零信任的首要原则是什么？

说起零信任，大家都知道身份认证的重要，需要始终验证身份，但都忽视了一个重要原则，忽略了一个重要元素的始终验证，是什么呢？网站身份！Web 是互联网第一大流量，而各大厂商的零信任安全解决方案只关注人的身份，实现了人访问网站资源的始终验证。但所有零信任解决方案都千篇一律地忽略了网站身份的始终验证，这是一个巨大的技术方向失误。

据美国 PandaLabs 发布的数据，全球每周有 5 万 7 千多个新的假冒网站产生，大约使用了 375 个不同的知名品牌和公司品牌来吸引用户，65%的假冒网站模仿银行页面，其次是电商网站和拍卖网站，占 27%。这些假冒网站熟练掌握搜索引擎优化和索引技巧，使得粗心的上网用户会错误地点击这些假冒网站而上当受骗。被假冒的知名品牌包括 eBay、西联汇款、Visa、亚马逊、美国银行、PayPal 和美国税务服务等。最可怕的是：这些假冒网站都有安全锁标识，因为完全免费的 SSL 证书随手可得。这不得不让美国联邦调查局向消费者发出警告-不要再信任浏览器的 https 安全锁标识。这是对网站的零信任和对 https 加密的零信任。

据国家互联网应急中心(CNCERT)发布的 2020 年《中国互联网网络安全报告》中关于网页仿冒的数据，2020 年，CNCERT/CC 共抽样监测到仿冒我国境内网站的钓鱼页面 220,648 个(22 万多)。其中以“ETC 在线认证”为标题的仿冒页面数量呈井喷式增长，并在 2020 年 8 月达到峰值 5.6 万余个，占仿冒页面总量的 91%，这些假冒 ETO 网站诱骗用户提交姓名、银行账号、身份证号、手机号、密码等个人隐私信息，致使大量用户遭受经济损失。而受新冠肺炎疫情影响，大量行政审批转向线上。2020 年年底，出现大量以“统一企业执照信息管理系统”为标题的仿冒页面，仅 2020 年 11-12 月监测发现此类仿冒页面 5.3 万余个。不法分子通过该类页面诱骗用户在仿冒页面上提交真实姓名、银行卡号、卡内余额、身份证号、银行预留手机号等信息。此外，监测还发现大量以“核酸检测”“新冠疫苗预约”等为标题的仿冒页面，其目的在于非法获取用户姓名、住址、身份证号、手机号等个人隐私信息。而这些假冒网站基本上都没有部署 SSL 证书，如果用户使用浏览器访问的话，一定会提示“不安全”。但很遗憾的是，如果使用微信查看链接是没有“不安全”提示的。

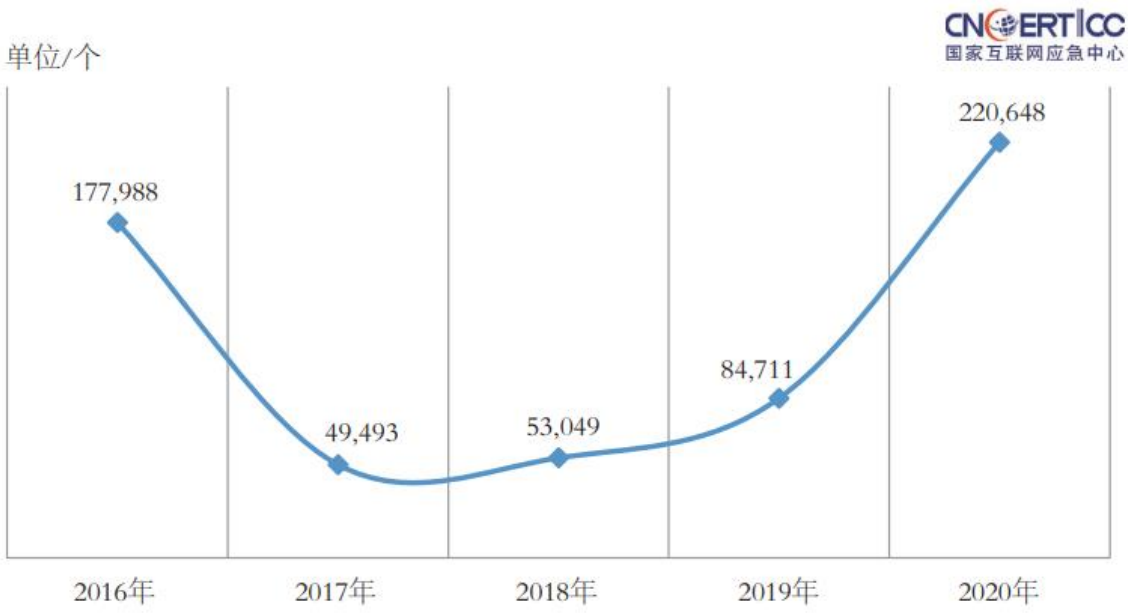


图 5-11　2016-2020 年仿冒我国境内网站的钓鱼页面数量统计（来源：CNCERT/CC）

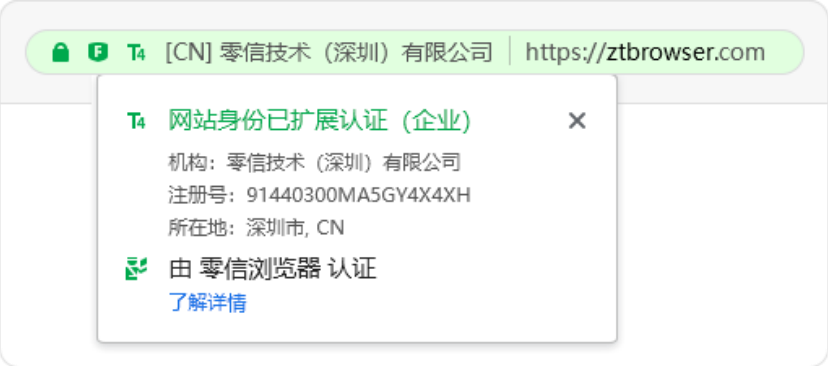
而即使网站部署了 SSL 证书，实现了 https 加密，我们仍然必须对每个访问的网站零信任，必须验证网站的真实身份。笔者认为：对网站身份的始终验证，应该是零信任的首要原则，其次才是对网站访问者的身份的零信任，而不能本末倒置或者根本不关心网站这个数据的源头的始终验证。如果用户访问的是假冒网站，那对用户的零信任始终验证又有何用？可能危害更大，因为一个真实的用户身份落入了假冒网站的手中！

那么，如何实现对网站身份的始终验证？这个任务就应该由浏览器来承担，因为浏览器是上网入口，为用户显著地展示正在访问的网站的真实身份，是一个好的浏览器必须做到的事情。而浏览器如何知道网站的真实身份并展示给用户？有两个实现途径，一是从用户正在访问的网站的 https 通信中获得网站部署的 SSL 证书中含有的网站身份信息，所有 SSL 证书的使用者字段会含有 CA 机构验证这个网站的身份信息，浏览器读取这个身份信息就可以直接展示出来给浏览器用户查看，这是最方便的最可靠的技术手段。因为 CA 机构在给网站颁发 SSL 证书时会按照验证过什么身份就把相应的身份信息写到 SSL 证书中的原则来签发 SSL 证书。

第二个途径就是浏览器厂商自己验证网站的身份并展示网站的身份，这个非常适合于部署了没有验证网站真实身份的 DV SSL 证书的网站。CA 在签发 DV SSL 证书时只验证域名所有权就签发了 SSL 证书，证书使用者信息只有域名，没有网站身份信息。所以，浏览器无法通过 SSL 证书来获得网站的身份信息，就只能自己来验证网站的身份了，这就是零信技术为何推出网站可信身份认证服务的主要动因，将有效地弥补了 DV SSL 证书中无网站身份信息的缺陷。

笔者认为：各大浏览器移除了对部署了 EV SSL 证书的网站的绿色地址栏和直接在地址栏

展示网站单位名称是一个非常错误的决定，浏览器不展示网站的真实身份间接地成为了欺诈假冒网站的帮凶！所幸的是，零信浏览器已经增强展示部署了验证网站身份的 EV SSL/OV SSL/IV SSL 证书的身份信息，能有效保证用户非常容易地了解正在访问的网站的真实身份，从而非常容易地做出正确的安全决策。



所以，零信任的首要原则应该是不信任没有通过第三方身份认证的网站，其次是不信任没有 https 加密的网站，第三才是不信任网站访问者的身份并始终验证访问者身份。这个顺序不能错，否则就是本末倒置，缘木求鱼。并且，这三个元素的零信任是环环相扣相关关联的，只有网站通过了第三方(如 CA 机构)的认证、部署 SSL 证书实现了 https 加密、每次验证访问者身份才是一个完整的零信任安全链，才能真正保证“正确的人”访问了“正确的网站”获取了“正确的数据”。

王高华

2022 年 6 月 1 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。