Measuring Domain Impersonation with Certificate Transparency Logs

Richard Roberts, Yaelle Goldschlag, Dave Levin

Motivation

TLS-validated domains aren't always who they appear to be:

- amazon.com.es-nav-youraccount-btn.es-login-signonv3.com
- account.paypal.com-page-auth-u7dn6x13is.ml
- apple.com.find-device-location.review
- docusign.com.common-oauth2.gq
- ebay.com-item-apple-iphone-x-gray-256gb-unlocked.kl7.us
- paypal.com.verif-unusual-id-000263-160526.com
- oldschool.runescape.com-wz.ml

Question Why and how often are attackers given impersonating certificates?

Methodology

censys — Active Scans & Certificate Transparency Logs

Alexa — Top 100k Domains Worldwide

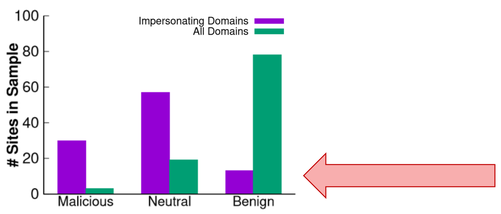
Filtering Process
- Include dots and dashes
  - example.com
  - example-com
- Whitelisting

Final Impersonating Set

Unique Domains
173,321

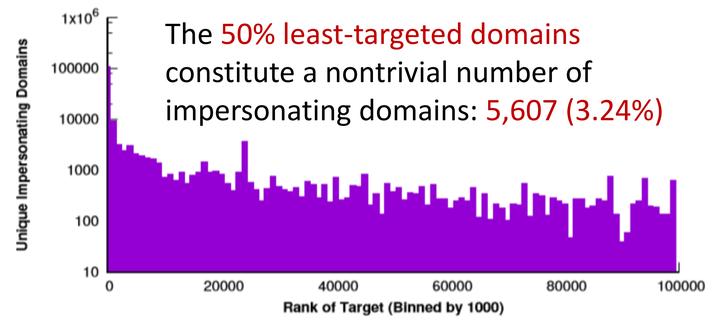
Unique Certificates
290,239

Impersonating domains are far more likely to be malicious



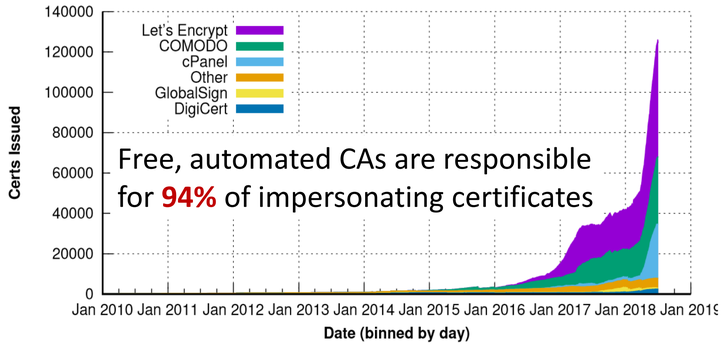
Who is being targeted?

Paypal and Apple are the most popular targets, but we see a long tail by the target's Alexa ranking.



The 50% least-targeted domains constitute a nontrivial number of impersonating domains: 5,607 (3.24%)

Who is Issuing Certificates?

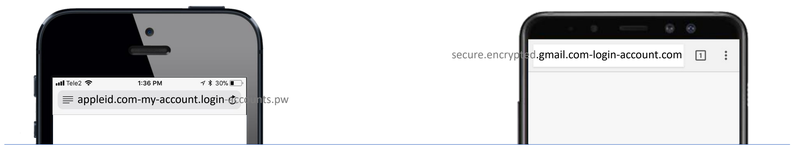


What is the barrier for entry?

Free

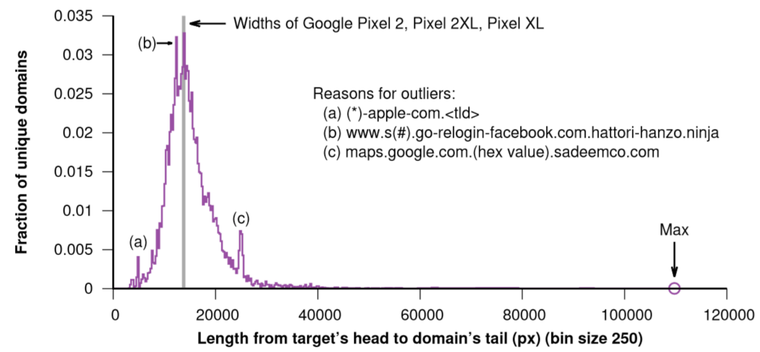
- Certificates — COMODO, Let's Encrypt
- Registrars — .ml, .gq, .tk, .cf, .ga
- Hosting — aws, CLOUDFLARE

Where does the target appear?



Safari on iOS
Left justifies entire domain

Chrome on Android
Right justifies from TLD



Are attacks evolving?

Attacks are increasing in complexity by composing multiple forms of domain impersonation, such as Unicode homographs:

www.facebook.com.msg130.top

Uncovering Large Campaigns

	RuneScape	Star Wars
	services.runescape.com-dos.ga	starwars.com.p58vfa15.top
	oldschool.runescape.com-ds.ml	starwars.com.dwm8jcz0ro.top
	secure.runescape.com-rb.ml	starwars.com.kyyvnnylj.bid
	services.runescape.com-zs.top	starwars.com.dvqzh83l6r.site
	secure.runescape.com-kn.cf	starwars.com.canjhstcs.bid
Google Safe Browsing	845 Unique Domains	1,079
CT Logs	4,522	3,071
Safe Browsing Coverage	18.89%	35.14%