



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

医疗行业勒索病毒防范

主讲人：李华生



CONTENTS

目 录

-  PART 01 医疗行业网络安全形势
-  PART 02 勒索病毒介绍
-  PART 03 勒索病毒处置解决方案
-  PART 04 结语



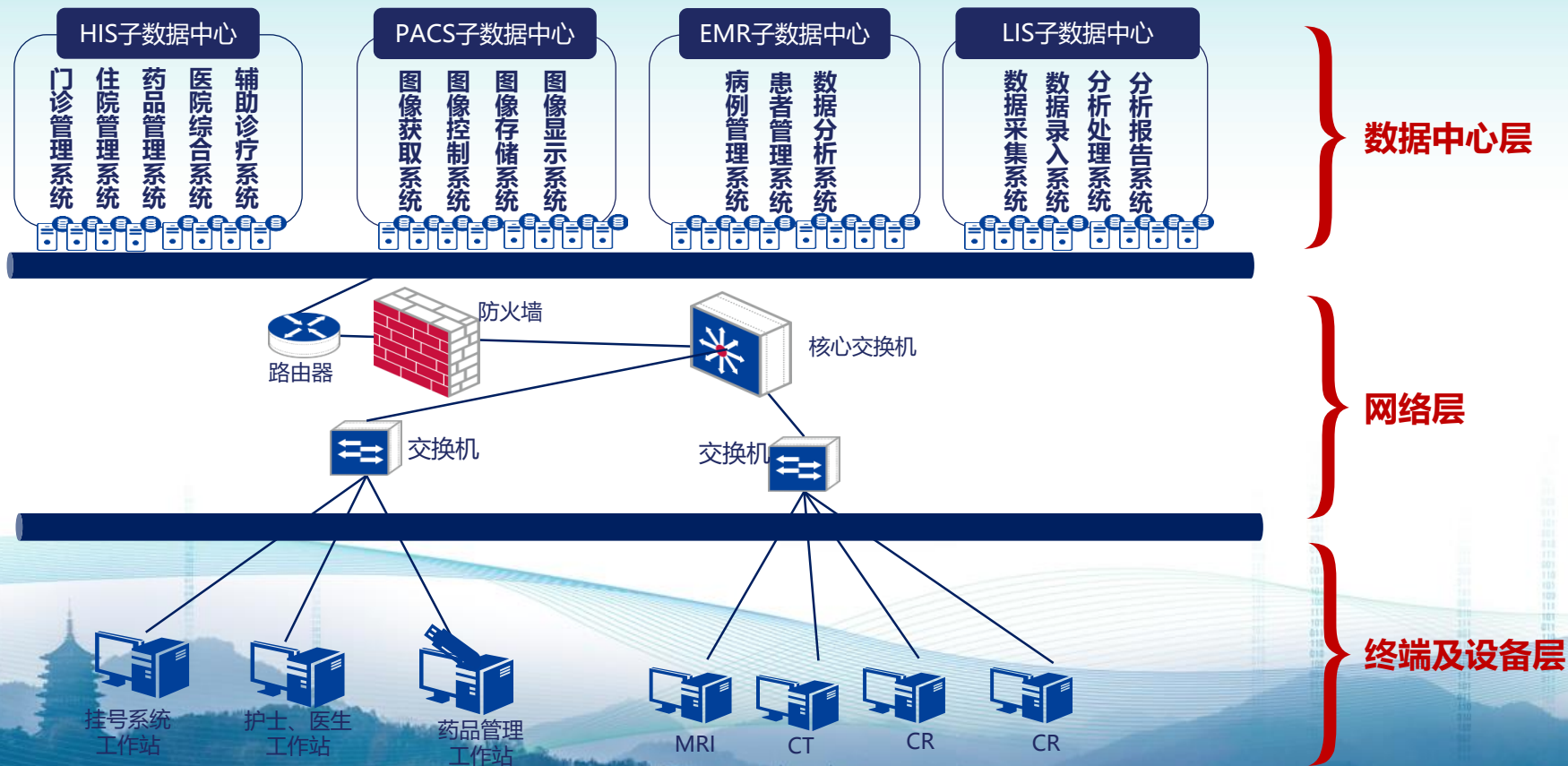
医疗行业网络安全形势

Network security status

- 医疗行业的网络安全威胁
- 医疗行业勒索病毒事件



医院信息系统及其构成要素



医院信息系统潜在的网络安全威胁



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

数据中心层的网络安全威胁：

1

- 数据库缺少审计和防护，容易引发攻击和数据泄露。
- 数据中心之间隔离不到位，对于单点威胁容易被横向扩散。
- 服务器防护不力，容易成为“肉鸡”。

2

网络层的流量安全威胁：

- 恶意流量无法完全识别和阻止
- APT攻击层出不穷，传统安全设备的能力有一定的滞后性

3

终端及设备层的网络安全威胁：

- 系统漏洞未及时修复
- 恶意软件泛滥
- 弱口令普遍存在
- 外设随意接入
- 防范薄弱成为入侵的入口

2019以来全国勒索攻击态势



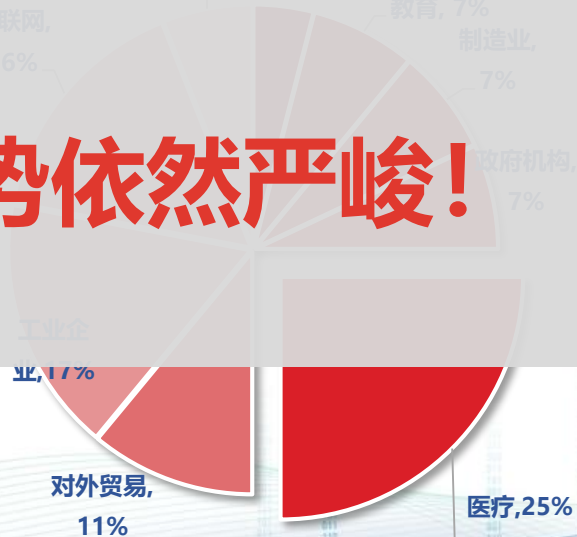
2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

地域分布

行业分布

其他, 6% 金融, 4%

全国医疗系统勒索病毒形势依然严峻!



近期医疗行业大规模勒索病毒事件 (1)



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

搜狐 > 健康 > 正文

鳳凰網 资讯 凤凰网资讯 > 社会 > 正文

朋友圈热文在这里!

看医界

200多家三甲医院检出勒索病毒！ 升级版勒索病毒攻陷湖北医院 黑客索要价值30万比特币

勒索病毒攻击最多的操作系统主要包括

Windows 7

Windows 10

Windows XP

Windows 2003

Windows server系列

国内两家省级医院遭勒索病毒攻击

2018-02-24 10:22

IT之家2月24日消息 根据国内某安全软件报道，目前，国内两家省级医院服务器疑似遭最新

勒索病毒攻击，医院内部系统已经瘫痪，同时数据库文件被加密破坏，正常就医秩序受到严重影响。

据悉，其中一家湖南省儿童医院受到的影响最为严重，从2018年2月24日7点左右，全院所有的医疗系统均无法正常使用。经过查实，医院服务器中了疑似最新的勒索病毒，目前，黑客要求院方在6小时内为每台中招机器支付1个比特币，根据目前比特币最新的价格，1枚比特币约合人民币6.5万元左右。

原标题：升级版勒索病毒攻陷湖北一医院 黑客索要比特币

23日上午，湖北襄阳市南漳县人民医院系统被植入升级版勒索病毒后陷入瘫痪，黑客要求支付比特币才能恢复正常。24日上午11时，该院回复上游新闻称，患者看病已不受影响，公安部门已介入调查。

上游新闻记者介绍，23日上午上班后，住院部医生发现，原来只能联内网的电脑可以正常发现，因系统瘫痪录入在电脑中的药价等数据不见了；还有医生发现，存储在电脑中的病例也消失了。

南漳县人民医院办公室值班人员介绍，系统瘫痪后，他们联系技术人员前来修理，并向南漳公安局报警；另一方面，医生克服困难，就诊秩序没受太大影响。

上游新闻记者了解到，2017年勒索病毒全球爆发。23日上午，南漳县人民医院电脑系统被植入了“升级版勒索病毒”，黑客要求医院支付比特币，才能恢复正常。

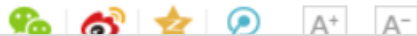
目前，医院已建立了一个新系统，但之前的数据尚未恢复。



近期医疗行业大规模勒索病毒事件 (2)

紧急预警：Globelmposter勒索病毒全国蔓延，大型医院已中招，企事业单位一定要做好这几项措施

2019-03-11 20:56:59 来源：中国金融商报



为什么勒索病毒总是攻击医院？

以十二生肖为后缀

安全薄弱、社会影响大！勒索病毒家族：2017年出现，2018年8月份演进为v3.0版本。整体特点如下：

后缀	词义	
Pig4444	猪	2018年8月
Snake4444	蛇	2018年9月
Dragon4444	龙	2018年9月
Ox4444	牛	2018年9月
Rooster4444	鸡	2018年9月
Tiger4444	虎	2018年9月
Horse4444	马	2018年10月
Help4444	帮助（非十二生肖）	2018年10月
SKUNK4444	臭鼬（非十二生肖）	2018年11月
Goat4444	羊	2018年12月
Rabbit4444	兔	2018年12月
Monkey4444	猴	2019年2月
ALCO4444	含义不明（非十二生肖）	2019年2月
Rat4444	鼠	2019年2月

加密方法：采用RSA和AES两种加密算法的结合。----无法破解！
主要的传播方式：扫描渗透+远程桌面登录爆破。----粗暴实用！
解密办法：暂无公开的破解方法。

V3.0版本特点如下：

- 1、将加密文件的后缀改成 动物名称+4444的样子。
- 2、当加密完成后，除了清除远程桌面登录信息，还添加了自删除的功能，让追溯分析难度更高。



勒索病毒介绍

Extortion virus

- 勒索病毒系列
- 勒索病毒原理与危害
- 勒索病毒最新趋势

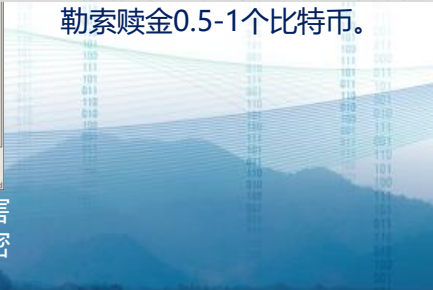
WannaCry家族

Petya家族

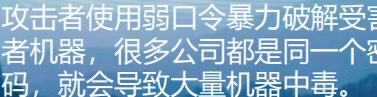
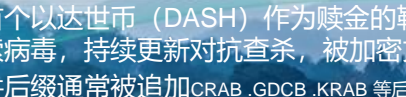
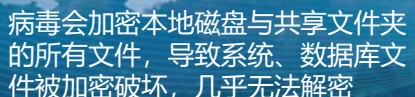
Bad Rabbit家族



Locky家族



20个家族*50个变种 = 1000种已知的勒索病毒



勒索病毒原理与危害



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

① 病毒进入内网

入



②

内网扩散

扩



③

病毒运行

加



中了勒索病毒，多久之后开始加密？

漏洞
邮件

程序木马
网页挂马
存储设备带入
office组件的病毒感染
人工投毒

永恒之蓝
双脉冲星

永恒之冠
永恒浪漫
永恒王者
永恒协作
等等

通过脚本文件进行Http请求
通过脚本文件下载文件

读取远程服务器文件
收集计算机信息
进程遍历文件
调用加密算法运行加密进程



传统杀毒软件在应对勒索时的困境

01

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

传统杀毒软件在勒索病毒面前力不从心！

Globelmposter
家族变种

.freeman、.panda
.reserve、.true+
.walker、.gotham
.techno、.chak等

02

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



勒索病毒处置解决方案

Emergency disposal

- 确认中招勒索
- 方案1：安恒EDR一剑封喉
- 方案2：预警防御一体化
- 方案3：安全建设平台化

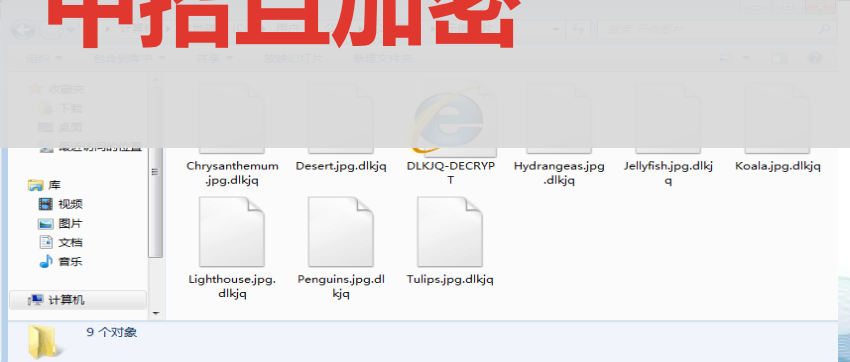
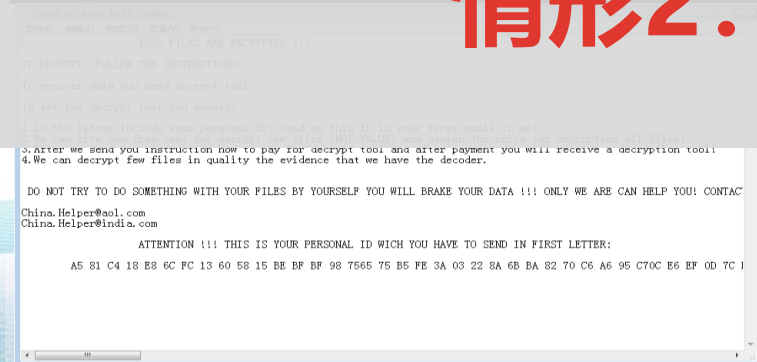
确认中招勒索



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE



情形1：中招未加密
情形2：中招且加密



勒索病毒处置方案1：安恒EDR一剑封喉



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

应急七步法

1.部署EDR

2.开启防御引擎

3.切断扩散

诱饵引擎，独家技术！
装了安恒EDR，承诺不被加密，支持保险赔付！

5.查杀已知病毒

6.阻止加密行为

7.巡检与加固

☐ 针对未知勒索病毒的精准识别与全网联动防御方法和系统

(公开)

申请号：CN201811180960

申请日：2018.12.19

IPC分类号：G06F21/56

申请(专利权)人：杭州安恒信息技术股份有限公司；

发明人：李华生；范渊；



勒索病毒处置方案1：安恒EDR超越用户的预期



集防御、检测、运维功能于一体的 主机安全及管理系统

安恒主机卫士（EDR）是一款集成了丰富的**系统防护与加固**、**网络防护与加固**等功能的主机安全产品。安恒主机卫士（EDR）通过自主研发的文件诱饵引擎，有着业界领先的**勒索专防专杀**能力；通过**内核级东西向流量隔离**技术，实现网络隔离与防护；拥有**补丁修复**、**外设管控**、**文件审计**、**违规外联检测与阻断**等主机安全能力。

应用场景：



挖矿病毒查杀处理



勒索病毒查杀处理



PC安全管理



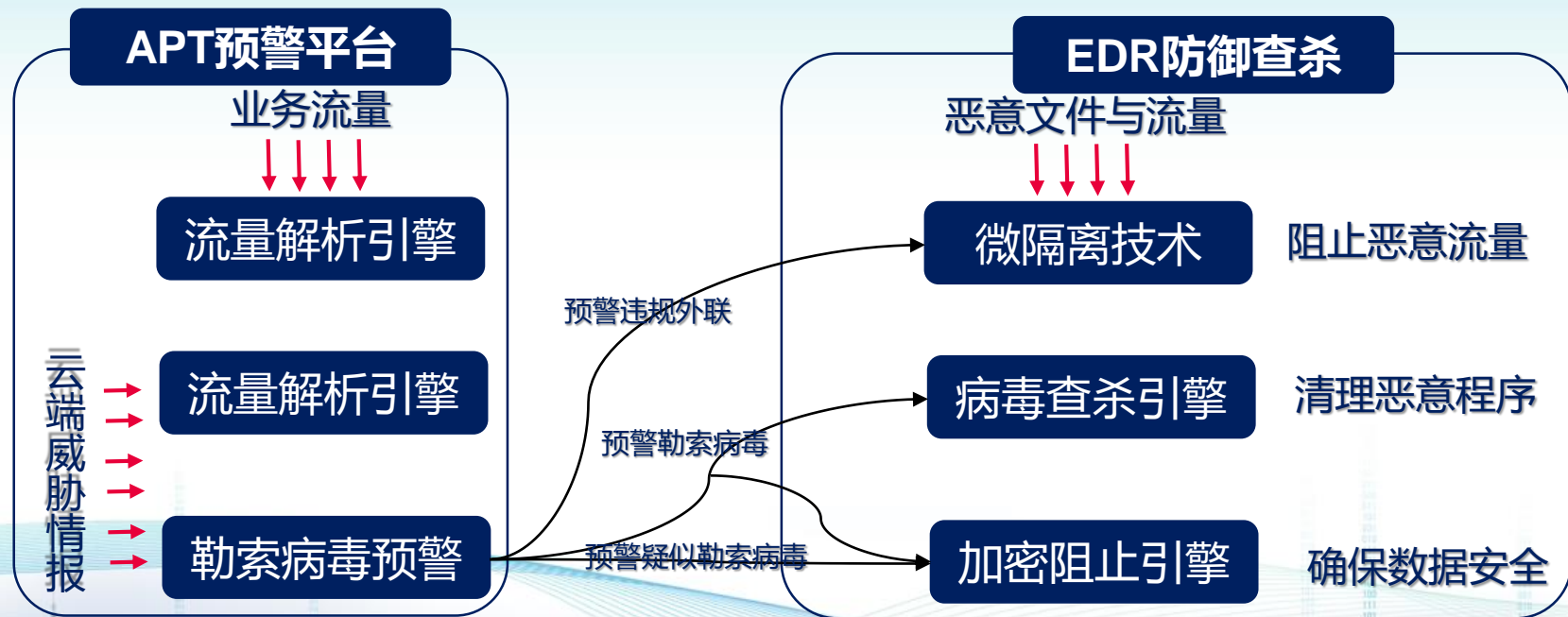
服务器安全运维



虚拟机安全管理



勒索病毒处置方案2：预警防御一体化



最佳搭档!



结语

Company introduction

- 困境与对策
- 厂商的社会责任

医疗体系的网络安全思考



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

01 医院的视角

- 1、事情多！
- 2、事情杂！
- 3、安全设备多！
- 4、采购审批难！
- 5、上了安全设备还不一定能抵御所有的风险！

04 建议

- 1、平台化思维！
- 2、避免监管部门的成为攻击跳板！
- 3、制定防御体系的基础方案！
- 4、牵头集中采购！
- 5、全面治理与大数据分析！



02 卫健委的视角

- 1、难以整体掌握辖区内医院的安全状况！
- 2、自身有可能成为病毒感染的源头！
- 3、各家医院防御能力参差不齐！
- 4、产品选型五花八门！
- 5、单点问题容易演变为全局问题！

03 厂商的责任

- 1、极简操作！
- 2、极简部署！
- 3、联动防御！
- 4、应急处置神器！
- 5、服务+产品+保险相结合！

社会责任与商业价值的统一 服务与产品齐头并进 与客户共同成长





2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

THANK YOU

谢 谢 观 看