

DNSMon

# 商业数字证书签发和使用情况简介(删减版)



Zhang Zaifeng

Mar 23, 2022 • 14 min read

## 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”，“.pф”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计，共同构成了用以描述全球网络空间变迁的DNSMon系统。

为了摸清楚数字证书在实际网络空间中的真实情况，本文利用网络证书数据库(CertDB)，从数据角度来衡量网络证书数据在使用者和签发者组织和国别之间的分布情况。

# 数据筛选

我们从DNSMon系统中筛选了如下条件的证书：

1. 在最近3个月活跃的；
2. 非Let's Encrypt, 非Cloudflare签发的；
3. 签发者信息中包含国家信息的；
4. 非自签名或者其他不被认为是安全的证书；

通过以上方法，共计得到1,141,907个证书。

以上证书筛选条件的说明：

- 如果证书超过3个月没有活跃，我们认为这些证书所承载的网站的业务已经停止或者活跃度小，证书即使被吊销，影响也有限。
- Let's Encrypt签发的免费证书是现在证书数据的绝对大头。不过因为Let's Encrypt签发的是DV证书，并没有提供OV或者EV证书（关于证书级别的解释见后），所以重要机构和用户目前不会使用Let's Encrypt签发的证书。同理Cloudflare会在其客户中普及使用https，使用Cloudflare的域名都会有一个SSL证书。这两类数据不涉及我们今天分析的主题，所以把它们过滤掉。
- 在收集到的证书中，有些证书主体信息中包含了证书主体所在的国家，有些则没有包含。尽管可以通过证书主体通用名（subject CommonName）中的域名的ccTLD来识别主体所在国家，但并不是所有的CommonName都是ccTLD，此外ccTLD和实际使用中的主体也存在一定的不确定性。因此这次统计中，我们只查看在证书数据中包括明确主体国别标识的证书。

根证书，中间证书

- 什么是根证书机构

根证书是内置在浏览器或者操作系统中的可信证书文件，是整个PKI系统可信上诉链条的顶点，是PKI系统的锚点。全世界只有数量较少的根证书颁发机构。比如在[这里](#)firefox列出了其使用的跟证书列表，总共只有49个根证书机构，颁发了138个根证书。windows系统，macOS系统等也类似都有自己的根证书列表。

- 什么是中间证书机构

根证书RootCA不会直接面向企业或者个人用户颁发证书。这些证书数量少，影响范围广，万一出现密钥泄漏，影响太大。所以为了保护根证书，CAs通常会颁发所谓的中间根。CA使用它的私钥对中间根签名，使它受到信任，即所谓中间CA (*Intermediate CA*) 或者中间根。然后中间根使用中间证书的私钥签署和颁发终端用户SSL证书。这个过程可以执行多次，其中一个中间根对另一个中间根进行签名，然后CA使用该根对证书进行签名。这些链接，从根到中间到叶子，都是证书链。

值得提的一点是中间证书机构尽管可以签发证书，不过其在运营策略上会受控于上游RootCA。

目前主流的证书验证级别分为三种，分别是*Domain Validated(DV)*, *Organization Validation(OV)*和*Extended Validation(EV)*：

- DV验证是身份验证最少的SSL证书，即使是恶意程序也可以快速的轻松获取。这类证书主要用在个人网站，自媒体以及不包含个人敏感数据的网站。
- OV证书需要验证企业身份信息后颁发。OV SSL证书是当前最常见的证书类型，适用于行政、企业、科研、邮箱、论坛等各类大中型网站。
- EV顶级SSL证书，又称扩展验证型SSL证书。安全级别最高，验证审核最严格，网站部署EV SSL证书后，浏览器地址栏将变成绿色并显示企业名称。EV SSL证书一般应用于金融、银行、电商等安全需求较高的网站。

## 数据分析

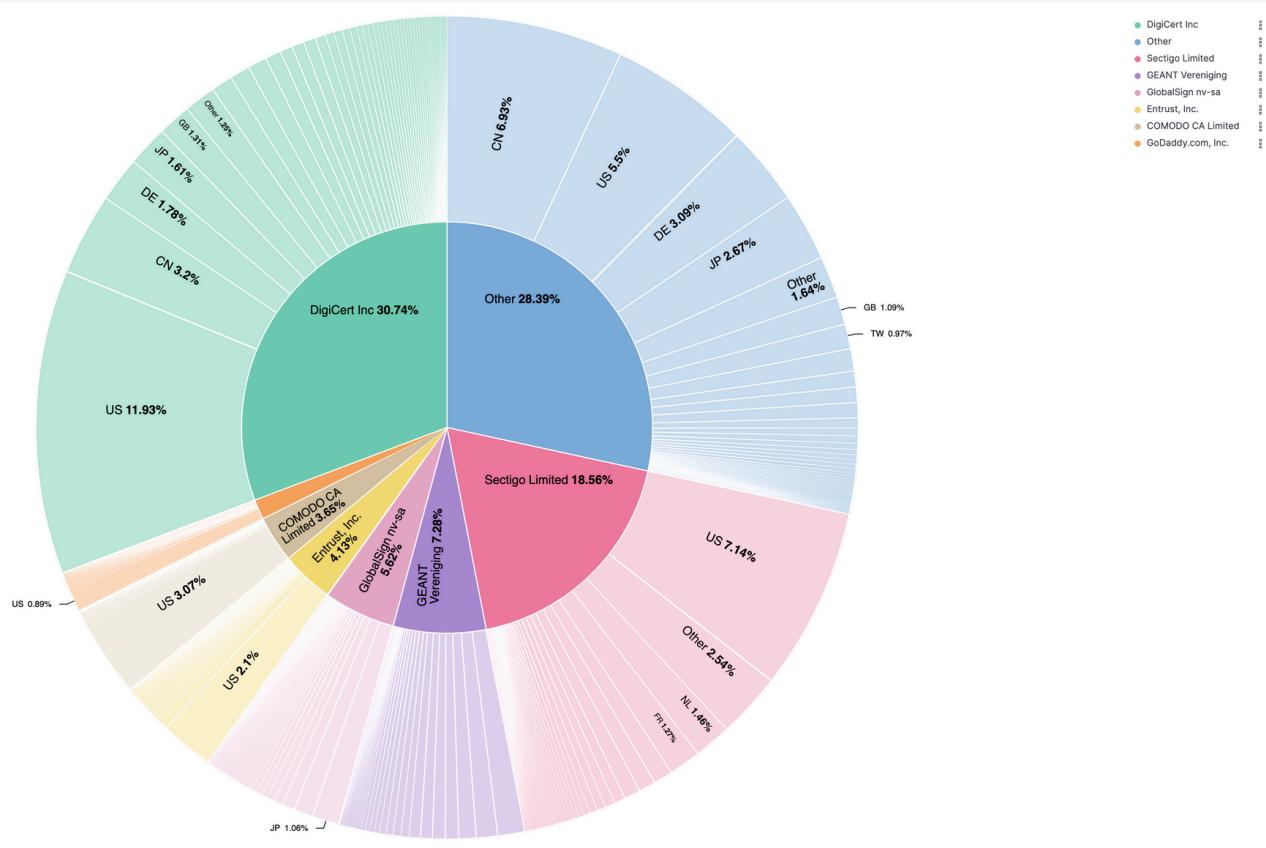
我们主要从两个角度即证书签发组织和证书签发组织所在国家来分析使用数字证书最多的50个国家和地区的情况。

由于无论是证书签发组织还是其所属国家，在网络证书数据中，均体现了二八定律，即少数的签发者签发了大量的证书，少数的国家签发了大量的证书。

所以我们分别选取了头部的签发机构和头部签发机构所在的国家来说明具体情况。

## 证书签发机构

在去掉Let's Encrypt和Cloudflare签发的证书之后，主要的证书签发机构就是一些大型的商业证书提供者。从证书签发机构的角度来看，其分布如下：

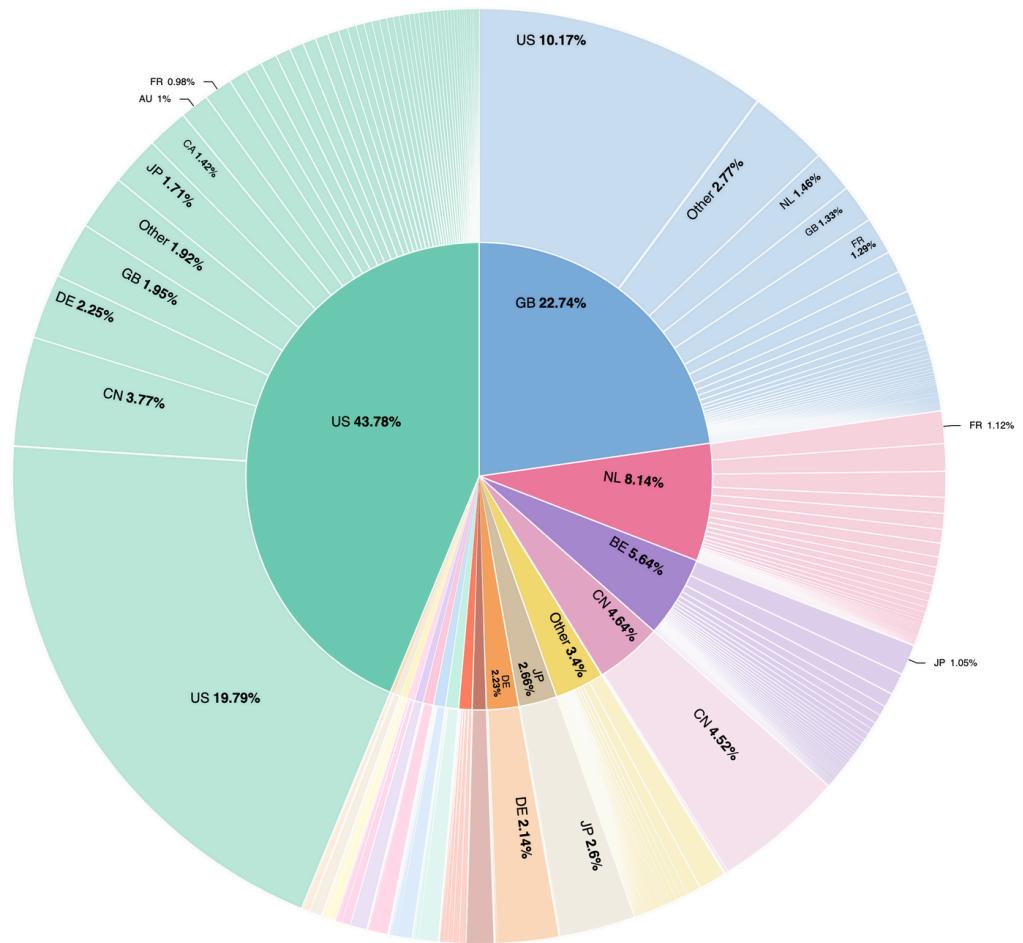


从上图可以得到：

1. DigiCert, Sectigo, GEANT Vereniging, GlobalSign和Entrust是从签发数量来说目前排名TOP5的证书提供商，占总证书数量的66%左右。
2. DigiCert相对来说提供的证书数量，区位覆盖度都要比其他的证书提供商更多更广泛。
3. 不同的证书提供商在不同区域的份额有显著的差异。比如：
  - 中国、日本、俄罗斯和巴西，DigiCert和GlobalSign的市场份额远大于Sectigo；
  - 美国、德国、荷兰和加拿大等地，Sectigo比GlobalSign更受欢迎；
  - 在欧洲国家，比如比利时、西班牙、法国和意大利等地，对GEANT Vereniging则情有独钟。
4. 其他的具体数据参见文后的详细数据。

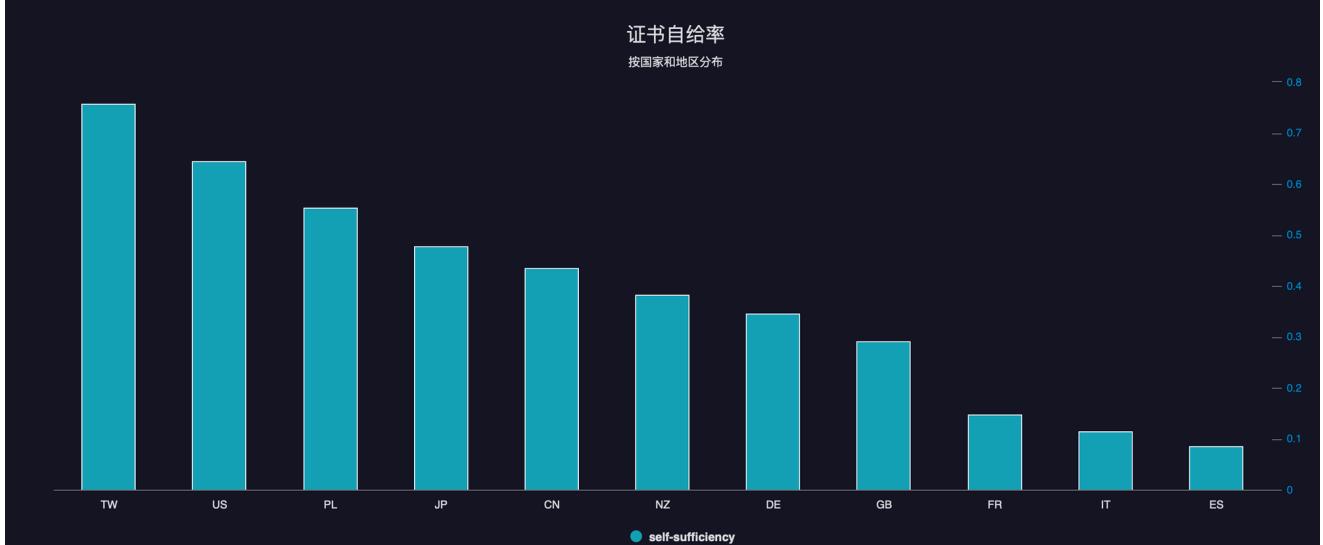
## 证书签发组织所在国家

为了看清楚证书提供商后面的国家分布，我们把签发主体中的C字段提取出来进行了统计。如下图：

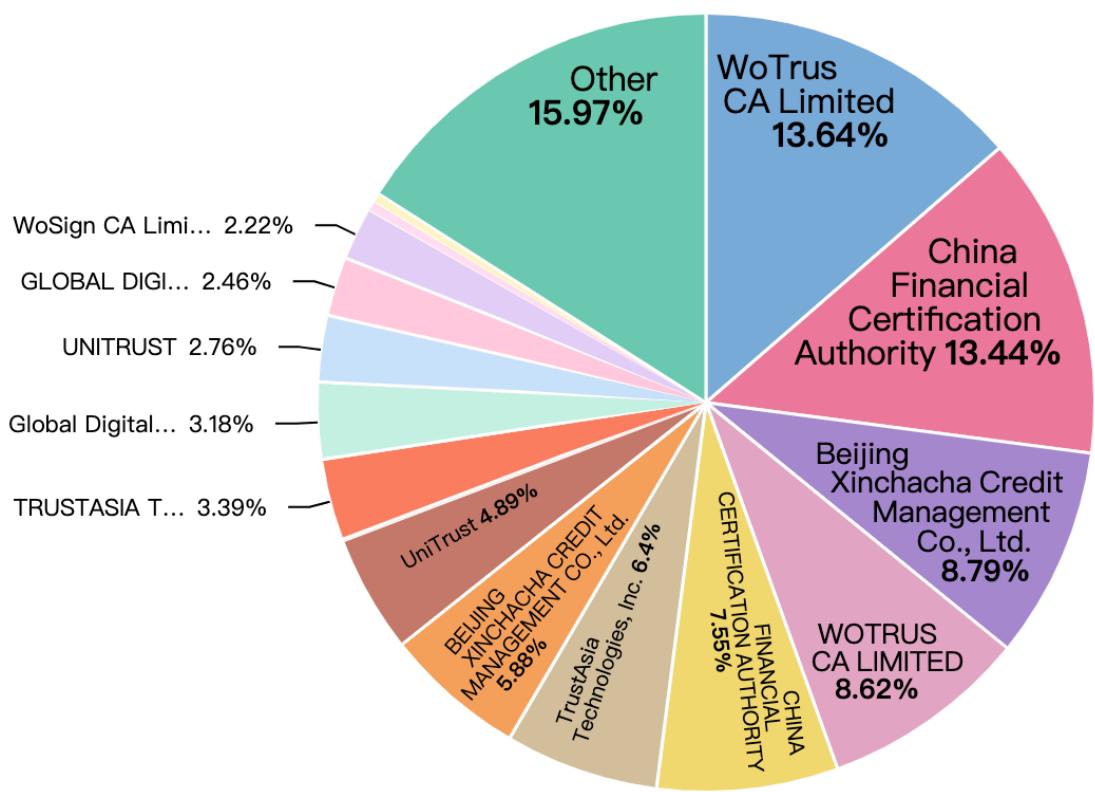


从图中可以看到：

1. 美国，英国，荷兰和比利时（如上节所示，比利时的份额主要是GlobalSign贡献，现被日本GMO公司收购）的整体份额加起来可以达到80.3%，占了绝对的统计地位。
2. 从服务的对象来看，美国，英国，荷兰，比利时等国家的证书注册机构的服务的对象是全球性的，覆盖广泛。国内的证书注册机构面向对象主要还是国内用户。
3. 从证书自给率上来看，中国台湾地区是自给率最高的，达到了75%，接下来是美国和波兰的自给率都超过了50%，分别达到了64%和55%；日本和中国大陆都超过了40%。其他国家都在40%以下。



4. 中国大陆头部的CA的占比如下：



可以看出国内主要是沃通，中国金融认证中心，北京信查查信用管理公司以及亚洲诚信等单位占据了国内证书市场的主流。

值得说明的时候，这些公司中，除了中国金融认证中心之外，其他的几个都是中间CA。其中沃通和北京信查查的上游CA是位于波兰的Certum。亚洲诚信的上游是DigiCert。沃通曾经是rootCA，后来因为多种原因被浏览器厂家相继屏蔽。

关于国内网站的证书普及情况以及相关的CA情况，后续大家也许会看到我们专门的介绍文章。

5. 其他具体的数据参见文后的数据。

## 证书自给率

证书自给率（数字证书自给率）是我们给出的一个词汇。主要用来衡量一个国家或地区在使用证书方面的对外依赖程度。证书自给率越高，表明该经济体的证书签发和使用程度越高，同时证书的对外依赖程度越低。

计算方法是通过计算证书的签发机构所属国别和证书主体所属国别是否一致来计算得到。即：

证书自给率 = 签发机构国家和证书主体国家相同的证书数量 / 证书主体国家全部的证书数量。

## 结论

1. 在去除掉大量的免费证书之外，在商业证书领域，少量的证书签发机构占据了大量的市场份额。
2. 如果从国家和地区的角度来看，第一点中提到的聚集性体现的更加明显，头部的4个国家签发的证书占全部证书的80.3%。
3. 中国大陆的证书自给率有43.6%（详见详细统计数据表二），目前尚缺乏在全球有竞争力的证书签发机构。

## 参考资料

1. <https://pastebin.com/DLbmYahS>
2. <https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-o2mar22-en.pdf>

## 详细统计数据

### 表一：证书使用国家按签发机构统计

注：表中为空项表示CA机构签发该国的证书数量较少，合并到了Other项中。

Top values of subject\_C|DigiCert Inc|Sectigo Limited|GEANT

Vereniging|GlobalSign nv-sa|"Entrust, Inc."|COMODO CA

Limited|"GoDaddy.com, Inc."|Other|sum

| - | - | - | - | - | - | - | - | - | - |

US|136185|81530||5548|24028|35088|10172|62861|355412  
CN|36579|542||8637|414|12|415|79145|125744  
DE|20369|8499|2202|3557|895|86|251|35302|71161  
JP|18369|894||12052|481||38|30524|62358  
GB|14904|7640|9609|2495|2183|1011|1528|12418|51788  
FR|9561|14486|12085|2727|758|255|85|10004|49961  
AU|9035|2427||263|1068|72|476|3519|16860  
CA|8602|7346||907|5852|907|857|1069|25540  
KR|7082|4480||1760||16||682|14020  
ES|5583|3573|5282|1402|821|411|171|2014|19257  
RU|5550|696||3972|||2421|12639  
IT|5500|5009|5705|1058|688|167|193|3339|21659  
CH|4643|2575||284|141|14|160|7099|14916  
SE|3951|1541|2399|797|58||175|2009|10930  
IN|3799|810||1526|1189||762|655|8741  
NL|3507|16635|7701|771|237|114|72|4555|33592  
HK|3109|1859||655|110|87|324|1252|7396  
BR|2574|1370||2477|187|9|374|1052|8043  
MX|2446|452||335|133||350|194|3910  
AT|2374|1504|3548|217|131||113|1111|8998  
AE|2048|||434|61||133|286|2962  
SG|1846|738||484|1419|9|140|184|4820  
DK|1752|451|421|1310||14|40|347|4335  
ID|1730|390||174|59|||2353  
CZ|1652|210|3670|44|||1182|6758  
NO|1575|1355|1905|259|76||46|644|5860  
FI|1568|658|1995||1384||59|1170|6834  
CO|1545|318||320|51||249||2483  
ZA|1411|897|||1105||50|223|3686  
NZ|1406|262|||347||54|1970|4039  
SA|1393|||70|112||28||1603  
TH|1261|||592|391||15||2259  
PL|1235|520|3159||72|||6843|11829  
MY|1222|342||807|375||62||2808  
BE|1194|3856|5191|1323|307||51|562|12484

AR|1051|394||44|40||82||1611  
 IE|963|379|742|65|97|38|57|856|3197  
 TW|926|1722||435|||302|11099|14484  
 CL|833|227||1010|41||57||2168  
 IL|760||542||||61||1363  
 PT|689|1154|2807|106|41|46|58|373|5274  
 GR|681|286|1168||58|||889|3082  
 TR|681|297||1318||566|45|263|3170  
 PH|642|||618|297||69||1626  
 VN|623|197||1205|141||12||2178  
 CY|558||176|||21||755  
 KW|556||||36||||592  
 PK|487|||||19||506  
 RO|420|263|509|||||286|1478  
 EC|417|||196|||26||639  
 Other|14221|33154|12336|1970|1271|2761|269|35764|101746

## 表二：证书使用国家按签发机构所属国家统计

注：表中为空项表示CA所属国签发该国的证书数量较少，合并到了Other项中。

TOP VALUES OF SUBJECT_C	US	GB	NL	BE	CN	JP	DE	
US	226208	116240		5550	595	20	89	
CN	43078	651	295	8659	51655	344	488	
DE	25761	8573	3390	3557	25	1	24494	
GB	22298	15144	10178	2495	8		2	
JP	19488	897		12052	7	29743	2	
CA	16203	8282		907	6		1	
AU	11401	2509	52	263	4	1	3	
FR	11201	14759	12832	2727	13		111	
KR	7276	4505		1760			17	
ES	6646	3993	5499	1402	7			
IT	6596	5184	6228	1058				

TOP VALUES OF SUBJECT_C	US	GB	NL	BE	CN	JP	DE
IN	5968	817		1526			
RU	5590	704		3972	9		
CH	5151	2592	484	284	12		28
SE	5122	1543	2492	798			2
NL	4431	16709	10825	771			7
HK	3657	1946		655	23	2	
SG	3490	747		484		2	
BR	3206	1379		2477			2
FI	3154	656	2189				
MX	3031	453		335			
AT	2888	1504	3806	217	4		82
ZA	2632	899					
AE	2374			434			
DK	2052	465	449	1310			
NZ	1914	264					
CO	1868	317		320			
ID	1822	392		174			
NO	1815	1358	2022	259			2
CZ	1713	213	4106	44			29
TH	1677			592			
MY	1674	342		807			
BE	1582	3857	5458	1585			9
SA	1564			70			
PL	1364	521	3333		19		18
TW	1300	1724		435	6	3	
IE	1209	418	797	65			
AR	1202	394		44			1
PH	1022			618			

TOP VALUES OF SUBJECT_C	US	GB	NL	BE	CN	JP	DE
CL	952	230		1010			
IL	847		576				
PT	804	1201	3030	106			
VN	789	201		1205			
TR	758	863		1318			
GR	757	287	1315				
PE	680	603		147			
CY	606		195				
KW	596						
PK	514						
EC	488			196			
Other	21910	35588	13494	1825	620	250	136

0 Comments

1 Login ▾

G

Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS [?](#)

Name



Share

Best [Newest](#) [Oldest](#)

Be the first to comment.

[Subscribe](#)

[Privacy](#)

[Do Not Sell My Data](#)

— 360 Netlab Blog - Network Security Research Lab at 360 —

## DNSMon



俄乌危机中的数字证书：吊销、影响、缓解

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

解析服务提供商对非授权域名解析情况的评估

[See all 28 posts →](#)

honeypot

## What Our Honeypot Sees Just One Day After The Spring4Shell Advisory

Background On March 31, 2022, Spring issued a security advisory[1] for the Spring4Shell vulnerability (CVE-2022-22965), this vulnerability has caused widespread concern in the security community. When we looked back at our data, our threat hunting honeypot System[2] had already captured activities related t...



Apr 1, 2022    17 min read



Botnet

## New Threat: B1txor20, A Linux Backdoor Using DNS Tunnel

Background Since the Log4J vulnerability was exposed, we see more and more malware jumped on the wagon, Elknot, Gafgyt, Mirai are all too familiar, on February 9, 2022, 360Netlab's honeypot system captured an unknown ELF file propagating through the Log4J vulnerability. What stands out is that the network



Mar 15, 2022    11 min read

