360 Browser Update (June 2019)

CA/BROWSER FORUM F2F47

Thessaloniki, Greece

June 12, 2019

Zhihui Liang
Haitao Huo (Halton) <huohaitao@360.cn>

Agenda

- 360 browser Update since March 2019
- 360 root store update
- Plan

360 Browser Update

Releases

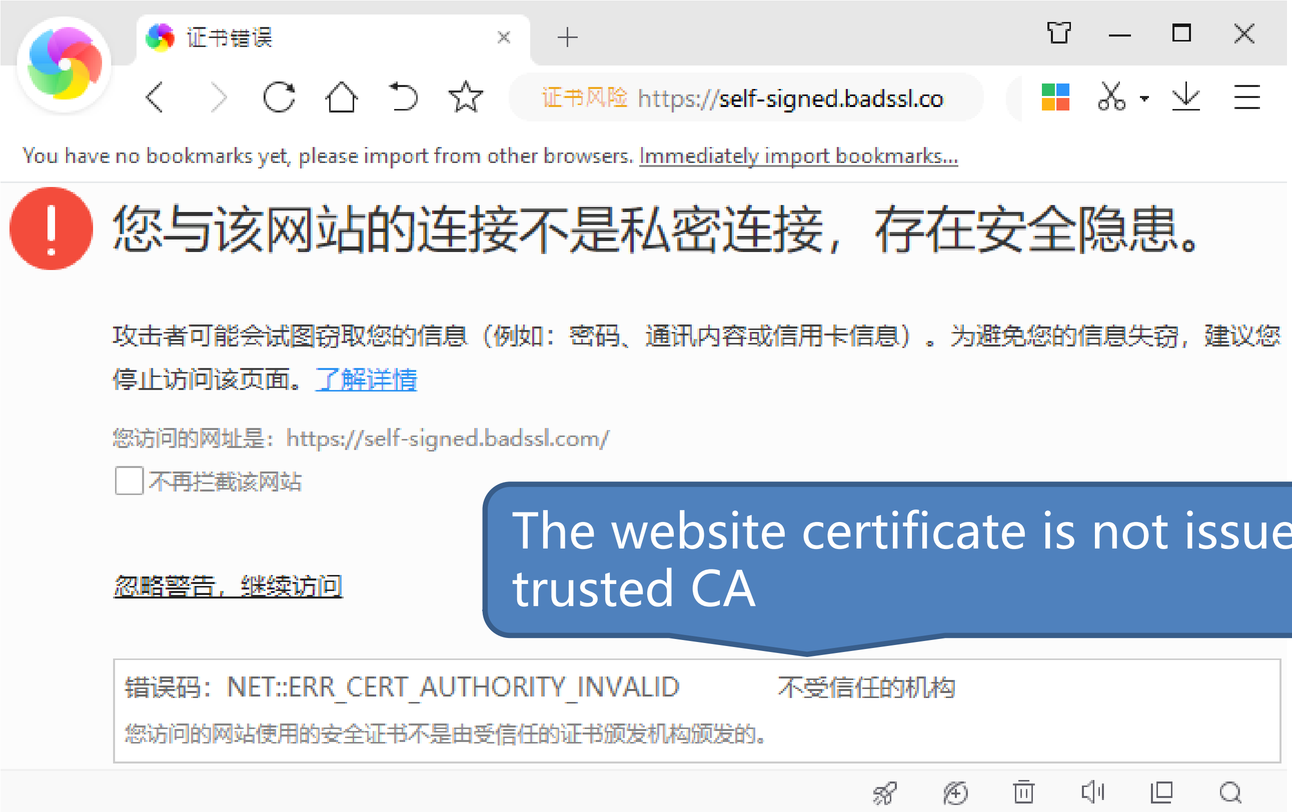
Product	Platform	Releases	Latest
Secure Browser (Chromium 63 based)	Windows	15	10.0.1840.0 (stable) 10.1.1775.0 (beta)
	Linux	5	1.0.1013.0
Extreme Browser (Chromium 69 based)	Windows	6	11.0.2116.0
	MacOS	7	1.0.1362.0

Secure related changes

- TLS 1.3 official edition support
  - Backport boringssl changes from Chromium72 and enable by default
  - Downgrade protection enabled
- CVE fixes backport, for eg:
  - CVE-2019-5786: Use-after-free in FileReader.
  - CVE-2018-20065 Handling of URI action in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to initiate potentially unsafe navigations without a user gesture via a crafted PDF file
- (New) CRLSets support
  - Like Google Chrome does, 360 maintain a global CRLSet in China
  - Aim to block problematic certificates in emergency situations
  - Currently, the list is maintained by admin.
- (New) Cert Error enhancement

Cert Error Enhancement

- Comprehensive message to help non-tech people to understand risks of certificates errors before click ignore/proceed.
- Support 9 usual errors including: NET::ERR_CERT_DATE_INVALID, N NET::ERR_CERT_AUTHORITY_INVALID etc.



You have no bookmarks yet, please import from other browsers. Immediately import bookmarks...

您与该网站的连接不是私密连接，存在安全隐患。

攻击者可能会试图窃取您的信息（例如：密码、通讯内容或信用卡信息）。为避免您的信息失窃，建议您停止访问该页面。了解详情

您访问的网址是：https://self-signed.badssl.com/

□ 不再拦截该网站

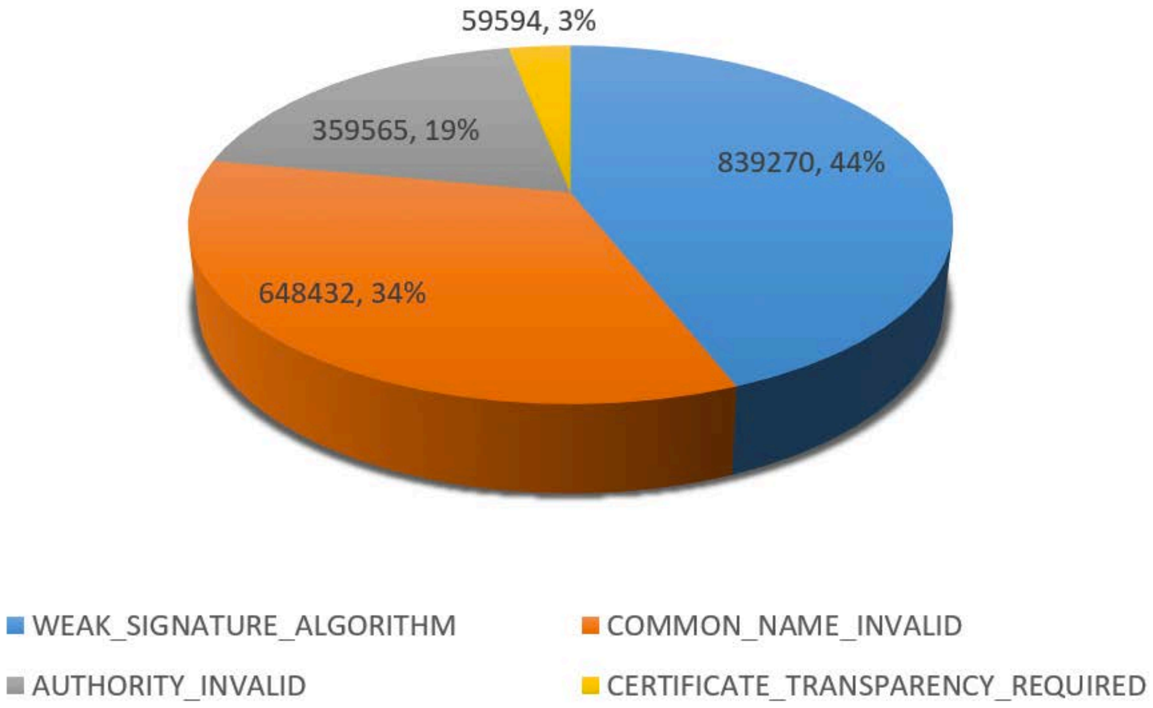
忽略警告，继续访问

错误码：NET::ERR_CERT_AUTHORITY_INVALID 不受信任的机构

您访问的网站使用的安全证书不是由受信任的证书颁发机构颁发的。

The website certificate is not issued by trusted CA

Statistics of error types (May 2019)



Top five URLs with fake certs (May 2019)

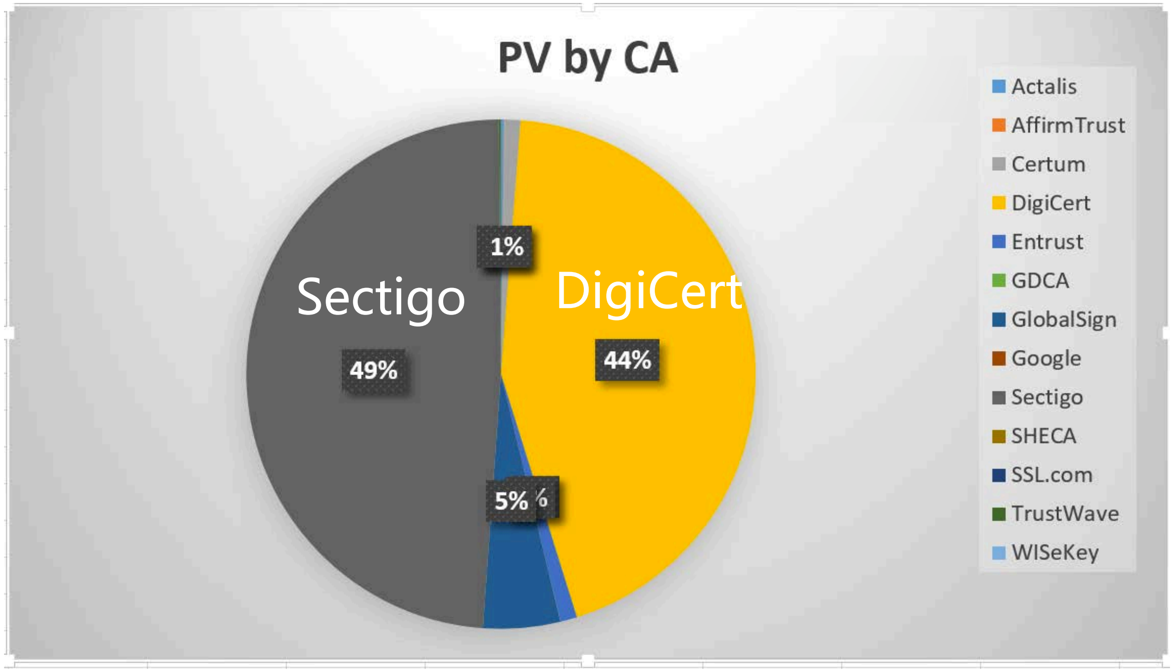
URL	Fake Cert Signature (SHA-1)	Blocks
www.51test.net	17298e3b71e6660405b9f4cd60b3ea419f331b5a	**797418**
v.qq.com	702b4965034f1b44816445eebfd1e8a81212e002	**757154**
v.qq.com	9f1d7a61b6afb332cf9f90362ad8b2af99aeb890	**586864**
mini.eastday.com	42be488a66afb288588c1e68607b8015f8639ad0	**443465**
www.baidu.com	d1f6323db6f2ec81e7023690f49b2d91e0c3993a	**282652**

Observations:

- Big concern the visits of above popular websites, need future investigation why it happens.

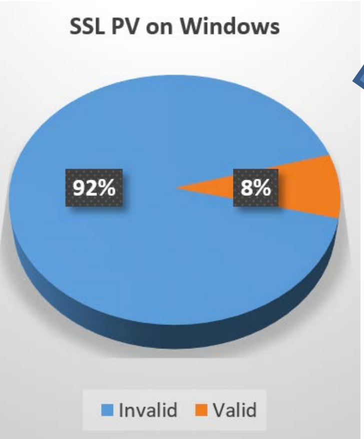
360 Root Store

Statistics of PV by CA (recent two weeks)

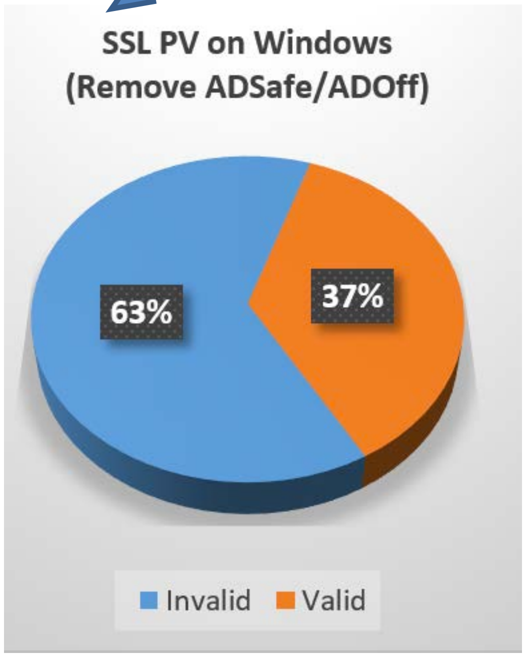


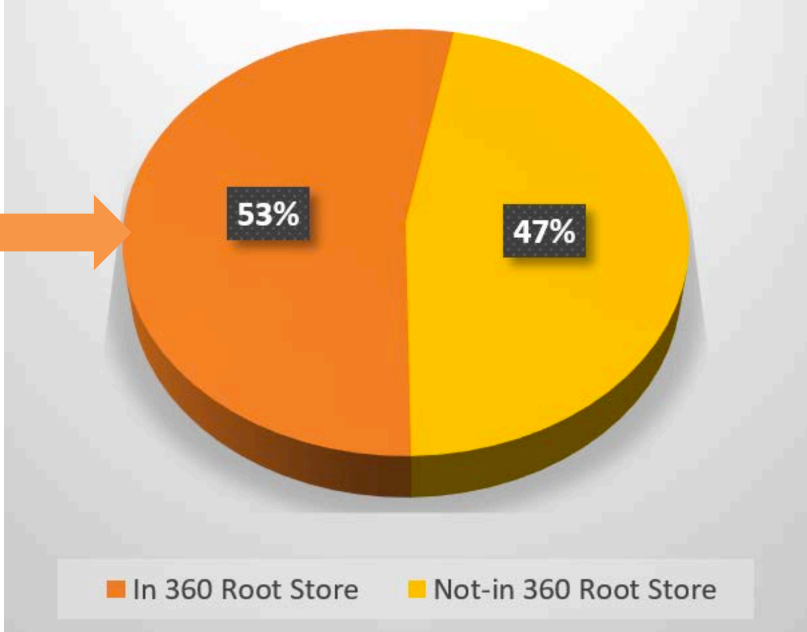
13 CAs, 53 roots jointed 360 CA program by June 2019

SSL PVs on Windows (recent two weeks)



Data clean to remove AD related





- AD related extensions generate lots cert errors
- Invalid Certs are still large portion (63%)
- Over half normal cert roots are in 360 root store

SSL.com (Feb 26, 2019)

Name	Public Key	Fingerprint (SHA1)	Valid Until
SSL.com EV Root Certification Authority ECC	ECC 384, SHA-256	4C:DD:51:A3:D1:F5:20:32:14:B0:C6:C5:32:23:03:91:C7:46:42:6D	Feb 13, 2041
SSL.com EV Root Certification Authority RSA R2	RSA 4096, SHA-256	FC:8E:2C:BC:87:41:5A:B6:49:A0:0C:EA:08:F5:11:BA:C9:AC:26:5C	May 31, 2042
SSL.com Root Certification Authority ECC	ECC 384, SHA-256	8F:65:0C:B9:C0:2E:39:CC:CE:1A:A1:7C:84:25:E1:6D:7F:22:DB:0B	Feb 13, 2041
SSL.com Root Certification Authority RSA	RSA 4096, SHA-256	B7:AB:33:08:D1:EA:44:77:BA:14:80:12:5A:6F:BD:A9:36:49:0C:BB	Feb 13, 2041

Certum (Feb 28, 2019)

Name	Public Key	Fingerprint (SHA1)	Valid Until
Certum Trusted Network CA	RSA 2048, SHA-256	07:E0:32:E0:20:B7:2C:3F:19:2F:06:28:A2:59:3A:19:A7:0F:06:9E	Dec 31, 2029

Sectigo (March 25, 2019)

Name	Public Key	Fingerprint (SHA1)	Valid Until
Sectigo (AAA)	RSA 2048 SHA-1	d1eb23a46d17d68fd92564c2f1f1601764d8e349	Jan 1, 2029
Sectigo (AddTrust)	RSA 2048 SHA-1	02faf3e291435468607857694df5e45b68851868	May 30, 2020
Sectigo (CCA)	RSA 2048 SHA-1	ee869387fffd8349ab5ad14322588789a457b012	Jan 1, 2031
Sectigo (formerly Comodo CA ECC)	ECC 384, SHA-384	9f744e9f2b4dbaec0f312c50b6563b8e2d93c311	Jan 19, 2038
Sectigo (formerly Comodo CA)	RSA 4096 SHA-384	afe5d244a8d1194230ff479fe2f897bbcd7a8cb4	Jan 19, 2038
Sectigo ECC	ECC 384 SHA-384	d1cbca5db2d52a7f693b674de5f05a1d0c957df0	Jan 19, 2038
Sectigo	RSA 4096 SHA-384	2b8f1b57330dbba2d07a6c51f70ee90ddab9ad8e	Jan 19, 2038

Google (June 4, 2019)

Name	Public Key	Fingerprint (SHA1)	Valid Until
GTS Root R1	RSA 4096, SHA-384	e1:c9:50:e6:ef:22:f8:4c:56:45:72:8b:92:20:60:d7:d5:a7:a3:e8	Jun 22, 2036
GTS Root R2	RSA 4096, SHA-384	d2:73:96:2a:2a:5e:39:9f:73:3f:e1:c7:1e:64:3f:03:38:34:fc:4d	Jun 22, 2036
GTS Root R3	ECC 384, SHA-384	30:d4:24:6f:07:ff:db:91:89:8a:0b:e9:49:66:11:eb:8c:5e:46:e5	Jun 22, 2036
GTS Root R4	ECC 384, SHA-384	2a:1d:60:27:d9:4a:b1:0a:1c:4d:91:5c:cd:33:a0:cb:3e:2d:54:cb	Jun 22, 2036
GS Root R2	RSA 2048, SHA-1	75:e0:ab:b6:13:85:12:27:1c:04:f8:5f:dd:de:38:e4:b7:24:2e:fe	Dec 15, 2021
GS Root R4	ECC 256, SHA-256	69:69:56:2e:40:80:f4:24:a1:e7:19:9f:14:ba:f3:ee:58:ab:6a:bb	Jan 19, 2038

Newly added Root CAs (SHECA)

SHECA (June 4, 2019)

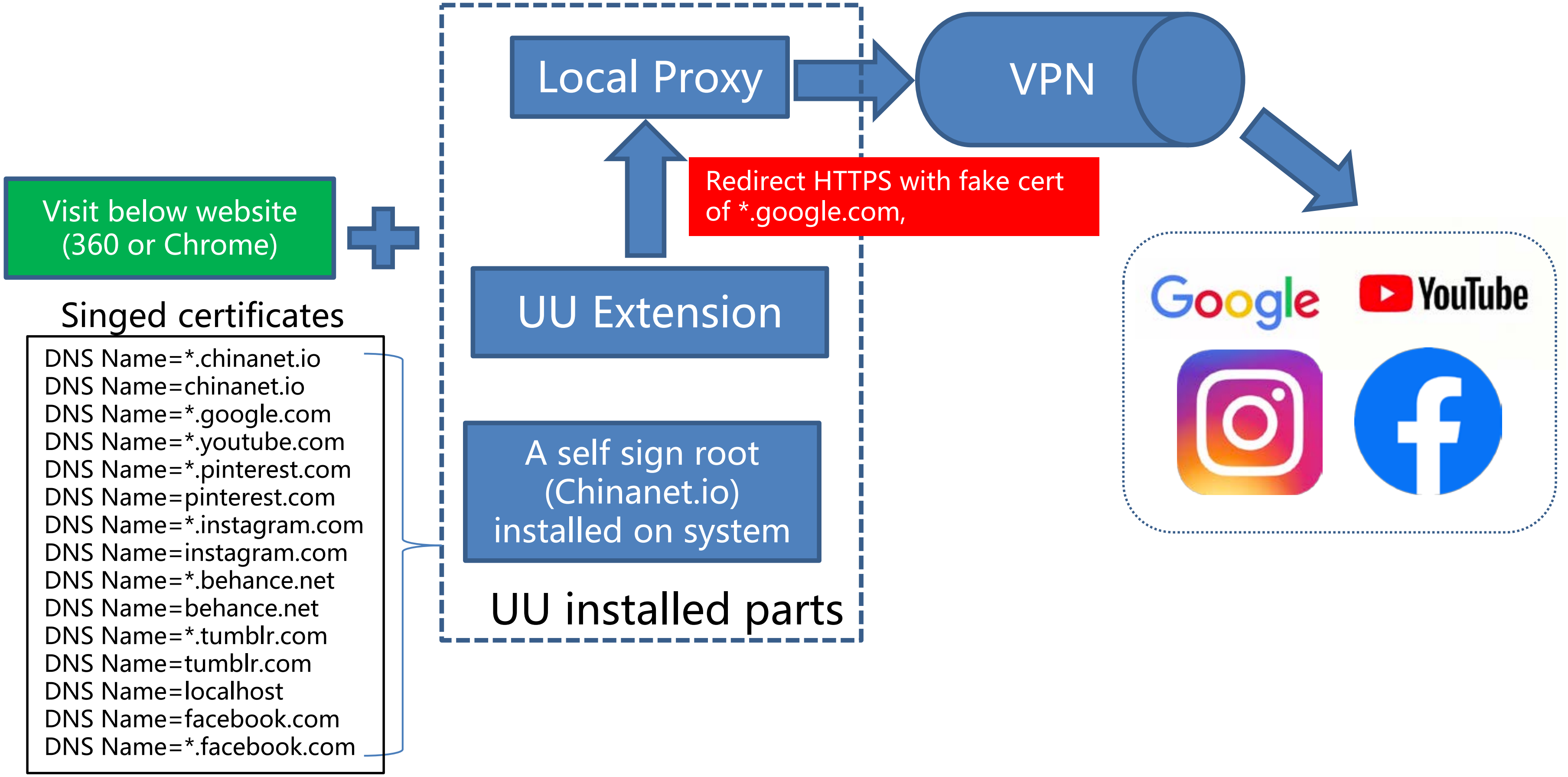
Name	Public Key	Fingerprint (SHA1)	Valid Until
UCA Global G2 Root	RSA 4096, SHA-384	28:F9:78:16:19:7A:FF:18:25:18:AA:44:FE:C1:A0:CE:5C:B6:4C:8A	Dec 31, 2040
UCA Extended Validation Root	RSA 4096, SHA-256	A3:A1:B0:6F:24:61:23:4A:E3:36:A5:C2:37:FC:A6:FF:DD:F0:D7:3A	Dec 31, 2038

Rejection and MISC

Name	Reason
China Unicom CA (CUCA)	RSA2048 but valid until 2036; According NIST Special Publication 800-57 Part1 [1], RSA2048 may unsafe after 2030
Self-sign website owner	• The website owner just want to remove the warnings of unsecure message (The warning does work) • Simply to guide them to request certs from official CAs
Non-CA related	Browser bugs, spams, etc

[1] https://www.jscape.com/blog/bid/75018/Securely-Retrieving-Email-from-GMail-using-Java-POP-Library

An app signed fake certificates – UU http://uu.ydtxhr.org/



Visit below website (360 or Chrome)

Singed certificates

DNS Name=*.chinanet.io
DNS Name=chinanet.io
DNS Name=*.google.com
DNS Name=*.youtube.com
DNS Name=*.pinterest.com
DNS Name=pinterest.com
DNS Name=*.instagram.com
DNS Name=instagram.com
DNS Name=*.behance.net
DNS Name=behance.net
DNS Name=*.tumblr.com
DNS Name=tumblr.com
DNS Name=localhost
DNS Name=facebook.com
DNS Name=*.facebook.com

Local Proxy

VPN

Redirect HTTPS with fake cert of *.google.com,

UU Extension

A self sign root (Chinanet.io) installed on system

UU installed parts

WARNINGS: UU CAN decrypt user traffic when user visit these websites.

What will happen next

- Releases
  - EE12 release (Chromium 76 based)
    - Support all platforms: Windows/MacOS/Linux
  - EE11 turns into SE11
  - SE10 for Linux public release (can be download from official website)
- CRLSets auto crawl support with CRL in certs
- Show warning to TLS 1.0/1.1 website of deperaction message, to be discuss
- TLS 1.3 and CVE important fixes backport

360
www.360.cn

Thank You!

谢谢！

北京朝阳区酒仙桥路6号院2号楼 100015
Building 2, 6 Haoyuan, Jiuxianqiao Road, Chaoyang District,Beijing,P.R.C. 100015
Tel +86 10 5682 2690   Fax +86 10 5682 2000