

DNSMon

俄乌危机中的数字证书：吊销、影响、缓解



Zhang Zaifeng

Apr 2, 2022 • 28 min read

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，我们有足够的坚实的数据基础来解读本次俄乌危机中俄罗斯网络空间中网站证书的变化情况。

3月初，乌克兰政府向互联网域名管理机构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。本文

利用DNSMon的证书数据库，从数据角度来更准确的衡量这个现象在实际数据中的表现。

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签发的
3. 证书主体国家是俄罗斯或者证书主体的CommonName的域名以.RU或者.SU[3]结尾
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336,330个证书。

证书以及以上证书筛选条件的说明：

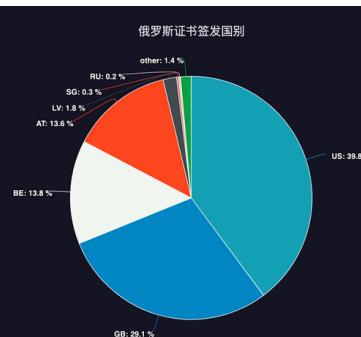
- 如果证书超过3个月没有活跃，我们认为这些证书所承载的网站的业务已经停止或者极度小，证书即使被吊销的影响有限。
- Let's Encrypt签发的免费证书是现在证书数据的绝对大头。不过因为Let's Encrypt签发的是DV证书，并没有提供OV或者EV证书[5]（关于证书级别本文后续有简要解释，读者也可自行搜索），所以重要机构和用户目前不会使用Let's Encrypt签发的证书。

数据分析

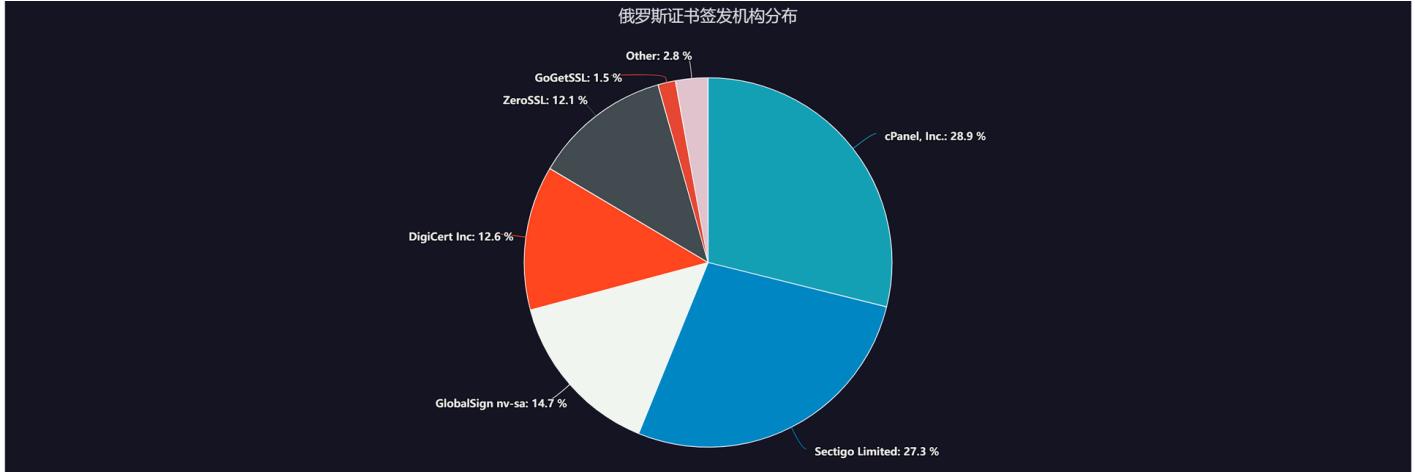
基本数据

在 336,330 个证书中：

签发的国家（证书数据中签发者的国家信息）有近30个，从下图可以看出主要集中在美，英，奥地利，比利时和拉脱维亚，占比达到了97.6%。俄罗斯自身的证书签发机构占比只有0.2%左右：



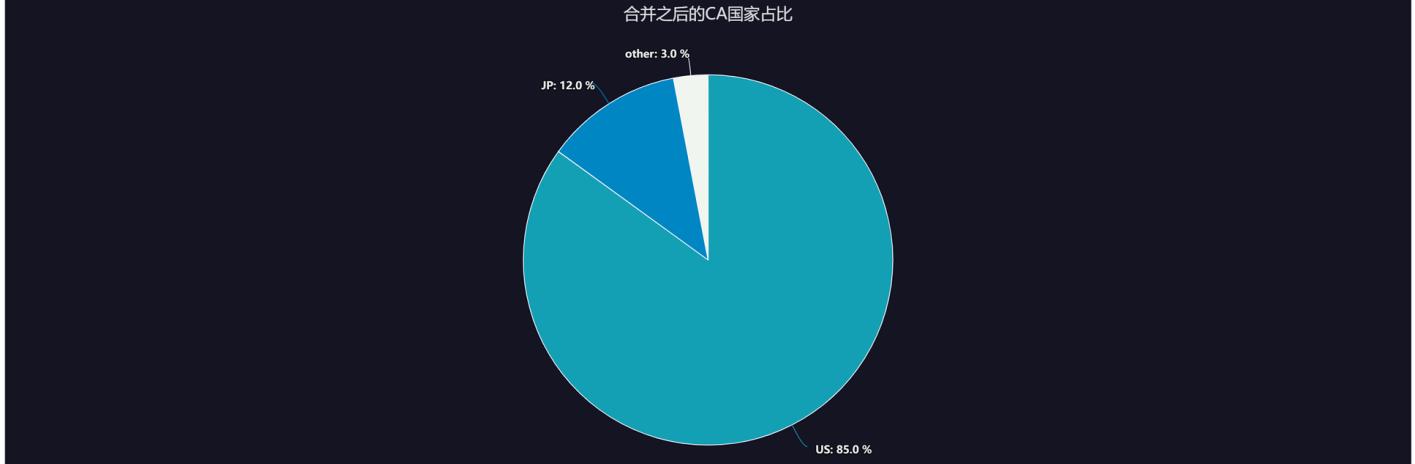
在这些所有的证书里面，涉及到的签发的机构有50+，其中top5的签发机构签发的证书占总数的95.6%。如下图所示：



在靠前的六家签发机构中，我们考察了其上游证书提供商及所属国别：

1. cPanel是一家美国的做web系统托管服务的公司，严格来说并不是CA厂商，不过它的证书是由comodo(已被如下排名第二的sectigo收购)签发的。
2. Sectigo是美国专门做证书服务的公司，也是使用范围最广的CA之一。它既是根证书机构，也是面向最终消费者的中间证书机构。
3. DigiCert是美国专业的证书服务公司。同Sectigo一样，也是使用范围最广的CA，既是根证书机构，也提供中间证书服务。
4. GlobalSign是比利时的专业证书服务公司，后来被日本GMO集团收购。同样既是根证书机构，也提供中间证书服务。
5. Zerossl是一家专门做SSL证书服务的位于奥地利的公司，不过其父公司被美国公司Idera收购，我们注意到该公司公告根据美国出口法规限制从2020年11月就不再给.ru的顶级域颁发证书了[11]。但从我们的数据来看，证书一直没有中断颁发，这其中尚不确定具体原因是什么。
6. GoGetSSL是一家专门做SSL证书服务的位于拉脱维亚的中间证书提供商。是DigiCert的白金合作伙伴和Sectigo的战略合作伙伴，在证书撤销方面本文后续可以看到它和Sectigo具有一致行动性。

如上，如果从中间证书的上游根证书所属国别来看，俄罗斯的证书签发机构所属的国家分布就变成了下图这样，即美国独自占85%，日本占12%。俄罗斯的选择余地实在很小。



在这336,330个证书中，来自俄罗斯的签发机构只有如下3个并且它们都不是根证书机构，也就是说俄罗斯并没有全球公认的根CA：

| NAME | UPSTREAM |
|---|---------------------------|
| RU-Center (ЗАО Региональный Сетевой Информационный Центр) | The USERTRUST Network |
| Yandex LLC | Unizeto Technologies S.A. |
| VTB BANK (PJSC) | GlobalSign |

证书相关小百科：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

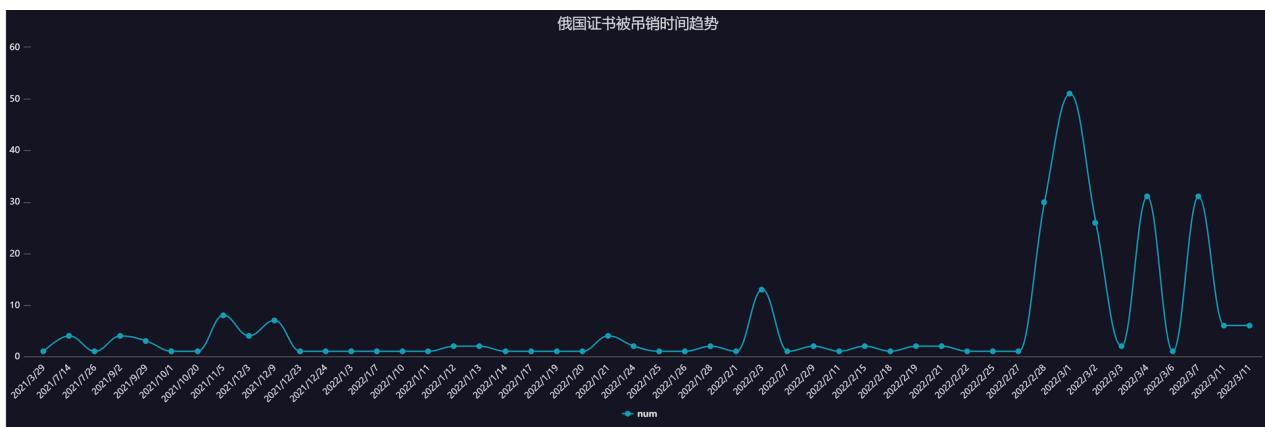
根证书RootCA不会直接面向企业或者个人用户颁发证书。这些证书数量少，影响范围广，万一出现密钥泄漏，影响太大。所以为了保护根证书，CAs通常会颁发所谓的中间根。CA使用它的私钥对中间根签名，使它受到信任，即所谓中间CA (*Intermediate CA*) 或者中间根。然后中间根使用中间证书的私钥签署和颁发终端用户SSL证书。这个过程可以执行多次，其中一个中间根对另一个中间根进行签名，然后CA使用该根对证书进行签名。这些链接，从根到中间到叶子，都是证书链。上面提到的俄罗斯的3个证书签发机构都是中间根。

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。

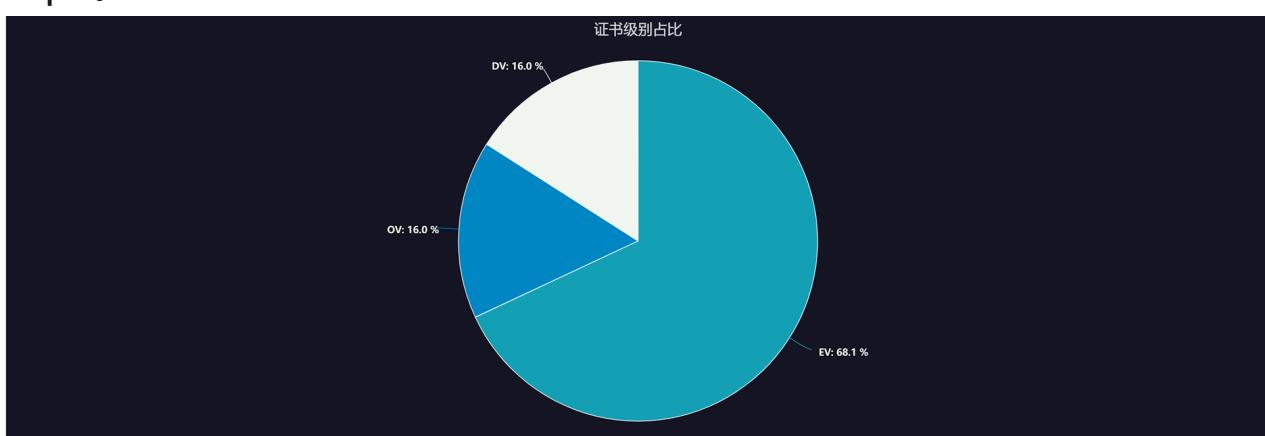
吊销数据

通过对整体数据进行分析，我们发现：

1. 目前有265个证书被吊销，其中2022年吊销了228个。
2. 从吊销时间上来看，主要集中在2022年的0228 ~ 0307这个段时间，这段时间共吊销了172个证书，占总数的64.9%。



3. 我们查看了对应证书吊销列表文件(CRL)中对吊销证书的吊销原因，发现绝大部分(95%)都没有明确的原因。
4. 从证书级别上来看，这次撤销的证书整体比较高，EV，OV的证书占比达到了84%。

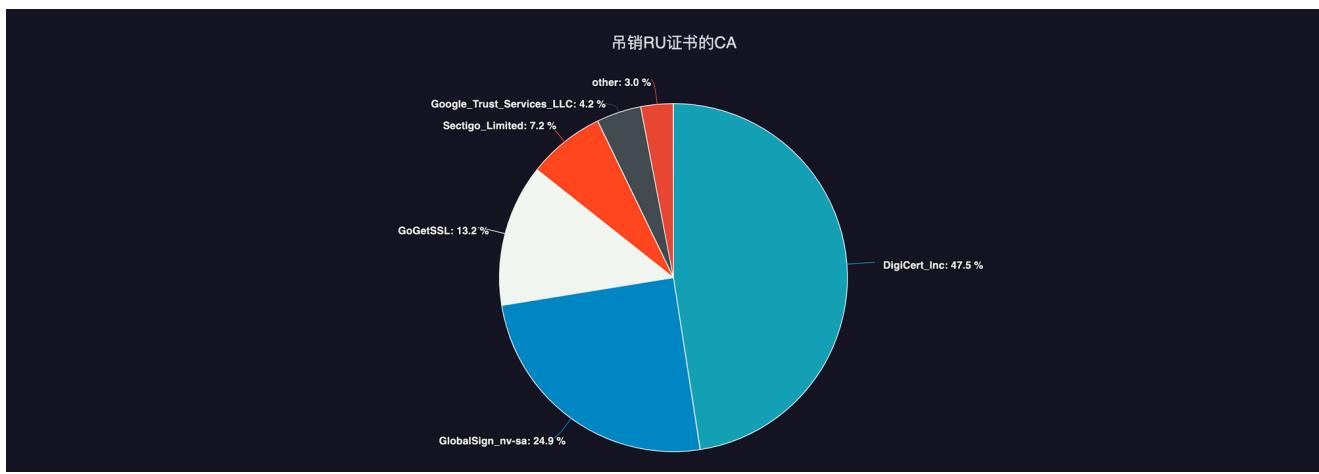


证书相关小百科：证书级别

- 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。

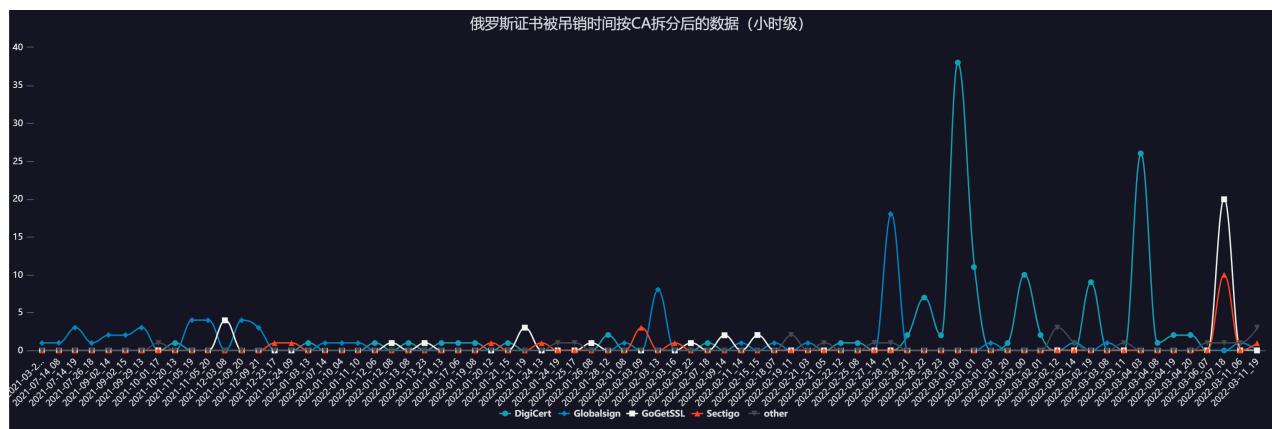
5. 这些被吊销的证书CA集中在少数几个CA上，总结情况如下：



这其中排名前4的分别是：DigiCert, GlobalSign nv-sa, GoGetSSL和Sectigo。

DigiCert撤销了126个（占DigiCert签发的俄罗斯的证书总数的0.5%），占总撤销总数的47.54%，更是占了2022年之后撤销总数的55.26%左右。

6. 我们将DigiCert, GlobalSign nv-sa, GoGetSSL和Sectigo以及其他涉及的CA拆分开，统计了其在小时级时间粒度上撤销证书的数量，见下图。



21: 00开始持续到3.1, DigiCert开始了其大量的吊销, 最高达到每小时38个, 接下来是GoGetSSL和Sectigo后两者在时间上有一致性。

我们进一步拨开这些数据看一下, 发现Globalsign nv-sa撤销的证书和其他三家CA有着显著的不同。

- 首先是证书的域名不同。Globalsign的撤销的证书的域名是新注册的域名, 并且子域名有着相似的特征(都包含有owa,audodiscovery,mail,www等子域), 可能是某些特定业务的域名。而其他三家撤销的则是老域名(域名列表见本文后面)。

| | | | |
|---|--------------|-----|------------|
| owa.recomend.ru | lrecomend.ru | 二级域 | 2022-02-18 |
| www.rodse.ru | rodse.ru | 二级域 | 2022-02-17 |
| autodiscover.stellos.ru | stellos.ru | 二级域 | 2022-02-15 |
| autodiscover.texlite.ru | texlite.ru | 二级域 | 2022-02-11 |
| www.kompase.ru | kompase.ru | 二级域 | 2022-02-10 |
| mail.kompase.ru | kompase.ru | 二级域 | 2022-02-10 |
| autodiscover.kompase.ru | kompase.ru | 二级域 | 2022-02-10 |
| owa.kompase.ru | kompase.ru | 二级域 | 2022-02-05 |
| www.plutus24.ru | plutus24.ru | 二级域 | 2022-02-05 |
| owa.plutus24.ru | plutus24.ru | 二级域 | 2022-02-04 |
| autodiscover.plutus24.ru | plutus24.ru | 二级域 | 2022-02-04 |
| mail.plutus24.ru | plutus24.ru | 二级域 | 2022-02-04 |
| mail.recomend.ru | lrecomend.ru | 二级域 | 2022-02-01 |
| www.lrecomend.ru | lrecomend.ru | 二级域 | 2022-02-01 |
| autodiscover.lrecomend.ru | lrecomend.ru | 二级域 | 2022-02-01 |
| owa.style365.ru | style365.ru | 二级域 | 2022-02-01 |
| mail.style365.ru | style365.ru | 二级域 | 2022-02-01 |
| autodiscover.style365.ru | style365.ru | 二级域 | 2022-02-01 |
| www.energias.ru | energias.ru | 二级域 | 2022-01-24 |
| www.dankirs.ru | dankirs.ru | 二级域 | 2022-01-24 |
| autodiscover.dankirs.ru | dankirs.ru | 二级域 | 2022-01-24 |
| mail.vira-sale.ru | vira-sale.ru | 二级域 | 2022-01-24 |
| mail.plaufo.ru | plaufo.ru | 二级域 | 2022-01-23 |
| owa.energias.ru | energias.ru | 二级域 | 2022-01-23 |
| www.plaufo.ru | plaufo.ru | 二级域 | 2022-01-23 |
| autodiscover.vira-sale.ru | vira-sale.ru | 二级域 | 2022-01-23 |
| www.vira-sale.ru | vira-sale.ru | 二级域 | 2022-01-23 |
| mail.dankirs.ru | dankirs.ru | 二级域 | 2022-01-23 |
| autodiscover.rodse.ru | rodse.ru | 二级域 | 2022-01-23 |
| www.deosal.ru | deosal.ru | 二级域 | 2022-01-23 |
| www.aveteks.ru | aveteks.ru | 二级域 | 2022-01-22 |

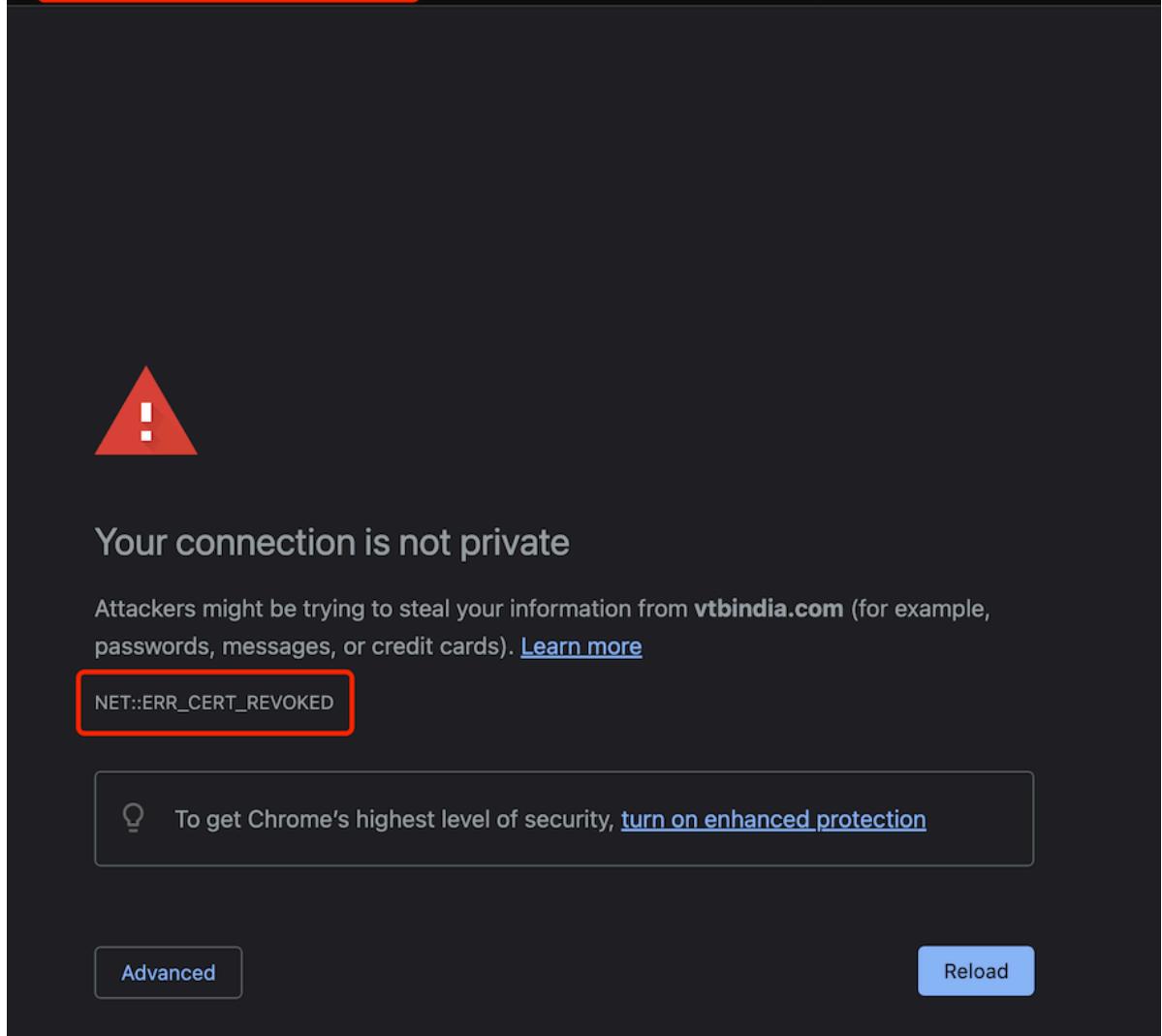
- Globalsign撤销的证书的域名通过搜索引擎搜索发现其并非特定或者关键行业的域名，其他三家撤销的证书的域名则是绝大多数都涉及到银行，保险等金融行业，还有一个证书涉及铁路行业。

考虑到证书吊销在时间上的集中性以及所属行业特点，我们合理判断总数265个证书中的144个是因为对俄罗斯制裁所产生的。撤销涉及DigiCert，GoGetSSL和Sectigo三个证书签发机构。

7. 被吊销之后域名使用的新的证书

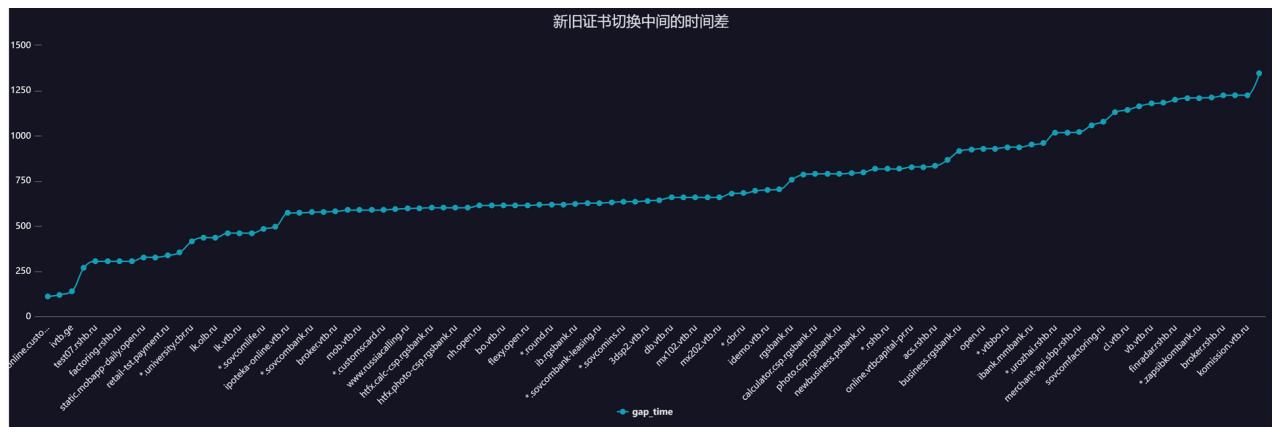
在被吊销之后，正常的业务访问会受限，比如浏览器会提示证书已经被吊销从而无法进一步访问业务。为了维持业务的正常运作，这些受影响的网站必须寻找替代的解决方案。因此我们考察了这些受影响网站是否启用了新的证书。如果启用了的话，是用的哪家，以及这个过程需要多长时间。经过我们统计之后发现受影响的俄罗斯金融机构大致有四种选择（详细信息见下表）：

- 原先有些单位本身就是中间根证书签发机构，这类单位现在使用的是自己单位签发的中间证书，其授权上游证书来自GlobalSign，因为有被浏览器承认的RootCA，所以这类证书使用起来没有问题。这类代表是俄罗斯外贸银行VTB集团。同类型的单位包括：VTB集团相关的所有域名。
- 使用Let's Encrypt签发的证书。Let's Encrypt是美国的一家免费证书提供机构，但是其不能提供OV和EV类型的证书，并且其证书的有效期也比较短。使用这类证书在某种程度上是被迫对证书安全性做了降级。这类的代表是跟保险行业较为紧密相关的sovcomins.ru，以及俄罗斯农业银行rgsbank.ru等相关的域名。
- 还有一类则从DigiCert切换到了 GlobalSign nv-sa 签发的证书。这类很好理解，弃用了DigiCert，转用了GlobalSign，业务暂时也不受影响。比如俄罗斯联邦中央银行crb.ru，以及部分rgsbank.ru的域名，open.ru的域名等。
- 还有少数金融机构比如vostbank.ru，vtbindia.com，psbinvest.ru等域名还在使用被吊销的证书，没有采取任何动作。目前访问的话，会提示证书被吊销，业务受到了影响。比如vtb印度的网站就会被chrome提示证书已经撤销，无法继续进行访问：



8. 证书切换对业务的影响

我们调查了这些受影响的域名在证书吊销之后启用新的证书之前，到底花了多长时间。从我们获取的数据来看，平均要花711分钟，也就是接近12个小时才能完成证书的切换。其中最快的用了109分钟(1.8小时)，最慢的则用了1346分钟（22.4小时）。



同时我们也对比了新证书的级别和老证书的级别发现：

- * 53%的网站的证书出现了降级
- * 45%的网站证书级别保持不变
- * 2%的网站证书级别进行了提升

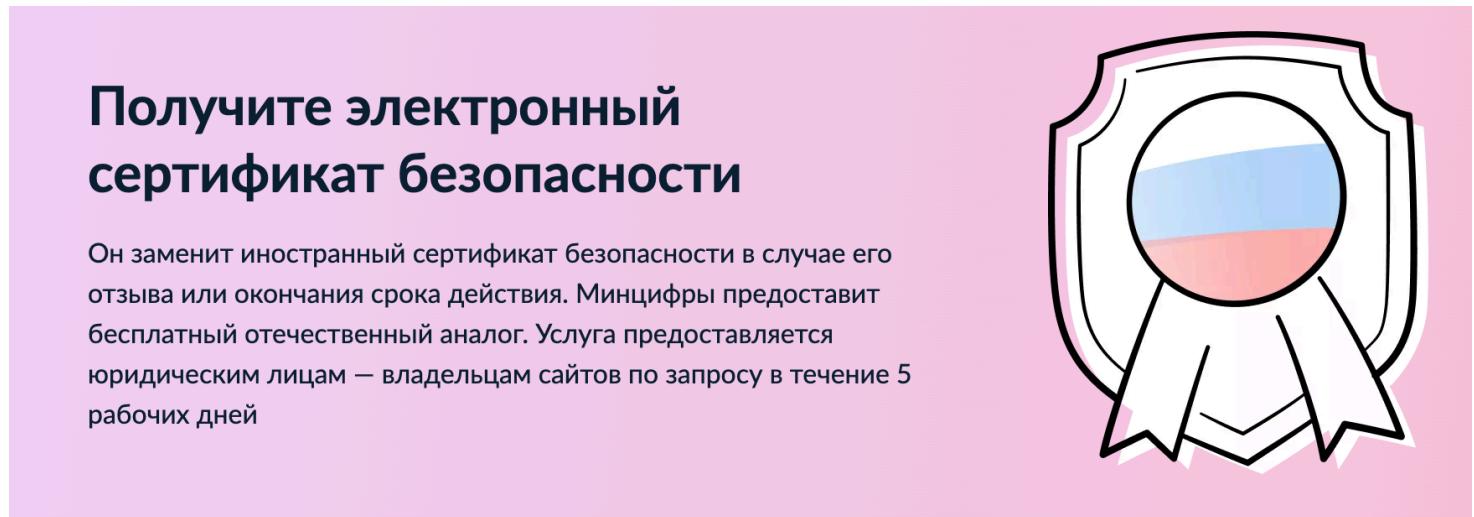
被吊销证书的列表

从2022-02-28之后在2022-03-11之前吊销和俄乌危机所引发的制裁相关的证书，涉及到DigiCert, Sectigo和GoGetSSL三个证书提供商，共包含144个证书。详细的证书列表见本文最后。

签发机构的态度和俄罗斯的动作

根据目前的消息[7]，Sectigo和DigiCert已经开始限制来自俄罗斯和白俄罗斯的业务。所以如果俄罗斯没有自己的证书签发机构和对应的可信RootCA的话，并且同时面对经济制裁的情况下，通用的付费方法可能也无法进行支付。所以即使目前的证书不吊销，现有证书过期之后仍然面临无证书可用的尴尬境地。

为了解决这个问题，俄罗斯推出了自己的CA:www.gosuslugi.ru [8]



但即便俄罗斯做了如此举动，仍然无法绕过一个核心问题，RootCA如果需要被广泛的用户终端/基础软件缺省内置是需要经过一系列庞杂繁琐的流程。在俄罗斯被广泛制裁的前提下，这个RootCA被外界广泛承认的可能性是0。比如从浏览器的角度来说，常见的chrome, Firefox, IE, opera等不支持此根，这个根的意义形同虚设。

值得提的一点是 www.gosuslugi.ru 自身使用的证书仍然是来自于Sectigo的签发。

目前网上流传着一份据说是俄官方的名单，要求198个重点域名使用这个CA[9]。我们注意到这个列表里面的6个域名（二级域）已经在我们这次看到的吊销的域名里面。

基本结论

目前来看，本文得到了如下的几个结论：

1. 受影响的网站比例并不高，被撤销的证书约为俄罗斯在用证书的0.04%左右；
2. 受影响的行业主要集中在银行及金融相关的行业，可能会对相关企业的客户带来一定程度的混乱，尤其是尚未部署新证书的业务；
3. 证书的主要撤销者是DigiCert，接下来是Sectigo和GoGetSSL。

参考资料

1. <https://pastebin.com/DLbmYahS>
2. <https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf>
3. <https://www.iana.org/domains/root/db/su.html>
4. <https://thehackernews.com/2020/09/ssl-tls-certificate-validity-398.html>
5. <https://letsencrypt.org/docs/faq/>
6. https://en.wikipedia.org/wiki/Certificate_authority
7. <https://www.gogetssl.com/news/27.html>
8. <https://www.gosuslugi.ru/tls>
9. https://www.documentcloud.org/documents/21408455-tls_list2?responsive=1&title=1
10. <https://www.bleepingcomputer.com/news/security/russia-creates-its-own-tls-certificate-authority-to-bypass-sanctions/>
11. <https://help.zerossl.com/hc/en-us/articles/360060119833-Restricted-Countries>

证书吊销列表

| REVOKE_TIME | SUBJECT_COMMONNAME | SHA1 |
|---------------------|-----------------------|--------------------------------------|
| 2022-02-28 21:17:23 | ibank.mmbank.ru | 0e2574eee86f03bad8737975c8e8c6b0e |
| 2022-02-28 21:17:43 | *.bvb.by | 747347ce6f5206d4abe44984beb222faf |
| 2022-02-28 22:02:32 | 3dsp.vtb.ru | 1ff80de2b0a83fadca20512c77625a3886 |
| 2022-02-28 22:06:28 | 3dsp2.vtb.ru | 95af9277b6ed216dc0734cd1e2c79253c |
| 2022-02-28 22:06:38 | *.vtbf.ru | 11aa6e2bf223fcc4aa83ef40fc40c563d8 |
| 2022-02-28 22:08:33 | *.customscard.ru | db4a27987a5cedfcfb4cd78144a74e298 |
| 2022-02-28 22:10:57 | online.customscard.ru | 82aa023ce89f3ea2406e3721dc77ecc82 |
| 2022-02-28 22:55:15 | *.cbr.ru | 23280fa352673271c377dec3041dee535 |
| 2022-02-28 22:55:30 | *.cbr.ru | 7aafcfc6c359f1184b686a2f57d5100f728 |
| 2022-02-28 23:02:21 | rgsbank.ru | f9756126c514426771c1ee2280fcc67065 |
| 2022-02-28 23:08:44 | open.ru | c2b40abb6e79744796d65887cc782f3e0 |
| 2022-03-01 00:12:35 | smtp1.open.ru | 905ee42c2722e5e1659e8896f656e52b |
| 2022-03-01 00:13:34 | mc.vtb.ru | bde9131020e014bbd71d7048ba2fe2ea1e |
| 2022-03-01 00:13:39 | ipoteka.vtb.ru | 37f4bc7254c469b0e8d3698aa299bc34 |
| 2022-03-01 00:13:49 | *.vtb.ru | 29ffe2f41fc0cdbac7addaf74f27804734f0 |
| 2022-03-01 00:14:47 | mob.vtb.ru | 314daeae50add8da4289367b4653fccf7c |
| 2022-03-01 00:15:18 | dachatbot.vtb.ru | 393e42d01f8bf9aa5c2986fc27bf82ab73 |
| 2022-03-01 00:16:40 | lk.olb.ru | 2b6186e5471cb85d0b2b446f4357576b |
| 2022-03-01 00:16:45 | dbo.vtb.ru | 9d5aa3fe0690d19de24629226f23abefd |
| 2022-03-01 00:16:49 | idemo.vtb.ru | 9ef7ab4ed17786ea152f1a152e2c347c8c |
| 2022-03-01 00:16:54 | webquik.vtb.ru | 4c192c7bcb57ff52993fd71bdd688e1a55 |
| 2022-03-01 00:17:11 | komission.vtb.ru | b9761633e595a6ca9eb651adb38601fc7 |
| 2022-03-01 00:17:29 | epa.api.vtb.ru | a0a6c1ba28fd7d70a306cace89a15230d |
| 2022-03-01 00:17:44 | mail.vtbstrana.ru | 3d2b0ee0665bfeddf1ccf7194cd896809 |
| 2022-03-01 00:17:48 | mail.vtb.com | e8d152170944f18b74e0895fb40c43e60 |
| 2022-03-01 00:17:55 | db.vtb.ru | 4af34f0f8ed1bb975b3ff3842131cc4a9c |
| 2022-03-01 00:18:37 | mx101.vtb.ru | 5a7170b3966d23634024b31fe4b373cf4 |

| REVOKE_TIME | SUBJECT_COMMONNAME | SHA1 |
|---------------------|-----------------------|-------------------------------------|
| 2022-03-01 00:18:41 | mx102.vtb.ru | 3df103b57e5f392c71df6f303e4777b983 |
| 2022-03-01 00:18:46 | mx201.vtb.ru | 4dac367f4357fc8e85a69105d9a73e716 |
| 2022-03-01 00:18:57 | mx202.vtb.ru | 5144a93d057eafbcd85bc24e52ecef923 |
| 2022-03-01 00:19:39 | *.vtbbo.ru | 9ec889fb87ba7df2a5d9f670253175db3 |
| 2022-03-01 00:19:55 | vtbbo.ru | 459c6cf187b637ddaf7315b0437adb3fc4 |
| 2022-03-01 00:23:51 | cl.vtb.ru | 86d51be25b4cea05a351cbd7cf99d69b2 |
| 2022-03-01 00:24:10 | mb-partner.bm.ru | b8b4490db23d10416b0d7b8bbdf4cb0 |
| 2022-03-01 00:24:42 | ipoteka-online.vtb.ru | b4968f1c438b6054603f07e0f491b36ca |
| 2022-03-01 00:24:53 | vtbrussia.ru | 24eb584f1e1e27c86bfa12eacf9867bdd5 |
| 2022-03-01 00:25:10 | Sbc-proxy.vtb.ru | 0867b10049bf1e005647befb83ee1bb96 |
| 2022-03-01 00:27:40 | bo.vtb.ru | d40c4b34b82519deb6ca811ecd4eea02 |
| 2022-03-01 00:28:04 | vb.vtb.ru | 7a3df1ce19a88f71741a5f176ded585fe9e |
| 2022-03-01 00:28:14 | data-fusion.ru | b571526a75cc3141abd0e928e8df35891 |
| 2022-03-01 00:34:54 | vtbindia.com | e7dfeda2ad46f54335b0da72aacc9dc9d |
| 2022-03-01 00:35:49 | acquiring.vtb.ru | b5447f597aa078a7cadae3b22d9a8865 |
| 2022-03-01 00:36:06 | www.vtb.com | 5573f1f57aedf665e6c3da73f702e8b81a |
| 2022-03-01 00:36:21 | lk.vtb.ru | 58295cf4e89be3be322474dc0028d129 |
| 2022-03-01 00:36:27 | crm.vtb.ru | 0f88adf4ab1b3599d3b60e4cc3887a44b |
| 2022-03-01 00:36:52 | mobi1.vtb24.ru | c2ac9dc39ea9e9c7fa276a02b37999530 |
| 2022-03-01 00:39:21 | *.zapsibkombank.ru | 8f22318ed13d74026e621796ddae0fd54 |
| 2022-03-01 00:39:26 | newbusiness.psbank.ru | 49332bdaeb5270f425b5d6245e72806c |
| 2022-03-01 00:39:41 | *.exiar.ru | f9b9ea6d9e4a66ce1431d7d8a8f526a1a |
| 2022-03-01 01:27:31 | *.psbank.ru | 7c68142b2cdd1630223055ddc86ae20b |
| 2022-03-01 01:31:28 | psbinvest.ru | 9f1398b5b7c9692b42b693523873aa89 |
| 2022-03-01 01:32:23 | *.payment.ru | d7ec65409697d900acc5af14d1e49a486 |
| 2022-03-01 01:33:04 | ib.psbank.ru | 9e171b1269ae6defa889bfe4aee0074356 |
| 2022-03-01 01:33:08 | *.exportcenter.ru | 8fd06cd8e2dee7357c2453e2747f93717 |
| 2022-03-01 01:33:41 | *.round.ru | f25d7f41847e1728d358df6b03072fedda |

| REVOKE_TIME | SUBJECT_COMMONNAME | SHA1 |
|---------------------|------------------------------|-------------------------------------|
| 2022-03-01 01:34:16 | online.rgsbank.ru | 7d15927eedff53fb2255a32ac61ec4fd2a |
| 2022-03-01 01:34:21 | ib.rgsbank.ru | 5e20dc4665c1ff3c32ffe6a8d9b0dc73a8 |
| 2022-03-01 01:34:39 | *.veb-leasing.ru | 3594e8d133ee4b40dbe422f57488a31c |
| 2022-03-01 01:35:15 | index.vtbcapital.ru | 05a89c6f02cf8d6af1b07bfe4ecedc08e2 |
| 2022-03-01 01:41:54 | *.pib.ua | a8f0b2ee09757d5c1c078a8ab09d02ada |
| 2022-03-01 20:49:38 | *.rdif.ru | 0aa035b197adec963573943750b87226 |
| 2022-03-02 00:17:47 | www.vtbcapital.ru | cd833e8b6c3bd7ba6ef82863e2d455f3 |
| 2022-03-02 00:48:49 | divrating.ru | ad6f7d3f3cf19b2f7d2bd8046d4b28216 |
| 2022-03-02 00:50:35 | retail-tst.payment.ru | 7382892d1cda4062c3c36fe9f7cb3aa98 |
| 2022-03-02 00:51:23 | business.psbank.ru | 0d7a666e2b8096bd855ee04cecaaaf7b1 |
| 2022-03-02 00:52:44 | *.fintender.ru | 590a671a7b999524da77eacf7a01f6f3a |
| 2022-03-02 00:53:11 | elf.sovcombank.ru | 51f335b5dc8dfcedd053595ce7efdd0e1c |
| 2022-03-02 00:53:27 | *.sovcomins.ru | 96e64d494478f94437fa0ec80c654cb3 |
| 2022-03-02 00:53:39 | *.sovcomins.ru | 5130c18cf167288432cb5e682fc75f020e |
| 2022-03-02 00:53:54 | *.halvacard.ru | 6e714e73b0e2aeaeb8570882268bc135 |
| 2022-03-02 00:54:52 | *.sovcombank-leasing.ru | 377d73b8debb805775e5d54a92a6ed9a |
| 2022-03-02 01:00:22 | *.sovcombank.ru | 095949796378475fab907593078f31171 |
| 2022-03-02 01:01:05 | www.russiacalling.ru | 4da16dec1f8f94ad4054827da076e7ed6 |
| 2022-03-02 19:21:51 | vtbcapital-pr.ru | 33e79ce3e482ec54b6e64bd4b7d79bf4 |
| 2022-03-02 19:25:11 | online.vtbcapital-pr.ru | ed33db76b7411f47914b801b9821a86dc |
| 2022-03-02 19:26:08 | factorext.sovcomfactoring.ru | 74ffb8eb4fc7d16df780e01bcb37a335fa3 |
| 2022-03-02 19:28:06 | sovcomfactoring.ru | e8aa6b085b51750279b4995c43f61084 |
| 2022-03-02 19:31:12 | 3ds.payment.ru | d416e7e0a63a3aee630ff53c771538bbd |
| 2022-03-02 19:33:43 | www.upravlyaem.ru | 6666da94e3dab49d944b0c8277e99fc2 |
| 2022-03-02 19:44:46 | esg.vtbcapital-am.ru | 376f20fe0b9864c93aeadf592946ff5814 |
| 2022-03-02 19:47:40 | online.vtbcapital-am.ru | 1c41fb355d03aeb0c9b8ae774d82f4793 |
| 2022-03-02 19:51:07 | vtbcapital-am.ru | 7d3d2993421c7a36e29efff424deffa9a6 |
| 2022-03-04 03:09:27 | mobile.broker.vtb.ru | 9c28db643025e0d19ab43f5d1d3b6529 |

| REVOKE_TIME | SUBJECT_COMMONNAME | SHA1 |
|---------------------|-----------------------------|--------------------------------------|
| 2022-03-04 03:10:37 | m.komission.vtb.ru | b9581d97f46630c0b3fa1e44abc3b87a18 |
| 2022-03-04 03:11:17 | broker.vtb.ru | bfd4503f97fc6e0cbc6ad343749c3f537c |
| 2022-03-04 03:21:19 | nh.open.ru | 5e30d7f5433f04335da04a3937a60ffca |
| 2022-03-04 03:21:20 | drive.rgsbank.ru | b857c6db95e11a2a8fd8035830d0eaa93 |
| 2022-03-04 03:21:20 | flexy.open.ru | 3d680c9008191aa5af8559ffd19f0b68a8 |
| 2022-03-04 03:21:20 | *.sovcomlife.ru | d7ca302ca85fd90ed27e7d67bfad871e3a |
| 2022-03-04 03:21:20 | wyse.open.ru | cadc73ba8feb33dda75771916cf2b06f4e |
| 2022-03-04 03:21:21 | aramis-mp.open.ru | 170bc71f8654b595a54e1510dfdd9ae4c0 |
| 2022-03-04 03:21:21 | htfx.calc-csp.rgsbank.ru | 85f1d60f52b7675a7f303ee3f98d9bf23e |
| 2022-03-04 03:21:21 | htfx.front-csp.rgsbank.ru | 41586bef0b15f80b8599251eb6566c08f |
| 2022-03-04 03:21:21 | htfx.photo-csp.rgsbank.ru | 60f9ec76418a966d0c1df5df0f13bc6197 |
| 2022-03-04 03:21:21 | htfx.pms-csp.rgsbank.ru | 52eb5e8380c18902d330200a1659c710 |
| 2022-03-04 03:21:21 | mx1.vtbcapital.com | 5e71797ed517cb6b849b416da0a13a43b |
| 2022-03-04 03:21:21 | mx2.vtbcapital.com | 48117270c174d1f612c94ea8ca2e5691d2 |
| 2022-03-04 03:21:21 | mx3.vtbcapital.com | 9d7864b28da25ce62c482153df67e7cc2 |
| 2022-03-04 03:21:21 | mx4.vtbcapital.com | 4aaac0294ce0f2738e77d32ad6d06c49c |
| 2022-03-04 03:21:21 | private.fintender.ru | 2e835225e225caa7513c58673b56b47a |
| 2022-03-04 03:21:22 | ctx-mdm.open.ru | 3a30376b94476adfbb6dca5cabe4da140 |
| 2022-03-04 03:21:22 | tst-ctx-mdm.open.ru | d575be8cfa22ee2819721a0e83efbeb021 |
| 2022-03-04 03:21:23 | static.mobapp-daily.open.ru | 22ad762875824d98e74ad61d245002c6 |
| 2022-03-04 03:21:25 | calculator.csp.rgsbank.ru | 325a187de3994fac667498c2fb6043530 |
| 2022-03-04 03:21:25 | front.csp.rgsbank.ru | 3ce8b3fae0fa1fa747c48fac6c40bfff6f72 |
| 2022-03-04 03:21:25 | photo.csp.rgsbank.ru | d86f49038701c42c5719887fced0990ac |
| 2022-03-04 03:21:26 | bi.rgsbank.ru | 010f750d54eb3ed9b557b1f5b5a2d8975 |
| 2022-03-04 03:21:26 | *.university.cbr.ru | c41d962ddf81f3e46eb2ebc0727212d183 |
| 2022-03-04 08:05:19 | vonage.ru | 5757ed730113c3dba2b72e9b91cac8699 |
| 2022-03-04 19:48:24 | *.vtb.ge | 10be80e75a31324fb62e72400721a01fb6 |
| 2022-03-04 19:48:54 | ivtb.ge | 5a8b15c09ee02f8cbf453dc054531df24 |

| REVOKE_TIME | SUBJECT_COMMONNAME | SHA1 |
|---------------------|--------------------------|------------------------------------|
| 2022-03-04 20:02:11 | online.vostbank.ru | ae5dbf5b47fbf0e6f7c180696f73c26de8 |
| 2022-03-04 20:02:24 | vostbank.ru | 3089301610a7d4f3d6af3410375860e7a |
| 2022-03-07 18:55:59 | open.ru | e3d4bcbb295c4e2801c2652e5bbe376 |
| 2022-03-07 18:56:00 | *.urozhai.rshb.ru | 9c2db763f9fbb10b02a325ee001200b09 |
| 2022-03-07 18:56:01 | business.rgsbank.ru | c4be431e66306ee421c830e3a84f0a1b1 |
| 2022-03-07 18:56:02 | acs.rshb.ru | 85de94c42a694d79a2aeea2a4c7cae38 |
| 2022-03-07 18:56:02 | rshb.ru | 8b9aff36b06a60ce3031947f2a370c859 |
| 2022-03-07 18:56:04 | online.rshb.ru | d027380e5c0a0ab27967e886bcfee70fe |
| 2022-03-07 18:56:05 | *.rshb.ru | dcf6fc810d4a66b7582ea01461ddc9ad5 |
| 2022-03-07 18:56:06 | *.mes.rshb.ru | 91fba72984fb02fa86690ab86cba99168 |
| 2022-03-07 18:56:08 | ecom.alfabank.ru | 81d4da7893e9c2f7e0ce89361d856706c |
| 2022-03-07 18:56:08 | *.sbud.rshb.ru | ad297055882cb67f39e1fd8155ad79335 |
| 2022-03-07 18:56:09 | coins.rshb.ru | 3c724fca6a93b4a793f58e539dc6420f3 |
| 2022-03-07 18:56:09 | ebs-bio.rshb.ru | 06275cd5f4fb577f65084811edd9ceb8b |
| 2022-03-07 18:56:09 | factoring.rshb.ru | 19d403511413170b32609c23bce7a412d |
| 2022-03-07 18:56:09 | finradar.rshb.ru | f45b8bbb777d7edd267c50aebf438a5d9 |
| 2022-03-07 18:56:09 | lk.factoring.rshb.ru | 517b298ccf43a18b55334929b268578a1 |
| 2022-03-07 18:56:09 | mx1.rshb.ru | 6af4f13c7bad1eca2909a7ce73852c2c97 |
| 2022-03-07 18:56:09 | mx2.rshb.ru | 03c96fb7670b4d1e38e062e231cf6067e |
| 2022-03-07 18:56:09 | rrdg.factoring.rshb.ru | 6c765c5105719c9f0001e7dabf49acd81a |
| 2022-03-07 18:56:09 | *.sbud.rshb.ru | 3a41b87715bc4d4fe106aad7e6d78be7e |
| 2022-03-07 18:56:09 | smx.rshb.ru | 49ada6266390ab055b6d0f09593eae20 |
| 2022-03-07 18:56:09 | travelergo.rshb.ru | a9edd5ac03f386d04ef4b853028bb1b7e |
| 2022-03-07 18:56:09 | travelerrf.rshb.ru | e7d5b471a3705abf7082124ce7fe3f859e |
| 2022-03-07 18:56:10 | merchant-api.sbp.rshb.ru | 5ab3718a93beda27f449b32b042473e6 |
| 2022-03-07 18:56:10 | mx1.rshb.ru | 2288b60c7d3e48657985ce904d59a6fk |
| 2022-03-07 18:56:10 | *.plc.rshb.ru | 097d0a314edbc0804996b31050cbe759 |
| 2022-03-07 18:56:10 | test07.rshb.ru | f4774d7c5dc4d566eb31785e475714a59 |

| REVOKE_TIME | SUBJECT_COMMONNAME | SHA1 |
|---------------------|------------------------|-----------------------------------|
| 2022-03-07 18:56:10 | xapi.factoring.rshb.ru | bdd72b1e18d71c3b11530c744b87529a0 |
| 2022-03-07 18:56:11 | broker.rshb.ru | 172a20e5fa0950478f0550971461a5b57 |
| 2022-03-07 18:56:11 | *.crimearw.ru | 9a8305c0f610a8ae6f6fd3a21c58b6552 |
| 2022-03-07 18:56:11 | quik.rshb.ru | af736621443bec16668533737afc2435f |
| 2022-03-11 19:26:00 | sberinsur.ru | 93b10cb245f35e7d2c9ecbba5c10d7b5a |

0 Comments

1 Login ▾



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS [?](#)

Name

1

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



Botnet

新威胁：闷声发大财的Fodcha僵尸网络

honeypot

Spring4Shell在野漏洞传播分析

商业数字证书签发和使用情况简介(删减版)

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 →

本报告由国家互联网应急中心(CNCERT)与三六零数字安全科技集团有限公司共同发布。概述近期，CNCERT和三六零数字安全科技集团有限公司共同监测发现一个新的且在互联网上快速传播的DDoS僵尸网络，通过跟踪监测发现其每日上线境内肉鸡数（以IP数计算）已超过1万、且每日会针对超过100个攻击目标发起攻击，给网络空间带来较大威胁。由...



Apr 13, 9 min



2022 read

背景介绍 2022年3月31号，Spring针对Spring4Shell漏洞(CVE-2022-22965)事件发布了安全公告[1]，并提供了漏洞修复程序，此次漏洞事件在安全社区引起广泛关注。360网络安全研究院高级威胁狩猎蜜罐系统[2]通过被动监测方式看到了该漏洞在野传播过程，我们也看到了Mirai僵尸网络入场，相关在野漏洞攻击威胁情报已通过自动化形式输出。...



Apr 1, 18 min



2022 read