精译版

QakBot 又回来了

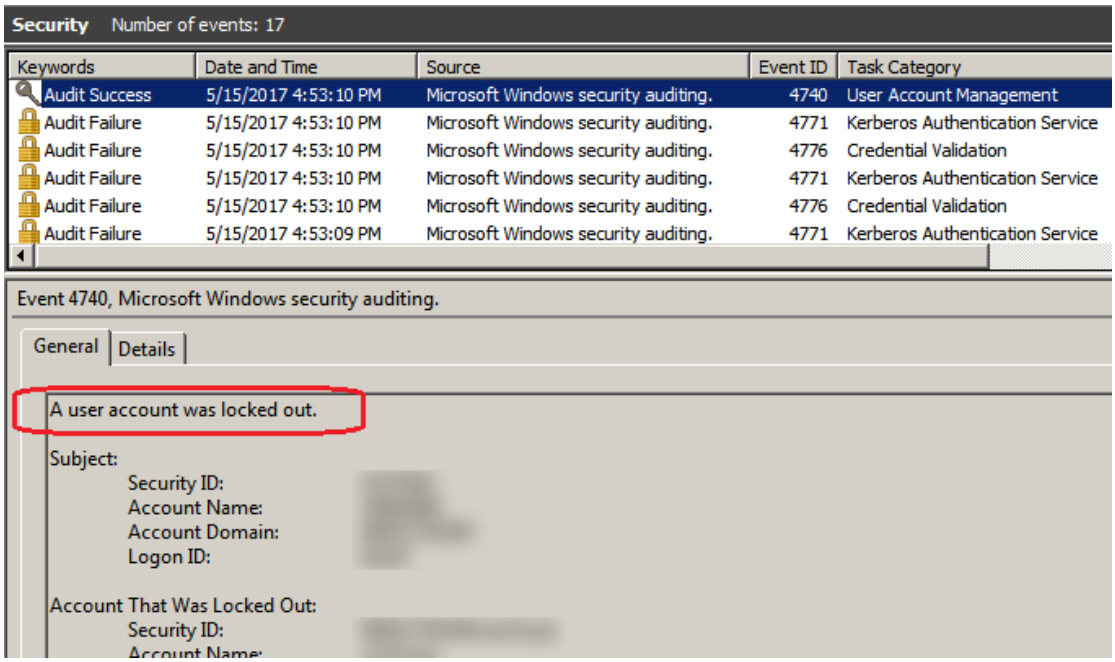
非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	QakBot Returns, Locking Out Active Directory Accounts		
原文作者	Chris Brook	原文发布日期	2017 年 6 月 5 日
作者简介	Chris Brook 是 Threatpost 的副编辑。https://www.linkedin.com/in/chris-brook-91223712/		
原文发布单位	Threatpost		
原文出处	https://threatpost.com/qakbot-returns-locking-out-active-directory-accounts/126071/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

QakBot 又回来了

Chris Brook

2017 年 6 月 5 日



QakBot 是一种类似蠕虫的信息窃取恶意软件，从 2009 年开始活跃，如今再次浮出水面。

该恶意软件一直是管理员的痛。在一段时间的沉寂之后，研究人员发现，它与最近的大量微软 Active Directory（活动目录）锁定事件有关。

Active Directory 是微软的目录服务器，允许管理员从单个位置控制网络。管理员通常使用数据库来验证和授权用户。

上周五，IBM X-Force 研究团队的 6 位研究人员（包括 Michael Oppenheim，Kevin Zuk，Matan Meir，Limor Kessem 等）表示，这是 QakBot 第一次执行锁定攻击，导致用户无法访问受影响的域上的端点、公司服务器和网络资产。

QakBot 利用投放器通过端点进行传播。该投放器等待 10 到 15 分钟才会执行，旨在规避沙箱或反病毒系统的检测。该投放器打开一个可执行文件，注入一个 DLL，并覆盖原始文件，然后下载 QakBot 的载荷。

在过去，QakBot 表现出类似蠕虫的功能，例如通过共享驱动器和可移动媒体进行自我复制。而这一次，它一直通过网络传播，通过循环访问用户和域凭证来锁定用户的账户。该恶意软件使用不同的密码猜测方案进行登录，包括使用字典中的单词来猜测密码。

研究人员在周五发布的博文中说："QakBot 可能会收集受感染机器的用户名，并使用它来尝试登录域中的其他计算机。如果它无法枚举域控制器和目标计算机的用户名，就会使用硬编码的用户名列表。"

研究人员说，字典风格的攻击已经取得成功，并且认为 QakBot 就是用这种方法来锁定账户的。

研究人员说："在某些域配置下，QakBot 的字典攻击可能会导致多次失败的身份验证，最终导致账户锁定。"

研究人员指出，QakBot 早就被证明善于规避检测了，而且具有持续性。它利用注册表运行键和计划任务来躲避系统重启和删除。利用注册表运行键，每次系统重启后，它都能够自动启动；而利用在 schtasks.exe 中编写的计划任务，它能够按时间间隔运行。

正是得益于这种持续性机制，QakBot 在 2011 年感染了马萨诸塞州的两个政府机构：失业救助部和职业服务部。这两个机构表示，W32.QAKBOT 有可能窃取了个人姓名、社保号、雇主识别号和电子邮件地址。

这两个机构指出："W32.QAKBOT 可能影响了失业救助部和职业服务部多达 1500 台电脑，包括一站式职业中心的电脑。"

这个恶意软件也与 2011 年投资和保险公司 The Hartford 的攻击有关，该公司员工用来远程访问 IT 系统的几台服务器遭到了攻击。

IBM X-Force IRIS 的全球研究负责人 Mike Oppenheim 在周一表示，虽然研究人员发现的大部分攻击面向医疗和科技行业，但是他们并不认为该恶意软件针对任何特定的行业。

Oppenheim 补充说："目标组织和大部分目标银行位于美国。"

Active Directory 锁定只是 QakBot 攻击活动的副作用。研究人员说，QakBot 并没有失去窃取银行登录信息的诀窍。

QakBot 能够利用多种机制搭载受害者的银行会话。它利用浏览器中间人

（man-in-the-browser）功能，从攻击者控制的域向网上银行银会话中注入恶意代码。这样一来，攻击者就能够窃取用户击键、缓存凭证、数字证书和会话验证数据了。

Oppenheim 指出，Active Directory 锁定和银行攻击的方式相同。

“在这两种情况下，QakBot 都是通过钓鱼邮件中的恶意链接到达目标机器的。”Oppenheim 说。

“需要注意的是，这是一个复杂的犯罪组织，我们已经发现数百个受感染的设备与其 C2 中心通信了。该组织试图感染尽可能多的机器。他们感染了大量的基础设施，其 C2 服务器以小时为单位推出新的，稍微调整的 QakBot 版本，以增加他们的经济收益。”

该恶意软件已经运行了将近 8 年，貌似短期内也不会消失。

BAE Systems 的研究人员去年 4 月表示，QakBot（也被称为 Qbot）应为 5.5 万起感染负责，其中 85%的感染影响了美国的系统。当时，BAE Systems 网络威胁情报负责人 Adrian Nish 告诉 Threatpost，攻击者不断地重新编译代码并重新打包，以便规避检测。

“Qbot 的作者每天都在重新编码，并重新打包。今天杀毒扫描能够发现它，第二天可能就发现不了了。” Nish 说。

周五，IBM 的研究人员表示该恶意软件的隐秘性归功于位于东欧的开发人员。这些开发人员不时地将其下线，微调其代码、持续性机制、抗杀毒能力和抗研究能力。

研究人员说，攻击者的沉寂是一种有目的的行为，“可能是为了将攻击限制在最低限度，避免执法机构的调查。”