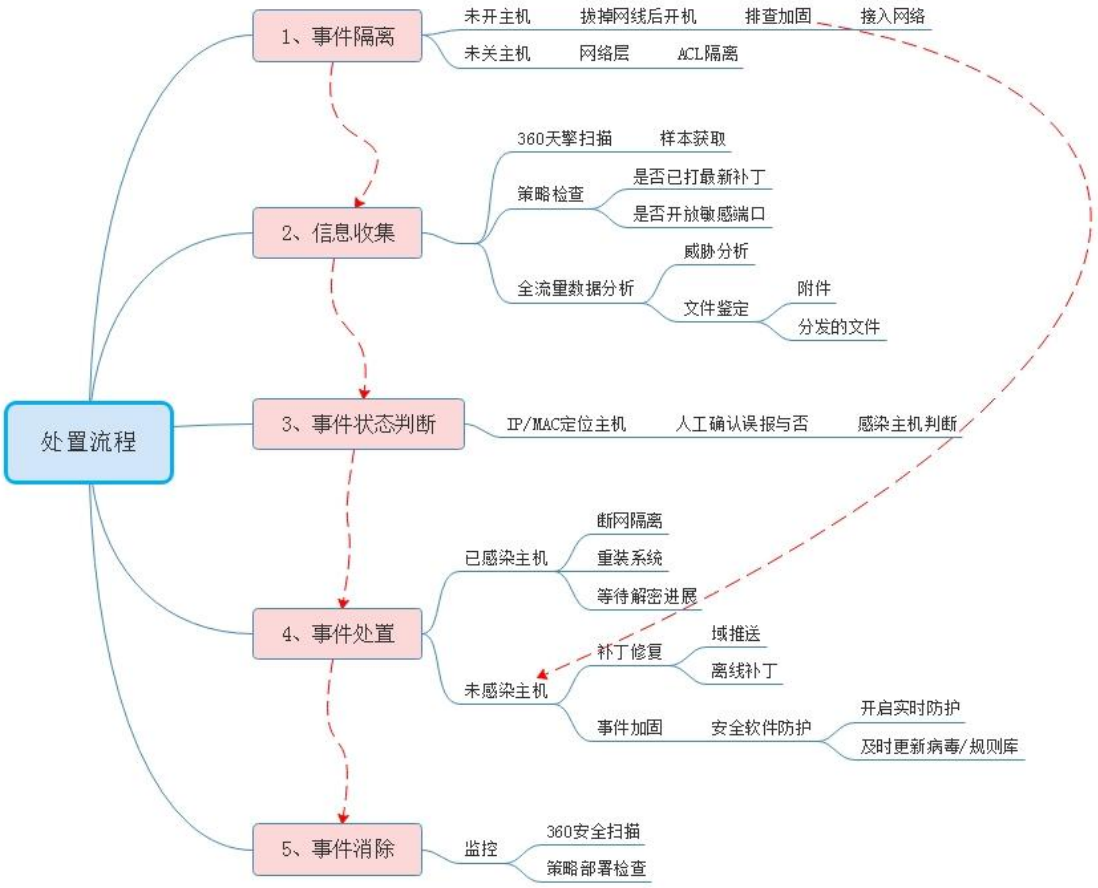
1、勒索病毒事件应急操作手册



处理流程图

1.1 现场访谈

1.1.1 了解勒索病毒事件表现

1. 文件被加密
2. 设备无法正常启动
3. 定时删除文件
4. 勒索信息展示
5. 桌面有新的文本文件并记录加密信息及解密联系方式。

1.1.2 了解勒索病毒事件发现时间

1. 文件加密时间
2. 设备无法正常启动的时间
3. 新的文本文件的出现时间

1.1.3 了解系统架构，如服务器类型、业务架构、网络拓扑等

系统名称	IP 地址	端口开放	物理机/虚拟机	主机名	设备型号	操作系统类型
BIDW（数据库）节点 01	10.2xx.xx.xx	80、22	物理机	Bnnnn	IBM P595	AIX
操作系统版本	**管理后台 IP 地址**	**中间件类型**	**中间件版本**	**数据库类型**	**数据库版本**	**应用 URL**
AIX 5.3	10.xx.xxx.79	was	6.1.0.47	oracle	V11g	gmcc.net
应用端口	**储存设备类型**	**储存设备型号**	**web 框架**	**中间件版本**	**第三方组件**	
80	磁带库	3584/L52	struts	2.4	编辑器	

1.2 判断安全事件状态

根据访谈结果，判断是否误报

1. 是否有勒索信息展示
2. 文件是否被加密
3. 设备是否无法正常运行

1.3 确认勒索病毒对象

了解勒索病毒的对象以及内容,统计失陷主机：

1.→IP 地址、设备类型(以表格形式统计)

IP 地址	操作系统	资产状态
10.1.2.3	Windows 2008 R2	失陷

被感染文件特征：

1. 操作系统桌面是否有新的文本文件,文本文件中是否有详细的加密信息及解密联系方式；

2. 被加密的文件类型：

.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .ott, .sxw, .stw, .uot, .3ds, .max, .3dm, .ods, .ots, .sxc, .stc, .dif, .slk, .wb2, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm, .mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .frm, .myd, .myi, .ibd, .mdf, .ldf, .sln, .suo, .cpp, .pas, .asm, .cmd, .bat, .ps1, .vbs, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .3gp, .mkv, .3g2, .flv, .wma, .mid, .m3u, .m4u, .djvu, .svg, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png, .bmp, .jpg, .jpeg, .vcd, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .tbk, .bz2, .PAQ, .ARC, .aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .602, .hwp, .snt, .onetoc2, .dwg, .pdf, .wk1, .wks, .123, .rtf, .csv, .txt, .vsdx, .vsd, .edb, .eml, .msg, .ost, .pst, .potm, .potx, .ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotx, .dotm, .dot, .docm, .docb, .docx, .doc

3. 加密后的文件后缀：

.WNCRYT，.lock，.pre_alpha，.aes，.aes_ni，.xdata，.aes_ni_0day， .pr0tect，.[stopstorage@qq.com].java， 文件后缀无变化。

4. 还可以借用在线查询查看对应的勒索病毒类型

https://lesuobingdu.qianxin.com/

https://lesuobingdu.360.cn/

1.4 确认勒索病毒时间

确定勒索病毒对象感染的时间，从而梳理出事件的发生时间。

被感染文件：

Linux

执行命令 stat[空格]文件名，包括三个时间 access time（访问时间）、modify time（内容修改时间）、change time（属性改变时间），如：

stat /etc/passwd

Windows

右键查看文件属性，查看文件时间

1.5 问题排查

根据事件时间、传播方式进行问题的排查。

1.5.1 Windows 系统排查

1.5.1.1 文件排查

1. 检查桌面及各个盘符根目录下是否存在异常文件。根据文件夹内文件列表时间进行排序，查找可疑文件；

2. 查看文件时间，创建时间、修改时间、访问时间。对应 linux 的 ctime mtime atime，通过对文件右键属性即可看到详细的时间（也可以通过 dir /tc 1.aspx 来查看创建时间）；

3. 使用 systeminfo 命令查看系统补丁情况；

4. 使用 net user 查看系统账户情况，或者通过计算机—右键—管理—本地用户和组；

5. 借助天擎等杀毒软件查看是否存在异常文件。

1.5.1.2 进程排查

1. 检查是否存在异常进程。使用 netstat -ano 查看目前的网络连接，查看是否存在可疑 ip、端口、进程；

2. 使用 tasklist 命令查看可疑进程；

3. 检查是否存在异常计划任务；

4. 检测 CPU、内存、网络使用率；（通过资源管理器查看）

5. 注册表项检测。

1.5.1.3 日志排查

查看事件管理器：

系统日志：查看是否有异常操作，如创建计划任务、关机、重启；

安全日志：查看是否有异常的登录行为；

应用日志：查看应用是否有异常程序运行；

开始->运行-> 执行“ 控制面板->管理工具->本地安全策略->审核策略”。

审核登录事件，双击，设置为成功和失败都审核：

- 审核策略更改；
- 审核登录事件；
- 审核对象访问；
- 审核进程跟踪；
- 审核目录服务访问；
- 审核特权使用；
- 审核系统事件；
- 审核账户登录事件；
- 审核账户管理；

1.5.2 Linux 系统排查

1.5.2.1 文件排查

1. 查看桌面是否存在异常文件。针对可疑文件可以使用 stat 进行创建修改时间、访问时间的详细查看，若修改时间距离事件日期接近，有线性关联，说明可能被篡改或者其他；

2. 查找 777 的权限的文件 find/ *.jsp -perm 4777 ；

3. 查找隐藏的文件（以 "."开头的具有隐藏属性的文件 ls –al）；

4. 查看 CPU、内存、网络使用率；

5. find / -uid 0 -print：查找特权用户文件；

6. md5sum -b filename：查看文件的 md5 值；

7. rpm -qf /bin/ls：检查文件的完整性（还有其它/bin 目录下的文件）；

8. crontab -u root -l：查看 root 用户的计划任务；

9. cat /etc/crontab 查看计划任务；

10. 查看分析 history (cat /root/.bash_history)，曾经的命令操作痕迹；

11. cat /etc/passwd 分析可疑帐号，可登录帐号。

1.5.2.2 进程排查

1. 使用 netstat 网络连接命令，分析可疑端口、可疑 IP、可疑 PID 及程序进程；

2. 使用 ps 命令，分析进程

ps -aux：查看进程

lsof -p pid：查看进程所打开的端口及文件

检测隐藏进程：

ps -ef | awk '{print }' | sort -n | uniq >1

ls /proc | sort -n |uniq >2

diff 1 2

1.5.2.3 日志排查

1. 使用 lastlog 命令，系统中所有用户最近一次登录信息；

2. 使用 lastb 命令，用于显示用户错误的登录列表；

3. 使用 last 命令，用于显示用户最近登录信息（数据源为/var/log/wtmp，var/log/btmp）；

4. utmp 文件中保存的是当前正在本系统中的用户的信息；

5. wtmp 文件中保存的是登录过本系统的用户的信息；

6. 查看 cron.log 中是否有计划任务信息。

1.5.3 网络流量排查

1. 有全流量的记录设备（如天眼）；

2. 分析内网是否针对 445 端口的扫描和 MS17-010 漏洞的利用；

3. 分析溯源被勒索终端被入侵的过程；

4. 分析邮件附件 MD5 值匹配奇安信威胁情报中心的数据判定是否为勒索病毒；

5. 分析在网络中传播的文件是否被二次打包、进行植入式攻击；

6. 分析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 等软件漏洞的攻击。

1.6 专家研判

通过事件排查，确定勒索病毒特征和传播方式。

病毒特征：全球主流的敲诈者病毒家族（类型）有 75 种之多，（按字母排序）如下：

7ev3n	CryptoJoker	KimcilWare	Radamant
8lock8	CryptoMix	Kriptovo	RemindM
Alpha	CryptoTorLocker	KryptoLocker	Rokku

AutoLocky	CryptoWall	LeChiffre	Samas
BitCryptor	CryptXXX	Locky	Sanction
BitMessage	CrySiS	Lortok	Shade
Booyah	CTB-Locker	Magic	Shujin
Brazilian	Ransomware	DMA	Locker
BuyUnlockCode	ECLR	Ransomware	MireWare
Cerber	EnCiPhErEd	Mischa	Surprise
Chimera	Enigma	Mobef	TeslaCrypt
CoinVault	GhostCrypt	NanoLocker	TrueCrypter
Coverton	GNL	Locker	Nemucod
Crypren	Hi	Buddy!	Nemucod-7z
Crypt0L0cker	HydraCrypt	OMG!	Ransomcrypt
CryptoDefense	Jigsaw	PadCrypt	WonderCrypter
CryptoFortress	JobCrypter	PClock	Xort
CryptoHasYou	KeRanger	PowerWare	XTBL
CryptoHitman	KEYHolder	Protected	Ransomware
Maktub	Locker	SNSLocker	SuperCrypt
UmbreCrypt	VaultCrypt	Virlocker	

传播方式：（详见见附录一）

服务器入侵传播、利用漏洞自动传播、软件供应链攻击传播、邮件附件传播、利用挂马网页传播

攻击特点：（详见见附录二）

无 C2 服务器加密技术流行、攻击目标转向政企机构、攻击目的开始多样化、勒索软件平台化运营、影响大的家族赎金相对少、境外攻击者多于境内攻击者。

1.7 问题消除

1.病毒清理及加固：

- 安装天擎，对被感染机器进行安全扫描和病毒查杀；
- 对系统进行补丁更新，封堵病毒传播途径；
- 制定严格的口令策略，避免弱口令；
- 结合备份的网站日志对网站应用进行全面代码审计，找出攻击者利用的漏洞入口进行封堵；
- 配合全流量设备（如天眼）对全网中存在的威胁进行分析，排查问题；

2.感染文件恢复：

- 通过奇安信提供的解密工具恢复感染文件；
- 支付赎金进行文件恢复；

3．事件防御：（详见附录三）

个人终端防御技术、企业级终端防御技术。

附录一：勒索病毒传播方式

（一）服务器入侵传播

黑客先通过弱口令、系统或软件漏洞等方式获取用户名和密码，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。

这种攻击方式，一旦服务器被入侵，安全软件一般是不起作用的。

管理员账号密码被破解，是服务器被入侵的主要原因。其中，管理员使用弱密码被黑客暴力破解，部分黑客利用病毒或木马潜伏用户电脑盗取密码，黑客还可从其他渠道直接购买账号密码（这里就涉及到敏感数据泄露问题了。）

（二）利用漏洞自动传播

通过系统自身漏洞进行传播扩散，是 2017 年的一个新特点。WannaCry 勒索病毒就是利用永恒之蓝（EternalBlue）漏洞进行传播。

此类勒索软件在破坏功能上与传统勒索软件无异，都是加密用户文件勒索赎金，但因传播方式不同，更难以防范，需要用户提高安全意识，及时更新有漏洞的软件或安装对应的安全补丁。

（三） 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，利用软件供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，该病毒通过税务软件 M.E.Doc 的升级包投递到内网中进行传播。

（四） 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，一旦用户打开邮件附件，便会执行里面的脚本，释放勒索病毒。

这类传播方式针对性较强，主要瞄准公司企业、各类单位和院校，电脑中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。

（五） 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，没有特定的针对性，中招的受害者多数为“裸奔”用户，未安装任何杀毒软件。

使用了 MS17-010 远程高危漏洞进行自我传播复制

敲诈者通过文件加密方面的编程较为规范，流程符合密码学标准（RSA+AES 加密），很难通过其他手段对勒索文件进行解密。

附录二：勒索病毒攻击特点

(一) 无 C2 服务器加密技术流行

2017 年，我们发现黑客在对文件加密的过程中，一般不再使用 C2 服务器了，也就是说现在的勒索软件加密过程中不需要回传私钥了。

这种技术的加密过程大致如下：

1） 在加密前随机生成新的加密密钥对（非对称公、私钥）

2） 使用该新生成新的公钥对文件进行加密

3） 把新生成的私钥采用黑客预埋的公钥进行加密保存在一个 ID 文件或嵌入在加密文件里

解密过程大致如下：

1） 通过邮件或在线提交的方式，提交 ID 串或加密文件里的加密私钥（该私钥一般黑客会提供工具提取）；

2） 黑客使用保留的预埋公钥对应的私钥解密受害者提交过来的私钥；

3） 把解密私钥或解密工具交付给受害者进行解密。

通过以上过程可以实现每个受害者的解密私钥都不相同，同时可以避免联网回传私钥。这也就意味着不需要联网，勒索病毒也可以对终端完成加密，甚至是在隔离网环境下，依然可以对文件和数据进行加密。显然 ，这种技术是针对采用了各种隔离措施的政企机构所设计的。

(二) 攻击目标转向政企机构

2017 年，勒索软件的攻击进一步聚焦在高利润目标上，其中包括高净值个人、连接设备和企业服务器。特别是针对中小企业网络服务器的攻击急剧增长，已经成为 2017 年勒索软件攻击的一大鲜明特征。据不完全统计，2017 年，约 15%的勒索软件攻击是针对中小企业服务器发起的定向攻击，尤以 Crysis、xtbl、wallet、arena、Cobra 等家族为代表。

客观的说，中小企业往往安全架构单一，相对容易被攻破。同时，勒索软件以企业服务器为攻击目标，往往也更容易获得高额赎金。例如：针对 Linux 服务器的勒索软件 Rrebus，虽然名气不大，却轻松从韩国 Web 托管公司 Nayana 收取了 100 万美元赎金，是震惊全球的永恒之蓝全部收入的 7 倍之多。Nayana 所以屈服，

是因为超 150 台服务器受到攻击，上面托管着 3400 多家中小企业客户的站点。这款勒索病毒的覆盖面有限，韩国几乎是唯一的重灾区。

(三)　针对关键信息基础设施的攻击

以 WannaCry、类 Petya 为代表的勒索软件，则是将关键信息基础设施作为了主要攻击目标，这在以往是从未出现过的严峻情况。关键基础设施为社会生产和居民生活提供公共服务，保证国家或地区社会经济活动正常进行，其一旦被攻击将严重影响人们的日常生活，危害巨大。

(四)　攻击目的开始多样化

顾名思义，勒索软件自然就是要勒索钱财。但这种传统认知已经在 2017 年被打破。以网络破坏、组织破坏为目的的勒索软件已经出现并开始流行。其中最为典型的代表就是类 Petya。与大多数勒索软件攻击不同，类 Petya 的代码不是为了向受害者勒索金钱，而是要摧毁一切。类 Petya 病毒的主要攻击目的就是为了破坏数据而不是获得金钱。此外，以 Spora 为代表的窃密型勒索软件在加密用户文档时，还会窃取用户账号密码和键盘输入等信息，属于功能复合型勒索软件。

这些不仅以“勒索”为目的的“勒索软件”，实际上只是结合了传统勒索软件对文件进行加密的技术方法来实现其数据破坏、信息窃取等其他攻击目的。相比于勒索金钱，这种攻击将给对手带来更大的破坏和更大的威胁。这不仅会引发网络犯罪“商业模式”的新变种，而且会反过来刺激网络保险市场的进一步扩张。

(五)　勒索软件平台化运营

2017 年，勒索软件已经不再是黑客单打独斗的产物，而是做成平台化的上市服务，形成了一个完整的产业链条。在勒索软件服务平台上，勒索软件的核心技术已经直接打包封装好了，小黑客直接购买调用其服务，即可得到一个完整的勒索软件。这种勒索软件的生成模式我们称其为 RaaS 服务，而黑市中一般用“Satan Ransomware（撒旦勒索软件）”来指代由 RaaS 服务生成的勒索软件。

RaaS 服务允许任何犯罪者注册一个帐户，并创建自己定制版本的撒旦勒索软件。一旦勒索软件被创建，那么犯罪分子将决定如何分发勒索软件，而 RaaS 服务平台将处理赎金支付和增加新功能。对于这项服务，RaaS 服务平台的开发者将收取受害者所支付赎金的 30%，购买 RaaS 服务者将获取剩余 70%的赎金。

(六)　境外攻击者多于境内攻击者

2017 年，勒索软件的攻击源头以境外为主。绝大多数的勒索软件攻击者基本都是境外攻击者，国内攻击者较少，而且国内攻击者技术水平也相对较低，制作水平也不高。有些国内攻击者编写的勒索软件程序甚至存在很多漏洞，因此也比较容易被破解。比如：MCR 勒索病毒，我们可以直接获取到密钥从而恢复文件。

附录三：勒索病毒事件防御

一、个人终端防御技术

(一)文档自动备份隔离保护

文档自动备份隔离技术是奇安信独创的一种勒索软件防护技术。这一技术在未来一两年内可能会成为安全软件反勒索技术的标配。

鉴于勒索软件一旦攻击成功往往难以修复，而且具有变种多，更新快，大量采用免杀技术等特点，因此，单纯防范勒索软件感染并不是“万全之策”。但是，无论勒索软件采用何种具体技术，无论是哪一家族的哪一变种，一个基本的共同特点就是会对文档进行篡改。而文档篡改行为具有很多明显的技术特征，通过监测系统中是否存在文档篡改行为，并对可能被篡改的文档加以必要的保护，就可以在相当程度上帮助用户挽回勒索软件攻击的损失。

文档自动备份隔离技术就是在这一技术思想的具体实现，奇安信将其应用于奇安信文档卫士功能模块当中。只要电脑里的文档出现被篡改的情况，它会第一时间把文档自动备份在隔离区保护起来，用户可以随时恢复文件。无论病毒如何变化，只要它有篡改用户文档的行为，就会触发文档自动备份隔离，从而使用户可以免遭勒索，不用支付赎金也能恢复文件。

奇安信文档卫士的自动备份触发条件主要包括亮点：一、开机后第一次修改文档；二、有可疑程序篡改文档。当出现上述两种情况时，文档卫士会默认备份包括 Word、Excel、PowerPoint、PDF 等格式在内的文件，并在备份成功后出现提示信息。用户还可以在设置中选择添加更多需要备份的文件格式。比如电脑里的照片非常重要，就可以把 jpg 等图片格式加入保护范围。

此外，奇安信文档卫士还集合了“文件解密”功能，奇安信安全专家通过对一些勒索软件家族进行逆向分析，成功实现了多种类型的文件解密，如2017年出现的“纵情文件修复敲诈者病毒”等。如有网友电脑已不慎中招，可以尝试通过“文档解密”一键扫描并恢复被病毒加密的文件。

(二)综合性反勒索软件技术

与一般的病毒和木马相比，勒索软件的代码特征和攻击行为都有很大的不同。采用任何单一防范技术都是不可靠的。综合运用各种新型安全技术来防范勒索软件攻击，已经成为一种主流的技术趋势。

下面就以奇安信安全卫士的相关创新功能来分析综合性反勒索软件技术。相关技术主要包括：智能诱捕、行为追踪、智能文件格式分析、数据流分析等，具体如下。

智能诱捕技术是捕获勒索软件的利器，其具体方法是：防护软件在电脑系统的各处设置陷阱文件；当有病毒试图加密文件时，就会首先命中设置的陷阱，从而暴露其攻击行为。这样，安全软件就可以快速无损的发现各类试图加密或破坏文件的恶意程序。

行为追踪技术是云安全与大数据综合运用的一种安全技术。基于奇安信的云安全主动防御体系，通过对程序行为的多维度智能分析，安全软件可以对可疑的文件操作进行备份或内容检测，一旦发现恶意修改则立即阻断并恢复文件内容。该技术主要用于拦截各类文件加密和破坏性攻击，能够主动防御最新出现的勒索病毒。

智能文件格式分析技术是一种防护加速技术，目的是尽可能的降低反勒索功能对用户体验的影响。实际上，几乎所有的反勒索技术都会或多或少的增加安全软件和电脑系统的负担，相关技术能否实用的关键就在于如何尽可能的降低其对系统性能的影响，提升用户体验。奇安信研发的智能文件格式分析技术，可以快速识别数十种常用文档格式，精准识别对文件内容的破坏性操作，而基本不会影响正常文件操作，在确保数据安全的同时又不影响用户体验。

数据流分析技术，是一种将人工智能技术与安全防护技术相结合的新型文档安全保护技术。首先，基于机器学习的方法，我们可以在电脑内部的数据流层面，

分析出勒索软件对文档的读写操作与正常使用文档情况下的读写操作的区别；而这些区别可以用于识别勒索软件攻击行为；从而可以在“第一现场”捕获和过滤勒索软件，避免勒索软件的读写操作实际作用于相关文档，从而实现文档的有效保护。

二、企业级终端防御技术

(一)云端免疫技术

在国内，甚至全球范围内的政企机构中，系统未打补丁或补丁更新不及时的情况都普遍存在。这并非是简单的安全意识问题，而是多种客观因素限制了政企机构对系统设备的补丁管理。因此，对无补丁系统，或补丁更新较慢的系统的安全防护需求，就成为一种“强需求”。而云端免疫技术，就是解决此类问题的有效方法之一。这种技术已经被应用于奇安信的终端安全解决方案之中。

所谓云端免疫，实际上就是通过终端安全管理系统，由云端直接下发免疫策略或补丁，帮助用户电脑做防护或打补丁；对于无法打补丁的电脑终端，免疫工具下发的免疫策略本身也具有较强的定向防护能力，可以阻止特定病毒的入侵；除此之外，云端还可以直接升级本地的免疫库或免疫工具，保护用户的电脑安全。

需要说明的事，云端免疫技术只是一种折中的解决方案，并不是万能的或一劳永逸的，未打补丁系统的安全性仍然比打了补丁的系统的安全性有一定差距。但就当前国内众多政企机构的实际网络环境而诺言，云端免疫不失为一种有效的解决方案。

(二)密码保护技术

针对中小企业网络服务器的攻击，是 2017 年勒索软件攻击的一大特点。而攻击者之所以能够渗透进入企业服务器，绝大多数情况都是因为管理员设置的管理密码为弱密码或帐号密码被盗。因此，加强登陆密码的安全管理，也是一种必要的反勒索技术。

具体来看，加强密码保住主要应从三个方面入手：一是采用弱密码检验技术，强制网络管理员使用复杂密码；二是采用反暴力破解技术，对于陌生 IP 的登陆位置和登陆次数进行严格控制；三是采用 VPN 或双因子认证技术，从而使攻击者即便盗取了管理员帐号和密码，也无法轻易的登陆企业服务器。