特权用户可用来危害ACTIVE DIRECTORY的3种方式

降低风险和提高恢复能力的8种方式

Quest

简介

一个可引以为戒的故事

UBS Paine Webber的IT管理员Roger Duronio对自己的奖金感到不满，因此编写了50行代码，并利用用于为公司系统提供合法文件的标准Unix管理工具将这些代码部署到其公司网络中数以千计的系统中。

然后，他辞职了。

但是他的逻辑炸弹还在。该逻辑炸弹有数周的延迟爆发时间，使Duronio有时间抛售价值2万美元的UBS/PW股票。然后，在一天早上，这个炸弹引爆了。据报道，有效负载都变成了“rm -rf /”，这表示删除一切内容。

这让一切陷入了混乱。UBS/PW不得不采用纸笔的方式进行交易。他们仅在IBM那里就花费了300万美元的费用使系统从备份中恢复。而总成本是多少就不得而知了。

关于本文

这只是一个关于不满或粗心的特权用户如何造成灾难的示例。

实际上，在Windows环境中，这是非常容易的事情，因为一切都依赖于Active Directory (AD)。如果Active Directory中断，则整个网络就会中断， 即使您的任何服务器和应用程序都没有问题也是如此。

有多么容易？ 本电子书介绍了特权用户（或窃取了特权凭据的攻击者）可用来使AD中断继而使网络其余部分中断的许多方式中的3种。

然后，我们介绍了8种重要的妥善做法，可帮助您降低该风险并提高您在遇到灾难情况时的恢复能力。

特权用户可用来危害AD的3种方式

方法1: 拒绝登录权限

用户可用于登录Windows的方法有五种：在本地、通过网络、以批处理作业形式、以服务形式以及通过远程桌面服务。对于上述每种登录方法，都有一对登录权限：一个用于允许登录，另一个则用于拒绝登录。

通过以适当的方式分配五个拒绝登录权限，特权用户可以使操作停止。

- 用户将无法登录其工作站。
- 管理员将无法进入域控制器，甚至在控制台中使用本地键盘和屏幕也是如此。
- 服务帐户将无法登录。
- 应用程序无法启动。

这是一种双重困境：您无法通过域帐户登录，而且无法远程修复该问题。相反，您需要以物理形式访问PC，以便重新引导至DSRM中并开始从此处恢复操作。

通过以适当的方式分配拒绝登录权限，特权用户可以使操作停止。

方法2：使DNS中断

Active Directory使用DNS作为查找域控制器(DC)的机制。每个Windows Server 2003或更高版本的Active Directory域都具有DNS域名，且每个Windows Server 2003或更高版本的计算机也具有DNS名称。

为了危害Active Directory，特权用户只需删除一个DC的所有DNS条目即可。这些更改很快就会复制到使用缓存DNS的其他所有DC。然后，DNS高速缓存将超时，以致任何人都突然无法找到任何内容。尤其是，工作站使用DNS找不到域控制器。它们会求助于NetBIOS名称解析功能，该功能可能起作用，也可能不起作用。

如果DNS中断，则一切都会中断。

Quest

方法3：利用操作系统中的漏洞

一天，运行Windows Server 2008的某个企业发现其所有DC都陷入了无尽的重新引导循环中。结果证明，某个特权用户进入了子网并意外地将某个IPv6设置更改为无效的IP地址。当知识一致性检查器(KCC)复制设置进程遇到该无效设置时，就发生了崩溃。这导致DC重新引导，但是这在将无效设置复制到整个环境中的其他DC之后才发生，以致所有DC都开始不停地重新引导。

未知或未修补的漏洞会使AD中断。

Microsoft发布了针对此问题的修复，因此如果您仍在使用Windows 2008或2008 R2，请确保已安装最新的补丁。但是，这不能保证没有其他漏洞被特权用户故意利用或意外遇到，从而导致类似的灾难性后果。

不只是不满的内部人员

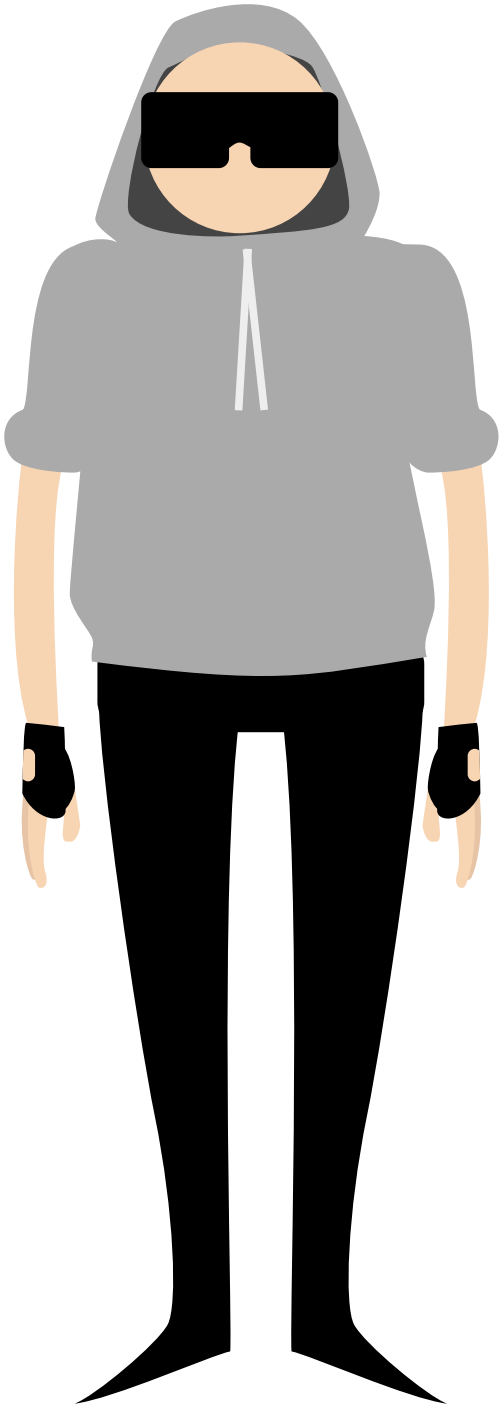
许多企业尝试通过宣称他们没有任何不满或恶意的特权用户成为内部人员威胁，来否定这些类型的情况产生的风险。即使您可能以某种形式保证这是真实的（包括现在和未来），您仍面临风险，原因有两个。首先，即使非常可敬的管理员也会犯错误，例如我们刚刚介绍的无效IPv6设置。其次，具有恶意意图的各种威胁实施者可通过网络攻击窃取并滥用特权凭据，例如：

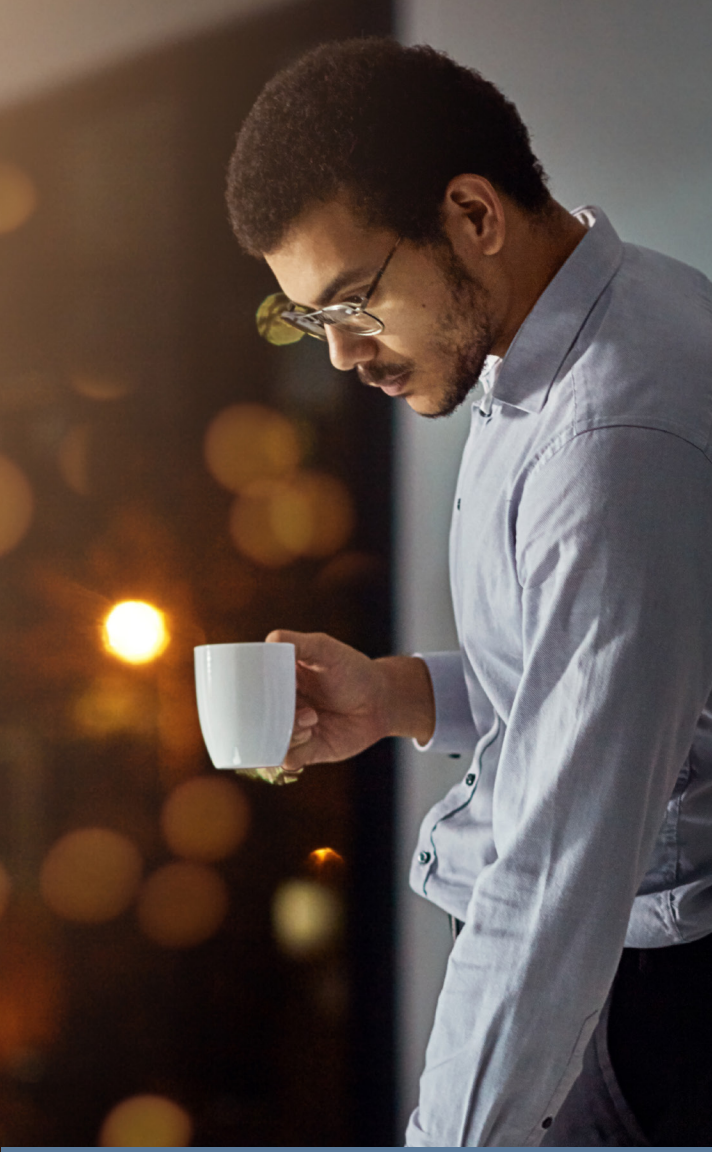
- 黑客
- 敌对国家/地区赞助的团队
- 竞争对手
- 有过错的一方
- 虚无主义者

公司对于用户粗心、疏忽或受危害的凭据所导致的数据泄露的担心(51 %)与对于恶意内部人员导致的泄露的担心(47 %)相当。

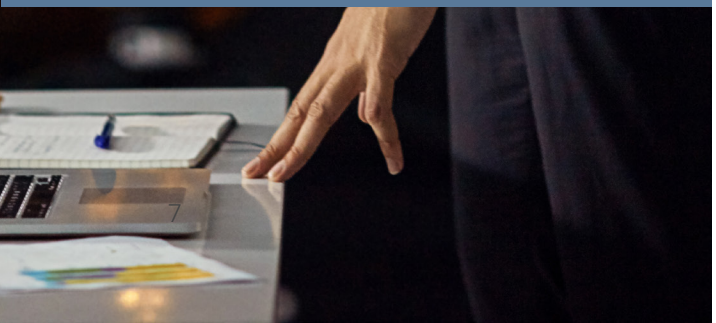
来源: *2018 Insider Threat Report（2018内部人员威胁报告）*, *Cybersecurity Insiders*

请记住，所有这些攻击者都会花费所需的时间和精力来窃取您的数据。他们有些人只是想中断您的服务和损害您的业务，而这容易得多。





严格控制特权组中的
成员资格非常重要。



8种AD安全妥善做法

很明显，特权帐户存在实际且严重的风险。当然，您不能消除这些帐户，它们对于保持系统正常启动和运行至关重要。幸运的是，您可以通过一些成熟的步骤来降低特权帐户有意或无意被滥用的风险，并确保您可以在那些预防措施未能发挥作用时可以尽快恢复。以下是可以实施的8种重要的妥善做法。

1. 限制特权访问。

严格控制特权组中的成员资格非常重要，包括以下成员：

- 域管理员
- 企业管理员
- 模式管理员
- 管理员
- DHCP管理员
- 组策略创建者/所有者
- 域控制器
- 网络配置操作员
- 服务器操作员
- 备份操作员

此外，仔细控制影响域控制器的所有组策略对象(GPO) 以及安装在DC中的所有软件。例如，如果安装了某个代理程序，则有权访问该代理程序的人员很可能是域管理员。

控制特权访问的好方法是使用完全成熟的权限帐户管理(PAM)和权限会话管理(PSM)解决方案，并且对会影响整个域的访问级别进行人工审批和实时监督。由于没有人会每天都要访问域控制器，因此实际可行的做法是对于所有活动都要求两个人在场：一个人进行工作，另一个人负责监督。即使以远程方式或通过同事进行监督，也可削弱一个人独自危害您的业务的能力。此外，增强责任制并要求两个人在场可以降低出现代价高昂的错误的风险。

Quest

2. 保护红色森林中的特权帐户

对生产森林进行足够的强化来保护具有很高特权的管理员帐户且不破坏域中的功能是非常困难的事情。因此，Microsoft现在提供相应的方法将这些帐户放在专门的管理森林中，其正式名称为“增强的安全管理环境”(ESAE)，而非正式名称为“红色森林”，其中“红色”表示凭据的重要性。

“红色森林”模型的主要特征是将管理员帐户分为3个安全级别：

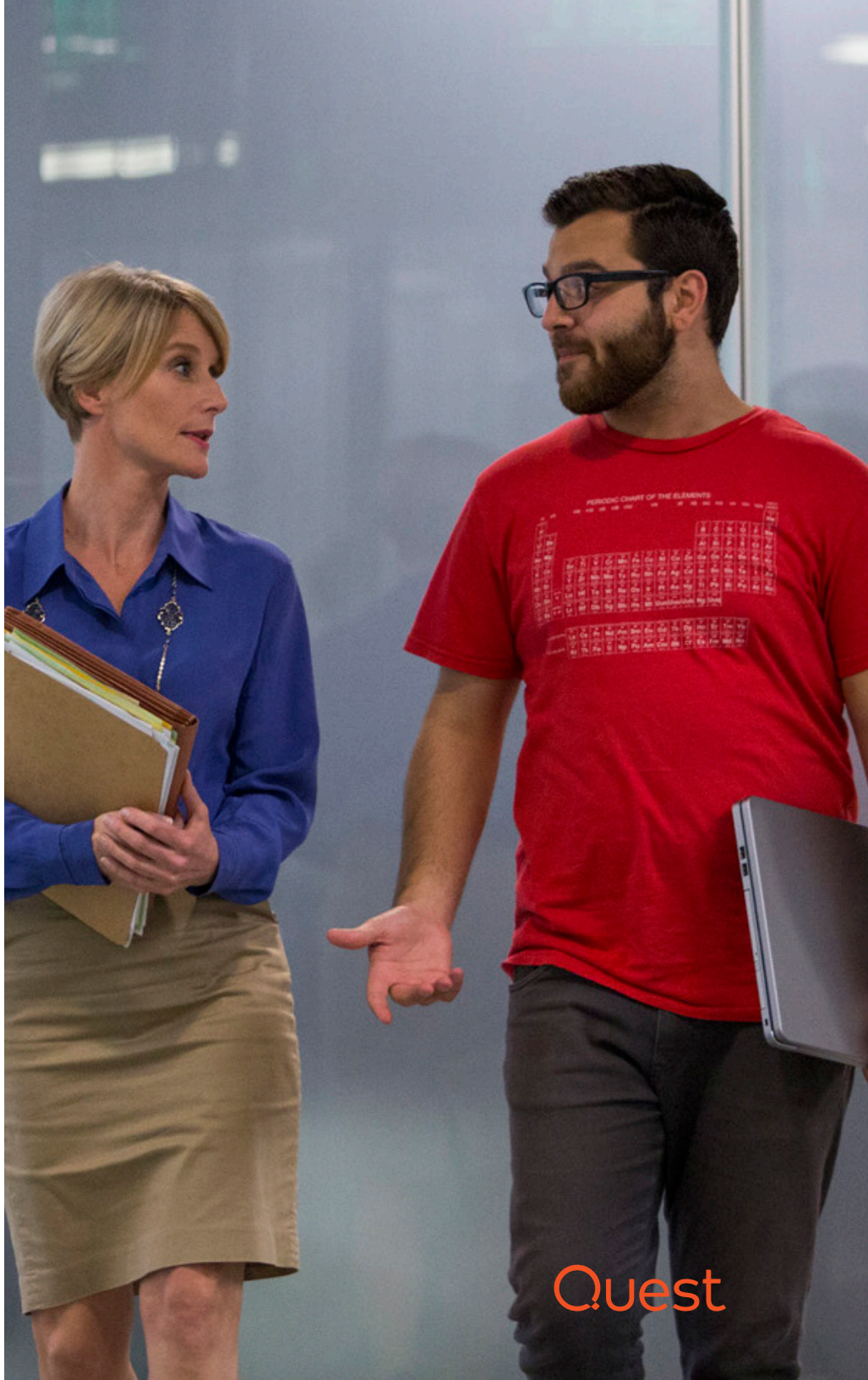
- **第0层 —** 森林级别管理员授权（企业管理员）
- **第1层** — 服务器、应用程序和云管理员授权
- **第2层** — 工作站和设备的管理控制

通过将所有第0层帐户放在单独的森林中，您可以更加轻松地密切监视它们，并且更加轻松地应用其他安全要求，例如要求他们从强化的工作站登录或强制实施双重身份验证。

当然，部署一个管理森林不是一项简单的任务。有关详细信息，请观看录制的网络广播，在此视频中，安全专家Randy Franklin Smith介绍了您可能遇到这种麻烦的原因，以及“红色森林”模型的限制。

3. 在将更改推送到生产环境之前，对其进行测试。

为了降低出现危害AD的错误的可能性，设立一个测试实验室，在将升级或其他更改推送到生产环境之前，可以在该实验室中查看它们的影响。测试实验室与生产环境的贴合度越高越好。



审核Active Directory中的所有重要更改，并发出相应警报。

4. 审核。

全面的审核非常重要，原因有多个。它有助于确保责任到位，从而阻止内部人员执行恶意操作，还可激励有良好意图的特权用户更加小心地进行操作，从而降低错误数量和严重性。此外，它还可帮助您快速确定出错的内容并采取纠正措施，以及了解如何避免以后出现同样的问题。

确保您的审核跟踪包括本机事件、应用程序系统安全日志、目录服务日志和其他关键数据，并且您可以快速查看、搜索和分析这些数据。另外，确保您的审核系统在出现AD故障的情况下也可访问。

5. 监控关键更改并发出相应警报。

确保您可以即时了解对任何关键对象的更改，例如特权组或影响域控制器的GPO。由于这些更改很少见，因此您不会收到大量这样的警报。可以将有关合法更改的警报看作是确认您的监控系统运转正常。关于未授权更改的警报则使您可以快速做出响应，或许能够及时避免严重的后果。

6. 记录您的AD结构。

花时间来记录您的AD结构。确保记录最新的信息，并离线进行存储（例如，在Dropbox中），以便即使AD中断也可访问这些信息。确保包括关于以下方面的信息：

- 森林
- 域
- 信任
- DNS
- 子网以及它们之间的复制链路
- 每个域控制器，包括其IP地址、其物理位置、其控制的域、其上的灵活的单主机操作以及其是否为全局目录

Quest

7. 备份ACTIVE DIRECTORY。

通过企业级备份解决方案备份Active Directory。不要只依靠回收站恢复方法。

请记住，回收站只是一项便利功能而已。它存在许多严重的限制，我们在白皮书《The Windows Server 2016 and Azure AD Recycle Bins, and Quest Recovery Solutions》（Windows Server 2016和Azure AD回收站以及Quest恢复解决方案）中对此进行了介绍。例如，是否还记得我们之前说过某个人可能通过删除您的所有DNS记录来危害您的AD？不通过删除记录，某个恶意用户可能会将设置替换为无效的IP地址。回收站无法帮助您恢复那些属性。

8. 测试您的备份。

及早发现备份错误而不是等到错误实际发生非常重要。通过实际安装备份并从其读取对象来检查备份的可行性。此外，在测试环境中定期重建Active Directory森林以确保您可以从重大问题中快速恢复。

通过企业级备份解决方案备份Active Directory，并对备份进行测试。

结论

当电话亮起而且一切都不工作时，您不知道发生了什么或问题波及的范围。这可能是某个不满的内部人员执行的恶意操作。可能是您遭遇了武器化的恶意软件的攻击。或者是某个意外错误造成您的AD出现故障。

遵循本文介绍的妥善做法可以降低出现这些不良情况的可能性，但是无法完全消除风险。因此，您还需要采取措施来促进快速的Active Directory恢复，包括维护清晰全面的审核跟踪，以及确保您具有可靠的备份。

您可能听到过尝试在周末重建AD的悲惨故事。恢复AD不像还原被删除的文件那样简单。而且其很难进行测试或模拟，部分原因在于适当的AD恢复步骤取决于特定的灾难情况。

但是拥有适当的解决方案，您单击一下便可重建整个Active Directory森林。有关详细信息，请阅读我们的白皮书《可怕的那一天：Active Directory灾难和避免灾难的解决方案》。

拥有适当的解决方案，您单击一下便可重建整个Active Directory森林。

Quest

关于QUEST

Quest的宗旨是通过简单的解决方案解决复杂的问题。为实现此宗旨，我们秉持注重卓越产品和优质服务的理念，并且追求易于合作这一总体目标。我们的愿景是提供无需在效能和效率之间做出选择的技术，这意味着您和贵公司可在IT管理上投入更少的时间，从而将更多时间用在业务创新上。

如果您对本材料的可能用途存有任何疑问，请联系：

Quest Software Inc.
收信人：LEGAL Dept

请访问我们的网站(www.quest.com/cn)，了解有关地区和国际办事处的信息。

Ebook-3WaysToHoseYourAD-US-GM-zh_CN-WL-32410

Quest