BIG-IP GTM

DNSSEC 機能

F5ネットワークスジャパン株式会社



DNSキャッシュポイズニング攻撃 ~カミンスキー攻撃~

※bank.comは存在するが、01.bank.comは存在しない前提 キャッシュサーバは、キャッシュにない情報 01.bank.com なので、権威サーバにクエリを送信する。 02.bank.com このとき、クエリ毎に異なる、 「トランザクションID(16bit:65536通り)」 0n.bank.com を付与する。 実在しないFQDNを指定して、大量のクエリを生成する。 bank.comの "NXDOMAIN" 権威DNS キャッシュDNSサーバ (=存在しない)を 回答 bank.comの権威DNSのIPアドレスを詐称& 「トランザクションID」をランダム生成し、 ③のDNSリプライを偽装。 さらに、そのリプライに、 「ADDITIONAL SECTION」を含ませることができる。 例: **ANSWER SECTION** 01.bank.com 123 IN A 誘導したいIPアドレス **AUTHORITY SECTION** 権威DNS 123 IN NS 詐称ドメイン(1) 権威DNS 123 IN NS 詐称ドメイン(2) **ADDITIONAL SECTION** 詐称ドメイン(1) 123 IN A 誘導したいIPアドレス キャッシュからの回答を得ることで、攻撃者が指 詐称ドメイン(2) 123 IN A 誘導したいIPアドレス 定したIPアドレスを取得してしまう。

DNSキャッシュポイズニング攻撃 (Cont.) ~カミンスキー攻撃~

■ 正しいDNSリプライかどうかの判断

- キャッシュDNSサーバは、DNSリプライの偽装を防止するために、16ビットのランダムなトランザクションIDを付与して、権威DNSに問合せる(DNSクエリ)。 そして、以下2つを照合することで、正規の回答であることを確認する。
 - 送信したDNSクエリのトランザクションIDとDNSリプライのそれが一致すること
 - 送信したDNSクエリの送信元IPアドレス&ポート宛への応答であること

■ 攻撃方法

- 攻撃者はこの穴をつく。権威DNSのIPアドレスを詐称し、想定できるDNSクエリのポート番号とトランザクションIDをランダムに生成。それらの値で、総当たり (ブルートフォース)で虚偽のDNSリプライを仕掛ける。
- 図中①で行うDNSクエリに、"存在しないFQDN"を使うことで、総当たり攻撃試行チャンスをほぼ無限に増やし、成功確率を圧倒的に高くできる。
- さらに、「ADDITIONAL SECTION」を含ませることで、任意のドメイン/FQDNの組合せをキャッシュさせることができる。
 「ADDITIONAL SECTION」は自由に設定することが可能であるため、さらに広範なドメイン/FQDNの詐称が可能となる。

DNSSECの動作概要 ※DNSSEC対応



BIG-IP GTM

01.bank.com 02.bank.com

0n.bank.com 実在しないFQDNを指定して、 大量のクエリを生成する。

キャッシュサーバは、キャッシュにない情報 なので、権威サーバにクエリを送信する。 このとき、クエリ毎に異なる、 「トランザクションID(16bit:65536通り)」 を付与する。

3(4)(5)

5

DNS

リプライ

ハッシュ値

③ハッシュ関数で、DNSリプライのハッシュ 値を計算

④そのハッシュ値を、権威DNSの秘密鍵で 暗号化=これが電子署名

⑤平文のDNSリプライに電子署名を添付し て、キャッシュDNSサーバへ返答

キャッシュDNSサーバ

(6)(7)(8)(9)

⑥ハッシュ関数で、DNSリプライの ハッシュ値を計算

⑦電子署名を権威DNSの公開鍵で 複合化

⑧これら2つのハッシュ値を比較

⑨比較の結果が同じならキャッシュ

DNS ハッシュ値 リプライ bank.com 権威DNSの <u>ハッシュ値</u>(6) 8 比較 キャッシュ

bank.comの権威DNS

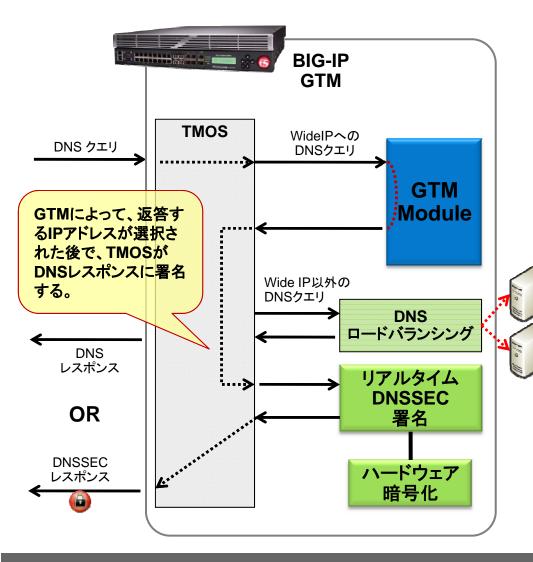
リプライ bank.com 権威DNSの

DNS

(10)

署名を持たないDNSリプライはキャッシュし ない。

リアルタイムDNSSEC



- BIG-IP GTM DNSSEC機能は、DNSレスポンスにリアルタイムにサインして、既存環境に素早く、簡単にDNSSECを展開する方法を提供。
- リアルタイム署名は、ユーザが地球上の様々 なロケーションからリクエストが発生する環境 においては重要である。
- 静的DNSのDNSSECを提供することは、 BINDを使えば、比較的簡単である。
- しかし、特にクラウド展開においては、GSLBタイプの、動的なDNSのDNSSECを提供することは、かなり難しい。
- F5は、GSLB環境で正しく機能する、真の DNSSECソリューションを持つ唯一のGSLBプロバイダーである。
- 他社は、考え得るDNSレスポンス全てに対して、事前に署名するシステムを提案するのに対して、F5は、これが実現可能なアプローチではないと判断した。

