Domain parking: A look at the business model and cybersecurity implications

Posted on January 26, 2021

In this white paper, we describe the notion of domain parking, introduce its motivation, stakeholders, and ecosystem. We go through the main security issues it poses, discuss the detection of parked domain names, and comment on the possibility of mitigating the risk posed by them.

Table of Contents

---

1. The business model of domain parking

Internet domain names represent the identity of an organization or a brand. Hence, domain names have a business value and they can be purchased and sold on the market like stocks. Hence, they can be used as an investment and speculating with them is also common.

But what do you do with a domain if there is no intention to use it for an actual service? These domains get **parked**: they resolve in the Domain Name System (DNS), are registered, but aren't used to host a specific web page or for handling email traffic. And there are numerous ways they can generate profit: a number of parking providers offer monetizing services for domain owners. They host advertisement pages that result in pay-per-click and other means of making profit. In a recent blog of Unit 42, the global threat intelligence team at Palo Alto Networks reported that from March to September 2020, they identified 5 million newly parked domains, making domain parking a billion-dollar business.

1.1 The domain parking ecosystem

The first important players in this business are **domain owners**. Many of them invest into domains with speculative purposes, even with a definite goal of making money from parked domains. Buying a domain is cheap and easy, making this kind of business attractive.

As it is about domain registration or purchase, we cannot ignore the role of domain registrars, the entities to whom ICANN, the Internet Corporation for Assigned Names and Numbers delegates the registration and resell activity of Internet domains, or those who are responsible for dealing with domains under country-code top-level domains. They have an interest in keeping the domain business active and increase its volume, hence, most of them prefer making a domain registration or purchase as simple as possible.

The next relevant set of entities is that of **parking providers**. They are specialized in providing flawless services for those who want to park their domains, and provide them with a revenue so that the whole business is profitable also for them. They do so by collaborating with and getting paid by **advertisement syndicates**. Hence, both the domain owners and the parking providers

have their interest in the high number of visitors of the parked pages as this is the metric determining their income.

The **advertisement syndicates** (Google is the maybe most famous amongst them) have the aim of efficiently reaching their audience with targeted advertisements. They are typically also interested in high visibility, that is, many visitors of the pages where the ads are hosted. Their additional interest is in collecting preference data about the visitors in support of targeted advertising.

On the other end of the chain, there are the **advertisers** who pay for the advertisements. While proper advertisements are important for any company, unfortunately, some of them aren't always ethical or benign.

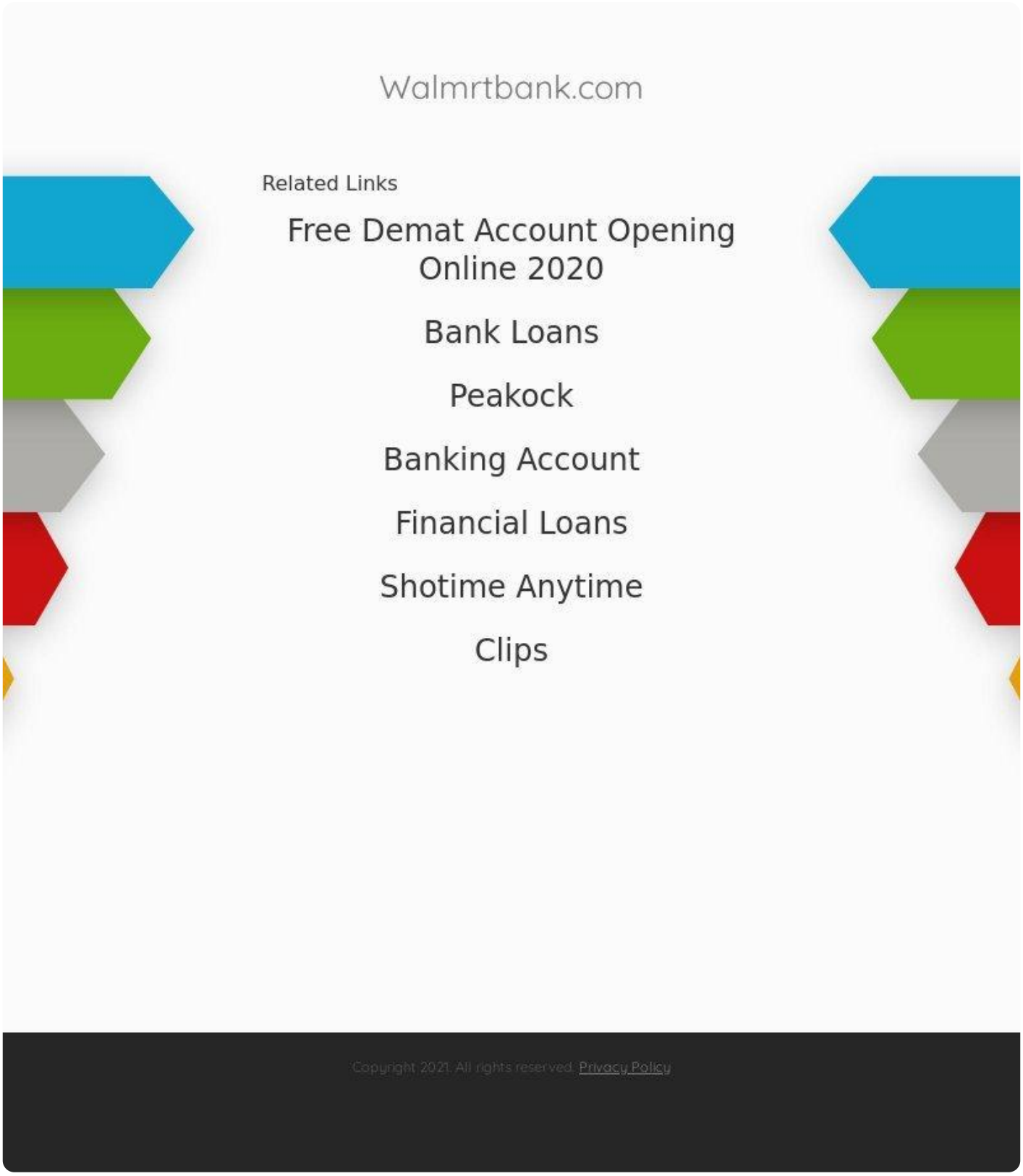
1.2 Domain parking infrastructure

Let us now take a quick look at the technology behind this scene. A registered domain is operational if and only if it is there in the Domain Names System (DNS). Also, it has a WHOIS record that is supposed to reveal the ownership of the domain. Unfortunately, as a consequence of new regulations such as the Generic Data Protection Regulations (GDPR) of the European Union, and maybe more importantly their purposive misinterpretations, the owners of most domains are hidden, a fact seriously undermining many security measures of the operation of the Internet. Yet data from the domain name system, notably:

- IP addresses associated with the domain,
- Authoritative name servers,
- The registrar's identity,
- Registration, update, and expiry dates,
- and registrant country information

are essential when considering any domain-related activity.

When viewed with a browser, the parked domain will either redirect or directly resolve to a **landing page**. These are frequently run by the parking provider and serve a tremendous amount of parked domains. They are responsible for displaying the advertisement contents to direct the visitor to the appropriate target, and also to evaluate the measures that are the basis of the payments, e.g. number of clicks. A typical landing page looks like this:


Walmrtbank.com
Related Links
Free Demat Account Opening Online 2020
Bank Loans
Peakock
Banking Account
Financial Loans
Shotime Anytime
Clips
Copyright 2021. All rights reserved. Privacy Policy

(We shall see later that this screenshot is a good illustration of multiple issues.)

It is clear from this scenario that there are many points where the whole process can turn out harmful. The fact that the domain parking business is largely unregulated further increases the risks. Let us revise some of the possible attack vectors.

2. The dark side of domain parking

In what follows we shall not deal with types of fraud whose victims are the stakeholders themselves. Such illicit activities include, e.g., the parking provider being dishonest to the domain owner with respect to traffic measures or the generation of fake traffic (aka "click fraud"); we refer to the literature, notably the work of Alrwais et al. (proc. of the 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA 2014, pp. 207-222) for the details of these. Here we focus on the illicit activities against entities outside of this ecosystem, notably, users of the World Wide Web, brands, and organizations.

2.1 Typosquatting

Typosquatting is the use of domain names resembling a target domain name. According to the definition in the work of Szurdi et al. (proc. of the 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA 2014, pp. 197-206), a very detailed and important research paper on the topic, a typosquatting domain, in a strict sense, is lexically similar to the target domain, it was "registered to benefit from traffic intended for a target domain" and is "the property of a different entity". Given a popular domain name as a target, there is a huge zoology of possibilities to generate alternatives that can be confused visually by the target or can be entered via an eventual misspelling. These possibilities include: simple typos (faxebook), registration in a different top-level domain (facebook[.]fun), IDN homoglyph attacks (e.g. replacing one of the letters "o" with the identically looking Greeks omicron), etc.

The owners of the typically targeted pages also register lexically similar domains, actually to prevent typosquatting, and these typically redirect to or land at the legitimate page of the owner. But this is just a small portion of such domain registrations. Beside a number of other possible motivations

like, e.g. using the domain in a phishing attack, harvesting emails sent to misspelled addresses, trying to sell it to the legitimate owner, or expressing a different opinion than the one on the legitimate page, a frequent reason behind registering typosquatting domains is to park these domains and to monetize them.

As an illustration, see the landing page screenshot in the previous Section. (We leave to the reader to find out the name of the targeted brand.) This kind of use of typosquatting domains is distressing. In principle the domain owners exploit someone else's reputation and properties (i.e., brand names, domains) to get financial profit without permission. It may also happen that the ad page leads the visitor to the page of a competitor of the targeted brand or company. And unfortunately, the original brand owners have limited opportunities to fight against it legally. In the US, for instance, Anticybersquatting Consumer Protection Act (ACPA) provides some armamentary, however, this is a complicated matter which is not really affordable for smaller actors. Meanwhile, the number of registered typosquatting domains is tremendous.

But actually, such parked domains are misleading for their visitors, too. Usually, they do not contain any sign to draw the attention of the visitor to the fact that he or she is probably seeing this page because he may have misspelled something. Nor do they contain any reference to the targeted page. Hence any visitor who is less aware of this kind of business can be misled and think that he is actually visiting the page he was looking for.

And unfortunately, this is not the end of the description of the risks parked pages pose. Typosquatting pages, and also other parked pages attract other forms of cybercrime, too.

2.2 Phishing and malware

Many of the potential risks introduced by parking pages are rooted in the lack of the interest of the stakeholders to fight malicious activity. This is a big business with a lot of entities involved, and everything is designed to be easy and flexible. Therefore, domain registrars are not so greatly interested in verifying their registrants; they can do well with a number of illicit registrations without a significant decline in their reputation. Parking providers are interested in attracting as many domain owners and advertisers as possible, and as long as the business pays off, their interest in checking whether an advertiser or a domain owner is malicious or benign is also limited.

Therefore, not surprisingly, parked pages attract more and more malware and they also contribute

to phishing and other illicit activities. The aforementioned Unit 42 blog on domain parking lists a number of these. For instance, there is no warranty that an "advertisement" by a malicious client of the parking provider will not redirect e.g. to a page with an exploit kit that will then fingerprint the visitor's browser and silently track his activity.

Many parked pages tend to have a malicious life cycle: as newly registered domains are frequently considered as suspicious, the miscreant parks them first: they appear as ad money collectors with a landing page for a while, also making a profit this way. Later, however, they will serve different goals: those of distributing Trojans like EMOTET or pretending to be a bank's login page from a phishing email.

Unfortunately, parking providers are also not always benign. There have been examples when the landing pages were themselves tracking user behavior and collecting private information illegally. According to Unit 42, over 30% of the parked domains turn into something which is at least suspicious later.

3. Parked domain detection and risk mitigation

While domain parking is not considered illegal at the moment, a certain part of this business is ethically questionable. As it is a largely unregulated area, many things could happen, and in the light of the above-described risks, parked pages need attention. This especially holds true for typosquatting domains.

The identification and characterization of parked domains is addressed by numerous research projects, c.f., for instance, this research of CISCO, the work of Vissers et al. (in proc. of the Network and Distributed System Security Symposium. San Diego, CA: Internet Society, 2015.) or Lai et al. World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering 11 (2017): 679-689.) to mention a few. The methods are typically based on analyzing the contents of the web pages with respect to structural features such as link to text ratio, source length, 3rd party html ratio, etc. and behaviors such as redirections, third-party requests, etc. The check of IP addresses may also be relevant.

As the number of parked domains is growing, the task of identifying them is challenging. In

addition, the unfortunate consequences of new data protection regulations on WHOIS data, the ownership of domains is very hard to investigate, and WHOIS data hold less relevant features than they used to.

A possible option to find a list of newly registered daily domains is the use of WhoisXML API's Typosquatting Data Feed. Its operation principle is to take all newly registered domains every day, and perform a clustering based on a text distance measure to find groups of domains whose name is similar to each other. As typosquatting domains especially tend to be registered in bulk, this feed captures several domains that deserve attention. Many of them are parked ones, including several typosquatting domains. In a next post we shall demonstrate how this data feed can be used efficiently for mitigating the risk introduced by parked domains.