在Umbrella中启用新显示的域安全类别

目录

简介

本文档介绍Cisco Umbrella中的“新发现的域”(NSD)安全类别。

背景信息

新发现的域(NSD)是识别过去24小时内由Cisco Umbrella DNS服务（包括家庭用户的免费OpenDNS服务）的任何用户首次查询的域的安全类别。 此安全类别的功能与任何其他安全类别相同，并且可作为现有安全设置或新安全设置的一部分启用。域在列表中保留24小时。

Cisco Umbrella如何将域定义为“最新发现”

新域通常作为新恶意软件活动的一部分创建。这些攻击活动背后的恶意攻击者使用新的域，因为传统的基于签名的方法无法识别它们来阻止已知的恶意网站。例如，网络钓鱼活动可以创建一个新域，以配合大型垃圾邮件活动，鼓励用户点击链接。此链接尚未被识别为此活动的一部分，并且未被已知恶意域的标准列表阻止。在将链接添加到这些列表之前，犯罪分子有足够的时间来窃取数据、安装恶意软件并获得网络访问权限。

新发现的域(NSD)安全类别通过检查DNS日志来查找以前从未见过的域。由于无效查询的数量，要将域标记为新可见，客户端查询必须收到正确答案。首次看到域后，会将其添加到列表中24小时。在此时间段之后，该域将不再可见，并且会从列表中删除。

报告记录查询域时域所属的类别。因此，如果某个域在查询时被分类为新发现的域，则会在Activity Search或Security Activity报告中报告此类域。但是，一旦域从列表过期，根据域的相关当前数据对该域进行透视处理(尤其是使用新的Destinations或Identities报告，Investigate Console或Investigate API)不再将该域显示为新可见的域。简而言之，几天后重新访问域无法再显示为Umbrella中的新域。这是有意安排的，但可能会导致一些初步的混乱。

新发现的域的唯一定义是：这是最近才看到的。因此，分类为新发现的域中有很大一部分不是恶意的，并且合法域检测预计会在此安全类别中发生。针对这种情况的预防措施已经实施，尤其是针对某些服务和CDN，如Akamai和Cloudfront，它们会生成随机子域来服务内容。针对诸如Facebook和

Google等非常受欢迎的域名的传统保证也被用于确保这些域不包括在内。

此外，只有完全限定域名（第二级域或第二级域的子域）才被视为新发现的域。顶级域和国家代码顶级域不包含在新显示的域中，以避免阻止大型域分组。

有关实施的重要说明

鉴于可能会出现一些不需要的检测，Cisco Umbrella强烈建议开始在审核模式或仅检测模式下使用此报告，而不阻止或采取任何操作。默认情况下，安全设置中带有此类别的所有用户都将新发现的域视为报告中的检测项。这实际上意味着，此功能在默认情况下启用时不会有任何阻塞。在大多数情况下，用户必须使用报告来查看与该类别匹配的流量，并使用该信息更深入地研究这些域，以确定它们是否可能构成安全威胁而不是自动阻止。

另一个主要注意事项是允许对域的第一个查询。这是因为Cisco Umbrella以前从未看到对该域的查询，因此，日志记录系统尚未处理过该查询，因此该查询未被包含在Newly Seen Domains类别中。首次查询域和出现在匹配类别的域列表之前的时间间隔大约为五分钟，但可能超过此时间，因为Cisco Umbrella不一定处理100%的DNS查询日志（由于处理时间和数量原因）。

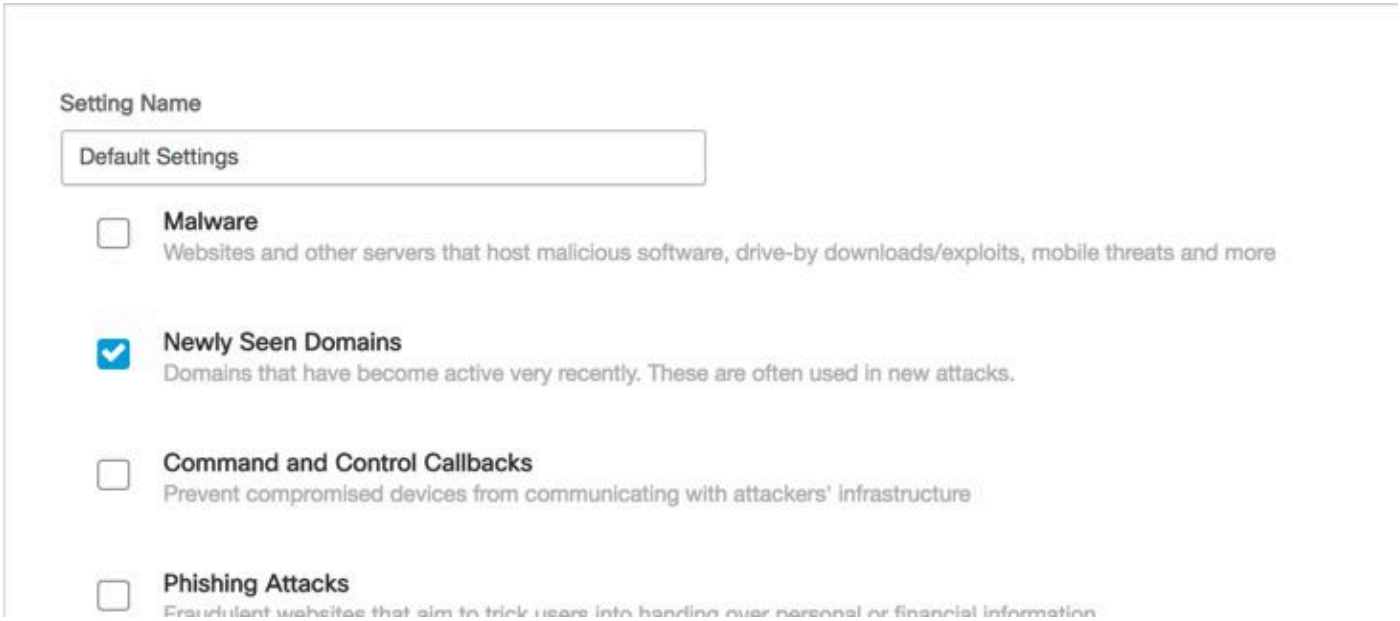
代理新显示的域

使用Umbrella智能代理的客户还发现，NSD类别中的某些域是代理的。这是有意设计的。Umbrella Labs团队使用通过代理这些新域收集的数据来确定是否可以立即将这些新域添加到恶意软件类别中。此问题的一个副作用是发送到新发现的域（也正被代理）的非标准流量在代理级别被丢弃。智能代理仅代理端口80和443，这些端口通常用于网络流量。无论类别是否被阻止，代理启用后都会自动发生这种情况。要防止代理单个新发现的域，请将其添加到相应的允许列表。

有关智能代理的详细信息，请参阅文档启用智能代理。

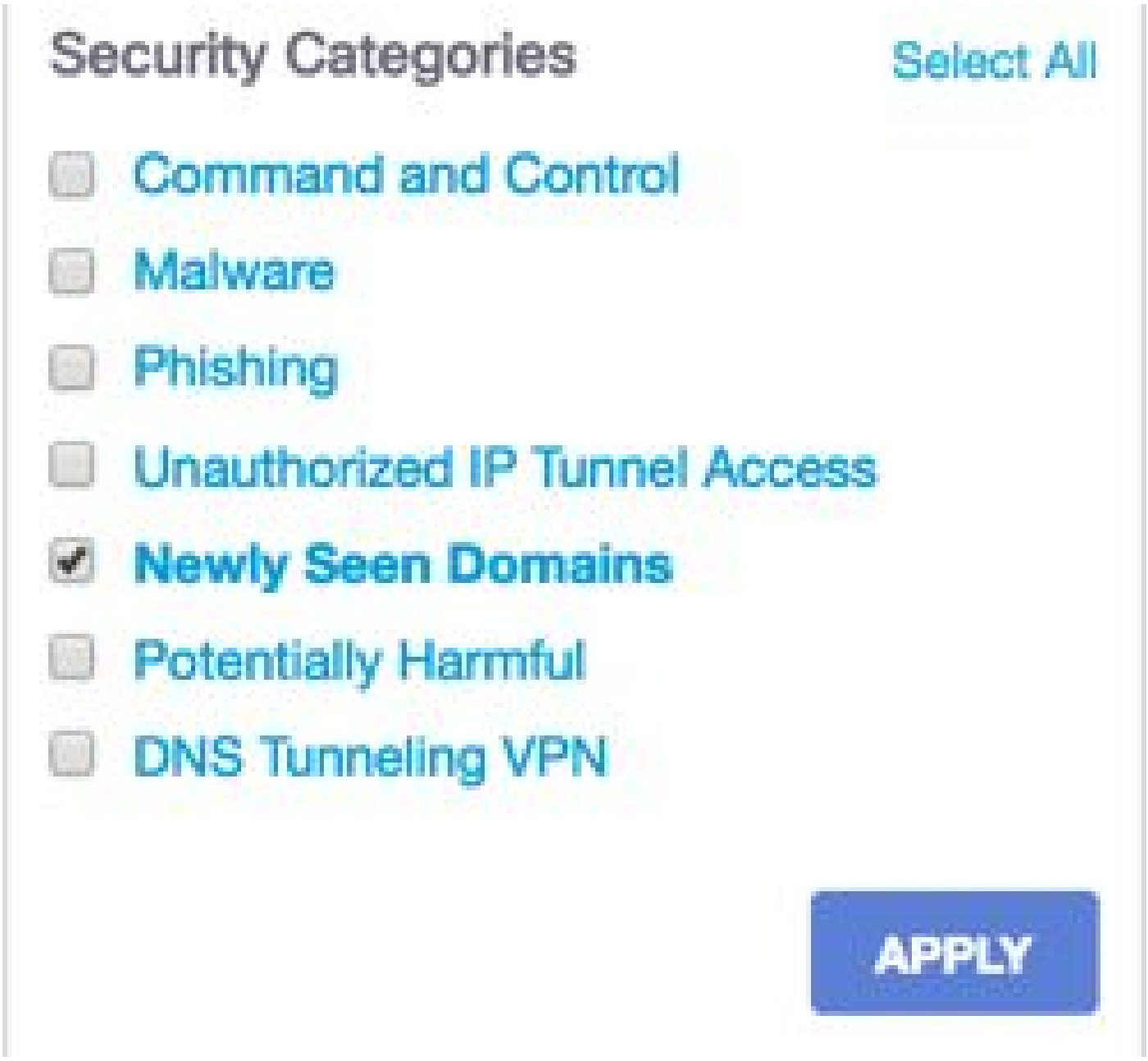
启用新显示的域

可以像启用策略>安全设置下的任何其他类别一样启用新建域安全类别，然后编辑现有安全设置。或者，也可以在策略配置向导自身中执行此操作。



115014822286

新发现的域也可以在某些报告中过滤，例如活动搜索。



115015007423

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。