サブドメインテイクオーバー攻撃の脆弱性検知ツール『SDHJChecker』

茨城県立IT未来高等学校 3年次
Ko:Hack; 大庭 悠希

1. 研究背景

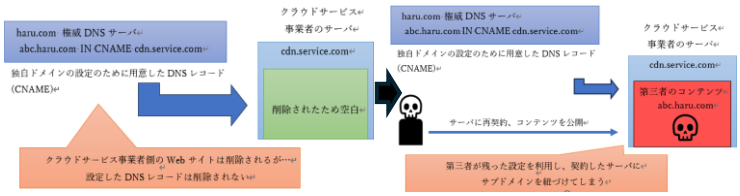
・2025年1月14日にサブドメインテイクオーバー攻撃により政府機関ドメイン(go.jp)でオンラインカジノに誘導する広告サイトを開設していた事案が確認された。[1]
・この攻撃への対策は、管理者がクラウドサービスとの契約期間及びDNSレコードの利用状況といった目視による確認作業が必要になり、負担となっている。
・CLIベースの脆弱性検知ツールは存在するが、対象となるクラウドサービスの網羅が難しく、普及していない。
・この攻撃を知らない人でも簡単に扱え、あらゆるクラウドサービスを網羅する脆弱性検知ツールが求められている。

2. 研究目的

(1) 簡単に扱えるサブドメインテイクオーバー攻撃の脆弱性検知ツールの開発
(2) 権威DNSサーバに組み込むための脆弱性検知機能のライブラリの作成

3. サブドメインテイクオーバーとは?

・クラウドサービスを独自ドメインで利用する際に設定したDNSレコードをクラウドサービス解約後もDNSレコードを削除せず放置したことにより第三者が悪用しサブドメインを乗っ取る攻撃です。
⇒第三者が不正にサブドメインを扱えてフィッシングページ等を公開できる



設定したDNSレコードはクラウドサービス解約後も削除されない
放置されたDNSレコードを用いて攻撃者がクラウドサービスに再契約
(JPRSの記事を参考に作成[2])

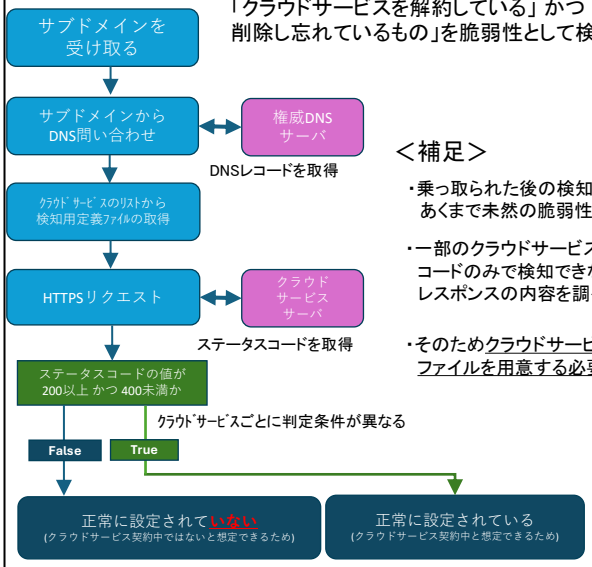
・有償のサブドメインテイクオーバー攻撃対策ツールは存在しない。
・無償の対策ツールはあるが、対応の網羅性やサポート体制から普及していない。
⇒対策は人力による管理の徹底にとどまってしまっている。

4. 「SDHJChecker」の特徴

subjack[3]やsubzy[4]などの既存ツールとの違い
・CLI 及びWebツールとして提供している。
・利用者から対応ｸﾗｳﾄﾞｻｰﾋﾞｽ追加リクエストを受け取り、対応ｸﾗｳﾄﾞｻｰﾋﾞｽを自動的に追加する機能が存在する。
・検知機能をJavaのライブラリとして利用することが可能であり、既存アプリに組み込めるといった拡張性がある。
・このライブラリを活用し、Webツールを新たに作成した。

5. 検知方法

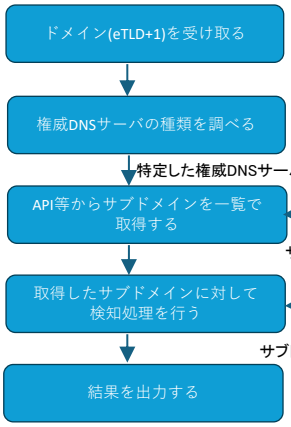
「クラウドサービスを解約している」かつ「DNSレコードを削除し忘れているもの」を脆弱性として検知する。



＜補足＞
・乗っ取られた後の検知は不可能である。あくまで未然の脆弱性検知のみに対応
・一部のクラウドサービスはステータスコードのみで検知できないため、レスポンスの内容を調べて検知する。
・そのためクラウドサービスごとに検知用定義ファイルを用意する必要がある。

6. Webツールの機能【新規追加】

簡単に扱えるサブドメインテイクオーバー攻撃の脆弱性検知ツールとして、Webツールを制作した。
・DNSの仕様上、ドメイン(eTLD+1)に含まれるサブドメインを特定することができない。
・CLIツールでは、ドメイン(eTLD+1)全体を一括検知ができず、一つ一つサブドメインを入力するのが手間となっていた。
⇒Webツール版では独自機能としてドメイン(eTLD+1)を入力することでドメイン(eTLD+1)に含まれる全てのサブドメインを一括検知できる機能を作成した。



＜補足＞
・ドメイン(eTLD+1)に含まれるサブドメインを特定する方法は権威DNSサーバによって異なる。
・現時点ではCloudflareの権威DNSサーバにのみ対応している。

＜使用方法＞

開発したWebツール:https://sdhjweb.onrender.com

入力画面

検知結果

サブドメイン	RecordType	Record 作成日時	判定対象か	判定結果
badstatusrender.tkue.net	CNAME	2025-08-27T01:01:25.899821Z	○	危険(削除する必要有り)
githubpages.tkue.net	CNAME	2025-08-27T01:37:07.942161Z	○	正常
goodrender.tkue.net	CNAME	2025-08-27T00:49:59.483081Z	○	正常
verceltest.tkue.net	CNAME	2025-08-27T00:54:34.281969Z	○	正常

7. まとめ

・簡単に扱えるサブドメインテイクオーバー攻撃の脆弱性を検知できるWebツールは完成した。
・検知機能本体のJavaのライブラリ化に成功していることが確認できた。
・今のWebツール上では脆弱性が存在するDNSレコードの削除を行えない。
・現状対応しているドメイン(eTLD+1)の一括検知機能は、Cloudflareで管理しているもののみに対応している。

8. 今後の目標

・対応しているクラウドサービス数を有償のものを含めて増やし、利便性を向上させたい。
・継続的にCLI及びWebツールに機能追加やデバッグなどの改善を施していきたい。
・実際の権威DNSサーバへの組み込みなどを実施して、より汎用性を高めていきたい。
・攻撃者側の利用といった想定外の利用への対処方法も考慮して、脆弱性検知ツールの開発を続けていきたい。

9. 参考文献

[1] 日経 Xtech (掲載日2025年2月26日)
政府機関の「go.jp」を使うWebサイトを第三者が設置、設定ミスを突く悪用手口
https://xtech.nikkei.com/atcl/nxt/column/18/00001/10169
[2] サブドメインテイクオーバー JPRS (参照日 2025年10月29日)
https://jprs.jp/glossary/index.php?ID=0267
[3] subjack GithubRepository hacker (参照日 2025年10月29日)
https://github.com/haccer/subjack/tree/master
[4] subzy GithubRepository PentestPad (参照日 2025年10月29日)
https://github.com/PentestPad/subzy
[5]第二回全国情報教育コンテスト 大庭悠希 (発表日2025年04月03日)
https://youtu.be/XXcJuRf6rRU

10. ソースコード

SDHJChecker(CLI・ライブラリ)
https://github.com/HaruTkue/The_Check_SDHJ

SDHJChecker(Web)
https://github.com/HaruTkue/SDHJCheckerWebEdition