勒索病毒应急响应处置手册

目录

勒索病毒，是伴随数字货币兴起的一种新型恶意程序，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加密，并添加一个特殊的后缀，用户无法读取原本的文件，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自行解密，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攻击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恶意程序。常见的 Globelmposter、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、更新频繁、配合人工投毒方式，已经成为政企机构面临的最大的网络威胁之一。

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块，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，因此特整理了常见的勒索病毒种类、特征及常见传播方式，供大家参考了解：

一、WannaCry

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。

常见后缀：wncry

传播方式：永恒之蓝漏洞

勒索特征： 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

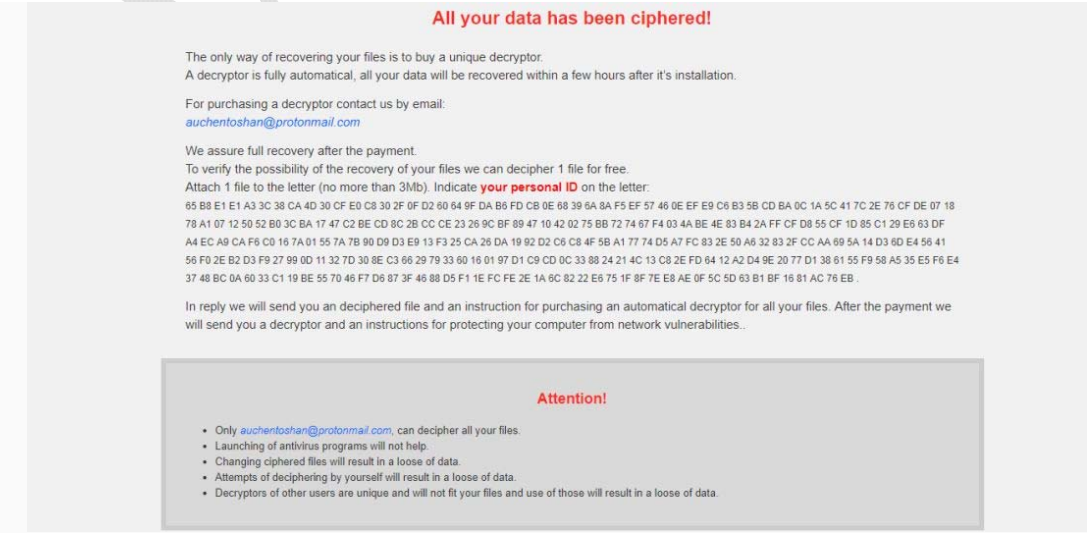
二、GlobeImposter

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。

常见后缀：auchentoshan、十二生肖英文名称+4444

传播方式：RDP 爆破 垃圾邮件 捆绑软件

勒索特征：释放在%appdata%或%localappdata%



三、Crysis/Dharma

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。

常见后缀：【id】+勒索邮箱+特定后缀

传播方式：RDP 爆破

勒索特征：勒索信位置在 startup 目录

样本位置在%windir%\System32

Startup 目录

%appdata%目录

四、GandCrab

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。

常见后缀：随机生成

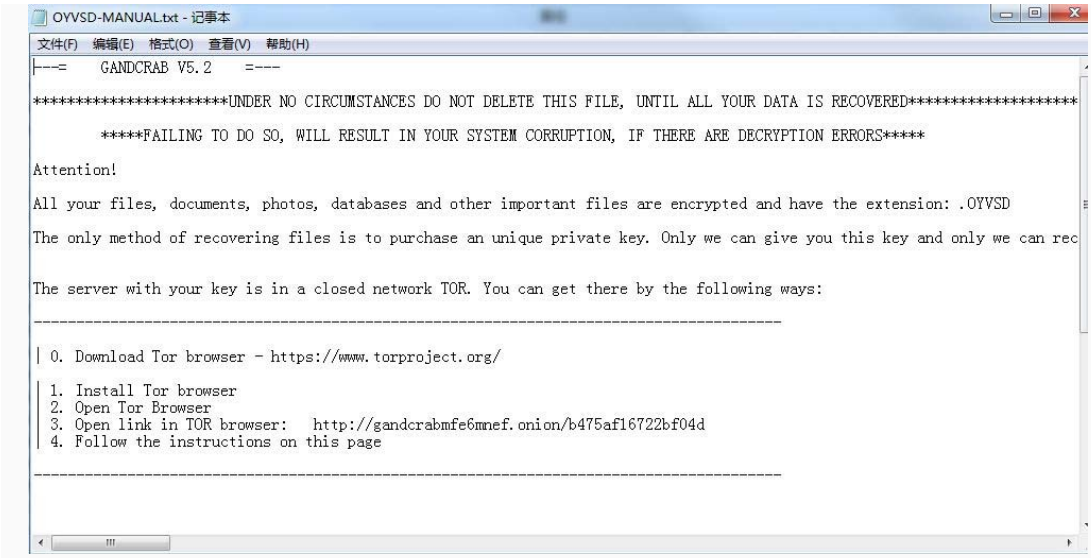
传播方式：RDP 爆破 钓鱼邮件 捆绑软件 僵尸网络 漏洞传播 ……

勒索特征：样本执行完毕后自删除

修改操作系统桌面背景

后缀-MANUAL.txt

后缀-DECRYPT.txt



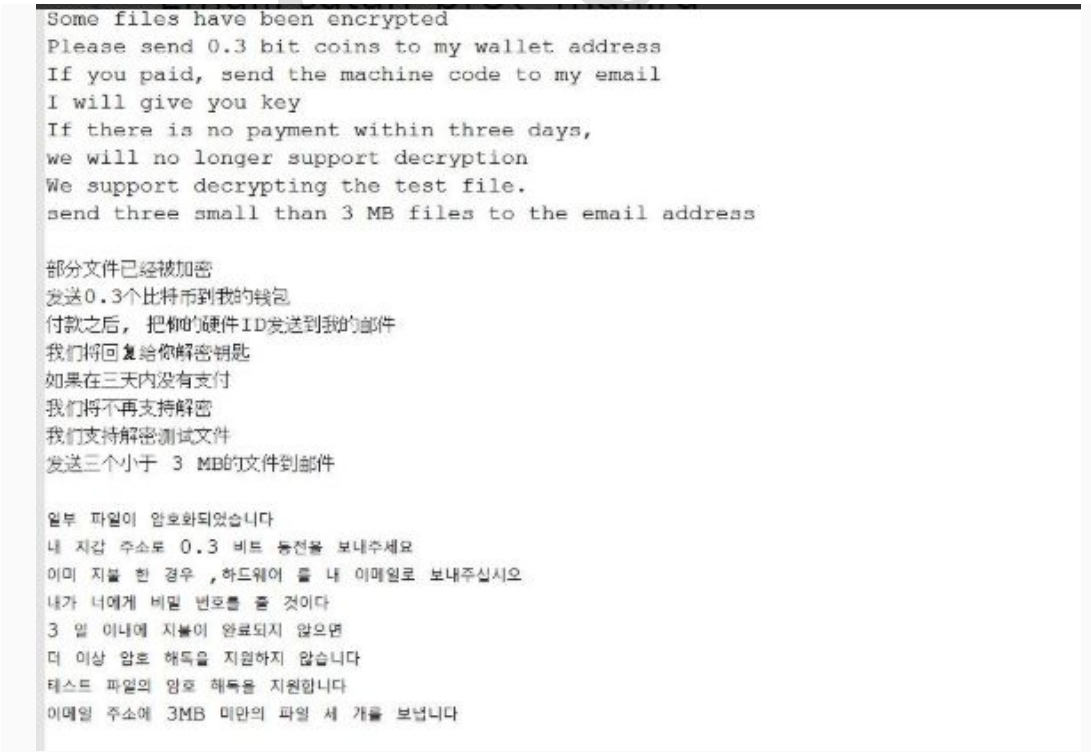
五、Satan

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，还通过多个漏洞传播，详见第六章。

常见后缀：evopro sick …

传播方式：永恒之蓝漏洞 RDP 爆破、JBOSS 系列漏洞、Tomcat 系列漏洞、Weblogic 组件漏洞等

勒索特征：最新变种 evopro 暂时无法解密，老的变种可解密



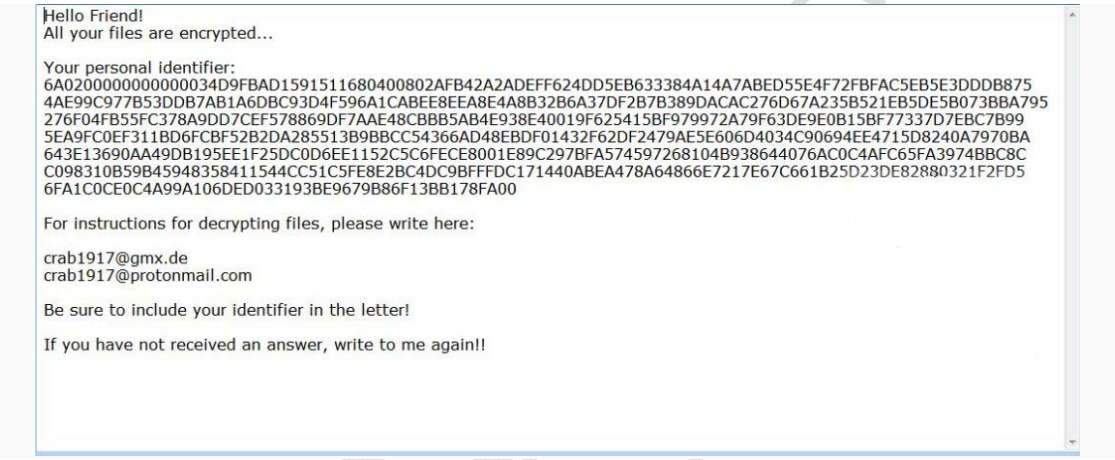
六、Sacrab

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。

常见后缀：.krab .Sacrab .bomber .Crash ……

传播方式：Necurs 僵尸网络 RDP 爆破 垃圾邮件 ……

勒索特征：样本释放%appdata%\Roaming

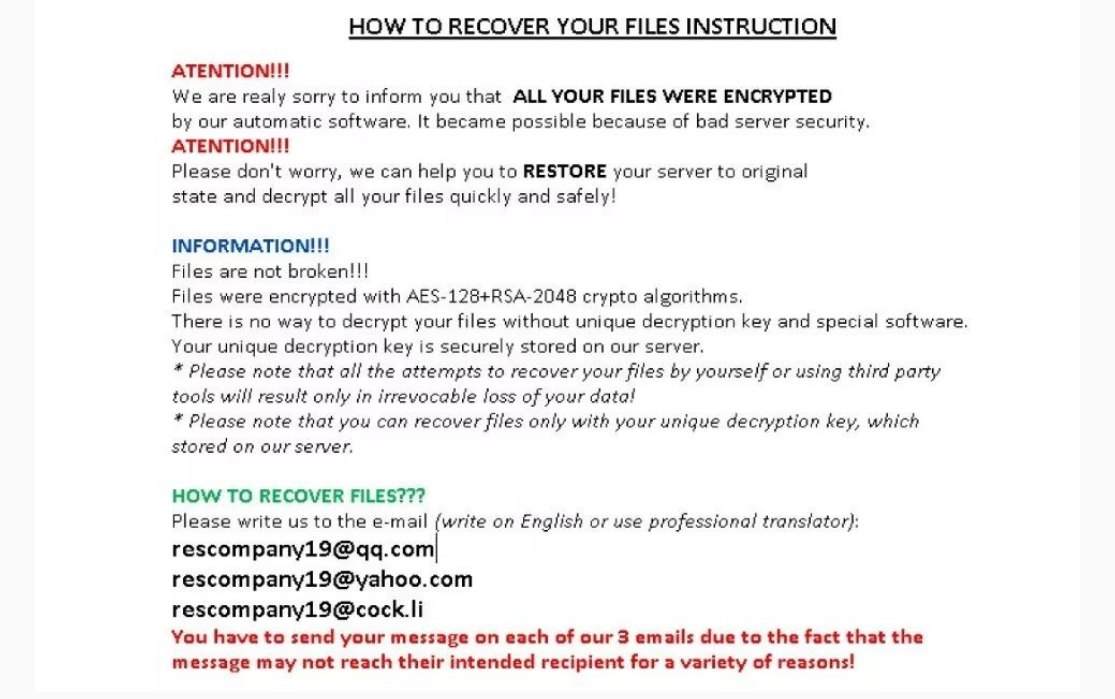


七、Matrix

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。

常见后缀：.GRHAN .PRCP .SPCT .PEDANT …

传播方式：RDP 爆破



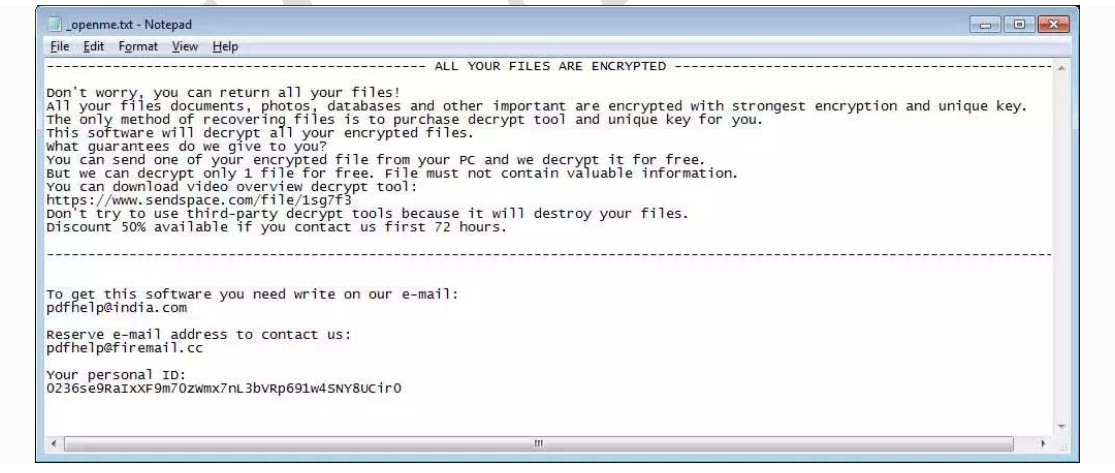
八、STOP

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。

常见后缀：.TRO .djvu .puma .pumas .pumax .djvuq …

勒索特征：样本释放在%appdata%\local\<随机名称>

可能会执行计划任务

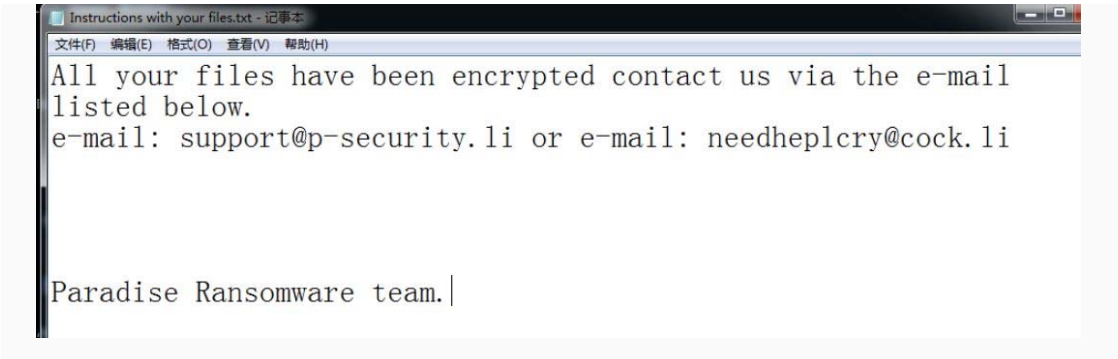


九、Paradise

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



加密文件后缀：文件名_%ID 字符串%_{勒索邮箱}.特定后缀

勒索特征：将勒索弹窗和自身释放到 Startup 启动目录

十、Phobos

Phobos 勒索病毒复用了 Crysis 的部分代码，与 Crysis 高度相似(文件后缀与勒索信)，该勒索病毒多通过 RDP 弱口令进行传播，使用 RSA+AES 算法加密文件，在没有相应 RSA 私钥的情况下无法解密。

传播方式：RDP 弱口令

勒索特征：勒索信名称为"info.txt"、"info.hta"

常见后缀：.Banta、.phobos、.actin、.PISCA、. caleb…

十一、Sodinokibi

该勒索病毒继承了部分 GandCrab 勒索病毒的代码与传播渠道，在 GandCrab 停止运营后，此勒索病毒活跃度逐渐提升。该勒索多通过 RDP 弱口令、钓鱼邮件、Oracle WebLogic CVE-2019-2725 漏洞进行传播，其中钓鱼邮件多伪装成海关、公安、法院、DHL 快递等内容。

该病毒使用 Salsa20 算法加密文件，在文件加密结束后，会修改桌面壁纸为蓝色，并提示您文件已被加密，阅读勒索信。目前无法解密。

传播方式

RDP 弱口令、钓鱼邮件、Oracle WebLogic CVE-2019-2725 漏洞

勒索特征

勒索信名称为"随机字符-readme.txt"

常见后缀

被加密文件后缀为 5-10 个随机字符

十二、RYUK

Ryuk 勒索病毒最早在 2018 年 8 月由国外某安全公司发现并报道，此勒索病毒多根据企业规模进行定制性攻击，攻击目标多为大型企业与政府机构，攻击成功后索要赎金数额巨大。该勒索使用 RSA+AES 算法对文件进行加密，在没有相应 RSA 私钥的情况下无法解密。

传播方式

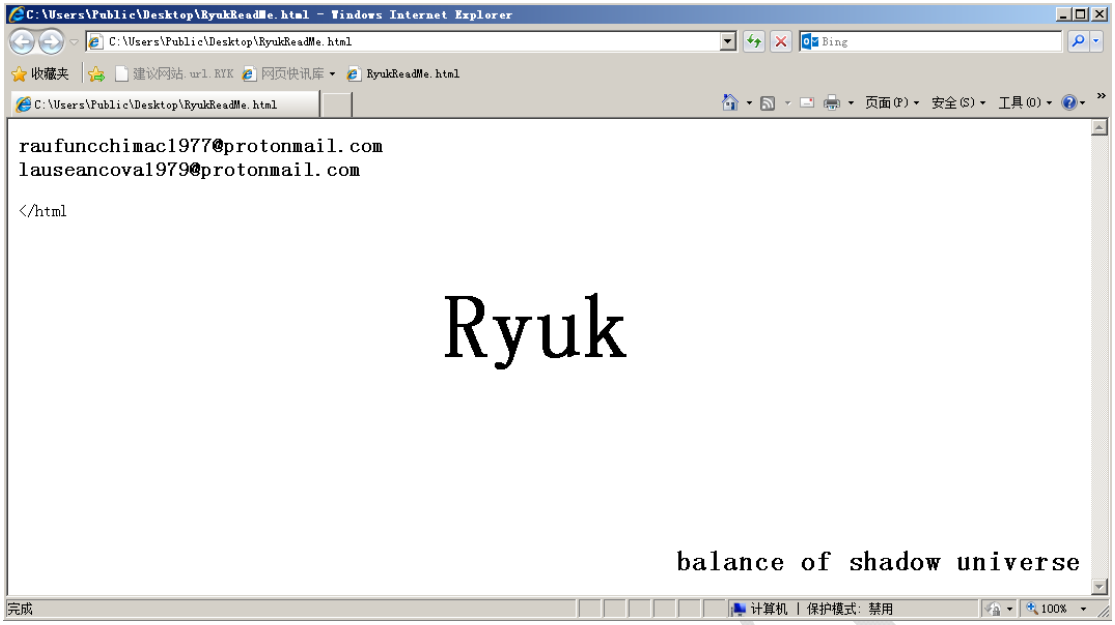
垃圾邮件或漏洞利用工具包、Trickbot 银行木马

勒索特征

勒索信名称多为"RyukReadMe.html"或"RyukReadMe.txt"

常见后缀

.ryk



十三、MedusaLocker

MedusaLocker 勒索早期勒索信与 GlobeImposter 非常相似，曾被认为是 GlobeImposter 的变种。该勒索病毒使用 RSA+AES 算法对文件进行加密，在没有相应 RSA 私钥的情况下无法解密。

传播方式

RDP 弱口令

勒索特征

勒索信名称为："RECOVER_INSTRUCTIONS.html"、"INSTRUCTIONS.html"

常见后缀

".ReadTheInstructions"，".READINSTRUCTIONS"

十四、CryptON

CryptON 勒索，又名 X3M、Cry9 等等，该勒索多通过 RDP 弱口令进行传播，使用 3DES 和 RC4 算法加密文件，因加密后，密钥文件会保存在本地(temp000000.txt)，所以该勒索可以解密。但目前发现的用户现场内，该文件多被黑客取走，导致无法解密。

传播方式

RDP 弱口令

勒索特征

勒索信名称为"!!!DECRYPT MY FILES!!!.txt"、"_RESTORE FILES_.txt"

常见后缀

"X3M"

"firex3m"

"WECANHELP"

"YOU_LAST_CHANCE"

```
*** ALL YOUR WORK AND PERSONAL FILES HAVE BEEN ENCRYPTED ***

To decrypt your files you need to buy the special software ?"Nemesis
decryptor"
You can find out the details/buy decryptor + key/ask questions by email:
wecanhelpyou@elude.in, w3canh3lpy0u@cock.li OR wecanh3lpyou2@cock.li

IMPORTANT!
DON'T TRY TO RESTORE YOU FILES BY YOUR SELF, YOU CAN DAMAGE FILES!
If within 24 hours you did not receive an answer by email, be sure to write
to Jabber: icanhelp@xmpp.jp


Your personal ID: 2102102989
```

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

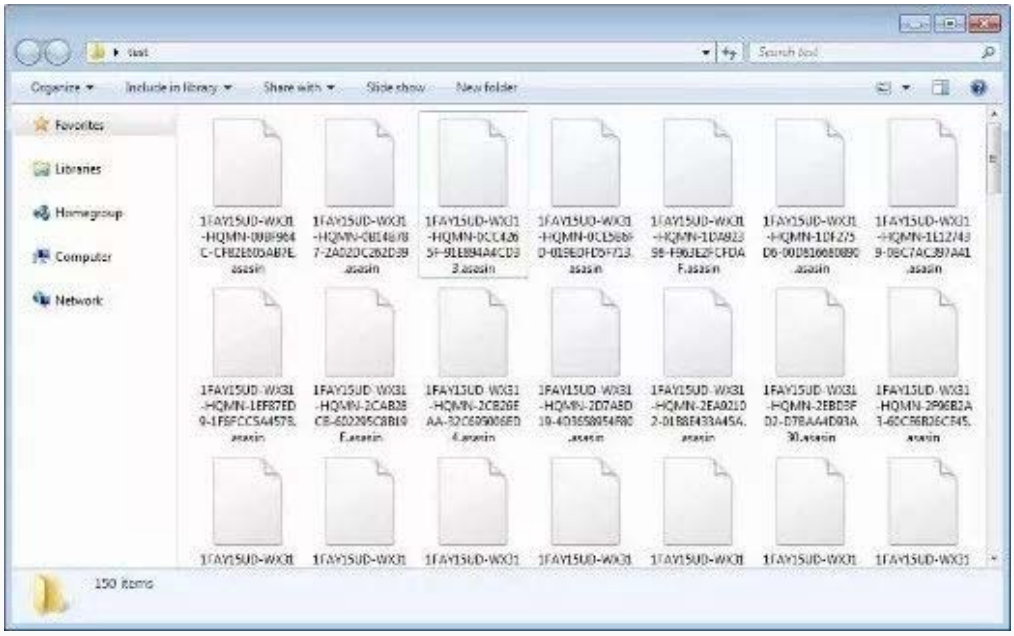
服务器被感染勒索病毒后，最明显的特征是电脑桌面发生明显变化，即：桌面通常会出现新的文本文件或网页文件，这些文件用来说明如何解密的信息，同时桌面上显示勒索提示信息及解密联系方式，通常提示信息英文较多，中文提示信息较少。

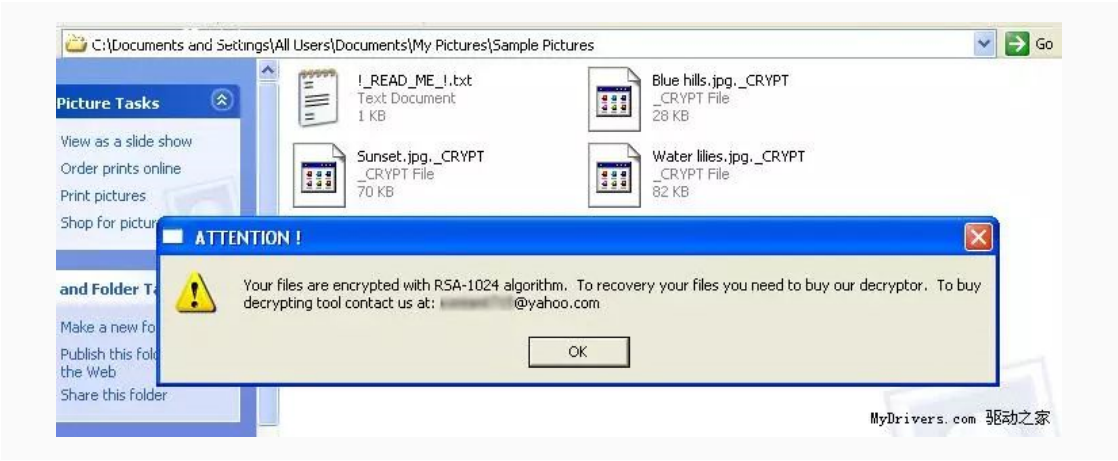
下面为电脑感染勒索病毒后，几种典型的桌面发生变化的示意图。

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、如何进行处置

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

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。

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。

一、历史备份还原

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。

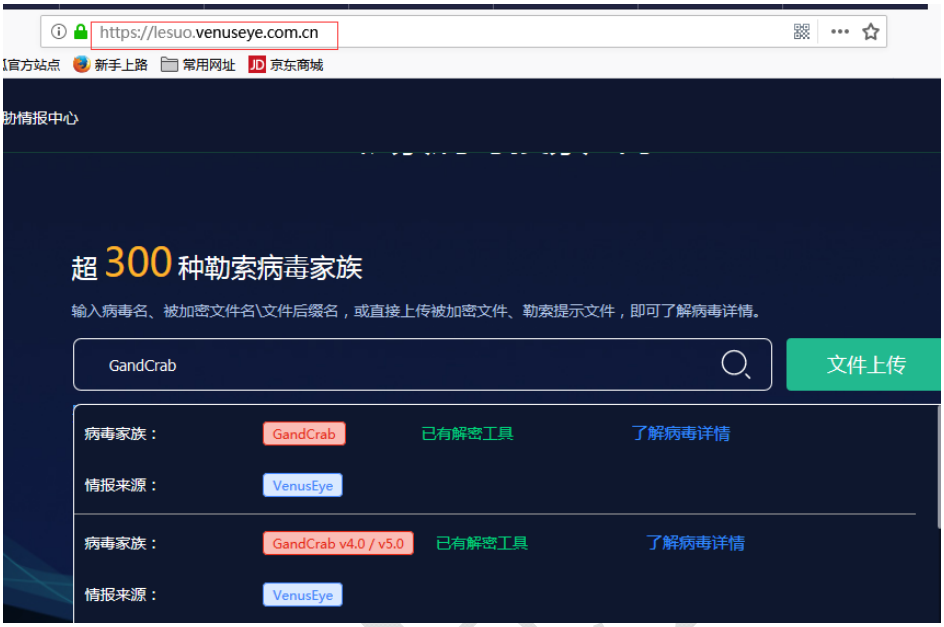
但是，对于以下三种情况，可以通过解密工具恢复感染文件。

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。

可以通过网站（https://lesuo.venuseye.com.cn/）查询哪些勒索病毒可以解密。例如：大规模流行的 GandCrab 家族勒索病毒，GandCrabV5.1 及以前的版本可以下载解密工具进行解密。



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

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。

安全源自未雨绸缪，诚信贵在风雨同舟

第五章、如何加强防护

面对屡屡爆发的勒索攻击，启明星辰推出“云端感知，网端检测，终端防护，系统加固“的立体解决方案。

一、“云”端感知

在“云”端，VenusEye 威胁情报中心监测全球勒索病毒态势，推出汇集了超 300 种勒索病毒家族的搜索引擎（lesuo.venuseye.com.cn）。用户可使用勒索病毒名，加密文件名等查询到这些勒索病毒的情报信息，并获得相关的解决方案及处置建议。

二、“网”端检测

在“网”端可以部署：

天镜脆弱性扫描与管理系统对包含勒索病毒利用漏洞的资产进行检测；

天阗高级持续性威胁检测与管理系统对网络中的未知勒索病毒进行检测；

天清邮件安全管理系统对邮件中的勒索病毒进行精准拦截；

天阗入侵检测与管理系统，天清入侵防御系统斩断勒索病毒的传播途径。

1.通过部署天镜脆弱性扫描和管理系统，确认如下的扫描策略已经升级下发，并使用该策略进行勒索病毒利用漏洞的资产扫描：

（1）通过 SMB 和 RDP 漏洞进行传播的支持方法：

传播方式	扫描策略名称
漏洞传播	windows 中常见勒索软件使用漏洞策略

策略名称如下：

windows中常见勒索软件使用漏洞策略	默认策略	99	41	14	8	是

策略包含的 SMB 漏洞如下：

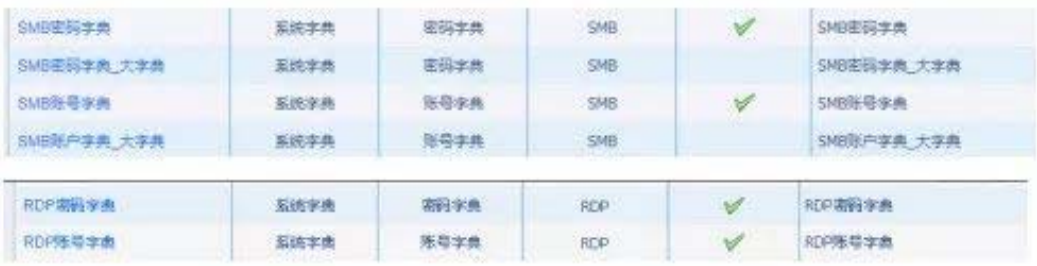
策略包含的 RDP 漏洞如下：

（2）通过 SMB 和 RDP 弱口令进行传播的支持方法：

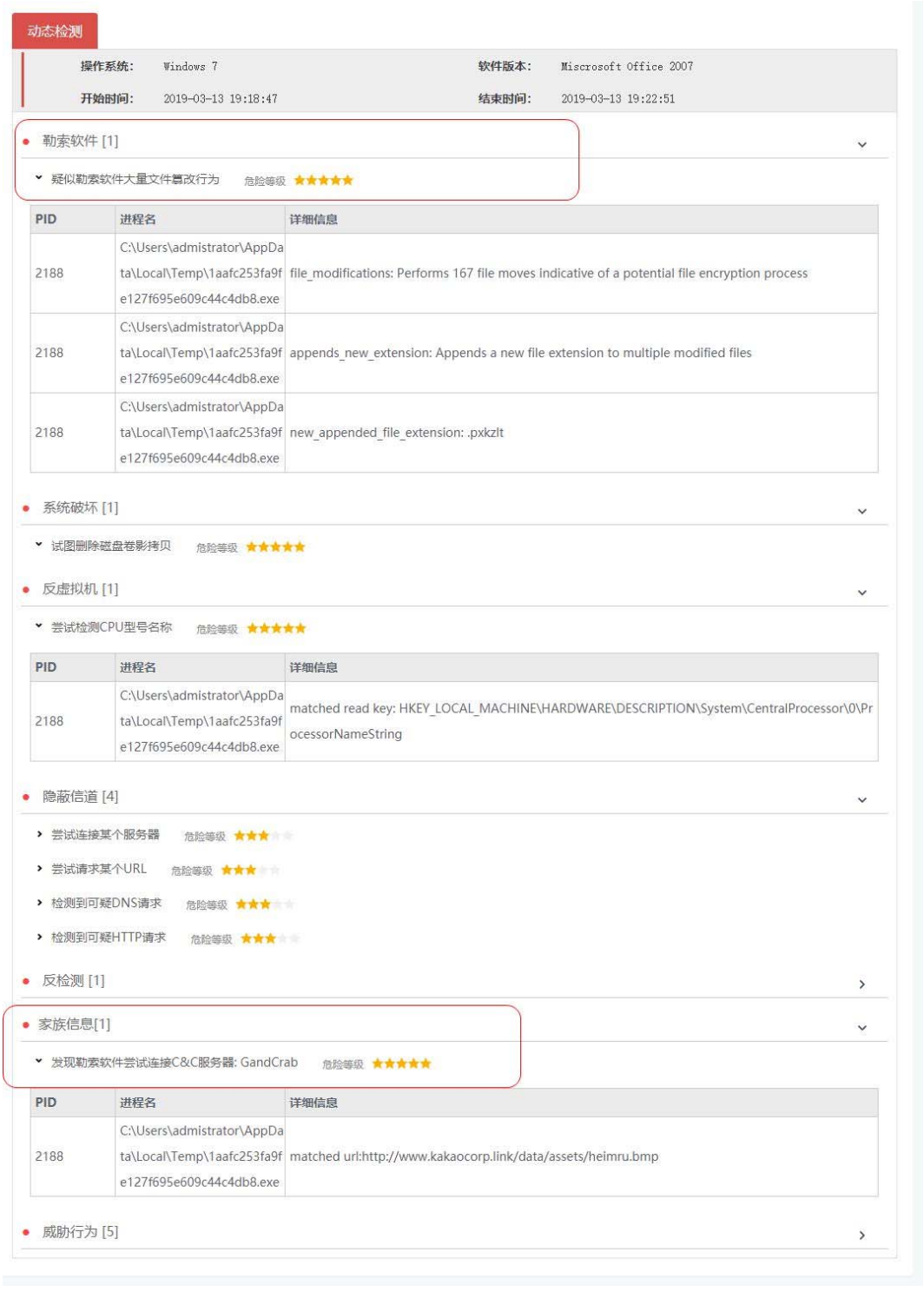
传播方式	扫描方式
弱口令传播	下发弱口令扫描任务

下发弱口令扫描任务，选中，SMB 和 RDP：

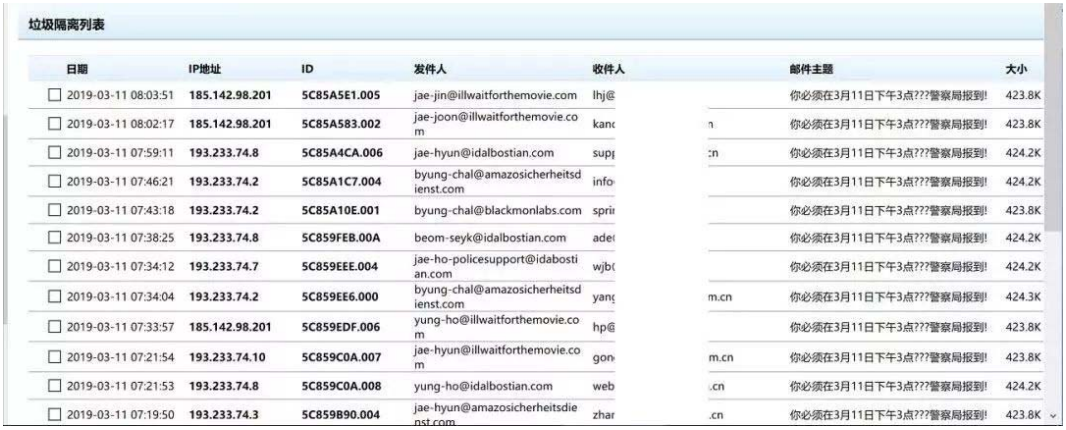
使用最新的勒索病毒弱口令：



2.通过部署天阗高级持续性威胁检测与管理系统，无需升级即可有效检测流量中的未知勒索病毒。



3.通过部署天清邮件安全管理系统，精准发现通过邮件传播的勒索病毒。



4. 通过部署天阗入侵检测与管理系统、天清入侵防御系统，并确认如下事件已经下发，即可有效检测、阻断勒索病毒通过弱口令以及漏洞进行传播。

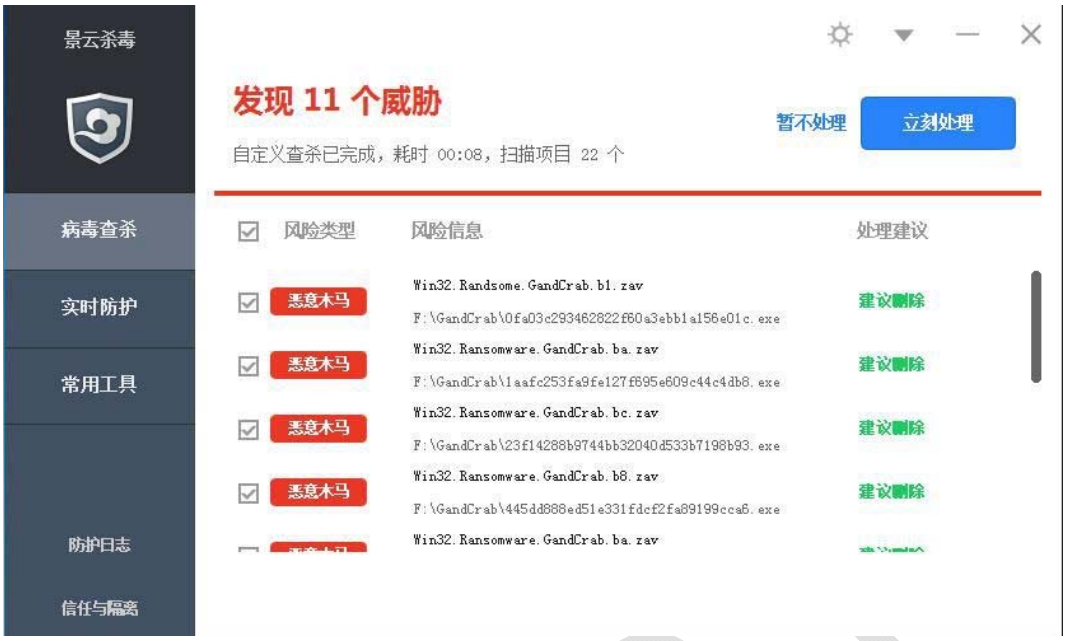
传播方式	事件名
弱口令传播	TCP_RDP 远程桌面登录口令穷举
	SMB_共享口令穷举探测
	SMB_登录失败
漏洞传播	TCP_NSA_Windows_SMB_DoublePulsar 植入成功[CVE-2017-0143]
	TCP_NSA_Windows_SMB_Pcdllluancher 工具执行成功
	TCP_NSA_SMB 远程代码执行漏洞 shellcode 植入
	TCP_NSA_MS17-010 漏洞工具扫描
	TCP_NSA_EternalRomance_(永恒浪漫)_SMB 远程代码执行漏洞[MS17-010]
	TCP_NSA_EternalBlue_(永恒之蓝)_SMB 远程代码执行漏洞 1[CVE-2017-0144/0147]
	TCP_NSA_EternalBlue_(永恒之蓝)_SMB 远程代码执行漏洞_shellcode 植入
	TCP_NSA_EternalBlue_(永恒之蓝)_SMB 远程代码执行漏洞[MS17-010][CVE-2017-0144/0147]
	TCP_NSA_EternalBlue_(永恒之蓝)_SMB 漏洞利用(win8.1/2012-x64)
	TCP_NSA_EternalBlue_(永恒之蓝)_SMB 漏洞利用(win7/2008-x64)
	TCP_NSA_EsteemAudit_(尊重审查)_Windows_RDP 远程代码执行漏洞[CVE-2017-9073]
勒索病毒	HTTP_GandCrab_5.2 勒索病毒_连接
	HTTP_勒索软件_GandCrab_v4

提示：当发现上述弱口令事件且源 IP 地址属于非白名单 IP 时，则风险更大。

三、“终端”防护

在终端/服务器可以部署具备完善勒索病毒防护体系的景云网络防病毒系统，形成勒索病毒的最后一道防线。

1.病毒检测与实时监控功能可以有效检测出已知勒索病毒。



2.开启 U 盘防护功能，可以拦截通过移动存储介质传播的勒索病毒。

3.日常使用补丁扫描功能，及时修补各种系统补丁，防止勒索病毒通过系统漏洞进入。

4.景云还具有基于多步行为序列分析引擎实现的反勒索防护系统，实现勒索病毒的事前防御、事中监控拦截、事后恢复全套的闭环的三重纵深防护。

四、系统加固

在有效部署各种安全产品的同时，还应该对系统进行全方位加固，以确保万无一失。

1. 尽量关闭不必要的服务和端口。如：135，139，445 端口，对于远程桌面服务（3389），VNC 服务需要进行白名单设置，仅允许白名单内的 IP 登陆。

2. 禁用 GUEST 来宾用户。尽量不要使用局域网共享，或把共享磁盘设置为只读属性，不允许局域网用户改写文件。

3. 采用不少于 10 位的高强度密码，并定期更换密码。
4. 及时更新系统，给系统打补丁，修补漏洞。
5. 定期对重要文件以及数据库做非本地备份。
6. 不点击来源不明的邮件以及附件，切断勒索病毒的邮件传播方式。

第六章、勒索病毒已知被利用漏洞列表

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

联系我们

010-82779088 北京市中关村软件园 21 号楼 www.venustech.com.cn