

DNSMon

A collection of 29 posts

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件。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件。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

DNSMon

DNSMon: using DNS data to produce threat intelligence (3)

Background This article is the third in our series of articles introducing DNSMon in the production of threat intelligence (Domain Name IoC). As a basic core protocol of the Internet, DNS protocol is one of the cornerstones for the normal operation of the Internet. DNSMon, which was born and raised



· Feb 9, 2021 · 7 min read

DNSMon

DNSMon: 用DNS数据进行威胁发现(3)

--- Linux, Windows, Android, 一个都不能少 背景 本文是介绍DNSMon在生产威胁情报(域名IoC)系列文章的第三篇。DNS协议作为互联网的一项基础核心协议，是互联网得以正常运行的基石之一。在祖国960万平方公里的土地上，那一张纵横交错的数据网络里，每一秒都有数万亿计的DNS数据包在高速穿梭着，它们或来自于机房的服务器，或来自于办公室的电脑，或来自于我们身边的手机，或来自于场景繁多的IoT，总之DNS无处不在。生长于斯的DNSMon，依托DNS协议的基础性，天然具备宽广的视野，对那些发生在不同行业或不同平台的安全事件，都能有所涉猎。在DNSMon科普系列的前两篇博文中，第一篇提及的Skidmap是感染Linux平台的云主机；而第二篇提及的一组域名是网吧的Windows平台被感染后发出的；本文则是一个涉及Android平台的案例。如果仔细阅读文章并理解其中内容，可以看到DNSMon在面对3个差异巨大的平台时，所使用的知识点或者说规则并没有根本性的变化，几乎做到了无差别预警。对未知威胁的拦截 最近，我们注意到DMSMon从

2021-01-10



· Feb 8, 2021 · 10 min read

DNSMon

DNSMon: 用DNS数据进行威胁发现(2)

----DNSMon抓李鬼记 背景 本文是介绍DNSMon在生产威胁情报(域名IoC)系列文章的第二篇。为了对抗安全人员的分析，钓鱼域名是恶意样本经常采用的一种技术手段。从字符组成和结构上看，钓鱼域名确实具有混淆视听的功效，但对于DNSMon这种具备多维度关联分析的系统来说，模仿知名公司域名的效果则适得其反，因为这样的域名一旦告警，反而更容易引起分析人员的注意。本案例从一组疑似钓鱼域名出发，逐步介绍DNSMon是如何利用whois, ICP备案，域名解析内容和图关联等信息，让一组干瘪的域名逐渐一点点丰富起来直至最后恶意定性的。意料之外的是，随着线索的展开，我们发现这是一起失陷设备数量巨大的安全事件，从我们的数据测算，感染规模远超100w设备。为此，我们进行了较为细致的逆向分析和回溯，但限于篇幅，样本分析细节及其家族演变，将在后续再另起一篇介绍。通常威胁分析普遍的惯例是先知道样本恶意再逆向，有时根据DNS数据估算感染规模。这次DNSMon系列文章里揭示的，更多是先根据DNS数据发现异常并定性，再进一步探寻还原事件真相。即从先逆向再统计，变成了先统计再逆向。这个顺序



· Dec 31, 2020 · 14 min read

DNSMon

DNSMon: 用DNS数据进行威胁发现(1)

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，越来越多的业内人士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

DNSMon

Ongoing Credit Card Data Leak [Continues]

DNSMon is a network-wide DNS malicious domain analysis system we build here at 360Netlab. With the 10%+ total DNS traffic coverage in China, plus the other multi-dimensional security data and security...



· May 14, 2019 · 3 min read

DNSMon

信用卡数据泄漏持续进行中 [快速更新]

DNSMon是一个全网DNS异常发现分析系统。基于我们可以看到的中国地区 10%+ 的DNS流量，加上我们多年积累的其他多维度安全数据以及安全分析能力，我们可以在一个独特的视角来实时监测 全网 每天 正在发生的事情，我们可以“看见”正在发生的威胁。黑客在行动 5月8号，我们发布文章 <信用卡数据泄漏持续进行中>，揭露了一个通过入侵购物网站来窃取信用卡信息的案例。文章发布后不久，我们发现黑客们开始做调整，原始域名 magento-analytics[.]com 已经下线。但不久，我们的 DNSMon 系统在UTC时间 2019-05-13 凌晨时候捕捉到该黑客的2个更新，被用于同样的信用卡信息窃取。更新1：启动了一个新域名：jqueryextd[.]at 对应的恶意JS链接为 “hxps://jqueryextd.at/5c21f3dbf01e0.js”，脚本中上报地址也对应的改为了“hxps://jqueryextd.at/gate.php”



· May 14, 2019 · 3 min read

DNSMon

Ongoing Credit Card Data Leak

Our DNSMon flagged an abnormal domain name magento-analytics[.]com, been used to inject malicious JS script to various online shopping sites to steal the credit card owner/card number/expiration time/ CVV information.



· May 8, 2019 · 6 min read

数据泄漏

信用卡数据泄漏持续进行中

我们的DNSMon发现了一个异常域名 magento-analytics[.]com，通过持续的跟踪，以及和WEB数据的关联，发现该域名通过渗透侵入购物网站，植入自己的JS脚本，实时判定用户信用卡的输入情况，将信用卡的所有人/卡号/过期时间/CVV 信息回传，实现对信用卡数据的窃取，进而可以盗刷。当前估算，失陷的购物网站应该超过1000+。



· May 8, 2019 · 10 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 (Nitro) 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

DDoSMon

RSA大会 '2018, 360Netlab的威胁情报服务

RSA大会'2018 即将在4月16日至19日期间在美国旧金山Moscone中心举办。在今年的这次大会上，360Netlab将首次集中展示威胁情报服务能力。您可以在 [这里](#) 观看介绍视频，记得可能需要手动调到1080P。您也可以试用在线系统，包括 DDoSMon 和ScanMon 。 DDoSMon、ScanMon和DNSMon，是360Netlab本次展示威胁情报服务能力的三个主要组成部分。三者分别提供拒绝服务、网络扫描、域名异常的监控能力，应对全球网络流量实时处理。 * DNSMon是2018年新推出的能力。在DNSMon里面，我们实时的分析海量的DNS流量，并对流量中的各种异常和关联关系予以分析，从而发现大网流行的恶意代码行为。另一方面，DNSMon将我们指向未知威胁发现领域，我们期待在这个领域内作出更多成果。DNSMon相关已经公开的成功案例，包括之前公布的“偷电”系列分析文章。 * ScanMon早先在2016年ISC和2017 RSAC大会上两次公布。利用ScanMon，我们可以第一时间感知网络扫描行为，并方便有效的识别对应的攻击者。例如，360网络安全研究院在针



· Apr 13, 2018 · 2 min read

Mining

A Case Study: How One Big Player Could Impact the Coinhive 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

Browser Mining

是谁悄悄偷走我的电（二）：那些利用主页挖取比特币的网站

我们在早先的文章 中提到，大约有 0.2% 的网站在使用主页中嵌入的JS代码挖矿： - Alexa 头部 10万网站中，有 241 (0.24%)个 - Alexa 头部 30万网站中，有 629 (0.21%)个 我们决定还是公开文中提到的全部站点列表，这样读者可以采取更多的行动。我们的 DNSMon 在2018-02-08 生成的列表，其格式如下： Alexa_Rank Website Related-Coin-Mining-Domain/URL 1503 mejortorrent.com |coinhive.com 1613 baytpbportal.fi |coinhive.com 3096 shareae.com



· Feb 13, 2018 · 1 min read

Browser Mining

The List of Top Alexa Websites With Web-Mining Code Embedded on Their Homepage

On our previous blog, we mentioned over 0.2% websites have web mining code embedded in their homepage: 241 (0.24%) out of Alexa Top 100,000 websites, and 629 (0.21%) out of Alexa Top 300,000 websites. And after some discussion, we figured it makes sense to release



• Feb 8, 2018 • 1 min read