Day165　应急响应-勒索病毒检测指南&Win&Linux样本演示&家族识别&分析解密

蓝队应急-小迪安全

异常特征

- 主机安全
  - CPU满负载
  - 服务器莫名重启
  - 其它
- 网站安全
  - 被植入暗链
  - 出现Webshell
  - 网页文件被篡改
  - 其它
- 流量安全
  - 网络阻塞
  - 网络异常
  - 其它
- 数据安全
  - 泄露
  - 篡改
- 文件安全
  - 丢失
  - 异常
- 设备告警
  - 防火墙
  - 杀毒软件
  - 感知平台
  - 检测系统
  - 其它

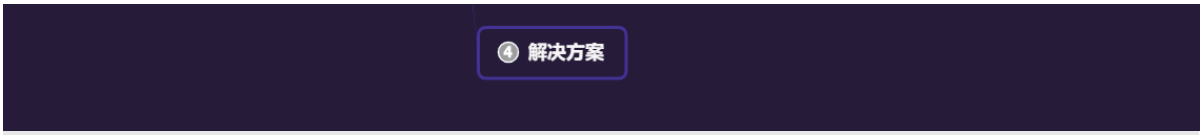
处置流程

1. 准备阶段
   - 获取事件信息
   - 准备设备工具
2. 保护阶段
   - 断网
   - 备份
   - 数据恢复
   - 物理隔离
3. 检测阶段
   - 技术分析
4. 取证阶段
   - 确定攻击事件
   - 确定攻击时间
   - 确定攻击过程
   - 确定攻击对象
5. 处置阶段
   - 提出安全问题
   - 提出解决方案
   - 业务恢复
6. 总结阶段
   - 完整事件报告编写

问题排查

- 系统
  - Windows
    - 远控后门
      - 进程
      - 网络
    - 勒索病毒
      - 表现
    - 挖矿程序
      - 进程
      - 网络
    - 爆破攻击
      - 系统日志
    - DDOS攻击
      - 网络流量
      - CPU爆满
  - Linux
- Web
  - 源码
  - 数据库
  - 中间件
- 其他

工具平台



1.知识点

- 1、勒索病毒危害影响?
- 2、勒索病毒怎么传播的?
- 3、勒索病毒有哪些家族?
- 4、勒索病毒如何进行处置?

2.内容点

```
应急响应：
1、抗拒绝服务攻击防范应对指南
2、勒索软件防范应对指南
3、钓鱼邮件攻击防范应对指南
4、网页篡改与后门攻击防范应对指南
5、网络安全漏洞防范应对指南
6、大规模数据泄露防范应对指南
7、僵尸网络感染防范应对指南
8、APT攻击入侵防范应对指南
9、各种辅助类分析工具项目使用
```

```
朔源反制：
威胁情报，信息库追踪，设备反制，IDS&IPS等反制，工具漏洞反制，蜜罐钓鱼反制等
```

```
威胁情报相关平台：
Virustotal
深信服威胁情报中心
微步在线
venuseye
安恒威胁情报中心
360威胁情报中心
绿盟威胁情报中心
AlienVault
RedQueen安全智能服务平台
IBM X-Force Exchange
ThreatMiner
```

3.演示案例

1、什么是勒索病毒？

勒索病毒是一种新型电脑病毒，主要以RDP爆破、邮件、程序木马、网页挂马的形式进行传播。该病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。这种病毒利用各种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。2019年末，勒索已然呈现出“双重勒索”的趋势，即先窃取商业数据，然后实施勒索，如果未能在规定时间内支付赎金，将于网上（通常暗网）公开售卖企业的商业数据。

2、勒索病毒危害影响？

（1）系统瞬时CPU占用高，接近100%，这个现象主要是在批量加密文件。

（2）所有应用都被无法使用和打开。

（3）系统应用文档被加密无法修改。

（4）文件后缀被修改并留下勒索信。

（5）桌面主题被修改。

（6）杀毒软件告警。（可能你并不懂告警了CrySiS是什么东西）

3、勒索病毒怎么传播的？

见上图

4、勒索病毒常见家族及确定？

（1）LockBit：LockBit于 2019 年 9 月首次以 ABCD勒索软件的形式出现，2021年发布2.0版本，相比第一代，LockBit 2.0号称是世界上最快的加密软件，加密100GB的文件仅需4分半钟。经过多次改进成为当今最多产的勒索软件系列之一。LockBi使用勒索软件即服务 (RaaS)模型，并不断构思新方法以保持领先于竞争对手。它的双重勒索方法也给受害者增加了更大的压力（加密和窃取数据），据作者介绍和情报显示LockBi3.0版本已经诞生，并且成功地勒索了很多企业。

3 （2）Gandcrab/Sodinokibi/REvil：REvil勒索软件操作，又名Sodinokibi，是一家臭名昭著的勒索软件即服务 (RaaS) 运营商，可能位于独联体国家（假装不是老毛子）。它于 2019 年作为现已解散的 GandCrab 勒索软件的继任者出现，并且是暗网上最多产的勒索软件之一，其附属机构已将目标锁定全球数千家技术公司、托管服务提供商和零售商,一直保持着60家合作商的模式。（2021年暂停止运营，抓了一部分散播者）。

4 （3）Dharma/CrySiS/Phobos：Dharma勒索软件最早在 2016 年初被发现， 其传播方式主要为 RDP 暴力破解和钓鱼邮件，经研究发现 Phobos勒索软件、CrySiS勒索软件与 Dharma勒索软件有 许多相似之处，故怀疑这几款勒索软件的 作者可能是同一组织。

5 （4）Globelmposter（十二生肖）：Globelmposter又名十二生肖，十二主神，十二.....他于2017年开始活跃，2019年前后开始对勒索程序进行了大的改版变更。攻击者具有一定的地域划分，比如国内最常见的一个攻击者邮箱为 China.Helper@aol.com

6 （5）WannaRen（已公开私钥）：WannaRen勒索家族的攻击报道最早于2020年4月，通过下载站进行传播，最终在受害者主机上运行，并加密几乎所有文件；同时屏幕会显示带有勒索信息的窗口，要求受害者支付赎金，但WannaRen始终未获得其要求的赎金金额，并于几天后公开密钥。

7 （6）Conti：Conti勒索家族的攻击最早追踪到2019年，作为“勒索软件即服务（RaaS）”，其幕后运营团伙管理着恶意软件和Tor站点，然后通过招募合作伙伴执行网络漏洞和加密设备。在近期，因为分赃不均，合作伙伴多次反水，直接爆料攻击工具、教学视频、以及部分源代码。

8 （7）WannaCry：WannaCry（又叫Wanna Decryptor），一种“蠕虫式”的勒索病毒软件，由不法分子利用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，WannaCry的出现也为勒索病毒开启了新的篇章。

（8）其他家族：当然，勒索病毒的家族远远不止如此。

人工分析：
（1）通过加密格式来判断
（2）通过桌面的形式来判断
（3）通过勒索者的邮箱来判断家族
（4）通过勒索者留下的勒索信为例
（5）通过微步云沙箱/威胁情报/暗网论坛
平台分析：
勒索病毒搜索引擎
360：http://lesuobingdu.360.cn
腾讯：https://guanjia.qq.com/pr/ls
启明：https://lesuo.venuseye.com.cn
奇安信：https://lesuobingdu.qianxin.com
深信服：https://edr.sangfor.com.cn/#/information/ransom_search

勒索软件解密工具集
腾讯哈勃：https://habo.qq.com/tool
金山毒霸：http://www.duba.net/dbt/wannacry.html
火绒：http://bbs.huorong.cn/forum-55-1.html
瑞星：http://it.rising.com.cn/fanglesuo/index.html
Nomoreransom：https://www.nomoreransom.org/zh/index.html
MalwareHunterTeam：https://id-ransomware.malwarehunterteam.com
卡巴斯基：https://noransom.kaspersky.com
Avast：https://www.avast.com/zh-cn/ransomware-decryption-tools

```
Emsisoft：https://www.emsisoft.com/ransomware-decryption-tools/free-download
Github勒索病毒解密工具收集汇总：https://github.com/jiansiting/Decryption-Tools
```

```
5、勒索病毒有常见处置？
-淘宝、闲鱼找专业人做
-Github公开工具资源搜
-各类安全公司及杀毒平台
勒索病毒搜索引擎
360：http://lesuobingdu.360.cn
腾讯：https://guanjia.qq.com/pr/ls
启明：https://lesuo.venuseye.com.cn
奇安信：https://lesuobingdu.qianxin.com
深信服：https://edr.sangfor.com.cn/#/information/ransom_search

勒索软件解密工具集
腾讯哈勃：https://habo.qq.com/tool
金山毒霸：http://www.duba.net/dbt/wannacry.html
火绒：http://bbs.huorong.cn/forum-55-1.html
瑞星：http://it.rising.com.cn/fanglesuo/index.html
Nomoreransom：https://www.nomoreransom.org/zh/index.html
MalwareHunterTeam：https://id-ransomware.malwarehunterteam.com
卡巴斯基：https://noransom.kaspersky.com
Avast：https://www.avast.com/zh-cn/ransomware-decryption-tools
```

Emsisoft：https://www.emsisoft.com/ransomware-decryption-tools/free-download
Github勒索病毒解密工具收集汇总：https://github.com/jiansiting/Decryption-Tools

附录目前国内外收集的工具：
1、【Bitdefender】REvil/Sodinokibi 勒索病毒通用解密工具
http://www.bitdefender-cn.com/downloads/tool/BDREvilDecryptor.zip
2、【腾讯】Petya解密工具
https://habo.qq.com/tool/detail/petya
3、【腾讯】TeslaCrypt解密工具
https://habo.qq.com/tool/detail/teslacrypt
4、【腾讯】Allcry解密工具
https://habo.qq.com/tool/detail/allcrykiller
5、【腾讯】XData解密工具
https://habo.qq.com/tool/detail/xdatacrack
6、【腾讯】WannaCry解密工具
https://habo.qq.com/tool/detail/searchdky
7、【腾讯】哈勃勒索病毒解密助手
https://habo.qq.com/tool/detail/ransomware_recovery_tools
8、【火绒】GandCrab勒索病毒专用解密工具
https://bbs.huorong.cn/thread-55035-1-1.html
9、【Bitdefender】GandCrab勒索病毒解密工具-GandCrab v5.1
https://bbs.kafan.cn/thread-2143312-1-1.html
10、【火绒】Bcrypt专用解密工具
https://bbs.huorong.cn/thread-52034-1-1.html
11、【火绒】Aurora勒索病毒专用解密工具
https://bbs.huorong.cn/thread-56687-1-1.html

12、【EmsiSoft】 Decryptor解密工具
https://www.emsisoft.com/ransomware-decryption-tools/
13、【金山】UNNAMED1989勒索病毒
http://bbs.duba.net/thread-23530814-1-1.html
14、【ESET】Crysis 勒索解密工具
https://support.eset.com/en/kb6274-clean-a-crysis-or-wallet-infection-using-the-eset-crysis-decryptor?locale=en_US&viewlocale=en_US
15、【瑞星】CryptON 勒索解密工具
http://it.rising.com.cn/dongtai/19600.html
16、【瑞星】Satan 勒索解密工具
http://bbs.ikaka.com/showtopic-9353573.aspx
17、【腾讯】FBI敲诈专杀工具
https://habo.qq.com/tool/detail/fbi
18、【腾讯】勒索软件专杀工具
https://habo.qq.com/tool/detail/ransomwarekill

✒[Apocalypse勒索软件解密工具]
https://www.pcrisk.com/removal-guides/10111-apocalypse-ransomware
✒[Alcatrazlocker勒索软件解密工具]
https://files.avast.com/files/decryptor/avast_decryptor_alcatrazlocker.exe
✒[Alma勒索软件解密工具]
https://info.phishlabs.com/blog/alma-ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter
✒[Alpha勒索软件解密工具]
https://dl.360safe.com/Decryptor_AlphaDecrypter.cab
✒[AL-Namrood勒索软件解密工具]

https://www.pcrisk.com/removal-guides/10535-al-namrood-ransomware

✎[Apocalypse 勒索病毒解密工具]

http://blog.emsisoft.com/2016/06/29/apocalypse-ransomware-which-targets-companies-through-insecure-rdp/

✎[Autolocky勒索软件解密工具]

https://www.bleepingcomputer.com/news/security/decrypted-the-new-autolocky-ransomware-fails-to-impersonate-locky/

✎[Bart勒索病毒解密工具]

http://phishme.com/rockloader-downloading-new-ransomware-bart/

✎[BitDtak勒索软件解密工具]

https://download.bleepingcomputer.com/demonslay335/BitStakDecrypter.zip

✎[BarRax勒索软件解密工具]

https://blog.checkpoint.com/wp-content/uploads/2017/03/BarRaxDecryptor.zip

✎[CryptON 勒索病毒解密工具]

http://blog.emsisoft.com/2017/03/07/emsisoft-releases-free-decrypter-for-crypton-ransomware/

✎[CoinVault勒索软件解密工具]

https://www.bleepingcomputer.com/virus-removal/coinvault-ransomware-information

✎[CryptXXX勒索病毒解密工具]

http://www.bleepingcomputer.com/virus-removal/cryptxxx-ransomware-help-information

✎[Crypt0勒索软件解密工具]

https://download.bleepingcomputer.com/demonslay335/Crypt0Decrypter.zip

```
https://www.pcrisk.com/removal-guides/10478-crypt0-ransomware
✎[Crypt38Keygen勒索软件解密工具]
https://download.bleepingcomputer.com/demonslay335/Crypt38Keygen.zip
✎[Crypren勒索软件解密工具]
https://github.com/pekeinfo/DecryptCrypren
http://www.nyxbone.com/malware/Crypren.html
✎[CryptComsole勒索软件解密工具]
https://download.bleepingcomputer.com/demonslay335/CryptConsoleDecrypter.zip
✎[Crytomix勒索软件解密工具]
https://files.avast.com/files/decryptor/avast_decryptor_cryptomix.exe
✎[CryptoHostKeygen勒索软件解密工具]
https://github.com/Demonslay335/CryptoHostKeygen
✎[Cry9勒索软件解密工具]
https://www.pcrisk.com/removal-guides/11199-cry9-ransomware
http://blog.emsisoft.com/2017/04/04/remove-cry9-ransomware-with-emsisofts-free-decrypter/
✎[CoinVault勒索软件解密工具]
https://www.nomoreransom.org/uploads/CoinVaultDecryptor.zip
✎[Cryptinfinite勒索软件解密工具]
https://www.pcrisk.com/removal-guides/9568-cryptinfinite-ransomware
✎[CrazyCrypt勒索密钥生成工具]
https://edr.sangfor.com.cn/file/tool/CrazyCrypt_Password.rar
✎[DXXD勒索病毒解密工具]
```

```
http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/
✎[DoNotOpen勒索软件解密工具]
https://download.bleepingcomputer.com/demonslay335/DoNotOpenDecrypter.zip
✎[Decrypt Protect[mbl advisory]勒索病毒解密工具]
http://www.malwareremovalguides.info/decrypt-files-with-decrypt_mblblock-exe-decrypt-protect/
✎[Enigma勒索软件解密工具]
https://www.im-infected.com/ransomware/remove-enigma-ransomware-virus-removal.html
✎[EduCrypt勒索软件解密工具]
https://www.bleepingcomputer.com/news/security/the-educrypt-ransomware-tries-to-teach-you-a-lesson/
✎[GhostCrypt勒索病毒解密工具]
http://www.bleepingcomputer.com/forums/t/614197/ghostcrypt-z81928819-help-support-topic-read-this-filetxt/
✎[GhostCrypt勒索软件解密工具]
https://download.bleepingcomputer.com/demonslay335/GhostCryptDecrypter.zip
✎[Gomasom勒索软件解密工具]
https://www.bleepingcomputer.com/news/security/gomasom-crypt-ransomware-decrypted/
✎[GandCrab勒索软件解密工具]
https://www.bleepingcomputer.com/news/security/fbi-releases-master-decryption-keys-for-gandcrab-ransomware/
✎[Hidden tear勒索软件解密工具]
```

```
https://files.avast.com/files/decryptor/avast_decryptor_hiddentear.exe
https://download.bleepingcomputer.com/demonslay335/hidden-tear-decrypter.zip
✎[HydraCrypt/UmbreCrypt勒索病毒解密工具]
http://blog.emsisoft.com/2016/02/12/decrypter-for-hydracrypt-and-umbrecrypt-available/
✎[HydraCrypt勒索软件解密工具]
https://tmp.emsisoft.com/fw/decrypt_hydracrypt.exe
✎[Hidden Tear勒索软件解密工具]
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/hidden-tear
✎[InsaneCrypt勒索软件解密工具]
https://download.bleepingcomputer.com/demonslay335/InsaneCryptDecrypter.zip
✎[ImsOOrry勒索软件解密工具]
https://securityaffairs.co/wordpress/88376/malware/imsOOrry-ransomware-decryptor.html
https://www.emsisoft.com/decrypter/imsOOrry
✎[Jigsaw勒索软件解密工具]
https://www.bleepingcomputer.com/news/security/jigsaw-ransomware-becomes-cryptohitman-with-porno-extension/
✎[JuicyLemon勒索软件解密工具]
https://dl.360safe.com/Decryptor_JuicyLemonDecoder.cab
✎[JigSaw勒索软件解密工具]
https://download.bleepingcomputer.com/demonslay335/JigSawDecrypter.zip
✎[Lockcrypt勒索软件解密工具]
```

```
https://labs.bitdefender.com/wp-content/uploads/downloads/lockcrypt-ransomware-decryptor/
✎[Legion勒索病毒解密工具]
http://botcrawl.com/legion-ransomware/
✎[LockedIn勒索软件解密工具]
https://download.bleepingcomputer.com/demonslay335/LockedInDecrypter.zip
✎[MirCop勒索软件解密工具]
https://download.bleepingcomputer.com/demonslay335/MirCopDecrypter.zip
✎[Mblblock勒索软件解密工具]
https://tmp.emsisoft.com/fw/decrypt_mblblock.exe
✎[Marlboro勒索软件解密工具]
https://www.bleepingcomputer.com/news/security/marlboro-ransomware-defeated-in-one-day/
✎[Nullbyte勒索软件解密工具]
https://www.bleepingcomputer.com/news/security/the-nullbyte-ransomware-pretends-to-be-the-necrobot-pokemon-go-application/
✎[NullByte勒索软件解密工具]
https://download.bleepingcomputer.com/demonslay335/NullByteDecrypter.zip
✎[Nanolocker勒索软件解密工具]
https://github.com/Cyberclues/nanolocker-decryptor
✎[NMoreira勒索软件解密工具]
https://www.pcrisk.com/removal-guides/10689-nmoreira-ransomware
✎[NanoLocker勒索病毒解密工具]
```

```
http://blog.malwareclipboard.com/2016/01/nanolocker-ransomware-analysis.html
✎[OpenToYou 勒索病毒解密工具]
http://blog.emsisoft.com/2016/12/30/emsisoft-releases-free-decrypter-for-opentoyou-ransomware/
✎[Odcodc勒索病毒解密工具]
http://www.nyxbone.com/malware/odcodc.html
✎[ODCODCDecoder勒索软件解密工具]
https://dl.360safe.com/Decryptor_ODCODCDecoder.cab
✎[Pclock勒索软件解密工具]
https://www.bleepingcomputer.com/forums/t/561970/new-pclock-cryptolocker-ransomware-discovered/
✎[PopCorn勒索软件解密工具]
https://www.elevenpaths.com/downloads/RecoverPopCorn.zip
✎[Ransom.Cryakl勒索病毒解密工具]
http://blog.checkpoint.com/2015/11/04/offline-ransomware-encrypts-your-data-without-cc-communication/
✎[Shade勒索软件解密工具]
https://blog.kaspersky.com/shade-decryptor/12661/
✎[SanSam勒索软件解密工具]
https://download.bleepingcomputer.com/demonslay335/SamSamStringDecrypter.zip
✎[Unlock92勒索软件解密工具]
https://download.bleepingcomputer.com/demonslay335/Unlock92Decrypter.zip
✎[Unlocker勒索软件解密工具]
```

```
https://github.com/kyrus/crypto-un-locker
🔪[Wildfire勒索软件解密工具]
https://downloadcenter.mcafee.com/products/mcafee-avert/wildfiredecrypt/wildfiredecrypt.exe
```

3.1 Linux-GonnaCry-感染&识别&解密

```
样本：https://github.com/tarcisio-marinho/GonnaCry
```

3.2 Windows-Satan3.X-感染&识别&解密

```
样本：https://bbs.pediy.com/thread-245987.htm
```

3.3 Windows-WannaCry-感染&识别&解密

```
样本：https://bbs.pediy.com/thread-267595.htm
```