What is Typosquatting and what can we do about it?

Matej Lazarević

OWASP Croatia, October 2021

tl;dw

- Definition of typosquatting
- Is it really a big deal?
- Preventing headaches caused by typosquatters
- Open source tools

whoami

- Frontend Dev at Barrage, Osijek
  - https://barrage.net & https://www.blockchain.hr
  - Email: matej.lazarevic@barrage.net & matej.lazarevich@gmail.com
  - Github: https://github.com/dekadentno
  - Linkedin: https://www.linkedin.com/in/matej-lazarevich/
- AppSec enthusiast and newbie

Typosquatting

- Registering domains with misspelled names
- Targeting (mainly) popular domain names
- Confusing users into believing that the targeted brands own that domain

Typosquatting

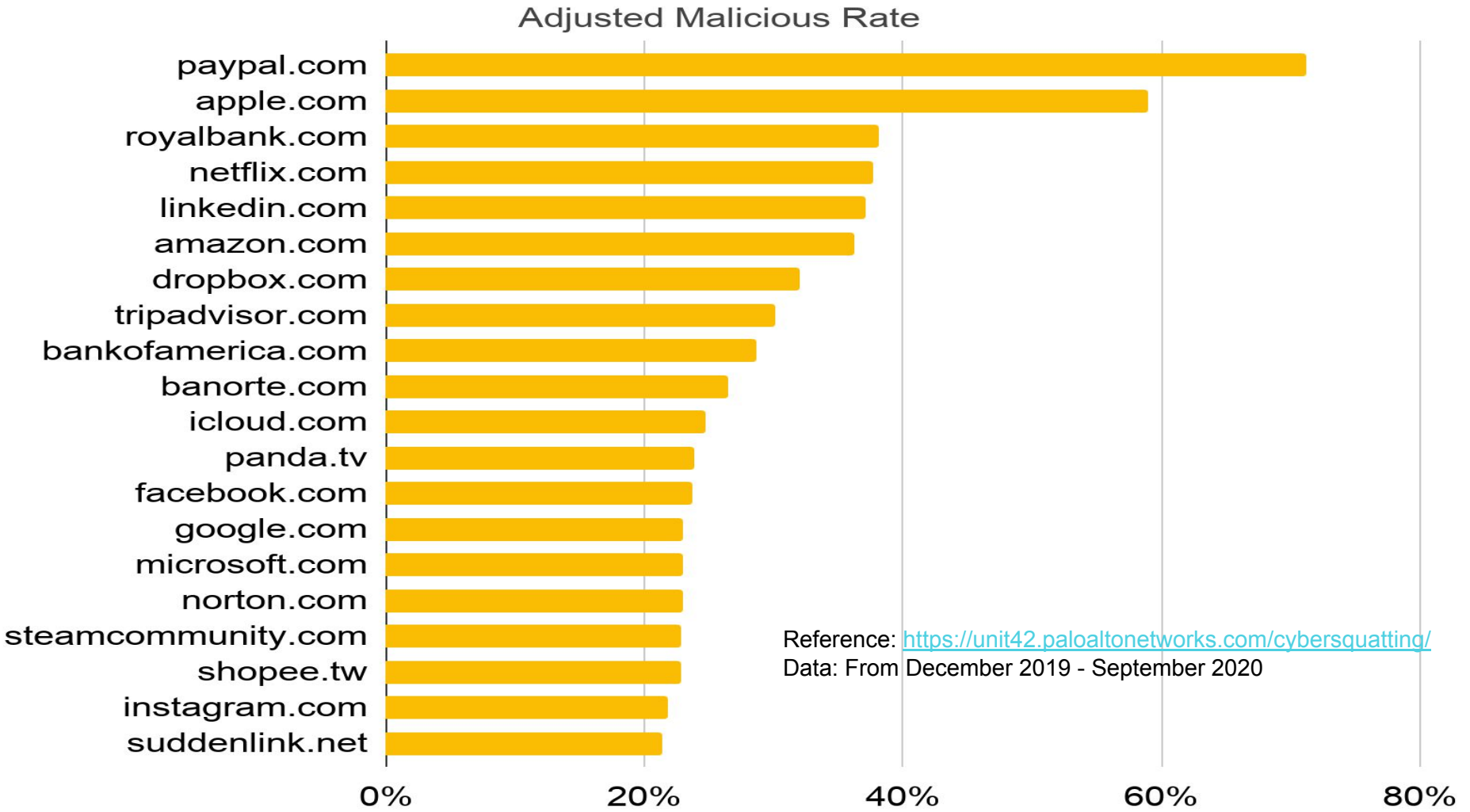
- Reasons
  - Phishing
  - Distributing malware
  - Ads
  - Affiliate marketing
  - Redirecting to unintended destinations
  - Stealing traffic
  - Selling domains at higher prices (*cybersquatting*)
  - Intentionally violating someone’s reputation
  - Re-bill scam
  - Potentially unwanted program (PUP)
  - Reward scam
  - Technical support scam

Typosquatting

- Techniques
  - Omission (removing chars) - facebok.com
  - Addition (adding chars) - gooogle.com
  - Substitution (swapping chars) - paypa1.com
  - Transposition (relocating chars) - linekdin.com
  - Homoglyphs (lookalikes, using cyrilic or other characters) - páýpal.com (*homographsquatting*)
  - Hyphenation - linkedin-login.com, netflix-payments.com, youtube-live.com, facebook-auth.co (*combosquatting*)
  - Homophone variants (words that sound alike) - weather ➡ whether, forever21.com ➡ 4ever21.com (*soundsquatting*)
  - Top level domain abuse - .co, .cm
  - Fat-finger errors (physical proximity on the keyboard) - hoogle.com, foogle.com
  - Doppelganger domains (missing dot) - login.facebook.com ➡ loginfacebook.com
  - Subdomain in link - safety.microsoft.com.lkjrihgrk.ooh3rhi3i3ir3o.com (*levelsquatting)*

Is it really a big deal?

- Social-Engineer Toolkit - https://github.com/trustedsec/social-engineer-toolkit
- Effective strategy regardless of the experience of the user
- Stats (Palo Alto Networks, Oct 2021.)
  - 13,857 squatting domains registered in December 2019 (450 per day avg)
  - 19% are malicious (malware, phishing...)
  - 37% are high risk (association with malicious URLs)
- Typosquatting of NPM packages


Adjusted Malicious Rate
paypal.com
apple.com
royalbank.com
netflix.com
linkedin.com
amazon.com
dropbox.com
tripadvisor.com
bankofamerica.com
banorte.com
icloud.com
panda.tv
facebook.com
google.com
microsoft.com
norton.com
steamcommunity.com
shopee.tw
instagram.com
suddenlink.net
0%
20%
40%
60%
80%
Reference: https://unit42.paloaltonetworks.com/cybersquatting/
Data: From December 2019 - September 2020

What can we do about it?

- User recommendations
  - Avoid clicking on links and verify them before clicking (good luck with that)
  - Use password managers
  - Enable 2FA
  - Use U2F / FIDO2
  - Use bookmarks (or search engines)
  - Use antivirus software

What can we do about it?

- Technical recommendations
  - Register domain variations before others do
  - Register your trademark
  - Notify customers and stakeholders
  - Use whois
  - Use SSL
- Legal
  - https://www.govinfo.gov/content/pkg/CRPT-106srpt140/html/CRPT-106srpt140.htm
  - If the domain is registered in Cambodia, there's nothing you can do

What can we do about it?

- dnstwist - https://github.com/elceef/dnstwist
- gfyp - https://github.com/0xd34db33f/gfyp
- And then what?
  - Blacklisting
  - URL filtering
  - Report to public lists (e.g. The Domain Block List, PhishTank)
  - Report to Google

Demo time 🤞

Conclusion

- Users rely on domain names to identify brands and services
- Security awareness
- Use 2FA, password managers, U2F / FIDO2
- Stay vigilant and pay attention
- dnstwist + gfyp (you surely have a rpi somewhere in your desk)
- Continuous monitoring and analysis are necessary

Questions?

References

1. https://sectigostore.com/blog/what-is-typosquatting/
2. https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting
3. https://www.csoonline.com/article/3600594/what-is-typosquatting-a-simple-but-effective-attack-technique.html
4. https://unit42.paloaltonetworks.com/cybersquatting/
5. https://www.upguard.com/blog/typosquatting
6. https://github.com/elceef/dnstwist
7. https://github.com/0xd34db33f/gfyp