10分でわかる幽霊ドメイン名…と浸透問題の関係

DNSOPS.JP BoF
2012年4月25日

森下 泰宏
@OrangeMorishita

幽霊ドメイン名とは？

- 2012年2月8日に中国・清華大学のHaixin Duan（段海新）氏らのグループが論文で報告
  - “Ghost Domain Names: Revoked Yet Still Resolvable”
- 親（上位）ゾーンにおける委任情報（NSレコード）の削除・変更後も長期にわたり、古い情報を参照させ続けるように仕向けることができる脆弱性
- 消える（見えなくなる）はずのものが残り続ける
  - Ghost Domain Name（幽霊ドメイン名）

何が起こるのか？

- フィッシングやボットネットの制御、マルウェアの伝播など、不正な目的で使われているドメイン名を強制的に使用不能にすることを妨害される（NS削除の妨害）
- 不正使用されているドメイン名を強制的に移転することを妨害される（NS強制変更の妨害）
- ドメイン名を新規登録したら、昔誰かが使っていて幽霊つき（昔の名前で出ています）だった

いずれも広域的には発生させづらいが、局所的（プロバイダ限定）には十分に発生させ得る

…これって「浸透問題」じゃないの？

- そう思ったあなたは鋭い！
- 幽霊ドメイン名
  - ドメイン名の持ち主が脆弱性を持つキャッシュDNSサーバーに対し攻撃をしかけ、古い権威DNSサーバーを使わせ続けるように仕向ける
- 浸透問題
  - ドメイン名の持ち主は新しい権威DNSサーバーの情報を参照してほしいのに、一部の古いキャッシュDNSサーバーが古い権威DNSサーバーを使い続けてしまう

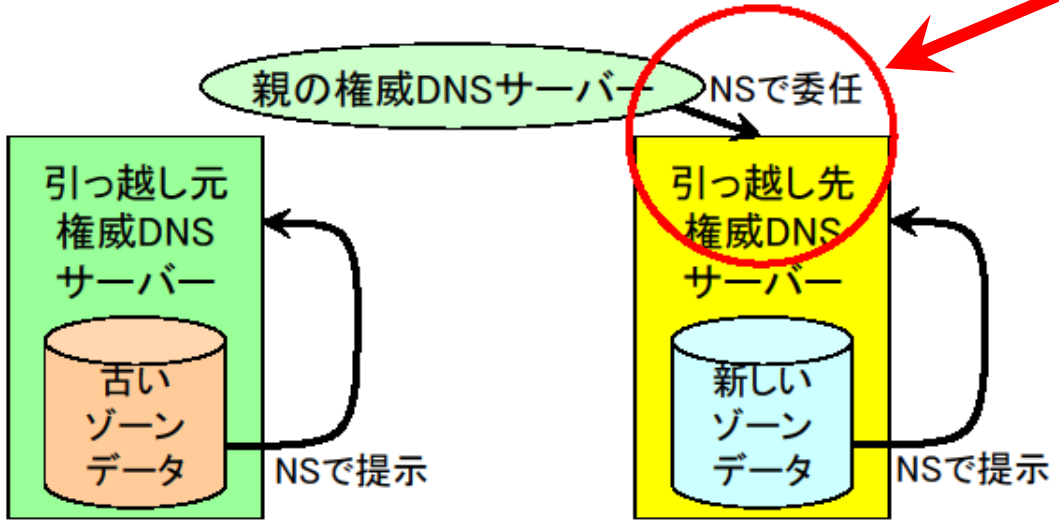
⇒つまり、結果として起こっていることは同じ！

浸透問題のおさらい

- Internet Week 2011ランチセミナー資料p.18より

浸透問題が起こりうる引っ越し方法

- 親のNSの切り替えだけを実施し、**引っ越し元の権威DNSサーバーの古いゾーンデータはそのまま**
- 実際の引っ越し（プロバイダの変更）でよくある形



これはまさに、「NS強制変更」ではないかっ！（海原雄山風に）

浸透問題と幽霊ドメイン名は同じもの？

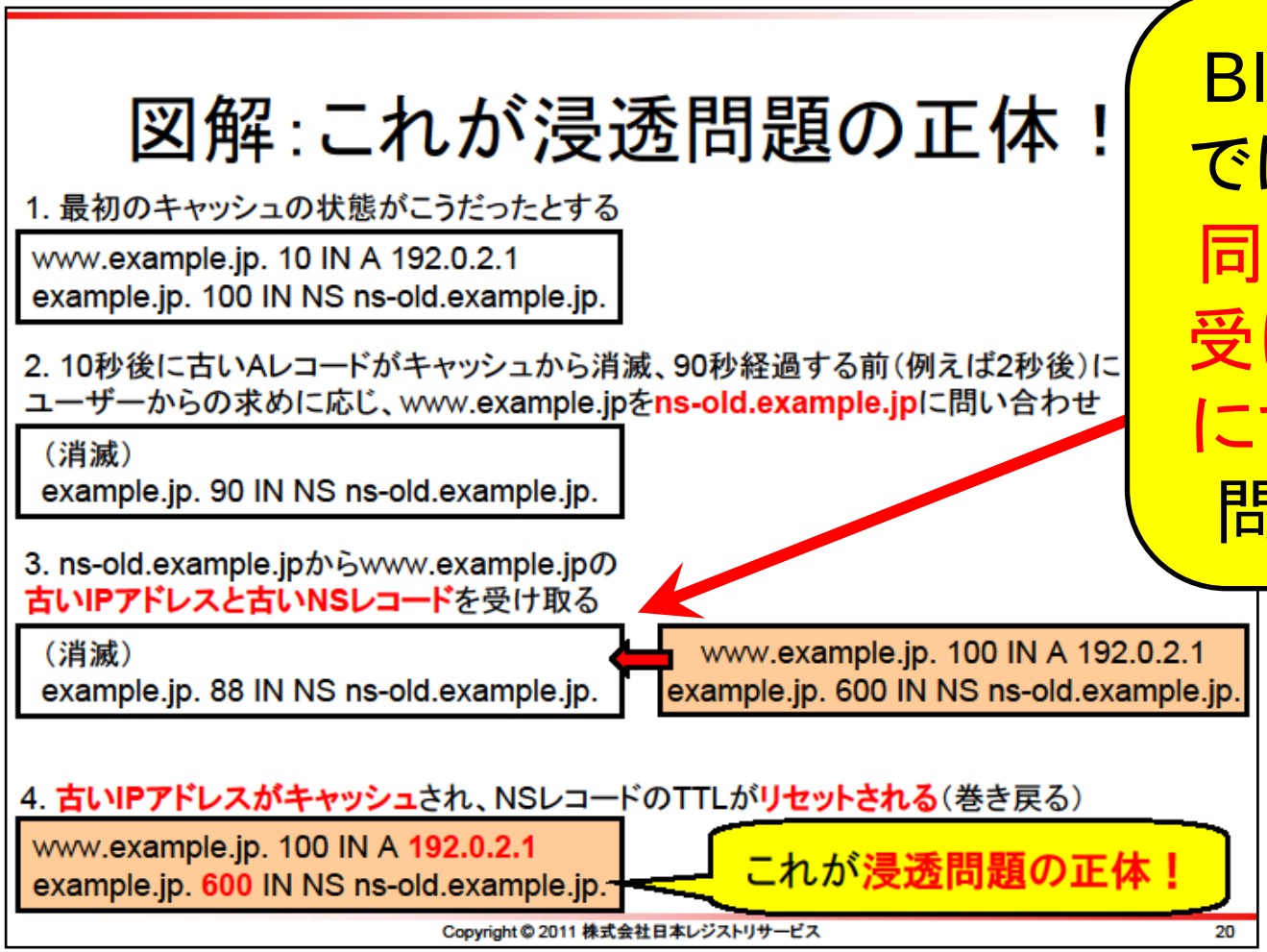
- 浸透問題は9.2.3で対策されたはず
- でも、BIND 9ではつい最近まで幽霊ドメイン名問題が発生していた
  - 9.9.0/9.8.2/9.7.5/9.6-ESV-R6で対策
- 実は、BIND 9の浸透問題対策は不十分だった！
- 浸透問題は対策されていたが、幽霊ドメイン名は残っていた
  - 浸透問題対策をすり抜ける方法で攻撃された
- 実は、幽霊ドメイン名の攻撃方法は次で説明する「浸透妨害攻撃（仮称）」の応用であると言える

「浸透妨害攻撃（仮称）」とは

- 9.2.2までのBIND 9では「浸透妨害攻撃」が成立する
- どんな攻撃方法か？ ⇒実はとてもシンプル！
- 方法：浸透問題を持っている古いBIND 9で動いているキャッシュDNSサーバーに対し、キャッシュから情報が消えるよりも前に、対象となる名前を検索するだけ
- これだけで、古い権威DNSサーバーを使わせ続けるように仕向けることができる
  - 幽霊ドメイン名問題と同じ！
- つまり、古いBIND 9に対し「おかしいな、DNSがまだ浸透しないぞ」と言って名前を引き続けると、いつまでたっても古い情報が残り続けてしまうことになる！
- ナチュラルな攻撃が成立

BIND 9における浸透問題対策

- Internet Week 2011ランチセミナー資料p.20より



BIND 9.2.3以降ではNSの内容が同じだった場合、受け入れないようにすることで浸透問題を回避した

ということで、幽霊ドメイン名の攻撃方法は？

- 「NSレコードの内容（ホスト名）は違うが、NSで指定されているホスト名のA／AAAAレコードの内容（IPアドレス）は同じ」設定を意図的に作成
- 浸透妨害攻撃と同じように攻撃を仕掛ける
  - 対象となる名前を意図的に検索する
- これにより、浸透問題が発生している時と同じ状態を意図的に発生させることができる

ns1.example.jp. 46400 IN A 192.0.2.1
example.jp. 46400 IN NS **ns1**.example.jp.

ns2.example.jp. 86400 IN A 192.0.2.1
example.jp. 86400 IN NS **ns2**.example.jp.

名前（NS）は違うがIPアドレス（A）は同じ！

Unbound/BIND 9における対策

- NSの設定は受け入れるが、TTL値は増やさない（今持っている値よりも大きくしない）
- Unboundのこの対策（1.4.8で実施）はそもそも「浸透問題」に対するものであった
  - Fix so a changed NS RRset does not get moved name stuck on old server, for type NS the TTL is not increased.（ChangeLogより）
- つまり、Unboundの浸透問題対策の方が、かつてのBIND 9の浸透問題対策よりも賢かった
  - 現在のBIND 9はUnboundと同様の対策がされている
- TTLは「キャッシュしてよい時間」なので、この動作はRFCに違反していない

この問題をもっと知りたい

- まずは論文を読みましょう
  - うまく書かれており、平易な英語で読みやすいです

    段海新さんの公式Web: http://netsec.ccert.edu.cn/duanhx/
  - 論文の内容を理解することで、DNSの委任のしくみや関係する諸問題に関する深い理解が得られます
- JPRSの技術文書

  「ghost domain names（幽霊ドメイン名）」脆弱性について

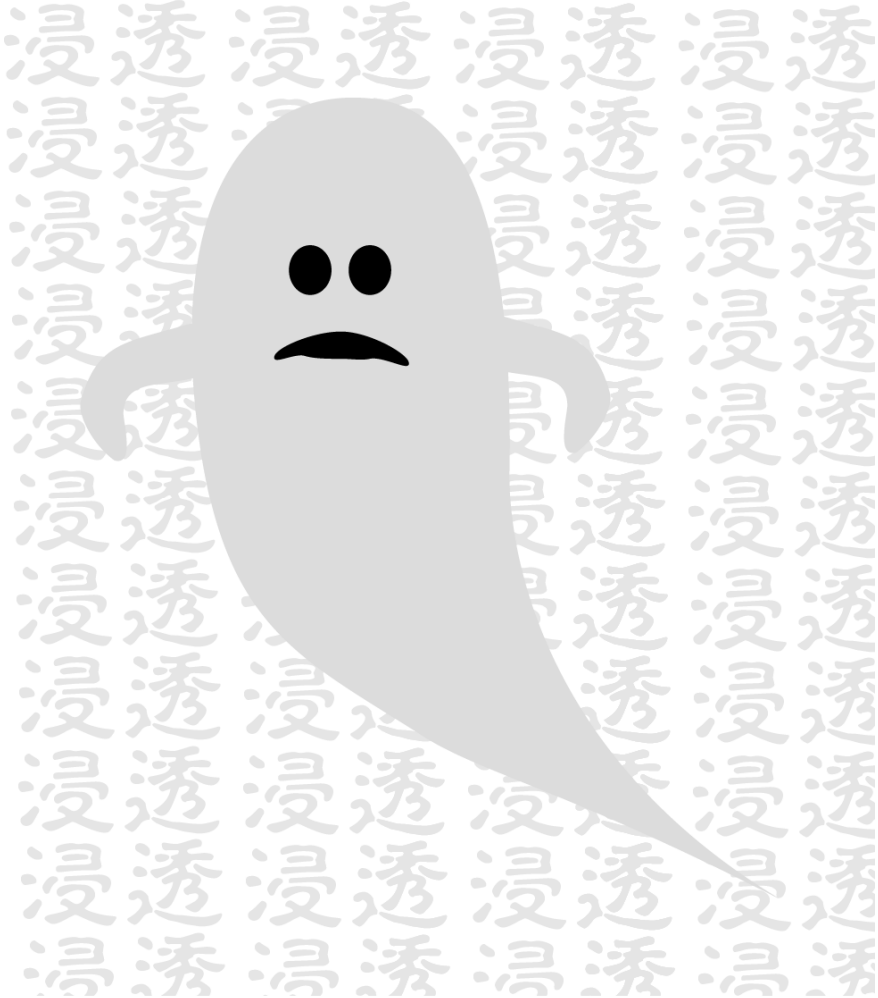
  http://jprs.jp/tech/notice/2012-02-17-ghost-domain-names.html

  （2012年4月5日更新）
- あきみちさんのブログ記事（Geekなページ）

  「DNS浸透問題」は脆弱性だった！「幽霊ドメイン名脆弱性」

  http://www.geekpage.jp/blog/?id=2012/3/21/1

ご清聴ありがとうございました！



©あきみち 2012