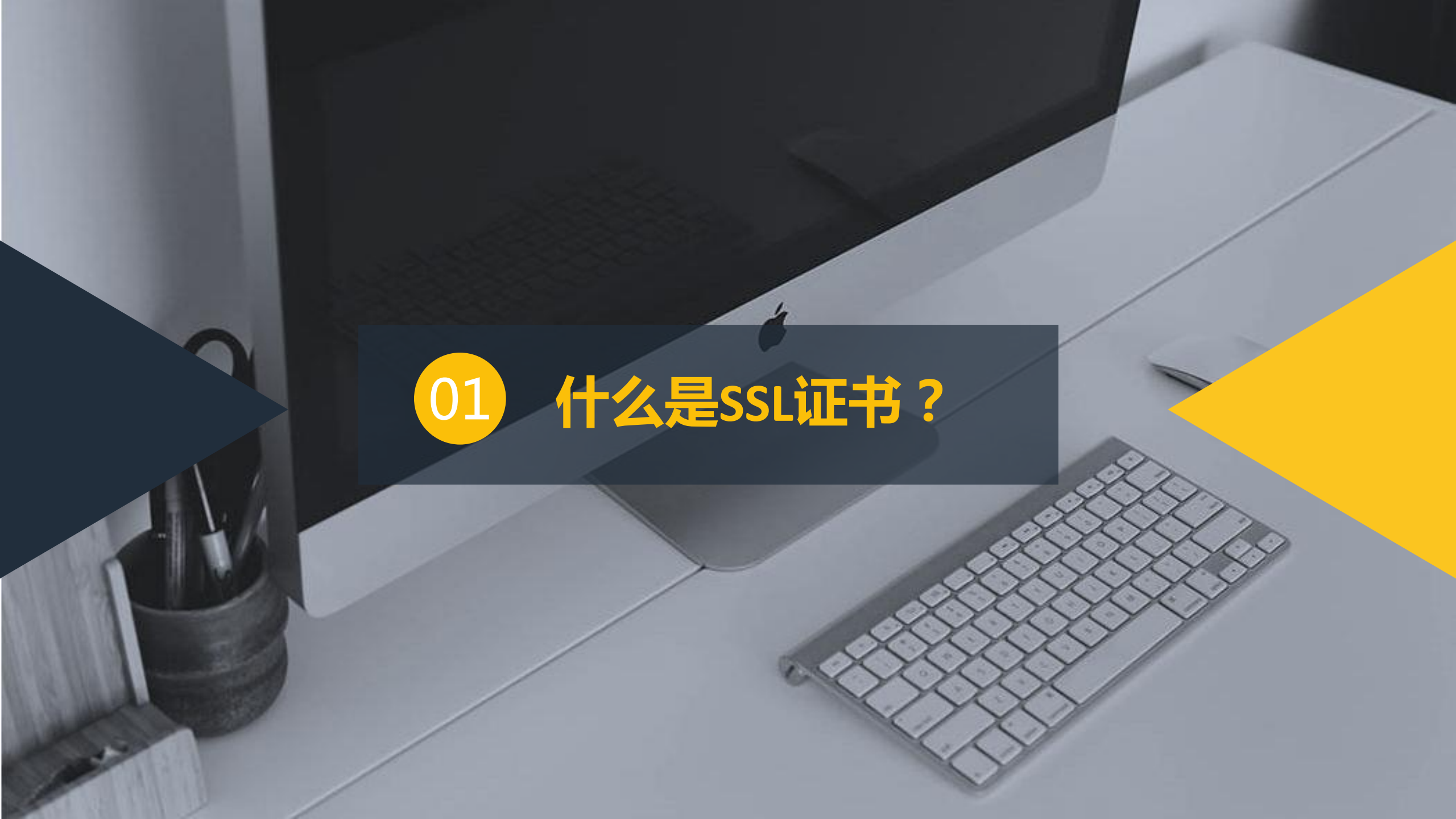
中资源

SSL证书内容介绍

DIRECTORY
目录



01 什么是SSL证书？

如果没有SSL证书

您的网站是否在谷歌浏览器中存在这种情况？

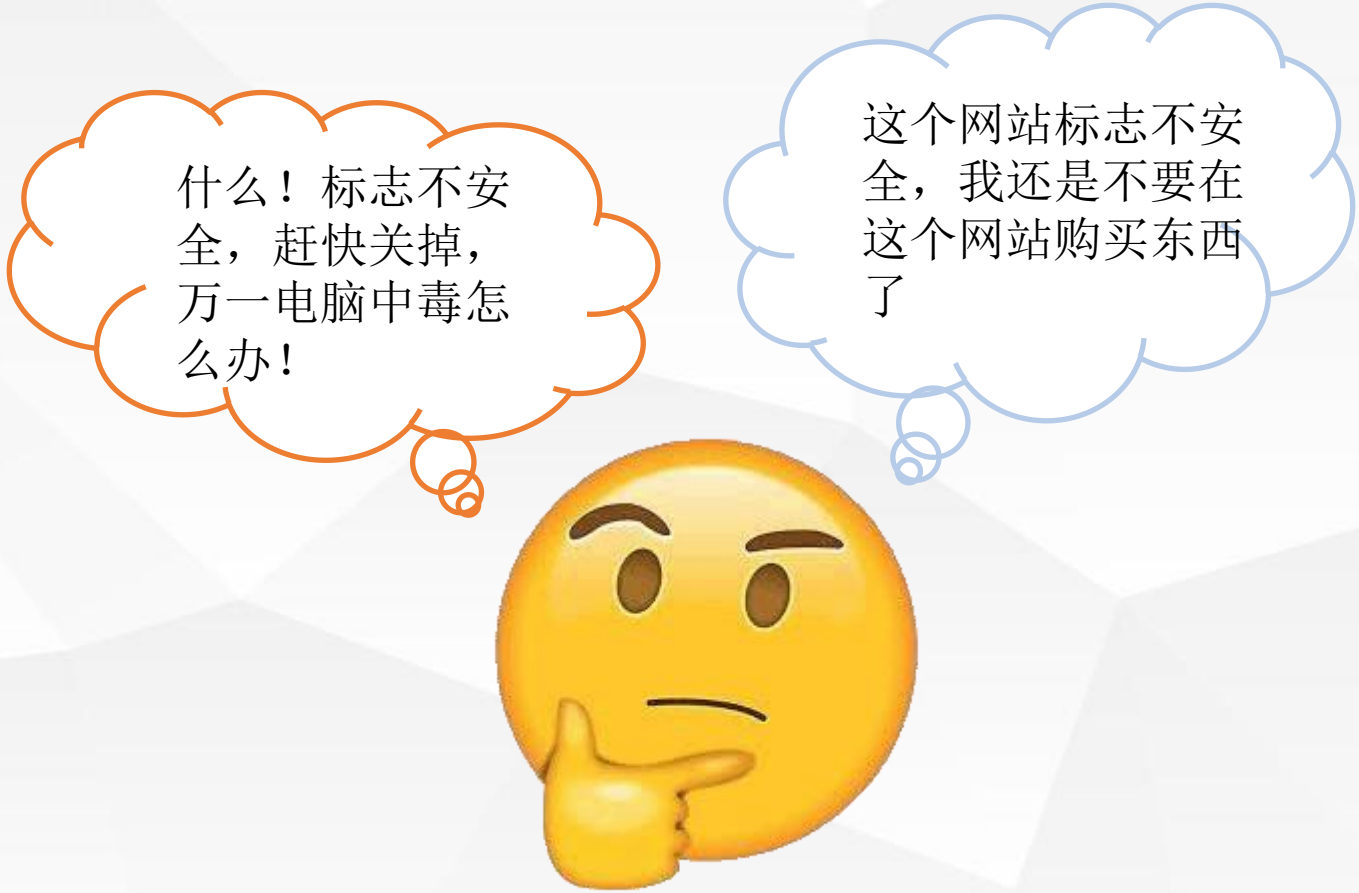
如果没有SSL证书

又或者在火狐浏览器存在这些情况？

如果没有SSL证书

当网站显示不安全的时候，用户会想这个网站是不是有病毒；

如果是购物网站，即有可能会损失60%的用户



如果没有SSL证书

什么是HTTPS？

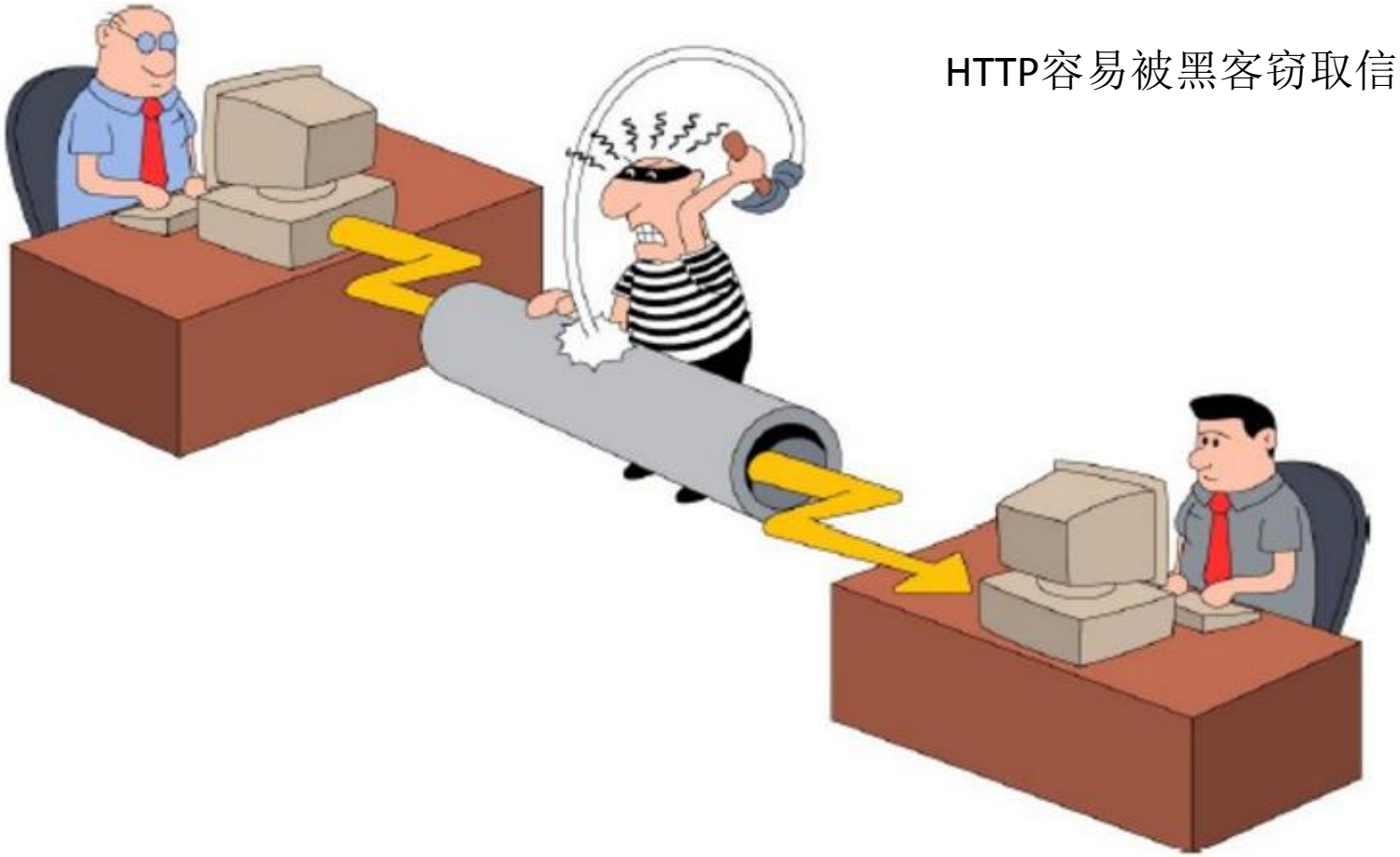
我们大多数人每天都使用加密通信，如你用百度搜索东西，你在淘宝上买了一件喜欢的衬衫，HTTPS能防止你的数据在网络传输过程中不被其他人窃取。

如果没有SSL证书

HTTP的危害

如果你访问一个网站默认了超文本传输协议（HTTP），其内容将明文传输。这意味着每个人在你和服务器之间的位置都可以看到你与网站的每个交互内容。当用HTTP传输私人信息（姓名，电子邮件，家庭住址，信用卡详细信息等），黑客可以轻易的从网络流量中截取你发送信息，因为这些都是明文传输。这种攻击方式就叫中间人攻击，当然因为这个衍生出来的还有缓存投毒，DDOS定向流向转发等，这个中间人存在你的客户端和服务端的每个部分，例如，如果您连接到Wi-Fi热点，则您和服务器之间通过HTTP传输的所有内容将对热点中的每个参与者都可见。（是不是非常可怕，这也是不要轻易连接免费Wi-Fi的原因！！！）

如果没有SSL证书



HTTP容易被黑客窃取信息

如果没有SSL证书

用专业的术语总结一下HTTP的问题：

（1） 窃听风险：第三方可以获知通信内容。

（2） 篡改风险：第三方可以修改通信内容。

（3） 冒充风险：第三方可以冒充他人身份参与通信。

HTTP网站的威胁

1.HTTP 协议通信过程是完全开放的，可以轻易的监听和修改途经的数据报，导致信息的泄露和恶意篡改。

2.HTTP协议没有用户和网站的身份验证机制，用户在浏览器上敲入的网址， 有可能被DNS劫持，从而导致用户浏览器被导向了伪造的网站，重要信息如账号密码被骗取。

3.HTTP通信过程被恶意劫持和篡改是普通用户无法分辨的，所有问题责任归咎于网站或者APP开发者， 对网站和APP的正常经营和品牌造成不利影响。

4.黑客在HTTP通信过程中，插入恶意代码或病毒，进行双向入侵和攻击。

HTTP与HTTPS的对比

HTTP: 不安全的信息传输
→ HTTPS：安全加密链接

- 没有https的安全警告
- 所有政府开始向https网页移动
- 主流浏览器开始只支持https
- Http2只支持https
- Referrer data只能通过https

微信小程序服务端请求必须HTTPS

小程序一直被誉为“APP杀手”。微信庞大社交用户基础，可能带来的业务爆发性上，这一波微信红利，开发者怎可错过?

但是微信对小程序也是有诸多的限制，例如文件大小、请求服务端必须是HTTPS等等。实现服务器端HTTPS请求，需要在服务器端配置ssl证书实现。

微信小程序服务端请求必须HTTPS

HTTP明文协议是不安全的传输协议，无法进行服务器端真实身份校验，也不能为传输数据提供加密保护，通过HTTP协议传输的数据时刻处在被窃听、篡改、冒充的风险中。HTTPS传输协议在HTTP的基础上加入了SSL协议，SSL依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信进行加密，确保数据传输到正确的服务器端，并防止中间人窃取传输数据。

微信小程序服务端请求必须HTTPS

目前全球互联网正在从HTTP向HTTPS的大迁移，Chrome和火狐浏览器将对不采用HTTPS加密的网站提示不安全，苹果要求所有APP通信都必须采用HTTPS加密，小程序强制要求服务器端使用HTTPS请求，正是顺应了互联网安全的趋势。

每个微信小程序必须事先设置一个通讯域名，并通过HTTPS请求进行网络通信，不满足条件的域名和协议无法请求。也就是说，请求request地址必须是合法域名，需要有SSL证书认证过。




安全事故

国家互联网应急中心
互联网安全威胁报告 2017 年 1 月

摘要：

本报告以 CNCERT 监测数据和通报成员单位报送数据作为主要依据，对我国互联网面临的各类安全威胁进行总体态势分析，并对重要预警信息和典型安全事件进行探讨。

2017 年 1 月，互联网网络安全状况整体评价为良。主要数据如下：

- 境内感染网络病毒的终端数为近188万个；
- 境内被篡改网站数量为4,981个，其中被篡改政府网站数量为171个；境内被植入后门的网站数量为3,265个，其中政府网站有90个；针对境内网站的仿冒页面数量为2,442个；
- 国家信息安全漏洞共享平台（CNVD）收集整理信息系统安全漏洞552个，其中，高危漏洞237个，可被利用来实施远程攻击的漏洞有512个。

2015中国互联网网络安全报告 发现的网络安全事件中，数量排前三位的类型分别是:

网页仿冒事件(占59.8%)、

漏洞事件(占20.2%)

网页篡改事件(占9.8%)。

网络安全信息与动态周报
2 月 27 日-3 月 5 日

境内感染网络病毒的主机数量	•41.14万	↑ 2.3%
境内被篡改网站总数 其中政府网站数量	•2893 •134	↑ 14.9% ↑ 28.8%
境内被植入后门网站总数 其中政府网站数量	•1220 •33	↓ 22.3% ↓ 13.2%
针对境内网站的仿冒页面数量	•614	↓ 36.4%
新增信息安全漏洞数量 其中高危漏洞数量	•229 •115	↓ 32.6% ↓ 22.8%

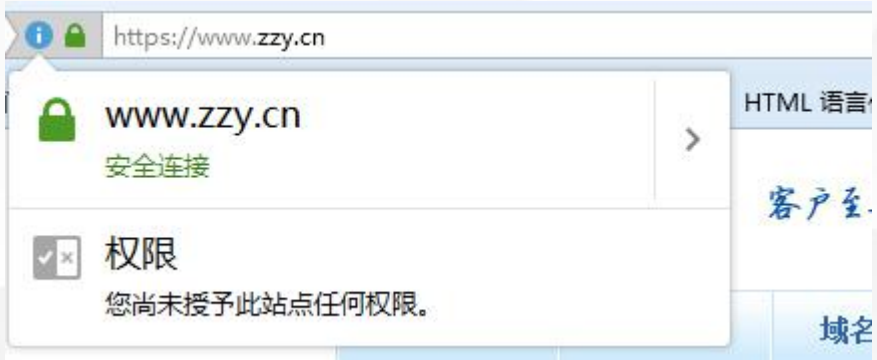
什么是SSL证书

SSL 证书提供了一种在互联网上身份验证的方式,是用来标识和证明通信双方身份的数字信息文件。使用 SSL 证书的网站，可以保证用户和服务器间信息交换的保密性，具有不可窃听、不可更改、不可否认、不可冒充的功能。

SSL 证书由浏览器中“受信任的根证书颁发机构”在验证服务器身份后颁发,具有网站身份 验证和加密传输双重功能。

什么是SSL证书

Google Chrome显示



火狐显示

当网站添加了SSL证书以后，谷歌和火狐浏览器上都显示安全可信赖的网址，使用户不必担心自己浏览的网站是否存在病毒，提高网站的点击量。

Google Chrome

Chrome 68 arrives with new APIs and all HTTP sites marked as not secure

EMIL PROTALINSKI @EPRO JULY 24, 2018 9:30 AM

据国外媒体Venturebeat报道Chrome 68带有新API，所有HTTP站点都标记为不安全。

原文地址：

https://venturebeat.com/2018/07/24/chrome-68-arrives-with-new-apis-and-all-http-sites-marked-as-not-secure/

Google Chrome

progress for yourself here).

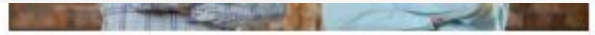
With Chrome 68, here is how HTTP sites now appear in the address bar:

Treatment of HTTP pages:

Current (Chrome 64)	example.com
July 2018 (Chrome 68)	Not secure | example.com

Here is how Google explains its thinking behind the change:

> *Chrome's new interface will help users understand that all HTTP sites are not secure, and continue to move the web towards a secure HTTPS web by default. HTTPS is easier and cheaper than ever before, and it unlocks both performance improvements and powerful new features that are too sensitive for HTTP.*



Columbus' Root now valued at $1 billion for its mobile data-driven car insurance

Xiaomi makes global play with budget Android brand, Poco, starting at $300

NYC library turns Instagram into ebook reader for 'Alice in Wonderland'

Google Chrome浏览器有SSL证书和无SSL证书的区别

Google Chrome 把没有SSL证书的网站设为不安全

Mozilla Firefox

Mozilla Restricts All New Firefox Features to HTTPS Only

By Catalin Cimpanu — January 17, 2018 — 04:00 AM — 3

In a groundbreaking statement earlier this week, Mozilla announced that all web-based features that will ship with Firefox in the future must be served on over a secure HTTPS connection (a "secure context").

"Effective immediately, all new features that are web-exposed are to be restricted to secure contexts," said Anne van Kesteren, a Mozilla engineer and author of several open web standards.

This means that if Firefox will add support for a new standard/feature starting tomorrow, if that standard/feature carries out communications between the browser and an external server, those communications must be carried out via HTTPS or the standard/feature will not work in Firefox.

The decision does not affect already existing standards/features, but Mozilla hopes all Firefox features "will be considered on a case-by-case basis," and will slowly move to secure contexts (HTTPS) exclusively in the future.

Mozilla将所有新的Firefox功能限制为仅限HTTPS

地址原文：https://www.bleepingcomputer.com/news/software/mozilla-restricts-all-new-firefox-features-to-https-only/

Mozilla Firefox

地址原文：http://www.freebuf.com/news/157612.html

火狐浏览器有SSL证书和无SSL证书的区别

火狐也把没有SSL证书的网站设为不安全

苹果强制安全强化

2017年起，ATS安全标准 (App Transport Security) 成为苹果APP强制性要求， 应用程序与Web服务之间的所有连接必须通过HTTPS.

Jun 14, 2016

Security

Apple will require HTTPS connections for iOS apps by the end of 2016

by *Kate Conger*

During a security presentation at Apple's Worldwide Developers' Conference, the company revealed the deadline for all apps in its App Store to switch on an important security feature called App Transport Security — January 1, 2017. App Transport Security, or ATS, is a feature that Apple debuted in iOS 9. When ATS is enabled, it forces an app to connect to web services over... **Read More**

10

02

SSL证书的好处

SSL证书的好处

SSL证书将会带来前所未有的安全加密和更快速的访问体验

- √ 防止中间人流量劫持
- √ HTTPS加密使网站更安全
- √ 保障用户隐私信息安全
- √ 帮助用户识别钓鱼网站
- √ HTTP将被标记“不安全”
- √ 提升搜索排名
- √ 提升公司形象和可信度

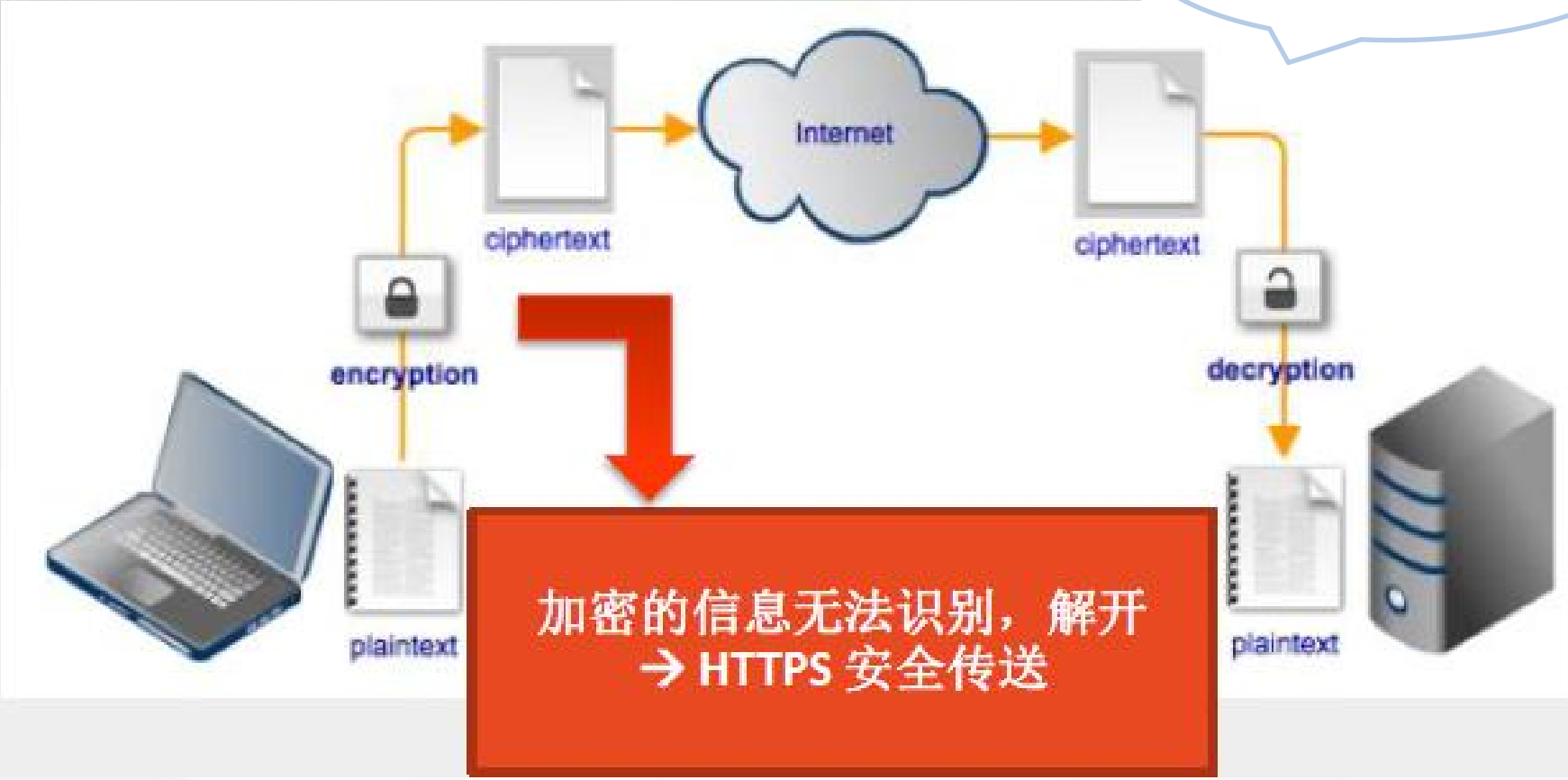
SSL证书的好处

SSL可以解决什么问题？

- 机密性问题：防止网上交易时黑客盗走客户的银行卡，帐号等机密信息。
- 完整性问题：防止非法恶意篡改客户的银行卡号等个人信息。
- 真实身份认证：验证网站的真实性，树立可信赖的企业形象，辨别钓鱼网站。
- 交易不可否认：保证每笔交易都有可靠的记录。
- 提高搜索排名顺序，数据推荐参考，为SEO的目标和网站增强了安全系数。

SSL证书的好处

一眼识别钓鱼网站

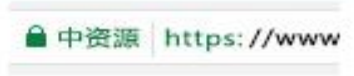


这些大厂都在使用

互联网金融，电商，互联网支付行业早就使用全站HTTPS来提高应用的安全性。

- 2015年3月，百度宣布进入全站HTTPS时代，将所有对百度搜索访问变为加密状态。百度成为中国第一个进入全站HTTPS的互联网公司。
- 2015年5月，百度搜索引擎全面支持收录HTTPS站点，并在排名上优先对待。
- 2015年7月，阿里巴巴旗下淘宝、天猫全站启用HTTPS，成为中国首家进入全站HTTPS的电商平台。
- 2016年6月，苹果公司宣布到2017年1月1日 App Store中的所有应用都必须启用 App Transport Security安全功能。
- App Transport Security（ATS）是苹果在iOS 9中引入的一项隐私保护功能，屏蔽明文HTTP资源加载，连接必须经过更安全的HTTPS。

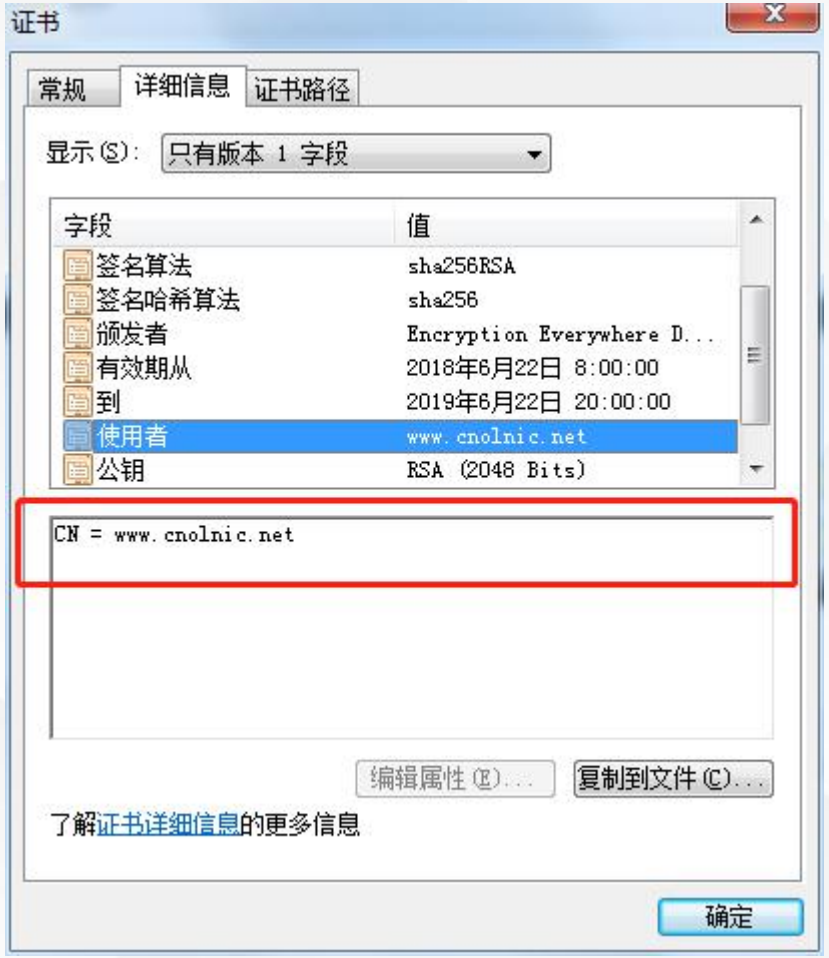
03 DV/OV/EV证书的区别

证书类型	域名型（DV）	企业型（OV）	增强型（EV）
绿色地址栏 （以Google Chrome为例）	 小锁	 小锁	 绿色地址栏
颁发时长	10分钟~1个工作日	2~3个工作日	3~5个工作日
适合网站	个人，小微企业等网站	企业官网、门户等网站	金融、电商等网站
证书可信度	低	高	超高
包含企业名称信息	×	√	√
验证企业名称合法性	×	√	√
查询电话验证	×	√	√
支持苹果ATS标准	免费版不支持	√	√
支持小程序	√	√	√
恶意软件扫描 Symantec特有	×	√	√
域名验证方式	域名whois邮箱	域名whois邮箱，同时验证公司名称与whois是否一致	域名whois邮箱，同时验证公司名称与whois是否一致

DV证书

DV SSL证书是只验证网站域名所有权的简易型（Class 1级）SSL证书，可10分钟快速颁发，能起到加密传输的作用，但无法向用户证明网站的真实身份。目前市面上的低价证书都是这个类型的，只是提供了对数据的加密，但是对提供证书的个人和机构的身份不做验证。

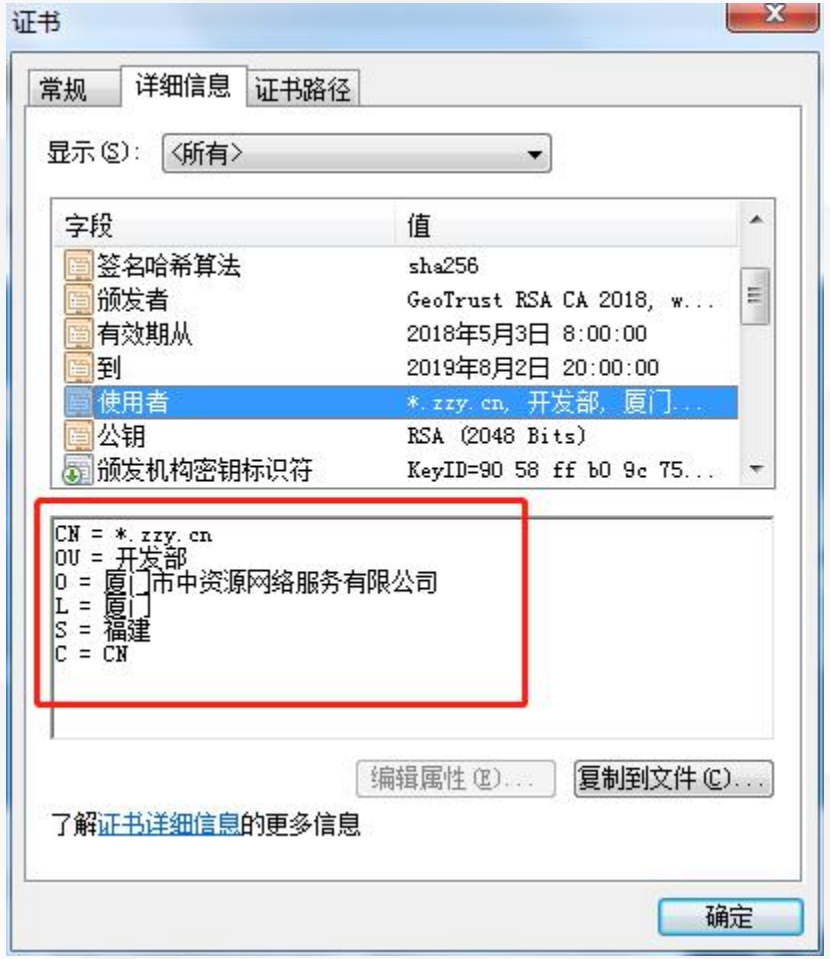
域名型（DV）使用者一栏只显示域名。建议选择OV和EV证书。



OV证书

OV SSL证书提供加密功能,对申请者做严格的身份审核验证,提供可信身份证明。和DV SSL的区别在于，OV SSL 提供了对个人或者机构的审核，能确认对方的身份，安全性更高。

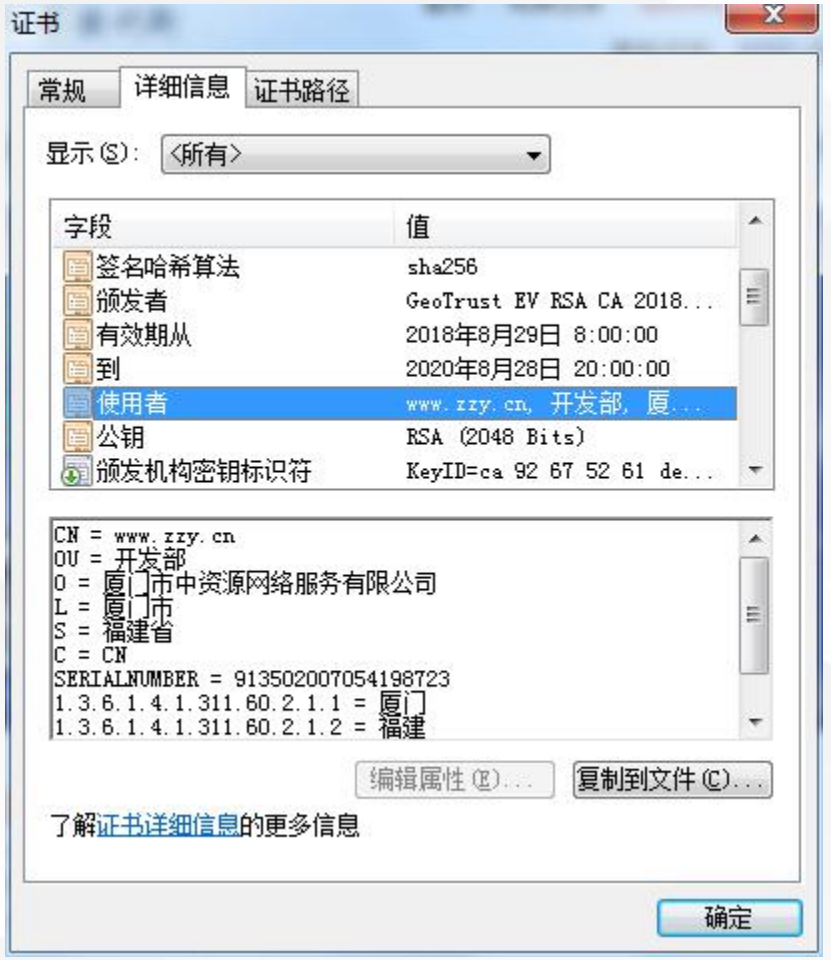
企业型（OV）使用者这一栏有详细的公司名称，安全性有了更大的保障，还能防止钓鱼网站，建议中小型企业使用。



EV证书

EV SSL证书遵循全球统一的严格身份验证标准，数据加密严格，是目前业界安全级别相当高（Class 4级）SSL证书。同时在浏览器显示公司名称。金融证券、银行、第三方支付、网上商城等，重点强调网站安全、企业可信形象的网站，涉及交易支付、客户隐私信息和账号密码的传输。

增强型（EV）使用者一栏会有详细的用户名称，安全系数最高，并且浏览器上面还会显示公司的名称，建议大型企业、特别是金融企业使用。



EV证书在各个浏览器的效果

谷歌

火狐

360

IE

04 SSL证书品牌的区别

SSL证书品牌

Geo Trust

GeoTrust 最为中国占有率最高的颁发机构(CA)，也是身份认证和信任认证领域的领导者。

Symantec

赛门铁克强大的PKI基础架构包括军事级数据中心和灾难恢复站点，可实现无与伦比的客户数据保护，可用性和安心。赛门铁克当下是SSL行业中最受认可和值得信赖的品牌。

Thawte

Thawte由南非Mark Shuttleworth创立，是第一家向美国以外的公共实体颁发SSL证书的认证机构，并且占据了全球SSL市场的40%。

RapidSSL 是一家国际知名的SSL证书提供商。公司以努力保护用户的利益为使命。

SSL证书品牌

域名型（DV）

- 加密功能
- 快速发证

GeoTrust

thawte

RapidSSL

企业型（OV）

- 企业身份合法性验证
- 加密功能
- 火狐浏览器蓝色地址栏
- 网站安全性

Symantec.

GeoTrust

thawte

增强型（EV）

- 绿色地址栏
- 加密功能
- 显示企业名称
- 企业身份验证
- 网站安全性认证

Symantec.

GeoTrust

thawte

SSL证书品牌

Symantec 高端

Symantec于2017年被digicert收购，签发单位显示为Digicert，但Symantec品牌不会做任何改变。

Thawte中端

推荐

GeoTrust 性价比之王

GeoTrust的性价比远高于其他品牌，市场占有率位于前两位，特别是购买多域名，更加实惠，建议首选。

RapidSSL 低端

SSL证书应用的行业

金融业	政府机关	门户网站
大专院校	社会团体	电信移动
电商	企业网站	应用程序
more		

中资源的优势

7*24小时服务

中资源拥有7*24小时客户电话，让您的问题立马解决。

24小时客服电话：0592-2958888

更优质的企业

中资源先后被评为：福建省科技小巨人领军企业、福建名牌产品、国家网络安全优秀单位、Google优秀合作伙伴等资质荣誉。

更贴心的服务

“客户至上，服务第一”是中资源企业文化的核心。我们从事互联网基础服务20年，始终保持最优质、贴心的服务。

更安全的用户体验

中资源成立于1999年，多年来，中资源不忘初心，永远把用户的安全体验放在首位。

End

为了您的网站安全

请给“他”添加一个SSL吧！


中资源
THANKS YOU