HongKe 虹科

启用指南

启用LEPIDE进行勒索软件防护

目录

1 导言 3
2 针对勒索软件调整 Lepide 3
3 Lepide核心能力 6
3.1 - Lepide 识别 6
3.2 - Lepide 信任 7
3.3 - Lepide 审计 8
3.4 - Lepide 检测 9

1 导言

勒索软件可以说是目前最紧迫、最具潜在破坏性的安全威胁。

勒索软件是指对公司数据进行加密、勒索赎金并在支付赎金后释放数据的软件。

勒索软件通常从网络钓鱼电子邮件开始，导致 Active Directory 账户泄露，然后利用该账户在企业网络中传播。

然后，它会试图提升其访问权限，以访问更多数据，从而造成最大程度的破坏。

在所有情况下，勒索软件都依赖 Active Directory 作为其在网络中移动的手段，而且几乎在所有情况下，受勒索软件影响的数据都涉及存储在企业数据存储区（如 Windows 文件服务器、OneDrive 或 SharePoint）中的数据。

凭借我们对 Active Directory 和这些企业数据存储的深入而独特的了解，使用 Lepide 可以让客户以更快的速度检测、响应和限制勒索软件攻击造成的损害。

2 针对勒索软件调整 Lepide

为了能够检测、预防、调查和响应勒索软件攻击，您需要能够回答一些关键问题

在下表中，我们将lepide技术与这些问题结合起来:

类别	应采取的行动	实施技术
检测	检测特定用户账户的用户行为变化	异常检测和分析 (Lepide 检测)
	检测“大规模”加密事件发生在文件服务器，OneDrive等	

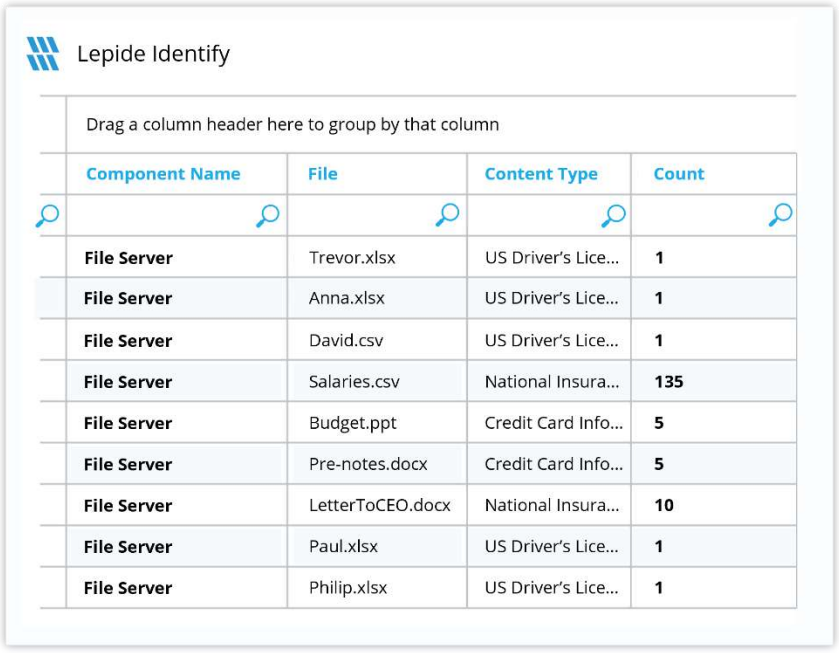
	检测特定用户帐户的权限升级 检测看起来异常的访问尝试失败的多个实例 快速检测试图访问大量数据的用户或用户组	潜在勒索软件攻击威胁模型 (Lepide 检测) 权限升级(组)威胁模型 (Lepide 检测)
预防	仅根据需要限制数据访问，从而减少攻击面	非活动用户报告 (Lepide 审计) 用户权限过多报告 (Lepide 信任) 用户权限报告 (Lepide 信任) 有管理权限的用户报告 (Lepide 信任) 公开股份 (Lepide Trust) 数据分类 (Lepide Identify) I增加威胁表面积威胁模型 (Lepide 检测)
调查	识别潜在的威胁来源，而不必依赖于Windows事件日志 根据受影响用户的访问权限，查看哪些数据可能受到威胁的影响	文件服务器中的所有修改 (Lepide 审计) 潜在勒索软件攻击威胁模型 (Lepide 检测

		文件重命名 (Lepide 审计) 读取失败 (Lepide 审计) 用户权限报告 (Lepide 信任) 用户权限过大 (Lepide 信任)
回应	检测到勒索软件攻击症状时自动做出响应 指示您的 SIEM 或 SOAR 平台根据这些行为进行参与 使用移动设备在非工作时间应对此类威胁	带有自动脚本的潜在勒索软件攻击威胁模型 (Lepide 检测) SIEM 集成 (Lepide 检测) 使用自动脚本向手机 应用程序发出警报 (Lepide 检测)

3 Lepide 核心能力

3.1 - Lepide Identify

在创建时自动扫描、发现数据并进行分类，帮助您随时掌握敏感数据的位置。利用近距离扫描技术消除误报。与大多数分类解决方案相比，这有助于进一步提高准确性。根据合规性、风险、发生率、货币价值等因素对数据进行分类和评分，随时掌握最敏感的数据。

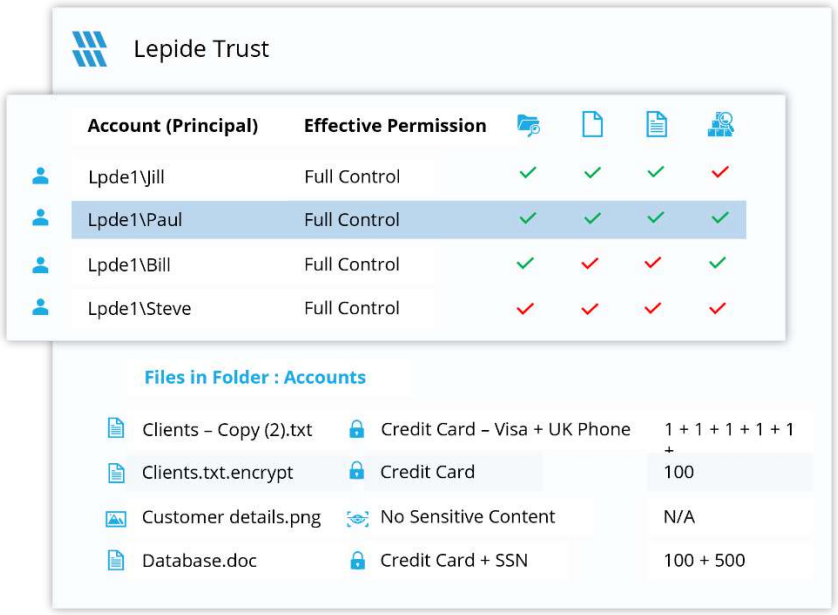


总之：

- 在真实 Tag 数据中发现数据并对其进行分类。
- 数据估值。
- 识别风险最大的数据。

3.2 - Lepide 信托基金会

报告谁可以访问最敏感的数据，以及他们是如何被授予访问权限的。针对权限过大的用户的特定报告能让你发现哪些用户最有可能成为内部威胁。在权限发生变化时及时发现并逆转，从而维护零信任策略。

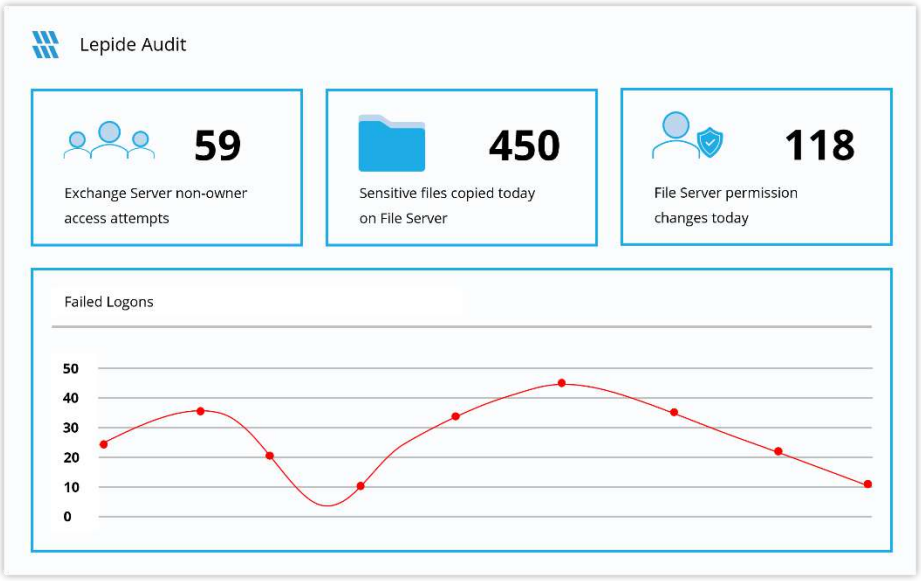


总之：

- 分析权限。
- 识别特权过大的员工（最小特权）。
- 查看历史许可。
- 跟踪权限更改。

3.3 - Lepide 审计

对敏感数据和混合环境所做的更改进行审计、报告和警报。回滚不需要的更改并恢复已删除的对象，以维护系统的完整性。跟踪用户对关键文件和文件夹所做的任何更改和修改。

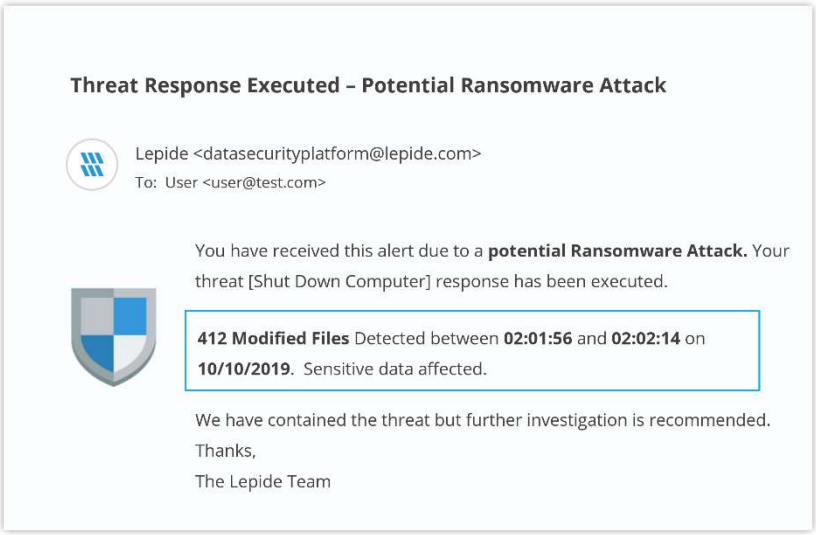


总之：

- 查看与数据的交互。
- 查看与管理数据访问的系统之间的互动。
- 员工审计日志。
- 调查事故和违规情况。

3.4 - Lepide Detect

机器学习支持的异常点发现技术可让您确定用户何时成为内部威胁。针对特定数据安全威胁定制的数百种威胁模型可在数据安全受到威胁时生成实时警报。可触发自动威胁响应，执行威胁缓解措施，如关闭受影响的计算机或服务器。



总之：

- 利用预定义的威胁模型实时检测威胁。
- 员工行为基准/档案。
- 识别异常员工行为。
- 实时警报并应对威胁。

HongKe 虹科

虹科电子科技有限公司

www.haocst.com
network@hkaco.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼1-7层

T (+86) 400 - 999 - 3848
M (+86) 135 3349 1614

各分部：广州 | 成都 | 上海 | 苏州 | 西安 | 北京 |
台湾 | 香港 | 日本 | 韩国 | 美国硅谷

版本：V1.0 - 23/09/07

联系我们

获取更多资料

haocst.com