网络，当工控系统设备在勒索病毒攻击下出现异常或停车时，会影响上下游生产，这需要运营管理人员准确判断当前情况，并迅速做出处理降低对生命财产的损害。这需要对 IT 运营人员进行必要的工控知识培训。

另外，工控系统操作人员的安全意识非常重要，应加强安全技术和意识的培训，让相关操作人员从思想意识形态上认识到工业信息安全的重要性，杜绝一切人为失误。

完全依赖安全设备或管理制度均不可取，加强工控系统安全需两者结合。

(2) 安全域边界

工控环境最基本的防护手段是根据功能集合划分安全域，安全域间做隔离。每个安全域代表一个或多个生产车间、工段的功能集合，

对工控系统网络中的设备进行识别，发现存在安全隐患或者存在已知漏洞的设备，及时修复，对于不便停机升级的设备进行必要的隔离保护，关闭工控系统网络中所有非必要的通讯端口，监测审计网络工控网络中的流量。另外，工控主机需要长期运行，一般在投产后就很少进行系统升级、漏洞修复操作，企业应该意识到这些操作的必要性并创造机会实施。

（3）安全域内的异常检测

作为以防万一的保障，确保在发生攻击事件后有能力追查攻击来源、造成的影响和所有设备是否已经被完全恢复。

（4）工控主机卫士特点

安恒工控主机卫士采用静默安装方式，兼容主流自动化厂家的工控软件，通过统一管理平台维护管理工业网络里所有主机，支持离线升级，方便企业在不停车情况下对工控主机进行升级。

安恒工控主机卫士通过白名单加黑名单机制，有效控制主机非法外联。对网络的边界进行保护，对接入网络的终端和使用进行合规检查，杜绝不安全的电脑、U 盘等设备未经充分检查接入工控系统。

（5）制订备份与恢复计划

对于生产资料和系统进行备份，将备份文件用单独的设备离线储存或保存到安全的环境中，并准备恢复计划。

六 勒索保险

1 功能说明

安恒信息网络勒索保险是一款根据客户实际需求、产品使用场景，针对网络勒索风险，定制开发的保险产品。网络勒索保险与 EDR 产品配套使用，通过 EDR 防护产品与勒索保险结合，为客户提供一站式的网络勒索风险解决方案。主要内容如下：

- 发生勒索事件后，聘请专业安全团队应急响应、系统升级加固发生的费用由保险公司负责赔偿。
- 对于已被加密的主机，在通过技术无法立即解密且是重要文件的情况下，网络勒索保险先行支付等值赎金及时解决客户问题。

2 保险责任

（1）技术鉴定费用

实际或疑似发生网络风险事件，对被保险人因此发生的技术鉴定服务费，保险公司在赔偿限额内并扣除免赔额（率）后承担赔偿责任。

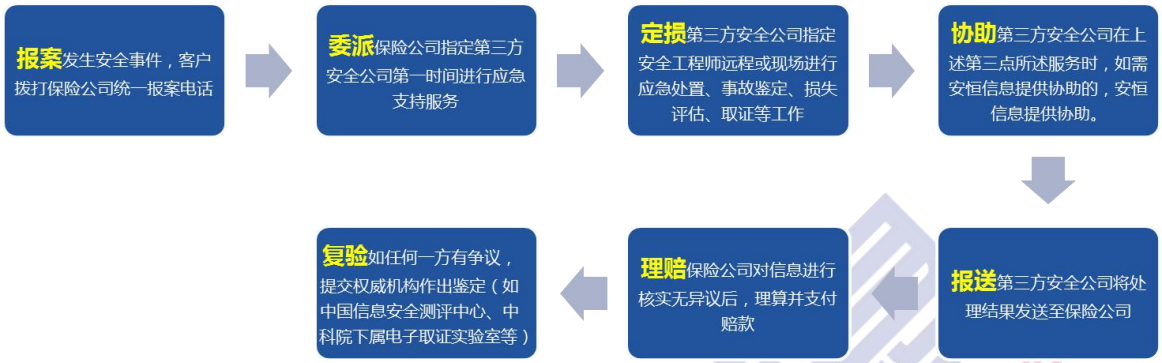
（2）网络安全加固费用

发生网络风险事件，避免损失或影响的恶化，保险合同列明的第三方专业安全机构对网络运维环境进行防御、加固、修复、升级所发生的合理费用和支出，保险公司在赔偿限额内并扣除免赔额（率）后承担赔偿责任。

(3) 网络勒索责任

由于受到网络攻击、网络安全威胁而被勒索，导致产生以下的损失和费用，保险公司在赔偿限额内并扣除免赔额（率）后承担赔偿责任。

3 理赔流程



以上产品、服务，可咨询：400-6059-110