

# 灰犀牛和避风港计划

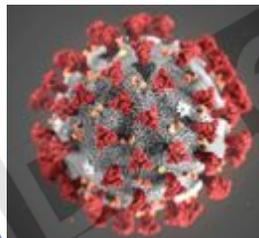


Resiliency Plan  
Activation

刘庆宇  
数据保护首席架构师  
戴尔科技集团

2021-3-27

# 黑天鹅还是灰犀牛



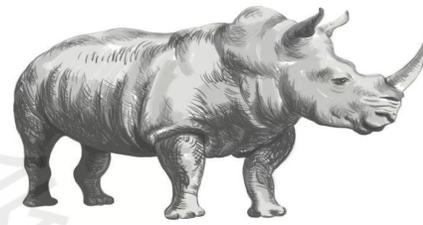
早在公  
天鹅比  
much lik

“黑天鹅”这一术语是美国经济学家纳西姆·尼古拉斯·塔勒布在2001年创造的。

遗传多样的蝙蝠  
SARS样冠状病毒

2012年希腊金融危机后发  
，而是一系列预警和明显征兆（a series of  
and visible evidence）之后爆发出来的问题。灰犀  
个袭击时，极具爆发力，且不可阻挡

# 灰犀牛正在来的路上



2020

2019

2018

2017

2016

2015

TeslaCrypt 勒索软件  
瞄准的是主要游戏平台的  
玩家们  
Chimera 2015-9月份首  
次出现，但已经推出了勒  
索软件服务商业模式，从  
中收取客户50%的利润。  
比较有趣的是，他们招募  
的勒索软件运营人员主要  
是他们的受害者

Ransom32 赎金高达13比特币

Locky 登上了多家报纸头条。威胁行为人马上  
发现，感染医疗保健必备设施的相关系统会  
带来巨大收益，因为多家医院都立即支付了  
赎金

SamSam 包含了一个信道，可供攻击者通过一个  
.onion 网站与受害者直接实时联系。Petya  
如果其索要的431美元赎金未在7天之内收到，  
赎金金额还会翻倍。

Makto 是第一款利用Crypter(加壳器)加密自  
身源代码的勒索软件Jigsaw《电锯惊魂》系列  
电影里的Jigsaw角色。如果150美元的赎金未  
被支付，它将会每60分钟删除一份文件。另  
外，如果受害者试图终止该进程，或者重启  
机器，它就会马上删除1000份文件

CryptXXX 散布最严重的最新勒索软件变体。  
：反沙箱技术、鼠标活动监测、定制C2通信协  
议、Tor 赎金支付。

ZCryptor 有自繁殖技术，能感染外部设备和  
网络中的其他系统，加密每台机器和共享硬  
盘。  
Ransomware-as-a-Service (RaaS) 的  
兴起

IBM：2016 年勒索软件增长 60 倍，赎金  
规模 10 亿美元  
赛门铁克 个人消费者仍然是勒索软件  
的主要攻击目标 (57%)。但长期趋势表明，  
以企业为攻击目标的勒索软件正在缓慢且  
稳步地增长。

WannaCry 勒索病毒  
全球大爆发，至少  
150个国家、30万名  
用户中招，造成损失  
达80亿美元，已经影  
响到金融，能源，医  
疗等众多行业，造成  
严重的危机管理问题。  
5月12日：全球近74  
个国家受到严重攻击  
24小时内监测到的  
WNCRY 敲诈者蠕虫  
攻击次数超过10W+

台积电芯片制造基地  
遭遇“勒索病毒”，  
损失超过11亿  
波音位于南卡罗来纳  
州查尔斯顿的生产工  
厂遭到了WannaCry  
勒索软件的网络攻击。  
这可以说是近日2018  
年以来，被媒体曝出  
来的首例WannaCry  
勒索病毒攻击案例。  
2018年1月，  
GandGrab 勒索家族  
首次出现

GandCrab 狂赚20  
亿美元金盆洗手  
加拿大两大银行支付  
赎金  
国内多家医疗政府被  
勒索  
CyberEdge 2019年，  
选择支付赎金的受害  
者比例是45%，  
2018年则是39%。

波音/本田/佳能/佳明/  
德国AG SOFTWARE/  
研华/富士康/智利银行/  
阿根廷电信/企业旅行社  
CWT/在线教育巨头  
K12.....  
Ryuk  
RagnarLocker  
DoppelPayme  
.....

# 勒索病毒的发展趋势



2016 比特币均价 \$700

2020 Q4 比特币均价 \$20000

28倍

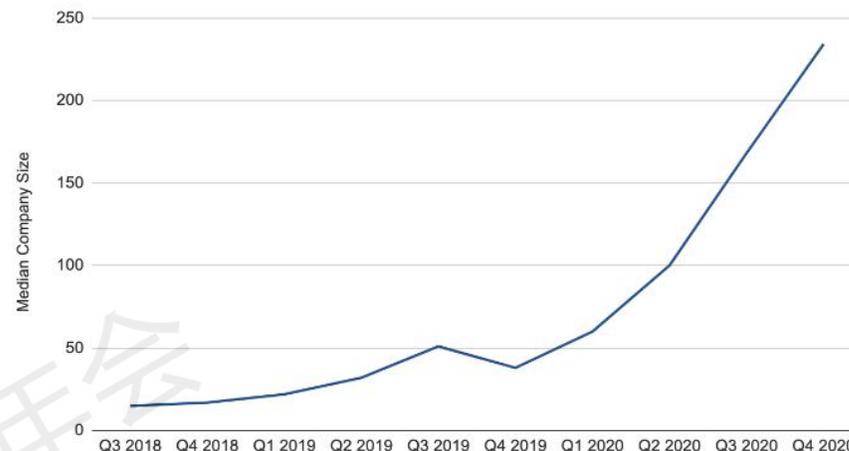
从2015年年末至今，勒索软件的平均赎金增长超过2倍，从294美元增长至679美元。2020 Q4达到15万美元

Palo Alto: 机构平均支付赎金从 2019 年的 115123 美元增加到 2020 年的 312493 美元，同比增长 171%。

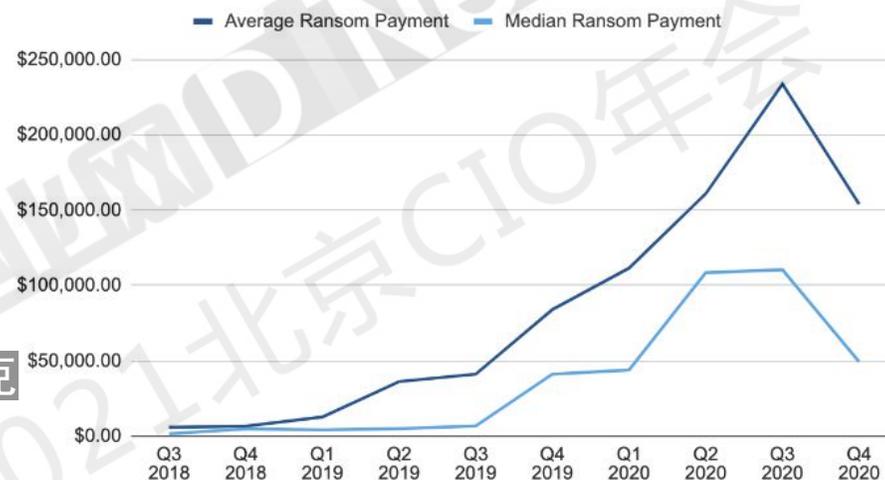
网络犯罪分子已经变得越来越贪婪。

220倍

Median Size of Companies Targeted by Ransomware



Ransom Payments By Quarter



如果你想避免出现黑天鹅事件，就要先处理好灰犀牛事件-----米歇尔·渥克

# 安全公司给出的建议

深信服发现 Rapid 勒索病毒新变种

国家互联网应急中心

2019年我国互联网网络安全态势...

### 漏洞公告

- 关于防范黑客通过仿冒“ETC在线...”
- 关于Microsoft远程桌面服...
- 国家互联网应急中心开通Wanna...
- 关于MongoDB数据库不当配置...
- 关于境内大量家用路由器DNS服务...
- 关于一种新型勒索病毒有关情况的通报

### 恶意代码

- 关于一种新型勒索病毒有关情况的通报
- 一例境外滥用我国境内网络资源发...
- 关于软件下载站传播计算机恶意程序...
- 安卓“勒索”病毒的威胁信息共享通报
- 可用于诈骗的“相册”类安卓恶意程...

### 其他威胁

- 关于近期境外黑客组织拟对我国视频...
- 关于防范网络不法分子利用新型肺炎...

- 及时给电脑打补丁，修复漏洞。
- 对重要的数据文件定期进行非本地备
- 不要点击来源不明的邮件附件，不
- 尽量关闭不必要的文件共享权限。
- 更改账户密码，设置强密码，避免使
- Rapid勒索软件会利用RDP(远程桌面
- 深信服下一代防火墙、终端检测响应
- 深信服下一代防火墙用户，建议升级

同时，

- 及时修复系统漏洞。
  - 采用高强度密码，杜绝弱口。
  - 定期备份重要资料，建议使用
  - 加强安全配置提高安全基
- 135等不用的高危端口等。

用github、CSDN、豆瓣、简书、QQ空间等网站页面作为下发指令的C&C服务器，加密受害者文件并勒索赎金，同时窃取支付宝等软件密码。CNCERT获得火绒、腾讯报送的信息后，立即开展对C&C及下载服务器的协调处置工作。

## 一、勒索病毒介绍

该病毒采用“供应链感染”方式进行传播，通过论坛传播植入病毒的“易语言”编程软件，进而植入各开发者开发的软件，传播勒索病毒；同时，该病毒还窃取用户的账号密码，包括淘宝、天猫、支付宝、QQ等。

该勒索病毒在感染用户计算机后不会勒索比特币，而是弹出微信支付二维码，要求受感染用户使用微信支付110元，从而获得解密密钥，这也是国内首次出现要求使用微信支付的勒索病毒。目前，微信运营商判定该支付二维码存在违规行为，并表示已无法通过扫描二维码支付赎金解密。

## 二、措施建议

在此提醒广大用户及时采取如下措施进行防范：

- 安装并及时更新杀毒软件，目前市场主流反病毒软件都已支持针对该勒索病毒的防护与查杀。
- 不要轻易打开来源不明的软件，该勒索病毒通过易语言编写的程序传播，减少使用来源不明的软件可有效预防。
- 如已经感染勒索病毒，可使用相关解密工具尝试解密。目前，许多公司已经针对该勒索病毒开发了解密工具，包括火绒Berypt专用解密工具、腾讯电脑管家“文档守护者”、360安全卫士“360解密大师”等。（解密工具链接附后）
- 已感染勒索病毒的用户，在清除病毒后，尽快修改淘宝、天猫、支付宝、QQ等敏感平台的密码。
- 定期在不同的存储介质上备份计算机中的重要文件。

其次，定期数据备份。数据备份和数据恢复，而复任务。

最后，采用具有未知威胁检测能力的安全产品和方案，实时检测和阻断勒索软件的入侵。勒索软件和APT威胁检测手段，被勒索软件的“阶段式”攻击轻松绕过。因此，需要引入未知威胁能力检测的产品，比如沙箱类分析这些行为之间的关联关系，判断其是否为勒索软件。

## 4.勒索软件检测和防御

安全意识培训和数据备份，前者是在勒索软件诱骗之前，后者防备勒索中招之后。绿盟科技高级威胁分析产

文件一旦进入本地，就会自动运行。接下来，它会连接到C&C服务器，进而上传本机信息，私钥的攻击者本人，其桌面等明显位置生成勒索，对常规的杀毒软件都具有，对常规的特征检测的安全产品

GandCrab勒索病毒家族的总结

APT邮件网关，可全方位守护企业邮箱安全。依托哈勃分析系统的核心技术，学习，御界防APT邮件网关通过对邮件多维度信息的综合分析，可迅速识别AP邮件、病毒木马附件、漏洞利用附件等威胁，有效防范邮件安全风险，保护企业损失。

(图：腾讯御界防APT邮件网关)

对于普通个人用户，腾讯安全反病毒实验室负责人、腾讯电脑管家安全专家马劲松建议，不要轻易打开来历不明的文件和邮件附件，及时安装操作系统漏洞补丁。此外，腾讯电脑管家“文档守护者2.0”功能，通过对系统引导、边界防御、本地防御执行保护、改写保护、备份等多个环节的保护构建完整的防御方案，能够全面抵御勒索

# 安全体系不能100%防住勒索病毒

## 传统备份成为勒索病毒绕不开的一道坎

勒索方证实，他们于11月29日袭击了富士康在北美的工厂，但并未袭击整个公司。

作为此攻击的一部分，威胁人称，已加密了约1,200台服务器，并删除了20-30 TB的备份。

### BY THE FBI MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud;  
Intentional Damage to a Computer



#### DESCRIPTION

<b>Aliases:</b> Maksim Yakubets, "AQUA"	<b>Place of Birth:</b> Ukraine
<b>Date(s) of Birth Used:</b> May 20, 1987	<b>Eyes:</b> Brown
<b>Hair:</b> Brown	<b>Weight:</b> Approximately 170 pounds
<b>Height:</b> Approximately 5'10"	<b>Race:</b> White
<b>Sex:</b> Male	



Garmin官方微博

7月28日 18:42 来自 微博 weibo.com  
Garmin 系统和服相关公告

尊敬的用户您好:

我们诚挚地宣布，目前暂停运作的 Garmin 系统和服，包括 Garmin Connect 国际服务器相关服务等，已陆续恢复运行。由于目前我们仍在处理部分数据资料，因此某些功能暂时仍然不可用。我们真诚地感谢所有用户的耐心配合与理解!

2020年7月23日，我们受到了网络攻击，导致我们许多在线服务受到了影响，包括网站功能、客户服务支持、终端应用程序和公司通讯等。Garmin 高度重视数据安全与客户服，因此我们当下立即评估了攻击的性质、危害的范围并紧急开启了应对措施。



Products Mandiant Solutions Customers

## Threat Research

### Unauthorized Access of FireEye Red Team Tools

December 08, 2020 | by FireEye

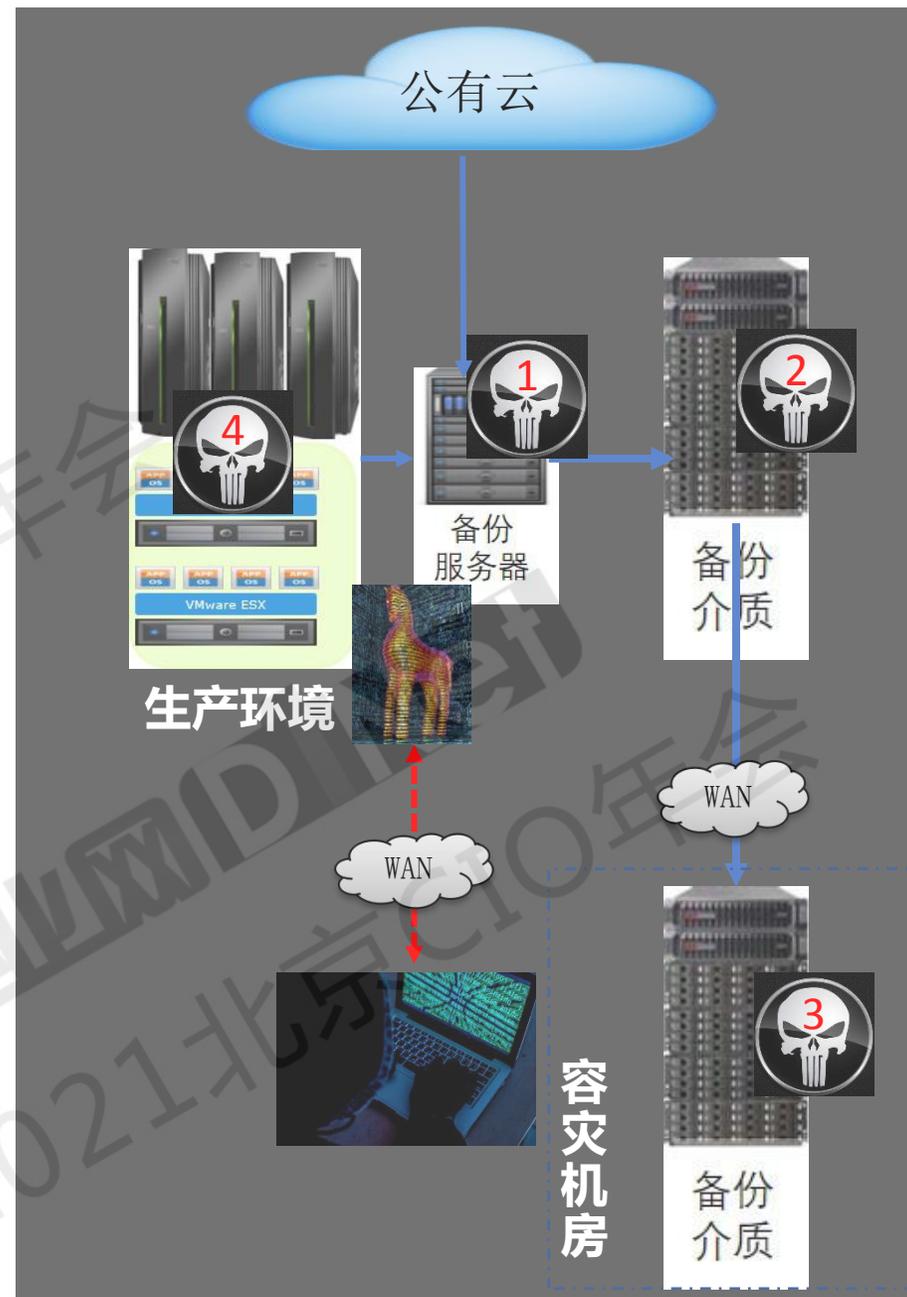
FIREEYE TOOLS RED TEAM

#### Overview

A highly sophisticated state-sponsored adversary stole FireEye Red Team tools. Because we believe that an adversary possesses these tools, and we do not know whether the attacker intends to use the stolen tools themselves or publicly disclose them, FireEye is releasing hundreds of countermeasures with this blog post to enable the broader security community to protect themselves against these tools. We have incorporated the countermeasures in our FireEye products—and shared these countermeasures with partners, government agencies—to significantly limit the ability of the bad actor to exploit the Red Team tools.

You can find a list of the countermeasures on the FireEye GitHub repository found [HERE](#).

Red Team Tools and Techniques



# 人们不去做一件事的原因之一就是，他们觉得自己没有那么大的力量改变事物

-----米歇尔·渥克

WSJ Banks Build Line of Defense for D... x

wsj.com/articles/banks-build-line-of-defense-for-doomsday-cyberattack-1512302401

THE WALL STREET JOURNAL

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ Magazine

Subscribe | Sign In

Search

By [Tetis Demos](#)  
Dec. 3, 2017 7:00 am ET

PRINT TEXT

48

U.S. banks have quietly launched a doomsday project they hope will prevent a run on the financial system should one of them suffer a debilitating cyberattack.

The effort, which went live earlier this year and is dubbed *Sheltered Harbor*, currently includes banks and credit unions that have roughly 400 million U.S. accounts. The effort requires member firms to individually back up data so it can be used by other firms to serve customers of a disabled bank.

While most people worry about their money being stolen in a hack, banks fear something more sinister: an attacker destroying, or even simply locking, data.

Such moves could cripple a bank, leaving it unable to operate for hours, days, or perhaps much longer. If people suddenly can't access their accounts and money at one bank, customers at other banks could panic, thinking they might be vulnerable, too. This could prompt them to withdraw funds as a precaution and, in a worst-case scenario, spark a run on the wider banking system.

"So far, most people think about cyber in terms of having a credit card stolen," said Stuart Madnick, a professor of information technologies at the MIT Sloan School of Management. "What you're talking about now is a nuclear attack: If you can't get to the ATM and get it to work."

TO READ THE FULL STORY

**MOST POPULAR NEWS**

1. What You Can and Can't Do if You've Been Vaccinated: Travel, Risk Factors, What You Need to Know
2. Two Men Charged in Assault on Officer Slicknick During Capitol Riot
3. Hasland Confirmed as Interior Secretary in First for Native American
4. The Pandemic Ignited a Housing Boom—but It's Different From the Last One
5. Germany, France, Italy Suspend Use of AstraZeneca's Covid-19 Vaccine

**MOST POPULAR OPINION**

1. Opinion: Andrew Cuomo Becomes Expendable
2. Opinion: Come Back to Florida for Spring Break
3. Opinion: The Biden Border Mess

国家互联网应急中心

cert.org.cn/publish/main/98/2017/20171215154431361111976/20171215154431361111976\_.html

积极预防 及时发现  
快速响应 力保恢复

网站地图 RSS订阅 English 邮件订阅

搜索

首页 威胁预警 态势报告 新闻资讯 CERT在线 CERT讲堂 应急体系 关于我们

**CNERT动态**

- 国家互联网应急中心2020年网络...
- CNERT/CC圆满完成202...
- 国家信息安全漏洞共享平台2019...
- 关于2019中国网络安全技术对抗...
- 2019亚信非政府论坛第三次会议...

更多>>

**国内要闻**

- 关于印发《App违法违规收集使用...
- 国家互联网信息办公室关于《网络安...
- 国家互联网信息办公室关于《个人信...
- 中央网信办等四部委联合开展互联网...
- 第七届中英互联网圆桌会议成果文件...

更多>>

**国际新闻**

**美银行建防御系统：备份数据应对网络攻击影响**

来源：中新网 时间：2017-12-15

中新网12月4日消息 据外媒12月4日报道，美国银行业推出了一个应对末日网络攻击的计划，希望在一家银行遭到严重网络攻击时，避免整个金融系统受到波及。据报道，目前参与进来的银行和信用联盟总共拥有约4亿账户，参与这项计划的银行，需根据自身规模每年支付250美元到25000美元不等的费用。

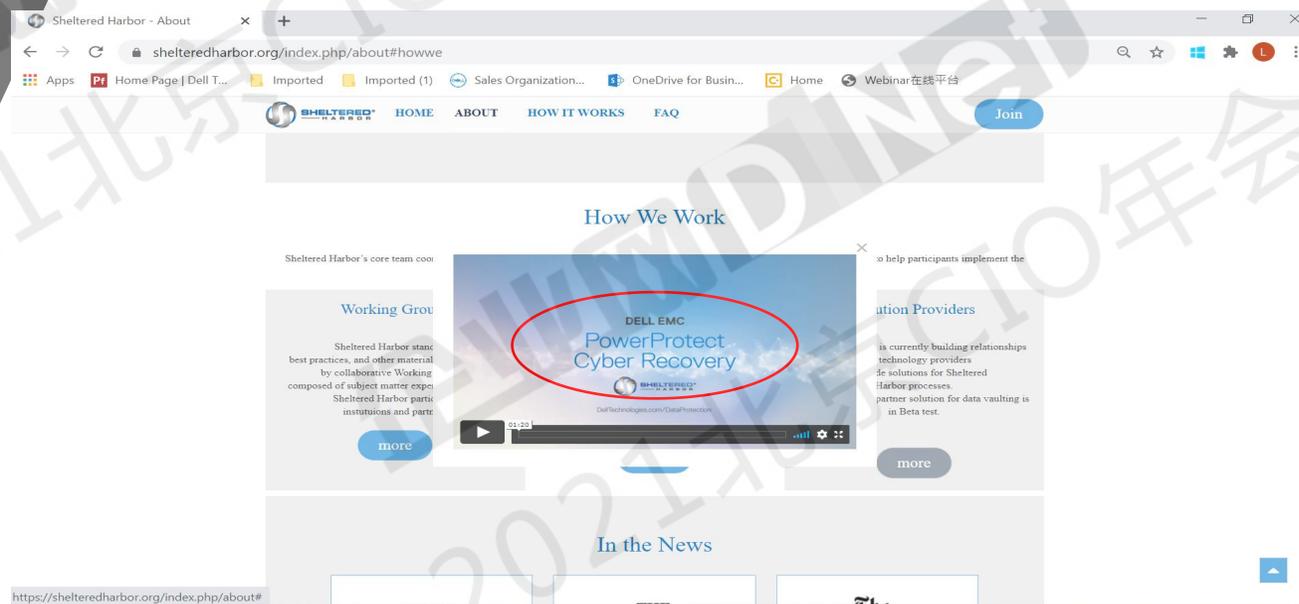
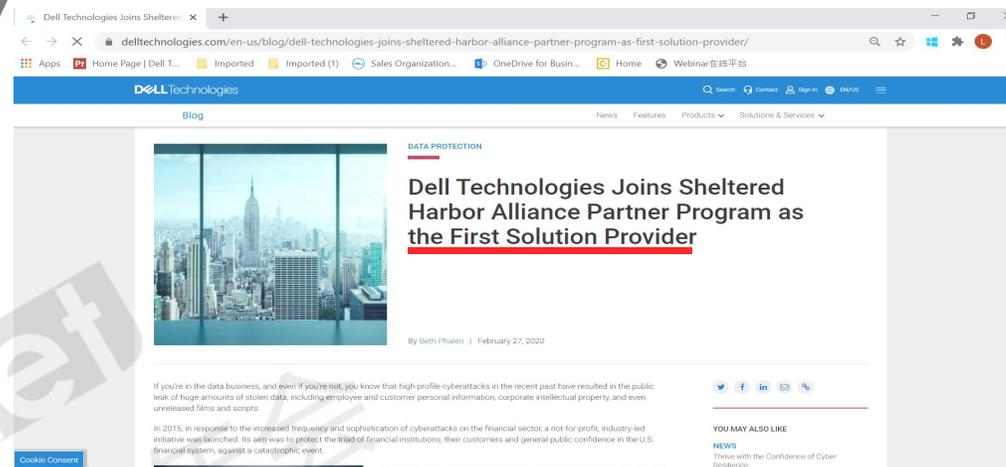
据悉，这项名为Sheltered Harbor的计划在今年早些时候启动，目前参与进来的银行和信用联盟总共拥有约4亿账户。该计划要求成员公司各自备份数据，以便在某家银行的网络陷入瘫痪时，其他公司可以使用备份数据为其客户提供服务。

在遭到黑客攻击时，多数人担心的是钱财被窃，但银行担心的事情更为凶险，那就是攻击者毁坏或锁住数据。这类行动可能让一家银行陷入瘫痪，使其在几小时、几天、甚至更长时间内无法开展业务。

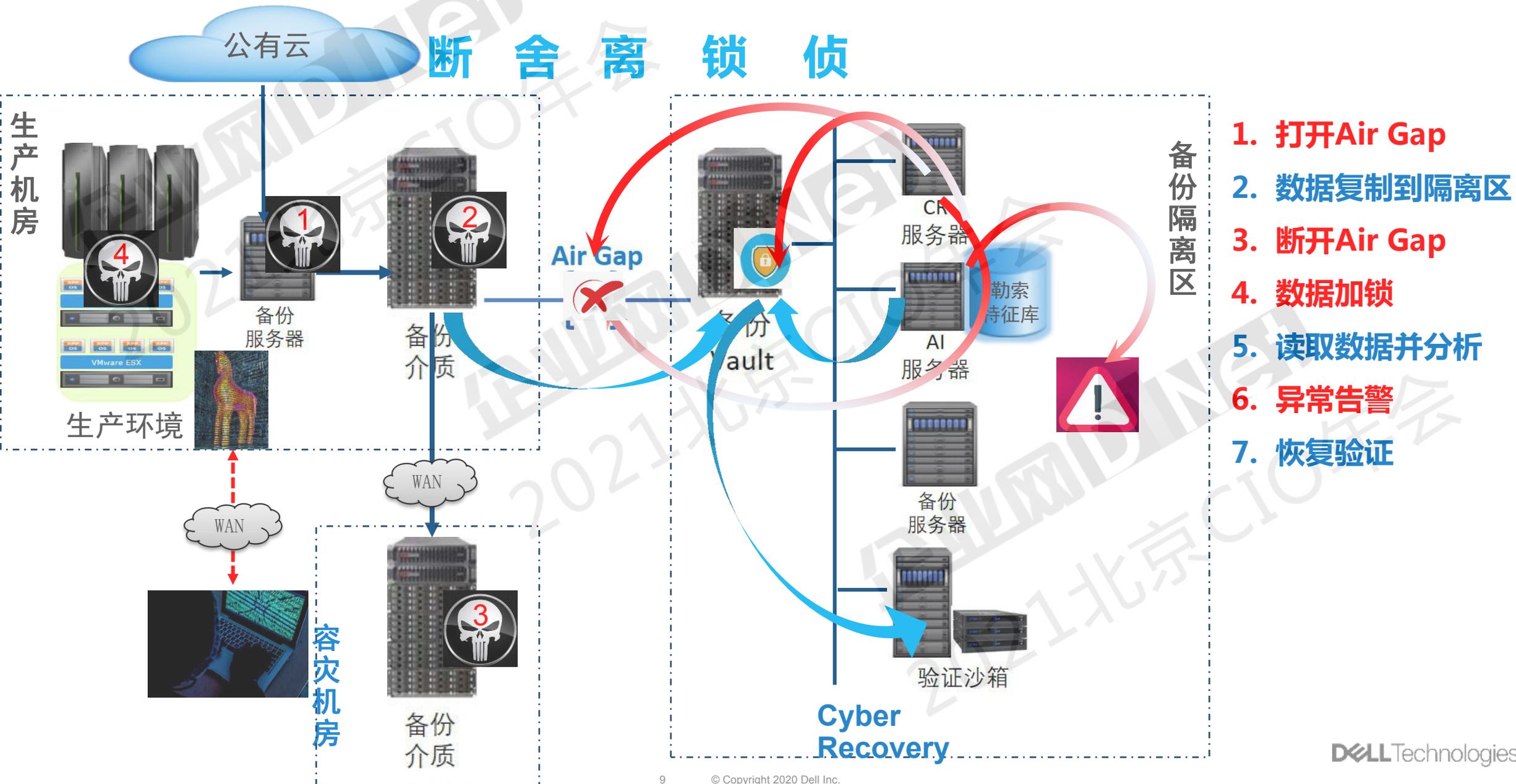
同时，报道称，如果某家银行的客户突然无法进入自己的账户并获取资金，其他银行的客户可能会跟着恐慌，担心自己的账户和资金也不安全，为了防患于未然而取出资金，在最坏的情境下，风波会蔓延至更广泛的银行系统。

据报道，令银行尤其不安的是，美国政府可能难以抑制黑客袭击造成的恐慌。

# DELLEMC 成为避风港计划 第一个也是唯一入选的 解决方案供应商



# 流程是功能实现的保障

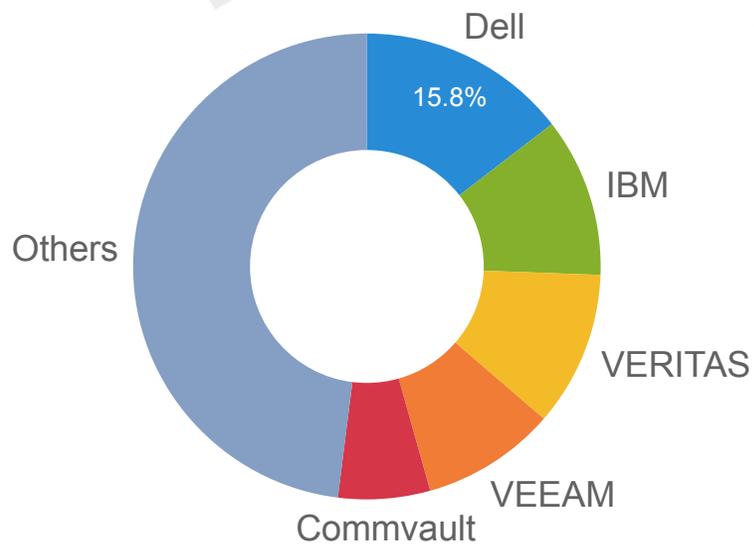


# DELLEMC - 数据保护领域领导者

**20年** Gartner魔力象限领导者

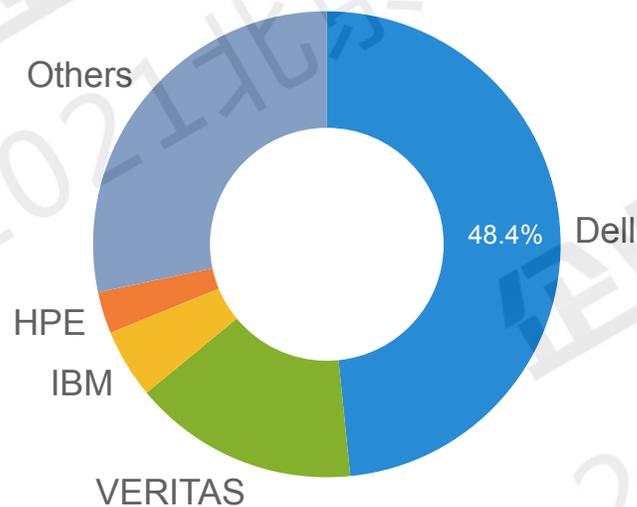


软件全球市场份额第一 @15.8%



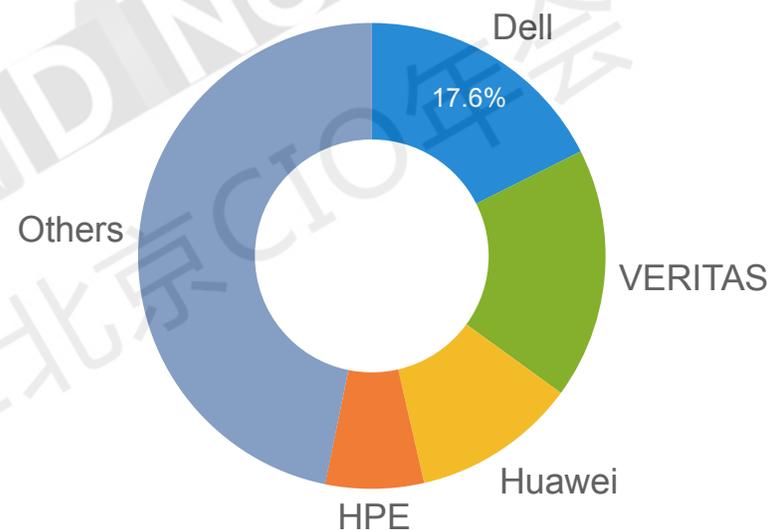
来源：IDC 2020Q2 Storage SW QView, Sept 2020;

PBBA全球市场份额第一 @48.4%



来源：IDC 2020Q2 PBBA Tracker, Sept 8 2020

PBBA大中国区市场份额第一 @17.6%



来源：IDC 2020Q2 PBBA Tracker, Sept 8 2020

# 在中国，为中国

## 戴尔科技集团中国研发集团



数据来源: 2019年《中国科技统计年鉴》

长江大讲堂

CKGSB Dialogue: The Gray Rhino

如何驯服危险的“灰犀牛”

- 一. 承认危机的存在。
- 二. 定义灰犀牛式危机事件的性质。
- 三. 不要静立不动。
- 四. 不要浪费危机。
- 五. 站在顺风处。最好的领导会在危险尚未靠近的时候就采取行动。

当危险只远在天边，人们就需要提前制订一系列的计划。

- 六. 成为发现灰犀牛式危机的人，成为控制灰犀牛式危机的人。

米歇尔·渥克