ドメイン名ハイジャックされないために

其田 学
DNSOPS.JP

DNSOPS.jp
DNS Operators Group, Japan

本日のゴール

- ドメイン名登録者の方々
  - ドメイン名の保護、顧客の保護の方法について知る。
  - そして、レジストラ選択の重要性を理解する。
- レジストラの方々
  - ドメイン名を守るために必要な機能を知る。

自己紹介

其田　学(Manabu Sonoda)

- IIJでDNS業務全般やってます。
- 個人的に複数のドメイン名を管理しているのと、複数のレジストラを使ってるのでお鉢が回って来ました
- 今回の発表は会社は関係ないです。。

ドメイン名に対する攻撃

ドメイン名に対する攻撃 – 分類

- ドメイン名ハイジャック
  - 攻撃者にドメイン名がトランスファーされてしまい、管理権限を乗っ取られること。
- ネームサーバハイジャック
  - ドメイン名のネームサーバ情報が書き換えられてゾーンが乗っ取られること
- 経路ハイジャックなどのMITM
  - ネームサーバのIPアドレスが乗っ取られてゾーンが乗っ取られること
- キャッシュポイズニング
  - フルリゾルバのキャッシュに偽の情報をキャッシュさせ、偽応答をスタブリゾルバに変えさせること

ドメイン名に対する攻撃 – 分類

・ドメイン名ハイジャック

・攻撃者にドメイン名がトランスファーされてしまい、管理権限を乗っ取られること

今回はこの部分をドメイン名ハイジャックとして扱います

・ネームサーバハイジャック

・ドメイン名のネームサーバ情報が書き換えられてゾーンが乗っ取られること

今回はスコープ外

ドメイン名に対する攻撃 – 歴史

- ２０１２年ー２０１４年頃
  - 攻撃者による示威行為が主流
  - 政治的、宗教的なメッセージの書き換え、転送など

ドメイン名に対する攻撃 – 事例
ieドメインの不正書き換え

２０１２年１０月にyahoo.ieやgoogle.ieがドメイン名ハイジャックされ
トランスファーされてしまった事件

レジストリが使用していたCMS Joomlaの脆弱性を突かれて発生

レジストリがやられたら登録者としてはどうしようもない。

セキュリティのしっかりしたレジストリのドメイン名を使用しましょう。

ドメイン名に対する攻撃 – 事例
国内サイトのドメイン名ハイジャック

２０１４年９月から１０月にかけて、nikkei.comやはてなブックマークに不正なNSレコードが追加され、マルウェアの注入を図ったと思われる事件

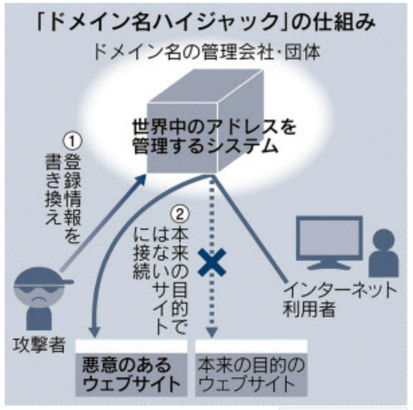
インターネットの根幹の仕組みに攻撃、本社も対象に

2014/11/5付

保存 共有 印刷 その他

インターネット上の住所であるアドレス（ドメイン名）を管理する仕組みがサイバー攻撃を受けたことが分かった。「～・ｃｏｍ」のアドレスを利用する一部企業のサイトを閲覧した場合、異なるサイトにつながるように仕組まれていた。ネットの安全情報をまとめる社団法人、ＪＰＣＥＲＴコーディネーションセンター（東京・千代田）は５日、ネットの根幹を揺るがしかねない問題として企業などに注意喚起を始めた。

今回の攻撃は「ドメイン名ハイジャック」と呼ばれる手法。世界中のアドレスを集中管理するシステムを狙い、企業などに「～・ｃｏｍ」を割り当てる米国の管理会社などに不正アクセスしてアドレス情報を書き換えた疑いがある。目的のサイトを閲覧しようとした利用者は気付かないうちにコンピューターウイルスなどが仕込まれた別のサイトに誘導される恐れがあった。



攻撃は９月から10月にかけてあったとさ

引用元）https://www.nikkei.com/article/DGXLASDZ05H3S_V01C14A1000000/

レジストリのネームサーバ情報が不正に書き換えられ、ゾーンが一部のっとられ、マルウェア配布サイトに誘導

ドメイン名に対する攻撃 – 歴史

２０１５年ー現在

- 金銭目的の攻撃主流
  - 広告の差し替え
  - 仮想通貨の盗難
- 攻撃手法
  - レジストリ情報の不正書き換え
    （なりすまし攻撃が非常に多い）

ドメイン名に対する攻撃 – 最近の主な事例

2014年11月	gigya.com	レジストリの登録情報の不正書き換え（登録者になりすまし）
2017年9月	fox-it.com	レジストリの登録情報の不正書き換え（登録者になりすまし）
2017年10月	coinhive.com	DNSプロバイダの設定内容の不正書き換え
2017年12月	etherdelta.com	レジストリの登録情報の不正書き換え（登録者になりすまし）
2018年4月	myetherwallet.com	Amazon Route 53の権威DNSサーバーの経路をBGPハイジャック

ドメイン名に対する攻撃 – なりすまし攻撃

いつもお世話になっております。●●Jサポートセンターです。

お客様のご登録いただいておりますドメイン名 example.jpについて

登録者情報の更新をお願いしております。

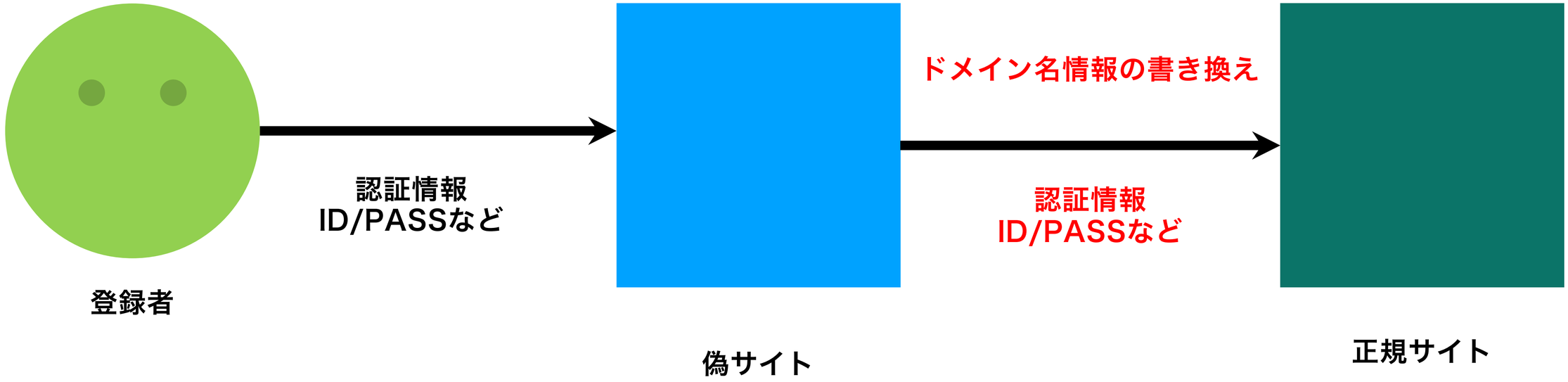
更新していただけない場合、レジストリの規定に基づきドメイン名が利用停止になる恐れがございます。

ドメイン名情報の更新は下記URLより行えます。

https://●●j.jp/login

ご不明な点がございましたら、 ●●Jサポートセンタにお問い合わせください。

ドメイン名に対する攻撃 – なりすまし攻撃



ドメイン名に対する攻撃 – 被害

トランスファーに成功すると、管理者なので全てできます

- ドメイン名の移管
- ゾーンを書き換えて行う中間者攻撃
- TLS証明書の発行

ネームサーバが変更できると、ゾーン情報が書き換え可能になります

- ゾーンを書き換えて行う中間者攻撃
- TLS証明書の発行

ドメイン名に対する攻撃 – まとめ

- ドメイン名ハイジャックされると、WEBサイトを乗っ取られたり、通信を傍受されたり、サービス止められたりする。

- 最近増えてきているのは標的型攻撃による、コントロールパネルの管理権限の不正アクセス

- 特に価値があるドメイン名をお持ちのあなた
  あなたの認証情報は狙われています！

対策

コントロールパネルへの認証への対策

- 多要素認証
- コントロールパネルへのACL

情報書き換えに対する対策

- 管理画面のロック
- レジストリロック
- レジストラロック

コントロールパネルへの認証への対策

コントロールパネルへの認証への対策 - 多要素認証

- ID、パスワードに加えて、他の要素でも認証する方法で、単純にIDとパスワードが漏れてもログインできない
  - FIDO **なりすましサイト対策**
  - TLSクライアント証明書認証 **オフラインな多要素認証**

  - TOTP/HOTP **オフラインな多要素認証**
  - SMS認証

  - メール認証 **オンラインな多要素認証**

コントロールパネルへの認証への対策 - FIDO

- 公開鍵暗号方式を使った今後の認証のスタンダードになる（はず）の規格
- キーデバイス上にドメイン名毎に暗号化鍵、復号鍵を格納
- 認証するサーバに対して、復号化鍵を登録
- 認証時は、サーバから送られてきたチャレンジを暗号化して送り返すことで認証します。
- ドメイン名毎に鍵が作られるため、元サイトに似せた名前の「なりすましサイト」に対して効果があります。

コントロールパネルへの認証への対策
TLSクライアント証明書認証

- TLSクライアント証明書を用いて認証を行う。
- 日本だとJPNICとかJPRSが採用
- 証明書のライフサイクル管理が大変面倒
  （特に証明書を物理媒体でやり取りする場合）
- 秘密鍵がないとTLSセッションを張れないので、
  なりすましサイト経由で正規サイトをいじられることはない。

コントロールパネルへの認証への対策 - TOTP/HOTP

- ワンタイムパスワードや、時間によって変わるパスコードを入力させることで、認証する方式
- Google authenticatorとかIIJ SmartKeyとかのアプリケーションを使ったり、パスコード生成機を使ったりする。
- なりすましサイトには効果がない

コントロールパネルへの認証への対策 - SMS認証

- ID,パスワードでのログイン成功時に、SMSでワンタイムパスワードを送信し、追加認証する方式
- 携帯電話を持っていないと認証が通らない
- なりすましサイトには効果がない

コントロールパネルへの認証への対策 - メール認証

- ID,パスワードでのログイン成功時に、メールでワンタイムパスワードを送信し、追加認証する方式
- 無いよりはマシという感じ
- ドメイン名に依存しているので、BGPハイジャックとかでも乗っ取れてしまうので、これだけに頼るのは微妙
- メールが受信できるPCにマルウェアが感染した時点でアウト
- なりすましサイトには効果がない

コントロールパネルへの認証への対策 - ACL

- コントロールパネルにログインできるIPを制限することで、そのIP以外からのなりすまし攻撃を防ぐことが可能
- マルウェア感染などで、端末に侵入されたら効果はない

コントロールパネルへの認証への対策 -まとめ

- FIDOいいよ！！
- 最低でもTOTP/HOTPぐらいは対応したいところ。
  - 大手のレジストラはほぼ対応していると思う。

情報書き換えに対する対策

情報書き換えに対する対策 - 管理画面のロック

コントロールパネル上での情報変更をできなくする機能

- どうせ、登録者情報やネームサーバ情報は滅多と変更しない
- ロックしたままにしても特に問題ない

問題になるのは解除方法

- コントロールパネルだけで、解除できるロックにはなんの意味もない。
  推奨されるロック解除方法は、ドメイン名や、ゾーン情報に依存しない情報での認証。
  - コールバック認証（ただし連絡先の電話番号もロック対象）
  - 代表印あり、もしくは登録者の印鑑証明付きの押印がある書面による申請

情報書き換えに対する対策 - レジストラロック

- レジストラ上でトランスファー申請や情報変更申請を拒否する機能
- Whois情報のDomain Statusに状態が記載されている

名前	状態
clientTransferProhibited	トランスファー禁止
clientUpdateProhibited	ドメイン名情報変更禁止

情報書き換えに対する対策 - レジストリロック

- レジストリ上でトランスファー申請や情報変更申請を拒否する機能
- Whois情報のDomain Statusに状態が記載されている

名前	状態
serverTransferProhibited	トランスファー禁止
serverUpdateProhibited	ドメイン名情報変更禁止

情報書き換えに対する対策 - レジストリロックの解除の例

- 各レジストリによって様々
  - ベリサイン（com ,net ,tv ,cc）
    - レジストラが承認した人がベリサインに要求して、ベリサインがコールバックし、パスフレーズで認証
  - JPRS(.jp)
    - レジストラ（指定事業者）がJPRSに対してロック解除要求を出し、JPRSが指定事業者に電話確認する形。

いずれも事前に登録された電話番号でのコールバックが必要。

情報書き換えに対する対策 - レジストリロックの解除の例

- 登録者がレジストラを経由してロック解除を申請する場合
  登録者ーレジストラ間も同じレベルの認証が必要。

- コントロールパネルからコールバック認証なしで解除できるレベルでは
  レジストリロックは意味がない。

そもそも…

インターネット上で情報変更できない
レジストラであればいい？

- だいたいあってる！！
- だけど、そういう会社は小規模な場合が多く、システム化されておらず業務用PC内にレジストラとの認証情報などが入っている場合がある。
- その場合、そのPCが標的型攻撃の対象になったら終わるよね。。

情報書き換えに対する対策 – まとめ

- いろんなロックがあるけど、解除方法も重要
  - レジストラを選ぶときにはここも注意して選びましょう。
- 無いよりはマシなので、予算があれば積極的に使っていきましょう。

まとめ

- ドメイン名登録者はレジストリと特にレジストラのセキュリティ対策をよく見てドメイン名、レジストラを選びましょう。
- また、レジストラが提供しているセキュリティ機能を積極的に利用しましょう。
- 登録者情報などは常に最新にしましょう。
- レジストラは、顧客のドメイン名を保護するために常にセキュリティを見直しましょう。
    - FIDOイイヨ