# 病毒之勒索软件

- Lynx 高级安全研究员

# 目 录



# 前言


venus X64 2.0
Windows 7 x86 勒索软件...
Windows 7 x86 勒索软件...
勒索软件样本
勒索软件样本 密码：hackerhouse
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Chinese (simpl:
我的电脑出了什么问题？
您的一些重要文件被我加密保存了。
照片、图片、文档、压缩包、音频、视频文件、exe文件等，几乎所有类型的文件都被加密了，因此不能正常打开。
这和一般文件损坏有本质上的区别。您大可在网上找找恢复文件的方法，我敢保证，没有我们的解密服务，就算老天爷来了也不能恢复这些文档。
有没有恢复这些文档的方法？
当然有可恢复的方法。只能通过我们的解密服务才能恢复。我以人格担保，能够提供安全有效的恢复服务。
但这是收费的，也不能无限期的推迟。
请点击 <Decrypt> 按钮，就可以免费恢复一些文档。请您放心，我是绝不会骗你的。
但想要恢复全部文档，需要付款点费用。
是否随时都可以固定金额付款，就会恢复的吗，当然不是，推迟付款时间越长对你不利。
最好3天之内付款费用，过了三天费用就会翻倍。
还有，一个礼拜之内未付款，将会永远恢复不了。
对了，忘了告诉你，对半年以上没钱付款的穷人，会有活动免费恢复，能否轮
Payment will be raised on
5/18/2017 23:06:27
Time Left
Your files will be lost on
5/22/2017 23:06:27
Time Left
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $600 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt
大小
1 KB
2 KB
3,392 KB


INDUSTRY
PLATFORM
SEARCH
FINANCE
COMMUNICATION
NETWORK
WEBSITE
DATABASE
COLLABORATION
APPLICATION
MONITORING
CLOUD
ONLINE SHOPPING
RUNTIME
OBJECT STORAGE
MEDICAL
IDENTITY
COMPUTE
CONTENT
BLOG STORAGE
INFRASTRUCTURE
SEO

# Wanna Cry 简介

该勒索软件是通过445端口并利用SMB服务漏洞而进行的攻击，基本确定是基于此前“Shadow Brokers”批漏多款涉及Windows SMB服务漏洞而产生的了勒索攻击，对用微软的漏洞公告是MS17-010。

由于恶意代码开源或 利用开源代码（包括漏洞的shell code / POC / EXP 等）快速构建恶意代码，未来将层出不穷，对现有企业中信息网络基础设施将面临越来越大的运维和应急响应压力。

杀软 / Firewall / IDS等传统的安全防护设备，本质均是“事后响应”，防护能力在层出不穷的网络安全威胁面前将逐渐弱化，且呈加速下降趋势；因此，研究新型安全防护产品和机制十分必要。

# 目 录



一、勒索软件为何如此猖獗。

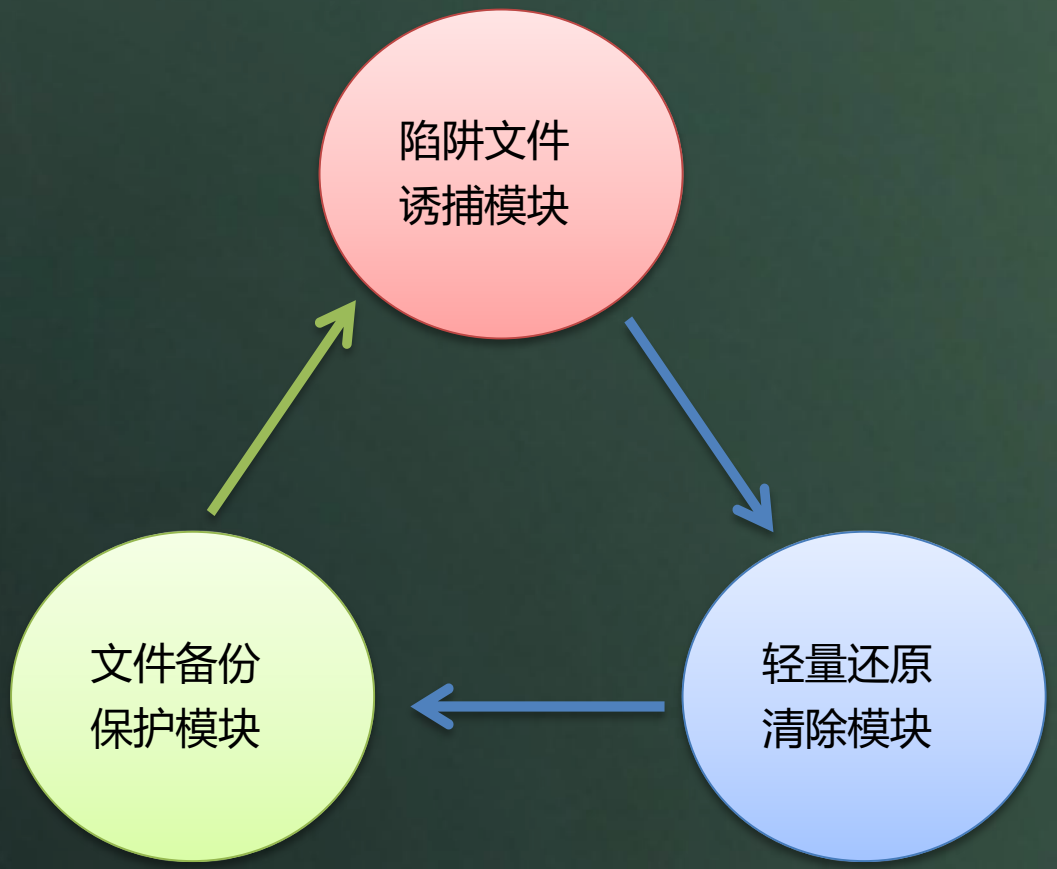
1、匿名支付的兴起

2、移动互联网的高速发展

3、主流安全技术对抗勒索软件时的无奈

# 目 录




陷阱文件
诱捕模块
轻量还原
清除模块
文件备份
保护模块

# 构造符合勒索软件加密类型的陷阱文件放入磁盘

设原磁盘文件遍历序列为：

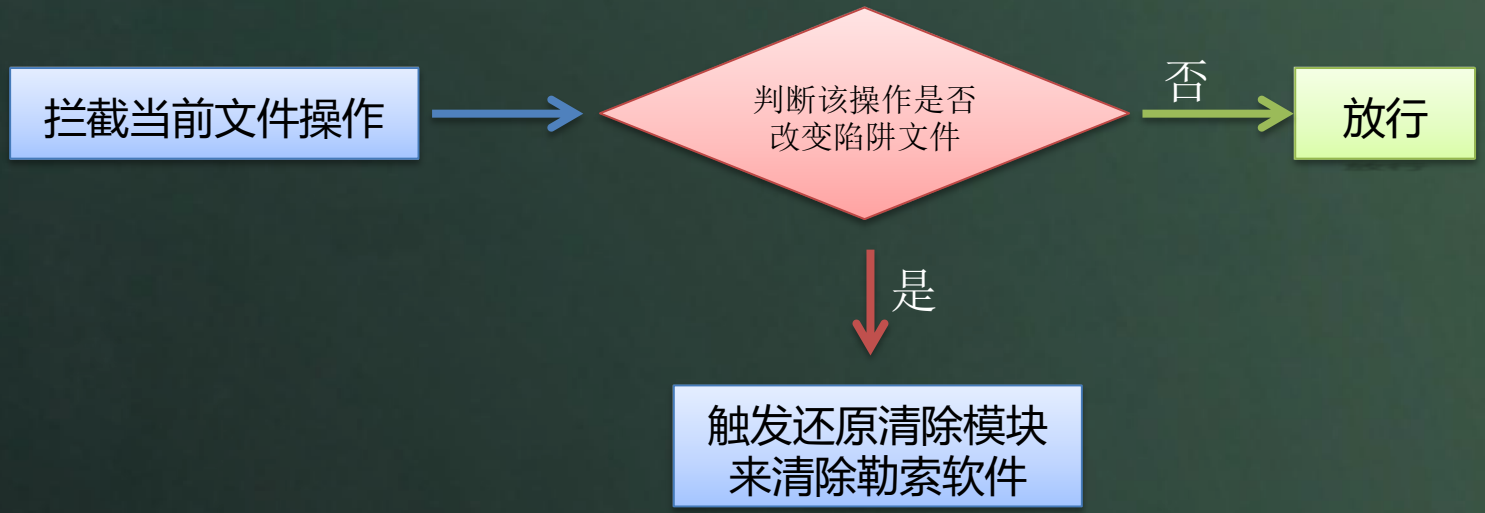
1.doc　2.doc　3.doc　4.doc　5.doc　6.doc

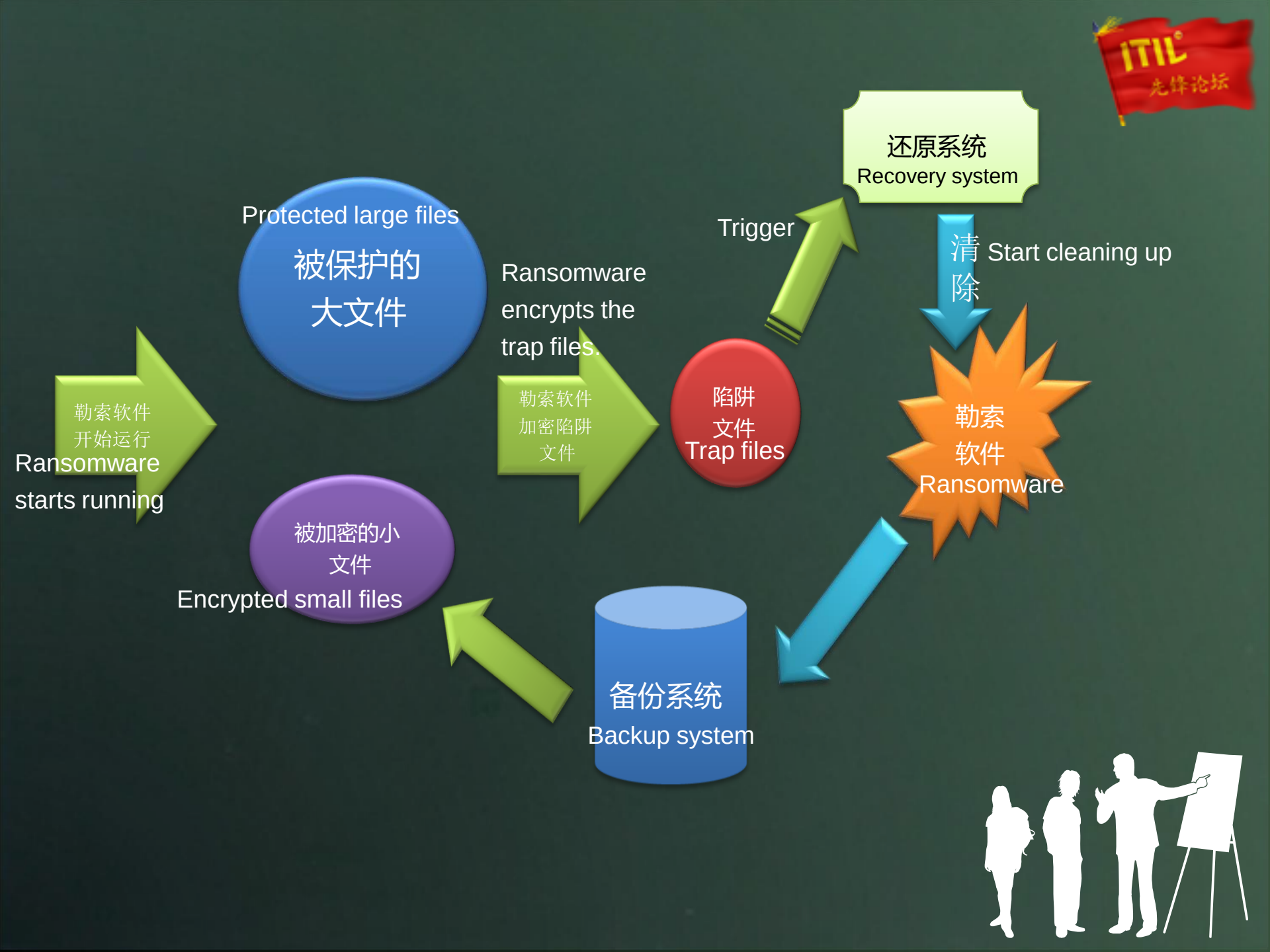
放入陷阱文件后的磁盘文件遍历序列为：

1.doc　2.doc　a.doc　4.doc　一.xls　1.doc　b.doc　1.doc

陷阱文件列表注意防护

# 陷阱模块运作逻辑





还原系统
Recovery system
Trigger
清除 Start cleaning up
Protected large files
被保护的大文件
Ransomware encrypts the trap files.
勒索软件开始运行
Ransomware starts running
勒索软件加密陷阱文件
陷阱文件
Trap files
勒索软件
Ransomware
被加密的小文件
Encrypted small files
备份系统
Backup system

# 备份保护模块导论

1 、小文件进行备份

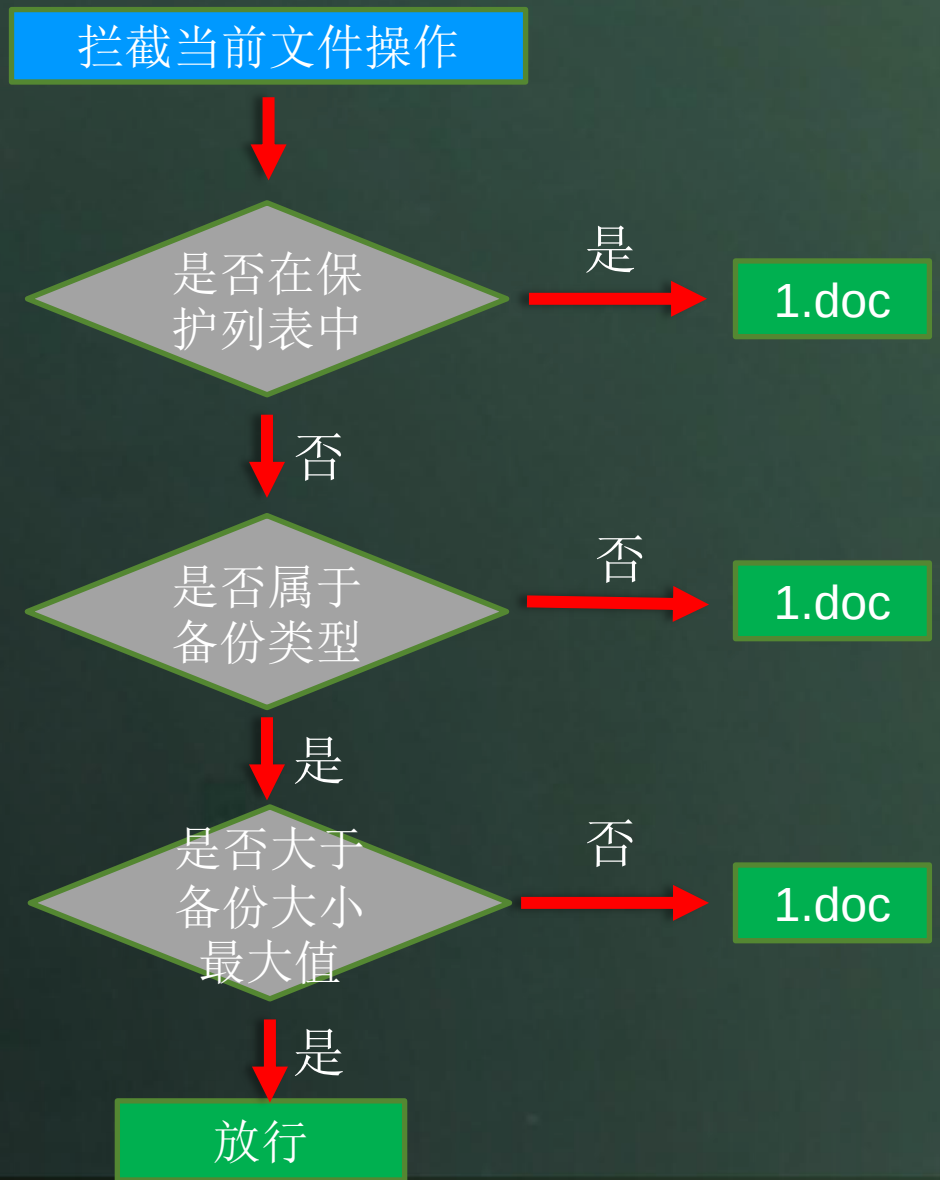
2 、对大文件进行保护

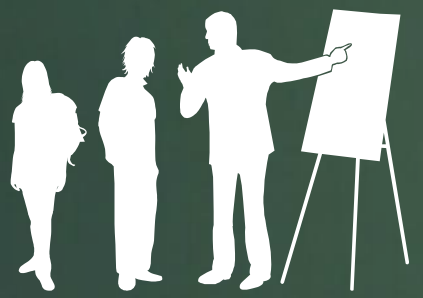
3 、预设需备份文件类型

4 、预设文件备份最大值

5 、预设文件保护列表

# 备份保护模块运作原理


拦截当前文件操作
是否在保护列表中
是
1.doc
否
是否属于备份类型
否
1.doc
是
是否大于备份大小最大值
否
1.doc
是
放行



# 目前国内外安全厂商在反勒索领域的进展

At present, the progress of security vendors in China and foreign countires in the field of anti-ransomware.

# 目 录



勒索软件再次来袭，
你怎么办？

信任
危机

# 总结归纳

**爆发前：**

企业未及时更新安全补丁，对于功能性更新补丁可以忽略，但对于安全补丁，一旦微软官方推出，就说明这个漏洞能造成一定的影响。没能及时修补，体现了企业安全建设中“预防”能力不足。

**爆发中：**

企业安全或IT部门无法根据攻击事件相关的威胁情报，修改企业防火墙/IPS等安全产品规则和策略配置，具备一定的“响应能力”。

**爆发后：**

对某些不常用端口访问等异常行为没有持续性监测，并进行关联分析。表现出“监控和测评能力不足”。

另：

加强同事及所在企业员工

对勒索攻击等安全事件的认知和安全防范意识的教育

举例：邮件钓鱼 / 浏览站点 ……

# 目 录



- Q&A

?

# 给国内信息安全从业者打点鸡血！！！

# 温馨提示

•ITIL先锋论坛专家直播讲堂，每周四晚上8:30指定QQ大群

**•专家讲堂视频&PPT合集，请猛击链接**

•看预告&PPT更新，请关注右边二维码

•找培训，请看下图：

# 谢谢！