litao3rd

PassiveDNS

An assessment of Non-Authorized Domain Name Resolution provided by DNS Resolution Service Provider

Summary In a previous article, we disclosed that the Specter botnet uses api. github[.]com and other white domains to provide C2 services as a way to evade detection by security products based on signature and threat intelligence matching. The botnet can do this because the Domain Name Resolution provider

· Dec 8, 2021 · 8 min read

PassiveDNS

解析服务提供商对非授权域名解析情况的评估

概要 在之前的文章中，我们披露了Specter僵尸网络序利用api[.]github.com等白域名提供C2服务，以此来逃避基于签名和威胁情报匹配的安全产品的检测。其具体原理经过分析之后，发现其利用了某些域名注册/托管商(cloudns)的权威DNS服务器在解析非其客户域名方面的漏洞。 我们对此现象，即域名注册/托管商，公有云提

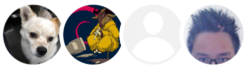
供商等能够提供域名注册和解析服务的供应商（以下统称为解析服务提供商）对非自己服务域名的DNS请求是否能够返回正确应答的情况，进行了系统的测量和评估。 这篇文章对此现象进行了分析。 数据选择及评估方法 被测域名 被测试域名：Alexa top500。选择他们作为被测域是因为： 1. 这些域名都会使用自己专有的DNS服务器，他们并不会使用外部的解析服务提供商提供的解析服务。所以如果这些域名可以被外部的解析服务提供商的NS服务器解析，那么大概率是非授权的。 2. 这些域名本身也因为其庞大而知名的业务，会被加入到各种白名单中。一些出于探测目的的人也更容易随手添加一些知名网站，而干坏事的人微了躲避检测黑名单检测，也愿意使用这些白域名。


· Dec 6, 2021 · 16 min read

DNS

The Pitfall of Threat Intelligence Whitelisting: Specter Botnet is 'taking over' Top Legit DNS Domains By Using ClouDNS Service

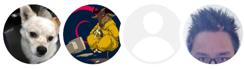
Abstract In order to reduce the possible impact of false positives, it is pretty common practice for security industry to whitelist the top Alexa domains such as www.google.com, www.apple.com, www.qq.com, www.alipay.com. And we have seen various machine learning detection models that bypass


· Nov 18, 2021 · 6 min read

DNS

白名单之殇：Specter僵尸网络滥用ClouDNS服务，github.com无辜躺枪

摘要 威胁情报的应用，始终存在着“漏报”和“误报”的平衡，为了减少可能的误报带来的业务影响，你的威胁情报白名单中是否静静的躺着 www.apple.com、www.qq.com、www.alipay.com 这样的流行互联网业务域名呢？你的机器学习检测模型，依照历史流量，是否会自动对 .qq.com、.alipay.com 这样的流量行为增加白权重呢？ 但安全是对抗，白帽子想“判黑”，黑客想“洗白”。我们看到的白，不一定是真的白，可能只是黑客想让我们以为的白。 我们BotnetMon最近的跟踪发现，Specter僵尸网络家族的样本，会使用api.github.com这种域名作为CC域名来通信，通过“可定制化”的DNS服务，将“白域名”引导到黑IP上来实现自己恶意指令通信。 这种“过白”手法，在流量检测的场景下，


· Nov 18, 2021 · 11 min read