阿里云 | 云盾先知 安全情报

如何真实有效的对抗勒索软件

Is there an effective way to fight against Ransomware?

先知白帽大会
开放创新 · 先知先行

目录
Content

- 1、勒索软件为何如此猖獗。
  Why Ransonmware is so rampant?
- 2、主流安全技术对抗勒索软件时的无奈
  The helpless of prevailing security technology fighting against the Ransomware.
- 3、如何有效的防御抗勒索软件
  Is there an effective way to fight against Ransomware?

目录 Content

1

为何勒索软件如此猖獗

Why Ransonmware is so rampant?

1、黑产的发展与勒索软件之间的关系

The relationship between the development of cyber underground market and the ransomware.

2、匿名支付的兴起

The rise of anonymous payments.

3、移动互联网的高速发展

The rapid development of mobile Internet.

目录 Content

2

主流安全技术对抗勒索软件时的无奈

The helpless of prevailing security technology fighting against the Ransomware.

阿里云 | 云盾先知 安全情报

特征码扫描引擎遭遇勒索软件时的困境

The dilemma of signature based AV softwares to detect the Ransomware.

先知白帽大会
开放创新 · 先知先行

主动防御遭遇勒索软件时的困境

The dilemma of proactive AV softwares to detect the Ransomware.

阿里云 | 云盾先知 安全情报

传统备份技术遭遇勒索软件时的困境

The dilemma of traditioal backup softwares facing the the Ransomware.

先知白帽大会
开放创新 · 先知先行

阿里云 | 云盾先知 安全情报

云备份技术遭遇勒索软件时的困境

The dilemma of traditioal cloud-based backup technology facing the Ransomware.

阿里云 | 云盾先知 安全情报

逆向工程遭遇勒索软件时的困境

The dilemma of reverse engineers to dissect the Ransomware.

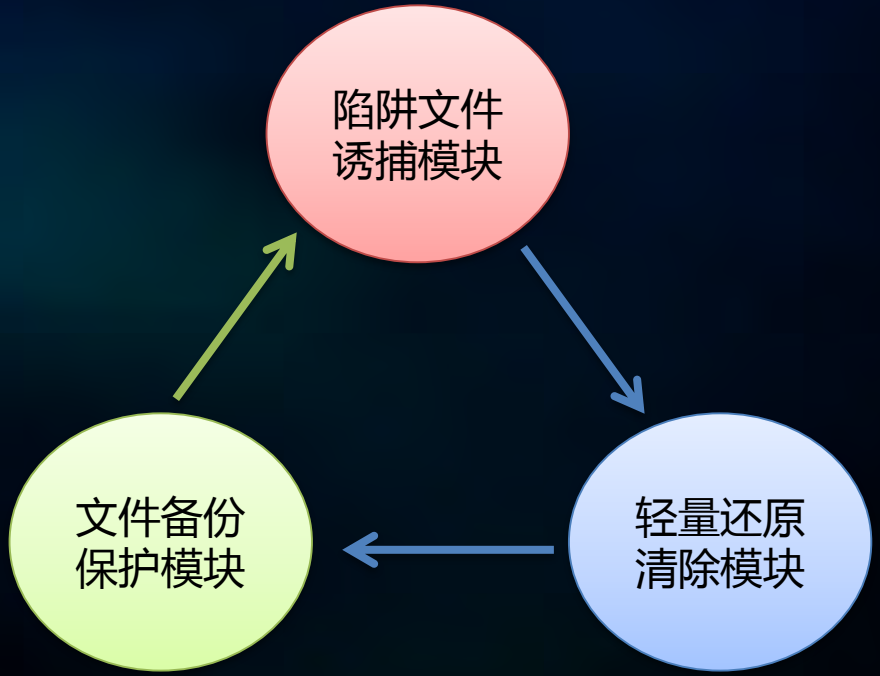
先知白帽大会
开放创新 · 先知先行

目录 Content

3

如何有效的防御勒索软件

Is there an effective way to fight against Ransomware?


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：

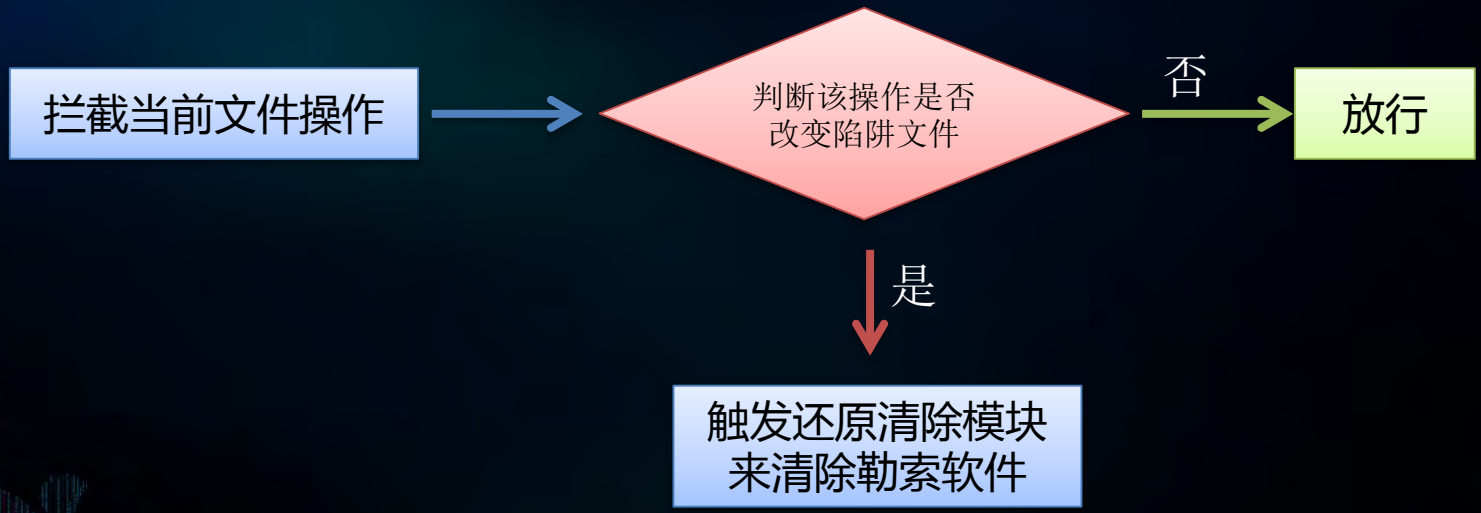
1.doc 2.doc 3.doc 4.doc 5.doc 6.doc

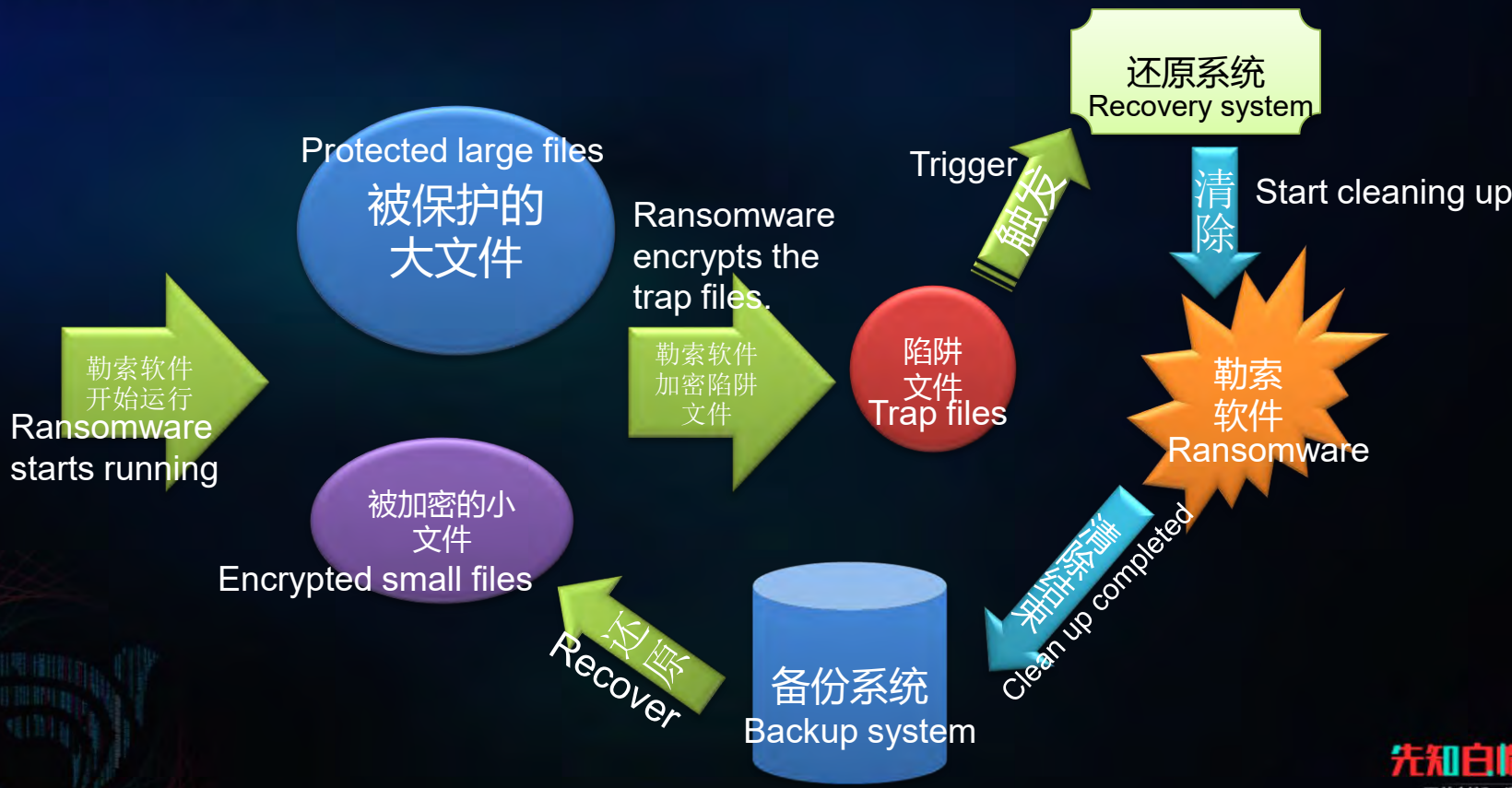
放入陷阱文件后的磁盘文件遍历序列为：

1.doc 2.doc a.doc 4.doc 5.doc b.doc 7.doc 8.doc

陷阱文件列表注意防护

陷阱模块运作逻辑





备份保护模块导论

1、小文件进行备份

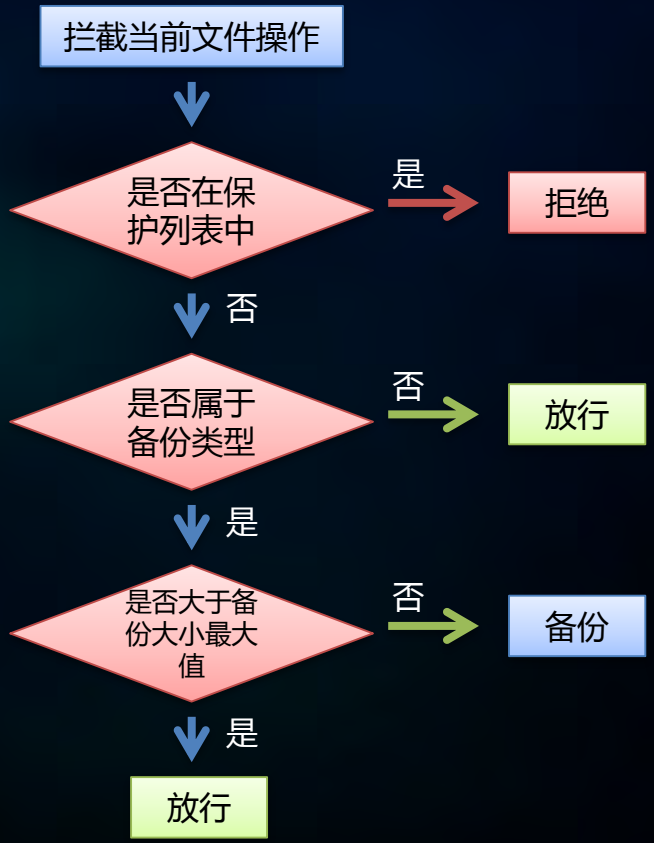
2、对大文件进行保护

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



浅谈几种可能存在的攻击方法

设当前磁盘文件遍历序列如下：黄颜色文件每个100MB

1、如果只有陷阱系统没有备份系统将会出现的问题？

2、备份空间太小时所导致的问题？（ Intercept-X 300M的备份空间）

3、最佳备份空间大小的探讨。

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.

阿里云 | 云盾先知 安全情报

我们的进展

Our progress

先知白帽大会

开放创新 · 先知先行


阿里云
云盾先知
安全情报
让我们干一些能真正促进安全领域向前迈步的事情吧!
Let's do something that really promotes the field of cyber security for moving forward!


阿里云
云盾先知
安全情报
THANKS!