Who is living off your domain name?

Swapneel Patnekar
swapneel.patnekar@shreshtait.com

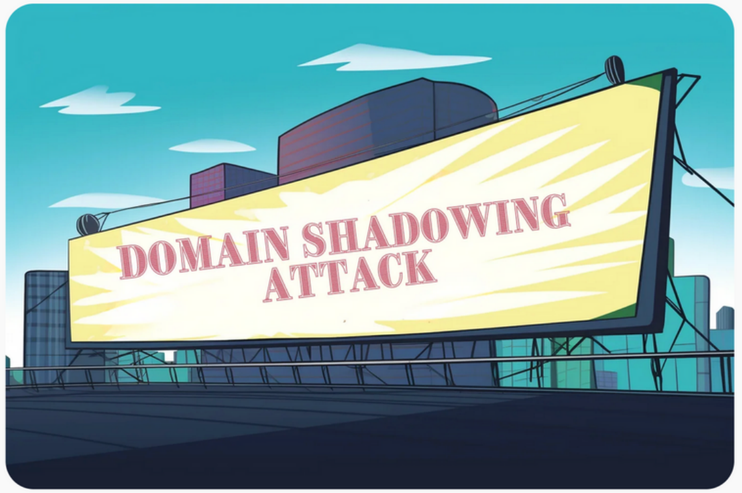
About me

- CEO at Shreshta, India - a DNS Security and cyber threat intelligence company
- Co-chair of DNS Abuse SIG & FIRST Liaison (India)
- APNIC Community Trainer

Domain Shadowing attacks

- November 2022, research into domain shadowing attacks

- Large scale abuse under ccTLDs such as .lk, .np etc



Attackers targeting .lk domains using domain shadowing attack

Nov 29, 2022 — by Swapneel Patnekar

Before we deep dive into how attackers target .lk domains using domain shadowing attack, first, a primer on registration of a domain name under .lk namespace.

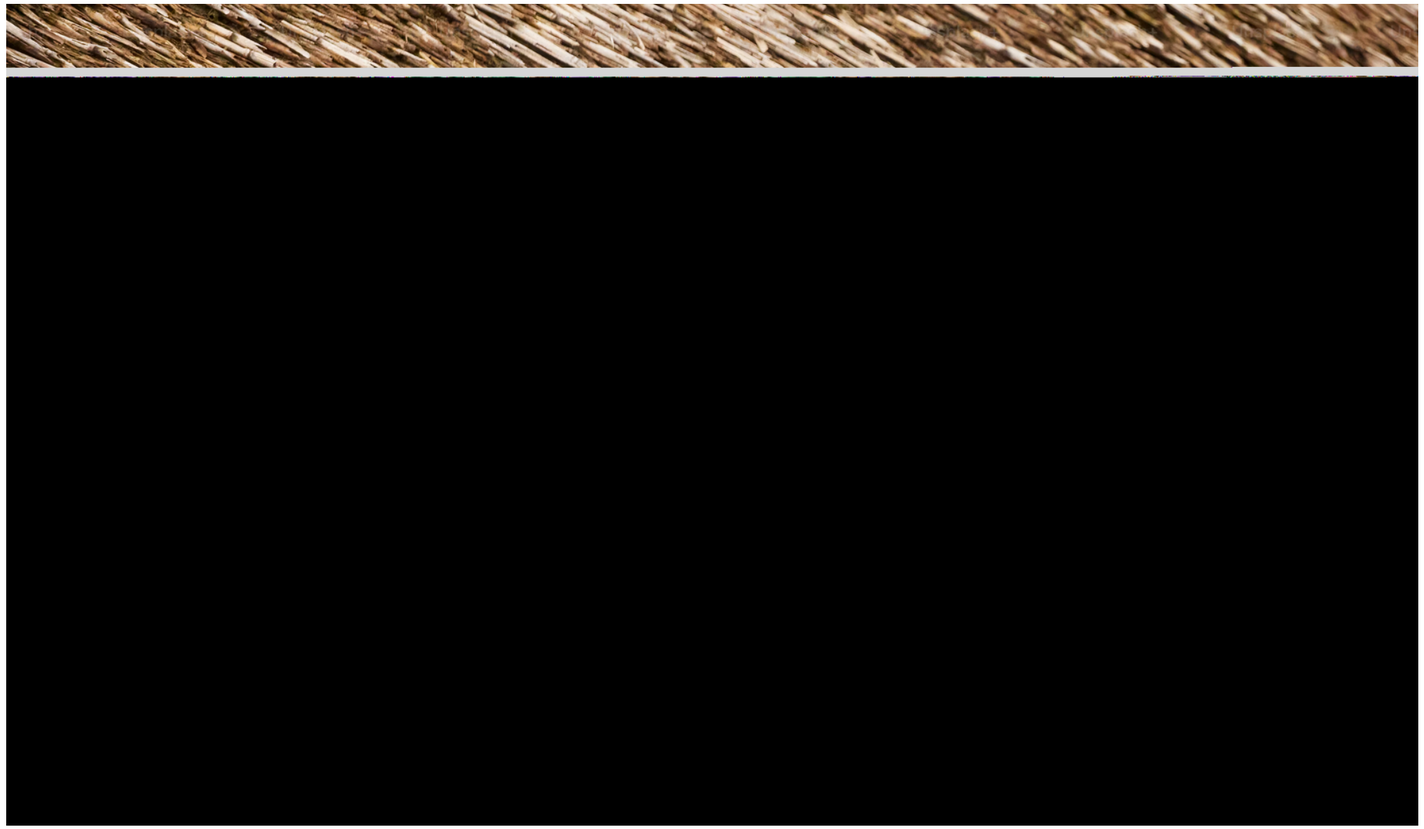
tl;dr registration of a domain name under .lk namespace is regulated

The domain registration policy says the LK registry may ask for documents supporting the request for a domain name registration. Depending on the category the domain registration would fall under, the list of documents would vary,

Blog post - https://shreshtait.com/blog/2022/11/attackers-targeting-lk-domains-using-domain-shadowing-attack/

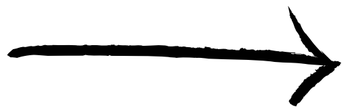
Domain Shadowing attack

- Threat actors gain control of the DNS control panel of the domain name (possibly brute force)
- Stealthily insert subdomains under the compromised domain name
- The DNS records of the main domain name are untouched
- The DNS records of the subdomain point to the threat actors network infrastructure



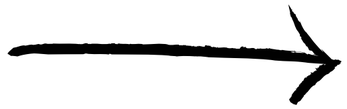
Domain Shadowing attack overview

example.com
login.example.com
cpanel.example.com



192.0.2.1
AS64496

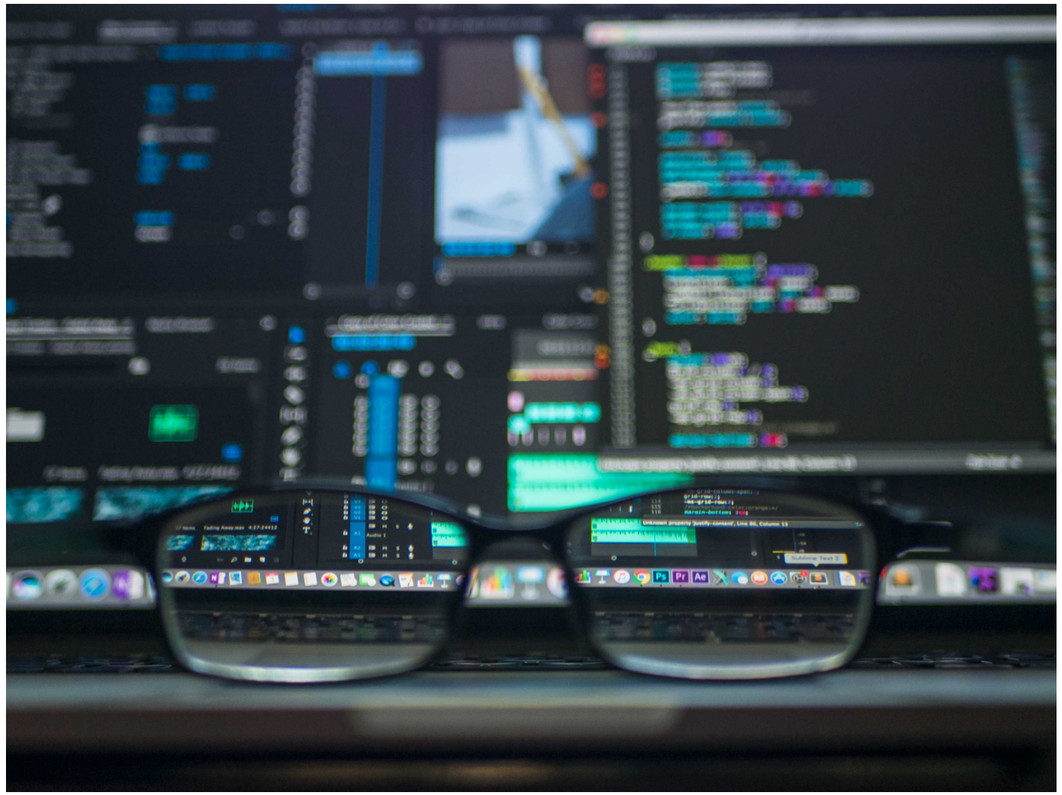
phish.example.com
bank.example.com
c2.example.com



198.51.100.1
AS64511

Threat actors perspective

- Use the reputation of a legitimate domain name
- Evade detection
- Eliminate efforts into buying a domain(with stolen funds ofcourse!) name for malicious purposes



Detection

- Deviations from the parent zone
- Subdomain names pointing to a different ASN
- Subdomain names pointing to a different country
- Subdomain names pointing at known threat actor network infrastructure

Why is this happening?

- Weak passwords - threat actors brute force
- 2FA is not available or not enabled
- No monitoring in place to monitor the DNS zone

Best practices

- Strong unique password for the domain name control panel
- Enable 2FA if it’s available
- Monitor the DNS zone - easier said than done. Hosted DNS providers do not provide any ability to monitor changes to the DNS zone

ShadowFinder

- Built for Registrants
- Detects and list subdomain names along with IP address, ASN, Country code etc
- Monitors and flags deviations in DNS zone data

https://shadowfinder.shreshtait.com

Under the hood

- Passive DNS analysis
- Subdomain enumeration techniques
- CT logs

ShadowFinder

Limitations

- Passive DNS visibility
- Subdomain name enumeration techniques

Early release, rough edges

Next release roadmap

- Enrichment with threat intelligence data - threat actor network infrastructure
- Reverse DNS data?
- Alert by email

Thoughts/Questions?

- Email - swapneel.patnekar@shreshtait.com