DNSAI Best Practice 001: Identifying Malicious Registrations

This best practice is intended to provide usable, practical information for front-line compliance and abuse personnel to distinguish between domains registered for malicious purposes and compromised websites.

It requires noting that neither algorithm nor human review is perfect. The goal here is to be able to quickly and easily identify the majority of cases. There will always be exceptions and edge cases. The rest of this blog presumes that there has been a report of a domain engaged in DNS Abuse, most commonly for phishing or malware distribution.

Useful attributes are easily found in:

- The domain name and any sub-domains
- The URL aside from the domain or sub-domains
- The domain registration meta-data
- The content of the homepage, as well as at reported URLs

Frequent Malicious Registration Attributes

A domain that was maliciously registered, is more likely to have some of the below features:

- Is more likely to be new, or reported shortly after registration,
- Contains dashes in the domain name,
- Contains common brand names or misspellings of brand names in the domain or subdomain(s),
- Contains common service related words like: login, support, or account in the domain or subdomain(s), or
- Uses subdomains in a reported URL.

An example of a malicious registration can be found here: https://urlhaus.abuse.ch/url/180466/

URL:	http://cashback-paypal.com/setup.exe
URL Status:	Offline
Host:	cashback-paypal.com
Date added:	2019-04-18 14:05:07 UTC
Threat:	Malware download

In this case, a domain was registered to appear to belong to PayPal and was used to distribute malware. It uses dashes, a common brand name, and was never renewed.

Frequent Compromised Website Attributes

A domain name that was registered for a legitimate or benign purpose, but had it's website subsequently compromised will likely have some of the below features:

- Has viewable content related to the domain name,
- Has been renewed or registered for longer than 1 year,
- Has a content management system, most commonly wordpress, and often visible in the harmful url, for example: /wp-includes/, wp-content or /wp-admin/,
- If there is a brand, it is in the URL and not the domain or subdomain, or
- If there are common service related words, like login, support, or account, they are in the URL and not the domain or subdomain.

Generally, the above attributes of a compromised website indicate that someone else has control over the website, but not the domain itself.

An example of a compromised website looks like this: https://urlhaus.abuse.ch/url/1721075/

ID:	1721075
URL:	https://brightwatercondominium.ca/wp-content/upgrade/UspSTRAck.jar
URL Status:	Online
Host:	brightwatercondominium.ca
Date added:	2021-10-27 19:21:05 UTC
Threat:	Malware download

In this case, a website with wordpress was compromised and used to distribute malware. There is content on the website that relates to the domain, it was registered in 2019 and subsequently renewed, and you can see a reference to wordpress (/wp-content/) in the URL.

Lastly, none of the above attributes are definitive alone or in isolation. One must consider all of the indicators and balance the information available.

Mitigation

Mitigating abuse at the DNS level is always an act of balancing harms with the proportionality of the response and the possibility for collateral damage. For registrars and registries, the only mitigation technique available is preventing a domain name from resolving, which can have serious consequences for a website that is providing legitimate services. The below are the recommended best practices.

Mitigating Malicious Registrations

It's worth noting that maliciously registered domain names are usually in violation of registrar registration agreements, terms of service, or acceptable use policies, providing a basis for domain name suspension.

Where a domain is reasonably determined to have been maliciously registered, a registrar should:

- Suspend the domain name,
- Notify the registrant of the suspension and provide a mechanism to dispute the suspension,
- Review other domains owned by the registrant or in their account for domains with malicious registration attributes.
- Notify the web hosting provider.

Mitigating Compromised Websites

Where a domain is reasonably determined to have been compromised, in order to minimize harm to the registrant, website visitors, and risk to themselves, the registrar should:

- Notify the registrant that the domain is compromised,
- If possible, provide resources to secure the website, and
- If possible, notify the web host.

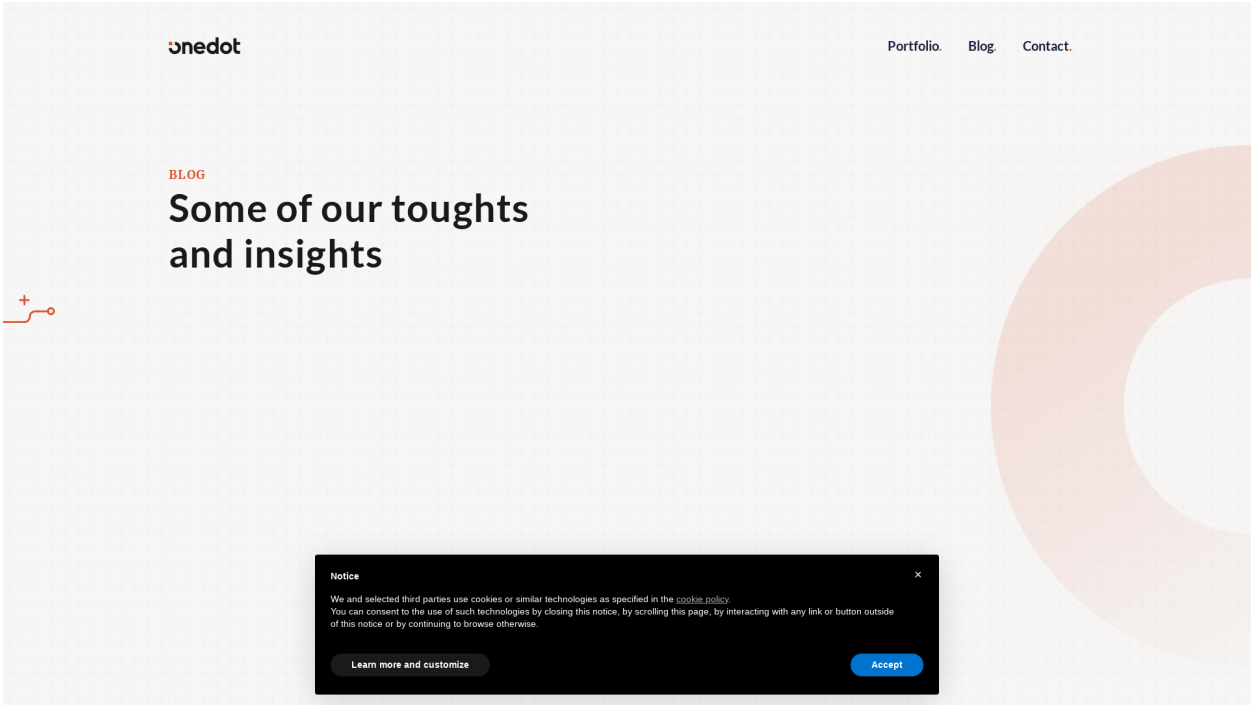
In the circumstance where the registrar determines the compromised website may cause substantial harm, or is unable to contact the registrant, it should provide the registrant with a reasonable time frame for remediation or response, typically 72 hours, and then suspend the domain.

Further Examples

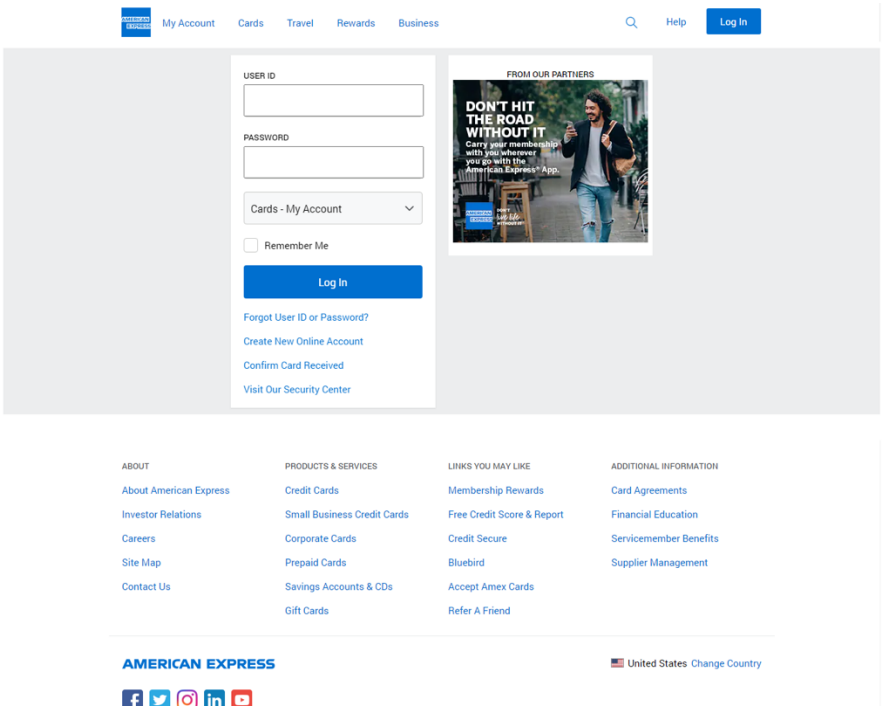
Compromised Website Example 1

Source	APWG
Submission Date	2021-10-12
URL Submitted	https://onedot.be/wp-admin/images/https/americanexpress.com.axpx-aUrlaxRX/home/?cmd=www.ssaonline-account-service.com-update_submit&id=.
Registration Date	2017-06-21

Homepage Screenshot:



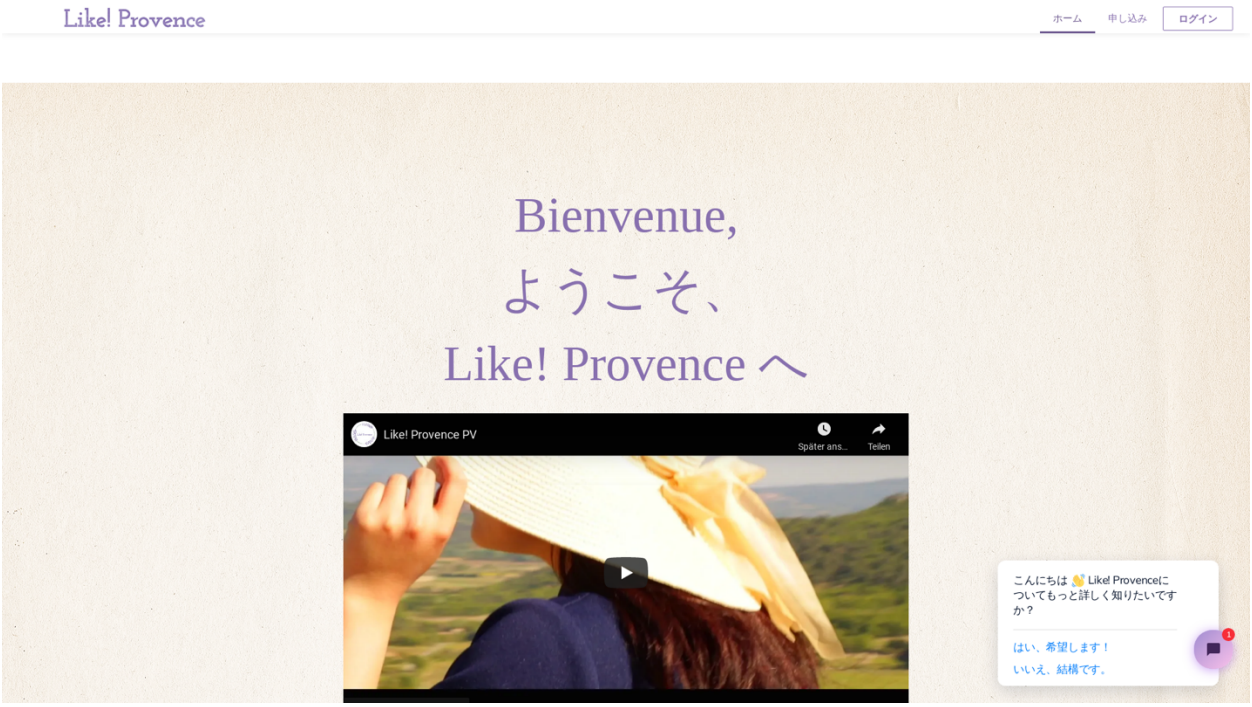
Harmful URL Screenshot:



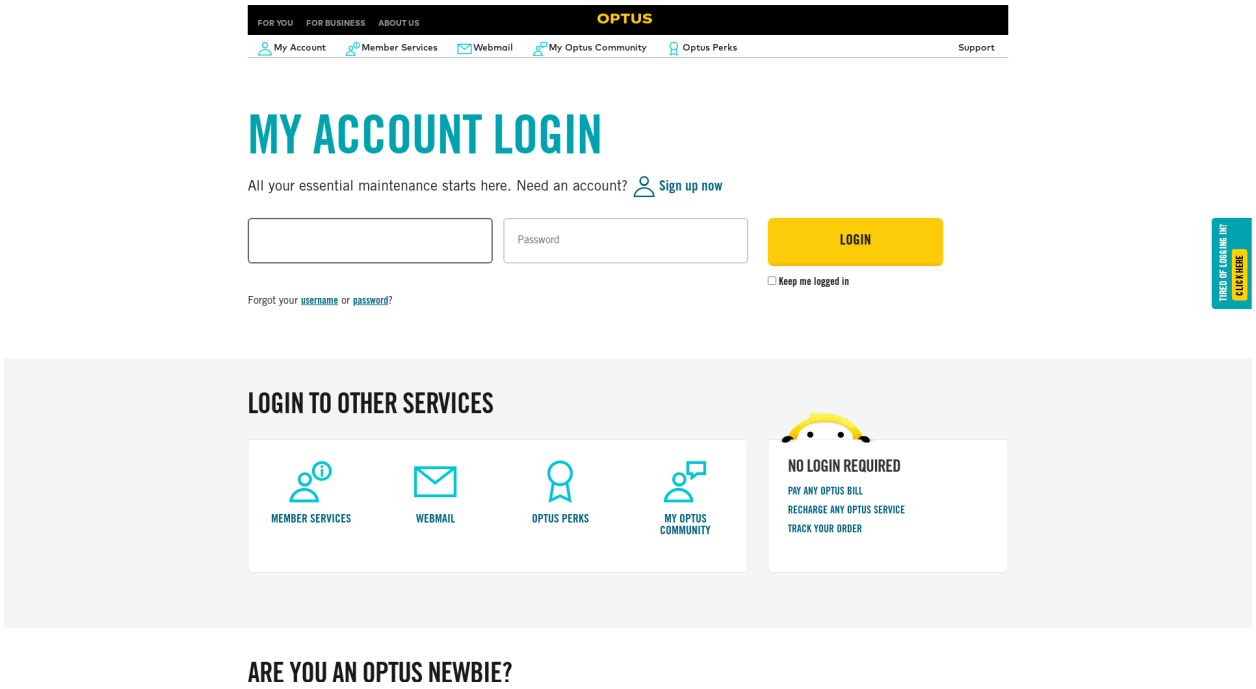
Compromised Website Example 2

Source	PHISHTANK
Submission Date	2021-09-30
URL Submitted	https://likeprovence.fr/wp-includes/theme-compat/index.php
Registration Date	2020-04-03

Homepage Screenshot:



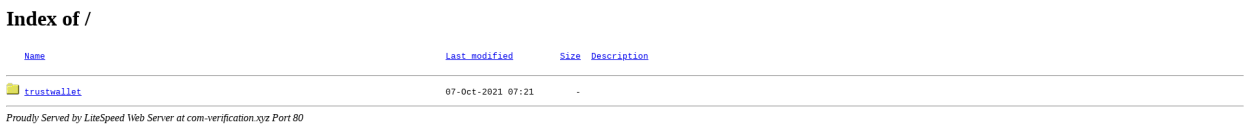
Harmful URL Screenshot:



Malicious Domain Example 1

Source	APWG
Submission Date	2021-10-07
URL Submitted	hXXp://trustwallet.com-verification.xyz
Registration Date	2021-10-06

Homepage Screenshot:

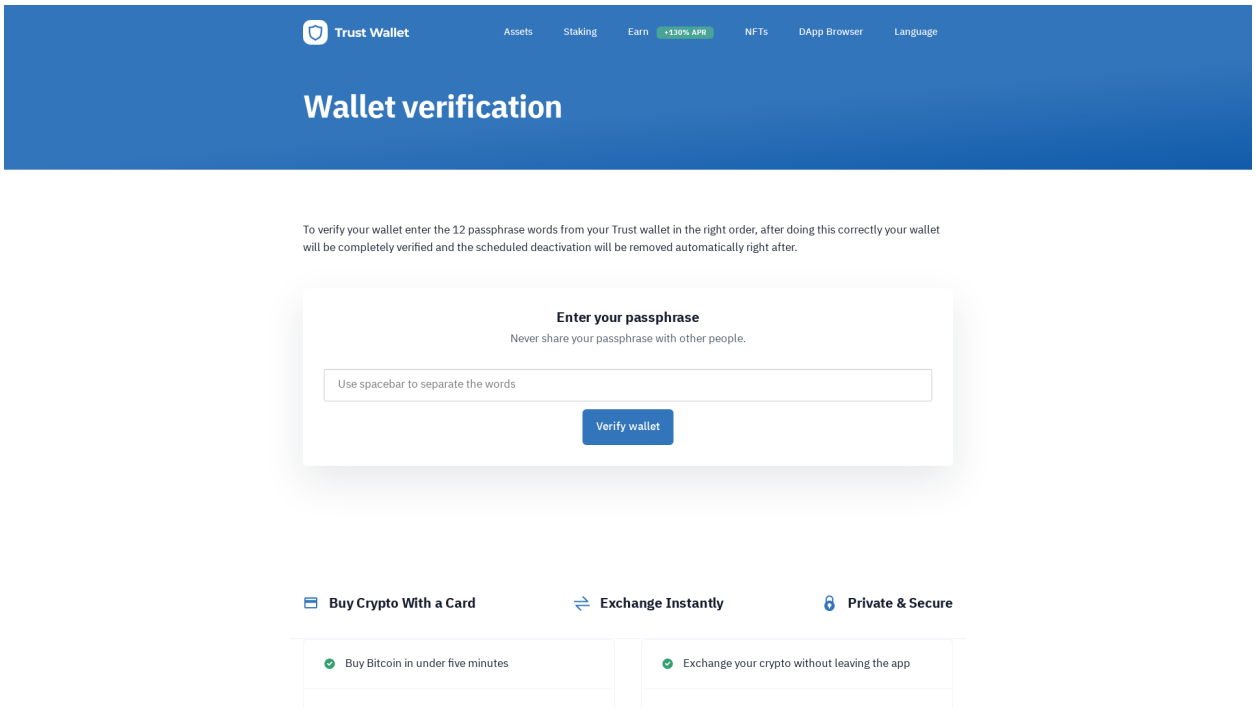


Index of /

Name	Last modified	Size	Description
trustwallet	07-Oct-2021 07:21	-	

Proudly Served by LiteSpeed Web Server at com-verification.xyz Port 80

Harmful URL Screenshot:



Malicious Domain Example 2

Source	APWG
Submission Date	2021-11-01
URL Submitted	hXXp://online-standardbank-za.com/login.php
Registration Date	2021-11-01

Homepage and harmful URL Screenshot: