2022-
2023年排名前24名的域名、IP以及DNS情报趋

发布于 April 12, 2023

大量的域名和DNS数据信息是丰富的情报来源，可为安全研究人员、机构和解决方案提供多种业务和网络流

多年来，WhoisXML API进行了多项网络调查，并将工作收集到的相关事实和研究数据整理如下：

与威胁、恶意活动和恶意软件集群相关的网络安全数据

我们不断检查分析和更新参与不同威胁活动的威胁指标（IoCs）清单列表，以下内容是我们在各类威胁和恶

- 有60%的IP地址被确定为威胁指标，而这些IP地理位置位于美国却被非美国的威胁者使用。
- 除美国以外，荷兰、日本和泰国也是IP地址被认定为威胁指标且被非美国的威胁者使用排名领先的国家
- 有69%的域名和URL被认定为威胁指标，显示其注册国为美国，但是却被非美国的威胁者使用。
- 除美国以外，俄罗斯、中国和荷兰也是域名和URL被认定为威胁指标排名领先的国家，且这些威胁指标

注：
上述统计数据来源于2022年10月至2023年2月期间对“叙利亚电子军队”、“Hive勒索软件威胁活动”、

与冒充或域名抢注相关的网络安全数据

新注册域名（NRDs）通常被用于针对美国财富500强的公司进行品牌冒充和网络钓鱼攻击。因此，我们调查

- 99.04%的新注册域名包含有主要金融机构的品牌名称，且这些域名与该品牌合法的域名并无匹配的W
- 97.81%的新注册域名包含有主要聊天应用程序品牌，且这些域名与该品牌合法的域名并无匹配的WHO
- 99.41%的新注册域名包含有顶级电子健康记录（EHR）软件供应商名称，且这些域名与该公司合法的

- 被用于冒充美国财富500强的公司的新增域名和子域名中有12%是恶意的，剩下的88%的域名目前还未
- 在冒充美国财富500强公司的域名中有79%都使用了“紧迫性”相关的字符串（如，授权、登录、支付
- 专门管理针对首席执行官和美国财富500强公司的抢注域名的IP主机且排名前十的互联网服务提供商中

注：上述统计数据来源于2022年7月至2023年2月期间对“Gigabud RAT”、“破坏性供应链攻击”、“医疗保健相关的网络攻击”、“通过谷歌搜索广告传播恶意软件”和“

按主题和事件分类的网络安全数据

我们的研究人员追踪了特定的全球性事件和热门新闻对DNS产生的影响，特别是在域名注册方面的影响。以

- 2022年第二季度与税收季相关的新增域名中有13%是恶意的。
- 节假日相关的域名注册会在每个节日的前2-3周有所回升。
- 2022年乌克兰-俄罗斯战争开始后的一周内，含有“俄罗斯”或“乌克兰”的新增注册域名数量增加了150%。
- 俄乌战争开始后的一个月内，含有“俄罗斯”或“乌克兰”的域名注册数量下降了数千个，但是仍然超
- 节假日主题的域名中有56%是在美国注册的，尽管多数国家也都会庆祝这些节假日。
- 除美国外，冰岛、加拿大和中国也是节假日相关域名主题的主要注册国。
- 85%的节假日主题的域名解析的IP地址位于美国。

注：
上述统计数据来源于2022年8月至9月2期间发布的“2022年第二季度域名注册趋势分析报告”和“2022年8

与常见的滥用顶级域相关的网络安全数据

2023年初，根据Spamhaus提供的关于域名滥用的数据信息，我们在《DNS滥用趋势白皮书》中分析了成千

- 在最为滥用的顶级域名中，有64%的域名有过WHOIS信息编辑的记录，如果这些域名出现在恶意活动
- 在最为滥用的顶级域名中有67%的新增注册域名的IP解析地理位置是位于美国。

- 除美国以外，中国、新加坡和德国也是最为滥用的顶级域名中新增注册域名解析最常见的IP地理位置。
- 在最为滥用的顶级域名中，28%的新增注册域名的注册国家为美国。
- 除美国以外，中国、冰岛和英国也是最为滥用的顶级域名中新增注册域名最为常见的注册国家。

与批量可疑域名注册相关的网络安全数据

根据一些威胁者利用注册商所提供的批量域名注册功能，我们研究后发现了这些批量注册域名背后的可疑模

- 在对“误植域名数据流”文件的分析后发现，在同一天注册的外观相似的域名中，有超过24%的域名
- 威胁者所做的整个注册域名组合量可能是他们在某一天注册域名的140倍。

—

我们将继续利用网络威胁情报数据来调查威胁、绘制出恶意的基础设施图，并跟踪域名的注册趋势。

??????????????????????????????????????