Kaminsky Attack 解説と対策 (後編)

DNS DAY ～利用者を守れ！～

Internet Week 2008 DNS DAY

Information Sharing Platform Labs. NTT
Tsuyoshi TOYONO
(toyono@nttv6.net)

目次

- 前編：解説 (民田さん@JPRS)
- 後編：現状と対策 (豊野)
  - 今回の攻撃への対応策
  - 周辺動向
  - 今後の対応

後半：現状と対策

今回の攻撃では どのような脅威があるのか(前半から)

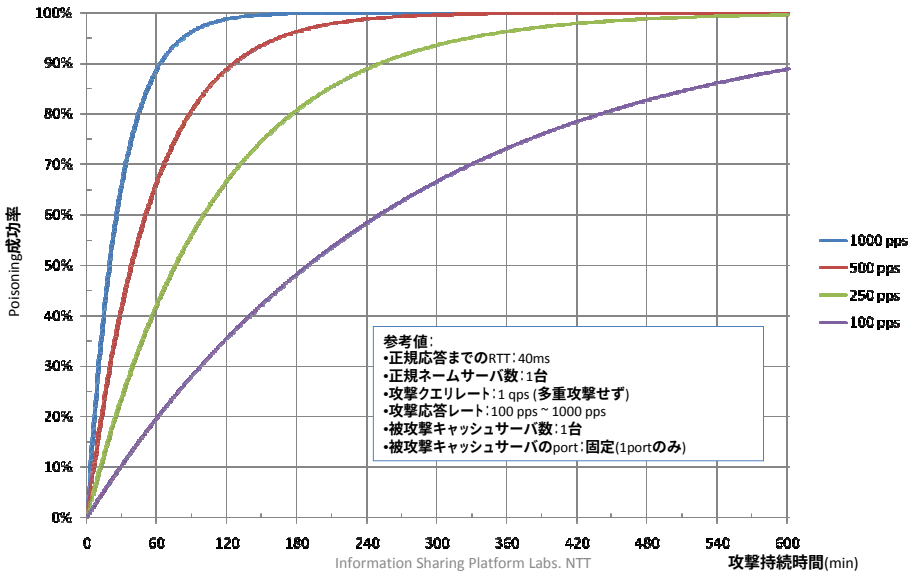
- DNSキャッシュサーバにおいて，ドメイン名が乗っ取られる可能性がある
  - 嘘の応答を正規の応答より先に返すことでDNSキャッシュサーバに偽情報をキャッシュさせる (DNS Cache Poisoning攻撃)
    - 正規応答を横取りするため，キャッシュサーバ(ひいてはユーザ)は正しい情報との判別ができない
- 本来の宛先ドメイン名に対するあらゆる通信を横取り出来てしまう
  - ドメイン名を用いているあらゆるサービスに対するPharmingが可能
  - IPアドレスごと書き換えてしまえるのだから当然何でもアリ
    - サービス不能攻撃
    - 全トラフィック横取り
    - 個人情報，アカウント，パスワードなどの略取
  - 著名サービスのドメイン名が乗っ取られると極めて危険度が高い
    - 証券，金融，銀行系のPharmingなどは直接金銭被害に結びつく可能性も

攻撃の成功率はどのくらいなのか

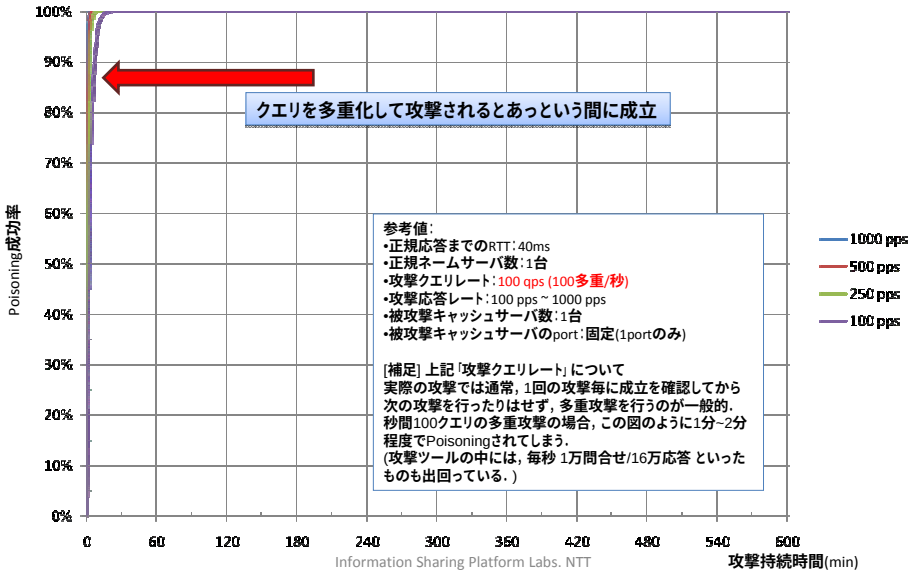
- Cache Poisoning攻撃は以前から知られていたが，今回の攻撃では攻撃間隔が0秒になったのと同じ攻撃が可能になった
  - 今回の攻撃ではキャッシュ記憶時間(正規リソースレコード(RR)の Cache TTL)を無視した連続攻撃が可能
- 仮に「秒間1000回の偽応答」の連続攻撃を許した場合
  - 約19分(1136 秒)で攻撃成功率が50%を超える
  - 約5時間半(271分)で攻撃は必ず成立(100%)
    - 攻撃され続けるとそのドメインは必ず乗っ取られてしまう
  - より高い攻撃レートやマルチスレッドでの攻撃を受ければ数秒程度で Poisoningされてしまうこともある

参考値:
•正規応答までのRTT:40ms
•正規ネームサーバ数:1台
•攻撃クエリレート:1 qps (多重攻撃せず)
•攻撃応答レート:100 pps ~ 1000 pps
•被攻撃キャッシュサーバ数:1台
•被攻撃キャッシュサーバのport:固定(1portのみ)

(参考) 攻撃の成功率の時間推移



(参考) 攻撃の成功率の時間推移



やられています

- AT&T (us)
  - 2008/7/29
  - metasploit blogにて報告
  - 汚染先:広告サイト

http://blog.metasploit.com/2008/07/on-dns-attacks-in-wild-and-journalistic.html

- CNC (cn)
  - 2008/8/21
  - Websense社blogにて報告
  - 汚染先:Malwareダウンロードサイト

http://securitylabs.websense.com/content/Alerts/3163.aspx

現状

- 攻撃に用いられている手法はDNSプロトコル自体のメカニズムに基づいており，根本的に対処する方法が現状のところ存在しない
  - 根本的な解決にはDNSにデジタル署名の認証機構を組み込んだDNSSECを利用するしかないとされるが，まだ実装･普及が不十分

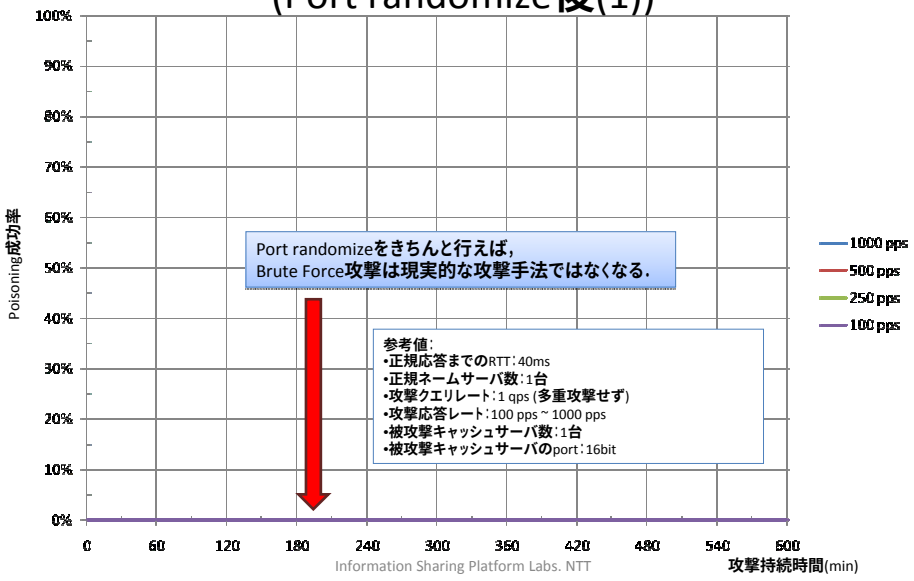
- 攻撃確率を低減する対策を講じる必要はある
  - 各DNSベンダのPatch対応がこれ

今回のPatchの仕組み

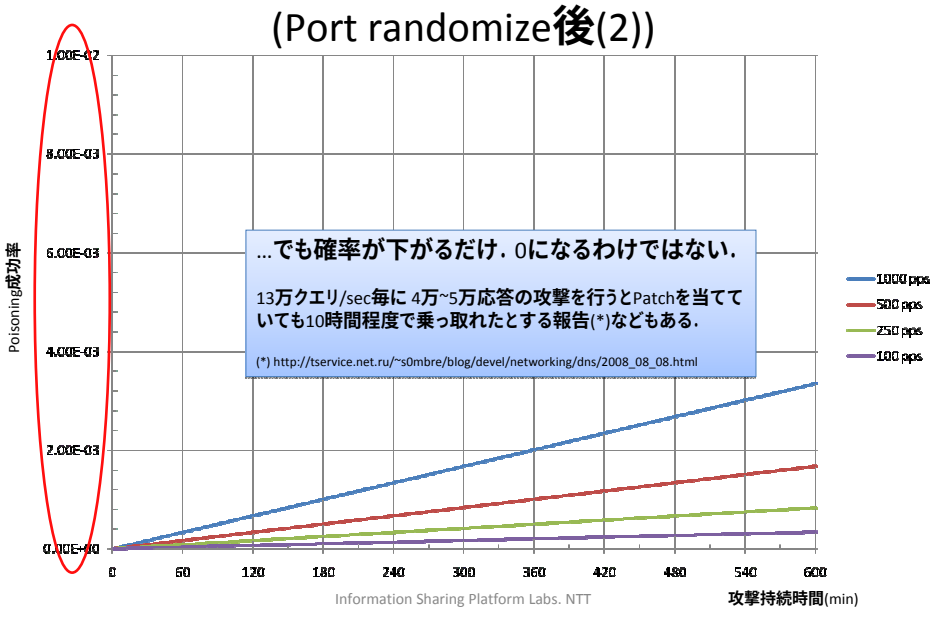
- DNSの問合せsource portをランダム化することで，攻撃を当てづらくする
  - 従来のTXID(16bit) * port番号(16bit)
    = 32bit分のランダム性を確保
    - ざっくり 1/65535 から 1/43億分 へ
    - Brute force 攻撃は「あまり」現実的ではなくなる
  - 対象はCaching serverとResolver(Client)
    - resolver patchもリリースされている(Windowsとか)
    - 攻撃範囲としては狭いが，脅威は同じ

- あくまで確率を下げる対策に過ぎない

(参考) 攻撃の成功率の時間推移
(Port randomize後(1))



(参考) 攻撃の成功率の時間推移
(Port randomize後(2))



キャッシュサーバの対策 (大前提)

- 大前提：今回の脆弱性の対応patch(port randomize)は必ず当てる
  - 自分の運用/利用しているDNS Serverをもう一度確認しましょう

  - 性能に影響するので設備設計から再変更が必要になることも
    - 毎回UDP socketを開き直すので一般的には以前よりパフォーマンスが低下する
      - 2割とか5割とか言われているが，ネットワーク構成や規模によってもかなり異なる
  - 設定を見直す①：Portを固定する設定が入ってしまうと Patchの意味が無い
    - Configでportの固定設定をしていないかどうか注意する
  - 設定を見直す②：NAT配下の場合など，別の機器で portが収束してしまわないように注意する
    - 場合によってはDMZへ収容替えするなどの対処の必要有り
    - ACLやFilteringの設定にも注意する
  - 設定を見直す③：他のdaemonとかも気にしてみる
    - 他のUDP high port利用プログラムとぶつかる事もある
    - 回避設定が組めるDNSソフトウェアも多い(BINDだとoption avoid)

キャッシュサーバの対策 (できること)

- Recursion(Cache応答する)範囲を見直す
  - 今回の攻撃ではクエリを継続して出し続けるため，なるべくクエリ範囲を絞ることが対策として有効
    - 攻撃を受けづらくする/内部ネットワークからのアクセスにのみ応答するよう限定する
    - ただしISP網など第三者が利用するネットワークでは内部利用者がBot感染して攻撃に加担などといった場合もあるので注意
- すなわち…
  - Open Recursion(外部ネットワークへのCache応答)を止める
    - 外部から自由に攻撃されてしまうのは非常に危険
  - Filtering/ACLを書いて応答範囲を制御する
    - Ingress Filteringとかu RPFとかも素敵
  - Authoritativeサーバとキャッシュサーバを分離するのも有効
    - 外部応答する権威サーバとは分けて運用した方が上記管理はしやすい
    - キャッシュサーバのIPアドレスが公開されるのはなるべく避けたい

キャッシュサーバの対策 (まだできること)

- ネームサーバからの単位時間当たりの応答クエリ数を制限する (rate limiting)
  - 通常ならば1つの問い合わせに対して，1つの応答が帰ってくるはず
    - Poisoningを狙われたドメインに対しては大量の偽応答が混じる
  - ただし正常な利用でも多くのトランザクションが発生していることもあり，実際に制限をかける場合は注意が必要
    - 通常でもgTLD, TTLの短いドメイン, サブドメインを多数保有するドメインなどのネームサーバとのトラフィックは多い
- キャッシュサーバ1台当たりの収容ユーザ数を減らす
  - やられた際の被害を最小規模に抑える
  - でもなんとなく後ろ向きな対策っぽい…

ネームサーバの対策 (何かできることはないのか?)

- (自分の管理するドメインに対する)Authoritativeサーバの台数を増やす
  - 正しい応答をする可能性のある(正規)ネームサーバを複数台設定しておくと，攻撃者は台数分の応答を偽造しなければならない
    - 確率低減に過ぎないが，やらないよりはマシか
    - 増やせば手間も増える．Lame delegationなど設定には十分注意したい
- 基本的にAuthoritativeサーバ側で出来ることは無い
  - 今回の攻撃にはTTLの設定も無力
    - 存在しないドメインをランダムに生成して攻撃に使われるので正規TTLを延ばしても効果は薄い
  - 狙われるのは自分のドメインかもしれないけれど実際に攻撃されるのはキャッシュサーバなのが悩ましい
    - 既存キャッシュの上書きがそれほど起こりえないのは救い

Monitoringしよう (1/2)

- **やっぱり攻撃の兆候は検知すべし**
  - UDP portだって資源．DoSで食い潰されたらつらい

- **キャッシュサーバ側で見る**
  - Poisoning「されたかどうか」を確認するのは結構難しい
    - 正当なキャッシュかどうかを判別するのは現状では困難
  - 「狙われているかどうか」は頑張れば監視できる
    - クエリしてもいないのに，返される応答をチェックする
    - 大量の偽応答が来始めたら要注意

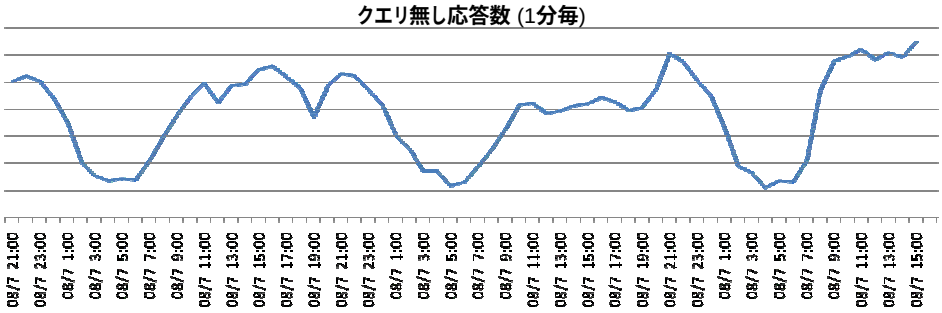
- Authoritativeサーバ側で見られる?
  - dns-operations@dns-oarc などで多少議論中

Monitoringしよう (2/2)

- **キャッシュサーバで「狙われているかどうか」の監視**
  - クエリとAuthoritativeサーバからの応答をマッチさせて，クエリしてもいないのに応答だけが増え始めたら狙われているかも
    - BIND:クエリ無し応答ロギングパッチ
      - http://member.wide.ad.jp/~fujiwara/
    - Vantioにも同じような実装有り
  - 外部検出ツール
    - ISC SIE cache poisoning attempt detection tool
      - https://www.dns-oarc.net/node/141
    - NTT PF研
      - https://www.dns-oarc.net/files/workshop-2008/toyono.pdf

- **より簡単に…**
  - 手法：(UDPがDNS Packetだと仮定して)サーバIFのパケットカウンタのIn/Out値で類推するという手も割と有効
    - UDP In/Outの比率が1：1から大きくずれ始めたらもしかしたら狙われているかも

Monitoringしよう (おまけ)
クエリしてないのに応答するネームサーバたち



案外，定常的に発生している…
- 問い合わせると必ず3発くらいの応答を送ってくる xxx.cnとか
(ロードバランサのバグ?)
- たまに狂ったように数百発の応答を送ってくる xxx.cnとか
(DNSソフトそのもののバグ?)

DNSの危弛化は広く影響を及ぼす

- クライアントにもPatchを
  - クライアントキャッシュもPoisoningの可能性有り
  - 攻撃範囲としては狭いが，脅威は同じ
    - WindowsなどOSはもちろん，DNS機能を有するSOHOルータやAppliance boxも
- WWW以外にもMX, ENUM, ACL, Reputation, Load balancing, ID管理…依存サービスだらけ
  - OpenIDなどの認証系も影響の検討を行っている
    - ドメイン名に依存して認証(をproxyできたり)する部分もあることから検証レポートなどが出されている
- 様々な攻撃手法の高度化
  - 受動型攻撃にも即応用される
    - Web redirectと組み合わせドメイン名を羅列したサイトに誘導…などなど
  - ドメイン名乗っ取りを応用した各種攻撃手法が開発され続ける
    - Web Pharming/Phishing, SPAM, Account Cracking …

さらなる確実性に向けての動き

- より「破られにくい」プロトコルに向けて…
  - しかし，あまりにインターネットの「あらゆる部分」に浸透しすぎていて改変とDeployが大変な面も
- 0x20 dns (大文字小文字変換)
  - DNSでは大文字小文字は区別されないが，サーバで問い合わせるときに故意にランダムにして，エントロピーを今よりも更に増やす
    - 例：FoObAr.com と foobar.com 等を使い分け，正規応答かを精査
    - 主にサーバ周辺の実装改変のみで済みそう
- 各種「エントロピー増やせ増やせ」案
  - 常に2回ずつ聞くとか．TCP Fallbackとか．IPv6 Dual Queryとか．
  - でもそんなことをしたらサーバ負荷も上がる
- DNSCurveとか

DNSSEC !?

- 根本的な解決としてのDNSSEC
  - DNSに公開鍵認証を組込みデータの改ざんを検出できる
  - 普及できればドメインハイジャックは激減する
  - (一応)RFC化が完了している

- 本当に来るのか…?
  - 世界的には動き始めている
    - ICANNはプロポーザル済: 2009年6月までにroot signed
  - でも問題は山積み
    - 世界中のみんなが対処しないと認証Chainがユーザまで広がらない
      - SOHO/dslルータやFirewallなどのAppliance boxもまともな実装をしていない
    - レジストリ/レジストラ/ドメインサービス事業はどうなるのか?
    - 現実的なソフトウェア性能が出るのか？
      - 多数のドメイン名/大きなZoneを抱えるネームサーバの更新は?
      - 大規模なキャッシュサーバは数千クエリ/secを捌きつつ認証を辿れるのか?

まとめ

- 今回のDNSの脆弱性は…
  - 非常に危険で影響力が大きい
  - きちんとしかるべき対応を取る
  - 現在の対策は暫定対処であることを理解しておく
- 今後のDNSは…
  - 新しい攻撃が継続的に生み出される
  - 新しい対策を継続的に行う必要がある
    - いずれDNSSEC, その他大規模なプロトコル拡張が普及してくるかもしれないので注視しておく

参考資料

(参考) 攻撃が成功する確率

$$P_{(t)} = 1 - \left(1 - P_{(S)}\right)^{t \times Rq}$$

$$= 1 - \left(1 - \frac{Rr \times W}{N \times Port \times ID}\right)^{t \times Rq}$$

P(t): **攻撃成功確率**
P(s): 1**回のクエリで攻撃が成功する確率**

t: **攻撃持続時間**
Rr: (1**クエリ当たりの**)**応答攻撃レート**
Rq: **クエリ攻撃レート**
W: **正規応答が帰ってくるまでの**RTT
N: **攻撃対象のレコードを保持するネームサーバ数**
Port: Query port**の数**(**固定**port**の場合**1)
ID: DNS**の**ID (16bit = 65536)

(参考) 参考URI

- Security Alert**や解説**
  - JPRS (**日本語**)
    - http://jprs.jp/tech/security/multiple-dns-vuln-cache-poisoning-update.html
    - http://jpinfo.jp/topics-column/009.pdf
  - JPNIC (**日本語**)
    - http://www.nic.ad.jp/ja/topics/2008/20080709-02.html
  - JPCERT/CC (**日本語**)
    - http://www.jpcert.or.jp/at/2008/at080014.txt
  - NTTv6 (**日本語**)
    - http://www.nttv6.net/files/DKA-20080723.pdf
  - US-CERT
    - http://www.kb.cert.org/vuls/id/800113
  - CVE
    - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447
  - Dan Kaminsky
    - http://www.doxpara.com/DMK_BO2K8.ppt
    - http://www.doxpara.com/?p=1204
  - Steve Friedl's Unixwiz.net
    - http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
- **テストサイト**
  - OARC
    - https://www.dns-oarc.net/oarc/services/dnsentropy
  - Dan Kaminsky's DNS Checker
    - http://www.doxpara.com/
- **分析など**
  - OARC
    - https://www.dns-oarc.net/node/131
    - https://www.dns-oarc.net/oarc/workshop-2008/agenda
  - CERT.at
    - http://cert.at/static/cert.at-0802-DNS-patchanalysis-aug18.pdf