李先生 您好:

感谢您的电话接听。

确认您的问题已经解决，我将归档此案例。

工单的归档并不会影响我们为您提供技术支持服务，如有其他问题，您可以随时联系我们。

案例总结：

问题定义：

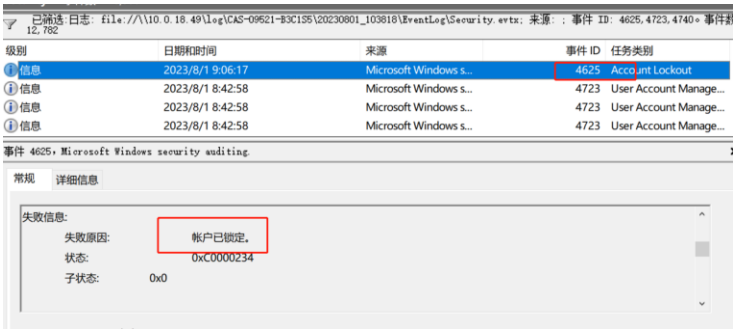
用户反馈单位内部多台电脑出现帐户锁定问题，等待半小时后自动解锁，输入密码可以正常进入系统，需要排查问题原因。

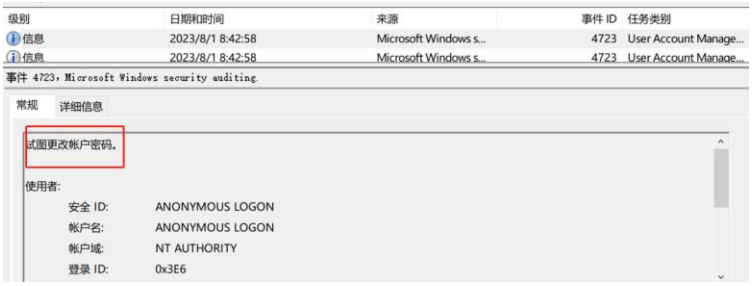
问题总结：

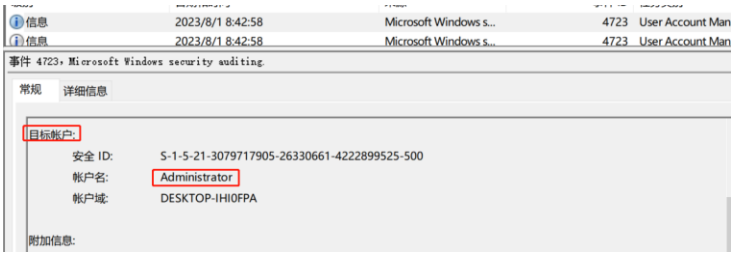
经过排查，确认是瑞星安全软件的密码加固功能导致的帐户锁定，瑞星厂商更新软件版本后解决问题。

问题排查：

在系统的安全日志中，通过筛选事件 ID **4625,4723,4740** 的事件，可以发现是由于有应用在尝试更改 Administrator 帐户的密码失败，触发了 5 次密码错误帐户锁定的功能。







在 8:39 开机到 8:43 的时间段中，记录的 4723 事件有 1 万多条，通常出现这种问题是安全软件在验证密码安全性等类似功能引起的。

建议排查故障机上的各种**安全或者检查软件**，是否有类似的**密码安全性检查**的功能。

以上，如您后续有任何问题，可随时与我们联系，谢谢。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2023 年 8 月 1 日 15:50
收件人: '李先生' <196403@qq.com>
抄送: Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号：CAS-09521-B3C1S5] % 福建省外事服务中心用户需要排查账户锁定原因 % 初次响应 CMIT:0001474

李先生 您好:

Procmon.zip 工具见附件。

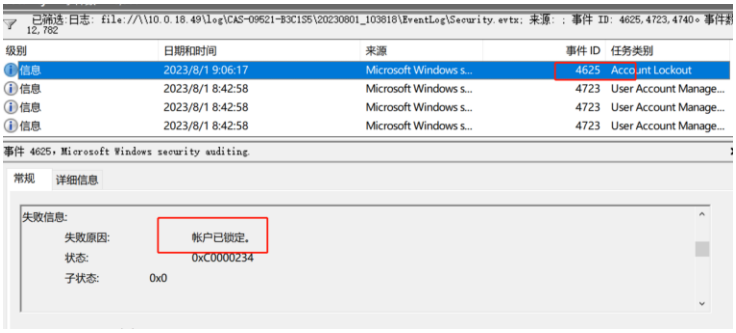
危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

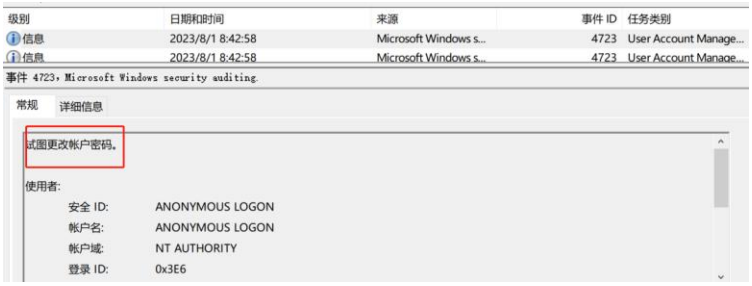
发件人: Wei Liang
发送时间: 2023 年 8 月 1 日 15:48
收件人: '李先生' <196403@qq.com>
抄送: Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号：CAS-09521-B3C1S5] % 福建省外事服务中心用户需要排查账户锁定原因 % 初次响应 CMIT:0001474

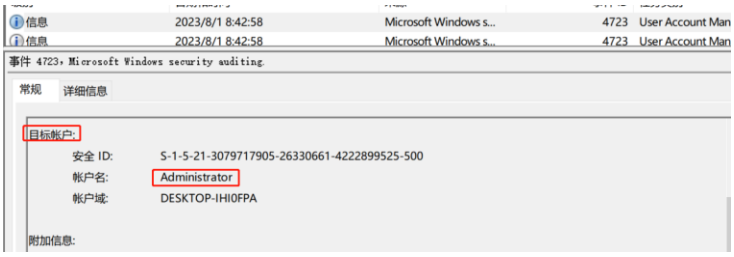
李先生 您好:

感谢您的电话接听。

查看您提供的日志，在安全日志中，通过筛选事件 ID **4625,4723,4740** 的事件，可以发现是由于有应用在尝试更改 Administrator 帐户的密码失败，触发了 5 次密码错误帐户锁定的功能。





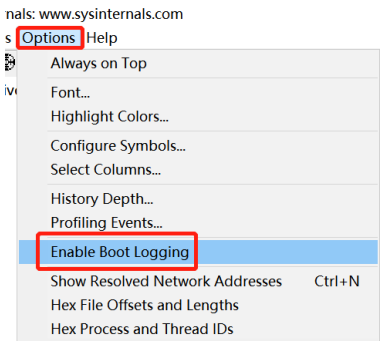


在 8:39 开机到 8:43 的时间段中，记录的 4723 事件有 1 万多条，通常出现这种问题是安全软件在验证密码安全性等类似功能引起的。

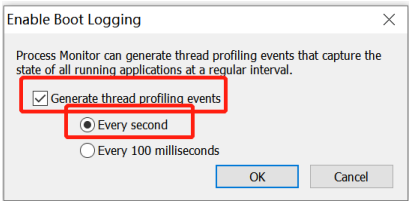
当前的日志无法查找到是谁发起了“试图更改帐户密码”的操作，请您按照以下操作进一步排查并收集相关日志：

1）查看故障机上的各种**安全或者检查软件**，是否有类似的**密码安全性检查**的功能。

2）下载附件中的 procmon.zip 文件，解压后运行 procmon.exe，选中 options->Enable Boot Logging：



3）配置 Boot Logging 选项：



4）**断开网线重启设备，及时登录系统后，等待 5 分钟左右，再运行 procmon.exe**，会弹出窗口提示 boot log 日志已经收集，请点击 Yes 保存，并将文件存储到为 **boot_log.pml，将此日志压缩后**上传。

5）运行 CMGELogCollectorV2.exe，勾选**所有选项**，点击**收集**获取对应的系统日志，将生成的日志压缩包通过 **CDUC** 上传。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

神州网信 CMIT

发件人: Wei Liang
发送时间: 2023 年 8 月 1 日 10:34
收件人: 李先生 <196403@qq.com>

抄送: Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-09521-B3C1S5] % 福建省外事服务中心用户需要排查账户锁定原因 % 初次响应 CMIT:0001474

李先生 您好:

感谢您的电话接听。

根据您提供的信息，我谨在此阐述我们双方针对这个问题所涉及范围界定:

问题定义:

用户反馈单位内部多台电脑出现帐户锁定问题，等待半小时后自动解锁，输入密码可以正常进入系统，需要排查问题原因。

问题范围:

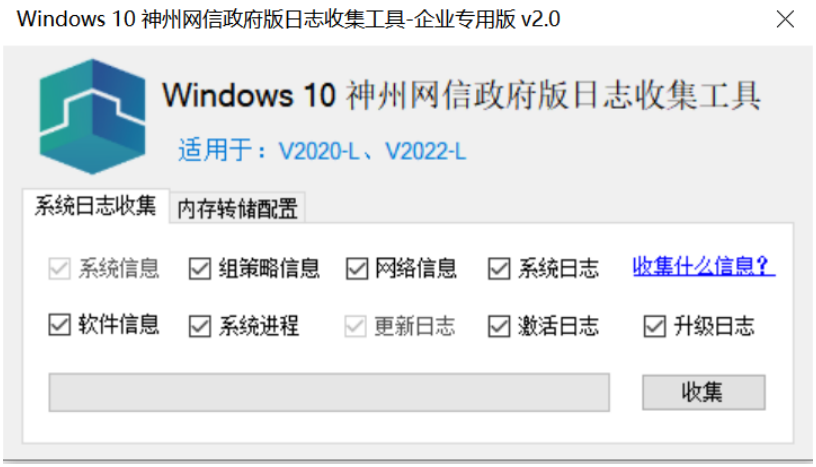
我们将协助您分析处理上述问题，并对定义的问题给予最大的技术支持。

如果能及时解决问题，或问题属于产品设计的行为，或问题涉及到三方，我们将考虑关闭案例。如果存在多个问题，则我们考虑拆分案例进行分析。

接下来，我们将开始合作解决这个问题。如果您对以上的问题范围界定有任何异议，请尽快告知。如果您有其他任何疑问。也欢迎随时与我联系。

麻烦您下载附件中的日志收集工具，选择**最近的出现帐户锁定问题**的设备（防止帐户锁定的日志被覆盖），并按照以下操作收取日志，协助我们进一步排查这个问题。

将附件中的工具解压，复制到出现账户锁定问题的设备，双击运行 CMGELogCollectorV2.exe，勾选**所有选项**，点击**收集**获取对应的系统日志，将生成的日志压缩包通过 **CDUC** 上传。



日志上传方法：

您可以登陆 https://cduc.cmgos.com，通过数据上传系统上传您所收集的日志信息。**（用户名密码区分大小写）**

用户名：wsfwzx

密码：wsfwzx

注意：添加文件，点击上传后，跳转到新的页面点击保存。

==========

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为向您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括：

(1) 神州网信已获得您的明确授权；

(2) 根据适用法律的要求，神州网信负有披露义务的；

(3) 司法机关或行政机关基于法定程序要求神州网信提供的；

(4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。

(5) 为了解决您的系统故障问题，神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下，第三方会承担与神州网信同等的隐私保护责任的，神州网信会在合理范围内对您的信息进行披露。

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前，务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

神州网信
CMIT

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2023 年 8 月 1 日 10:10
收件人: 李先生 <196403@qq.com>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号：CAS-09521-B3C1S5]% 福建省外事服务中心用户需要排查账户锁定原因 % 初次响应 CMIT:0001474

李先生 先生/女士，您好！

感谢您联系神州网信技术支持中心。 我是技术支持工程师 危亮 。 很高兴能有机会协助您解决该问题。 您可随时通过邮件回复以及该问题事件号码 CAS-09521-B3C1S5 与我联系。

如果您有任何其他疑问，请随时与我联系。

此致,

敬礼
