Lenovo
NetApp

勒索病毒最新趋势及应对措施

丽达
联想凌拓产品经理

2021 Lenovo NetApp. All rights reserved.

2020年勒索病毒造成了多少损失?

2020最大一笔被勒索的赎金是?

WHAT WAS THE LARGEST RANSOMWARE DEMAND?

10 MILLION EUROS

The largest 2020 ransomware demand, totaling around $11.8 million, made to French construction firm Bouygues.

AVERAGE RANSOM DEMAND

The average demanded ransom in 2020 was around $178,000. The average requested ransom for small businesses, though, was only $5,900.

Cloudwards

勒索病毒的成功率有多少?

平均每起勒索事件造成多少损失?

2021 Lenovo NetApp. All rights reserved.

最常见的勒索病毒感染方式

2021 Lenovo NetApp. All rights reserved.

预计未来勒索攻击的方向是?

FUTURE PREDICTED TRENDS IN RANSOMWARE ATTACKS

IoT devices

IoT devices will become a more prominent attack vector

Social media

While social networks beef up internal security, tainted links targeting users will increase in numbers

Utility infrastructure

Critical infrastructure will be targeted more, in efforts to have a better chance of ransom payment.

2021 Lenovo NetApp. All rights reserved.

2020年知名勒索病毒大事件

*本信息来自于网络新闻媒体

2021 Lenovo NetApp. All rights reserved.

台湾电子巨头富士康在今年2020年最后一个感恩节周末期间，其墨西哥工厂遭遇勒索软件攻击。此后，Bleeping Computer表示，黑客要求用比特币支付3470万美元的巨额赎金。

富士康被认为是全球最大的电子制造公司。Bleeping Computer指出，该公司仅在2019年就拥有1720亿美元的收入。这家科技公司旗下还拥有超过80万名员工。

2021 Lenovo NetApp. All rights reserved.

*本信息来自于网络新闻媒体

据《计算机周刊》报道，2月17日的勒索软件攻击迫使总部位于丹麦的设施管理公司ISS World关闭网络，并使数十万员工无法访问他们的系统和电子邮件。三天后，ISS World表示，攻击的根本原因已经查明，公司正在与外部专家合作，逐步恢复我们的IT系统。

到3月20日，ISS世界公司表示，它已经重新获得了大部分IT基础设施的控制权，并正在系统地重新启动关键业务系统，尽管功能有所减少。ISS表示，它预计到2020年底将完成系统和IT资产的恢复和重建。

ISS预计将花费4500万至7500万美元用于：补救IT事件；采取变通措施，以实现服务的持续交付；因系统宕机而导致的服务表现不佳；以及与合同运营相关的成本重复。由于该公司的一些信息技术资产遭到破坏，重建基础设施服务社的部分信息技术基础设施，预计将花费2 250万美元至4 500万美元。

2021 Lenovo NetApp. All rights reserved.

*本信息来自于网络新闻媒体

在4月份，IT服务巨头--Cognizant承认，该公司曾面临勒索软件的攻击。这家IT巨头透露，其网络已经感染了Maze勒索软件，这是一个勒索软件集团，如果受害者不支付解密费用，就会向公众释放被盗数据。

据消息人士透露，预计在2020年第二季度，勒索软件攻击带来的收入和相应的利润影响将在5000万至7000万美元之间。

2021 Lenovo NetApp. All rights reserved.

*本信息来自于网络新闻媒体

“勒索行业”趋势

*本信息来自于网络新闻媒体

2021 Lenovo NetApp. All rights reserved.

2020年的6个勒索软件趋势

勒索软件泄露不合规受害者的数据

不同勒索软件家族之间的合作日渐增多。

与其他类型恶意软件的协调

专题事件的武器化

越来越多的逮捕涉及勒索软件的行为人

Deepfake勒索软件。未来的勒索软件?

2021 Lenovo NetApp. All rights reserved.

2021年勒索软件三大趋势值得关注

越来越多的VIP暗网论坛被用来做数据泄露的广告

为每一次泄漏建立专门的网站

手机是最新的武器?.....没有什么比接到勒索软件团伙的电话更刺激的了，他们掌握着你公司泄露的数据。

2021 Lenovo NetApp. All rights reserved.

我们该如何应对?

*本信息来自于网络新闻媒体

2021 Lenovo NetApp. All rights reserved.

我们通常如何应对?

- 确保您的反病毒软件是最新的
- 了解整个网络正在发生什么
- 扫描和过滤电子邮件
- 制定计划以应对勒索攻击并进行测试
- 付赎金之前，请考虑…
- 最重要的数据建立有效的备份
- 了解您的网络连接
- 让勒索病毒游览你的整个网络变得更困难
- 培训人员以识别可疑邮件
- 更改所有访问点的默认密码
- 应用软件补丁以保持系统最新状态
- 请勿随便插入U盘

Lenovo NetApp

2021 Lenovo NetApp. All rights reserved.

仅靠备份软件不够吗?

2021 Lenovo NetApp. All rights reserved.

传统方式应对勒索病毒的局限性

传统备份软件如何打击勒索病毒？唯一的答案：从备份中恢复受感染的系统。

备份软件厂商通常使用一些有关将勒索病毒隔离出生产系统并尽量减少攻击造成的损害的建议，来包装此解决方案，包括：

•缩短备份间隔，增加全备份次数，并遵循3-2-1备份规则：将备份存储在不同的介质上，并将其保留在不同的位置，至少一个副本位于异地，通常在云存储中（带来使用成本的增加）

•培训用户避免最常见的勒索软件陷阱，如在网络钓鱼电子邮件中打开链接和附件（主观操作不确定因素大）

•定期修补操作系统和应用程序，以关闭勒索病毒可以利用的已知软件漏洞作为攻击媒介（增加了业务中断的可能性和停机时间）

•部署硬件防火墙等端点防御，以检测和阻止广为人知的勒索病毒（增加了额外的部署成本）

•使用网络分段隔离技术（如VLAN）阻止某些勒索病毒变体在生产网络中传播蠕虫功能（增加了网络拓扑图的复杂程度）

2021 Lenovo NetApp. All rights reserved.

传统方式应对勒索病毒的局限性

固然这些都是有效的方案，然而它们并没有解决大多数传统备份软件应对勒索病毒方面非常有限这一事实。

首先，大多数勒索病毒制造者都明白，一个执行良好的备份计划的公司将更抗拒支付赎金：他们将从过往的备份中还原他们受感染的系统以恢复生产环境。为了削弱备份作为反勒索策略的有效性，新的勒索病毒不仅加密用户的文件，还会主动攻击备份代理和备份存储库。而受勒索病毒感染的备份，在恢复生产系统时毫无用处，因此受害者更有可能支付赎金。

某些供应商提供轻度的防御，防止对备份的勒索软件攻击，例如，拒绝从备份程序以外的所有进程写入保护备份路径，或以其他方式限制对备份存储库的访问并保持脱机状态。

一些供应商提供的附加功能是，每天检查系统上的文件，以查看是否发生了任何看起来像遭受勒索病毒攻击的可疑情况，并发送警报到备份控制台（如果有）。（当大多数 IT 操作人员注意到这样的不频繁警报时，攻击可能已经蔓延到本地网络上的所有其他终结点。）

2021 Lenovo NetApp. All rights reserved.

传统方式应对勒索病毒的局限性

某些供应商还会吹嘘其备份和恢复功能的全面性和速度：我们备份您的所有系统，我们有许多方法可以加快恢复过程。

这些确实很重要，然而从遭受攻击中快速、完整地恢复意味着需要更多的业务中断时间。

更糟糕的是，这些问题仍无从解决：

•在遭受勒索病毒的攻击后，检测、遏制、恢复、清理和攻击后取证、分析及报告期间，对业务运营产生的破坏性影响。

•重新创建自上次备份以来丢失的业务数据的成本。

•导致违反合规性、要求向当局和客户报告安全漏洞的攻击后的业务和声誉成本。例如，根据欧盟严格的最新数据保护条例，遭遇勒索病毒攻击构成对私人用户数据的侵犯。

•有可能再次遭受勒索病毒攻击，开始又一个代价高昂的受感染和响应周期。

2021 Lenovo NetApp. All rights reserved.

联想凌拓推荐如何应对?

2021 Lenovo NetApp. All rights reserved.

我们通常如何应对?

- 确保您的反病毒软件是最新的
- 了解整个网络正在发生什么
- 扫描和过滤电子邮件
- 制定计划以应对勒索攻击并进行测试
- 付赎金之前，请考虑…
- 最重要的数据建立有效的备份
- 了解您的网络连接
- 让勒索病毒游览你的整个网络变得更困难
- 培训人员以识别可疑邮件
- 更改所有访问点的默认密码
- 应用软件补丁以保持系统最新状态
- 请勿随便插入U盘

Lenovo NetApp

2021 Lenovo NetApp. All rights reserved.

我们通常如何应对?

数据集中

离线备份以防万一

统一防护

备份文件及应用

2021 Lenovo NetApp. All rights reserved.

联想凌拓防勒索病毒解决方案

DPA备份一体机

应用保护

TS系列磁带产品

离线保护

- 备份系统
- 长期归档数据

服务器端

（应用系统、数据库、虚拟化等）

*.*locked
*.*kraken
*.*crypto
*.*cry
*.exx

黑名单

.pdf
.xls
.doc
.jpg
.giv

白名单

Pattern:
SMB…
SMB…
SMB…
SMB…

深度学习

Crypto Spike

文件保护

- 黑白名单拦截勒索病毒
- 深度学习防范可疑用户（疑似感染病毒用户）
- 基于用户或文件类型快速恢复单个/多个文件

CIFS/NFS

客户端

（终端客户，Windows/Linux）

保护/物理链接

链接

防止勒索病毒白皮书免费下载

2021 Lenovo NetApp. All rights reserved.

联想凌拓防勒索病毒解决方案

2021 Lenovo NetApp. All rights reserved.

CS如何屏蔽勒索病毒

黑名单

- 阻止已知的勒索软件签名和文件类型
- 自动更新
- 过滤器也可以手动添加

白名单

- 阻止所有文件（允许的文件列表除外）
- 安全性好，但限制文件类型
- 在细粒度应用时有效（例如，会计文件夹仅允许Excel文件）

深度学习模式

- 监视文件系统上的用户行为以检测Day-one threat
- 检测异常行为（例如一段时间内写入的文件过多）并切断用户访问权限

2021 Lenovo NetApp. All rights reserved.

颗粒保护策略

- 可以应用颗粒策略
- 整个阵列的单个策略，或在SVM，卷，文件夹级别的自定义
- 允许不同的小组要求
- 例如: 工程文件夹允许.exe文件，但可以从市场营销文件夹中阻止它们

Lenovo NetApp All rights reserved.

用户阻止和文件恢复

阻止危险用户

- 勒索软件与受感染的用户相关
- 通过调用Ontap FPolicy服务器阻止了用户（阻止=设置为只读文件系统访问）

目标文件恢复

- CS识别受感染的文件
- 使用DM/FAS快照一键式恢复受感染文件
- 无需回滚整个卷或文件夹

用户修复

- 确定受感染的用户
- 这使IT安全团队可以从网络中提取受感染的设备并采取补救措施

2020 Lenovo NetApp. All rights reserved.

联系我们

官方网站： www.lenovonetapp.com

官方微信： 联想凌拓

官方Bilibili公众号： 联想凌拓空中沙龙

服务热线： 400-828-3001（服务与技术支持）

400-116-0099（销售热线）

Lenovo NetApp

2020 Lenovo NetApp. All rights reserved.