Zhang Zaifeng

DNSMon

俄乌危机中的数字证书：吊销、影响、缓解

背景 当前这场始于2021的俄乌危机已经注定载入史册，不仅因为危机中的冲突会对传统政治地缘产生深远影响，也因为这些冲突历史性的全面蔓延到网络空间。我们（360Netlab）从独立采集到的数据出发，观察分析并呈现冲突中各利益相关方采取的行动和反制行动，希望有利于安全社区思考自身在网络空间中的定位、态度和行动。 本文中的观察分析基于网络资产的SSL证书数据库CertDB，它是360Netlab 运营的网络空间基础数据之一，它采集了几乎全部活跃的网络空间中的网站证书。证书是整个现代webPKI系统的最核心的部分之一。如果说DNS数据标识了网络资产的地址，那么证书就是网络资产的身份证。丢失或者没有证书数据，就没有办法证明“我”就是“我”。因此作为互联网安全运营的基础数据，重要性不言而喻。 360Netlab同时运营着的网络空间基础数据库包括描述域名注册的WhoisDB、域名解析的PassiveDNS、网站页面的WebDB等等。这些基础数据库的条目以十亿或千亿为单位计，共同构成了用以描述全球网络空间变迁的DNSMon系统。 在CertDB的支持下，我们有足够坚实的数据基础来解

 · Apr 2, 2022 · 28 min read

DNSMon

商业数字证书签发和使用情况简介(删减版)

概要 数字证书是整个现代webPKI系统的最核心的部分之一。如果说DNS数据标识了网络资产的地址，那么数字证书就是网络资产的身份证。没有,丢失或者被吊销数字证书，就没有办法证明“我”就是“我”。因此PKI系统及其数据已经成为网络真正的基础设施，作为互联网安全运营的基础数据，重要性不言而喻。 3月初,乌克兰政府向

互联网域名管理结构ICANN书面请求将俄罗斯相关顶级域名“.ru”, “.рф” 和“.su”从互联网撤销[1]，但ICANN并没有认同这份请求[2]。近日，我们注意到俄罗斯相关的一些国家基础设施网站的证书被证书机构陆续吊销。360Netlab成立之后不久就通过主动、被动相结合的方式收集网络数字证书，并以此为基础构建了网络证书数据库CertDB。目前该库包含证书规模和涉及的IP端口数据达到十亿级，历史数据可追溯超过5年，是360Netlab基础数据分析系统DNSMon的重要组成部分。此外360Netlab同时运营着的网络空间基础数据库包括描述域名注册的WhoisDB、域名解析的PassiveDNS、网站页面的WebDB等等。这些基础数据库的条目以十亿或千亿为单位

 · Mar 23, 2022 · 14 min read

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

PassiveDNS

被拦截的伊朗域名的快速分析

伊朗新闻网站被美国阻断的事成为了最近的新闻热点，报道的主要内容是： 美国司法部查封36个伊朗的新闻网站，其中许多网站与伊朗的“虚假信息活动”有关。这些网站首页通知显示，根据美国法律，这些网站已被美国...

 · Jun 25, 2021 · 10 min read

Import 2022-11-30 11:16

DNS data mining case study - skidmap

As the foundation and core protocol of the Internet, the DNS protocol carries data that, to a certain extent, reflects a good deal of the user behaviors, thus security analysis of DNS data can cover a decent amount of the malicious activities. In the early days, typical scenarios for early

 · Nov 30, 2020 · 9 min read

DNSMon

DNSMon: 用DNS数据进行威胁发现

----发现skidmap的未知后门 更新记录 * [2020-12-07] 在本文发布之后不久，我们注意到该后门的访问模式有了一定的调整。并在最近DNSMon发现攻击者已经启用了新的域名IOC。具体来说有如下变化： 1. 将rctl子域名变更为 r1 2. 新启用了mylittlewhitebirds[.]com，howoldareyou9999[.]com（比原先的

howoldareyou999[.]com多了一个字符'9')，franceeiffeltowerss[.]com(比原先的franceeiffeltowers[.]com多了一个字符's')三个域名作为后面的备用域名。 具体如下： r1.googleblockchaintechnology[.]com r1.howoldareyou9999[.]com r1-443.howoldareyou9999[.]com r1-443.franceeiffeltowerss[.]com

 · Nov 25, 2020 · 19 min read

DNSMon

360netlab上线域名IOC（威胁情报）评估标准及评估数据服务

版本一：程序员版 一直以来，由于高门槛，安全圈里对威胁情报质量没有一个很好的评估手段， PR狠的公司的威胁情报就更好么？ 名头响的公司的威胁情报就更好么？ 使用了机器学习人工智能这些热词的威胁情报就更好么？ 拿了一堆排排坐吃果果的奖的公司的威胁情报就更好么？ 难有人能给个说法，所以最后我们看到用户只能回到一个聊胜于无的方法，哪家的威胁情报的总数多哪家就好，出现的告警次数多哪家就好！ 这个方法其实巨坑，举个?： A和B厂家提供两份威胁情报，A有10万条IOC，B有5万条IOC。 A的10万条IOC在实际网络中总命中IOC不到1000条，产生了20000次告警。 B的5万条IOC在实际网络中命中IOC15000条，也产生了20000次告警。 你愿意选择哪个？ 那咋办？ 经过一段时间的准备，我们推出来了个一个公益的评估标准，而且还免费提供大网的实际评估数据从而让客户有真实数据评估。 我们这么干是为啥？ 是不是有啥阳谋，要怎么收数据之类的？ （答案，没有，看看我们的正经页面就能懂） 另外我们很欢迎有经验的用户提供反馈修正等，对于采用的

 · Nov 2, 2020 · 4 min read

DNSMon

Look at NTP pool using DNS data

With the rapid development of the Internet, more and more people have realized the importance of network infrastructure. We don’t hear people talk about NTP (Network Time Protocol) much though. Whether NTP can work well will affect the operation of most time-based computer system. For example, IPSEC tunnel establishment,

 · May 26, 2020 · 8 min read

DNSMon

从DNS角度看NTP pool服务器的使用

随着互联网的快速发展，其已经深入到日常生活中的方方面面，越来越多的业内人员对于网络基础设施的重要性有了非常深入的认识。不过谈到基础设施，通常都会谈及DNS协议，但是还有一个关键的协议NTP（Network Time Protocol）却没有得到应有的重视。 NTP是否能够良好的工作会影响到计算机系统的大部分基

于时间判定的逻辑的正确运行。比如DNSSEC是否过期，IPSEC的隧道建立，TLS证书的有效性校验，个人密码的过期，crontab任务的执行等等[1]。 NTP协议同DNS类似，是互联网最古老的协议之一，主要作用如其名字所说，用来保持设备时间的同步。在我们使用的操作系统比如windows，Android或者Macos都配置有自己的NTP时间服务器来定期同步设备上的时间。 NTP pool 是什么？ 由于互联网的发展以及NTP业务的特殊性（时间需要定期同步），少量的NTP服务器的负载越来越大，并且公共一级NTP授时服务器存在被滥用的问题，2003年1月NTP pool项目正式设立。 其基本原理通过域名“pool.ntp.org”基于特定规则划分为多个子域名并在这些子域名上

 · May 26, 2020 · 12 min read

DNSMon

一些网站https证书出现问题的情况分析

[20200328 17:00 更新] 更新数据到20200328 16:00. 20200326下午，有消息说[1]github的TLS证书出现了错误告警。证书的结构很奇怪，在其签发者信息中有一个奇怪的email地址：346608453@qq.com。明显是一个伪造的证书。 为了弄清楚其中的情况，我们对这一事件进行了分析。 DNS劫持？ 出现证书和域名不匹配的最常见的一种情况是DNS劫持，即所访问域名的IP地址和真实建立连接的IP并不相同。 以被劫持的域名go-acme.github.io为例，我们的passiveDNS库中该域名的IP地址主要使用如下四个托管在fastly上的IP地址，可以看到其数据非常干净。 对该域名直接进行连接测试，可以看到，TCP连接的目的地址正是185.199.111.153，但其返回的证书却是错误的证书。因此github证书错误的问题并不是在DNS层面出现问题。 劫持如何发生的？ 为了搞清楚这个问题，可以通过抓取链路上的数据包来进行分析。为了有较好的对比性，我们先后抓取了443端口和80端口的数据。如下图 左边的数据包为https连接

 · Mar 27, 2020 · 6 min read

Botnet

Malicious Campaign luoxk Is Actively Exploiting CVE-2018-2893

Author: Zhang Zaifeng, yegenshen, RootKiter, JiaYu On July 18, in an officially released routine patch update, Oracle fixed CVE-2018-2893, an Oracle WebLogic Server remote code execution vulnerability. Three days later, at 2018-07-21 11:24:31 GMT+8, we noticed that a malicious campaign that we have been tracking for a

 · Jul 23, 2018 · 3 min read

Botnet

恶意代码团伙luoxk正在积极利用 CVE-2018-2893 传播

文章作者：Zhang Zaifeng, yegenshen, RootKiter, JiaYu 7月18日，Oracle在官方发布的例行补丁更新中修复

了CVE-2018-2893，一个Oracle WebLogic Server 远程代码执行漏洞。一般认为漏洞影响严重且相关PoC已经公开，建议相关用户尽快进行评估升级。 三天后，2018-07-21 11:24:31 开始，我们注意到一个长久以来我们跟踪的恶意代码团伙正在积极利用该漏洞传播自身。由于该团伙经常使用 luoxkexp[.]com ，我们将其命名为 luoxk 。 该恶意代码团伙第一次触发我们的警铃是在一年前的2017年3月17日，我们的DNSMon系统，在该恶意代码团伙域名注册后的第二天根据算法自动判断该域名异常。 在那以后，我们持续观察了该恶意代码团伙的行为，包括： * DDoS攻击：使用DSL4（Nitol）恶意代码，对应的C2 luoxkexp.com * 挖矿：挖矿使用的钱包地址是 48WDQHCe5aRDeHv1DkkdwQiPRQSqYw2DqEic7MZ47iJVVTeQ1aknD

 · Jul 23, 2018 · 5 min read

Mining

A Case Study: How One Big Player Could Impact the Cohive Business in China

"Who is Stealing My Power" is a series of articles on the topic of web mining that we observed from our DNSMon system. As we mentioned in this series of one, two, and three , the players in the market can be mainly divided into mining sites and content/

 · Mar 9, 2018 · 3 min read

Mining

是谁悄悄偷走我的电（四）：国内大玩家对Coinhive影响的案例分析

《是谁悄悄偷走我的电》是我们的一个系列文章，讨论我们从 DNSMon 看到的网页挖矿的情况。在这个系列的之前的 一 、 二 和 三 中，我们已经介绍了整个Web挖矿的市场情况。当前我们知道，市场中的玩家主要可以分为挖矿网站和内容/流量网站，前者提供挖矿能力、后者提供流量，二者合力利用终端用户的浏览器算力挖矿获利。 当前，挖矿网站中最大的玩家是 coinhive 家族，按照被引用数量计，占据了 58% 的市场份额。这些在我们之前的文章中已经提及。 那么，流量网站的情况如何，有哪些有意思的情况？ Coinhive 的关联域名 DNSMon 有能力分析任意域名的 关联域名，在这个案例中可以拿来分析 coinhive 家族关联的 流量网站。通过分析这些流量网站的 DNS 流量，可以观察到很多有意思的事情。 下面是一个域名访问规模图： 在上图中: * 横轴：代表时间，从 2018-01-31到2018-02-15 * 纵轴：

 · Mar 9, 2018 · 6 min read

Mining

Who is Stealing My Power III: An Adnetwork Company Case Study

We recently noticed that one of the ad network provider started to perform in-browser coinhive

cryptojacking when users visit websites which use this provider's ad network service. As early as mid 2017, this ad network provider has been using domain DGA technology to generate seemingly random domains to bypass

 · Feb 24, 2018 · 6 min read

Mining

是谁悄悄偷走我的电（三）：某在线广告网络公司案例分析

我们最近注意到，某在线网络广告商会将来自 coinhive 的javascript网页挖矿程序，插入到自己广告平台中，利用最终用户的浏览器算力，挖取比特币获利。 P公司是一家在线广告网络公司，负责完成广告和广告位之间的匹配，并从中获取收入；Adblock 是一种浏览器插件，用户可以利用来屏蔽广告。显然，上述两者之间有长久的利益冲突和技术对抗。 在2017-09之前，我们就注意到 P公司 会利用类似 DGA 的技术，生成一组看似随机的域名，绕过 adblock，从而保证其投放的广告能够到达最终用户，我们将这组域名称为 DGA.popad。 从2017-12开始，我们观察到P公司开始利用这些 DGA.popad 域名，插入挖矿代码牟利。 广告网络公司与广告屏蔽插件之间的对抗并不是新鲜事，但是广告网络公司参与到眼下流行的网页挖矿，这值得引起我们的注意。 P公司背景简介 P公司是一家在线广告网络（adnetwork）公司。所谓在线网络公司，其主要工作是连接广告主（advertiser）和媒体（publisher），聚合publisher提供的广告位，并与广告主的需求进行

 · Feb 24, 2018 · 9 min read

Mining

Openload.co and Other Popular Alex Sites Are Abusing Client Browsers to Mining Cryptocurrency

As of December 24, 2017, we noticed a group of Alex top websites abusing client browser's computing power in cryptocurrency mining. The javascript code is based on CoinHive with tricks to completely circumvent CoinHive's own operations to avoid CoinHive's commission fee. A total of

 · Dec 29, 2017 · 4 min read

Mining

openload.co 等网站绕过 CoinHive 使用客户端浏览器算力挖取门罗币

从2017年12月24日，我们注意到一组网站正在滥用客户终端浏览器的算力在挖矿。攻击者在利用了 CoinHive 的浏览器端挖矿代码基础上，完全绕过 CoinHive 自己运营，避开了 CoinHive 的抽成费用。提供挖矿服务的域名成组出现，共计22个，最早活动时间是2017-11-29。 涉及使用上述挖矿服务的网站，包括openload.co，

oload.stream，thevideo.me，streamcherry.com，streamango.com。其中，openload.co 网站的Alex排名为136，流行程度非常高，这意味着全球范围内有较多的终端用户算力会被攻击者攫取。 5个异常域名 dnsmon 是我们的dns异常检测系统。在2017-12-24日，系统报告了一组域名的访问异常，这组域名和对应的访问曲线如下： do69ifsly4.me hzsod71wov.me kho3au7l4z.me npdaqy6x1j.me vg02h8z1ul.me 上图中可以注意到域名访问曲线惊人的一致，这意味着不同域名之间，很可能被同源的流量驱动。

 · Dec 29, 2017 · 8 min read

PassiveDNS

Fraudulent Top Sites, an Underground Market Infrastructure

[Update History] * 2017-01-16 First English version. Updates in original Chinese version is merged. Overview Some domain names contains strings representing well-known companies are noticed in our abnormal traffic detecting system, including 360, ali, baidu, cloudflare, dnspod, google and microsoft. We later found these strings are adopted by a mature dedicated

 · Jan 16, 2017 · 7 min read

PassiveDNS

以大站的名义：专注地下产业的网络基础设施

【历史更新记录】 * 2017-01-10 原始版本 * 2017-01-16 补充了对服务器IP地址同源性的分析，此处分析指向性较弱，仅为完备性考虑 概述 在奇虎网络安全研究院(netlab@360.cn)，我们建立了一个基于DNS的异常流量监测系统，每天会检出若干异常流量以及对应的域名/IP。通常这些被检出的域名/IP都属于地下产业链条。 但是，我们注意到一些代表知名公司的字符串也出现在这些被检出的域名中，包括360, ali, baidu, cloudflare, dnspod, google和microsoft。通过分析，我们认为这是有人冒用大站名义，为赌博、色情、私服等地下产业提供网络基础设施服务。 这一基础设施结构错综复杂，运营时间长、支撑能力强、实际支撑的黑色灰色站点数以万计，已经构成了一个成熟的地下产业生态系统。 域名和所仿冒的大站品牌 我们检测到的这类域名如下表。 如果只看域名，这些域名看起来非常象是大站提供的CDN服务。但分析可以看出，这些域名实际是某种基础设施，为赌博、色情、私服等地下产业服务。 基于上述域名的错

 · Jan 10, 2017 · 10 min read

PassiveDNS

DNS中的“无效Rdata”

所谓Rdata是指在DNS记录中与类型相关的数据部分。比如对于DNS的A记录中的IPv4地址或者MX记录中的主机名及其优先级。 在分析DNS的数据过程中，常常能见到各种不同种类的怪异的Rdata。我们把不能有效反应域名和rdata的对应关系的数据称为“无效Rdata”。对这些无效Rdata进行分析是理解DNS数据的一个有趣的切入

点。 另外，结合最近火爆的威胁情报，发现很多的数据源中，都包含了这些“无效的Rdata”，它们降低了这些威胁情报的质量。因此对这些无效rdata的过滤是提高威胁情报质量的一个重要手段。 尽管还有很多其他类型的无效的rdata，但是相比IP地址来说，其他种类的数据影响较小。因此本文主要讨论IP地址。 DNS Sinkhole的IP地址 DNS Sinkhole是安全厂商为了研究恶意软件的行为，将恶意软件的网络流量进行接管的一种方式，具体参见wiki的定义。 从PassiveDNS中的数据来看，sinkhole的域名主要集中在使用DGA技术产生随机域名的恶意软件上。比如上一篇blog中提到的conficker，以及大名鼎鼎的GOZ等。现在来

· Oct 9, 2016 · 8 min read

PassiveDNS

Conficker域名被滥用情况分析

根据对conficker域名的跟踪，我们发现conficker的域名存在明显的滥用。主要表现为浏览器访问conficker域名后，会跳转到广告页面（既有正常业务，也有赌博/色情等灰色业务），有时候还会存在一些垃圾软件（比如虚假的杀毒软件）的推广等。 由于conficker的DGA域名的巨大数量，我们希望了解产生这种状况的原因以及其现在的规模。 Conficker域名现状及被滥用状况 Conficker简介 Conficker是出现于2008年11月，曾感染了数百万台电脑。Conficker有一个独特的特性是它使用了DGA技术。利用随机生成的域名来防止网络设备的封堵。自此以后DGA技术也开始逐渐流行起来。关于conficker和DGA的细节，请参考[1] [2]。 校验数据集及passvieDNS中的命中情况 我们选取了2010-01-01到2016-09-15这段时间内，由conficker.a 和conficker.b生成的全部的DGA域名作为数据全集，共1225000条域名。 检查这些域名在passiveDNS中的命中情况。排除NXDOMAIN之外

· Sep 2, 2016 · 12 min read