DNS Threat Hunting amid Data Redaction

Since the European Union's General Data Protection Regulation (GDPR) took effect in 2018, more countries have passed similar laws. For instance, in the U.S., the California Consumer Privacy Act (CCPA) came into effect in January 2020. These and other data privacy laws have impacted how domain registries and registrars publish WHOIS registration details.

Since the implementation of these regulations, masking WHOIS records has become a norm in various circumstances. Even domain registrants that aren't covered by any data privacy law employ proxy or privacy services, bringing new levels of anonymity on the Internet.

While data redaction may have helped assuage legitimate privacy concerns, it is also prone to abuse. Criminal digital infrastructures are being built anonymously—hiding behind the premise of privacy protection—making them harder than ever to track and unmask.

Being at the forefront of global Domain Name System (DNS) data, we identified threat hunting tactics in this guide that can help uncover clues and track the footprints of malicious actors and resources even if they redact their WHOIS information, namely:

- Checking the domain age
- Looking through historical WHOIS records
- Probing bulk-registered and similarly-looking domains
- Checking the website content of suspicious cyber resources
- Pinpointing unjustifiable privacy redaction
- Inspecting DNS connections
- Determining associations with less reputable infrastructure providers

Data Redaction-Friendly Threat Hunting Techniques

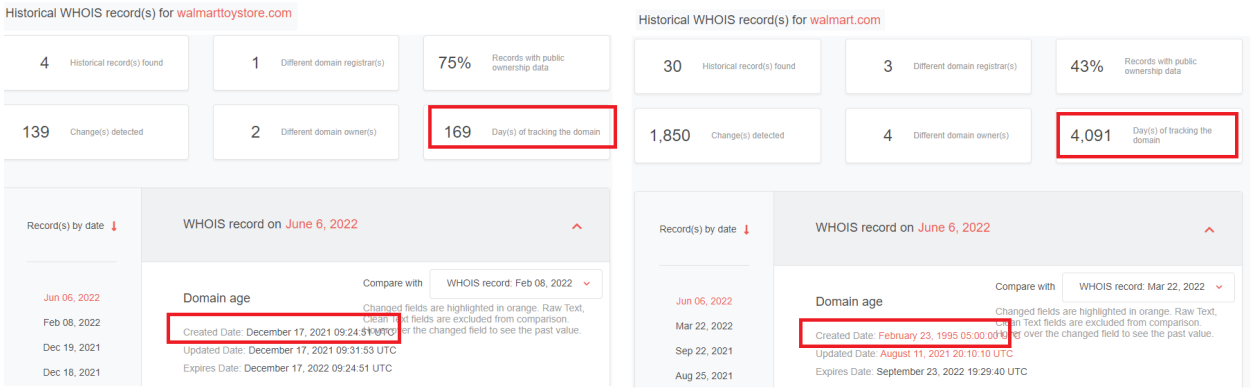
Data privacy laws may be stifling threat hunting efforts, but there are applicable techniques that have adapted to data redaction. We talked about seven of them in the following sections.

1. Check the Domain Age

Most cybersecurity policies generally block newly registered domains (NRDs) since threat actors have been known to use them often. However, recent cyber attacks, such as the SolarWinds hack, have brought to light that malicious actors are increasingly using older domains.

As such, threat hunting techniques can be updated to screen domain age not only for NRD blocking but also threat enrichment. Here's an example.

The age of cybersquatting domains can be a sign of illegitimacy. For instance, walmarttoystore[.]com appears valid and believable to several parents. The domain was created on 17 December 2021, so most security tools won't see it as an NRD anymore, strictly speaking.



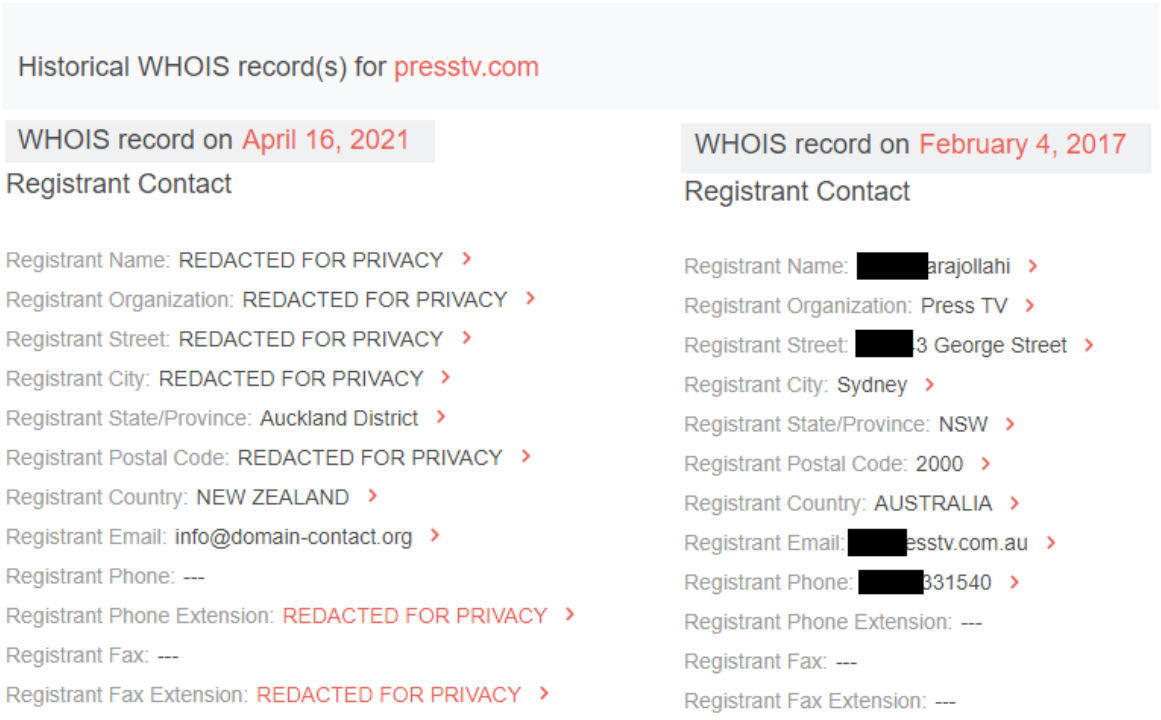
But if threat hunting techniques account for the domain's age, walmarttoystore[.]com would raise a red flag as it's too new compared to the official Walmart domain, which was created way back on 23 February 1995. As such, domain age can provide more context and accuracy to threat hunting results.

2. Look into the Past through WHOIS History

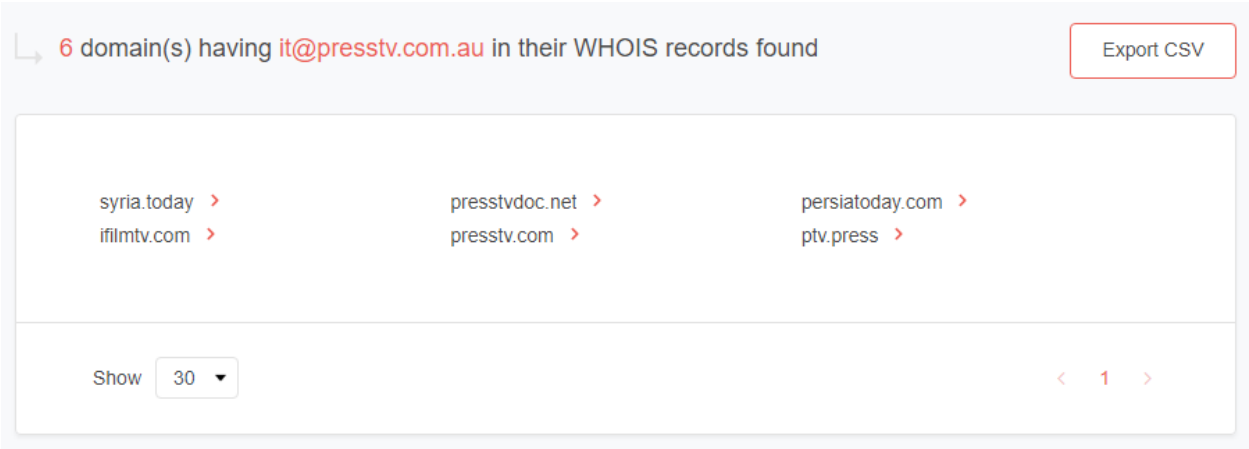
While it's true that data privacy laws and WHOIS privacy protection services make domain attribution difficult, historical WHOIS details may help shed some light on the actors behind suspicious or malicious properties.

Keeping in mind that data redaction only went large-scale in 2018, the WHOIS information of many domains before then remains publicly available. WHOIS history lookup services allow us to access these records.

Take a look at the WHOIS history of presstv[.]com, one of the misinformation domains seized by the U.S. Department of Justice (DOJ) last year. Its recent WHOIS records are all redacted. However, actionable threat data can be gleaned from its 2017 WHOIS details.



Pivoting off these historical records, particularly the registrant's email address, can help unveil a suspicious network of domains.

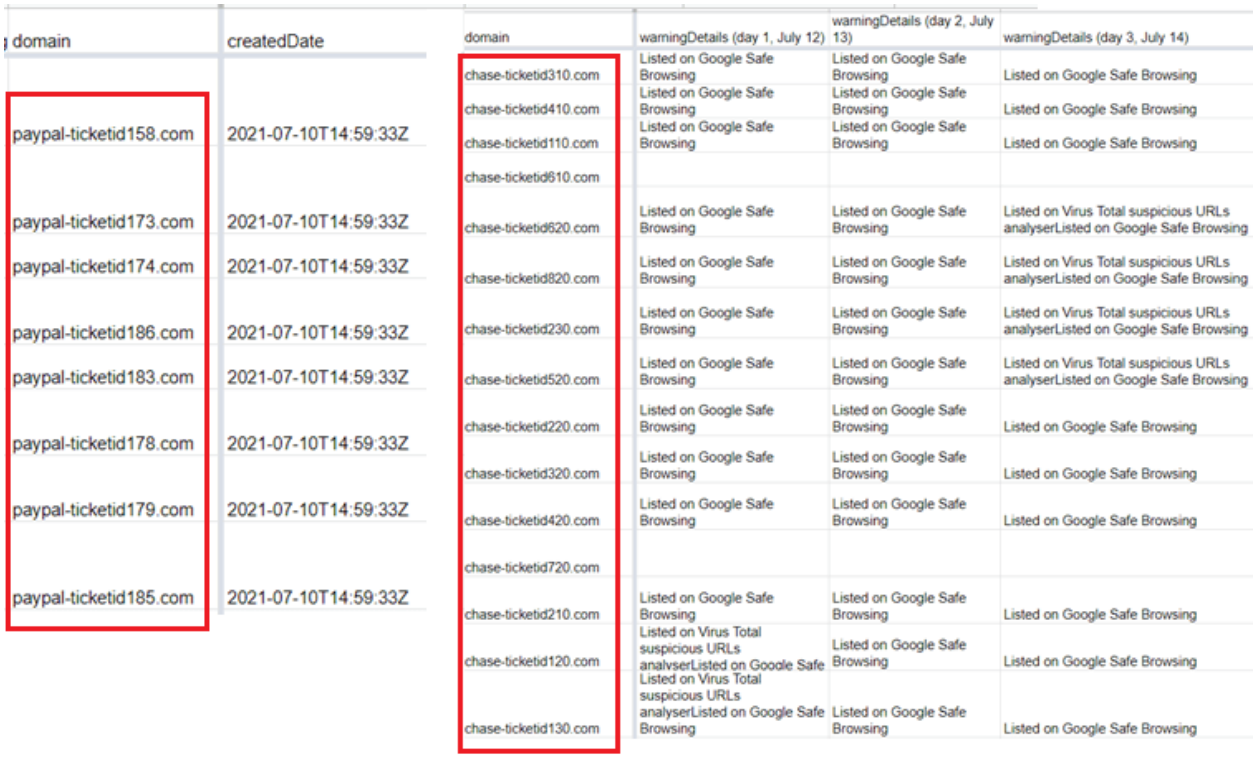


3. Probe Bulk-registered and Similarly-looking Domain Names

Domain bulk registration has made it easy to register hundreds or thousands of domains in one go. This capability offered by registrars is a massive help to companies and domain name investors with large domain portfolios. But malicious actors also take advantage of the same feature, as they bulk-register hundreds of domains at a time and gradually weaponize them.

In fact, a study involving 2,400 typosquatting groups revealed that threat actors register several domains and progressively activate them in malicious campaigns. Each group consisted of look-alike domains registered on the same day. While bulk registration of malicious properties may sound ingenious and challenging to counter, we can make it work for our threat hunting efforts. How?

Checking domain groups for recurring strings can help uncover more suspicious footprints. Below are two groups with domains containing the string “ticketid.” Several domains on the “chase-ticketid” group on the right have been flagged as malicious.



domain	createdDate
paypal-ticketid158.com	2021-07-10T14:59:33Z
paypal-ticketid173.com	2021-07-10T14:59:33Z
paypal-ticketid174.com	2021-07-10T14:59:33Z
paypal-ticketid186.com	2021-07-10T14:59:33Z
paypal-ticketid183.com	2021-07-10T14:59:33Z
paypal-ticketid178.com	2021-07-10T14:59:33Z
paypal-ticketid179.com	2021-07-10T14:59:33Z
paypal-ticketid185.com	2021-07-10T14:59:33Z

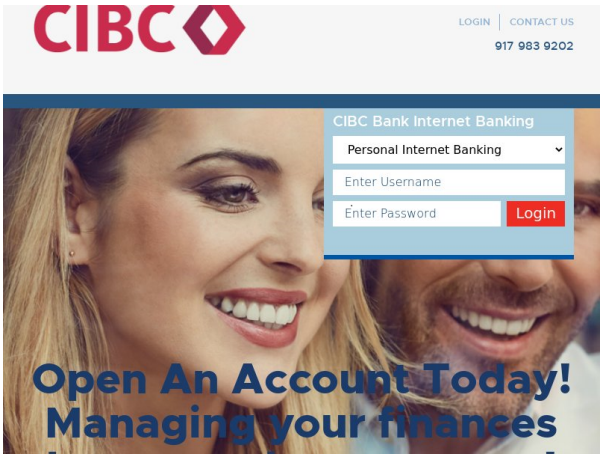
domain	warningDetails (day 1, July 12)	warningDetails (day 2, July 13)	warningDetails (day 3, July 14)
chase-ticketid310.com	Listed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Google Safe Browsing
chase-ticketid410.com	Listed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Google Safe Browsing
chase-ticketid110.com	Listed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Google Safe Browsing
chase-ticketid610.com			
chase-ticketid620.com	Listed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Virus Total suspicious URLs analyserListed on Google Safe Browsing
chase-ticketid820.com	Listed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Virus Total suspicious URLs analyserListed on Google Safe Browsing
chase-ticketid230.com	Listed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Virus Total suspicious URLs analyserListed on Google Safe Browsing
chase-ticketid520.com	Listed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Virus Total suspicious URLs analyserListed on Google Safe Browsing
chase-ticketid220.com	Listed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Google Safe Browsing
chase-ticketid320.com	Listed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Google Safe Browsing
chase-ticketid420.com	Listed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Google Safe Browsing
chase-ticketid720.com			
chase-ticketid210.com	Listed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Google Safe Browsing
chase-ticketid120.com	Listed on Virus Total suspicious URLs analyserListed on Google Safe	Listed on Google Safe Browsing	Listed on Google Safe Browsing
chase-ticketid130.com	Listed on Virus Total suspicious URLs analyserListed on Google Safe Browsing	Listed on Google Safe Browsing	Listed on Google Safe Browsing

We can find more suspicious domains bearing the exact text string but targeting other companies.

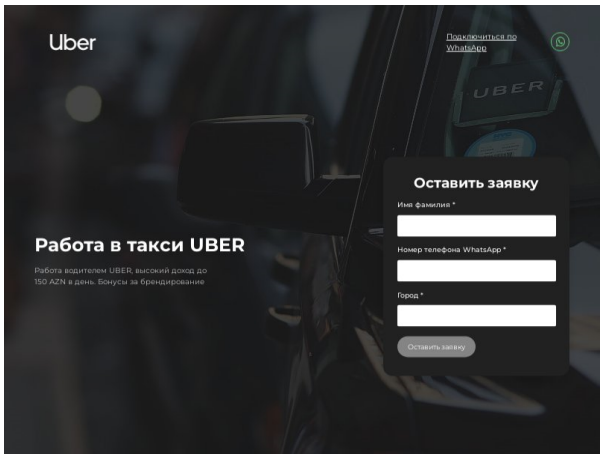
4. Verify the Website Content of Suspicious Properties

Over the course of threat hunting efforts, several suspicious properties would be unveiled. Some of these domains may be fronts for misinformation, credential theft, counterfeiting, and other crimes. Checking their content can help distinguish actively dangerous domains from those that are dormant.

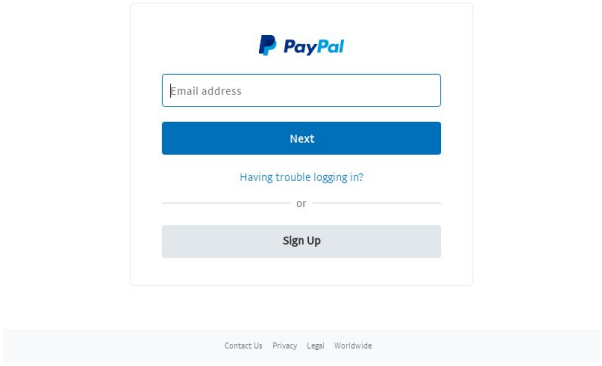
Below are some examples of cybersquatting domains hosting suspicious content. Including website analysis can add more value when assigning or assessing the risk scores of suspicious properties.



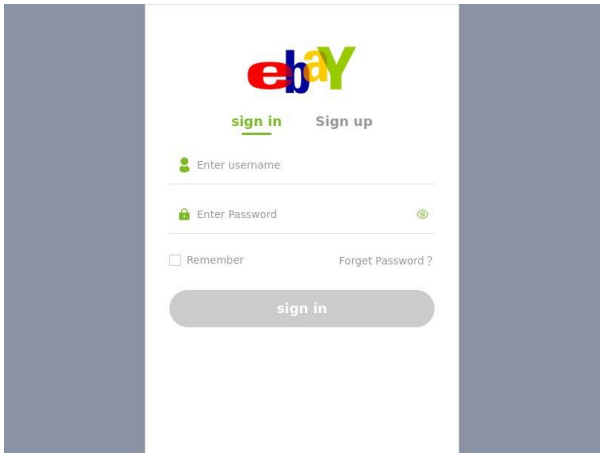
Screenshot of cibchw[.]com



Screenshot of uber-az[.]site



Screenshot of bettina-ebay[.]de

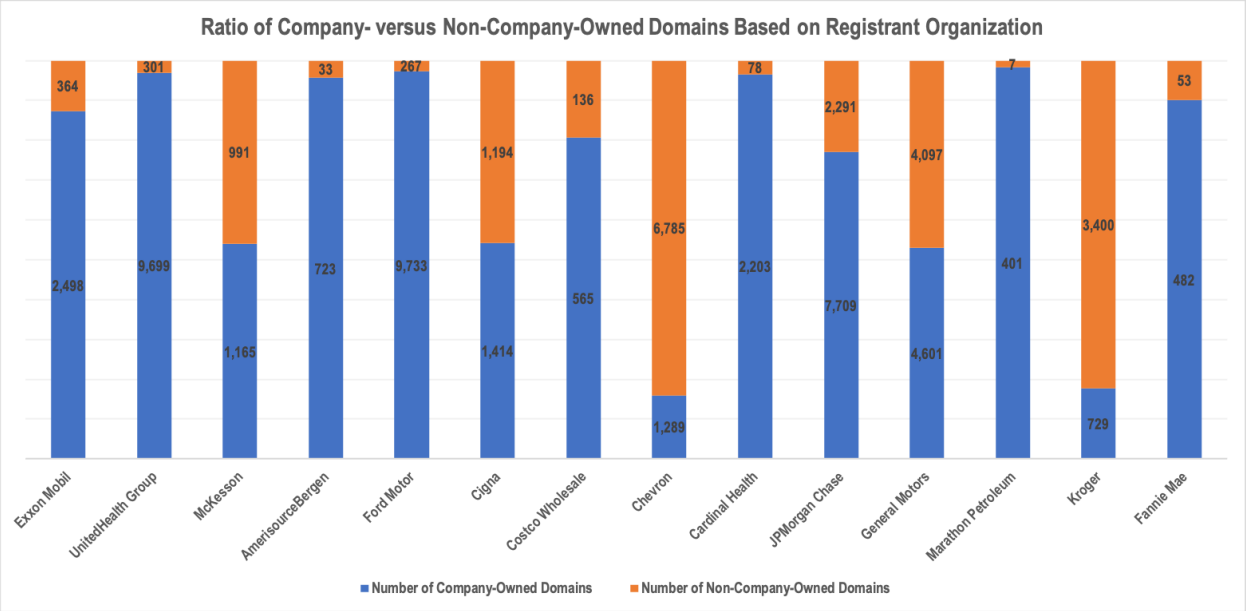


Screenshot of ebay-h9[.]com

5. Pinpoint Unjustifiable Privacy Redaction

Several large corporations, including those in the Fortune 500 and those commonly impersonated, choose to keep their WHOIS records public. As such, cybersquatting domains targeting these companies become even more suspicious when their WHOIS records are redacted.

The chart below shows the attribution of more than 63,000 domains containing the names of 14 Fortune 500 companies. About 34% of these domains can’t be attributed to the target organizations, which already makes them look dubious.



Source: CircleID

6. Inspect DNS Connections for Anomalies

Another characteristic of large companies is that they seldom use shared hosting infrastructure. Financial institutions, for instance, may use a hybrid cloud approach, but critical data and processes are most likely hosted on private servers for better security and control. As such, it may be prudent to keep an eye on look-alike domains that resolve to shared IP addresses.

Take, for instance, the DNS A records of chase[.]com and its malicious cybersquatting domain, chasebankw[.]com. The legitimate domain resolves to a dedicated IP address, while the malicious one connects to an IP shared among hundreds of other domains.

The same is true for other DNS elements, such as nameservers and mail servers. If you see legitimate-looking domains imitating major brands during threat hunting, checking their DNS connections can help weed out suspicious properties.

7. Determine Associations with Less Reputable Domain Infrastructure Providers

While some threat groups have huge budgets for building their infrastructures, other malicious go for cheap or even free providers. The table below shows some free top-level domains (TLDs) and their badness index based on Spamhaus, alongside more reputable TLDs.

Free TLDs	Badness Index	TLDs	Badness Index
.cf	2.46	.biz	.68
.ga	2.41	.com	.58
.gq	2.80	.net	.37
.ml	2.56	.org	.12
.tk	1.77	.uk	.20

As you can see, the free TLDs have higher badness indices compared with the major TLDs. This means these TLDs have a high percentage of malicious domains on their roster.

Of course, TLDs are not sole indicators of a domain's potential to become malicious. You may also take into account the entities behind the domains—hosting companies, registrars, and other infrastructure providers that are seemingly bulletproof.

—

Threat hunting techniques must continue to evolve and adapt to security community changes, including the global phenomenon of data redaction. A comprehensive view of the world's DNS can significantly improve the accuracy and depth of threat hunting efforts at a time when ownership attribution has become difficult due to the implementation of data privacy laws.

Are you interested in applying any of the threat hunting techniques we discussed above? Contact us for more details about how our DNS intelligence can enrich your cyber ecosystem.