SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

勒索病毒应急响应流程

面向未来 有效保护

勒索病毒应急响应流程

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

最近有多个客户爆发勒索病毒，针对在客户端的应急实际情况，输出一套简单、实用的应急流程，供大家参考。

一、保留现场，断开网络

1）根据灾情状况，第一时间将所有中招主机进行网络隔离，建议采取物理隔离方式如拔网线，这样可以防止进一步扩散，造成二次伤害。至于其它未中招的主机，建议根据灾情实际情况，选择是否隔离网络。理论上来讲，如何灾情特别严重，建议所有主机都隔离网络，待应急结束，加固完成后，再放通网络。

2）中招主机隔离后，建议保留现场，不要破坏环境或者格式化系统，除非不需要做溯源取证和入侵原因分析，不然会给后续做防御加固、解密恢复带来困难。通常来讲，**中招主机也不要断电，不要重启，如果真的需要数据恢复，可以找专业的厂商来解决。**

勒索病毒应急响应流程

二、判断家族，尝试解密

深信服 EDR 官网查询

(1)通过 EDR 官网查询勒索病毒家族，官网地址如下: https://edr.sangfor.com.cn/#/information/ransom_search

勒索病毒应急响应流程

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

二、判断家族，尝试解密

(2)在搜索框中输入加密后缀进行查询(注:部分使用随机后缀的家族无法通过此方 法搜索)，如 POSEIDON666:

勒索病毒应急响应流程

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

二、判断家族，尝试解密

(3)或者通过黑客邮箱进行查询，如 true_offensive@aol.com:

勒索病毒应急响应流程

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

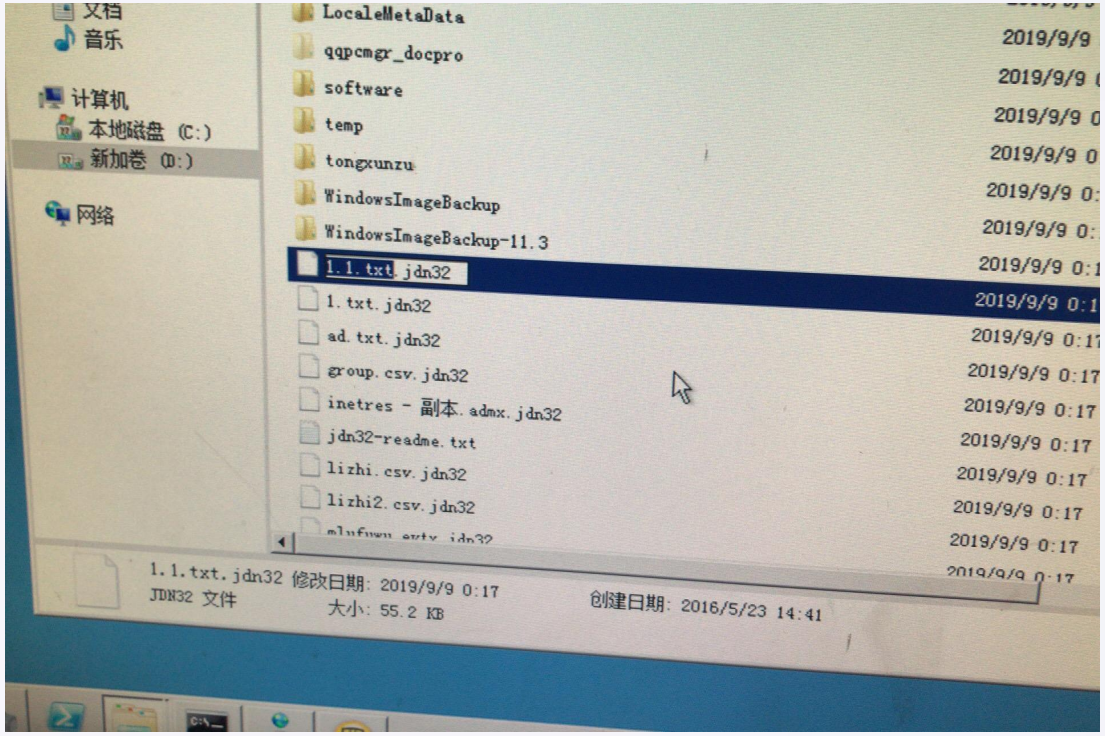
二、判断家族，尝试解密

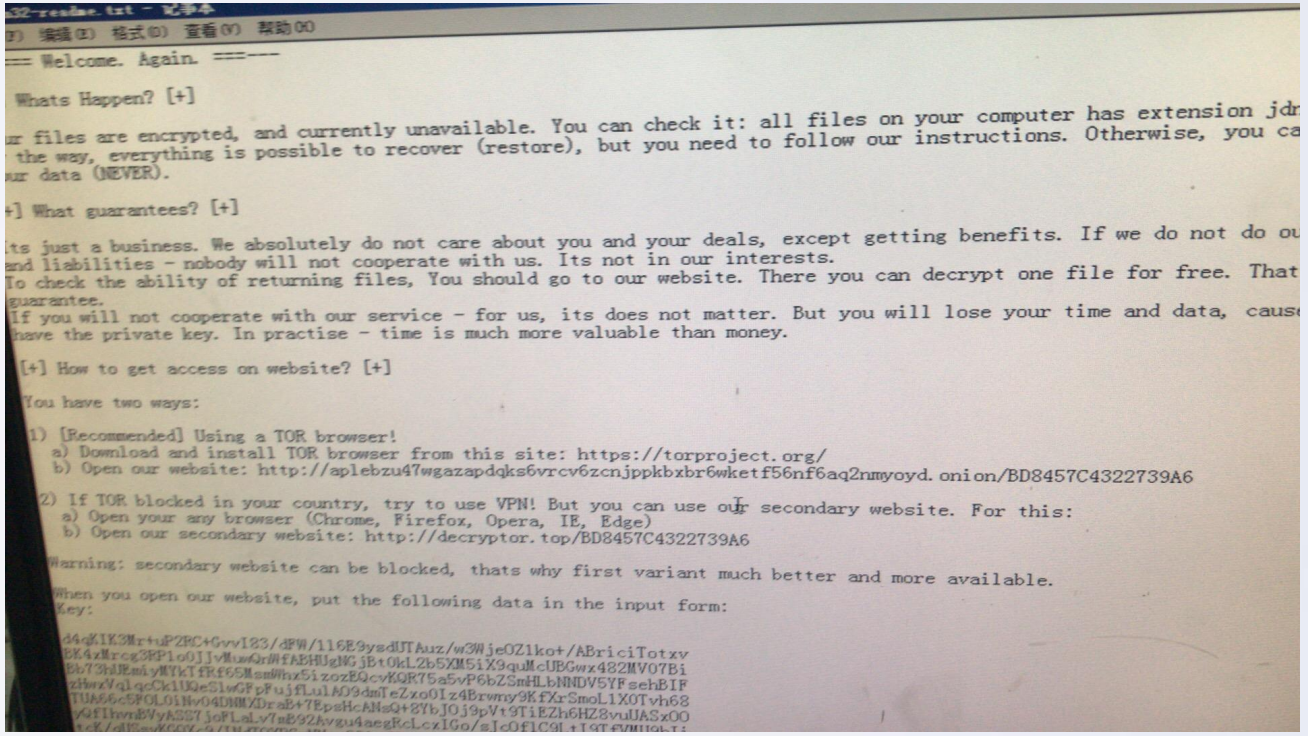
(4)也可以通过家族名称搜索相关信息，如果有解密工具，可以进行下载:

勒索病毒应急响应流程

二、判断家族，尝试解密

(5)如果无法通过深信服 EDR 官网查询到家族，则需要反馈加密后缀、勒索信息文件 (hta、html、txt 文件等)、样本(如有)等，后续反馈至微信沟通群内。



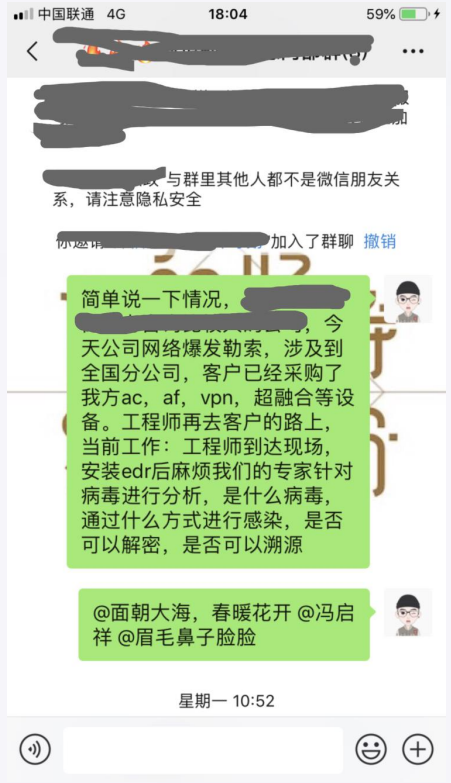


勒索病毒应急响应流程

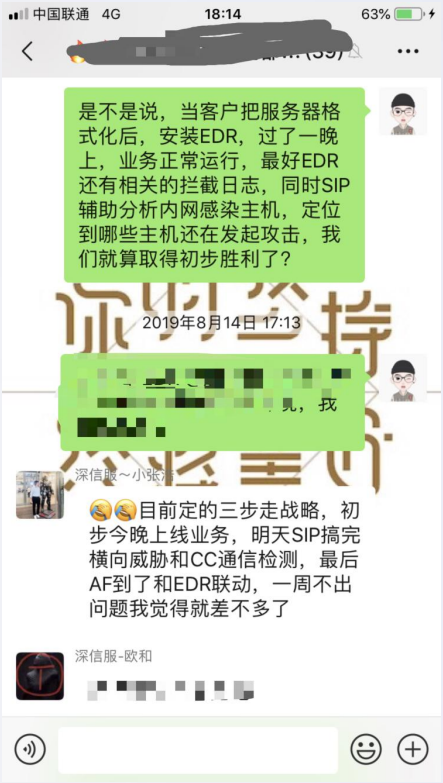
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

三、建立微信群，消息同步

建立微信群，优先联系EDR部门同事，冯启祥、张艺峰、欧和、樊谦君、吴德正入群。同时说明目前情况，及客户需求。**注意：建议优先完成EDR部署、远程环境等工作，加快处理速度。检测电脑必须具备远程环境，便于问题定位。**



明确客户需求：告知总部同事只是需要确保内网没有勒索病毒了，还是需要溯源。



勒索病毒应急响应流程

四、提

协

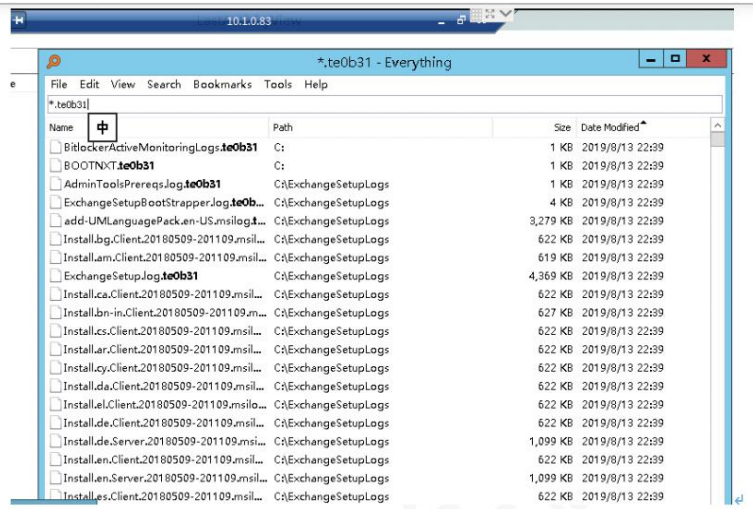
索病毒

可以精

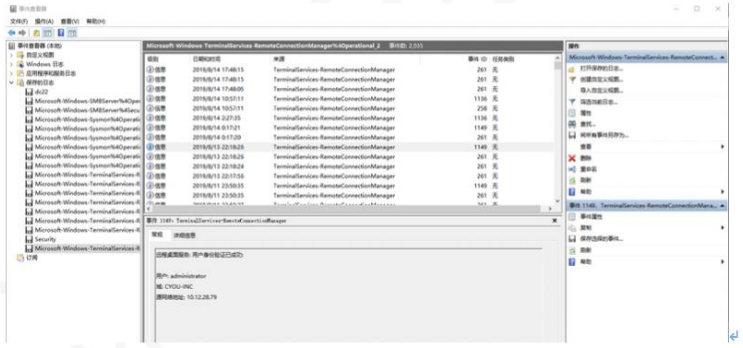
DR

· 2.2.2 查看日志

首先排查服务器 10.1.0.83 最早被加密文件时间，发现本机最早被加密于 8 月 13 号晚上 22:39：

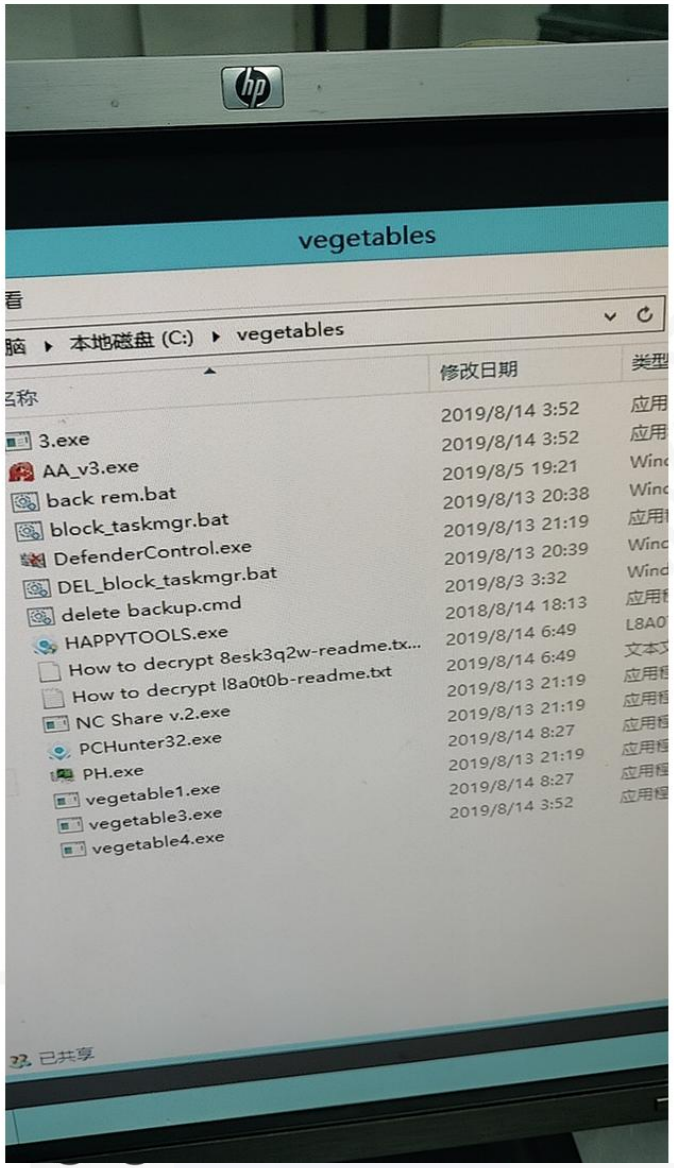


根据最早被加密时间排查主机远程登录日志，在 22：18 左右有一个登录记录，：



通过工具查看主机上执行过的操作日志，最接近加密时间的登录在 22:29，日志中疑似被删除了一小段时间的记录：

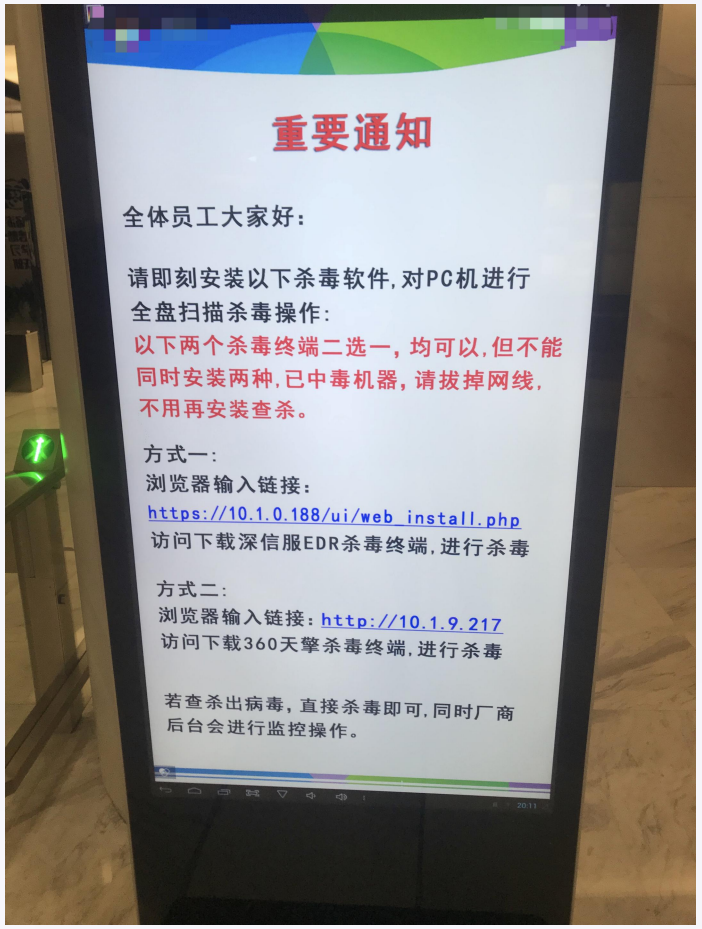
排查该服务器上面的加密时间最近一次登录记录的 IP 为 10.12.28.79，与客户沟通后，发现这台主机是供应商来同步数据到客户内网的一台主机，同样被加密，在 C 盘下发现一个名为 vegetables 的目录，跟勒索病毒的名称一样：



勒索病毒应急响应流程

五、终端部署EDR，进行防御

定位到勒索病毒后，建议客户的终端全部部署EDR，避免内网二次感染。同时把文件实时防护、勒索诱饵功、暴力破解检测等功能全部开启，并建议客户把补丁都打上，打完补丁后可以选择用户自行重启。



注意事项：

1、在大面积部署EDR或用EDR进行查杀时建议至少2名同事在客户现场，因为现场会出现过各种问题，一个人根本应付不过来。

2、针对于查杀结果，可能会出现误报也可能出现软件本身没办法解决的问题，将此类问题汇总后反馈在内部群中，同时最好是有远程环境，可远程查看，更加方便定位问题与解决问题。

3、针对勒索诱饵，类似腾讯软件可以会触发诱饵报警，确认非病毒文件后，建议将此类文件加白。

4、SMB爆破检测需要多注意 由于协议的原因 导致SMB的暴力破解检测误报率会偏高，需要与客户沟通，是开启自动阻断还是仅上报，不阻断。

勒索病毒应急响应流程

六、定位网络失陷主机

在EDR部署、检测完成后，建议通过SIP发现内网中是否还存在其他问题主机，并用EDR进行处置，强调联动效果。

勒索病毒事件分析

经我们全网定位，发现目前存高风险的PC主机列表如下：

连接11域控服务器的风险终端	连接12域控服务器的风险终端	其他风险服务器	其他风险PC
10.1.0.11	10. 1. 0. 12	10. 1. 35. 158	10. 12. 0. 90
10. 1. 35. 158	10. 12. 5. 127	10. 1. 8. 182	10. 12. 5. 176
10. 1. 8. 182	10. 12. 20. 163	10. 1. 151. 250	10. 12. 28. 65
10. 12. 160. 124	10. 12. 20. 32	10. 1. 16. 123	10. 12. 28. 50
10. 12. 28. 96	10. 12. 16. 176	10. 1. 0. 12	10. 12. 5. 130
10. 12. 144. 67	10. 12. 0. 115	10. 1. 0. 12	10. 12. 17. 6
10. 1. 9. 105	10. 12. 0. 39	10. 1. 8. 13	10. 12. 8. 173
10. 12. 0. 2	10. 12. 32. 14	10. 1. 16. 154	10. 12. 1. 144
10. 12. 4. 246	10. 12. 0. 198	10. 1. 0. 14	10. 12. 28. 66
10. 12. 12. 50	10. 12. 8. 46	10. 1. 8. 143	10. 12. 12. 34
10. 12. 5. 127	10. 12. 144. 67	10. 1. 1. 245	10. 12. 32. 2
10. 12. 21. 3	10. 1. 9. 105	10. 1. 1. 247	10. 12. 20. 72
10. 12. 28. 118	10. 12. 4. 246		10. 12. 8. 87
	10. 12. 28. 96		10. 12. 21. 25

其中截止到16日19:49 已安装深信服终端安全响应检测软件PC主机列表如下（标红为已安装），建议迅速安装其他主机，最好保证是深信服的，这样深信服可以联动内网设备进行处置闭环：

连接11服务器	连接12服务器	其他服务器	其他PC
10.1.0.11	10. 1. 0. 12	10. 1. 35. 158	10. 12. 0. 90
10. 1. 35. 158	10. 12. 5. 127	10. 1. 8. 182	10. 12. 5. 176
10. 1. 8. 182	10. 12. 20. 163	10. 1. 151. 250	10. 12. 28. 65
10. 12. 160. 124	10. 12. 20. 32	10. 1. 16. 123	10. 12. 28. 50
10. 12. 28. 96	10. 12. 16. 176	10. 1. 0. 12	10. 12. 5. 130
10. 12. 144. 67	10. 12. 0. 115	10. 1. 0. 12	10. 12. 17. 6
10. 1. 9. 105	10. 12. 0. 39	10. 1. 8. 13	10. 12. 8. 173
10. 12. 0. 2	10. 12. 32. 14	10. 1. 16. 154	10. 12. 1. 144
10. 12. 4. 246	10. 12. 0. 198	10. 1. 0. 14	10. 12. 28. 66
10. 12. 12. 50	10. 12. 8. 46	10. 1. 8. 143	10. 12. 12. 34
10. 12. 5. 127	10. 12. 144. 67	10. 1. 1. 245	10. 12. 32. 2
10. 12. 21. 3	10. 1. 9. 105	10. 1. 1. 247	10. 12. 20. 72
10. 12. 28. 118	10. 12. 4. 246		10. 12. 8. 87
	10. 12. 28. 96		10. 12. 21. 25

注意事项：

1、内网中若存在DNS服务器，SIP需要镜像终端到服务器之间流量，同时用EDR对DNS服务器进行检测，检测无问题后，建议先将DNS服务加白。

勒索病毒应急响应流程

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

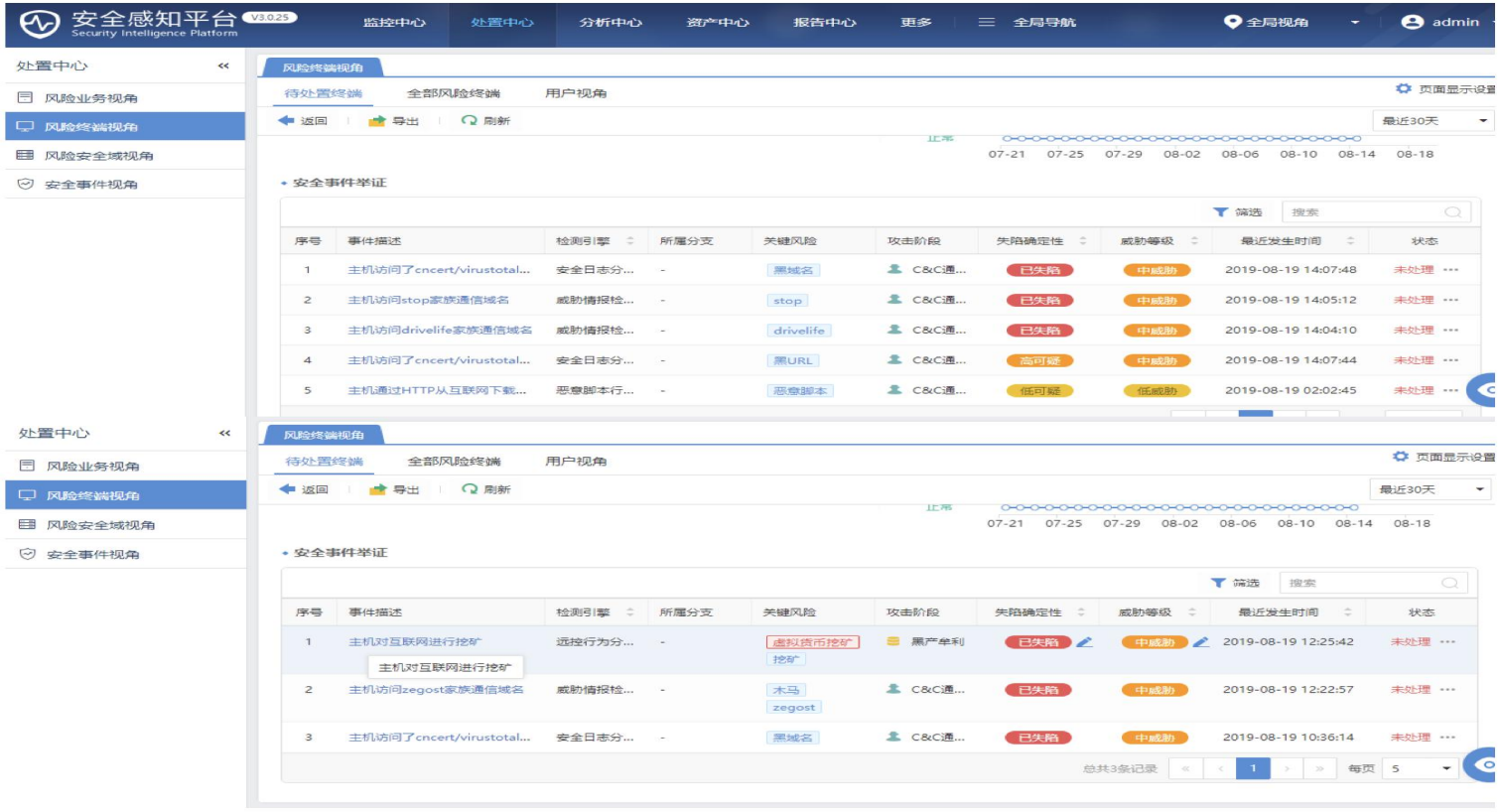
7、持续跟进，保障效果

在SIP、EDR上线一段时间，网络问题基本稳定后，此时需要帮助客户持续关注网络情况，最好是形成文档，让客户直观的看到我们的防护效果。

其他安全事件分析

SANGFOR 深信服科技

目前已经针对全网的勒索病毒事件，已经有效得到控制！经过SIP分析平台，目前和勒索相关的事件行为已经没有！就目前网络就剩下一些挖矿和木马等病毒！



勒索病毒应急响应流程--总结

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

快速建群

- 应急，速度和效率是第一位，当了解客户端出现安全问题，要迅速建立保障群，群内应包含销售、BU、产品线专家、技服、安服同事
- 明确每条产品线的接口人，用简短、清晰的文字将情况说明
- 了解客户需求，是快速定位问题，还是处理病毒事件等等
- 备注：尽可能将AF+SIP+EDR的整体应急方案，不要单上SIP或者EDR

明确职责

- 针对当前客户情况进行分工、销售协调测试设备、BU制定初步方案、技服明确实施方案、安服进行安全事件分析，各产品线专家给出初步建议
- 群内同步客户需求，明确客户当前希望到达的效果，分阶段完成。
- 快速部署设备、进行数据采集、分析，同时建议与专家配合，结果最好以报告形式交付，提告专业度。
- 备注：一定要定好当前需要解决的问题，如可先通过部署EDR让专家分析病毒类型、传播途径，当前主机是否还有其他风险，再通过SIP进行全网威胁定位。做好分工、事半功倍，反馈慢，就电话联络，不要让问题卡在一个阶段长时间不解决。

问题解决

- 针对EDR检测到的问题向客户进行反馈，前期建议仅上报不处置。
- 同时在部署EDR或EDR进行查杀时建议至少2名同事在客户现场，因为现场会出现过各种问题，一个人根本应付不过来。
- 针对于查杀结果，可能会出现误报也可能出现软件本身没办法解决的问题，这时不要慌，把问题在群内说清楚，最好是有远程环境，远程查看，更加方便定位问题与解决问题。
- 要相信只要前后端配合的好，问题都可以解决，我们在现场不要慌，因为我们一慌客户对我们也就不信任了，有问题多沟通，共同寻找解决办法与应对话术。

SANGFOR
深信服科技

深信服智安全
SANGFOR SECURITY

THANK YOU

面向未来 有效保护