Cracking the Wall of Confinement: Understanding and Analyzing Malicious Domain Take-downs

Eihal Alowaisheq[1,2], Peng Wang[1], Sumayah Alrwais[2], Xiaojing Liao[1], XiaoFeng Wang[1], Tasneem Alowaisheq[1,2], Xianghang Mi[1], Siyuan Tang[1], and Baojun Liu[3]

[1]Indiana University, Bloomington. {ealowais, pw7, xliao, xw7, talowais, xm, tangsi}@indiana.edu
[2]King Saud University, Riyadh, Saudi Arabia. salrwais@ksu.edu.sa
[3]Tsinghua University, lbj15@mails.tsinghua.edu.cn

***Abstract*—Take-down operations aim to disrupt cybercrime involving malicious domains. In the past decade, many successful take-down operations have been reported, including those against the Conficker worm, and most recently, against VPNFilter. Although it plays an important role in fighting cybercrime, the domain take-down procedure is still surprisingly opaque. There seems to be no in-depth understanding about how the take-down operation works and whether there is due diligence to ensure its security and reliability.**

In this paper, we report the first systematic study on domain takedown. Our study was made possible via a large collection of data, including various sinkhole feeds and blacklists, passive DNS data spanning six years, and historical WHOIS information. Over these datasets, we built a unique methodology that extensively used various reverse lookups and other data analysis techniques to address the challenges in identifying taken-down domains, sinkhole operators, and take-down durations. Applying the methodology on the data, we discovered over 620K taken-down domains and conducted a longitudinal analysis on the take-down process, thus facilitating a better understanding of the operation and its weaknesses. We found that more than 14% of domains taken-down over the past ten months have been released back to the domain market and that some of the released domains have been repurchased by the malicious actor again before being captured and seized, either by the same or different sinkholes. In addition, we showed that the misconfiguration of DNS records corresponding to the sinkholed domains allowed us to hijack a domain that was seized by the FBI. Further, we found that expired sinkholes have caused the transfer of around 30K taken-down domains whose traffic is now under the control of new owners.

I. INTRODUCTION

Domain take-down is a powerful tool against cybercrime. When a domain is involved in illicit activities, such as malware distribution, pharmaceutical, and counterfeit goods trading, it can be seized by a law enforcement agency (e.g., FBI) or other take-down parties (e.g., Conficker Working Group [4]). The seizure is based on a court order or a formal complaint to stop an ongoing cyber criminal activity. The seized domain is then blocked by redirecting all visits to a *sinkhole* or by refusing to resolve the domain. It can be *released* later, once it becomes "clean", i.e., no longer involved in any malicious activities.

Challenges in understanding domain take-downs. Although domain seizures are addressed in ICANN guidelines [55] and in other public articles [14, 31, 38], there is a lack of prominent and comprehensive understanding of the process. In-depth exploration is of critical importance for combating cybercrime but is by no means trivial. The domain take-down process is rather opaque and quite complicated. In particular, it involves several steps (complaint submission, take-down execution, and release, see Section II). It also involves multiple parties (authorities, registries, and registrars), and multiple domain management elements (DNS, WHOIS, and registry pools). In addition, little information is available about the taken-down domains, take-down parties, and the operators controlling them. Therefore, this information needs to be collected to make the study possible. Furthermore, evaluating the security and performance of the take-down party requires nontrivial effort as each party manages its own DNS settings.

Our study. In this paper, we report the *first* systematic study on domain take-down aiming at answer a set of questions critical to understanding the security and reliability of this process. For example, how long does an abusive domain remain active before it is taken down? How long has a seized domain been confined before being released? Once released, how soon does the domain become available for purchase? Are there any security loopholes in this process? What is the best take-down practice?

Seeking answers to these questions was made possible by our broad collection of data, including multiple feeds for sinkhole lists, eight domain blacklists, passive DNS (PDNS) data that spans the past six years, and historical WHOIS data provided by our industry collaborator. Using these datasets, we design and implement a unique methodology that utilizes various reverse lookup techniques to find taken-down domains. More specifically, we manually build a list of sinkhole nameservers and IP addresses by searching various online posts, and reverse WHOIS lookup on known sinkhole registrant information, such as contact information, to find hidden sinkholes. Further, our approach leverages PDNS to determine their sinkhole duration and release date, and addresses the challenges introduced by the PDNS data aggregation.

To discover delisted taken-down domains, which are not resolved by nameservers, and are therefore invisible to the PDNS, we designed an algorithm that automatically analyzes the historical WHOIS data to identify these domains and

Network and Distributed Systems Security (NDSS) Symposium 2019
24-27 February 2019, San Diego, CA, USA
ISBN 1-891562-55-X
https://dx.doi.org/10.14722/ndss.2019.23243
www.ndss-symposium.org

their take-down durations. Using such domain and duration information, not only can we analyze the taken-down domains' lifecycles, but we are also able to study the effectiveness of the take-down operations and the security assurance they provide.

Findings. By processing and analyzing the collected dataset, our research sheds new light on the elusive take-down process and brings to light new security-critical observations. In particular, we found 600K seized domains and analyzed their take-down lifecycles over six years. On average, malicious domains have been taken-down for two years (see Section IV-B). We observed that some malicious domains have been controlled by the criminal again after being released. For example, the domain ugnazi.com was taken down in 2012 and was re-registered by the attacker in 2017 (see Section V-B).

Our study revealed certain weaknesses in the administration and management of some take-down actions. Most concerning is that some sinkhole nameservers' domains have expired and been allowed to be repurchased by the public. We identified one sinkhole operator, Conficker working group, with three sinkhole nameservers' domains that expired in 2011 and were repurchased by different parties, giving the new owners access to more than 30K taken-down domains.

Interestingly, we also found that some take-down parties utilize a Cloud DNS service for sinkholing and leave their NS records outdated after they have stopped using the cloud DNS service. We discovered such a problem in the FBI's take-down action and successfully took over a domain taken-down by the FBI with an outdated `NS` record, and redirected its traffic to a web server under our control.

Another issue revealed by our research is the erroneous settings of seized domains. Some of these domains quickly expire, well before their expected take-down duration ends. This causes them to be returned to the registration pool and be available for repurchase by the adversary. More than 14% of domains taken down over the past 10 months have been released back to the domain market. This amount of time is much shorter than the expected "forgetting" duration after release for completely disconnecting the domains from malicious activities. Such a problematic treatment makes it easy for these domains to fall back into the adversary's hand.

Contributions. The contributions of the paper are as follows:

- **New understanding of domain take-down**. We conducted the first in-depth study on domain take-down, an elusive process with few publicly available details. Using a large passive DNS dataset spanning over six years and a unique methodology, we were able to investigate 19 sinkhole operators and acquire a new understanding of their take-down process.
- **Security analysis of take-down parties**. Based on the new understanding, we further analyzed domain take-down parties' security protection. We discovered problematic settings of their nameservers and misconfigurations in the domains they control. These discoveries will help in identifying a set of best practices important for avoiding such pitfalls.

Roadmap. The remainder of the paper is organized as follows: Section II provides the background information. Section III introduces the methodology and the datasets used in our study. Section IV analyzes the variation in the sinkholing duration by different parties and some loopholes in the sinkhole process. Section V reports malicious reuse of previously taken-down domains and the availability of malicious domains. Section VI discusses the limitations of the study and the best practices for configuring take-down operations. Section VII reviews the related prior research, and Section VIII concludes the paper.

II. Background

Domain take-down[1] is the process of repossessing a domain name from its currently registered owner due to a violation of the Acceptable Use Policies (AUPs) defined by ICANN, registries and registrars,, which are involved in the domain registration process. Violations of AUPs can range from name disputes, such as typos of brand names [58], to illicit content distribution, such as websites selling counterfeit products and those hosting malicious content. Domain take-down is a complicated process involving the collaboration of a number of parties at different levels, sometimes in different countries, each with its own rules and regulations. These parties include: the *take-down requester*, the *take-down authority*, and the *take-down executor*. It also involves the affected elements of the Internet name system, such as DNS, WHOIS and registry domain pools.

The take-down process is initiated by a *take-down requester* who essentially reports the domain's violations and submits a request to suspend its operation. The request may be in the form of filing a complaint with the domain's registrar, for example [16], or through a court order, such as the take-down of Citadel domains [3]. A take-down request using a court order forces the compliance of the parties named in the order, such as registries, registrars, and hosting providers. These court orders are usually prepared in accordance with the guidelines provided by ICANN [55], which details the necessary steps for submitting a take-down request to the court. *Take-down authorities* are third-party services specializing in domain take-down, such as brand-name protection companies, but in most cases we find they are within the same party as the *take-down requester*. *Take-down executors* carry out the take-down operation by modifying the Internet name system to reflect the changes specified in the court order, as explained next.

In some cases, the take-down operation involves transferring the ownership of the domain to the *take-down requester* (e.g., law enforcement). In this case, the request to possess the domain is specified in documents prepared for the court. The advantage of transferring the ownership is that it provides the *take-down requester* full control over the domain, such as obtaining measurement on the traffic they receive. The registration fees might be waived, especially for law enforcement agencies or when the operation is carried out against a large malware campaign [5, 55]. However, when possessing a domain is not necessary, registries or registrars are ordered by the court to implement requested changes without transferring the ownership to the *take-down requester*.

A. Operational Elements

A domain take-down is accomplished by making changes to the Internet name system, essentially revoking its current owner's access. This can be achieved by redirecting the domain's traffic (i.e., sinkholing) and delisting the domain.

Domain sinkholing. Sinkholing is a way to redirect the taken-down domain's traffic to a new destination, a *sinkhole*. Take-

[1]Throughout this paper, we use the terms "domain take-down" and "domain seizure" interchangeably.

```
msofwarestore.com. NS dns[1-4].registrar-servers.com
msofwarestore.com. A  209.126.99.155
```

(a)

```
msofwarestore.com. NS ns[7,8].fbi-cyber.net.
msofwarestore.com. A  54.84.58.149
```

(b)

Fig. 1: Changes in DNS records (NS and A) for malicious domain msofwarestore.com (a) Original DNS configuration. (b) DNS configuration after being sinkholed by the FBI.

```
17nfl.biz.          NS ns1.17nfl.biz.
ns1.17nfl.biz.      A  74.81.170.110
```

Fig. 2: Malicious domains 17nfl.biz sinkholed by setting the A record for the nameserver to point to an IP sinkhole controlled by the FBI.

down parties opt for sinkholing for a number of reasons; some parties intend on showing warning banners for victims visiting the domain, while others mimic the operation of a command and control center (C&C) to keep the compromised machine from attempting to connect to a new C&C domain or to collect the traffic for research purposes [57]. Sinkholes are operated and managed by either third-party services, such as Shadowserver [32], take-down authorities, such as the FBI, or take-down executors, such as GoDaddy.

Technically, domain sinkholing is performed by changing the configuration of a domain's DNS records. DNS is a hierarchical system that maps a domain name to its IP address. To resolve a domain properly, the owner has to set an NS record at the registrar, which, in turns, points to the IP address (i.e., the A record) of the domain/host. In order for sinkholing to take effect, the registrars and registries named in the court order set the DNS records of the taken-down domain to point to the sinkhole. This can be done by setting the nameserver (i.e., NS record) to point to the nameserver of the sinkhole. As a result, the traffic will be diverted from the malicious domain. Figure 1 shows the changes in the DNS records for the malicious domain msofwarestore.com before and after being sinkholed by the FBI. Alternatively, Figure 2 shows a less popular option, which is setting the A record of the domain's NS record to point to the IP address of the sinkhole IP directly.

Domain delisting. Domain delisting is essentially the process of deactivating a domain by removing it from DNS and responding with nonexistence (i.e., NXDomain) to any DNS queries. However, removal from DNS is not enough to delist a domain, as it may return to the pool of available domains at the registries. Delisting goes a step further by modifying the WHOIS records of the domain and placing a *hold* on the domain, thus stopping it from being released back to registries until it either expires or the hold is removed.

The WHOIS domain database is an Internet directory containing domain registration information, such as contact details of its registrants, administrator, and technical support staff. Additionally, a WHOIS record includes domain Extensible Provisioning Protocol (EPP) status codes [12], which define how a domain's registration can be managed. EPP codes can indicate if a domain is active or whether it can be transferred, modified, or deleted. For example, an OK EPP code indicates a normal state. There are two types of EPP codes: client and server codes. Registrars are allowed to set client EPP status codes, while server EPP status codes can only be set by registries when necessary to override other EPP codes that may be set by the registrar (i.e., client EPP codes). In the process of domain take-down, registries and registrars may delist a domain by setting its EPP status code to SERVERHOLD and CLIENTHOLD, respectively. Placing a domain on hold in this way causes it to be nonexistent in the DNS and unavailable for purchase through registrars. Typically, domains taken down in this way remain delisted until their old registration records expire.

In addition to domain sinkholing and delisting, we also observe very rare cases in which a domain becomes RESERVED as part of a seizure process. Reserved domains are the ones locked by their TLD registry. These domains are not included in the public pool of available domains. Reserved domains are locked for different reasons (e.g., due to name collision, or due to short domain name) and not necessarily because of a take-down process. We consider these reserved domains out of the scope of our study as they are rarely used in seizure actions, and it is not clear how to identify taken-down domains from them, and thus will introduce noise to our list of domains.

Example. Microsoft is renowned for its take-down operations of botnets exploiting vulnerabilities in their products. Microsoft has taken down five botnets, Dorkbot [9], Ramnit [28], Shylock [33], Citadel [3], and ZeroAccess [35], where they obtained domain and IP seizure orders by suing an unnamed defendant, John Does, for violations of federal and state laws operating a botnet causing harm to Microsoft customers, and for trademark infringement. Upon examination of the provided evidence of the cited violations, the court issued seizure notices for hundreds of domain names and IP addresses. These notices detailed the specifics of the domain seizure approach, which was to sinkhole the seized domains by setting their NS records to point to Microsoft's sinkhole, *.microsoftinternetsafety.net. Incidentally, in these take-down operations, Microsoft is the *take-down requester* and the *sinkhole operator*, while the *take-down executors* are a number of registries and registrars, according to the listed domains' TLDs and registration records.

B. Threat Model

In our research, we consider an adversary who is capable of exploiting loopholes in the domain take-down process to regain control of previously taken-down domains. This not only renders the domain take-down process less effective but also opens the door for new attack vectors such as the exploitation of outdated sinkhole configuration settings.

III. FINDING TAKEN-DOWN DOMAINS

In this section, we elaborate on the design and implementation of the techniques we use to identify domains that have been taken down either by sinkholing, or delisting. We conducted a measurement study on seized domains using the methodology pipeline as shown in Figure 3. We analyzed around 1M malicious domains to identify seized domains and their take-down durations. For this purpose, we first collected a set of malicious domains, including blacklisted domains and domains hosted on sinkhole servers. To collect the latter, we first identified a set of sinkhole nameservers/IPs from different sources and then defined a set of criteria to validate these sinkholes. In addition, we utilized some techniques to discover new sinkholes, as presented in Section III-A. Then,

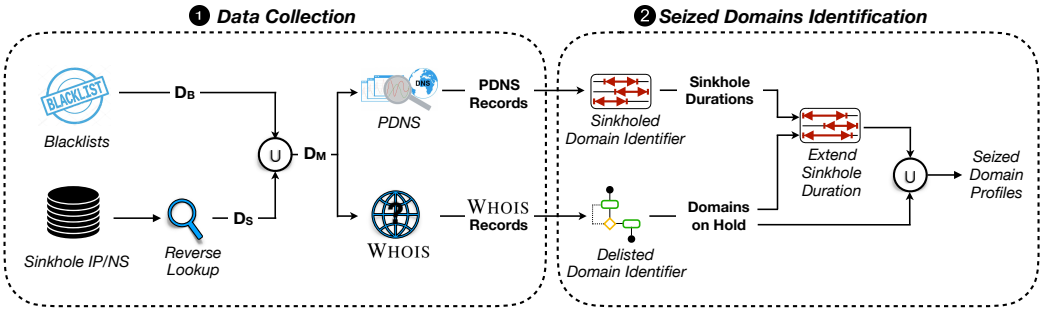


Fig. 3: Workflow of our measurement approach, where D_B is the blacklisted domains, D_S represents possible sinkholed domains, and D_M denotes the union of D_B and D_S.

we collected domains resolved by these sinkholes to find 606,880 domains, which are combined with 465,942 domains from eight blacklists. Finally, we used passive DNS (PDNS) and historical WHOIS to identify taken-down domains, as discussed in Sections III-B and III-C. As a result, we found 625,692 seized domains and profiled their take-down durations.

A. Data Collection

Our malicious domain list D_M is collected from two sources: possible sinkholed domains (i.e., D_S), which is retrieved using identified sinkhole operators, and blacklisted domains (i.e., D_B). To identify taken-down domains (either by sinkholing or delisting) and to analyze their lifecycle, we also collected PDNS and historical WHOIS for each malicious domain in our list.

Identifying sinkhole operators. Our goal here was to compile a list of confirmed nameservers/IP used as sinkholes. We then used this list of sinkholes to collect all domains that historically pointed to them. This list of sinkholes is also utilized in Section III-B.

To get a list of nameservers and IPs used for sinkholing, we searched the Internet to collect three types of sinkhole feeds: take-down notices and reports, domain removal lists, and existing sinkhole lists. We manually reviewed the published take-down court orders [3, 9, 28, 33, 35] and security reports that described take-down incidents, such as [14, 31, 38], to find sinkhole IPs, sinkhole nameservers, and the malicious domains to be sinkholed. We then used the PDNS data to check the changes in the `NS` and `A` records for these sinkholed domains during the report time to find the nameservers/IPs responsible for sinkholing them. In addition, we used the ZeuS domain removal list, which includes a list of domains that no longer pose harm either because they have been cleaned or seized [37]. We checked the nameservers/IPs of these sinkholed domains. We also utilized some sinkhole lists, such as the Emerging Threat rules [11] and other online lists [6, 22].

Before including any of the sinkholes to our verified list, the following criteria had to be satisfied: 1) the sinkhole must be operated by an identifiable party, 2) the nameserver is exclusively used for sinkholing, and 3) the ownership of the domain used in the nameserver sinkhole did not change due to expiration.

To find undocumented sinkhole nameservers, we also used a sinkhole operator's email address to retrieve all domains related to it (i.e., performing reverse lookup via email). For example, we used a commercial tool [8] to perform a reverse WHOIS lookup on an FBI email `cyd-dns@ic.fbi.gov`. This email address was obtained from a WHOIS record of a taken-down domain 444pay.org. As a result, the reverse WHOIS lookup returned a list of around 1,700 domains. Most were seized domains and not domains that hosted sinkholes. To identify domains used as sinkhole nameservers, we used PDNS to retrieve all domains that used one of these possible sinkholes as a nameserver and considered only sinkholes that returned more than 1K domains. Next, we randomly sampled those returned domains and checked their names for signs of previous malicious use. In this way, we could confidently determine that the nameserver that resolved this domain is a sinkhole. We inferred previous malicious use from the domain name semantics (e.g., containing keywords such as "pills", "drugs", etc.) or their affiliations with blacklists. In this way, we discovered a domain named kratosdns.net, which the FBI uses as a nameserver to sinkhole malicious domains.

Table I shows the sinkhole operators and their corresponding nameservers/IPs we compiled. These sinkholes belong to 19 sinkhole operators, including a law enforcement agency (the FBI) or their contractors, technology cooperates (Microsoft), security companies and working groups, and registrars. We further utilized the list of verified sinkholes to collect possible sinkholed domains. That is, we collected all domains/subdomains that happened to point to one of these sinkholes (i.e., performed reveres lookup). More specifically, we queried PDNS to return all domains/subdomains that pointed to any nameserver/IP used as a sinkhole, denoted as D_S. This list served as the possible sinkholed domains list, which had 606,880 apex domains (i.e., domain name without the host/-subdomain part).

Collecting blacklisted domains. We complemented our list of malicious domains with a set of blacklisted domains. Table II contains the eight public blacklists we used, along with their corresponding number of unique domains. The blacklists that provide historical data are: hpHosts [17], PhishTank [26], and Malware Domain Blocklist [20]. For PhishTank, we excluded any domains labeled as ad/tracking (ATS), misleading marketing (MMT), or to be verified label (TBV), as we are only interested in malicious domains. Some blacklists do not provide historical data. These are: ZeuS Tracker [36] and Malc0de [19]. In order to complement them, we used WayBack Machine [18] to crawl any available snapshots of the domains on these lists. We also considered malware blacklists such as Conficker [2] and Ransomware Tracker [29]. The unique apex domains extracted from the blacklists is denoted as D_B, with a total of 465,942 domains.

We combine the list of possible sinkholed domains D_S

Operator	# of Identified Sinkholed Domains	Type of Operator	Nameservers	IP Addresses
NameCheap	194,772	Registrar	blockedforabuse[1, 2].**pleasecontactsupport.com**[*] blockedduetophishing.**pleasecontactsupport.com**[*] blockedduetospam.**pleasecontactsupport.com**[*]	-
FBI	131,875	Law Enforcement	ns[1, 2, 3, 4, 5, 6, 7, 8].**cirfu.net**[*] (exp: 2016/04/01) pleasedropthishost155[25, 26, 27, 28, 29, 30][*].**cirfu.biz** ns[1, 2, 7, 8].**fbi-cyber.net**[*] ns[1, 2].**kratosdns.net**[*] ns[1, 2].**seizedservers.com**[*] ns1[1, 2].**cyberwatchfloor.com**[*]	142.0.36.234 74.81.170.110 74.81.170.109 74.81.170.108 66.212.148.115 74.208.15.160 (2010-11-30 – 2018-03-04) 54.83.43.69 (2014-10-01 – 2018-01-24) 174.129.233.242 (2015-08-12 – 2018-03-20) 23.21.206.195 (2012-04-28 – 2018-03-14)
Microsoft	103,853	Tech Company	ns[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 149, 150, 085, 086].**microsoftinternetsafety.net**[*]	199.2.137.0/24 207.46.90.0/24
Shadowserver	87,974	Non Profit	sinkhole-[00, 01, 02, 03, 04, a, b].**shadowserver.org**[*] sinkhole03.**shadowserver.org**[*] ns[1, 2].sinkhole.**shadowserver.org**[*] dns[1, 2].sinkhole.**shadowserver.org**[*] k[a, b, c, d].sinkhole.**shadowserver.org**[*] sc-[a, b, c, d].sinkhole.**shadowserver.org**[*] sinkhole.**shadowserver.org**[*]	87.106.250.34 (2010-11-04 – 2017-11-30) 85.17.31.82 (2016-03-15 – 2017-11-30) 74.208.164.166 (2010-11-04 – 2015-03-30) 87.106.24.200 (2010-11-04 – 2015-02-11) 216.218.185.160/29 (2015-10-23 – 2017-11-30)
Security Scorecard	39,034	Security Vendor	ns[1, 2].**honeybot.us**	-
Spamhaus	9,940	Security Vendor	n[1, 2, 3, 4].**sinkhole.ch**[*] ns[1, 2, 3, 4].**sinkhole.ch**[*] ns.**sinkhole.ch**[*]	23.88.254.179 (2016-06-30 – 2017-11-30) 87.255.51.229 (2012-04-03 – 2017-11-30) 192.42.116.41 (2014-04-09 – 2017-11-30) 192.42.117.14 (2015-04-20 – 2017-11-30) 192.42.117.41 (2014-11-27 – 2017-11-30) 192.42.118.41 (2014-11-27 – 2017-11-30) 192.42.119.41 (2014-04-28 – 2017-11-30) 198.98.120.157 (2016-02-17 – 2017-11-30) 198.98.120.158 (2017-06-08 – 2017-11-30) 199.231.211.108 (2016-02-16 – 2017-11-30) 198.98.120.157/24 (2016-01-19 – 2016-02-15) 199.231.211.108/24 (2016-01-16 – 2016-02-14)
Arbor	6,714	Security Vendor	ns[1, 2, 10].**arbor-sinkhole.net**[*]	-
Cert Polska	1,229	CERT in Poland	sinkhole.**cert.pl**[*] sinkhole112.**cert.pl**[*]	148.81.111.60/30 148.81.111.64/27 148.81.111.96/28 148.81.111.112/29 148.81.111.120/30
Zinkhole	1,149	Other	**zinkhole.org** ns[1, 2].**suspended-domain.org**[*]	-
LogicBox	997	Other	ns[1, 2].ofac.**suspended-domain.com**[*]	-
Kaspersky	392	Security Vendor	-	95.211.172.143[*] (2014-12-17 – 2017-11-30)
GoDaddy	525	Registrar	ns[1, 2].**suspended-for.spam-and-abuse.com**	-
CWGSH (Conficker Working Group)	26,345	Working Group	ns.**cwgsh.org** (exp: 2011-02-26) ns.**cwgsh.net** (exp: 2011-02-26) ns.**cwgsh.com** (exp: 2011-02-26) ns.**0xc0f1c3a5.com** ns.**0xc0f1c3a5.net** ns.**0xc0f1c3a5.org** ns.**conficker-sinkhole.net** ns.**conficker-sinkhole.com** ns.**conficker-sinkhole.org**	-
Conficker (China)	3,642	China Internet Network Information Center, .cn registry	ns.**conficker-sinkhole.cn**	-
Wapack	22	Other	-	23.253.46.64 (2014-07-26 – 2017-11-30)
Fitsec	15	Security Vendor	-	193.166.255.171 193.166.255.170
Anubis	363	Security Vendor	-	195.22.26.192/26 (2013-02-15 – 2017-11-30) 212.6.183.192/26 (2013-02-11 – 2017-11-30)
GaTec	160	Academic	smaug.gtisc.**gatech.edu**	143.215.130.33
Team Cymru	5	Security Vendor	-	38.229.0.0/16 (2007-09-18 – 2017-11-30)
Total # of Unique Identified Sinkholed Domains	**608,557**			

TABLE I: Sinkholes used in our study. The (*) denotes sinkholes used for reverse lookup. The rest were used for labeling only. The IPs were verified to be used as a sinkholes during the dates provided.

Blacklist	# of Unique Domains	Time Range
hpHosts [17]	337,065	2009-05-05 – 2017-10-01
Conficker [2]	90,884	2017-10-31
Malware Domain Blocklist [20]	24,243	2015-11-10 – 2017-10-02
Malc0de Database [19]	20,049	2017-05-15 – 2017-10-31
PhishTank [26]	9,400	2007-10-03 – 2017-10-31
Ransomware Tracker [29]	5,968	2016-11-17 – 2017-09-29
ZeuS Tracker [36]	1,309	2017-05-15 – 2017-10-31
Malware Domains List [21]	895	2009-05-08 – 2017-09-28
Total # of Unique Domains	**465,942**	

TABLE II: The blacklists used to collect blacklisted domains D_B considered in our dataset.

and the list of blacklisted domains D_B to form the final list of malicious domains D_M. We filtered out domains that belong to: cloud services, dynamic IP services, bulk registration, URL shortening services, and adNetworks. The total number of unique domains in D_M is 1,067,968. To identify taken-down domains from D_M (either by sinkholing or delisting) and analyze their lifecycles, we collected the following data sources for each domain in D_M:

•**PDNS**. In order to study the lifecycle of taken-down domains, we utilize the Passive DNS (PDNS) data provided by Farsight [13]. This dataset includes passively gathered DNS resolutions and zone files for some supported TLD zones. This dataset contains historical successful resolutions for domains, storing a variety of record types that include `A`, `NS`, `CNAME`, `SOA`, `PTR`, etc. The data is provided in an aggregated format. For each domain in D_M we queried all `A` and `NS` records in November 2017.

•**WHOIS**. When a hold is placed on a domain, the domain will not be active in the DNS. As a result, it can no longer be found from our PDNS data. To find such a domain, we resorted to the historical WHOIS data provided by our industry collaborator [25]. This dataset covers around 55% of our malicious domains D_M.

B. Identifying Sinkholed Domains and their Durations

Here, we elaborate on how we used PDNS data collected for domains in D_M to identify taken-down domains through sinkholing (i.e., sinkholed domains) and how to profile their sinkholing duration.

Identifying sinkholed domains. We utilized PDNS data collected for domains in D_M to identify sinkholed domains. Note that as mentioned in Section III-A, the list of possible sinkholed domains D_S is contained in D_M. Such apex domains that appeared in D_S may not necessarily be sinkholed but instead their subdomains were. Therefore, we traversed the resolution history of the PDNS records for each domain in D_M to look for indication of sinkholing by checking their `A` and `NS` records. We considered a domain to be sinkholed only if its apex domain or its nameserver are sinkholed. We eliminated those records that were only seen within a very short duration of time (a second)[2].

We marked each domain's PDNS record with one of the following labels: *sinkholed*, *possibleSinkholed*, or *notSinkholed*. We utilized the sinkhole list in Table I to label `NS` and `A` records. If the nameserver/IPs of the record was found on the sinkhole list, we labeled the record as *sinkholed*. Note that we extended our sinkhole list to include IP ranges. More specifically, given the existing IP sinkholes affiliated with

[2]This happens when the timestamp of `first-seen` field in a PDNS record is identical to its `last-seen`, indicating that the duration of the record is too short to be useful for our study.

```
First-seen:2018-01-15    Last-seen:2018-06-30
bailiwick: com.          rrtype: NS
rdata: ns.sinkhole.com.
```

(a)

```
First-seen:2018-03-15    Last-seen:2018-03-30
bailiwick: com.          rrtype: NS
rdata: ns.namseserver.com.
```

(b)

Fig. 4: PDNS record aggregation, two overlapping observations with different `rdate` values in (a) and (b) for malicious.com.

security organizations, we used IP WHOIS to recognize their IP ranges and add them into the sinkhole list. Note that this list is only used for labeling the records of malicious domains and that no additional reverse lookups were performed on these ranges. We believed it is safe to assume that a malicious domain is sinkholed if it resolves to an IP range that belongs to a sinkhole operator. We labeled a record as *possiblySinkholed* if the nameserver of the record included a keyword such as *sinkhole* or *seize* (e.g., `ns.seize.com`), or if it pointed to a reserved IP (e.g. localhost), or if it included unconfirmed sinkholes (e.g., those for which we could not identify their operators). Finally, the remainder were labeled as *notSinkholed*. At this point, PDNS records were labeled and we identified 608,557 sinkholed apex domains. So, the next step was to analyze the sinkhole durations.

Identifying sinkholed domains' durations. Once each record was labeled, we tried to find out the sinkhole duration for each domain and its release timestamp, again based on its related PDNS records. Here, we define the sinkhole duration as the duration in which the domain was resolved by a sinkhole nameserver or resolved to a sinkhole IP. We also define the release timestamp as the one when the domain was released from the sinkhole.

To determine these timestamps, first we had to understand how Farsight [13], the PDNS data provider, aggregates DNS records, which presented a challenge in estimating the durations. PDNS data provided by Farsight are aggregated record sets. It collects multiple DNS query records to generate a single record if the following fields are identical: bailiwick, record type (i.e., `rrtype`), and query answer (i.e., `rdata`). However, calculating the sinkhole duration is not straightforward. Subtracting the last-seen field from the first-seen without accounting for the existence of other overlapping records may lead to inaccurate estimations of the sinkholing duration. Figure 4 shows a hypothetical example of PDNS records for a sinkholed domain, malicious.com. The domain was resolved by a sinkhole nameserver `ns.mySinkhole.com`, as indicated in Figure 4a. However, the domain was also resolved by another nameserver (i.e., `ns.namseserver.com`) and overlapped with the previous record, as shown in Figure 4b. Therefore, when calculating the sinkhole duration, we had to account for the occurrence of `ns.namseserver.com` during March to break the sinkholing duration into two parts: 2018-01-15 to 2018-03-14, and 2018-03-31 to 2018-06-30.

Another challenge was that the DNS query records in the Farsight's PDNS were independently collected from two sources: TLD zone files (for some supported TLDs), and Farsight's DNS sensors. Further, the data received from the

sensors were also aggregated separately according to their TLDs or second-level domains. So, for each sinkholed domain, its sinkhole records came from the TLD zone files (for supported TLDs), Farsight's aggregated data based on TLD, and the aggregated data based on the second-level domain. Therefore, the data about duration is scattered across several records from different resources. The question then became how to leverage the records from all these sources to estimate a domain's sinkhole duration.

The records from all these sources are utilized to estimate the domain's sinkhole duration. We compared the different records of the domain to break a long duration into shorter ones or to merge two overlapping durations. Specifically, we first determined whether the domain's *sinkholed* records overlap with *notSinkholed* records in terms of their durations. If so, we had to update the first-seen and the last-seen fields for the domain's sinkhole timestamps to exclude the time intervals of the *notSinkholed* records. We then looked at the overlap between two *sinkholed* records, which allowed us to extend the domain's sinkhole duration to include the time intervals for both records. In this way, we could get a more accurate estimate of a given domain's sinkhole duration and accordingly its release timestamp. This information is used in our measurement study reported in Section IV and Section V.

Note that the sinkhole lifecycle measured in our research was based mainly on a domain's visibility in the PDNS. Such visibility could be limited, when Farsight's sensors did not observe resolution requests for the domain. Nevertheless, the information allowed us to come up with a rough estimate about the domain's sinkhole duration, which was important to understand the domain's take-down process.

C. Identifying Delisted Domains

Compared with sinkholed domains, delisted domains are more difficult to observe because they are not resolvable through DNS. Therefore, they will not appear in the PDNS data once delisted. To identify such domains we used WHOIS data.

Domain WHOIS status identification. To identify delisted domains, we used the domains' WHOIS records. As mentioned in Section II, a domain's WHOIS records include domain's registration status (i.e., EPP codes). Setting a domain's status to SERVERHOLD/CLIENTHOLD is an indicator of a possible take-down performed by a *take-down executor*. In our research, we utilized a set of historical WHOIS data provided by the 360 Netlab [25] to find out when a domain was delisted. This historical dataset covers around 55% of the domains in D_M and the earliest WHOIS record dates back to November 2014.

When a domain is taken down by the registry, its EPP status code is set to SERVERHOLD. Similarly, when a domain is taken down by the registrar, a hold will be placed using a CLIENTHOLD EPP status code, essentially removing the domain from the registry's DNS zone file, and therefore it will not be resolved. However, it is important to note that these two EPP status codes are not exclusively used for domain seizure. They are sometimes set by the registry or the registrar for other purposes for example, after the WHOIS verification duration has passed, or when the domain is subject to deletion [12]. To identify delisted domains, we use a set of heuristics to identify the occurrence of a take-down action, as illustrated in Algorithm 1.

Specifically, we first checked whether either REDEMPTIONPERIOD or PENDINGDELETE appeared in the domain's status field, which indicates deletion. We then looked for a sign for auto renewal (i.e., AUTORENEWPERIOD). If any of these codes were set along with a hold flag, this strongly indicated that the hold was not caused by the take-down action. One problem was that not all the registries/registrars implemented the above EPP status code. In other words, some domains may not have had the aforementioned flags after their expiration. Therefore, we had to set additional heuristics to determine whether a domain was about to be removed or was in the auto renewal stage.

Therefore, we first checked whether the hold was placed after the domain's expiration date. If not, we still have to look into the possibility that the hold was set due to auto renewal, which extends the domain for one additional year by some registries, even before the owner pays. Such a renewed domain would be placed on CLIENTHOLD, pending for the payment from the owner. We identified such records by looking at its update date and expiration date. If the difference was one year, we conservatively assumed that the hold was due to non-payment and did not consider the domain to be delisted.

Further, the registry requires a newly created WHOIS record to be verified by its registrant within 15 days. After that, CLIENTHOLD is set for unverified ones. We checked whether the hold was placed within 15 days of the creation of a domain. If so, we did not consider it as a delisted domain.

The proposed algorithm identifies a delisted domain based only on one snapshot of its WHOIS data due to limited number of snapshots available in our dataset. This method, however, may cause some domains to be labeled inaccurately [46]. Specifically, it would mislabel a seized domain as a non-seized one (i.e., introducing false negatives). For example, it will mislabel a seized domain that has been intentionally renewed on its auto renewal date as a non-seized domain. Similarly, it will misconstrue a seized domain that is placed on hold after its expiration date as a non-seized one (this case observed in `.org` domains). To measure the prevalence of such mislabeled cases, we evaluated our algorithm through sampling and manual validation. In particular, we investigated 52 domains in which we had at least two snapshots (one before the expiration, and the other after and placed on hold). For this set, we counted the number of domains that were on hold before the expiration and found only three cases (5.77%). In general, the algorithm we used introduced less than 4% of domains to our analysis. Therefore, the effect on our study is minimal.

Note that some other EPP status codes have been observed in take-down operations, such as TRANSFERPROHIBITED, DELETEPROHIBITED, and UPDATEPROHIBITED. However, they are not strong take-down indicators and could be used for additional protection. These EPP codes do not affect the resolution of the domain; actually the take-down action that set these records must be accompanied by DNS redirection (i.e., a sinkholing). Therefore, we ignored these codes and relied instead on the sinkhole detection, as mentioned earlier in Section III-B, to capture these taken-down domains.

Take-down duration extension. We also studied the cases in which malicious domains were first sinkholed and then delisted. These cases were identified using our approaches for identifying sinkholed domains (see Section III-B) and delisted domains. Once we identified a delisted domain, we looked it

Algorithm 1: EPP status analysis to identify take-down actions thought delisting

```
1  delisted = False
   // lastCheck is the date when WHOIS data were
      crawled
2  dateToCompare = lastCheck
3  if ! lastCheck then
4  |  dateToCompare = recordDate
5  end if
   // satusList contains all EPP status codes found
      in the current WHOIS record
6  if (pendingDelete ∉ satusList) &
     (redemptionPeriod ∉ satusList) &
     (autorenewPeriod ∉ satusList) then
7  |  if Hold || serverHold || clientHold ∈ satusList
   |    then
8  |  |  if dateToCompare < expDate then
9  |  |  |  if clienthold ∈ statusList & (UpdateDate
   |  |  |    is one year less than ExpirationDate ||
   |  |  |    UpdateDate is within 15 days of
   |  |  |    creationDate) then
10 |  |  |  |  delisted = False
11 |  |  |  |  note = "most likely due to auto
   |  |  |  |    renewal, or WHOIS verification"
12 |  |  |  else
13 |  |  |  |  delisted = True
14 |  |  |  end if
15 |  |  end if
16 |  end if
17 end if
```

up in the set of sinkholed domains discovered using the PDNS. If the domain was put on hold after being sinkholed, then its taken-down duration was extended until the expiration date of its WHOIS record.

IV. Analyzing Take-down Operations

In this section we discuss our new findings and understanding, based on analyzing the lifecycles of the 625,692 seized domains identified in our research and the security weaknesses in leading take-down parties.

A. Landscape

In total, we discovered 625,692 seized domains using the methodologies introduced in Section III. The number of confirmed sinkholed domains was 608,557 (96.55%), and the number of delisted domains was 21,757 (3.45%). Figure 5 illustrates the overlap between blacklisted, sinkholed, and delisted domains. As we can see here, 0.7% of the domains were sinkholed first and then delisted. Also, 5.6% of the domains on public blacklists were sinkholed, and 3.68% were placed on hold.

As mentioned earlier, domain take-down is often used for disrupting botnet C&C, where the seized domains are usually generated by domain generation algorithms (DGAs) [53]. Therefore, we identified the DGA domains in our seized domain list to measure the prevalence of take-down actions against C&C domains. Specifically, we utilized a DGA detection tool [7] that measures the randomness of domain characters, which reported 405,330 (64.78%) such domains in our dataset. The presence of the large number of DGA domains does not come as a surprise, as in take-down actions there

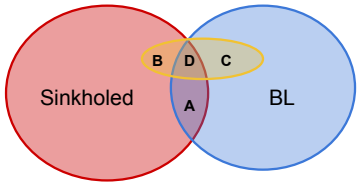


Fig. 5: Intersection between sinkholed, blacklisted (BL) and delisted domains. A (sinkholed ∩ BL): 35,045 domains; D (sinkholed ∩ BL ∩ delisted): 193 domains; B (sinkholed ∩ delisted): 4,429 domains; C (BL ∩ delisted): 17,135 domains.

is a tendency to seize (through preemptively registering) all possible domains once the DGA is reverse engineered.

B. Understanding Sinkhole Operations

We also investigated sinkhole operations more closely, given their importance in the whole take-down procedure (more than 97% of the domain seizure performed through sinkholing).

Preemptive actions. Take-down parties sometimes preemptively seize some domains that are more likely to be involved in cybercrimes before they are actually used by the malicious actors. Most of such domains are DGA domains that take-down parties reverse-engineered to identify all possible domains that a bot may connect to in the future. Once these domains are found, they are sinkholed before being used maliciously.

We identified preemptively sinkholed domains by checking the PDNS records. Specifically, if the first record of a domain points to a sinkhole, this indicates that the domain is captured at the very beginning of its lifecycle. Therefore, it is considered to be a possible preemptive domain seizure. We found 388,378 such domains in our dataset. However, due to the bounded history of PDNS data (the earliest record found in our data set was on 2010-04-09), this method incorrectly classified the domains that were maliciously active and then sinkholed sometime earlier in 2010 as preemptively captured. To address this issue, we utilized the domain's historical webpage snapshots from the Wayback machine [18]. We collected the snapshots of 5,296 domains found to be sinkholed from day one in our dataset. Nine turned out to have snapshots in the Wayback Machine before the earliest appearance in PDNS and therefore were dropped from our preemptive seizure list.

Ultimately, out of the 608,557 confirmed sinkholed domains, we found that 388,369 (63.81%) were preemptively taken down. We then utilized the DGA domain detection tool [7] to analyze these domains, which revealed that 92% of them were indeed generated by DGAs. We randomly sampled the remaining 8% of the domains (i.e. non-DGA domains but preemptively taken-down), and found that they were actually DGA domains but were misclassified by the tool as non-DGA. We present the percentage of preemptive actions against malicious domains per sinkhole operator and TLD registries (top 15 most frequent TLDs in our dataset) in Figures 6a and 6b, respectively. We observed that the percentage of preemptive actions taken by Microsoft, the FBI, and Shadowserver was high, as more than 90% of their sinkholed domains were due to preemptive actions. This could be due to their involvement in taking down pervasive campaigns, such as ZeuS and Conficker [5, 15]. Such campaigns led to preemptively registering a large set of DGA domains that were expected to be contacted by such campaigns. In addition, these reputable take-down actors might have managed to get the

registration fee waived [5, 55] and therefore did not have financial restrictions to register a very large set of domains. With regards to preemptive actions in different TLDs, `.cn`, `.in`, `.me`, and `.name` acted preemptively on more that 90% of the domains. This might indicate their high level of responsiveness towards notices and court orders.

Active duration. We defined the active duration of a domain as the timespan from its first appearance in the PDNS until the moment when it was found to be sinkholed. This duration reveals the intervention of different parties in the domain take-down action. To measure this duration accurately, we excluded the preemptively sinkholed domains, as they did not have active durations.

Figure 7a shows the distribution of the sinkholed domains' active durations by different operators in a box plot, where the box is the interquartile range (IQR) from the first quartile to the third quartile, which contains 50% of the data that reside around the median. The horizontal line in the box indicates the median value, and the × denotes the average. As illustrated in the figure, NameCheap and GoDaddy tend to intervene relatively quickly (indicated by the low median), which is expected because they operate as registrars so they can immediately act on complaints or take-down orders. Similarly, we observe that Spamhaus, which detects spam-related activities, reacts quickly, with 75% of the domains taken down in less than 100 days. However, apparently, the sinkhole operators for security companies/organizations vary in their response time in taking down malicious domains. For example, domains sinkholed by Arbor have longer active duration compared to Spamhaus.

Moreover, we found in our dataset that the FBI sinkholed around 2,000 domains (non-preemptively). Among them, 718 were active for a long duration ($\geq$ three years), shifting the distribution up as shown in Figure 7a. We randomly sampled 200 domains to examine their properties and found that the majority of them are pharmaceutical domains. This might indicate that these types of domains are less likely to be reported compared to other types of malicious domains, such as the ones involved in malware distribution, and child abuse.

Figure 7b illustrates the distributions over the active durations for the TLDs with the most sinkholed domains. As we can see here, almost half of the TLDs, such as `.biz`, `.info`, `.link`, `.pw`, `.work`, and `.xyz`, appeared to intervene quickly which might indicate fast response to take-down requests and court orders, as demonstrated by their corresponding medians that tend to be very low and IQRs that tend to be very narrow. The short active time of domains that belongs to these TLDs could be due to their involvement of notorious campaigns that required immediate actions.

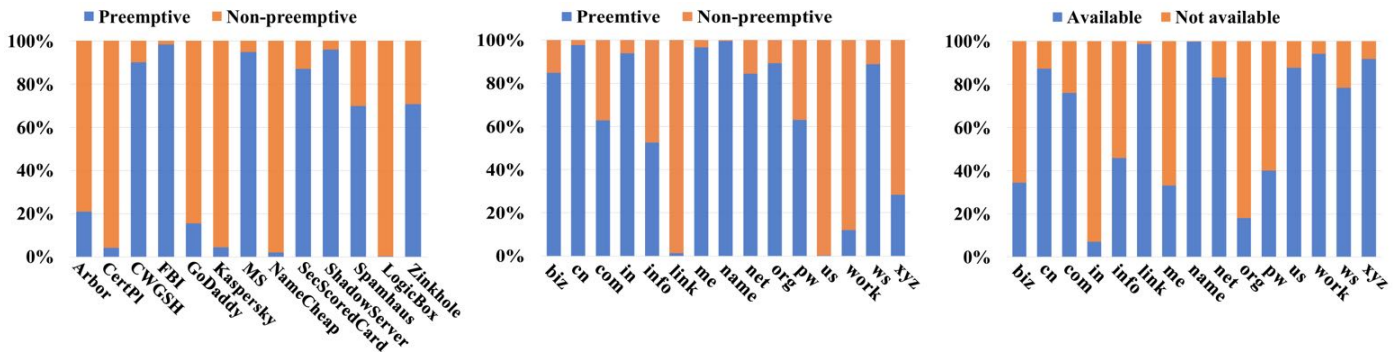
Sinkhole duration. The distributions of domains' sinkhole durations by each operator is shown in Figure 8a. We can see that the majority of the domains sinkholed by the registrars (e.g., GoDaddy and NameCheap) tended to have a relatively short sinkhole duration. Based on their third quartiles, we found that these domains rarely remained sinkholed beyond a year. We observed the transferring of some domains from registrars' sinkholes to other operators', such as the FBI. This will result in a short sinkhole duration at the registrars. This indicates that some sinkhole operators may reach out to the registrar first and file a request until the legalization logistics were completed.

We also observed that domains taken down by Microsoft or the FBI tended to be sinkholed for a long time (as shown by the high medians of their distributions). This could be due to their ability to provide compelling evidence when preparing take-down orders for court. For instance, Microsoft may have the incentive to sinkhole long-lasting campaigns against their products for a longer duration and could convince the court by providing the number of affected users as an evidence. Similarly, the FBI tended to keep domains that violate copyrights for a long time, such as megaupload.com. This appears to be a preventive measure taken by the FBI to prevent malicious actors from gaining control of the domain. Moreover, similar to our justification for the high percentage of preemptive actions taken by these two operators, financial reasons might also play a role in long sinkhole durations.

We also observed variations in the sinkholing durations. On one hand, some operators have relatively consistent sinkholing durations. For example, the IQRs of Shadowserver, SecurityScorecard, Kaspersky, Spamhaus, and Zinkhole are narrow, which might indicate that these operators have uniform polices that they apply to most of their sinkholed domains. On the other hand, we observed a large variation in this duration for the FBI and Microsoft sinkholes. This could be related to the type of malicious activity the domains were involved in. Specifically, domains involved in long-lasting campaigns get long sinkhole durations, whereas domains that no longer pose harm get released sooner. Another possible explanation is that the variation is due to external factors, such as registries policies, discussed next.

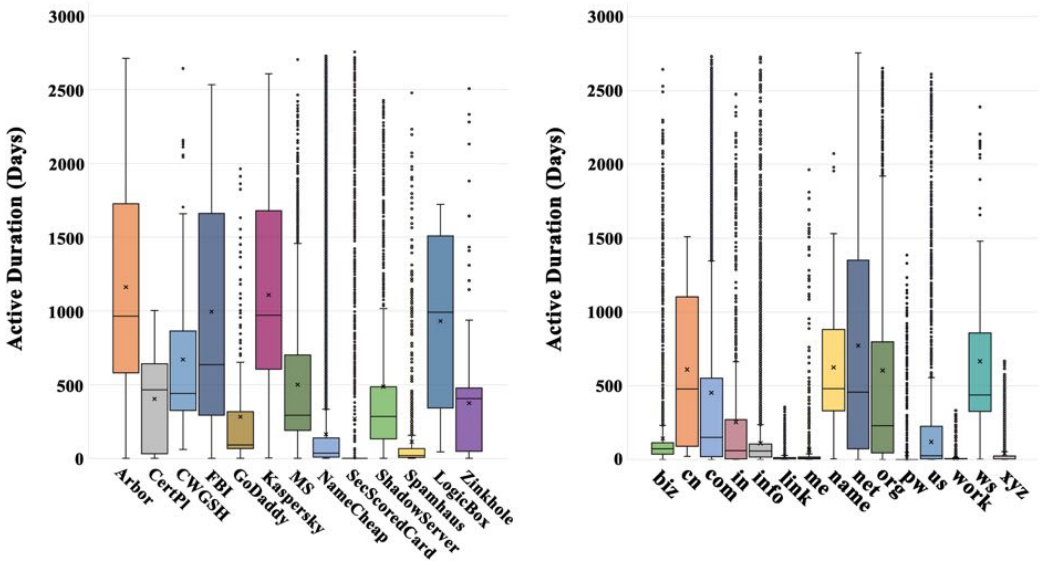
Figure 8b shows the distributions of sinkhole durations by the different TLDs. In general, most of the domains under `.org`, `.info`, `.biz`, and `.ws` have long sinkhole durations compared to the rest of the TLDs, as illustrated by their corresponding third quartile that expands on relatively high durations (on average about two years). This could indicate that the take-down duration of these domains was enforced by these registries' policy. For instance, the tendency of `.org` domains to be sinkholed for long durations agrees with the policy of `.org` registry, according to which it holds the domain until a further court order [27]. We also observed an interesting security practice applied by `.biz` registry in which a malicious domain was held in their reserved set. For example, the domain 4rme78bhg4bb3c64fw.biz was initially taken down by the FBI. However, even after it expired and the PENDINGDELETE duration passed, the registry kept this domain in their reserved set instead of releasing it to the public. This strategy is recommended for the most vicious domains to prevent them from being re-registered and abused.

Sinkhole hopping. From the analysis of sinkholed domains' lifecycles, we found that 4,418 domains were sinkholed more than once. Around 70% of them were sinkholed by the same sinkhole operator. This case could be occurring due to the expiration of the domain followed by a re-registration or other reasons, such as the "visibility" of PDNS. To estimate the cases of re-registration, we calculated the time between the two sinkholing actions based on the last seen date of the first sinkholing action and the first seen date of the second sinkholing action. We call this the release duration. If this time is more than 75 days, it could indicate that it is a new registration. We found that 340 domains seem to be re-registered domains, with an average release time of 237.5 days.



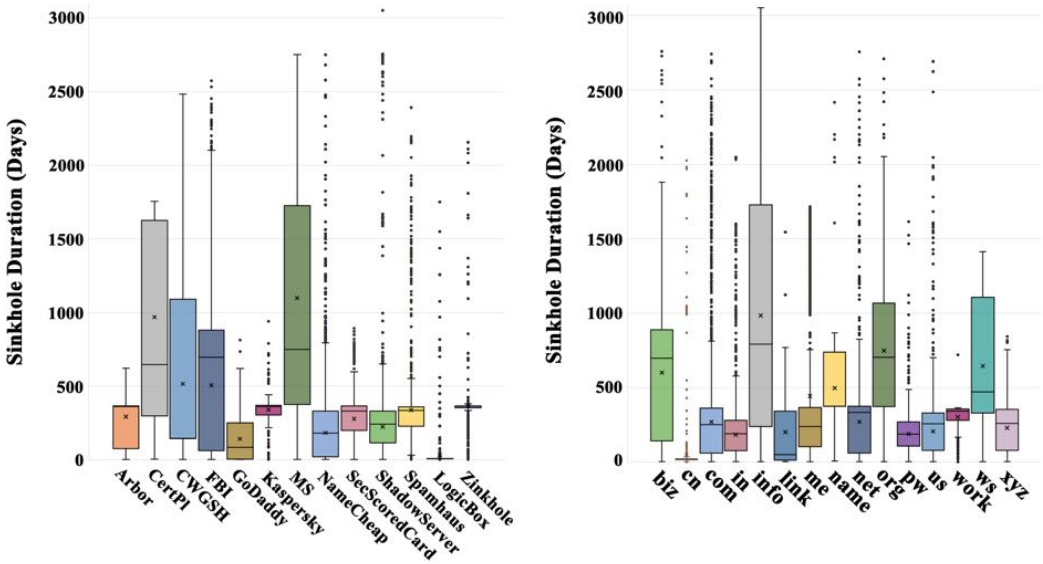
(a) **Preemptive actions by sinkhole operator.** (b) **Preemptive actions by TLD.** (c) **Availability by TLD.**

Fig. 6: Preemptive action and domain availability.



(a) **Active duration by sinkhole operator.** (b) **Active duration for the top 15 TLDs.**

Fig. 7: Active duration. The × denotes the average and the horizontal line denotes the median.



(a) **Sinkhole duration by sinkhole operator.** (b) **Sinkhole duration for the top 15 TLDs.**

Fig. 8: Sinkhole duration. The × denotes the average and the horizontal line denotes the median.

Although less prevalent, we observed that around 1,360 domains were seized more than once by different sinkhole operators. We looked into these "hopping" domains and observed that around 200 of them were suspended by GoDaddy and then by NameCheap. About 10% of these domains had a release duration of less than 75 days, suggesting that GoDaddy may have immediately deleted the domains and the adversary re-registered it. It could be also that the adversary managed to transfer the domains to another registrar and resumed his malicious activities until being sinkholed by the new registrar again. Moreover, we found 10 domains first sinkholed by the Conficker Working Group (CWG) [4] then by the NameCheap sinkhole. The average length of their release durations is around one year. As these domains appeared to be DGA domains and were sinkholed by the CWG, it might indicate that the adversary is interested in the domains related to old campaigns. This is true given that we exclude the case of name collision in which the new registrant happens to register a name matching a DGA domain.

Another explanation for the "hopping" between sinkholes is that a domain was released prematurely from the first sinkhole when it was still posing security risks, so it got sinkholed again by another sinkhole operator. For example, we found that around 300 domains hopped from Spamhaus to Microsoft, Shadowserver, or Arbor Networks. As illustrated in Figure 8a, 50% of the domains sinkholed by Spamhaus were sinkholed for less than 400 days, which may indicate that the second operator believed these domains still posed risks and decided to sinkhole them again. Another possible reason is that the operator of the second sinkhole wanted to control the traffic and assess the damage, inform the ISP of the infected host, or download scripts to disrupt the malware on the infected host.

C. Exploits during Take-down Operation

The sinkhole nameserver plays a critical role in the domain take-down procedure as it hosts a large amount of sinkholed domains. Therefore, the nameserver is expected to be stable, reliable, and also well managed. However, we identified two misconfiguration issues in real-world servers that led to a less effective take-down operations.

Dangling sinkhole. A dangling DNS record is a DNS record that points to "stale" information. Specifically, a dangling record is a DNS record (e.g., `NS`, `A`) that points to a service that is no longer assigned to the domain's owner [48, 59]. This could open an avenue for a domain hijacking attack in which the adversary manages to take over the stale resource and thus manipulate the name resolving process. In our research, we found this security risk in a sinkholed domain. The misconfiguration allowed the adversary to hijack the sinkholed domain by setting the `A` record to an IP address he/she controlled. We reported this issue to the domain's TLD registry.

Specifically, we found that a law enforcement agency utilized a managed DNS service provided by Amazon (i.e., Amazon Route 53). This service was used to manage DNS records of a malicious domain carders.org as part of a take-down operation. The DNS configuration of the domain during seizure is shown in Figure 9. Later, when the law enforcement's account at the DNS service was deactivated, Amazon Route 53 released the record sets to the available pool. However, the domain's `NS` records on the (`.org`) TLD zone were still pointing to the previous values provided by the

```
first seen in zone: 2012-06-27
last seen in zone:  2018-07-22
rrtype:     NS
rdata:      ns-9.awsdns-01.com.
            ns-922.awsdns-51.net.
            ns-1168.awsdns-18.org.
            ns-1876.awsdns-42.co.uk.
first seen: 2012-06-26
last seen:  2013-01-05
rrtype:     A
rdata:      204.236.228.238
```

Fig. 9: The PDNS records for carders.org (`NS` and `A`). The `NS` record is still set at .org TLD, even though the account at Route 53 was deactivated (i.e., dandling `NS`).

```
carders.org.        NS   ns-1601.awsdns-08.co.uk.
                    NS   ns-1168.awsdns-18.org.
                    NS   ns-762.awsdns-31.net.
                    NS   ns-226.awsdns-28.com.

www.carders.org.    A    8.188.96.3
carders.org.        A    ALIAS www.carders.org.
```

Fig. 10: Our takeover of carders.org exploiting the dangling `NS` record and setting a new `A` record. The set IP address points to our webserver.

DNS service. As a result, the `NS` record became a dangling record because it was not removed from the (`.org`) TLD zone by the domain's owner (i.e., the take-down party). So, once the adversary obtained at least one of the nameservers' values that were set for the taken-down domain, he/she could set a new `A` record and assign it to an IP that he/she controlled. As a result, the adversary could capture all the domain's traffic through the IP he/she chose.

We observed such a problem in a domain that was taken down by the FBI (i.e., carders.org). We successfully hijacked the domain and pointed it to an IP under our control. This domain was first identified by checking domains seized by the FBI that also utilized a managed DNS provider, such as Amazon Route 53. As mentioned in Section III-A, we collected a list of domains owned by the FBI by performing a reverse WHOIS lookup on the FBI's email. We then checked if any domain was resolved through a managed DNS provider and found one domain carders.org that utilized Amazon Route 53. As shown in Figure 9, when sinkholed on 2012-06-27 [34], carders.org was revolved by four nameservers provided by Amazon Route 53. These records were still appearing in the (`.org`) TLD zone. Also, as shown in the figure, the last seen timestamp of the domain's `A` record is 2013-01-05, and no further `A` records are seen after early 2013. Therefore, we further verified whether the hosted zone on Route 53 that manages carders.org is deactivated by querying the four nameservers using the `dig` utility. As a result, all queries returned `ServerFail`, which is an indicator that the account was deactivated. Thus, carders.org has dangling `NS` record set.

To prove that this dangling point could be controlled, we also used Amazon Route 53 to create a hosted zone for carders.org in the hope that at least one of the original domain's nameservers in Figure 9 would be assigned to us. After several attempts, we successfully acquired one such server on the `NS` record (i.e., `ns-1168.awsdns-18.org`) and set a new `A` record for carders.org to an IP under our control (18.188.96.3). Figure 10 shows the new `NS` and `A` records of carders.org.

We first reported this issue to the FBI (via `cyd-dns@ic.fbi.gov` found on WHOIS record retrieved

Domain	Re-registration Date	# of Domains	NS Activated?
ns.cwgsh.com	2011-05-15	88,392	Yes
ns.cwgsh.net	2012-02-22	59,359	Yes
	2015-10-01	59,359	Yes
ns.cwgsh.org	2012-03-01	29,677	Yes
	2014-07-22	29,677	Yes
	2015-08-26	29,677	No
	2016-11-26	29,677	Yes
	2018-02-14	29,677	Yes

TABLE III: Re-registration of cwgsh.{com,net,org} showing the number of domains resolved by the namservers after each re- registration.

on 2018-05-20). We did not hear back from them probably because the domain had expired already. Therefore, we reported the issue to the Public Interest Registry (`.org` TLD registry). We recommended that they address the problem by placing `ServerHold` on the domain, which they did on 2018-10-11.

Expired sinkhole. We found that some sinkhole nameservers' domains were allowed to expire without updating the `NS` record of the sinkholed domains. This allowed the adversary to purchase expired domains that were used as a nameserver sinkhole, set a nameserver on it, and then set `A` records for the sinkholed domains to point to IPs he/she controlled. Such changes are often stealthy, as the sinkhole operator may not continuously check whether these domains are still pointing to the sinkhole's IP, as they are supposed to be.

Our study brought to light the potential impacts of such a problem, particularly the one found in a major sinkhole operator, Conficker Working Group (CWG). CWG is a consortium formed to contain and take down the Conficker worm [4]. Its core members include Verisign (registry), Shadowserver Foundation, Neustar (registry), Microsoft, and others. The consortium used three nameservers (i.e., `ns.cwgsh.com`, `ns.cwgsh.net`, and `ns.cwgsh.org`) to sinkhole Conficker worm domains. However, these nameservers' own domains expired on 2011-02-26 and were re-registered multiple times, as shown in Table III. The new owners of these domains (i.e., cwgsh.com, cwgsh.net, and cwgsh.org) had full control over the traffic of thousands of Conficker domains that used to point to the sinkholes.

We studied the Conficker domains hosted on these three sinkhole nameservers. Originally, these nameservers were sinkholing 212K domains. After their domains expired, some seized domains they managed were moved to new sinkholes (i.e., `ns.conficker-sinkhole.{com,net,org}`) and some expired. However, 88,392 domains still used these three nameservers even after their expiration. Table III shows the number of the domains hosted on these three CWG sinkholes one day after the re-registration of cwgsh.{com,net,org} by new owners. Here, we calculated the number of the domains based on the `last_seen` and the `first_seen` dates reported by the PDNS, and identified whether an `A` record is set for `ns.cwgsh.{com,net,org}`, which suggests a potential attempt to capture the traffic of the seized domains. We also noticed that the IP address for the fourth re-registration of `ns.cwgsh.org` was pointing to 130.245.32.52 (State University of New York at Stony Brook), which may indicate that it was registered by a researcher.

It is not clear what exactly the new owners of the three domains have been doing with the traffic they receive from the seized domains. However, we observed that they are indeed actively utilizing some of them. For example, one of

```
www.zzyiwabmkz.info.    A    190.2.131.62
ww9.zzyiwabmkz.info.    A    166.78.101.108
```

Fig. 11: `A` records set for new subdomains of zzyiwabmkz.info observed in July 2018. After expiration of cwgsh.{com,net,org}.

```
aabdoeskhl.org.  NS  ns.cwgsh.com.
                 NS  ns.cwgsh.net.
                 NS  ns.cwgsh.org.
```

(a)

```
aabdoeskhl.org.  NS  ns.cwgsh.com.
                 NS  ns.cwgsh.net.
                 NS  ns.cwgsh.org.ns-not-in-service.org.
```

(b)

Fig. 12: Changes in `NS` record for aabdoeskhl.org (a) before and (b) after expiration of cwgsh.{com,net,org}.

the expired sinkhole domains' new owner set `A` records for new hosts he/she created under zzyiwabmkz.info (one of the sinkholed domains), as shown in Figure 11.

The most popular TLDs in these seized domains are `.org`, `.info`, and `.ws`. Interestingly, we observed that the `NS` records of all `.org` sinkholed domains were either updated to point to a new sinkhole, `ns.cwgsh.org.ns-not-in-service.org`, in about a month after the expiration of `ns.cwgsh.org`, or they expired. However, this particular update is not effective because the two expired sinkholes `ns.cwgsh.{com,net}` were still within the `NS` record set; an example is shown in Figure 12. A more effective update was performed on `.ws` domains several months after the expiration of the sinkholes. Specifically, `.ws` domains were set to be resolved by new sinkholes, `ns.conficker-sinkhole.{com,net,org}`. In contrast, as of July 1, 2018 no updates were performed on around 30K `.info` domains.

As of July 1, 2018, the total number of seized domains that are still pointing to the three expired sinkholes are 29,677, all belonging to the `.info` TLD. We reported this issue to Afilias [1], the `.info` TLD registry, and provided them the list of problematic domains. Although it is a good practice to sinkhole malicious domains as long as they pose a risk, when the domains of the sinkhole servers expire, this treatment could cause the seized domains to stay linked to the expired sinkhole domains for a long time. Therefore, sinkhole operators and registries are advised to maintain updated `NS` records for their seized domains, especially ones that are required to be taken-down for a long time.

V. Tracing Released Domains

In this section, we report on the malicious reuse of seized domains. We first measure the availability of previously taken-down domains for repurchasing after their release. We then reveal actual reuse cases of released domains.

A. Domain Availability

We first analyzed whether the taken-down domains in our dataset were available for purchase or not by querying a registrar (i.e., Dynadot [10]) via their API. This registrar supports a wide range of TLDs and has provided the availability information for around 95% of the taken-down domains in our dataset. We queried this API twice every week starting from October 2017 until May 2018 to monitor whether

these taken-down domains were on the market. We found that 350K domains (56.46%) of all the taken-down domains in the past six years have been released. Of these, 52.13% were DGA domains. More interestingly, we also found that 7,148 (14.14%) of the domains taken down in the past ten months have been released back to the public registry domain pools. This time span is regarded as short, as there is a low chance that infected hosts get cleaned during such a short duration [56]. In addition, domains that used to carry illicit activities can still have their customers back.

Looking at the percentage of all released domains in different TLDs (Figure 6c), we observed that `.org` and `.in` have less than 20% of their total taken-down domains available, followed by `.biz`, (34.51%) and `.me` (33.09%). The observation about `.org` aligns with our finding in Section IV-B, which shows that the `.org` TLD keeps the majority of their taken-down domains seized for a long time.

B. Malicious Reuse

We investigated whether the seized domains were abused again after they were purchased. However, we can not rely on historical blacklists to prove malicious reuse of taken-down domains due to the limited overlap between sinkholed domains and blacklists (see Section IV-A) [45]. Furthermore, blacklists contain not only released and reused domains but also sinkholed domains, making it impractical to prove the malicious reuse after the domain is released. Therefore, we have to resort to a more conservative approach.

To address this issue, we employed a set of heuristics to identify the confirmed abusive reuse of previously seized domains. Specifically, we first identified the domains that were sinkholed at least twice by different actors. For each of them, we marked the timespan between two sinkholed durations as its release duration. We then filtered domains in which their release duration was more than 75 days (which allowed for re-registering). Further, we checked whether these domains were indeed active during their release durations by checking the PDNS to find out whether they were assigned to IPs. In this way, we obtained 133 domains. To prove the malicious use for these domains, we checked the Wayback Machine [18] to see if it has historical snapshots of these domains and we found 28 domains that have snapshots. Further, we manually investigated their webpages' historical snapshots (28 domains' snapshots were available) to check their abusive behaviors during the calculated release duration. Thus, we found two confirmed cases, which are:

on-drugstore.com. This domain was seized three times. Before each seizure, the domain always hosted a website selling illicit pharmaceutical products. From historical WHOIS, we found that it was first taken down on 2008-12-07 and then moved to another registrar (i.e., NameCheap [24]) on 2009-03-01. Since then, the domain was active again. The second take-down occurred on 2010-06-07 when the domain was sinkholed by the registrar for at least 10 days based on historical WHOIS and PDNS. Then, the domain was dropped by the registrar and re-registered again on 2010-06-17 with another registrar (i.e., 101domain), based on historical WHOIS information. Then, the website was up and running. For the third and final time, the domain was taken down and sinkholed by law enforcement agencies, including the FBI, on 2017-03-16. Interestingly, its registrant email address appears to have remained the same since July 2007, which indicates that the domain was abused by the same operator during all the three seizures. Interestingly, we observed that this domain is a squatting domain for a reputable health and beauty care retailer, drugstore.com. Therefore, we believe the adversary kept tracing this domain because it was confusingly similar to a popular Internet brand that would attract large volume of traffic even after it was taken down three times.

ugnazi.com. This domain belongs to a hacktivist group. It was taken down by the FBI on 2012-06-26 [23] with its registrant information changed to the FBI. However, upon the domain's expiration, the registrant information went private, and the registrar was transferred from NameCheap [24] to Enom [30] based on historical WHOIS information. A snapshot of the website from the Wayback Machine on 2014-02-02 indicates that the domain was available for sale. On 2014-07-22, the record shows that the domain was repurchased by a group who claimed to be the original hacktivist group, and it is still running as of the date of writing this research.

VI. DISCUSSION

Domain take-down regulation. Our study uncovered shortcomings within the take-down procedures implemented today. We found that the sinkhole duration varies across different operators, as evident in Figure 8a. For example, Microsoft maintains an average take-down duration of three years, while registrars average one year. Further, delisting and releasing domains is operator specific and flawed in some cases such as domain hopping in Section IV-B. Lastly, outdated DNS configurations, such as deactivated accounts at cloud DNS services and expired nameserver domains, can lead to serious consequences, such as domain hijacking attacks where an attacker can takeover a sinkhole nameserver and subsequently control all domains using it. Unfortunately, other than the general guidelines provided by ICANN [55], there is no industry-wide regulation of these procedures allowing take-down authorities and executors to carry out a domain take-down as they see fit.

Based on our analysis of these take-down procedures, we recommend setting specific policies regulating them. These policies should address issues such as the update frequency of DNS settings, take-down duration, and release procedures. Here, we suggest several practices to consider.

Determining the duration of a domain take-down should take into account the nature of the malicious act the domain was involved in. The traffic that a domain receives should be factored into the decision to release the domain. When a domain is sinkholed, sinkhole operators should monitor the received traffic to determine when malicious traffic ceased to exist. Rezaeirad et al. [56] have designed a traffic analyzer to study sinkholed traffic which can be utilized further to determine when a domain is no longer receiving malicious traffic. This procedure is especially recommended for domains related to malware campaigns, such as C&C domains.

For other types of malicious domains, such as carding or pharmaceutical, we suggest considering three factors before releasing them. The first factor is the popularity of the malicious domain; popular malicious domains are more likely to be re-registered if they are released preemptively compared to unpopular ones. Another factor is the domain's current traffic; if the domain is still receiving traffic, then it gives an

indicator that it might resume its malicious activity if released and re-registered. The final and crucial factor is the degree of the domain's maliciousness; if the domain was involved in a serious criminal act, such as child abuse, then it is not wise to risk releasing it. This specific category of high-risk domains should be taken down indefinitely and never released back to the public. Technically, this could be performed by keeping these domains in the registries' list of `reserved` domains, which will prevent them from being available for purchase after their expiration. By taking these factors into account the domain holder can informally decide on the appropriate take-down duration.

Limitations. It is important to note that the take-down lifecycle (i.e., sinkhole duration and active duration) is limited by the "visibility" of PDNS. Therefore, if a domain's TLD is not within its daily feed list of supported TLDs zone set, the accuracy of a seized domain's lifecycle becomes dependent on the resolution requests for the domain. In other words, the accuracy of the duration depends on whether or not resolution requests occurred and consequently were captured by PDNS sensors.

Another limitation is that the algorithm in Section III-C might inaccurately label some domains due to the limited number of snapshots for each domain in our dataset. However, the proposed algorithm introduced less than 4% of domains to our analysis. Therefore, the effect on our study is minimal.

VII. Related Work

Study on domain take-downs. Previous works on domain take-down mainly focused on the effectiveness (in terms of the coverage of taken-down domains, malicious domain active duration, etc.) of the take-down procedures. Hutching et al. [42] conducted user interviews to reveal the expertise of different parties (e.g., law enforcement, take-down services) engaged in domain take-down. Moore et al. [51] studied the domain take-down speed for multiple types of cybercrime, such as phishing and child abuse. In particular, they examined the impact of domain take-down on phishing by analyzing the malicious active duration and the number of visitors [50]. They concluded that domain take-down can not completely mitigate phishing. Nadji et al. [53] investigated the malicious domain coverage of botnet take-down actions and proposed a system to identify the missed malicious domains during botnet take-down. Asghari et al. [39] analyzed logs of Conficker sinkholes and measured the effectiveness of the sinkholing effort carried against this botnet. Rezaeirad et al. [56] studied the victims of remote access trojans (RAT) by sinkholing RAT servers. Kuhrer et al. [45] investigated the effectiveness of malware blacklists by identifying the sinkhole servers in the blacklist. To the best of our knowledge, we conducted the first systematic study to provide a fine-grained view of the domain take-down procedure (e.g., sinkhole configuration, lifecycle) and have revealed multiple weaknesses of it.

DNS misconfiguration. Pappas et al. [54] revealed that DNS misconfiguration is widespread, which degrades the reliability of DNS. Jiang et al. [43] found that a malicious domain could remain resolvable due to the outdated data in upper-level DNS. Liu et al. [48] presented security threats related to dangling DNS records, such as domain hijacking. Vissers et al. [59] discussed possible scenarios in which the domain could be hijacked through their nameservers. Similarly, Borgolte et al. [40] showed a scenario for a temporary domain hijacking through their stale `A` records provided by cloud services. We investigated the DNS misconfiguration issue of sinkhole servers and its impact on the domain take-down procedure.

Domain abuse. Numerous studies have looked into abuse in the DNS ecosystem. Korczynski et al. [44] investigated abuse in the domains registered under the new gTLD. Visser et al. [60] studied the malicious campaigns in .eu TLD. Recently, some studies have investigated domain re-registration patterns and their relation to domain abuse. Hao et al. [41] found that spammers commonly re-register expired domains. Lauinger et al. [46] discussed domains' lifetime and showed the variations in how the duration of some stages is implemented differently by registrars. Moore et al. [52] found that failed bank websites have been re-registered and likely used for malicious purposes. Lever et al. [47] studied the maliciousness of re-registered domains after they expired and revealed their malicious behavior. Miramirkhani et al. [49] studied domain drop-catching services and found that there is a tendency to reuse malicious domains. In contrast to previous studies, our study revealed the maliciousness of take-down domain re-registration and explored its possible root causes.

VIII. Conclusion

This paper comprises the first systematic study on domain take-down to understand this process and investigate its security and reliability. We have highlighted the ability to utilize WHOIS information and PDNS data to determine taken-down domains and profile their take-down lifecycles. In analyzing 625,692 take-down domains and their lifecycles, our research sheds new light on the take-down operations and highlights security-critical observations about sinkhole operators. This helps in identifying a set of best practices important for avoiding the loopholes in these services and enhancing their effectiveness against cybercrime.

Acknowledgment

We thank our our shepherd Juan Caballero and the anonymous reviewers for their insightful comments and suggestions. This work was supported in part by National Science Foundation under grants CNS-1838083, 1801432, 1527141, 1618493, 1801365. Any opinions, findings, conclusions or recommendations expressed in this paper do not necessarily reflect the views of the NSF.

References

[1] "Afilias," https://afilias.info/.
[2] "Cert.at Conficker," http://www.cert.at/static/conficker/all_domains.txt.
[3] "Citadel Seizure Court Order," https://botnetlegalnotice.com/citadel/.
[4] "Conficker Working Group," http://www.Confickerworkinggroup.org.
[5] "Conficker working group lessons learned," http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.
[6] "Consolidated Malware Sinkhole List," https://tisiphone.net/2017/05/16/consolidated-malware-sinkhole-list/.
[7] "DGA Domain Detection using Bigram Frequency Analysis," https://github.com/philarkwright/DGA-Detection.
[8] "Domain Tools," https://www.domaintools.com/.
[9] "Dorkbot Seizure Court Order," https://botnetlegalnotice.com/dorkbot.
[10] "Dynadot," https://www.dynadot.com/.

[11] "Emerging Threat Rules," https://rules.emergingthreats.net/blockrules/.
[12] "EPP Status Codes," https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en.
[13] "Farsight Security," https://www.farsightsecurity.com/.
[14] "Feds Seized Hip-hop Site for a Year, Waiting for Proof of Infringement," https://www.wired.com/2012/05/weak-evidence-seizure/.
[15] "GameOver Zeus Botnet Disrupted," https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted/.
[16] "GoDaddy Report," https://supportcenter.godaddy.com/abusereport.
[17] "hpHosts," https://www.hosts-file.net.
[18] "Internet Archive," http://archive.org/.
[19] "Malc0de," https://www.malc0de.org/.
[20] "Malware Domain Blocklist," http://www.malwaredomains.com.
[21] "Malware Domain List," https://www.malwaredomainlist.com/.
[22] "Malware Sinkhole List," https://github.com/brakmic/Sinkholes.
[23] "Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce 24 Arrests in Eight Countries as Part of International Cyber Crime Takedown," https://archives.fbi.gov/archives/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown.
[24] "Namecheap," https://www.namecheap.com.
[25] "Network Security Research Lab at 360," http://www.netlab.360.com.
[26] "PhishTank," https://www.phishtank.com/.
[27] "Public Internet Registry Policies," https://pir.org/policies/ .
[28] "Ramnit Seizure Court Order," https://botnetlegalnotice.com/ramnit/.
[29] "Ransomware Tracker," https://ransomwaretracker.abuse.ch/.
[30] "Register Domains with Enom," https://www.enom.com.
[31] "Reports: Liberty Reserve Founder Arrested, Site Shuttered," https://krebsonsecurity.com/2013/05/reports-liberty-reserve-founder-arrested-site-shuttered/.
[32] "Shadowserver," https://www.shadowserver.org.
[33] "Shylock Seizure Court Order," https://botnetlegalnotice.com/shylock/.
[34] "Take Down Notices 2012," https://pir.org/policies/org-idn-policies/takedown-policy/tdn_2012/.
[35] "ZeroAccess Seizure Court Order," botnetlegalnotice.com/zeroaccess.
[36] "ZeuS Tracker," https://zeustracker.abuse.ch.
[37] "ZeuS Tracker Removal," https://zeustracker.abuse.ch/removals.php.
[38] "Avalanche Global Fraud Ring Dismantled," https://krebsonsecurity.com/2016/12/avalanche-global-fraud-ring-dismantled/.
[39] H. Asghari, M. Ciere, and M. J. Van Eeten, "Post-mortem of a zombie: Conficker cleanup after six years," in *USENIX Security Symposium*, 2015, pp. 1–16.
[40] K. Borgolte, T. Fiebig, S. Hao, C. Kruegel, and G. Vigna, "Cloud strife: mitigating the security risks of domain-validated certificates," in *Proceedings of Internet Society Symposium on Network and Distributed System Security (NDSS)*, 2018.
[41] S. Hao, M. Thomas, V. Paxson, N. Feamster, C. Kreibich, C. Grier, and S. Hollenbeck, "Understanding the domain registration behavior of spammers," in *Proceedings of the 2013 Conference on Internet Measurement Conference*. ACM, 2013.
[42] A. Hutchings, R. Clayton, and R. Anderson, "Taking down websites to prevent crime," in *2016 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2016, pp. 1–10.
[43] J. Jiang, J. Liang, K. Li, J. Li, H. Duan, and J. Wu, "Ghost domain names: Revoked yet still resolvable," 2012.
[44] M. Korczynski, M. Wullink, S. Tajalizadehkhoob, G. Moura, A. Noroozian, D. Bagley, and C. Hesselman, "Cybercrime after the sunrise: A statistical analysis of dns abuse in new gtlds," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. ACM, 2018, pp. 609–623.
[45] M. Kührer, C. Rossow, and T. Holz, "Paint it black: Evaluating the effectiveness of malware blacklists," in *International Workshop on Recent Advances in Intrusion Detection*. Springer, 2014.
[46] T. Lauinger, K. Onarlioglu, A. Chaabane, W. Robertson, and E. Kirda, "Whois lost in translation:(mis) understanding domain name expiration and re-registration," in *Proceedings of the 2016 Internet Measurement Conference*. ACM, 2016, pp. 247–253.
[47] C. Lever, R. Walls, Y. Nadji, D. Dagon, P. McDaniel, and M. Antonakakis, "Domain-z: 28 registrations later measuring the exploitation of residual trust in domains," in *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016.
[48] D. Liu, S. Hao, and H. Wang, "All your DNS records point to us: Understanding the security threats of dangling DNS records," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 1414–1425.
[49] 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 on World Wide Web*. International World Wide Web Conferences Steering Committee, 2018.
[50] T. Moore and R. Clayton, "Examining the impact of website take-down on phishing," in *Proceedings of the Anti-phishing Working Groups 2nd Annual eCrime Researchers Summit*. ACM, 2007, pp. 1–13.
[51] ——, "The impact of incentives on notice and take-down," in *Managing Information Risk and the Economics of Security*. Springer, 2009.
[52] ——, "The ghosts of banking past: Empirical analysis of closed bank websites," in *International Conference on Financial Cryptography and Data Security*. Springer, 2014.
[53] Y. Nadji, M. Antonakakis, R. Perdisci, D. Dagon, and W. Lee, "Beheading hydras: Performing effective botnet takedowns," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*. ACM, 2013, pp. 121–132.
[54] V. Pappas, Z. Xu, S. Lu, D. Massey, A. Terzis, and L. Zhang, "Impact of configuration errors on DNS robustness," in *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 4. ACM, 2004, pp. 319–330.
[55] D. Piscitello, "Guidance for Domain Name Orders," https://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf.
[56] M. Rezaeirad, B. Farinholt, H. Dharmdasani, P. Pearce, K. Levchenko, and D. McCoy, "Schrödingers rat: Profiling the stakeholders in the remote access trojan ecosystem," in *Proceedings of the 27th USENIX Security Symposium*, 2018.
[57] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, "Your botnet is my botnet: Analysis of a botnet takeover," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*. ACM, 2009.
[58] J. Szurdi, B. Kocso, G. Cseh, J. Spring, M. Felegyhazi, and C. Kanich, "The long "taile" of typosquatting domain names." in *USENIX Security Symposium*, 2014, pp. 191–206.
[59] T. Vissers, T. Barron, T. Van Goethem, W. Joosen, and N. Nikiforakis, "The wolf of name street: Hijacking domains through their nameservers," in *Proceedings of the Conference on Computer and Communications Security*. ACM, 2017.
[60] T. Vissers, J. Spooren, P. Agten, D. Jumpertz, P. Janssen, M. Van Wesemael, F. Piessens, W. Joosen, and L. Desmet, "Exploring the ecosystem of malicious domain registrations in the .eu TLD," in *International Symposium on Research in Attacks, Intrusions, and Defenses*. Springer, 2017, pp. 472–493.