International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org
Vol. 10 Issue 12, December -2020,
ISSN (O): 2249-3905, ISSN(P): 2349-6525 | Impact Factor: 7.196 |

Collabera: An EPP based Consolidated Framework for Re-Registration of Malicious Domains

Adhirath Kapoor[1],

Model Institute of Engineering & Technology,

Jammu City, J&K, India

Asil Stanikzai[2],

DEFEND Ltd.,

Auckland Central, Auckland, New Zealand

Salim Raza Qureshi[3],

Model Institute of Engineering & Technology,

Jammu City, J&K, India

Anirudhra Gupta[4]

Model Institute of Engineering & Technology,

Jammu City, J&K, India

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org
Vol. 10 Issue 12, December -2020,
ISSN (O): 2249-3905, ISSN(P): 2349-6525 | Impact Factor: 7.196 |

Abstract

With the digital progression, most of the industries have shifted their modus-operandi to digital work environments. This transition has made it easier for the masses to make the most use of the Work-from-Home model of operation. Technology is more accessible than ever. This has also led to an increased percentage in the cyber attacks worldwide. Cyber criminals are wreaking havoc all over the world through distribution of dangerous malware via exploitation of domains. Botnet Attacks are also being carried out via misapplication of domains. A major practice applied to mitigate the problem of domain exploitation is Sink-holing and is used to redirect the malicious traffic to the honeypot servers. However, as the evidence suggests, threat actors can gain the control back once the domain expires. There is a lot of literature available that deals with the study of Sinkholes and Domain Re-registration separately, but there is not any that visualizes both as one single research expedition. Hence, we propose a novel framework called Collabera that can be followed by registries worldwide for re-registration of sink-holed domains.

Keywords: Malware, Domain Registry, Sink-holing, Honeypot, Re-registration, DNS.

INTRODUCTION

With the progression of technology, the masses using the internet can now access information from any corner of the world. The seamlessness provided to the internet users is marvelous in its entirety. But there exists another genre of individuals that are on the quest to exploit everyone, ranging from regular users to highly advanced infrastructures and sectors like Healthcare and Military. Different attacks are being carried out by malicious actors in order to compromise highly critical user information. Criminals aim to bring down extremely advanced infrastructures through the acts of malware distribution and botnet attacks. In the recent years, attackers have been trying to exploit domains or websites so as to carry out illegal operations. These activities come into notice of Law Enforcement agencies, who then issue warrants for seizure of domains. This leads to the process of Domain take-down which is used to stop the criminals from further abusing the domain. Take-down sometimes involves redirection of traffic to a honeypot server maintained by the take-down operator. This helps in analyzing the C&C botnet behavior. There

can be some other cases where the take-down operator might even delist the domain so that it becomes unresolvable.

The main aim of a domain take-down is to halt the operations of the domain being maliciously used by the threat actors and confiscate it until it is sanitized and testified as a regular domain again. Anyhow, take-down operations are not feasible to implement because of the challenges they face. These challenges render the whole take-down process ineffective and can lead to criminals regaining access to the domains even if they are under custody. These challenges arise due to lack of a consolidated architecture which would monitor all the confiscated domains and prevent the criminals from gaining back access to the domains. The problem statement that arises from this situation is that even though the domains are confiscated or delisted by the Take-Down parties, somehow the attackers find ways to be able to use the domain again once its expiry date draws near. Once the domain expires, irrespective of being confiscated or unconfiscated, it is automatically placed in the Available Domain Lists and becomes obtainable for buying again. This time gap becomes a very huge problem for the Domain Take-down operators and erodes the effectiveness of the whole take-down operation. Many threat actors have abused this time gap and have been successful in resuming their halted operations. Some have even been able to abuse the vulnerabilities in the honeypots and redirect the traffic according to their own needs.

Existing works in the literature have studied sink-holing and the act of delisting incongruously and have proposed various frameworks. The main aim of these works was evaluate the effectiveness of sink-holing through a technical standpoint, but did not mention anything regarding the problem that arises after expiry and during re-registration of domains that have been sink-holed. (Alowaisheq et al., 2019) in their article carried out a detailed study of blacklists as well as sink-holed feeds in order to analyze the process of their formation. The authors brought out a very significant point through which a malicious domain was sink-holed. The sink-holing process involves manipulation of its Name Server's NS records as well as A records. (Kim et al., 2013) presented a novel framework for increasing the efficacy of the sink-holing operation via the method of double bouncing of e-mails. The authors also stated that their framework was extremely quick in pinpointing malicious URLs and blacklisting them. (Liu et

al., 2011) carried out an experiment in which real-time URI Blacklists were used along with their WHOIS records to delineate the role played by Domain Registrars in putting an halt to illicit ventures occurring on a domain. (Lever et al., 2016) created an algorithm known as Alembic, which automated the process of domain monitoring and could easily locate the negative trust numbers mapped to a domain. Alembic reduced the human effort required to put different domains in Available Domain Lists. (Lauinger et al., 2016) wrote a survey-based article on the complete operation of Domain expiry and Re-registration. The authors shed light on the real-world problems that arise due to the time gap between expiry and re-registration, thus creating complications during the process of re-registration. (Kidmose et al., 2018) developed a framework consisting of a heuristics-based filter to create a list of malicious domains. The filter-based system was created in order to reduce the manual effort to track down such domains so as to clean them before putting them up for sale.

Our research paper extensively looks at the operations that take place during Domain Registration, Domain Expiry and Domain Re-registration respectively and understand them from three different point of views. These views can be inferred from the perspectives of Registrar, Registry and the Sink-hole operators. We also conduct a study of different transfer secrets generated by Domain Registrars, also known as Extensible Provisioning Protocol (EPP) codes. EPP codes help in creating a better understanding of Domain Registration and Re-registration. We then propose a unique framework called Collabera that will lay down a set of rules along with algorithms that a registry needs to adhere to before making a decision regarding the placement of a domain present in the Sink-holed feed into the Available Domains List. After conducting an extensive research, we found that there is no co-ordination between the Sink-hole operators and the Domain Registrars so as to make a collective decision on when a malicious domain can be placed in the Available Domains List again. The only time they co-ordinate with each other is when the Sink-hole operator requests the Registrar to redirect the Malicious URL to their own honeypot servers for analyzing the C2C behavior. A Registrar's interest is making revenue and is not concerned with the content being published on the domains. Collabera ensures

that a domain goes through certain checkpoints in order to remove the negative trust associated with it.

RELEVANT LITERATURE

(Alowaisheq et al., 2019) were the first authors to study and analyze the process of domain take-down along with its effectiveness. The authors carefully surveyed sink-hole feeds and Domain Blacklists which are crested through the operations of Sink-holing and Domain Delisting respectively. The authors also proposed a recommendation-based system through the use of WHOIS database along with Passive DNS data lists. This recommendation system was able to evaluate and improve the sink-holing operation. This was the first research work that technically delineated both Sink-holing and Delisting. The authors also carried out a study of locked-out domains. Locked-out domains are the ones that get ejected from their Top-Level Domain Registry. In addition to the work highlighted above, the authors created an algorithm that could locate the seized domains from a database of sink-holed as well as blacklisted domains. Certain operations like reverse PowerDNS and WHOIS lookups were performed on the database to extract the seized domains. The reason for performing these two lookups simultaneously is that PowerDNS lookups quickly locate sink-holed domains while WHOIS lookups easily find domains that are delisted. The authors, after evaluating the effectiveness of the operations concluded that most of the sink-holed domains were running Botnet based C2C servers. They also touched base on dangling sinkholes. Our framework extricates all the major concepts explained in this article. Detailed information on DNS and EPP codes is delineated in the article and thus helped us in building Collabera. While the article's gist was finding out the duration of activity in the malicious domain and shortcomings in the sink-holing process, our framework focuses on what happens after sink-holing.

(Lever et al., 2016) carried out a detailed study on how malicious activities can affect the trust associated with a domain. This trust, in real scenarios, does not come into play when a malicious domain is due for re-registration. Threat actors can easily exploit the domains with negative trust values for C2C operations. Thus, this lays a ground for malicious domains falling into the hands of cyber criminals after their expiry. So, the authors devised a framework known as Alembic. It

was able to monitor and keep track of domain transfers. This led the authors to create a trail of domain's trust exploitation as well. The algorithm was backed by a successful experimentation using malware infected network traffic samples. Collabera is similar to Alembic in a sense that they both act as solutions for the problem of re-registration of domains associated with negative trust. Alembic sought to solve the problem by tracing the domain back to its owner while Collabera will be able to solve the problem as it will used by the governing bodies included in the process.

(Kidmose et al., 2018) gave an overview of the adversary techniques that can exploit the DNS system. The authors first extracted the set of malicious domains via heuristics-based methods. In this article, the authors made a significant contribution; a heuristics-based domain ranking framework. The framework would decrease the human effort required for the creation of the same. The heuristics-based framework was created using the Levenshtein distance. The framework was successful in practice as the authors were able to identify five domains that were used for malicious purposes. The identification also led to the discovery a lot of parameters that could eventually automate the complete functioning of the framework. In the framework, lower rank meant lower degree of abuse. The main shortcoming of this work that the framework could not be ported to the re-registration process.

(Kim et al., 2013) in their article, focused on the sink-holing process and illustrated its significance in the domain of cyber-threat intelligence. Sink-holing is very effective in extracting malware samples and their signatures as well as understanding the botnet behavior in C2C servers. The authors created a method of enhancing the security of sink-holing operations via usage double bouncing e-mails. This method extracted URLs from double bouncing mails to create a blacklist consisting of malicious domains. With this technique, the authors claimed that hostile actions of cyber-criminals would be detected quickly. Collabera takes inspiration from this article as we also recommend creation of a list of sink-holed domains that would be monitored by the registry on a continuous basis.

(Liu et al., 2011) carried out a study on the major parties involved in the sink-holing process. They claimed that the Registrars play an important role due to their intermediatory nature. The

authors also studied how domains can be used as tools for carrying out scam operations worldwide. The input dataset used real-time URI blacklists and WHOIS records to fetch domains with cases of spam-advertising. The paper was more policy based rather than technical and reported two major certitudes. Actions of scammers were dependent on the prices of domains. Also, with easy registration process involved in changing registrars and domains, spammers can easily buy a new domain after the previous one is shut down. The authors argued for a global price increase to avoid such scenarios. The authors also discussed tools like Legit Script, which was written to identify spamming websites. The authors touched base on a global level engagement via different parties. Collabera extends the concept put forward by this paper and aims to create a global level intercession via Registries, Registrars and Sink-holing parties.

(Lauinger et al., 2016) carried out an experimental study for a better understanding of the complete cycle of registration to re-registration. They studied the expiration process in detail as well. Throughout the paper, they identified some problems in WHOIS that can be exploited by malicious actors of technology. Thus, as a solution, the authors created a framework for Domain Discovery which would specifically monitor and trace the history of domains which were due to be deleted in the Domain Name System Zone files. They also discussed some discrepancies resulting from erroneous use of EPP codes which would leave a domain in an undefined state. This paper helped us understand EPP codes in a detailed manner, so that we would not make the same mistakes in designing Collabera. The paper also analyzed the Re-registration process using Kaplan Meir as a set of statistical values. Collabera also makes use of the knowledge shared in this paper regarding the common formats that need to be adopted for re-registration.

PROPOSED IDEA

In order to create our own framework as a solution to the problem statement described in the first section, it is essential to get acquainted with the different timeline-based operations namely Domain Registration, Sink-holing, Expiry and Re-registration.

There are three major entities that are involved in all the operations, starting from Registration till the process of Re-registration. They are Domain Registrant (buyer), Domain Registry and

Domain Registrar (Intermediator). A Registry is the supreme governing body when it comes to domain management and is responsible for formation, renewal and disbandment of domains. It also keeps a centralized directory for the Top-Level Domains. A registrant is a buyer of the domain and is the one who demands for the creation of a domain. A registry acts like an intermediator between the above two. It accepts the requests from the registrant and then passes those to the Registry to resolve those requests. The requests can be varying in nature. They can be for the creation of a domain, renewal of a domain, extension for a specific time period, etc.

As alluded to in the first section, Sink-holing refers to the whole operation of redirection of malicious traffic on a domain to a honeypot server to analyze the malware or botnet-based traffic. There are a few entities related to the DNS Protocol that need to be understood for carrying out a study on Domain Sink-holing. These are NS and A records. A Name Server Record is used to denote the name of the Authoritative Name Server. The Authoritative Name Server contains the actual DNS records for a particular domain. An A Record maps a domain to it IP address and is used to perform reverse and forward lookups for a domain. An essential understanding of these two records helped us create our own framework. We also studied the WHOIS protocol in a detailed manner. WHOIS is used for retrieval of information from a global database that contains the details of all the registered domains. WHOIS further uses Extensible Provision Protocol (EPP) which consists of different server and client codes. A server code is used by the registries and is used to describe properties of a domain from the Registry's perspective. A Client code is used by the registrars and assesses the domain from a Registrar's point of view. In TABLE - 1, the different server and client codes are explained.

TABLE – 1. Different EPP Codes

Code	Set by	Level	Description
auto-Renew-Period	Registry	Registry	When activated, Grace period is given to the domain which is about to expire.

client-Hold	Registrar	Registrar	When activated, sets the domain into an unresolvable mode.
server-Hold	Registry	Registry	When activated, puts the domain into an inactive mode in the DNS.
server-Renew-Prohibited	Registry	Registry	When activated, Registry asserts its authority over the Registrar and bars it from extending the renewal period of the domain.
client-Renew-Prohibited	Registrar	Registrar	When activated, Registrar asserts its authority over the Registry and bars it from extending the renewal period of the domain.
server-Transfer-Prohibited	Registry	Registry	When activated, no other Registrar can take over the selected domain.
client-Transfer-Prohibited	Registrar	Registrar	When activated, it will order the registry to forbid the shifting of the domain.
server-Update-Prohibited	Registry	Registry	When activated, domain will be locked and will not receive any DNS based updates.

The figure below explains the complete process of Sink-holing. After a complete investigation, the Law Enforcement agencies or Cyber Security engineers forward the logs along with the complete case description to the Takedown operators. The Takedown operators, in order to redirect the traffic to their honeypot servers, make a request to the Registry via the Registrar handing that domain. The redirection is performed via manipulation of NS and A records to that of the honeypot sink-holing server.

As a part of our research, we dug deep into finding out the technical details of the complete process as well as the governing bodies. We found out that due to no co-ordination between the

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org
Vol. 10 Issue 12, December -2020,
ISSN (O): 2249-3905, ISSN(P): 2349-6525 | Impact Factor: 7.196 |

Registrars, Registries and the Sink-hole operators, criminals can easily gain access back to the sink-holed domains, thus rendering the whole process inefficacious. One of the major reasons for this is due to the default auto-enabling feature of the EPP code, auto-Renew-Period. Auto-Renew-Period grants domain a grace period and then automatically feeds it as an input into the Available Domains list.

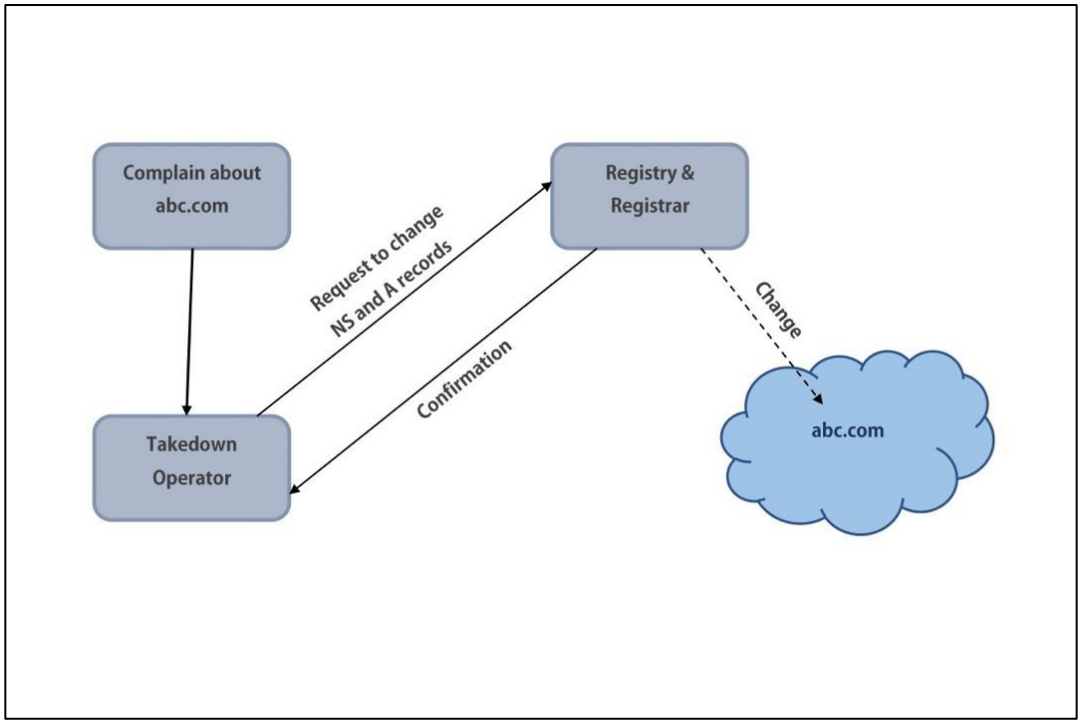

Fig-1: Interaction between different parties during Sink-holing Operation

Our paper aims to create a consolidated framework called Collabera, which as the name suggests, will ensure that malicious sink-holed domains will not fall again into the hands of threat actors after expiration date. Collabera has been created after a very detailed study of significant Server-based EPP codes. Collabera uses those codes to warrant the complete transition of a sink-holed domain from a blacklist to an Available Domains List. It will also ensure a good co-ordination between the parties involved so that proper decision making is guaranteed. Before diving deep into the working of Collabera, we will again highlight the issues that made it necessary for us to devise our own framework. The first issue was that the involved

parties, Registry, Registrar and the Sink-hole operators had no understanding regarding the timeline that would be used for removing the negative trust associated with the malicious domain. Collabera lays emphasis on such a timeline through which the trust will be manipulated for the sink-holed domain.

The second issue sheds light on the EPP codes that are enabled by default and act as a loophole for the malicious actors to exploit and regain control of C2C servers running on the sink-holed domains. Thus, the auto-Renew EPP code plays a significant role as its correct activation/deactivation can ensure the smooth transition of a domain from a sink-holed list to an Available domains list.

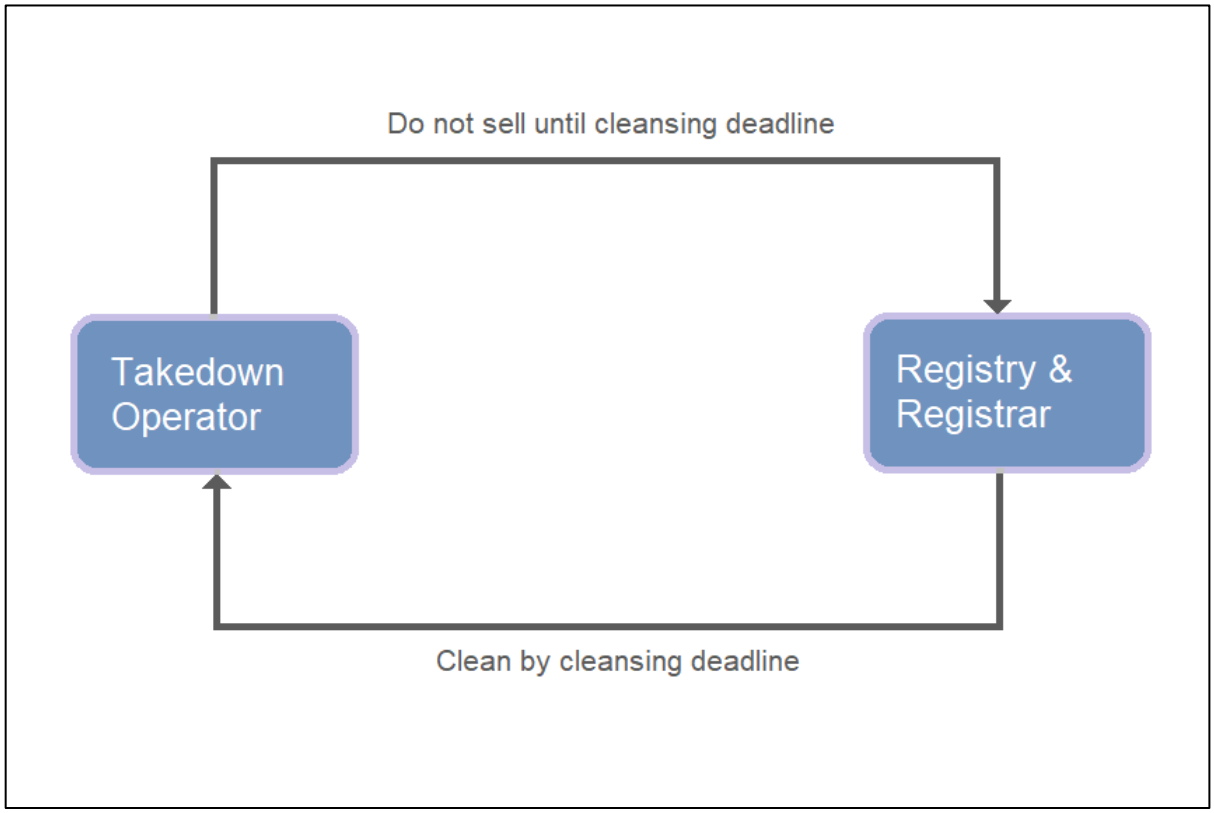

Fig-2: Collabera's Overview

Fig-2 gives an overview of Collabera. This aims to maintain complete collaboration between the two major parties. Collabera's complete working details are explained in Fig-3. After an investigation request for a malicious domain is issued, Take-down operative will issue a request for modification of DNS records and will have NS and A values changed to that of the honeypot server. The request for modification is handled by the Registrar first and then the final decision regarding it is made by the Registry. Registry will then make a note of the domain in consideration and not put it in the Available Domains List even after its expiry. For ensuring this, the concept of cleaning deadline will come into play and a check will be enforced which will see if the modification date of NS and A values is kept on or after the cleaning deadline has passed. This also means that the sink-hole operator must complete all the security and behavioral analysis of the domain before the set deadline and remove the negative trust associated with it. The registry will also have to comply with this and not place the domain in Available Domains list unless and until its purification deadline has passed.

As seen in Fig-3, the registry will put every domain through this framework that is about to expire, and it will be up for sale soon. The first check will be to find out if the domain has been sink-holed. If it has not been sink-holed, it will be put inside Available Domains List.

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org
Vol. 10 Issue 12, December -2020,
ISSN (O): 2249-3905, ISSN(P): 2349-6525 | Impact Factor: 7.196 |

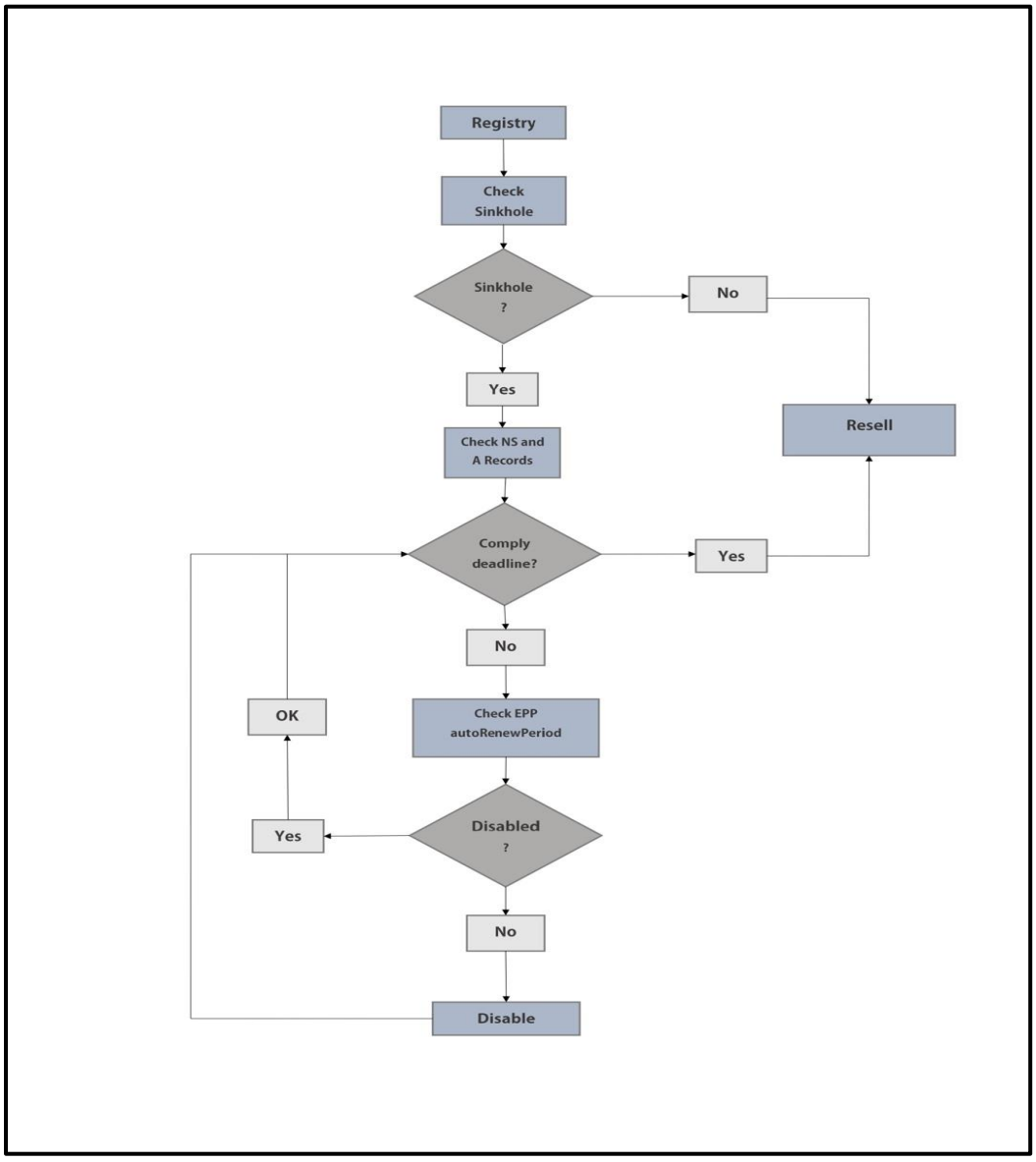

Fig-3: Flowchart for Collabera's operation

In the other case, if a domain has been sink-holed, it then goes through the second check where its DNS based records, NS and A will be checked for the date of modification. After this modification date has been recorded, it will then be compared with the set deadline for removing negative trust. It is to be noted that this deadline has been set after a very careful consideration by the Registry, Registrar as well as the Sink-hole operator. Now, after the comparison, there can

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org
Vol. 10 Issue 12, December -2020,
ISSN (O): 2249-3905, ISSN(P): 2349-6525 | Impact Factor: 7.196 |

be two possible scenarios. The first scenario is where the cleaning operation has been performed and has adhered to the set deadline. In this case, the domain again gets fed into the Available Domains List. The second scenario is quite different from the first one because here the deadline has not been complied with and thus, auto-Renew-Period should be checked. If it is enabled, it should immediately be disabled. After disabling the EPP code, the domain should go through an exhaustive process of cleaning again. Rest of the details are well-explained in the flowchart and it can be used for re-iterations as well. We have also created Collabera algorithm for the Registries, Registrars and Sink-hole operators worldwide to adhere to. This is explained in Fig-4.

```
1 sinkhole list
2 IF(DOMAIN_NAME != List [i])
  THEN
3 RESELL DOMIAN_NAME //
4 ELSE IF
5     DOMIAN_NAME EXPIRY_DATE < CLEANSING_DEADLINE
      THEN
6     CHECK autoRenewPeriod
7         IF(autoRenewPeriod == DISABLED)
          NO_ACTION
8         ELSE
          SET autoRenewPeriod == Disabled
9 ELSE
  GOTO 3
```

Fig-4: Algorithm for Collabera

CASE STUDY

With Collabera being completely novel in nature, we believe that if we include a short case study closely related to the problem statement, it will emphasize the need to adopt Collabera or any other similar framework in the future. Most of the sink-hole operators are concerned with analyzing the activity occurring in the sink-holed domains. After a careful examination of the traffic and extraction of entities' signatures that can help in building better security solutions, they do not barge in again and let the Registry and the Registrar handle the further processes. This marks the end of collaboration in the scenarios we have studied till now. Coming down to scenarios, we shift our focus to the most dangerous Ransomware attack ever created, WannaCry.

WannaCry0, the first strand of the Ransomware was stopped via DNS sink-holing. When the domain was about to expire, it was straight away placed into the Available Domains List without any collaboration between the registry and the sink-holing parties. Even though, the signature for WannaCry0 was extracted to mitigate the damage created by it, the threat actors were able to regain control and launch updated versions of WannaCry with signature evasion techniques.

We are in no position to criticize the methodologies adopted for WannaCry's sink-holing, but we strongly believe that if there was a better co-ordination between the involved parties after analysis of the domain, the cyber-criminals would not be able to regain control and re-launch the malware again. We think that even the strongest policies can fail if there are loopholes in their practical implementation. That is why, Collabera can lead to better enforcement and strict checking during reselling of domains.

CONCLUSION

To recapitulate the paper, we studied two major operations- The sink-holing process and the domain management process. These were studied exhaustively and hence, challenges and problems arising in and from these operations were identified. It was found that EPP codes play a significant role in domain management. Auto-Renew-Period, being activated by default, automatically extends the life of an expiring domain and then, after some time, puts it into the Available Domains List. The code's default behavior has proven to be a loophole, thus, leading the criminals to regain control of the sink-holed domains.

In the paper, we also shed light on the in-coordination between the governing bodies, which renders the sink-holing process ineffective. So, we proposed and created an algorithm called Collabera for which a major pre-requisite is setting up a deadline for removing negative trust associated with a domain. After the deadline has been set up, Collabera will make it mandatory for the governing bodies to run the domain through a series of checks, so that reselling of malicious domains does not lead to problems again. In Collabera, it is necessary to adhere to the deadline, so that the output results in a domain with neutral or positive trust. As we proposed a collaboration between the governing bodies in order to create error-free policies, we will soon

conduct another study to find limitations of the real-world policies currently in practice. We will also conduct an experimental study for comparing sink-holing and delisting using real test-cases.

REFERENCES

Alowaisheq, E., Wang, P., Alrwais, S., Liao, X., Wang, X., Alowaisheq, T., Mi, X., Tang, S., & Liu, B. (2019). *Cracking the Wall of Confinement: Understanding and Analyzing Malicious Domain Take-downs*. https://doi.org/10.14722/ndss.2019.23243

Kidmose, E., Lansing, E., Brandbyge, S., & Myrup Pedersen, J. (2018). Heuristic Methods for Efficient Identification of Abusive Domain Names. *International Journal on Cyber Situational Awareness*. https://doi.org/10.22619/ijcsa.2018.100123

Kim, H. S., Choi, S. S., & Song, J. (2013). A methodology for multipurpose DNS sinkhole analyzing double bounce emails. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-42054-2_76

Lauinger, T., Onarlioglu, K., Chaabane, A., Robertson, W., & Kirda, E. (2016). WHOIS lost in translation: (Mis)Understanding domain name expiration and re-registration. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*. https://doi.org/10.1145/2987443.2987463

Lever, C., Walls, R., Nadji, Y., Dagon, D., McDaniel, P., & Antonakakis, M. (2016). Domain-Z: 28 Registrations Later. *IEEE S&P*, *i*. https://doi.org/10.1109/SP.2016.47

Liu, H., Levchenko, K., Félegyházi, M., Kreibich, C., Maier, G., Voelker, G. M., & Savage, S. (2011). On the effects of registrar level intervention. *Usenix Large-Scale Exploits and Emergent Threats*.