Tag of the Dead: How Terminated SaaS Tags Become Zombies

Takahito Sakamoto
DataSign Inc.
sakamoto@datasign.jp

Takuya Murozono
DataSign Inc.
zonomuro@datasign.jp

***Abstract*—Software as a Service (SaaS) dies. Several SaaS die every day because it becomes too difficult to continue their business. SaaS lets website owners install a small amount of code, called a tag, on a website to extend its functionality of the website. However, sometimes that tag becomes a zombie. In this paper, we coordinate two studies to reveal the danger of the zombification of tags. (1) A research of domains used by dead SaaS tags. (2) An investigation of websites with dead tags. The results of our work show that of the 53 domains used with 49 dead SaaS tags, 18 domains have already been re-registered by a third party or are ready to be re-registered. We also scanned about 1.15 million websites of domestic companies and found 26 dead SaaS tags on approximately 18,000 websites. Finally, we found that three new SaaS tags have been abused by attackers, indicating the danger of zombification tags.**

I. Introduction

Software as a Service (SaaS) has become widely used in various businesses. For example, Google Analytics (GA) makes it easy to aggregate and analyze website visitors' data by putting a small amount of code, called a tag, on a website. According to the SolarWinds survey of the world's top 50 news sites, the average number of trackers present was 43, with a maximum of 85 trackers observed on news sites [14].

SaaS has become an integral part of business, but unfortunately, some SaaS may end their services because they find it difficult to continue their business. If a dead SaaS provided tags to many websites during its lifetime, the tags would also die, and many websites would put their tags to sleep. However, such tags may rise from the dead like zombies and attack visitors on the website.

There were concerns about attacks on website visitors. In May 2022, a zombification incident occurred. The domain `tracer.jp`, used by Visionalist, an access analysis SaaS, was released and re-registered by a third party, and suspicious JavaScript was delivered to many websites that still embedded Visionalist tags.

In this paper, we conducted two studies to determine the risk of tags becoming zombies in terms of how a case like Visionalist will probably happen in the future. The first is a lifecycle study of the domains used in 49 dead SaaS tags, which are known from our database of our product. The second is a crawl of about 1.15 million websites of domestic companies to determine the presence of dead SaaS tags. The results of this paper show that of the 53 domains used by the 49 dead SaaS tags, 18 have already been re-registered by third parties or are available for re-registration. We also scanned about 1.15 million websites of domestic companies and found 26 dead SaaS tags on about 18,000 websites.

The contributions of this paper are as follows.

- Three dead SaaS tags were already zombified, and we observed suspicious scripts being delivered to the 34 websites that still had the tags, so we took action to encourage website operators to remove the tags.
- There was a risk of four dead SaaS tags turning into zombies, and there were concerns about the impact on the 480 sites where the tags remained, so action was taken to announce SaaS providers.
- The three domains used by the three dead SaaS tags were available to anyone, so we re-registered them to prevent them from becoming zombies.

Section II describes the current state of zombie tags and outlines the research in this paper, Section III reports on a survey of domains used by dead SaaS tags, Section IV reports on the current state of dead SaaS tags on websites, Section V describes our activities and Section VI develops the discussion. Section VII presents related work, and Section VIII concludes.

II. Zombification

Figure 1 illustrates how a dead SaaS tag becomes a zombie. The SaaS that is the subject of this paper is the type that provides functionality by having a small amount of code, called a tag, installed on a website. In this type of SaaS, the website administrator obtains the tags from the SaaS management screen and installs them on the website. Popular SaaS has a large number of websites with tags installed. For example, Google Analytics (GA) allows you to visualize the access status of visitors to your website by putting a GA tag on your website with the GA administration screen.

If a SaaS that installs tags on a website terminates its service, the tags installed on the website will no longer function and become dead. Then, after a certain period, the SaaS provider releases the domain used by the SaaS, and a third party (an attacker) re-registers it. When a visitor accesses

Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb) 2023
3 March 2023, San Diego, CA, USA
ISBN 1-891562-87-8
https://dx.doi.org/10.14722/madweb.2023.23034
www.ndss-symposium.org

Fig. 1. How terminated SaaS tags are revived.

a website with a dead SaaS tag, a request to the domain used by the SaaS occurs. If the attacker delivers a malicious script in the response, the attacker is able to zombify the tag and attack the website visitors. Threats of malicious script execution on websites include the following.

- Leakage of cookies and other session information.
- Leakage of form information such as personal information, passwords, and credit card numbers.
- Unauthorized mining of cryptocurrency.
- Forced redirection to phishing websites.

A. Incident

In May 2022, an incident occurred in which a dead SaaS tag turned into a zombie. `tracer.jp`, a domain used by Visionalist, a SaaS for access analysis, was released and re-registered by a third party. 22 months later Visionalist announced the deletion of the tag, on April 30, 2022, the `tracer.jp` domain was still present on many websites, with communications being generated to it. Then, on May 5, 2022, a third party re-registered `tracer.jp` and began distributing suspicious scripts. After that, the name resolution to `tracer.jp` was shut down, and the website visitors were no longer affected. Although the scripts distributed in this case were not offensive, the dead tags were revived and ready to harm visitors to the website anytime. In addition, the incident has resulted in a takedown of the domain name, but there is no guarantee that name resolution will always be stopped immediately or permanently.

Thus, two factors can cause a dead SaaS tag to become zombified: released domain and buried tags.

B. Released domains

Domains (domain names) are called addresses on the Internet. They are registered information that ranges from a character display such as `example.com` to the IP address of a server like 93.184.216.34. The mechanism is maintained by the Domain Name System (DSN) [5]. Any corporation or individual can freely register domains by applying to a domain registrar. Some domains have high value (e.g., domain names for short, popular words) and are bought and sold on the free market for speculative purposes or through auctions.

On the other hand, the threat of domain names being released and re-registered by third parties has long been known. A study of domain drop catches that are immediately re-registered after a domain is deleted reports that about 11% of domains are immediately re-registered, with some domains being acquired for abuse [6]. In Japan, the guidelines of the Council of Anti-Phishing Japan urge that domains should be released at a cool-down time on an annual basis [2].

C. Buried Tags

Some SaaS services are provided by introducing a small amount of code, called a tag, into a website. For example, in the case of an access analysis tool, a tag is installed to send visitors' information to the access analysis SaaS when a user visits the website. Also, if a tag for a map service is installed, it is possible to display a map in some areas on the website.

However, the SaaS that has been introduced may stop providing the service. As in the case of Visionalist, it is possible that many websites do not respond to the SaaS tag simply by making an announcement. Even if the SaaS tags no longer extend their function on the website, they often do not affect the behavior of the website, so they tend to be left unremoved.

D. Motivation

Previous issues with domain name deletion have focused mainly on domains used for websites, and none have focused on domains used for SaaS tags. The Visionalist case study suggests that the threat is likely to be widespread if a domain is used in a terminated tag while a dead SaaS tag is still put on many websites. However, it is still being determined to what extent similar phenomena have happened or is likely to ensue. Therefore, in this paper, two studies reveal the danger of dead SaaS tags turning into zombies.

1) Domain research: Investigate the current status of domains used by terminated SaaS tags (Section III)
2) Website crawling: Investigate how many terminated SaaS tags remain on the websites (Section IV)

III. Domain Research

In this section, we investigate the current status of domains used in SaaS tags that are no longer offered as a service and report the results.

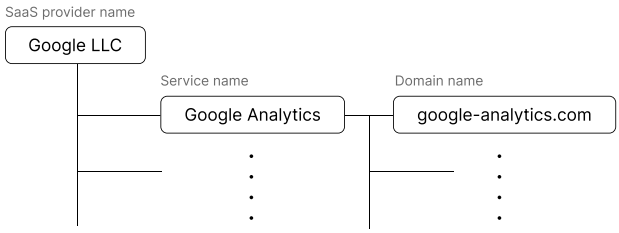

Fig. 2. Data structures of the webtru database for SaaS detection.

A. Dataset

The dataset used in this study is from the webtru SaaS database, a product of DataSign [3]. webtru is a consent management platform (CMP), and one of its features is a headless-chrome-based crawler that detects SaaS installed on a website. The webtru's crawler detects HTTP requests generated by a website and manages the name of the service providing the resource, the service provider name, and other resource information, such as domains and paths. Our system maintains the internal database for detection, as shown in Figure 2, with information on provider names, service names, and domains and paths used. The database currently contains more than 1,400 registered SaaS, mainly from Japanese providers. In addition, the database targets SaaS that are embedded in websites, so there is a wide range of SaaS types.

We primarily maintain the database of more than 1,400 registered SaaS manually. The database even includes 49 SaaS services and 53 domains used by the terminated SaaS services, related to those announced in the news about the termination of SaaS services. The dataset of this study is constructed from these terminated services and domains. The number of services and domains is different because one service may use two domains, or the same domain may be used for multiple services by the same service provider.

B. Methodology

We investigated the current status of 53 terminated SaaS domains by using WayBackMachine [16], WhoisXMLAPI [18], whois command, and actual access. Although some of the domains used by the terminated SaaS were subdomains, the domains surveyed were in units of eTLD+1, which is the portion of the domain that can be purchased by organizations and individuals. In the study, the current status of the domain is recorded as follows.

- **Keeping:**
  - The domain owner has not changed, and name resolution and response have stopped.
- **Deleted**
  - The domain name has been released and can be re-registered by anyone or is being held by the domain registrar.
- **Acquired**
  - The domain name has already been re-registered and used by a third party or is being abused.

For example, if the whois history information obtained by the WhoisXMLAPI confirms that the domain registrant has changed, the status is set to "Acquired". If the whois command is executed and there is no registration, it is assumed that the domain registration has been released, and the status is set to "Deleted."

The registration information in Whois records is reported to be often incomplete due to the use of domain registrars' privacy services [1]. Although it is difficult to obtain accurate organizational information from Whois, this study confirmed the deletion and registration dates of domains. They are accurate information.

In some cases, a SaaS business is "Transferred" through M&A[1], and the ownership of the domain used for the SaaS is also changed to the transferee company. In such a case, the service is not counted as a terminated service because the legitimate transferee company continues to provide the service.

TABLE I
STATUS OF DOMAINS USING THE TAGS OF TERMINATED SAAS.

Status	# of domains
Keeping	35
Deleted	**3**
Acquired	**15**
Total	53

C. Results

Table I shows the results of our survey of the 53 domains used by the 49 services that have been terminated. The results show that 15 domains had already been acquired by different third parties unrelated to the SaaS provider. In addition, three domains had been released and were available for re-registration by anyone. However, the majority of the domains remained with the same provider even after the SaaS was terminated.

If the three obsolete domains are passed on to an unknown third party, and if the tags using those domains remain on the websites, the zombification phenomenon, which is the issue in this paper, may occur. For this reason, we have re-registered all three of the obsolete domains we discovered during our research to ensure their safety.

If SaaS tags that have been re-registered by third parties are still on the website, they may attack visitors like zombies. In the next section, we conduct a crawling survey to determine how many SaaS tags remain on the website after 49 SaaS tags have been terminated.

IV. WEBSITE CRAWLING

This section examines and reports how many terminated SaaS tags remain on websites.

[1]We judge from M&A news as we do from the maintenance of other services.

A. Target websites

Our product, webtru, also provides a research service that crawls the websites of domestic companies and gives a research report on what kind of SaaS is being used on their websites.

We have a list of about 1.15 million URLs, as of June 2022. This URL list is created in our own way. First, we create the list by conducting Google searches based on corporate information obtained from the corporate number publication website operated by a government agency [10], and then combining the top-ranking website URLs and corporate information in a unique way while eliminating noise. Therefore, the target websites of this crawling survey are those owned by Japanese corporations.

B. Methodology

In this paper, we conducted a crawling survey of 1,149,718 URLs between June 22 and June 30, 2022, and detected HTTP requests from SaaS tags to the domains used. We then extracted 49 dead SaaS detections targeted in this paper from the crawling results. In the crawling survey, up to 5 URLs were scanned for each URL page of one website, including the pages under the URL page. These 5 URLs are extracted from the anchor elements in the HTML of the page and pages affiliated with the site, such as those with first-party domains, are selected. Although the crawling survey was conducted on a small number of pages (5 URLs per website), the crawling was conducted with a delay of about 1 second to avoid overloading the site side.

In addition, we accessed the sites where the dead SaaS tags were found to remain using a browser and manually checked for suspicious behavior using Chrome DevTools [4] with the browser in private. Specifically, the existence of dead SaaS tags was checked using "Elements" in the DevTools, the contents of the scripts called by the dead tags were checked using "Network>Response," and the call chain was checked using "Network>Initiator."

C. Results

The results of our investigation of the websites are shown in Table II. As shown in the results, we found that 26 of the 49 dead SaaS tags remained on the websites. The total number of websites with dead SaaS tags remaining was 17,920. The top two SaaS with the most tags were module distribution services that had many users. Both of these SaaS services disclose information on the service termination, but many websites have not yet removed the tags. The third and fourth SaaS with the most tags remaining were advertising services. These services do not have clear information on the service termination, making it difficult for sites that have installed tags to confirm their status. The fifth and sixth SaaS with the most tags remaining is map services. There are many websites with tags buried in these services, even though the service termination information is definitively announced and the map part of the service is no longer displayed.

For the SaaS using the 15 domains in the "acquired" state identified in Section III-C, seven SaaS tags were detected in the crawling survey and were found to remain in a total of 514 websites. Although the services vary, many of them are used for advertising and access analysis. In addition, the use of two of the three domains that we obtained for security purposes was found on 34 websites.

1) The walking dead: To determine whether the seven dead SaaS whose domains are in the hands of third parties have become zombies and been harming website visitors, we checked the websites where these SaaS tags were observed. We accessed the websites manually using Google Chrome's incognito mode and checked for suspicious request destinations and responses using the "Network" function of the DevTools [4].

In addition to Visionalist, three new dead SaaS tags were found to be zombie tags with suspicious behavior. These are marked "◯" in the "Maliciousness" column of Table II. In total, there were 34 websites with three dead SaaS tags.

Of the three dead SaaS tags, `mtburn.com` and `evorydsp.com` behaved the same, generating requests to the malicious domain `odnaknopka.ru`[2].

According to information from "Network>Initiator" of DevTools, the suspicious behavior observed on these two domains was sending request parameters with affiliate IDs to various website endpoints originating from `odnaknopka.ru`. This behavior is similar to ad fraud [19] in that it is assumed that website visitors respond to affiliate links so that the attacker can illegally skim affiliate fees.

This behavior was similar to ad fraud [19]. The attackers implicitly drove website visitors to affiliate links so that they could illegally skim affiliate fees.

On the other hand, the behavior observed on `bb-analytics.jp` forcibly redirected the pages of the websites where the tag was installed to a phishing website, making the website unusable. This behavior is expected to be easily detected by website operators. The zombie tags discovered during the June 2022 survey were found to have been removed from all websites where they were detected when we checked again in August 2022.

The reason Visionalist (`tracer.jp`) is listed as "•" in the "Maliciousness" column of Table II is that name resolution to `tracer.jp` had been shut down at the time of this investigation, and we were not able to confirm whether suspicious scripts were distributed. Third parties have already acquired the domains used by the remaining four SaaS, so there is a good chance that malicious behavior will be initiated. Websites need to remove dead SaaS tags as soon as possible, but there were 480 such websites.

2) Backseat zombies: Of the 26 dead SaaS found on the websites, 17 of the domains used by the SaaS were in the "keeping" state. Some of the "keeping" domains were used only for that service, while other services still used others.

[2]VirusTotal [17] determined that `odnaknopka.ru` was malicious by three security vendors.

TABLE II
THE NUMBER OF WEBSITES DETECTED REQUESTS TO TERMINATED SAAS.

Service name	# of websites	Description	Domain (eTLD+1)	Status	Maliciousness	Other use
Google Code	8253	Open source project.	googlecode.com	Keeping	-	-
RawGit	3356	Content delivery service.	rawgit.com	Keeping	-	-
nex8	1667	Retargeting ad service.	nex8.net	Keeping	-	-
BEYOND X	1003	Ad platform	adjust-net.jp	Keeping	-	-
Yahoo! Static Map API	958	Map service.	yahooapis.jp	Keeping	-	◯
Yahoo! JavaScript Map API	802	Map service.	yahooapis.jp	Keeping	-	◯
Yahoo! Custom Search	723	Search within the website.	yahoo.co.jp	Keeping	-	◯
Visionalist	319	Access analysis.	tracer.jp	**Acquired**	•	-
FreesaleAccessAnalytics	200	Access analysis.	fsaccess.jp	Keeping	-	-
HAYABUSA	114	Image conversion service.	hayabusa.io	Keeping	-	-
Audinece73	113	Behavioral targeting advertising.	audience73.com	**Acquired**	-	-
TRIVER	87	Access analysis.	triver.jp	Keeping	-	-
Access-Counter-Net	87	Free access counter.	access-counter.net	Keeping	-	-
3counter	66	Free access counter.	3counters.net	Keeping	-	-
Kaipara banner	47	Online store search engine.	kaipara.net	**Acquired**	-	-
CAMP	34	Measuring ad effectiveness.	ca-mpr.jp	Keeping	-	-
Lead Analyzer	33	Access analysis.	leadanalyzer.jp	**Deleted**	-	-
Hike	13	Advertisements for mobile.	mtburn.com	**Acquired**	◯	-
Yahoo! Geocities	11	Website creation service.	yahoo.co.jp	Keeping	-	◯
Evory	11	Managed advertisement.	evorydsp.com	**Acquired**	◯	-
BB-ANALYTICS	10	Access analysis.	bb-analytics.jp	**Acquired**	◯	-
Copybar	6	Website editing tool.	copybar.io	Keeping	-	-
CA Tag Solution	3	Tag manager.	tg-mr.jp	Keeping	-	-
3s	2	Engagement improvement tool.	3s-tools.com	Keeping	-	-
MobileMK	1	Mobile conversion tool.	mobilemk.net	**Acquired**	-	-
canata SG	1	Mobile conversion tool.	canata.biz	**Deleted**	-	-

As shown in the "other use" column of Table II, the domains used in the four SaaS tags are also used in other services of the SaaS provider, but the other domains are used only in that SaaS. For example, `yahooapis.jp` is a domain used by other services, and `hayabusa.io` is used only by the terminated SaaS.

Since website operators regularly inventory their domains, domains used only by terminated SaaS are likely to be released. Even domains currently "keeping" would be released and become available for anyone to acquire. There are 13 dead SaaS using such domains, which could lead to the situation described in the Visionalist case study.

V. OUR ACTIVITIES

The main stakeholders in the survey for this paper are SaaS providers, website operators, and website visitors. Based on our results, we report on our approach to each stakeholder and the implementation of information provision, considering the perspective of research ethics.

A. SaaS providers

According to the survey, seven domains that buried websites as a tag have already been acquired by third parties. In the series of activities in this study, we attempted to share information with seven SaaS providers concerned about the impact on the wide range of website visitors. Three providers could not be contacted because they were already out of business. However, four were contacted to encourage them to share information with website operators about the tags that need to be removed from websites. For example, we worked with the provider that provided Visionalist by sharing information about the websites identified in this survey to the extent that we could disclose it.

In Table II, the SaaS service names and domains are published in the hope that the current situation will be widely recognized and addressed. However, there are concerns about the impact on businesses that have "acquired" the domains.

We posit that the closure of these operators will not have any negative effects as they are no longer in business, and that continuing SaaS operators can mitigate any ethical concerns by encouraging their former customers (website operators) to announce the removal of tags and by taking considerate actions themselves. This can be achieved through the public announcements made by the SaaS providers listed in Table II.

In addition, there are 13 that use a dedicated domain with only dead SaaS tags. Such operators are affected by the effects described in this paper and are expected to manage their domains with consideration, such as keeping the domain until the tag is removed from the website.

B. Website operators

Website operators need to remove dead SaaS tags as soon as possible. In particular, there is an urgent need to address the three dead SaaS tags that have already become zombies, as identified in this study.

All websites with `bb-analytics.jp` tags installed have had their tags removed due to apparent malicious behavior. The remaining SaaS providers, mtburn.com and `evorydsp.com`, are no longer in business, so we could not contact them. Fortunately, the number of websites was small (24 websites). We contacted the website operators directly if there was a contact channel, such as a contact form or email.

The four dead SaaS whose domains have already been acquired by a third party also need to have their tags removed as soon as possible, although no attacks were observed. There were 480 such sites, and it was not able to be difficult for us to contact them individually in a realistic amount of time.

C. Website visitors

Direct approaches to visitors to websites with dead SaaS tags are difficult. On the other hand, the three obsolete domains discovered during the research for this paper were acquired by us. This prevents unknown third parties, which may be attackers, from acquiring the domains and sending suspicious scripts to the websites, thus protecting website visitors from future threats.

Two of the domains we acquired have been confirmed using on the website but will be retained at least until the dead SaaS tags are removed from the target website, or a suitable domain transfer party is found.

D. Notifications

The SaaS tag zombification problem targeted in this paper is characterized by the exploitation of the domain used by the SaaS tag. In response to domain abuse, takedowns that stop name resolution for specific domains are said to be effective. For example, Microsoft routinely requests injunctions and performs takedowns of unauthorized domains [15].

On the other hand, the Information-technology Promotion Agency, Japan (IPA) and the Computer Emergency Response Center (JPCERT/CC) have established a reporting flow for vulnerability and phishing information. However, these are the contact points for reporting when a domain used on a website is abused, so there is currently no appropriate contact point for reporting when a third party acquires a domain used in a SaaS tag for abusive use. Nevertheless, we provided information on `tracer.jp` and `bb-analytics.jp` to the contact points of the Japan Registry Service (JPRS) and the IPA because they are JP domains. The JPRS responded that it would be possible if the registration rules have complied with. Although it is unclear how this is related to the information we provided, `tracer.jp` is in a state of takedown because the name resolution has been suspended.

The remaining `mtburn.com` and `evorydsp.com` are both COM domains. Although it is difficult to apply for and conduct takedowns of COM domains from within Japan, we also provided information on the two domains to the IPA's information desk.

VI. Discussion

A. Against zombification

The zombification of tags is characterized by the domain name being the same and the domain owner being a third party, so the conventional client-side security mechanisms such as the Same-Origin Policy and Content Security Policy (CSP) are not effective countermeasures. In order to prevent dead SaaS tags from becoming zombies, the following two points must be strictly followed.

- The service provider does not release the domain used until the terminated SaaS tag is removed from the website.
- Website operator promptly removes terminated SaaS tags.

When both of these are not followed, the tag becomes a zombie.

In addition, the results in the table show that there are four cases where domains used for other services are used. Thus, it is considered effective to use subdomains for domains used for SaaS tags and not to use domains that can be deleted or registered (eTLD+1).

However, if the SaaS provider goes out of business, it is difficult for the provider to keep the domain, so the website must act quickly to remove the dead SaaS tag. If a website operator has accurate control of tags, Subresource Integrity (SRI) is also an effective way. Even if a website operator misses SaaS termination information, or if for some reason that a SaaS provider immediately releases the domain, the risk of an attack can be reduced.

B. Investigation approach

There are investigation approaches that analyze websites or applications to discover faulty resources remaining on them [11], [12]. For example, by observing that a resource being loaded on a website is failing to resolve its name or returning a 404 status code, the signs of an attack can be detected. Whereas this approach is relatively easy to detect a faulty condition, it is difficult to detect the signs of an attack if the resource domain owner has already been changed and the resource is loaded correctly.

On the other hand, our investigation approach begins with a lifecycle survey of the domains used in SaaS. Even if a terminated SaaS domain is in the hands of an unknown third party that is not intended to continue its service and delivers scripts that do not perform malicious behavior, we identify it as an incident. Even if the website where the terminated SaaS tag is placed seems to be loading a legitimate resource, we will consider it a threat if the provider of that resource has changed.

However, it is highly expensive to keep track of the status of domains used by SaaS. Thus, if there is an open environment where SaaS providers themselves can register and change the domains used by their SaaS, it would be possible for websites and researchers to keep track of the status of their SaaS.

C. Acquired domain

This study identified seven of the 15 acquired domains as dead SaaS tags on websites, with three domains confirming abuse. We checked the usage of the remaining 12 domains held by unknown third parties with no detected abuse at the time of our investigation. We found that two domains were affiliate blog sites using the original SaaS information, and two were operating as different service sites. The rest had domain parking or nothing content.

In this study, four of the seven domains observed on the website as dead SaaS tag domains had domain parking or no

content delivery. As shown in Section IV-C, the ownership of the four domains could change to an attacker at any time. The website operators need immediate action.

D. Limitations

Many of the SaaS surveyed in this paper are services for the Japanese domestic market, and the websites surveyed are Japanese corporations. Therefore, we believe that a mechanism for observing SaaS terminations on a global scale and a global survey of websites are needed to conduct further research on the issues addressed in this paper.

In addition, while the study in this paper focused on tags placed on websites, the zombification problem can also occur in SDKs (Software Development Kits) used in mobile applications, such as Android and iOS, when the domain of the SDK provider is re-registered. The study by Pariwono et al. examined obsolete domains and IP addresses in Android applications and reported that many applications had abandoned resources that third parties could obtain [12].

VII. Related work

The fact of domain names being deleted and re-registered has been investigated for some time. A study by Miramirkhani et al. reveals the reality of domain drop catches, where domains are re-registered soon after expiration [8]. They investigated about 28 million domains and found that about 10 percent of domains are re-registered within a day of expiration, and about 6,800 domains are abused. Lauinger et al.'s 2018 survey reported that about 11% of domains are re-registered on the same day, with 9.5% of re-registrations occurring in just zero seconds. They report that domains used for malicious activity are also acquired quickly [6]. A 2017 study by Lauinger et al. also details the activities of domain registrars in the domain lifecycle [7]. They report that users request domains on their behalf and that domain registrars deem valuable are acquired.

In a study of the discontinuation of domains used by certain websites and their acquisition by third parties, Moore et al. conducted a large survey of domains used by banks [9]. They report that 33% of the approximately 2,300 domains used by bank websites were given to third parties, some of which had similar sites, such as phishing sites. In Japan, there have been reports of cases where domains used for local government events and campaigns have been released and abused.

Nikiforakis et al. conducted a large-scale crawling of websites and found 56 domains available for registration by third parties on 47 of the top 10,000 websites [11]. They call this situation "stale inclusion" and warn that it is relatively easy to attack a wide range of Internet users.

So et al. re-registered an unspecified number of domains and analyzed the residual traffic [13]. The paper reports that they re-registered 201 domains and found that the Android library API and advertising system used some domains with observed traffic that appeared to be real users.

VIII. Conclusion

In this paper, we focus on the threats posed by obsolete domains used in SaaS, a type of SaaS where tags are placed on websites, and determine the extent to which threats occur through a domain lifecycle and a website crawling study. Of the 53 domains used in the 49 dead SaaS tags, 18 were already acquired or available for acquisition by third parties. In addition, a crawling survey of about 1.15 million domestic websites revealed that 26 dead SaaS tags were observed in about 18,000 websites. Three dead SaaS tags were identified to be exploited by third parties, indicating that a threat was occurring. The results of this paper suggest that similar threats of "dead SaaS tags turning into zombies" will continue to occur in the future. In order to prevent such threats, SaaS providers must manage their domains properly, and website operators must manage their tags thoroughly.

References

[1] R. Clayton and T. Mansfield, "A Study of Whois Privacy and Proxy Service Abuse," in *13th Workshop on the Economics of Information Security*, 2014.

[2] Council of Anti-Phishing Japan, "Anti-Phishing Guidelines (ver.2021, Japanese only)," https://www.antiphishing.jp/report/antiphishing_guideline_2021.pdf.

[3] DataSign Inc., "webtru," https://webtru.io/.

[4] Google LLC, "Chrome DevTools," https://developer.chrome.com/docs/devtools/.

[5] Internet Corporation for Assigned Names and Numbers (ICANN), "About Domain Names," https://www.icann.org/resources/pages/about-domain-names-2018-08-30-en.

[6] T. Lauinger, A. S. Buyukkayhan, A. Chaabane, W. Robertson, and E. Kirda, "From Deletion to Re-Registration in Zero Seconds: Domain Registrar Behaviour During the Drop," in *Proceedings of theACM Internet Measurement Conference*, 2018.

[7] T. Lauinger, A. Chaabane, A. S. Buyukkayhan, K. Onarlioglu, and W. Robertson, "Game of Registrars: An Empirical Analysis of Post-Expiration Domain Name Takeovers," in *26th USENIX Security Symposium*, 2017.

[8] N. Miramirkhani, T. Barron, M. Ferdman, and N. Nikiforakis, "Panning for gold.com: Understanding the Dynamics of Domain Dropcatching," in *Proceedings of the 2018 World Wide Web Conference*.

[9] T. Moore and R. Clayton, "The ghosts of banking past: Empirical analysis of closed bank websites," in *International Conference on Financial Cryptography and Data Security*, 2014.

[10] National Tax Agency, "Corporate Number Publication Site," https://www.houjin-bangou.nta.go.jp/en/.

[11] N. Nikiforakis, L. Invernizzi, A. Kapravelos, S. Van Acker, W. Joosen, C. Kruegel, F. Piessens, and G. Vigna, "You Are What You Include: Large-scale Evaluation of Remote JavaScript Inclusions," in *Proceedings of the 2012 ACM conference on Computer and communications security*.

[12] E. Pariwono, D. Chiba, M. Akiyama, and T. Mori, "Don't throw me away: Threats Caused by the Abandoned Internet Resources Used by Android Apps," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*.

[13] J. So, N. Miramirkhani, M. Ferdman, and N. Nikiforakis, "Domains Do Change Their Spots: Quantifying Potential Abuse of Residual Trust," in *2022 IEEE Symposium on Security and Privacy*.

[14] SolarWinds Worldwide, LLC., "How website trackers affect the performance of the world's top news sites," https://www.pingdom.com/blog/trackers-impact-performance/.

[15] TechCrunch, "Microsoft secures court order to take down malicious homoglyph domains," https://techcrunch.com/2021/07/19/microsoft-secures-court-order-to-take-down-malicious-homoglpyh-domains/.

[16] The Internet Archive, "Wayback Machine," http://web.archive.org/.

[17] VirusTotal, https://www.virustotal.com/.

[18] WhoisXMLAPI, "WHOIS History," https://whois-history.whoisxmlapi.com/.

[19] Wikipedia, "Ad fraud," https://en.wikipedia.org/wiki/Ad_fraud.