通过Umbrella漫游客户端了解第三方VPN检测启发式规则

目录

简介

本文档介绍Umbrella客户端的第三方VPN检测试探法。

背景信息

Umbrella客户端已实施自动检测机制来响应VPN更改，以确保维持DNS功能。这会导致客户端在VPN连接时暂时保持未保护状态。我们总结这些机制如下。

第三方VPN检测启发式算法

本文档讨论了Umbrella漫游客户端(URC)用于检测Windows系统上的VPN活动以避免与VPN客户端冲突的DNS保护活动的三种不同一般启发式方法。暂停的保护漫游客户端进入未保护状态。

第 1 种情况：VPN客户端使用自己的DNS IP地址预置DNS解析器列表

当URC主动将流量重定向到Umbrella解析程序时，系统上的各种网络适配器将使用127.0.0.1或：:1作为其DNS服务器（URC在该IP地址上运行本地DNS代理，侦听端口53）。 当检测到网络事件且已更改DNS设置时，URC会在每个网络适配器的DNS IP地址列表中查找127.0.0.1或：:1(取决于网络堆栈，127.0.0.1用于IPv4，以及：:1（用于IPv6）。如果找到IP地址，并且该IP地址已预先固定（例如10.0.0.23、192.168.2.23、127.0.0.1 DNS设置），则URC会暂停保护。 此状态将一直有效，直到活动网络接口的数量发生更改并重置客户端状态。

第 2 种情况：当DNS解析器发生更改时，VPN客户端会对其进行监控和重置

某些VPN客户端在设置DNS配置后，主动监控这些设置，如果它们偏离了VPN客户端指定的配置，则重置这些设置。 URC监控DNS地址恢复，如果在20秒内发生3次恢复，则URC会暂停保护。这包括每5秒或更短时间发生的任何恢复。在活动网络接口数量发生变化且客户端状态重置之前，此情况一直有效。

实例3：其它WRR加权修改VPN客户端在网络层截取和重定向A和AAAA记录

有些VPN客户端会干扰A和AAAA记录（即，它们仅重定向这些记录类型），而保留其他记录类型为独有。 在这种情况下，URC会与Umbrella解析程序进行通信，而不会导致TXT和其他问题。记录，但实际上未应用任何保护，因为A和AAAA记录未通过Umbrella解析程序进行应答。在实际应用

DNS保护之前，URC通过向Umbrella发送一些测试记录来检查A和AAAA记录干扰。如果响应未恢复或者不是预期结果，则URC会暂停保护。 由于在这种情况下不会触发任何网络事件，因此URC会定期检查此情况。此机制也可以在像Netskope这样的软件代理存在时触发。

其他案例

有些VPN客户端已经解释了Umbrella添加的兼容性。此支持明确适用于未来的Dell(Aventail)VPN客户端和Pulse Secure客户端。

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）。