Expired Domain Dumpster Diving

GIAC (GSEC) Gold Certification

Author: Christopher DeWeese, cndeweese@gmail.com
Advisor: *Russell Eubanks*

Accepted: *August 8, 2021*

Abstract

Every day 200,000 domains expire ("DomCop FAQ," n.d.), become available for purchase and possible exploitation by the new owner. These expired domains pose a risk to companies and individuals, leading to compromised accounts and resources that remain associated with those domains. Expired domains can be purchased, and services re-established to capture all data previously directed to the domain allowing for Domain Dumpster Diving. Five expired domains were selected and monitored for six weeks. The resultant data confirms that the data captured could be used to access accounts and resources related to the domain's previous owner. This research focuses on selecting candidate domains, an overview of data collected, and recommendations for defensive strategies for Domain Dumpster Diving.

1. Introduction

Domain names provide the ability to navigate the Internet easily. In some cases, domains are so well known that they are often in conversation as verbs. What most Internet users may not realize is that there are "200,000+ domains expiring daily" ("DomCop FAQ," n.d.). These expired domains become available for registration by new owners. Expired domains usually are valued based on the domain history and reputation. The use cases that come with expired domains include boosting Search Engine Optimization (SEO) (Prajjwal, 2021), domain squatting, domain takeover (Beynon, 2020), and Domain Dumpster Diving (SCHULTZ, 2021). Figure 1 covers the lifecycle of a domain name.

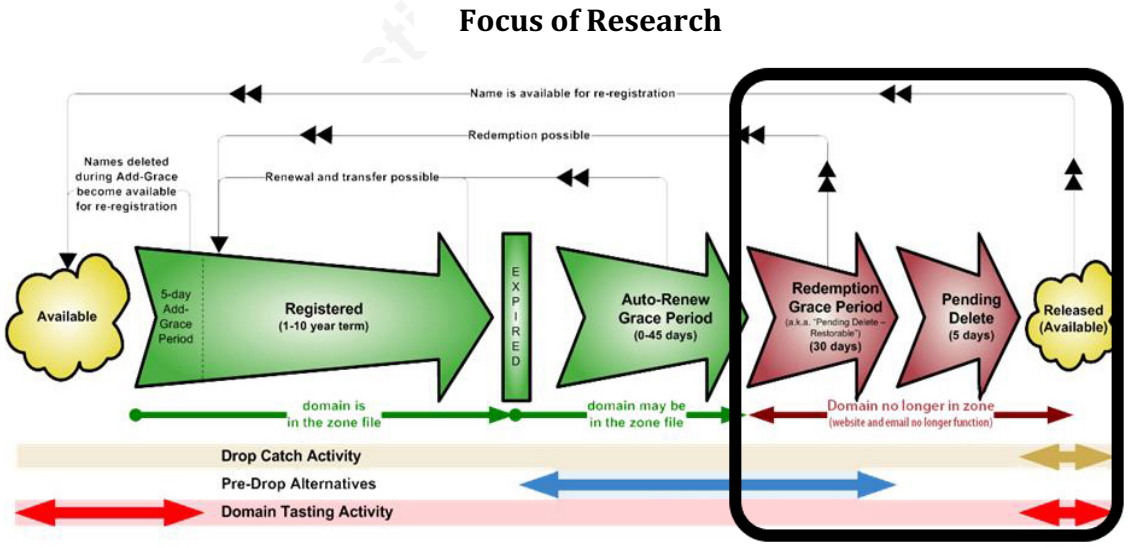


Figure 1: Lifecycle of a Domain Name

Following domain expiration, the domain is made available for re-registration. At this point, offensive strategies for Domain Dumpster Diving exist.

The offensive use of expired domains is not a new concept; expired domains that boost search engine optimization (SEO) for websites and exploits by security researchers and criminal activity groups are well documented. The domain WeLeakInfo.com provided breach data to 24,000 paid subscribers. Following a government takedown of

the site, a secondary domain was discovered and resulted in the leaking subscriber data as detailed in this report:

> The government shutdown WeLeakInfo.com as part of a government seizure in January 2020, but the seizure missed a secondary domain tied to this website. On March 12, 2020, someone acquired the secondary domain and then used the control of this domain to control the seized domain's payment processing service. Acquired data was leaked to the Internet, exposing the registration data of the 24,000 users who had subscribed to the WeLeakInfo.com site (Krebs, 2021).

In August 2013, security researchers in Australia gained control of six domain names previously registered to law firms following several firms that shutdown or completed mergers with other firms. After three months of research with these domains, the researchers captured approximately 25,000 emails in total, recovered the actual passwords (previously exposed in public data breaches), and successfully attempted password recovery of many popular online services and profession-specific portals (Szathmari, 2019).

Currently, there is no process to retire a domain name permanently. The most general guidance to secure a domain suggests maintaining ownership of a domain which requires paying a registrar for the domain indefinitely. Domain owners must assess the risk of abandoning a domain versus the cost of continued ownership of the domain. Consider the security impact of losing control of a domain—a domain name belonging to a business, person, or organization links to their identity and brand. The loss of control of a domain results in the immediate loss of the associated website, email, and history and could damage reputation.

A domain loss compromises the related emails tied to the domain. Defensive measures provide the ability to ensure those emails are protected. Once a domain owner chooses to release a domain back to the open market, they must be positive they have taken the appropriate actions to prevent abuse once the domain becomes available. To understand the risk, development of a domain selection process was created to select

domains for Domain Dumpster Diving. The potential offensive and defensive strategies related to using these expired domains were explored and validated.

2. Domain Selection Criteria

Before selecting expired domain names to use for Domain Dumpster Diving, the development of the selection criteria required research on the available domain attributes to use. This research uses only the .com Top-Level Domains (TLD) for the selection of the candidate domains. The .com TLD provides a standard domain TLD commonly known, trusted, and used for commercial purposes.

Several domain attributes provide the details needed to create the domain selection process. These attributes are:

- Cost
- Internet Archive Data
- Search Engine Optimization Data
- Backlinks
- Related TLDs
- DNS Historical Records

2.1. Cost

The cost of domain names varies for each of the TLDs. A one-year .com domain registration cost is less than $15 for 12 months of control (Monaghan, 2021). This pricing varies based on the registrar used and the additional services the registrar offers with the registration. More popular domains are available for auction or purchase from the current domain owner. These popular domains often sell for thousands of dollars. There is also the option of purchasing domains from drop catch services. These services grab expired domains before becoming available on the open market and sell them as their business model. Drop catch domains are often parked for a period rather than let go for purchase at cost. In this research project, domains outside the standard pricing model

were not considered. Domains for sale or auction may yield more data for Domain Dumpster Diving and may warrant further research.

2.2. Internet Archive Data

The Internet Archive Wayback Machine provides captures of the websites over time (Wayback Machine, n.d.). The website captures provide valuable information showing how the website existed in the past. The Wayback Machine data includes a histogram showing the number of website captures and the links to view the captured data. Using the capture data, one can view the website as it existed on the date of capture. Website capture data is beneficial for understanding how the domain name was used in the past. It indicates both the previous use of the domain name and if the domain previously links to any malicious activity. The Wayback Machine API provides some data that provides data for doing research, but viewing the data is required to gather the most context out of the data.

As seen from Figure 2, this website existed for at least November 22nd, 1999, and the most recent capture was January 27, 2021. The data also reveals website captures from about 2003 to 2007. When digging deeper into the data on the histogram, we learn that the most recent time the website was active was in 2019.

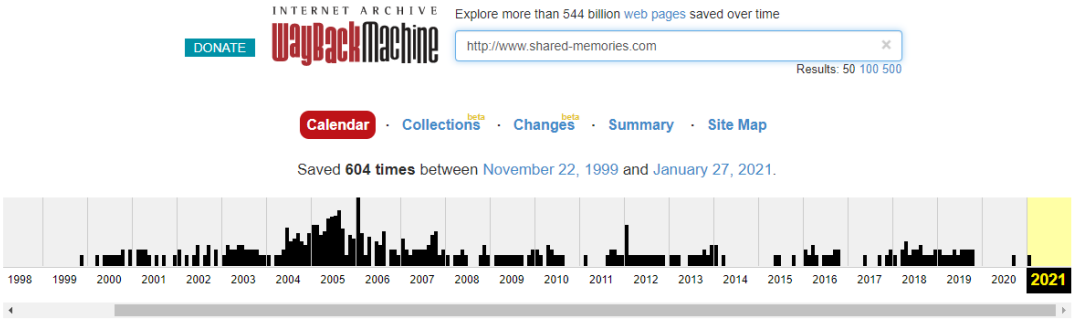


Figure 2: Histogram of Website Captures

The capture data in Figure 3 helps understand the historical website data, including approximately the last time the domain was active and if the site was also using the domain for email.

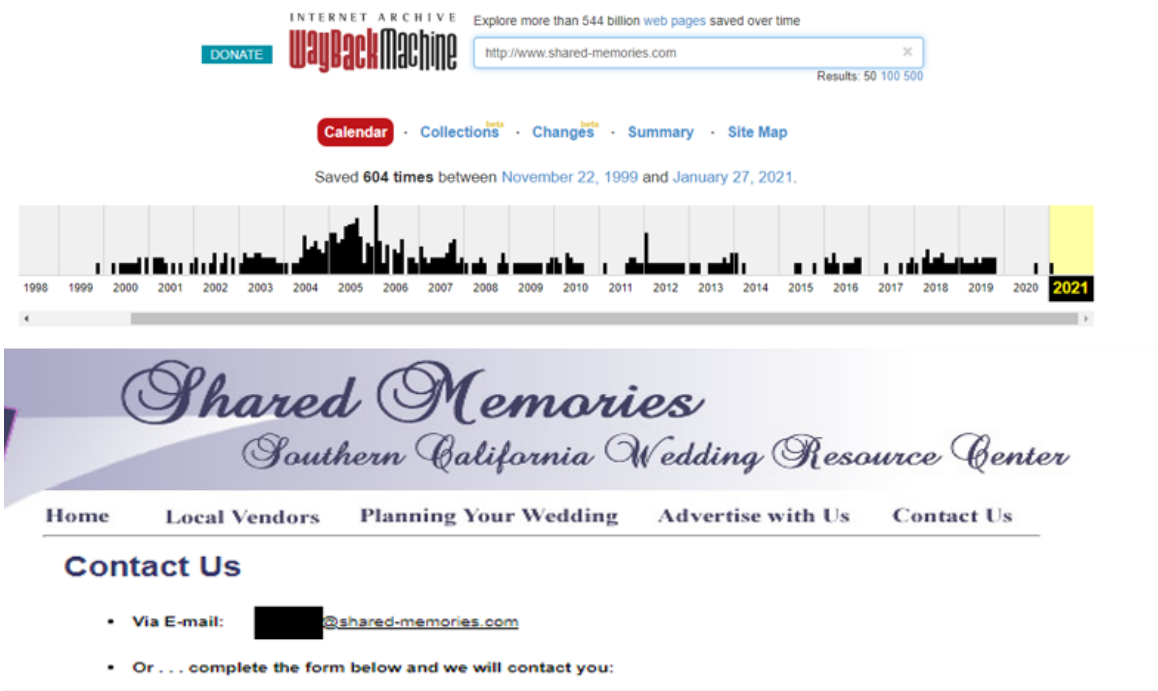


Figure 3: Example Website Capture

2.3. Search Engine Optimization (SEO)

Search Engine Optimization (SEO) is a method to configure a website to rank highly in a search engine using relevant search terms. SEO scoring provides a numerical value to a domain name based on known settings to increase the SEO ranking. The rankings from Alexa, Majestic, and DMOZ provided the details needed to evaluate the domains for selection.

2.4. Backlinks

Backlinks provide a numerical count of sites linking to the domain name and some insight into the previous use of the domain. A high number of backlinks indicates that the domain was previously popular, but it could also indicate that the domain used the links to boost SEO traffic to the site. A low number of backlinks indicates the website did not score highly for SEO and website traffic.

2.5. Related TLDs

Related TLDs provide information on how the domain name has operated in the past. Alternate TLDs can provide details and opportunities for sites that use the .net TLD, and

then the .com becomes available. They also pose a risk for cybersquatters who establish new domains on alternate TLDs to trick users into visiting the incorrect site.

2.6. DNS Historical Records

The Domain Name System (DNS) is the system used to manage the domain names. Historical DNS records provide data to understand the usage of the domain before the domain selection process. DNS history reveals if a mail exchange (MX) record existed previously, indicating that the domain supported email historically. The historical DNS records also reveal how the domain owner used the domain and what services existed. The services data include the website hosts used and the frequency with which the domain was updated. During the initial research of this project, there were no free sources of DNS history discovered that provided the desired information[1].

3. Domain Selection Process

The selection criteria provide the necessary information to begin the review and selection of candidate domains. The selection criteria are critical to reducing the search space by eliminating domains that would not support the Domain Dumpster Diving techniques.

3.1. Initial Review of Expired Domains

With 200,000 domains expiring daily, finding a source of data that provided most of the information required to conduct this research was necessary. ExpiredDomains.net provides a list of expired domains that is updated daily. This creation of an account allows the user to use filters on the domains and create a watchlist of domains while completing research.

[1] Following domain selection, a reliable free DNS history source is available, and the use of this resource will follow in the summary and recommendations for further research section.

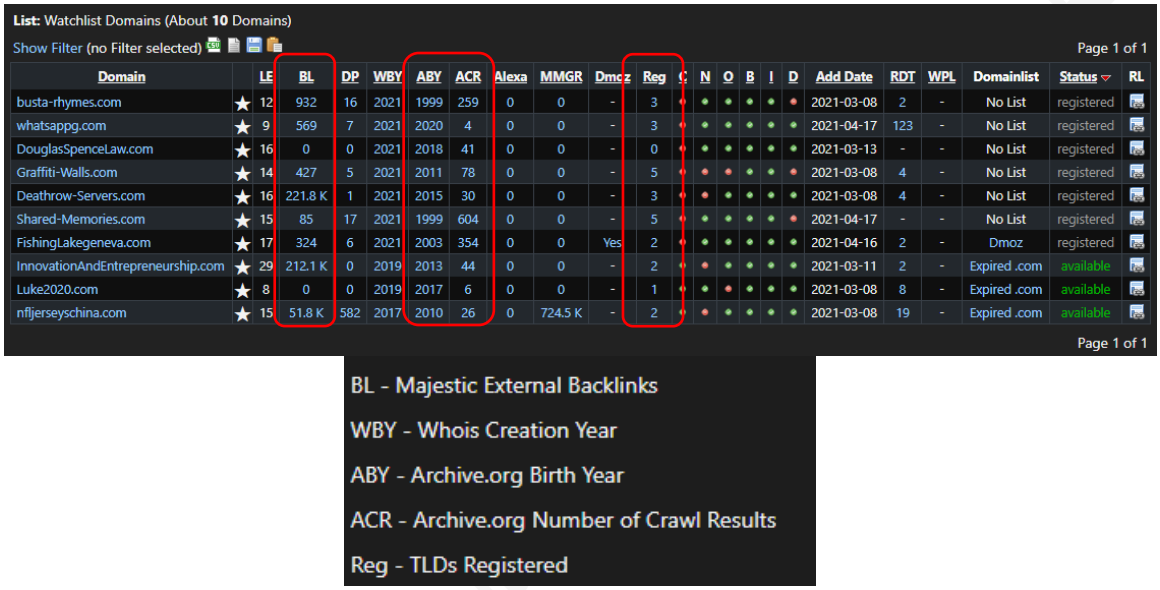


Figure 5: Personal Domain Watchlist for ExpiredDomains.net

Figure 5 displays the domains considered for this project following an initial screening of domains. The ExpiredDomains.net data provides three of the six desired criteria for this research. The data provides the details to complete the initial domain review and generate a watchlist of domains.

3.2. Selection Process Flow Chart

Analysts can use the domain watchlist to research the domains at archive.org. Archive.org provides the historical details needed to evaluate the domain. The SEO rankings were then evaluated, and the number of backlinks was recorded if data were available. The next piece of data reviewed was the existence of alternate top-level domains. If top-level domains did exist, research focused on the archive.org data to understand if a website existed before the domain became available. This research was manual since the API for archive.org did not provide the capability to pull back website images. Upon verifying previous website results, the historical site pages were evaluated to understand if the domain supported email. If all selection criteria match, the domain moves forward for further open-source research to determine if it is suitable for selection as part of the project. Figure 4 covers the process used to select domains.

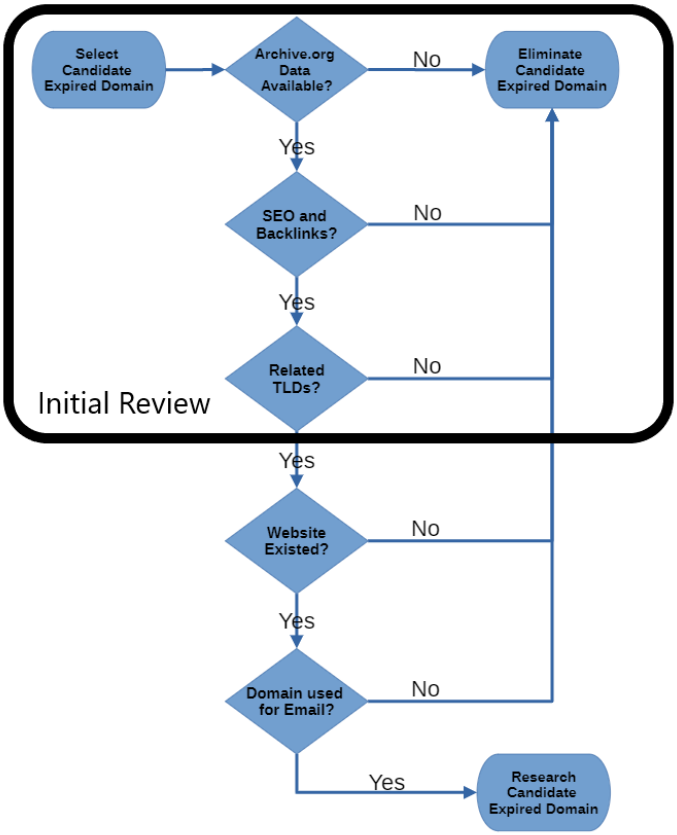


Figure 4: High-level process developed to review expired domains

The initial review section uses the ExpiredDomains.net site. Following this review, the Internet Archive and Google provides the data to complete open-source research for the candidate domains.

3.3. Final Selection Process

Open-source research supported the selection of five domains purchased using the selection criteria developed in this project. Figure 6 lists the domains selected for this project.

Domain #1	DouglasSpenceLaw.com
Domain #2	Graffiti-Walls.com
Domain #3	Shared-Memories.com
Domain #4	Deathrow-Servers.com
Domain #5	FishingLakeGeneva.com

Figure 6: Personal Domain Watchlist for ExpiredDomains.net

The selection of the domain was the result of following the process documented in the Figure 4 flowchart. Appendix A provides further details on the five domains selected during this scoring process.

4. Domain Data Collection

The collection of email data covered six weeks using the methods detailed in the following sections.

4.1. Have I Been Pwned Email Data

After establishing control of the domains, the Have I Been Pwned (HIBP) website provided the ability to determine if any email addresses from the acquired domains existed in any breach data. ("Have I been Pwned: Domain search," n.d.) Following the well-documented process from the HIBP website provides the data in Figure 7 for the domains selected.

Email	Breach
[redacted]@shared-memories.com	Verifications.io
[redacted]@shared-memories.com	Adobe
[redacted]@shared-memories.com	Adobe
[redacted]@shared-memories.com	Apollo, B2B USA Businesses, Exactis
[redacted]@shared-memories.com	B2B USA Businesses

Email	Breach
[redacted]@fishinglakegeneva.com	Apollo, B2B USA Businesses, Exactis, Verifications.io
[redacted]@fishinglakegeneva.com	Data Enrichment Exposure From PDL Customer, Verifications.io
[redacted]@fishinglakegeneva.com	B2B USA Businesses

Figure 7: Results of HIBP Domain Search

The results reveal that two of the five domains have emails found in data breaches collected by the HIBP sources.

4.2. Catch-all Email Collection

After purchasing domains, MX record updates completed the routing to capture all emails sent to the domain. A catch-all inbox for each domain allowed capturing and monitoring all emails sent to the domain. Despite these domains having up to

30 days of inactivity, four of the five domains received emails in the first week, and all five domains received emails by the end of the second week. Figure 8 details the frequency of emails received by the week.

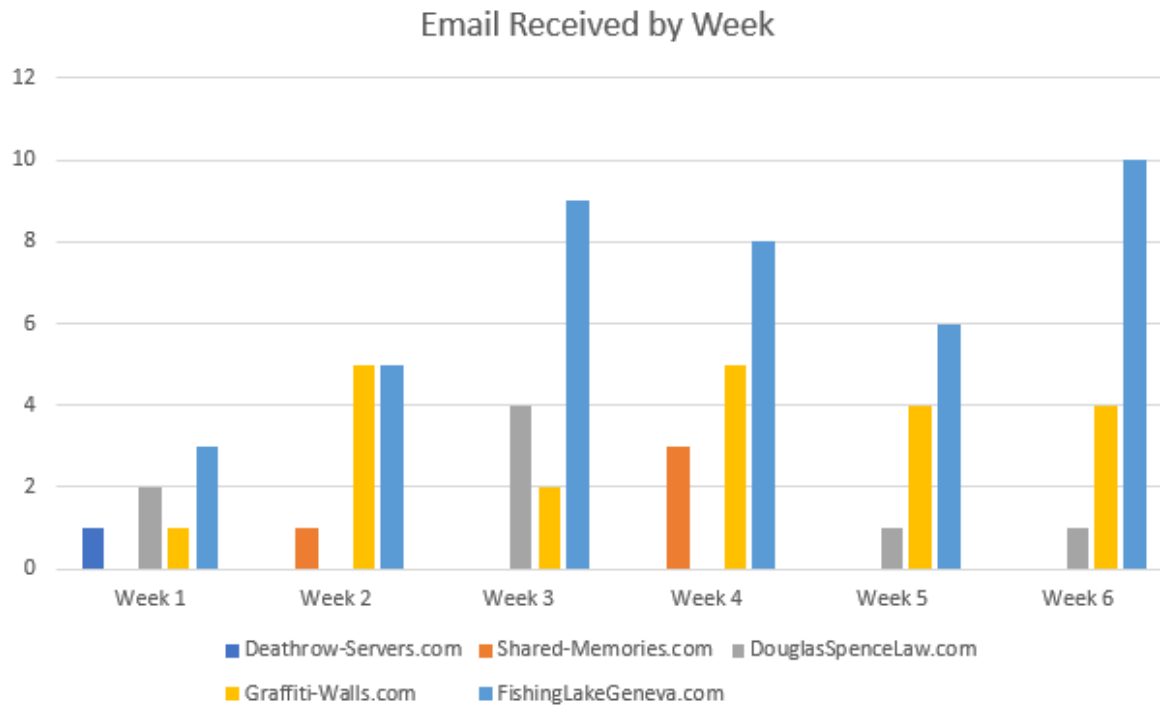


Figure 8: Number of Emails by Domain Per Week

Any email received during these six weeks was included in the data set. During the six weeks of data collection, no specific actions increased or decreased the volume of emails sent to the domains.

5. Analysis

5.1. Domain #1 - DouglasSpenceLaw.com

This domain served as a control domain given that it did not have any backlinks and limited history tied to it. The domain yielded interesting open-source details during the research phase, but the domain had no backlinks and limited web history. This domain name was tied to the law firm and did not yield any valuable data.

5.2. Domain #2 - Graffiti-Walls.com

All emails captured for this domain during the collection period were evaluated to be SPAM. All the SPAM emails target the info[at]graffiti-walls.com and support[at]graffiti-walls.com email addresses suggesting the spammers are generically targeting the domain over targeting a specific user.

5.3. Domain #3 - Shared-Memories.com

All emails captured for this domain during the collection period were evaluated to be SPAM. It is interesting to note that this domain exists in the HIBP breach data. However, no actionable emails we received to the email address from the breach data during the data collection period.

5.4. Domain #4 - Deathrow-Servers.com

This domain received precisely one email, and it was unique that the email received appears to be tied to an administrative Google Workspace account. Further investigation into the email did not confirm if the email still has access to this account. This domain has the highest total backlinks but provided minimal results. The low number of emails suggests other top-level domains were listed and potentially used for general purposes and that this email for this domain exists exclusively for administrative use.

5.5. Domain #5 - FishingLakeGeneva.com

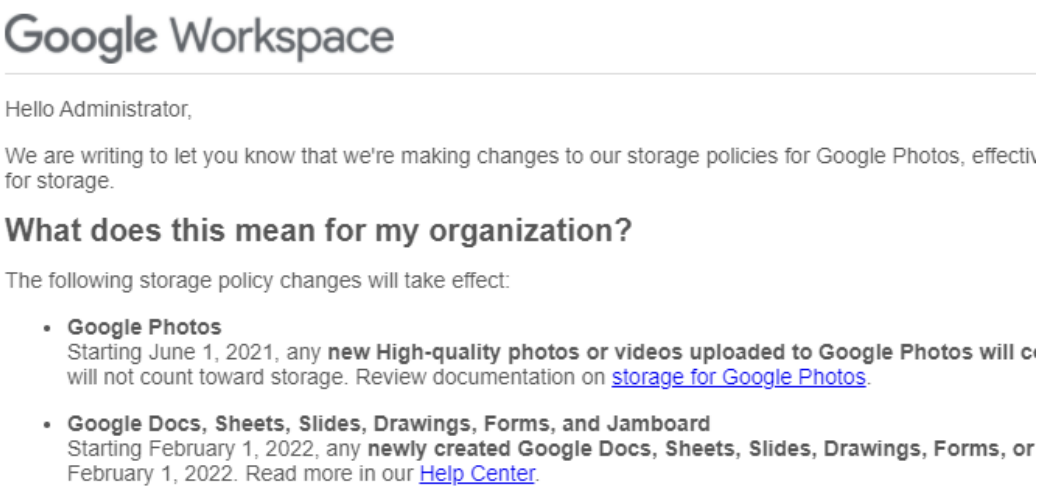
This domain belongs to a recently closed fishing business in Wisconsin. The data collection for this domain data results in potential access to a LinkedIn account, and it also provides details into the business and the employees.

6. Synthesis

The analysis required reviewing the emails daily to determine if the emails had actionable information within them. Three of the five domains resulted in only data that was evaluated to be SPAM, with none of the emails providing any actionable information. The remaining two domains provide data and information that yield offensive opportunities for exploitation.

6.1. Orphaned Account Exposure

Orphaned accounts are the result of accounts that are still connected to the Expired Domain email addresses. The email in Figure 9 demonstrates an orphaned account connected to a Deathrow-Servers.com email showing that this email appears to be connected to the admin account for a Google workspace.


Google Workspace

Hello Administrator,

We are writing to let you know that we're making changes to our storage policies for Google Photos, effecti
for storage.

What does this mean for my organization?

The following storage policy changes will take effect:

- **Google Photos**
  Starting June 1, 2021, any **new High-quality photos or videos uploaded to Google Photos will c**
  will not count toward storage. Review documentation on storage for Google Photos.
- **Google Docs, Sheets, Slides, Drawings, Forms, and Jamboard**
  Starting February 1, 2022, any **newly created Google Docs, Sheets, Slides, Drawings, Forms, or**
  February 1, 2022. Read more in our Help Center.

Figure 9: Email directed to Google Account administrator

Upon further investigation, there was no direct confirmation that the account exists. A link providing direct access to the account is not available in the email from Google. The Google Workspace password reset and account recovery options require detailed information that is not available or easily guessed. Further social engineering efforts could result in access to this account, but the research concluded with the account verification attempts.

6.2. Login via Email and Password Reset Exposure

An email from LinkedIn to the previous email owner that provides access to the LinkedIn account provides another exposure to explore. This email provided the ability to access the LinkedIn account simply by requesting a "magic link" from LinkedIn that provided access to the account if clicked within the next 15 minutes. The screenshot below is the result of requesting that link.

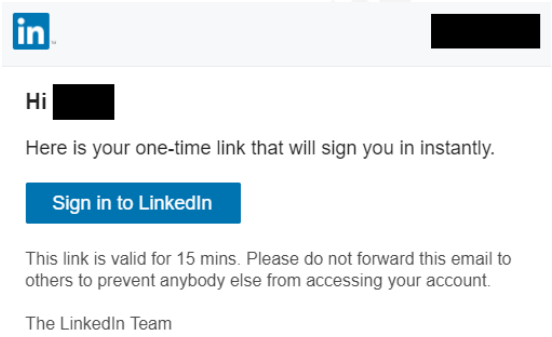


Figure 10: LinkedIn email granting access to an account without a password

Clicking on the link results in the single-click compromise of the account and gives access to the person controlling the email to gain further control over the account. While not typical, this user-friendly login recovery is also available on other sites to easily allow users to access their accounts.

Another similar exposure to those controlling the domain and associated email requires following the standard password account reset process. It is often trivial for an adversary to use the email and password reset process to update an application password gaining control of the account once they control a domain and related email.

6.3. Phishing Exposure

Using the identity of the expired domain, a malicious party can also leverage existing relationships that were not aware of the domain expiration to perform a social engineering attack on any people still sending email to identities within the expired domain. The breach data obtained from the HIBP website and context from emails allow

an attacker to develop a social engineering campaign leveraging the control of the domain and emails.

7. Defensive Strategies for Expired Domains

From a defensive perspective, there are several options to protect these domains from Domain Dumpster Diving. The challenge with protecting a domain is the time, effort, and cost to protect them. If that is not an option, one can consider setting up a similar environment and automation to minimize the email to this domain. The domain owner must consider at what point they need to pay for or give up the domain. A defensive approach requires both time and effort to prevent these domains from being leveraged once released.

7.1. Retain Control of the Domain

In some cases, it can be much easier to pay for the domain indefinitely. Currently, the max period for domain registration is ten years. ("FAQs for registrants: Domain name renewals and expiration," 2018). A process must be implemented to ensuring the renewal occurs, preventing the loss of the domain. In most cases, the registrar provides reminders to domain owners. The contact information for the registrar account must be kept up to date and monitored to ensure renewals occur before the release period.

7.2. Retire the Domain

Proper Domain retirement requires time and effort to ensure the domain can escape Domain Dumpster Diving attempts. The methods discussed in the research provide a playbook to simulate Domain Dumpster Diving before releasing the domain. Monitoring the domain provides the ability to ensure the risk is low before release.

7.3. Reduce the Value for Domain Dumpster Diving

Reducing the value of the domain requires an effort to eliminate any value that future owners could use. Working with sites to remove any existing backlinks can reduce the domain value to SEO users. Removal from the Internet Archive is also

possible while the owner controls the domain but will not be possible once the domain is released.

8. Further Research

There are many options to extend the Domain Dumpster Diving research, and the following topics provide several options to explore.

8.1. Email SPAM filtering

SPAM filtering to support the retirement of the domain before releasing it is an excellent option if time permits. Before retiring a domain, a domain owner can implement SPAM filtering to reduce incoming emails to the domain. Project Tar from junkemailfilter.com provides a free option to reduce domain SPAM using industry recommendations for SPAM defense ("Project tar," n.d.).

8.2. Refinement of Domain Selection

Refinement in the domain selection helps to select domains that reveal more information. Ideally, this domain selection using additional open-source information that can assist in finding a higher value domain. Specifically, researchers would benefit from domain name record history and further details on the domain history. Using the domain DNS history and additional criteria can refine the domain selections further and consider more domains providing a greater chance of success.

8.3. Domain Selection Process Automation

The current process developed requires a manual review of data, limiting the number of domains considered. Many solutions have APIs to automate processes and simplify the work required to review domains and follow selection processes.

8.4. Website Data Collection

Use of the domain for the collection of website data yields additional information about the domain usage. Website usage data would be valuable in deciding how to leverage the domain and resources for offensive operations.

9. Conclusion

Even with the limited success during the six weeks, one can conclude that care must be before releasing a domain name with a history. All five of the domains purchased produced emails, and two of them resulted in information that could result in a takeover of the related accounts. The Domain Dumpster Diving defensive strategies provide several choices to consider before releasing a domain to prevent data loss and resources previously tied to the domain.

References

Ballard, B. (2021, February 3). *Cisco antispam tool blocks thousands of emails following domain registration blunder*. TechRadar. Retrieved May 30, 2021, from https://www.techradar.com/news/cisco-security-tool-blocks-thousands-of-emails-as-spam-following-domain-blunder

Beynon, S. (2020, October 15). *VA has lost GIBill.com rights. Some worry it could prompt Scammers to target student vets*. Military.com. https://www.military.com/daily-news/2020/10/15/va-has-lost-gibillcom-rights-some-worry-it-could-prompt-scammers-target-student-vets.html

Chiles, A. (2017, March 1). *Leveraging expired domains for red team engagements*. Threatexpress. Retrieved May 30, 2021, from https://threatexpress.com/blogs/2017/leveraging-expired-domains-for-red-team-engagements/#domainhunter

Cyger, M. (2017, May 4). *How to grab an expiring domain name*. DomainSherpa.com. Retrieved May 30, 2021, from https://www.domainsherpa.com/how-to-grab-an-expiring-domain-name/

DomCop FAQ. (n.d.). Buy Expired Domains: Moz, Majestic, SEMrush, Estibot, SimilarWeb & more. Retrieved May 30, 2021, from https://www.domcop.com/faq

(n.d.). Expired Domains | Daily Updated Domain Lists for 477 TLDs. https://www.expireddomains.net/

FAQs for registrants: Domain name renewals and expiration. (2018, December). Retrieved August 8, 2021, from https://www.icann.org/resources/pages/domain-name-renewal-expiration-faqs-2018-12-07-en

Christopher DeWeese, cndeweese@gmail.com

Have I been Pwned: Domain search. (n.d.). Attention Required! | Cloudflare. https://haveibeenpwned.com/DomainSearch

Krebs, B. (2021, March 15). *WeLeakInfo leaked customer payment info — Krebs on security*. Krebs on Security. Retrieved May 30, 2021, from https://krebsonsecurity.com/2021/03/weleakinfo-leaked-customer-payment-info/

Life cycle of a typical gTLD domain name. (n.d.). Homepage. Retrieved May 30, 2021, from https://www.icann.org/resources/pages/gtld-lifecycle-2012-02-25-en

Monaghan, M. (2021, February 10). *How much does a domain name cost?* Website Builder Expert. https://www.websitebuilderexpert.com/building-websites/domain-name-cost/

Prajjwal. (2021, April 12). *Revealed: 9 secrets to buying powerful expired domains (Step by step)*. BidnessETC. https://www.bidnessetc.com/expired-domains/

Project tar. (n.d.). Main Page - Computer Tyme Support Wiki. Retrieved May 31, 2021, from https://wiki.junkemailfilter.com/index.php/Project_Tar

SCHULTZ, J. (2021, March). *Domain dumpster diving*. Cisco Talos Intelligence Group - Comprehensive Threat Intelligence. Retrieved May 30, 2021, from https://blog.talosintelligence.com/2021/03/domain-dumpster-diving.html

Statistics on our expiring and expired domains lists. (n.d.). Buy Expired Domains: Moz, Majestic, SEMrush, Estibot, SimilarWeb & more. Retrieved May 30, 2021, from https://www.domcop.com/stats

Szathmari, G. (2019, March 21). *Hacking law firms with abandoned domain names*. Iron Bastion Security Blog. Retrieved May 30, 2021, from https://blog.ironbastion.com.au/hacking-law-firms-abandoned-domain-name-attack/

(n.d.). Wayback Machine. Retrieved May 31, 2021, from https://web.archive.org/

Christopher DeWeese, cndeweese@gmail.com

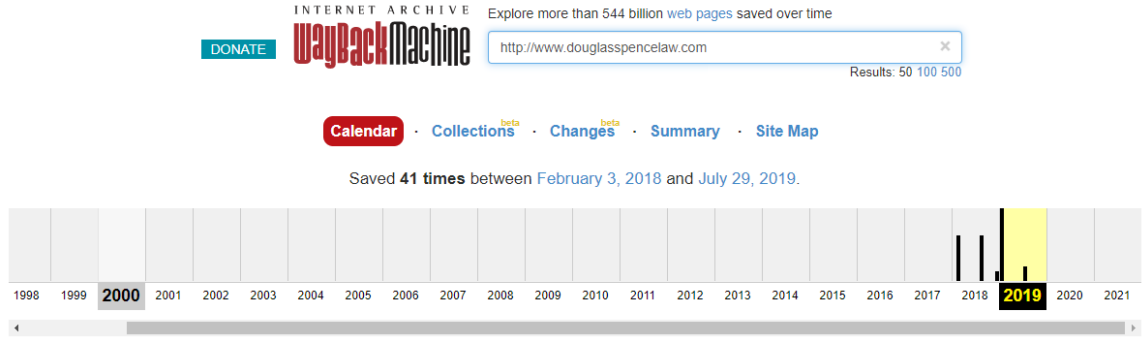
Appendix - A: Expired Domain Research Data

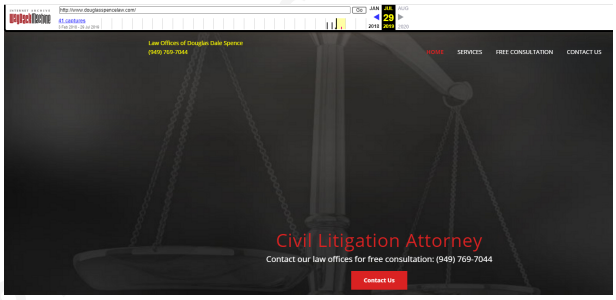
Domain Profile #1 - douglasspencelaw.com

Backlinks Count - 0

Related TLDs - None

Website Existed - Yes





Domain Used for Email – Yes – found on the website

Open-Source Research – This domain is for a lawyer in Newport Beach. The lawyer appears to be currently not practicing due to issues with the state bar association.

MX Record - Yes

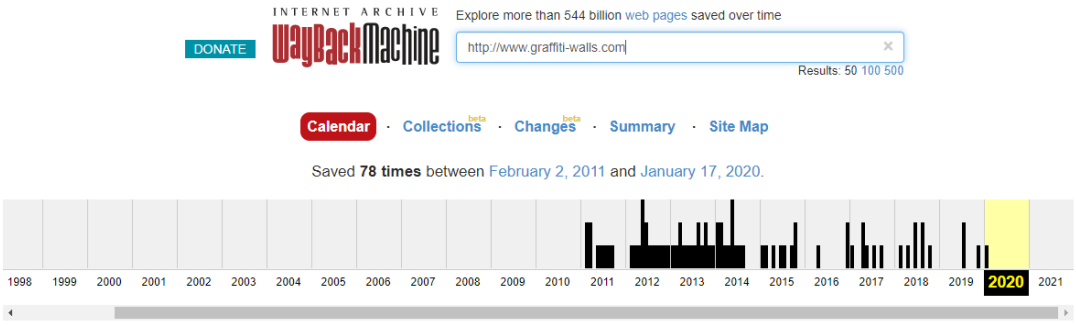
Christopher DeWeese, cndeweese@gmail.com

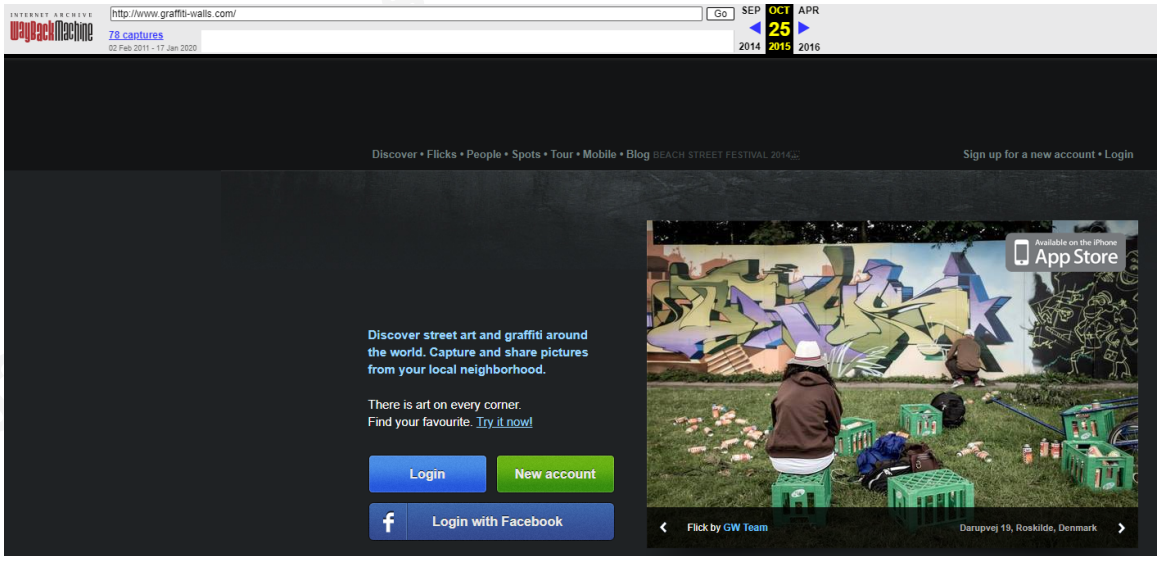
Domain Profile #2 - graffiti-walls.com

Backlinks Count - 421

Related TLDs - .NET / .ORG / .DE / .UK

Website Existed - Yes





Domain Used for Email – Unknown

Open-Source Research - This domain appears to be a website and application supporting street art and graffiti documentation.

MX Record - Yes

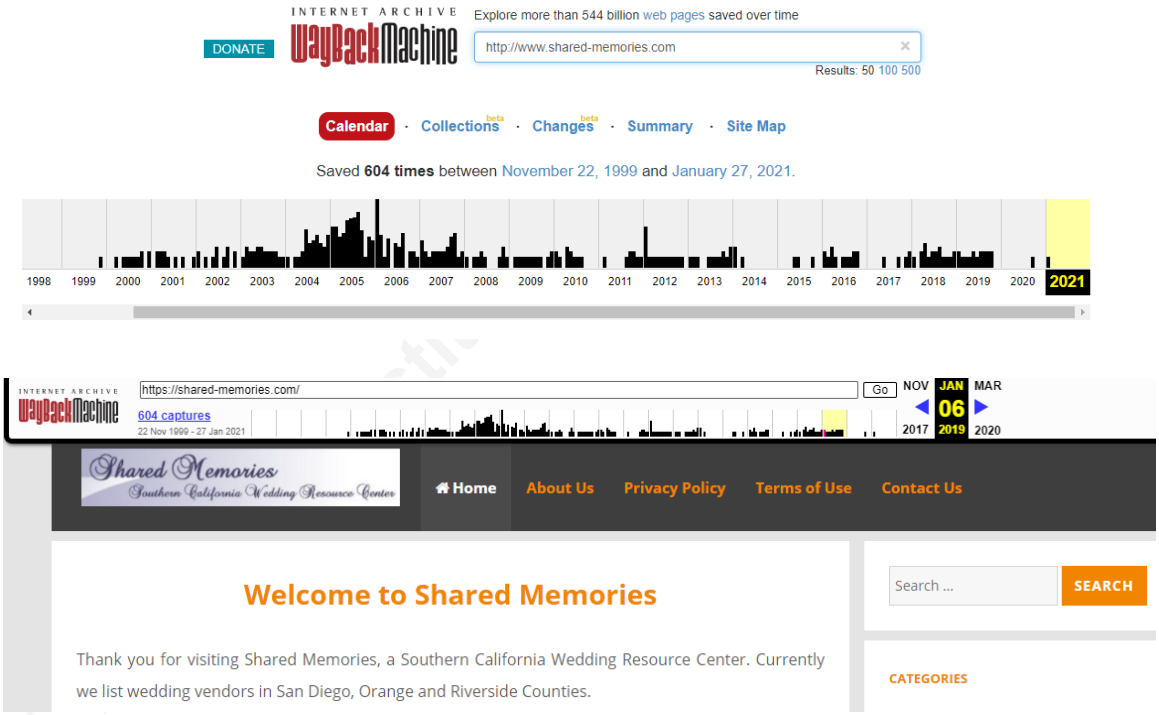
Christopher DeWeese, cndeweese@gmail.com

Domain Profile #3 - shared-memories.com

Backlinks Count - 135

Related TLDs - .DE / .BE / .NL

Website Existed



Domain Used for Email – Yes

Open-Source Research – This domain supports a website and business focused on weddings and supporting information in Southern California.

MX Record - Yes

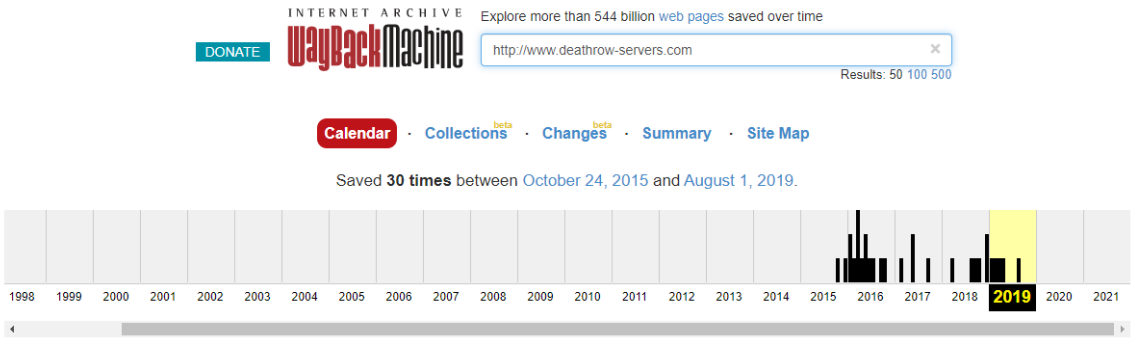
Christopher DeWeese, cndeweese@gmail.com

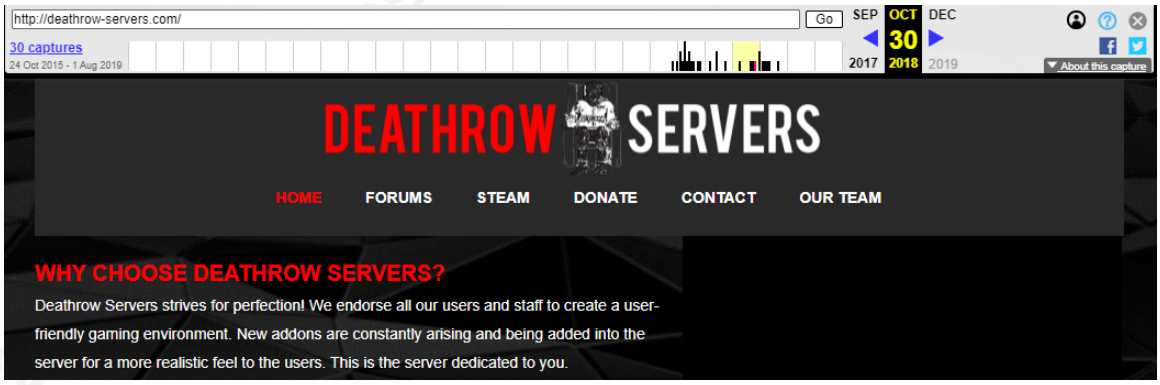
Domain Profile #4 - deathrow-servers.com

Backlinks Count - 148584

Related TLDs - .NET / .ME

Website Existed - Yes





Domain Used for Email – Unknown

Open-Source Research – This domain appears to support a gaming forum and server environment. One of the alternate domains may support the website email over this one.

MX Record - Yes

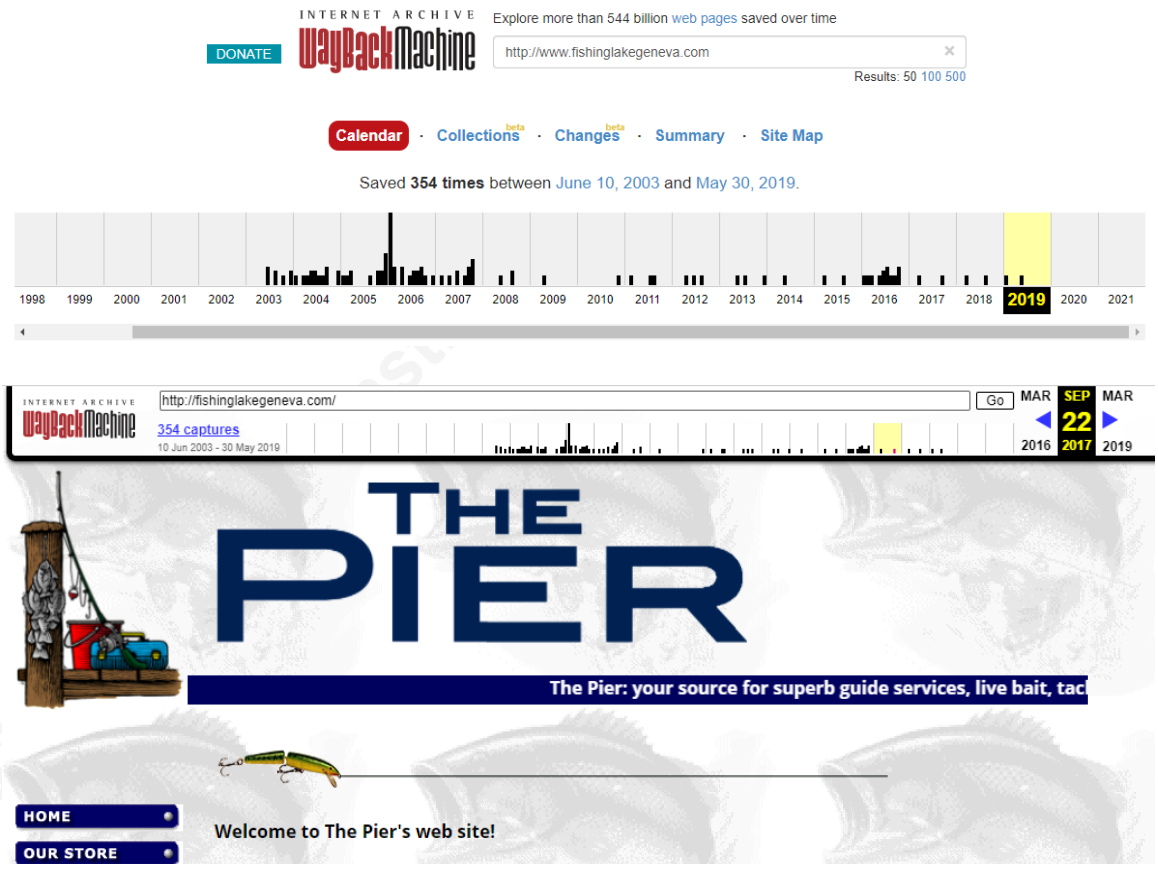
Christopher DeWeese, cndeweese@gmail.com

Domain Profile #5 - fishinglakegeneva.com

Backlinks Count - 329

Related TLDs - None

Website Existed



Domain Used for Email – Yes – Found on the website

Open-Source Research – This domain supports a business in Lake Geneva. Current records show the address for sale and the business currently closed.

MX Record - Yes

Christopher DeWeese, cndeweese@gmail.com